Cyber
Security
for Europe

Stories

The narrative of a European cybersecurity community

This book is the narrative of the work carried out on the CyberSec4Europe pilot project over the course of four frenetic years from 2019 to 2022. It captures the zeitgeist of the creativity, enthusiasm, energy and resilience of the project community of researchers from across Europe in universities, research institutes, SMEs and industry. These are the individuals who successfully collaborated in the relentless pursuit to secure European society's institutions, infrastructure and digital economy and to promote the future cybersecurity agenda.

This then is our story, a collection of short stories, that together is much greater than the sum of its parts.

CyberSec4Europe is funded by the European Union
under the H2020 Programme Grant Agreement No. 830929

Stories

The narrative of a European cybersecurity community

Project Partners

ABI Lab
Archimède Solutions Sàrl
Atos Spain S.A.
Austrian Institute of Technology GmbH (AIT)
BBVA Group
Computer Technology Institute and Press “Diophantus” (CTI)
Comune di Genova
CONCEPTIVITY Sàrl
Consiglio Nazionale delle Ricerche (CNR)
Cybernetica AS
Dawex Systems
Delft University of Technology (TU Delft)
Engineering Ingegneria Informatica S.p.A
Foundation for Research and Technology – Hellas (FORTH)
Goethe University Frankfurt
Informatique Banque Populaire
International Cyber Investigation Training Academy (ICITA)
Intesa Sanpaolo S.p.A.
JAMK University of Applied Sciences
Karlstad University
KU Leuven
Masaryk University
NEC Europe Laboratories GmbH
Norwegian University of Science and Technology (NTNU)
Open & Agile Smart Cities vzw (OASC)
Politecnico di Torino (POLITO)
Siemens AG
SINTEF AS
Technical University of Denmark (DTU)
Timelex
Trust in Digital Life Association (TDL)
University College Dublin
University of Cyprus
University of Luxembourg
University of Malaga
University of Maribor
University of Murcia
University of Piraeus Research Center
University of Porto
University of Trento
University Toulouse III – IRIT
VaF, s.r.o.
VTT Technical Research Centre of Finland Ltd

Contents

All reports in the book can be found at cybersec4europe.eu/our-results/deliverables Each report is referenced by its deliverable number after the title, eg (D0.0).

Common abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
CHECK	Community Hub of Expertise in Cybersecurity Knowledge
CSA	Cyber Security Awareness
DLT	Distributed Ledger Technology
EC	European Commission
ECCC	European Cybersecurity Competence Centre
ECSO	European Cyber Security Organisation
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
eIDAS	electronic Identification, Authentication and Trust Services
ENISA	The European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
IoT	Internet of Things
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
JRC	Joint Research Centre
NCC	National Co-ordination Centres
NISD	Network and Information Systems Directive
OT	Operational Technology
SDL	Software Development Lifecycle
SSI	Self-Sovereign Identity
SWOT	Strength Weakness Opportunity Threat
TEE	Trusted Execution Environment

Kai Rannenburg
Goethe University Frankfurt
and **CyberSec4Europe**
co-ordinator
—
November 2022

The CyberSec4Europe story

About five years ago, the planning for what in spring 2018 became CyberSec4Europe began. At the time we had little idea of the road ahead or the journey we would be going on. Inspired by the call from the European Union on 'Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap', many plans for new structures and concepts to improve the state of things were developed – and amended or even scrapped to agree on the best possible architecture – and to match the call.

CyberSec4Europe formed as a strong consortium of more than 40 participants from 22 Member States and Associated Countries, who aimed to not only strengthen the EU position in cybersecurity but also to enhance the concept of European cybersecurity by keeping it connected with European values like freedom and respect for the individual as well as protection for the most vulnerable, when they most need it.

While consortium building is always a story in itself, the building and disbanding of consortia for this call was special – maybe triggered by the size of the call or by the topic that raised much interest, not least with governments – and some participants sometimes felt like the Town Musicians of Bremen; but that is not a story for this book.

In February 2019, CyberSec4Europe met for the first time as a funded consortium at a kick-off meeting in central Brussels, hosted by the Representation of the State of Hessen to the EU, who supported us splendidly, not only on that occasion but throughout the project. Many of those who came to this first event had not met before, but before long they were discussing ideas and workplans and planning follow-up meetings.

At the same time, the Hessen Representation started to develop a reputation for being the place to be, when another CyberSec4Europe evening event brought together those who shaped the scenery for discourse and exchange. Then Covid-19 kicked in and things needed to go virtual.

It was hard to imagine how under these circumstances all the universities, knowledge institutes, SMEs, associations and major corporations from across Europe would come together and successfully produce 90 public deliverables, publish over 150 peer-reviewed scientific articles as well as organise and participate in innumerable conferences, workshops and summer schools. But we did it, even virtually, until eventually we could have real meetings again!

With the European Cybersecurity Competence Centre (ECCC) and the national competence centres, the EU is building the infrastructure to engage with a broad spectrum of stakeholders working in the sphere of cybersecurity as well as funding the research, development and innovation programmes to support the European cybersecurity agenda for generations to come.

Throughout the lifetime of CyberSec4Europe, we contributed to these goals through collective endeavour and grew together as a community; and, although our project funding ends at the end of 2022, the sense of fellowship and friendship will endure.

The collection of stories in this carefully curated book is not only a record of many years of intensive and dedicated work, but also intended as an inspiration for progress on the long road ahead.

Feedback is invited, as the story of European cybersecurity will not end with the funding of the four ECCC pilots. The conversations will continue!

There is a long list of people who deserve thanks from the world of Brussels, the Member States and of course CyberSec4Europe itself. As often happens in cybersecurity, it may not be advantageous for all of them to be named for their merits, so this list is rather short. For example, Friedhelm Gillessen is an external supporter, without whose advice the project might never have come into being.

Internally the work activity leaders deserve a special mention for keeping things together, and, in the case of this book, especially the communications team at Trust in Digital Life led by David Goodman and Christine Jamieson.

David Goodman
Trust in Digital Life Association
—
November 2022

Introduction

A key aspect of every European research project is engaging with a target audience, in our case the wider cybersecurity community in Europe, to keep them abreast of how the project is faring, what its results are and what its future legacy to European society will become when the project is no more. We approached this by designing a website that initially contained the bare bones of our work plans and ambitions and then gradually expanded its scope to incorporate new activities and connections, including news stories, and even opinion pieces.

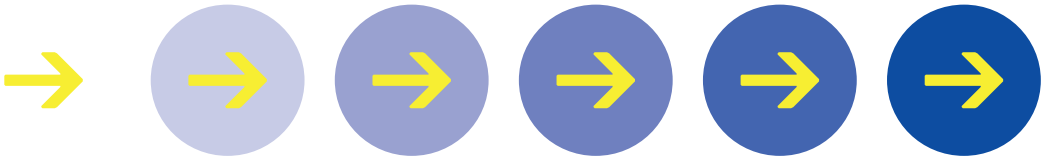
The main goal of the project's dissemination activities was to ensure that the findings of the project, as a whole, reached and engaged key stakeholders effectively. Hence, one of the philosophical underpinnings of our communication activities was to make the results of the project available and accessible to as wide a community as possible, including both technical and non-technical audiences.

Although we published every public report (deliverable) on the website, we asked authors to produce a blog, to illustrate the contents of each document as a news story, both to get the attention of our wider community as well as to make the gist of the work more easily understood to non-technical visitors and to act as an incentive for anyone more interested to explore the original material.

Hence, throughout the lifetime of the project, partner representatives regularly wrote about their work as well as sharing their news and opinions which were published on the website and posted through social media channels to our wider community.

Through these snapshots, this book, *CyberSec4Europe Stories*, captures the life of the project and a glimpse of our proud achievements. Ultimately, the impact of our more than four years' hard work and collaboration in so many different areas from multiple perspectives can only be measured by how much and how well we have told our story to the outside world.

That in a nutshell is the purpose of this book: a summation of all our activities demonstrating the breadth and creativity of the many approaches to advancing the European cybersecurity agenda.



Project timeline

2019		
Kick off meeting		Brussels, 25-26 February
Evening panel	What do stakeholders expect from the Cybersecurity Competence Network Centre pilot projects?	Brussels, 28 February
Evening panel	Keynote and discussion in the context of the Finnish Presidency	Brussels, 4 July
Concertation event	Cybersecurity for Europe 2019	Toulouse, 9-11 November
2020		
Evening panel	Governance and other issues regarding the Cybersecurity Competence Network	Brussels, 24 February
Evening panel	Realising Europe's cybersecurity strengths and capacity for the 2020s	Online, 9 July
Concertation event	CONVERGENCE 2020	Online, 9-11 December
Evening panel	Making a European cybersecurity competence network a reality	Online, 9 December
Webinar	Integrating an ecosystem perspective in cybersecurity standards	18 December
2021		
Training	First Flagship challenge	12-13 January
Webinar	Cybersecurity and standards – how StandICT.eu supports European specialists in the international landscape	29 January
Webinar	Towards more transparent security certifications – mining Common Criteria and FIPS140-2 certificates	19 February
Evening panel	Establishing the Competence Centre in Bucharest and building the network	Online, 24 February
Evening panel	SME cybersecurity resilience in Europe	Online, 5 May
Webinar	Developments in European regulations	17 May
Evening panel	Cross-border data flows: security and privacy issues within the EU and beyond	Online, 6 July
Webinar	Introducing fixed-time cybersecurity evaluation methodology for ICT products (FITCEM/prEN 17640)	17 July
Evening panel	Community perspectives on the future of cybersecurity in Europe	Brussels/online, 18 November
2022		
Training	Second Flagship challenge	25-26 January
Evening panel	Benefits and risks of emerging technologies and the GDPR	Online, 16 February
Concertation event	CONVERGENCE NEXT	Brussels/online, 1-3 June
Workshop	Expectations of the NCCs to the cybersecurity communities	Brussels, 15 September
Evening panel	What can Member States expect from their cybersecurity communities?	Brussels, 15 September
Summit Conference	Momentum!	Brussels, 1-2 December

1

Governance design and pilot

The shaping of CyberSec4Europe's bottom-up approach to governance design for Europe's Cybersecurity Centre and Network was conceptually proposed as a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs), which are envisioned as environments for community-level research, innovation and capacity building in cybersecurity.

Our ultimate goal as a pilot project was to design a governance structure to address the fragmentation of the cybersecurity competence community. Through research and practice, we explored bottom-up governance approaches and came up with the concept of a collaborative network of local cybersecurity hubs, 'Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)', which are envisioned as environments for community-level research, innovation and capacity building in cybersecurity.

To answer stakeholder demands, we combined and collected three inputs: requirements, empirical best practices and stakeholder feedback, bringing them together in an integration phase and then implementing and validating them in a pilot phase. Stakeholder input was key in building an initial governance model, which was later validated and broadened. The larger and possibly complementary or conflicting visions of the stakeholders identified from the pilots, specific developments in diverse Member States and legal analysis of the regulation, as well as a maturity assessment toolbox, were all instrumental in providing recommendations for the second version of the governance model.

Natalia I Kadenko
TU Delft
—
23 February 2020

Designing a governance structure for Europe's cybersecurity community

CyberSec4Europe is offering essential input on the governance structure of the European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Co-ordination Centres. The legislative proposal for the establishment of this body was first published by the European Commission in September 2018 and had its first reading in the European Parliament on 13 March 2019.

One of the tasks of the Competence Centre is to set up and help co-ordinate the national competence centres and the wider cybersecurity community.

The role and the structure of this community, which has been left open for interpretation in the regulation proposal, will be crucial in helping secure the Digital Single Market and increase the EU's autonomy in the area of cybersecurity.

The winter has come, and CyberSec4Europe is working hard on its New Year's gift for the cybersecurity community – the first report on a potential governance structure for Europe's proposed Cybersecurity Competence Centre and Network, setting out the first set of milestones for the goals of CyberSec4Europe by examining best practices and offering a first draft of the possible governance structure.

We are striving to make Europe more secure and more competitive: a global leader in cybersecurity. However, there are still some hurdles to realising this ambitious goal. Insufficient co-operation between Member States, industry and academia is leading to the isolation of research and development, as well as to a skills shortage; insufficient investment is not helping matters either.

The ultimate goal of CyberSec4Europe as a pilot project is to design the governance structure that will answer the main challenges faced in the field of cybersecurity today. Our first report *Governance Structure v1* (D2.1) is the initial milestone in an ongoing examination of the best practices and exploration of governance design. The regulation proposal of the European Commission contains ideas for the governance design, yet a lot of options remain unresolved. The role and the structure of the cybersecurity community, which was left open for interpretation in the regulation proposal, will be crucial due to its potential to resolve issues and help realise the goals outlined above. We are exploring a bottom-up approach, realised through local cybersecurity hubs, as a strategy to answer stakeholder demands and to give a fresh boost to cybersecurity development in Europe.

Christina von Wintzingerode
Goethe-Universität Frankfurt
—
25 January 2021

Fleshing out CyberSec4Europe's governance design for Europe's Cybersecurity Centre and Network

The latest reports from CyberSec4Europe's governance activity provide a maturation of the design ideas and assumptions outlined in the initial draft of the project's proposed governance structure for the Cybersecurity Centre and Network *Governance Structure v1* (D2.1) published in February 2020.

The design combined the top-down approach of the European Commission's proposed regulation with a bottom-up approach that would actively involve greater representation from the cybersecurity community. A key aspect of the new structure was a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs), an environment for community-level research, innovation and capacity building in cybersecurity.

Over the course of the last year, despite the Covid-19 limitations, the process for implementing two prototypes is now well underway in the following regions:

- New Aquitaine, Occitanie and Provence-Alpes-Côte d'Azur (CHECK-T)
- Murcia

The opportunity to observe the implementation process is providing valuable insights on the needs and expectations of stakeholders as well as details, challenges and possible obstacles that will have to be considered for the further development of the CHECK concept.

The latest work has validated some of the basic postulates and assumptions through a series of interviews, clustering and analysis of responses and comparison between different approaches.

We have also continued the development and maturation of the initial design of the governance structure, based on the experience from the test CHECKs, the ongoing examination of best practices and the identification of possible legal issues including the ongoing legislative ratification of the regulation. This significantly includes the development of the concept of CHECKs as a bottom-up element in the future Cybersecurity Competence Network.

David Goodman
Trust in Digital Life
—
30 November 2021

Community perspectives on the future of cybersecurity in Europe

On the evening of 18 November 2021, CyberSec4Europe, with the friendly support of the Representation of the State of Hessen to the EU, hosted a roundtable, at which national cybersecurity community representatives from across Europe shared their experiences, challenges and aspirations for the future of cybersecurity in Europe.

Each Member State has its own set of cybersecurity-related priorities or agenda relevant to the specific strengths of its key sectors, many of which have a common set of challenges. Of particular interest is the degree of connectedness of the communities with each other, both at national and supranational levels, which plays into expectations relating to the governance and decision-making processes of the national co-ordination centres and their relationship with the new European Cybersecurity Competence Centre in Bucharest.

During his welcome address, Mark Weinmeister, Secretary of State for European Affairs of the State of Hessen, observed how Europe was facing a diversity of issues, challenges and opportunities in cybersecurity, and that every Member State, region and municipality has its own approach and priorities. There are incredible opportunities in this diversity and for it to succeed we need a common framework, working together to fulfil the initiatives coming from the EU and the EC.

Following him, we were privileged to have as keynote speaker Miguel González-Sancho, Head of Unit, Cybersecurity Technology and Capacity Building, DG CONNECT, European Commission who is also acting executive director of the Bucharest Centre. Miguel picked up on the two themes of diversity and a common framework, and added a third – priority; all of which added up to what the regulation on the Cybersecurity Competence Centre and Network is about – a governance proposition. Miguel highlighted the three-layer model – the Centre, the national co-ordination centres and the community – and reflected how the regulation was inspired by the wider community and its expertise, and will continue to interact as an information feed for strategic and funding decisions from the top.

The roundtable moderator, David Goodman, Senior Consultant at Trust in Digital Life, invited each of the participants to introduce themselves and briefly share their challenges and expectations in the light of what they'd heard from the keynote speaker.

CyberSec4Europe

Natalia Kadenko is a postdoctoral researcher in Cybersecurity Governance and Disinformation at TU Delft and is leading the project work that is looking at the governance model for the cybersecurity community network.

Italy

Matteo Lucchetti is director of CYBER 4.0, a private-public partnership and one of eight competence centres set up by the Italian ministry, each with their own objectives and mission.

The Netherlands
Eddy Boot is director at dcypher, a collaboration platform for cybersecurity innovation, which is an independent public-private partnership, set up by the Ministry for Economic Affairs and Climate as will be the forthcoming NCCC.

Germany
Christian Mrugalla is Head of Division, International Cybersecurity and Cybersecurity Research at the Federal Ministry of the Interior. In Germany, the NCCC is going to be set up in the public sector (in the BFI) with the collaboration of several stakeholder ministries.

Spain
Juan Díez González, Head of support to research and innovation at INCIBE, the Spanish National Cybersecurity Institute, which is already doing many of the things a NCCC is expected to do.

Greece
Ioannis Alexakis is Head of the Directorate for Cybersecurity Strategic Planning in the General Secretariat of Telecommunications and Posts at the Ministry of Digital Governance.

Norway
Silje Johansen is an advisor at the Norwegian Digitalisation Agency, responsible for following cybersecurity under Digital Europe. Norway is not yet fully associated with the Competence Centre regulation but hopefully it is just a matter of time.

Ireland
James Caffrey is a staff engineer in the Cyber Security & Internet Policy Division in the Department of Environment, Climate and Communication; he pointed out that for many reasons Ireland is Anglocentric and is at home working with third countries, which can be a key challenge in terms of cohesion in a European context.

Having completed the tour de table, the participants addressed a question from the audience on the type of entities that constituted a community.

As the discussion drew to a close, David invited Miguel to sum up his reaction to the points raised by the roundtable participants. Miguel emphasised the structure embodied in the regulation and the way in which this framework could accommodate the wide diversity of experience and expertise across the wider European cybersecurity community.

A longer report and the video recording of the roundtable can be found on the project website.

2

From research to innovation

To address Europe's next generation cybersecurity challenges, CyberSec4Europe conducted research and innovation through technology advancements, supporting both the autonomy of the Digital Single Market as well as addressing the security of the European citizen, as well as Europe's economy and society as a whole.

2.1
Blueprint design and common research

CyberSec4Europe's work focussed on driving and development of the production of prototypes for cybersecurity solutions, products or services, as well as formulating a definition of a common research, development and innovation programme for the next generation of cybersecurity technologies and applications.

Key security and privacy areas

Identity management and authentication solutions over multiple non-federated providers

Security and privacy services to deploy a basic Edge computing platform

Technologies to reduce the system attack surface

Security mechanisms based on trusted execution environments (TEE) and framework for TEE-based cloud data processing

IoT privacy-preserving middleware platform

Improved integrated security and privacy-by-design approaches

Decentralised evidence-based authorisation and distributed access control using blockchain

Approaches that achieve extreme privacy- and integrity-preserving storage and processing of critical data with long-term protection requirements.

Research topics

Privacy-preservation, TEE and IoT-Edge security

Software development lifecycle (SDL)

Security intelligence

Adaptive security

Usable security

Regulatory management

Conformity, validation, certification

Continuous scouting

Impact on society

Our work involved conducting cutting-edge research, development and innovation in diverse areas of cybersecurity and privacy, thereby analysing, devising, implementing and validating cybersecurity components, enablers and assets and their lifecycle.

These components were conceived with a secure-by-design approach and from a usability perspective. In this sense, partners explored the privacy-preserving processing of data and decentralised authorisation and identification mechanisms in trusted execution environments, cloud applications and IoT ecosystems and, in addition, developed solutions for security intelligence, adaptive security and usability – as well as research into investigating the best ways of ensuring software development compliance with the GDPR.

A main project objective was to develop core innovative cybersecurity building blocks, providing pioneering technologies on top of innovative tools to enhance the security and privacy of services. The research we conducted and associate assets we produced scoped in diverse key security and privacy areas (*see sidebar 1*); to achieve this, we structured the diverse research topics accordingly (*see sidebar 2*).

We designed a global high-level functional architecture with the aim of organising the main functional components in a common framework. Common templates, following standardised taxonomies, were also designed to detail the assets in a consistent manner.

To validate the feasibility, effectiveness, novelty, soundness, accuracy and performance of the assets, different tasks defined common scenarios (eg, Smart University Campus) where different partners contextualised and in some cases integrated their assets for joint evaluation and demonstration. These scenarios describe a storyline, processes and test-cases employed to validate the assets implemented.

We devised, produced and evaluated 52 assets, categorised according to the EC's Joint Research Centre (JRC) taxonomy as well as the four main cybersecurity research and area priorities, ie, governance and capacity building, trustworthy ecosystems of systems, trust-building blocks and disruptive emerging development. A Github page was published with complete information (eg, videos, publications) about these assets and their associated research results.

An important number of these assets were also deployed and further evaluated as part of the application demonstrator use cases, marking an important correlation between the assets and real-world requirements.

Given the high amount of demonstrable quality research and innovation outcomes (eg research papers, software assets, videos) and their applicability in real pilots scenarios, we successfully defined how common research, development and innovation could be met in next-generation cybersecurity technologies, applications and services.

Antonio Skarmeta
University of Murcia

—

28 November 2019

Common framework for CyberSec4Europe

Part of the work of CyberSec4Europe is to produce a definition of common research, development and innovation objectives in next generation cybersecurity technologies (including dual-use), applications and services. The project is focusing its cybersecurity research activities on horizontal cybersecurity technologies and cybersecurity in critical sectors (eg, energy, transport, health, finance).

The aim is to provide common research support for the different work activities within the project, especially co-ordinated with the roadmapping and demonstration use case activities, connecting research and innovation with the industrial sectors covered. This first outcome of the work aims to assess the level of originality, detail, sustainability and conformity of the models and results to the CyberSec4Europe vision, providing common ground for their development. The first *Common Framework Handbook* (D3.1) includes the approach followed in CyberSec4Europe to manage the cybersecurity research activities, and to organise the progress behind the building blocks of the CyberSec4Europe ecosystem. It includes the common templates and cybersecurity taxonomies adopted in the project to describe, in a general and interoperable way, the research activities and assets devised, evolved, implemented and tested in the scope of the project.

The common framework also includes a general global architecture, split into different planes, aimed at organising how the different research activities and cybersecurity enablers fit and interact with each other for holistic cybersecurity and privacy management.

The aforementioned research aims are tackled and implemented across different tasks. The cybersecurity and privacy research topics are:

- Privacy-preservation, Trusted Execution Environment (TEE) and IoT Edge security,
- Software Development Lifecycle (SDL)
- Security Intelligence
- Adaptive Security
- Usable Security
- Regulatory Management

A template has been designed, which relies on diverse cybersecurity taxonomies and specifications from NIST, the Joint Research Centre (JRC) and the European Union Agency for Cybersecurity (ENISA) to categorise and describe, in a common and interoperable way, those assets and research activities that are going to be implemented and tested in CyberSec4Europe.

The common framework also includes a general, global CyberSec4Europe functional architecture, intended to organise how different functional building blocks fit and interact with each other for holistic cybersecurity and privacy control and management. The global architecture is divided into different planes and domains and categorises the functional blocks in those planes. The functional blocks in the architecture are also analysed by the research activities across different project tasks.

The *Common Framework Handbook* (D3.1) is available on the website.

Stephan Krenn
Austrian Institute
of Technology GmbH

—

28 November 2019

Identifying cross-sector enablers for privacy and cybersecurity

Cross-Sectoral Cybersecurity Building Blocks (D3.2) aims to identify both the generic and cross-sectoral enablers for privacy and cybersecurity, as well as the research challenges for common technologies in these domains. The report focuses on a variety of building blocks and assets that already exist within the CyberSec4Europe consortium, explaining how they can be used in the demonstration use cases, and identifying the initial research challenges.

In order to address Europe's next generation cybersecurity challenges, CyberSec4Europe is conducting research and innovation through technology advancements, supporting both the autonomy of the Digital Single Market as well as addressing the security of the European citizen, European industry, as well as Europe's economy and society as a whole. Specifically, the project is developing and implementing security and privacy enablers with a special focus on the following eight domains:

- Identity management and authentication solutions over multiple non-federated providers, with a special focus on user privacy while still giving high authenticity guarantees to the relying party;
- Security and privacy services for Edge computing platforms;
- Technologies to reduce the system attack surface;
- Security mechanisms based on trusted execution environments (TEE) and frameworks for TEE-based cloud data processing;
- Privacy-preserving middleware for the Internet of Things (IoT);
- Security and privacy-by-design approaches
- Decentralised, evidence-based authorisation and distributed access control using blockchains;
- Long-term privacy- and integrity-preserving storage and processing of critical data.

The document gives an overview of cybersecurity building blocks that have already been developed or are currently under development within the consortium. It catalogues a variety of cross-domain tools and technologies that solve specific cybersecurity challenges that occur in different application scenarios and that are flexible enough to be adapted for different needs.

By presenting technological building blocks, mapping them to a unified privacy architecture, and identifying open research challenges from the industrial demonstration use cases, the document is a connecting link between actual research, research roadmap design and the demonstration use cases themselves.

Davy Preuveneers
KU Leuven
—
9 January 2020

Research challenges and requirements to manage digital evidence

The goal of CyberSec4Europe's work on security intelligence is to analyse and research new threat detection, security intelligence and data analytic techniques to strengthen the security and privacy capabilities of cybersecurity applications in various vertical domains and use cases.

The key topics addressed can be summarised as follows:

- Mechanisms to share digital evidence
- Threat intelligence information systems and services
- Interoperability in privacy requirements and regulation
- Threat detection and security analytics
- Security intelligence in defensive systems

The work to date lists the relevant components, algorithms and software building blocks from the project partners that can help address these requirements. As these assets are at different levels of maturity, the forthcoming report will describe ongoing research tracks addressing the challenges and requirements to manage digital evidence:

- Lack of trust in the way threat intelligence information is handled by receiving parties is a key factor as to why organisations are reluctant to share information.
- The quality (rather than the quantity) of threat feeds and events must increase for a reliable and automated threat analysis and mitigation.
- The event-based sharing philosophy of threat intelligence platforms does not match well with data-driven and AI-powered threat intelligence.
- The application of security techniques – such as end-to-end encryption, onion routing etc – makes it harder to harvest security intelligence from monitoring data and event logs to detect new threats.
- The AI capabilities of contemporary threat intelligence platforms enable new kinds of attacks that allow adversaries to learn how to evade detection
- Machine learning models that underpin threat detection solutions may leak sensitive information and need strong protection to avoid privacy concerns or loss of reputation.

These research challenges and requirements will be the main drivers to enhance existing assets and develop new ones within the framework of this task to bridge the gap with the current state-of-practice and to increase technological readiness for the first set of demonstrator use cases.

More information on the ongoing results and outcomes of the task can be found in the CyberSec4Europe report *Research challenges and requirements to manage digital evidence* (D3.3).

Kimmo Halunen
VTT Technical Research
Centre of Finland Ltd

—

20 January 2020

Security, privacy and usability – can we have them all?

Even the best security and privacy solutions will be effective only if they can be used by end-users correctly and without undue hindrance to the main tasks at hand. Thus, it is important to see what effective measures there are to improve the usability of security and privacy technologies and which security and privacy technologies have (and have not) gained user adoption.

In CyberSec4Europe we have collected a variety of different methods and lessons learnt into a report that considers the problems related to combining security, privacy and usability. There are still many open research questions and even trade-offs between these three features that seem necessary today. We hope that in the future we can solve many of these and that usability will be taken more into account when developing new technologies and digital services.

Here are four recommendations that we found in our research. Adopting these measures should improve the security, privacy and usability of products and services.

1. Use of authenticated encryption in application layer or network layer communications whenever possible

The use of authenticated encryption protects both the integrity of the communications as well as the privacy of the content. There are many available tools for developers and website administrators to achieve this. The impact to end-users is minimal when this is done correctly.

2. Early user involvement should be ensured for new security and privacy features

User-centred design (UCD) approaches advocate the involvement of end-users in the early stages of the development process (eg, via brainstorming sessions and work analysis). User interfaces and user interactions that are the front end of security and privacy mechanisms should follow UCD processes to ensure that usability is considered from the very beginning and not ‘too little, too late’.

3. User modelling and/or user tests should be conducted for new security and privacy features

Collecting the information on users is not a straightforward task and both automated and other approaches have their shortcomings. However, it is not possible to improve the usability of new privacy and security technologies if no effort to that end is made. Thus, there should be some way to test and/or model users and their behaviour in the security and privacy systems.

4. Provide users with authentication methods that are both secure and privacy-friendly

User authentication is a security measure that is most visible to users in many cases. There are many options to do this and, at the moment, convenience and user experience seem to push towards the use of biometrics. It should be possible to conduct user authentication in a usable way while meeting security objectives and respecting users’ privacy.

Even if all the above recommendations are adopted, there are still many peculiarities in each use case and scenario, where security and privacy need to be protected. Furthermore, the way people use their devices and digital services and conduct their lives both online and offline is changing at a rapid pace. This means that solutions applicable today might be obsolete tomorrow. Re-evaluation of different methods and their impact on usability is therefore a must.

Future research at the crossroads of security, privacy and usability needs to consider many questions. What are the best ways to bring new security and privacy features more easily to developers of new technologies and services? How to solve user authentication and digital identity problems in a way that is usable, and also provides the necessary levels of security and privacy? We hope that activities through pro-active collaboration between researchers from different backgrounds will provide solutions to these and even more. An open networking approach as exemplified by CyberSec4Europe is an excellent way to work towards these.

Marko Hölbl
University of Maribor
—
30 January 2020

Helping Europe become GDPR compliant

The General Data Protection Regulation (GDPR) is the most significant change in data privacy legislation for over twenty years. At the same time, it also presents a complicated list of requirements that can be a major challenge for all organisations but especially for small and medium-sized enterprises (SMEs).

Taking all its requirements into consideration, businesses are finding ensuring GDPR compliance challenging. The requirements are at times either too vague or too open and therefore subject to interpretation, which is where businesses struggle with their compliance endeavours.

As part of CyberSec4Europe, we have established GDPR guidelines to help alleviate the challenges regarding the adoption of and compliance with the GDPR. These guidelines are a synthesis and combination of requirements from the GDPR, European Data Protection Board (EDPB) guidelines, frameworks and up-to-date standards relating to data privacy protection in the European Union.

The guidelines, which include the WP29 Guidelines endorsed by the EDPB, follow the latest standards, methods and frameworks for risk analysis and include a simple-to-follow methodology that was objectified to the largest possible extent. By following these guidelines, data controllers and processors can either execute a data protection impact assessment or use a step-by-step set of recommendations for GDPR compliance.

Our report combines and summarises known guidelines and opinions in the form of an actionable to-do list, supported by integrated checklists and concrete guidelines with explanations. It presents a baseline of identified risk to conduct threat analysis during a data protection impact assessment and an easy-to-follow set of instructions when additional information is needed to explain decisions taken.

It also includes documentation of the analysis process as well as the required data protection officer consultation template and an optional self-assessment template. However, the document does not replace the need to understand the GDPR requirements.

During our research, we identified many issues with regulatory harmonisation in the field of privacy in the EU which led us to design a questionnaire to collect information about additional privacy requirements across Member States. Please note that the specific requirements for Member States were briefly addressed in the report and the results only reflect the needs of the Member States (and countries in the European Economic Area) that we received replies from.

Preliminary results show that, currently, service providers and producers cannot avoid market segmentation due to differences in regulatory requirements. An example of this is the different minimum age required for consent across different Member States. Businesses have to understand the local requirements of every Member State in order to be able to adapt to local requirements.

Alessandro Sforzin
NEC Laboratories Europe GmbH
—
1 February 2021

Securing software with privacy-preserving enablers

The right to privacy is one of the fundamental rights included in more than a hundred national constitutions. It sets boundaries that protect individuals from external interference. The debate around privacy has gained traction since Edward Snowden's revelations about governmental mass surveillance programmes and, more recently, with the advent of artificial intelligence and data mining.

In this context, the term privacy-by-design broadly refers to the application of data protection best practices to system design. It is based on the idea that building privacy into a product or a service from the beginning of the design process is preferable to the alternative of adding privacy on top of an already existing system as an afterthought. Similarly, privacy-by-default designates a situation where the default settings in a product or a service provide the user with protection against privacy risks by themselves, without the need for any additional configuration or other changes.

These principles mandate stating clearly:

- the purposes for which data is being processed (purpose specification)
- the limitations on what data can be collected (collection limitation)
- the minimisation of the collected data (data minimisation)
- the limitations on use, retention, and disclosure of the data
- the notion that there should be a presumption of privacy, meaning that the default settings should provide the best possible privacy protection for users.

These are all issues that are still subjects of debate today in political and research circles.

CyberSec4Europe's report, *'Definition of Privacy by Design and Privacy Preserving Enablers* (D3.11), focuses on privacy. It defines a set of challenges in today's research, presented as three broad categories: data privacy challenges, identity privacy challenges, and legal and development challenges. These are open problems that CyberSec4Europe's enablers want to address over the course of the project's lifetime.

The document begins by presenting CyberSec4Europe's privacy-preserving enablers and privacy-preserving architecture, of which the enablers are critical components, and also comprises detailed explanations of the privacy-preserving enablers' functionalities.

This is followed by a three-part discussion of their relationship to the project's core research and development work; namely, its relation to the lines of research, its place within the research roadmap and how the demonstrator use cases could leverage their functionalities.

Therefore, this document is of interest to anyone looking for an overview of CyberSec4Europe's portfolio of privacy-preserving technologies, as well as the project's plans to address today's privacy research challenges.

This work is especially important today because privacy is at the centre of a convoluted debate. There are governments and corporations that harvest user data indiscriminately, using national security and "services tailored to your needs" as justification. These practices gained support by leveraging users' psychological state, such as their fear of terrorist attacks, or the comfort of using a recommended system. But as time goes by, they are increasingly perceived as dubious at best, and against human rights at worst.

And then there are those users who are worried about being tracked. Because of such users' protests, organisations are being scrutinised more than ever for adherence to privacy rules, with consequences for their public image if they are found guilty of breaching their users' privacy or lacking adequate data security protocols.

Perhaps the biggest obstacle to attaining a satisfying conclusion to this debate is the myth that privacy and usability are mutually exclusive. The strategy of today's software is to shower users with security warnings and pop-ups – often full of technical jargon – whenever there is a security incident. Through lack of understanding or patience to wade through what they've been bombarded with, users more often than not respond by ignoring the warnings, closing the pop-ups and carrying on. Therefore, it is crucial that researchers and industry leaders collaborate to create software that prevents such incidents altogether, while providing users with the simplest and most direct way to achieve their goals, with actions that are designed to preserve the privacy and security of their data.

Cross-border regulations, such as the GDPR, are important steps to further promoting best practices and shielding users from malicious third parties; but they are a complement to secure software, not a substitute. Together with increasing efforts to educate users on the steps they can take to secure their data, such measures could lead to a future in which everyone's online well-being is secured.

Marko Hölbl and
Marko Kompara
University of Maribor

—

9 September 2021

Heterogeneity of data protection legislation across the EU

The European Union (EU) wanted to unify and limit or at least ensure the proportionate use and adequate protection of personal data through the General Data Protection Regulation (GDPR) across all Member States. We took a brief look at how personal data protection legislation differs across the EU.

The report *Analysis of interoperability and cross-border compliance* (D3.18) addresses issues related to different eIDAS and GDPR implementations and legislation differences in EU Member States that will ultimately hamper the fulfilment of the Digital Single Market in Europe. The GDPR allows Member States to define or change some parts of the regulation in ways they choose. The prime example of this is the age of consent, which in the GDPR is 16 (persons aged 16 years and older do not require parental consent).

However, the regulation allows individual countries to change this and go as low as 13 years old. Member States can also have additional legislation that builds on top of the GDPR.

To this end, we performed a survey, where we asked National Supervisory Authorities (NSAs) from each Member State to fill in some information regarding current legislation in their own countries. The information-gathering was centred around different forms of data (eg, biometrics) and upgrading the GDPR requirement in separate national legislations. Data collected includes the following information on the legislation in each specific Member State:

1. Any other legislation on the use of biometrics (other than the GDPR).
2. Any other specific legislation on privacy, specifically with relation to:
    a. Video surveillance,
    b. Photography,
    c. Anonymisation,
    d. Pseudonymisation, and/or
    e. Audit trails.
3. Any additional legislation that extends specific sections of the GDPR, specifically with relation to:
    a. Verification of parental consent,
    b. Processing data of the deceased,
    c. Processing of genetic data,
    d. Use of biometric data for the purpose of identification,
    e. Processing of health data,
    f. Processing of data on the sex life of individuals,
    g. Processing of data on sexual orientation,
    h. Erasure of personal data,
    i. Data protection officer designation/appointment, and/or
    j. NSA consultations
4. Any additional legislation on backing up of data.
5. Whether or not the use of biometrics is allowed for the electronic acquisition of handwritten signatures.
6. Whether or not the use of biometrics is allowed in a work environment (eg, opening of server rooms with a fingerprint).
7. Minimum consent age of persons without requiring consent from a holder of parental responsibility.

We had previously also tried to collect the same data from DPOs (data protection officers) and other project partner employees working closely and/or familiar with the GDPR. However, the results were very inconsistent. We received a wide variance in the feedback from the same Member State. This was an obvious problem and an indication that asking people, even those working with the GDPR, will provide inconsistent data, and it would be difficult for us to recognise which feedback was accurate. This is the main reason we chose to change our approach and ask NSAs for their feedback, even knowing that we would not be able to get every NSA to respond to our queries.

In the survey, we managed to get feedback from 19 of the 27 Member States (Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Germany, Hungary, Latvia, Luxembourg, Malta, Poland, Romania, Slovakia, Slovenia and Spain). The responses were collected between April 2020 and May 2021 in many repeated solicitations of NSAs to participate in the survey.

The feedback was combined into a map of Europe containing the collected data from the NSAs. This interactive map can be viewed on the CyberSec4Europe website.

The map allows a quick overview of the data collected, where a country coloured yellow indicates that a Member State has a particular rule or legislation, and coloured blue means they do not. You can move between topics by selecting the topic under the map. The topics of additional legislation and extending the GDPR are a little different in that the colour of the map only tells us if there is any addition or extension: for further details, you have to hover over the Member State for which you wish to know more.

The results show that in the majority of cases Member States do not have additional/specific legislation (topics marked from 1 to 4). The areas of processing genetic data, using biometric data for the purpose of identification, and processing of health data appear to be the topics that are most often additionally covered with legislation other than the GDPR.

Luxemburg and Malta are the only countries that do not have any additional legislation on the topics covered in our survey, while all the other Member States that responded have at least one topic where they have other/additional legislation to the GDPR.

Based on the feedback from the NSAs, the most additional legislations relevant to the discussed topics are in Finland (15 green fields in topics from 1 to 4, from possible 17), Spain (14), Hungary (12), Germany (11) and Latvia (11). The use of biometrics for the electronic acquisition of handwritten signatures is allowed in 10 of the 19 countries – so a very even split, while only a handful of Member States do not allow the use of biometrics in a work environment (Germany, Malta, Slovakia, and Slovenia).

The conclusion of the research is that the GDPR is not really a unifying factor for compliance on personal data protection across the EU, but it is more the core or minimum standard that has to be reached in all Member States. However, for compliance in at least the majority of the countries, there are many more i's to dot and t's to cross before full compliance can be achieved.

Antonio Skarmeta
University of Murcia

—

11 October 2021

A new edition of the Common Framework Handbook (D3.12)

CyberSec4Europe is a project which aims to lead the next generation of challenges and innovations related to cybersecurity.

In particular, it wants to strengthen the research and innovative competencies and capacities at the national and European level. It comprises public and private research centres and universities, whose collaboration will help to investigate the needs of the present in order to devise competitive solutions for the future. Our latest document is the second version of the *Handbook*, previously published in October 2019.

To meet these project needs, one of the key activities is to research, design and implement cybersecurity components and their lifecycle. These components are conceived with a secure-by-design approach and from a user's usability perspective. In the report, partners explore privacy-preserving processing of data and decentralised authorisation and identification mechanisms in trusted execution environments, cloud applications and IoT ecosystems.

In addition, the project leads towards solutions for security intelligence, adaptive security and usability. Another aspect of this research is related to regulatory management in which partners are investigating the best ways to ensure software development compliance with the GDPR. The project's cybersecurity research activities focus on horizontal technologies and critical sectors (most of them identified in the demonstrator use cases).

Our work defines common research, development and innovation, especially co-ordinated with the roadmapping and use case activities and thus connecting innovation with the different demonstrations and sectors.

As part of this report an update of the common framework has been defined. The common framework proposed a global architecture to encompass the functional components that address the cybersecurity research goals previously identified. This architecture is composed of three planes that provide the intelligence and dynamic reaction to the framework. There are two different domains, one for the user of the framework, the other related to the infrastructure – both physical or virtual. A blockchain layer provides the capabilities of provenance, auditability and accountability to the framework. Each of these planes, domains and layers holds the functional components required to manage, control and analyse the managed domain. The functional components are instantiated by diverse enablers, tools, APIs, models and interfaces.

This *Handbook* aims to describe the collaborative approach followed in CyberSec4Europe to unify, organise and manage the research activities as well as their evolution and development within this project. It presents the evolution of the collection of assets, the brief modifications done in the common framework to describe this progress, and the synergies among the assets in different ecosystems and environments. In particular, the collaboration between the research and innovation with the project demonstrators is elaborated upon in this new *Handbook*.

Massimo Guarascio and **Giuseppe Manco**, Consiglio Nazionale delle Richerche, Italy

—

2 November 2021

The CTI landscape: limitations and opportunities

Sharing threat events and indicators of compromise (IoCs), such as the source IP address of an attack, the hash of a malicious executable file or the URL of a phishing website, enables quick and crucial decisions to be made in relation to effective countermeasures against cyber attacks.

Cyber threat intelligence (CTI) platforms are widely considered to be valuable tools for easing the management of threat information: these solutions allow organisations to easily handle the whole process of gathering, pre-processing, enriching, correlating, analysing and sharing threat events and associated data.

However, the current platforms do not allow easy communication and knowledge sharing among threat detection systems (TDS) which exploit machine learning capabilities. Privacy and trust in the shared information are further examples of the open challenges in defining a fully operational platform. Moreover, the lack of standards and solid approaches have resulted in different combinations of products and methodologies (sometimes erroneously) labelled as threat intelligence.

Finally, the situation is further exacerbated by some specific challenges when artificial intelligence (AI) technologies have to be integrated:

- The quality of threat feeds and events is not guaranteed and there is a need for a reliable and automated threat analysis and mitigation which is particularly problematic for AI-based intrusion detection systems (IDS), typically affected by high false alarm rates (FAR);
- The event-based sharing philosophy of threat intelligence platforms does not match well with data-driven and AI-powered threat intelligence.

Designing and developing a versatile and comprehensive framework

CyberSec4Europe's research activities have sought to address these challenges by defining a comprehensive platform for information sharing and awareness, capable of providing privacy-preserving key information about the threats suffered by a monitored system such as a computer network.

The developed prototype has the twofold objective of:

- improving the accuracy of TDS in detecting incoming attacks by exploiting threat information gathered from different sources (for example, honeypots); and
- enabling the sharing of reliable and relevant threat information and threat detection algorithms among organisations in a confidential and privacy-preserving manner.

Platform components

The devised solution integrates and enables the communication of several tools developed by the project partners focused on addressing the above-mentioned challenges. IDS based on machine learning and deep learning, privacy-preserving and encryption technologies as well as methods for estimating the risk of compromise are just some examples of the components co-operating to improve the degree of security of the organisations belonging to the network.

Application scenarios

To demonstrate the potential of the developed prototype, three relevant use cases concerning the co-operation of TDS and other cybersecurity tools have been set up.

The main idea involves highlighting how the co-operation can:

- improve the performance of the threat prevention and detection systems and minimise the attack surface by strengthening the robustness of machine learning and deep learning models, making them more robust to new threats, false positives and lowering the time to threat detection; and
- enable more robust threat intelligence by allowing a better contextualisation of threat data and devising of flexible strategies, methodologies and data formats for collaborative threat intelligence.

Sharing CTI in a confidential and privacy-preserving manner

The focus of the first scenario is on the sharing of CTI within and across communities, as this is a key enabler for co-operation between threat intelligence services and triggering the deployment of adaptive honeypots. By sharing CTI, other stakeholders or systems can leverage the shared information and collaborate to further analyse the data, increase confidence in the shared intelligence or to augment it with additional information, such as the reputation and trustworthiness of the reporting entities.

Enriching the information on detected threats via TDS co-operation gathered by means of honeypot instances

The main idea consists in enriching the information on detected threats with further details provided by different TDSs, several of which belong to the co-operation network sharing data on detected cyber attacks. Moreover, a honeynet allows for gathering further attack instances which will be used in the learning phase of the AI-based TDSs to improve their effectiveness.

Adaptive deployment

Gathering relevant information on attack strategies and sharing precious IoCs to improve the degree of security of the entities belonging to a co-operation network is the main objective of this use case. The scenario aims at demonstrating how internal information gathered by means of a pool of honeypots can be used in the context of the security of an infrastructure.

You can read more about this work in our report *Co-operation with Threat Intelligence Services for deploying adaptive honeypots* (D3.14)

João Resende
University of Porto (C3P)

—

18 January 2022

Proactive approaches for secure software development

The CyberSec4Europe report, *Proactive approaches for software development* (D3.15), presents a total of 13 assets that support different activities in the lifecycle of software. They address the current research challenges in terms of security and privacy for a number of key topics:

- Policy-based security management,
- Security modelling,
- Risk analysis/assessment,
- Certification security product and security enforcement, and
- Smart security/privacy-preserving tools.

The report is the work of the software development lifecycle (SDL) task and also references the smart cities demonstrator use case.

The demonstrator is based on a common scenario of a smart city platform featuring some of the security challenges typical of such platforms described above, with a special focus on the notion of cloud-based IoT applications that receive, analyse and manage data in real-time to help municipalities, businesses and citizens make decisions that improve the quality of their lives. Citizens engage with smart city ecosystems in a variety of ways, using smartphones and mobile devices. Pairing devices and data with a city's infrastructure and physical services can reduce costs and improve sustainability. Communities can improve energy distribution, optimise garbage collections, reduce traffic congestion and even improve air quality with the help of the IoT. All these challenges require software techniques that are significantly enhanced by improving the overall security of the devices.

The SDL demonstrator shows how security and privacy aspects in the software lifecycle can be effectively and proactively addressed with the support of automated instruments. The report focuses mainly on how these assets are integrated in a common IoT scenario, providing an understanding of the different components inside each category and how they can co-operate to improve software development.

Each asset covers a specific building-block of the global architecture and is used as follows:

- SEMCO: to model the high-level architecture and define security requirements and design patterns against common threats.
- Modssl-hmac and HoneyGen: to ensure privacy of passwords in the authentication system.
- Hermes and VTPin: to detect weak points to make the system resilient to attacks.
- PLEAK: to analyse potential privacy leaks in the data flows.
- SOBEK: to ensure security enforcement of user privacy location policies on their Android phones.
- PVS: to verify the protocols used in device-to-device communications such as 5GAKA.
- CORAS, BOWTIE++ and RISQFLAN: to model and assess security risks in traffic sensors and control.
- SYSVER and VEREFOO: to guarantee correct and efficient implementation and configuration of network security policies.

In the report each asset is described in detail with:

- a general overview of its functionality,
- a demonstration showing how the asset can be effectively applied in the smart cities scenario,
- a summary of the research challenges addressed by the asset, and
- a description of future research opportunities.

A set of companion videos for each asset can be found on the project website.

The report presents proactive approaches for secure software development, demonstrating the complementary activities of the 13 assets to the lifecycle of software, each one stemming from the need to address the security and privacy challenges identified in the report *Research challenges and requirements for secure software development* (D3.9) and practically demonstrating the necessary building blocks to address those challenges in the software development lifecycle.

In summary, this document provides a complete overview of CyberSec4Europe's secure software development technologies and their importance in the context of smart cities.

Outi-Marja Latvala
VTT Technical Research Centre of Finland Ltd
—
26 January 2022

Advances in usable security

Confidentiality, integrity and availability are the three major building blocks of security, collectively known as the CIA triad. In day-to-day life, they are necessary but insufficient qualities for a secure system: we need to supplement the CIA triad with usability, because the vast majority of end-users will refuse to use a product or service that is too difficult or makes the main objective harder to achieve when compared to the unsecured alternative.

CyberSec4Europe's report *Security Requirements and Risk Conceptualization* (D3.16) compiles the results of our research on the intersection of security and usability. It explores several usability solutions that are motivated by the need to empower users to make sensible security choices. The research also explores methods of how to advise or convince users on different security solutions such as authentication methods or privacy settings, and how to make visible the underlying structures such as security policies or cryptographic protocols.

We organised the research results under three main themes: data privacy and protection, solutions for fulfilling security requirements, and analysing and illuminating security for the benefit of users.

First, processing of personal data is a necessary step in many modern services. From the point of view of businesses, it is important to comply with regulations, eg, the General Data Protection Regulation (GDPR). From the point of view of the citizen, it is important to have knowledge and options on the ways your personal data is used.

The report describes three studies that discuss the intersection of privacy and usability. From the point of view of the end-user, we explored the way security and privacy properties of products affect their usability and user adoption.

From the point of view of the service provider, we present a way of facilitating one of the GDPR requirements, the data protection impact assessment (DPIA), in a usable manner. Finally, combining the two perspectives, we reported on a study in which the service provider aims to predict suitable privacy settings for the users, resulting in a smooth user experience when the prediction is successful, while allowing the users to modify the settings if they so choose.

For the second theme of the report, we highlight different kinds of tools or methods for eliciting and fulfilling security requirements. For example, we show how security games, which are usually developed for training purposes, can be used to elicit security requirements and improve security policies. From research into privacy notifications, we were able to infer a set of design guidelines for transparency enhancing technologies (TETs). Furthermore, we proposed a framework for adaptive authentication that can take into account users' preferences and privacy requirements.

The third theme is about enhancing the human understanding of security solutions. We present ways to analyse and model user behaviour and the usability of products or services, and frameworks for enhancing usability of security solutions.

For instance, we propose a generic method for systematically analysing the usability of security mechanisms in order to better assess the trade-offs between security and usability. Additionally, research on a tool for configuring multi-factor authentication discusses similar trade-offs. Next, we discuss the usability of authentication, one of the most common experiences a user can have in a digital landscape. Authentication is also applied as a use case for an expedition into human understandable cryptography. Lastly, we analysed access control policies in complex, heterogeneous systems using formal methods, and used automation and visualisation to enhance the usability of the analysis results.

In conclusion, ease of use is an important design consideration for security solutions. One would be wise to try, for example, modelling one's system to ensure its usability at an early stage of development. Games and visualisations are also convenient for making the human user understand abstract cybersecurity concepts more easily.

Célia Martinie
IRIT – Université Toulouse III – Paul Sabatier
—
9 February 2022

Demonstrating the application and usability of security and privacy software assets

One of the key goals of CyberSec4Europe is to promote collaboration between industrial and academic participants by fostering research and development to identify and analyse cybersecurity challenges in several selected application areas and to develop innovative cybersecurity solutions that address them.

One work activity drives the design and development of demonstrators in those application domains, and targets the production of prototypes for cybersecurity solutions, products or services that are secure-by-design.

Another work activity is responsible for the definition of a common research, development and innovation programme for the next generation of cybersecurity technologies, applications and services. In one case, it has used and further developed several software assets that go beyond the state of the art on the usability of security and privacy policies. The close co-ordination involved in the practical application of these research outputs is reported in the recently published report, *Integration to demonstration cases* (D3.17), which highlights the integration of the software assets dealing with the usability of security and privacy policies with the application use cases.

This report presents the systematic approach applied to selecting the most relevant integration opportunities as well as the implementation of the software assets in the use case demonstrators. The main outcomes were:

- a set of conclusions on how privacy notifications can enhance usability transparency in the context of privacy and identity management and to what extent the cultural context and other parameters – such as demographics, usage characteristics, the option for intervenability and modality of privacy notifications – can have an impact on their perceived usefulness;
- a proposal for the combination of the authentication methods Trustworthy APIs for threat sharing (TATIS), AuthGuide, Keycloak and End-to-end visualizably-encrypted and human-authenticated channel (EEVEHAC) to protect the malware information sharing platform (MISP);
- an extension of the MITIGATE maritime risk management methodology to identify additional threats by including task modelling in the risk assessment process;
- a usable identity management user interface for smartphone users in smart cities, and a user-centred tool to support the security analysis of smart cities.

Moreover, to show the relevance of the integration of all the software assets that deal with the usability of security and privacy policies, the report describes a unified smart campus scenario, where there are many people, with different mindsets regarding security and privacy, and yet all of them need usable solutions for their everyday tasks. Some parts of the campus are public spaces, accessible to everyone, upstanding citizens and malicious actors alike. Other parts are restricted to authorised personnel only. This unified scenario features several security and privacy policies and in so doing highlights the synergy of the assets in addressing the usability and user experience associated with the policies.

The scenario also provides the opportunity to go deeper in the understanding of the interplay of the assets by demonstrating how the assets interconnect and inter-execute in an application domain, and this for different types of users. In particular, the use case exemplifies how the assets can support both end-user as well as IT system administrator tasks.

The integration of the project's software assets within the application use cases is one of the significant objectives of CyberSec4Europe. The effort expended with integrating these software assets has had the benefit of not only consolidating collaboration between consortium partners, but also of initiating additional collaboration with other parties.

Antonio Skarmeta
University of Murcia

—

29 July 2022

A privacy-preserving architecture

The Blueprint Design and Common Research activity defined the common research, development and innovation in next generation cybersecurity technologies (including dual use), applications and services with a focus on horizontal cybersecurity technologies and cybersecurity in critical sectors (eg, energy, transport, health, finance). It provided the common research support for the different work areas in the project and was especially co-ordinated with the demonstration use cases and the associated roadmapping work, to connect the research and innovation with the demonstration application and industrial sector being covered. A key aspect of harnessing the diverse software assets from multiple partner organisations was the formulation of an overarching general architecture.

The privacy-preserving architecture is part of the general CyberSec4Europe architecture. It consists of several planes and high-level building blocks that expand over several intertwined domains, comprising user, web and IoT domains, as described in the *Cross-Sectoral Cybersecurity Building Blocks* (D3.2) which also contains a mapping of all the assets used with the corresponding block of the framework.

There are 22 assets, split into the services plane, user domain, administration plane, intelligence plane, control and management plane, blockchain plane, IoT domain and web domain.

The building blocks are defined for different purposes which range from compliance with current legal frameworks such as eIDAS and the GDPR to mechanisms related to hardware-based solutions for managing keys and applications securely.

Here we give an overview of some of the different building blocks described above.

The control and management plane

In the control and management plane, the identity and privacy-preservation services plane includes the building blocks considered in the CyberSec4Europe privacy-preserving architecture. This architecture is devoted to enabling privacy-respectful authentication based on the provision of anonymous credential systems and privacy-preserving identity management services. Some of these systems and services rely on the use of secure distributed ledger technologies such as blockchains to provide a self-sovereign identity (SSI) model. The identity and privacy-preservation services also include mechanisms for privacy-preserving computation technologies to reduce information leakage during computations in the managed domain, thereby verifying that the systems comply with users' privacy policies. Those privacy-preservation services can be run in the cloud so that the architecture includes confidentiality-preserving and end-to-end secure sharing of sensitive data in the cloud among stakeholders using, for instance, secret sharing technologies. Besides, the architecture considers the privacy brokerage aiming at enhancing user trust in public cloud storage systems, guaranteeing data confidentiality and improving availability. The privacy-preserving architecture includes functional building blocks for confidential and privacy-preserving storage that can employ techniques such as secret sharing to anonymise personal information during data analysis processes.

Similarly, it also embraces privacy-preserving mechanisms for analysing data from potentially different stakeholders in a way that gives high authenticity and integrity guarantees to the computation's result, while protecting the confidentiality and privacy of the input data and ensuring data integrity.

On top of that, the privacy-preserving architecture includes several mechanisms that use trusted execution environments (TEE) for different purposes that range from securely storing and managing secret keys to remote anonymous attestation even in the presence of compromised hardware. The building blocks can be used on the virtualised applications in the cloud or directly installed in the user domain.

The user domain

In the user domain, the privacy-preserving architecture encompasses the wallets and TEE needed to maintain securely protected credentials and manage key material obtained during the issuance and enrolment with diverse identity providers. The user domain is exemplified either with user mobiles, or software for desktop browsers. It contains the client-side software needed to perform authentication against service providers, eID-based authentication, and run protocols for proving privacy-attribute-based credentials and claims (including zero-knowledge proofs).

Therefore, the user domain plays the role of recipient and prover in the privacy-ABC model. To this aim, the user domain interacts with diverse online identity services (including identity providers, attribute providers, PKIs, biometric verifiers, eID verifiers) placed in the control and management domain of the CyberSec4Europe architecture. In addition to credentials, the user domain needs to manage the attestations obtained from diverse attributes and from identity providers (for single sign-on), and short tokens obtained from identity providers (for single sign-on in the case of service providers). The user domain might also include ID-proofing mechanisms, with client-side biometric software needed to authenticate on biometric servers as a second authentication factor.

Furthermore, the user domain considers the data anonymisation building blocks to share in a privacy-preserving way data in transactions online and between organisations using diverse different privacy models (eg, the k-anonymity, k-Map, average risk model, among others). In addition, in the user domain, the privacy-analyser enables the attack surface to be reduced preventing privacy breaches when sensitive personal data is managed.

The blockchain privacy-preserving SSI layer

Decentralised authorisation, privacy-preservation and distributed access control are also important features considered in this architecture. In the blockchain privacy-preserving SSI layer, this is achieved by means of building blocks that are aimed at making blockchain technologies and consensus mechanisms more scalable, efficient, guaranteeing on-chain transactional privacy. Besides, it includes building blocks for modifying transactions (fine-granular rewriting) already present in the blockchain in a limited and traceable manner, which may be important for legal reasons.

The architecture considers the privacy-preservation of identities and personal data in blockchains. To that aim and following the Decentralized Identity Foundation (DIF) standards and specifications, the architecture features the building blocks needed for the creation, resolution, and discovery of decentralised identifiers (DIDs) and names in heterogeneous blockchains through resolvers. In addition, the identity hubs keep secure, encrypted, privacy-preserving personal data storage and computation of data, where the resolver services link user DIDs employed in blockchain with identity hubs. The blockchain identity services provide the means to create, exchange and verify crypto credentials and claims in a decentralised identity ecosystem with the user, following a self-sovereign identity management model. Besides, the blockchain identity services might rely on authentication protocols, open standards and cryptographic protocols, including DIDs and DID documents.

Edge computing

Another group of solutions is intended to enable privacy preservation in cloud computing environments as well as its extension towards the user side with Edge computing. The privacy-preserving architecture provides building blocks for secure data storage and processing in public clouds. In particular, it considers distributed data storage and privacy-preserving analytics as well as mechanisms for compliance with the provisions of the GDPR regarding interoperability and cross-border data transfers.

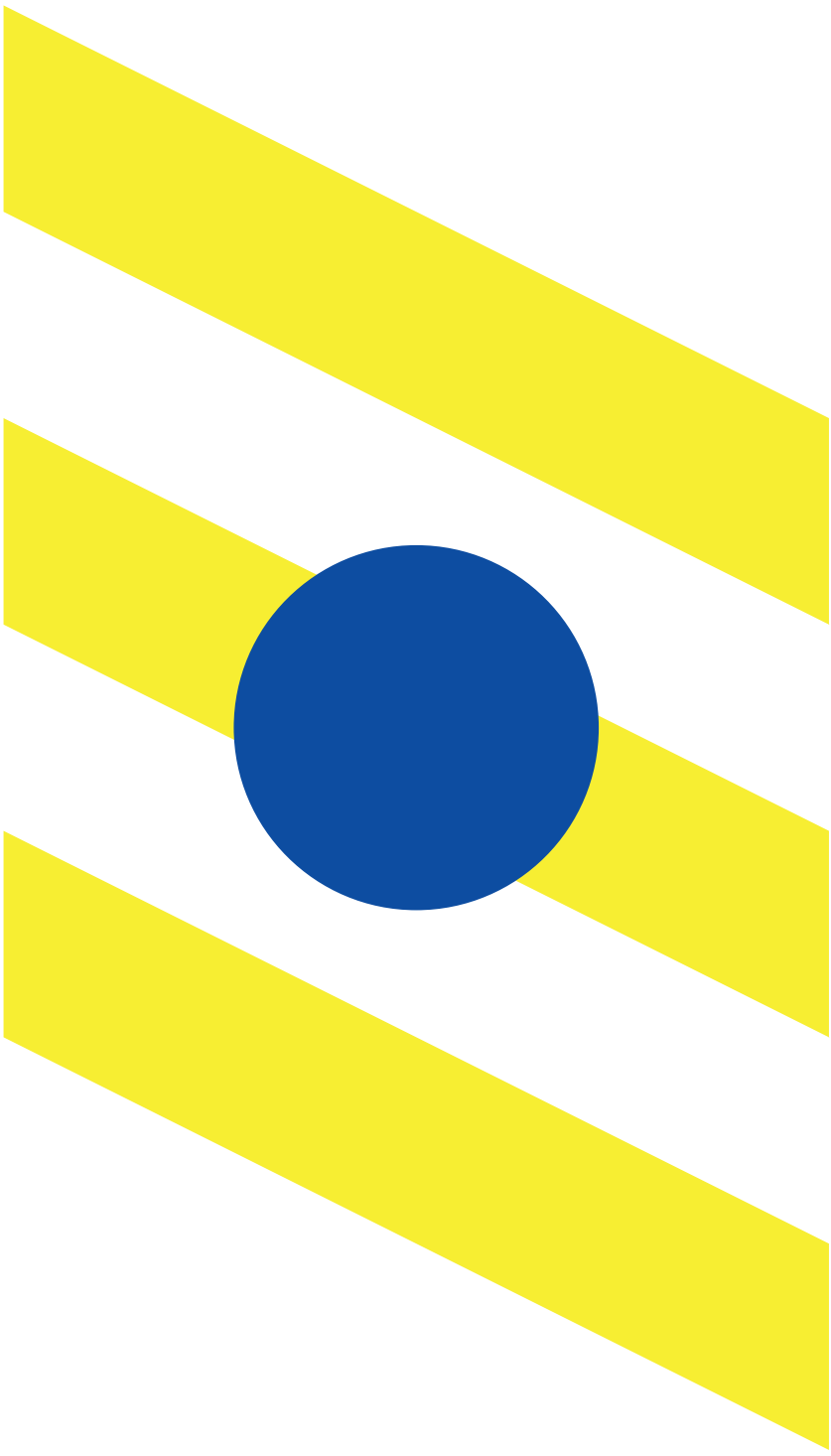
The Edge is considered in this architecture as a security and privacy enabler especially for the IoT domain, where devices are typically extremely resource-constrained and may be subject to compromise or interference. In this respect, the proposed architecture includes a data broker for both handling sensitive data according to a set of privacy policies as well as tools for monitoring and sanitising IoT devices for reducing the attack surface in this domain. Likewise, the privacy-preserving architecture considers the privacy-preserving middleware and software for the IoT domain aimed to ensure secure and authenticated communication channels between IoT devices.

The managed domain in the global IoT architecture can be also instantiated through processes related to the web domain (eg, eCommerce) in the CyberSec4Europe privacy-preserving architecture. In this case, the web domain is comprised of a set of functional components needed for service providers to authenticate their users, verify claims and privacy-preserving crypto-proofs (eg, zero-knowledge proofs). These service providers play the role of a verifier in the privacy-ABC model.

Summary

Finally, the privacy architecture also considers the application of security and privacy-by-design mechanisms by introducing components for GDPR-compliant software development as well as analysing the information leakage produced by some particular privacy solutions.

All software assets defined in the functional architecture are described in detail on the CyberSec4Europe and the GitHub websites.



2.2
Application demonstrators

CyberSec4Europe's application demonstrators are prototypes of a cybersecurity, secure-by-design solution, product or service and are focused on seven selected sectors: open banking, supply chain, privacy-preserving identity management, incident reporting, maritime transport, medical data exchange and smart cities.

The application demonstrator use cases provided the common research, development and innovation concepts developed by the design and research activity, ensuring their integration and fit into each of the demonstration use cases in each of the project phases.

Each demonstration use case was associated with a particular vertical sector which was co-ordinated, as far as possible, to ensure that as many common technologies as possible were identified: the target was to maximise the resources allocated to each of the research items.

The use case/demonstration case scenarios are:

- **Finance**, covering two inter-related areas:
  - **Open Banking** addressed the risks and vulnerabilities of cybersecurity attacks such as malware, phishing or social engineering and developing management policies to protect banks and their weaknesses in the design or implementation of APIs. In addition, we developed a pilot network to help prevent fraud and data loss in relation to monetary transactions by third parties in an open bank environment
  - **Incident reporting** developed a platform for sharing and reporting incidents according to different procedures and methods and in a secure way. The data-sharing is bi-directional, in a centralised or decentralised environment, trustworthy and secure.
- **Supply chain security assurance** provided blockchain-based blueprints for supply chain solutions for multiple sectors that allow managing trust across organisations without the need for a trusted third party. The main characteristics of this supply chain are that it should be traceable in all components, to assure quality and integrity, as well as be non-repudiable, support the detection of errors or manipulations and provide a quick response.
- In a **higher education** use case, through privacy-preserving identity management we enabled a distributed platform to manage identity and authenticated services and achieved strong, privacy-preserving authentication as well as providing consent for and controlling the data usage with privacy-preserving seamless ideals. One of the consequences was to supply trustworthy information exchange between official organisations as well as give transversal consciousness about how to control privacy and increase trust in online services.
- **Maritime transport** identified the cybersecurity challenges in the maritime domain covering the whole ecosystem including assets installed at the ship and at the port side. We developed updated security threat models and we responded to targeted threats, based on a combination of research activities, test deployment and validation that also engaged the relevant stakeholders.
- In the **medical data exchange**, we demonstrated the sharing and protection of medical data, both sensitive and personal, through a secure and trustworthy exchange of this information involving several actors and with different objectives and requirements in terms of security, data protection and trust issues, as well as in harmony with the applicable legislation and strategic policy framework.
- **Smart cities** connected cybersecurity challenges in an open smart city market environment based on the needs of two cities (Genova and Murcia) and their communities. It included an ecosystem where new ideas, needs, best practices, lessons learnt and other relevant information were shared.

Alessandro Sforzin
NEC Laboratories
Europe GmbH

—

30 April 2020

Composing a picture from the puzzle pieces

CyberSec4Europe is an ambitious project addressing cybersecurity issues in the Digital Single Market. The project focuses on seven selected sectors: open banking, supply chain, privacy-preserving identity management, incident reporting, maritime transport, medical data exchange and smart cities. The goal is to promote collaboration between industrial and academic partners to identify and analyse cybersecurity challenges in the selected sectors and develop innovative solutions to those challenges.

The demonstration cases – one for each of the seven selected sectors – are CyberSec4Europe's answer to the aforementioned challenges. They are the embodiment of the project's will to lead Europe's cybersecurity research and innovation with technology advancements catering to the complex reality of the Digital Single Market, as well as the security of European citizens and society as a whole. A demonstrator is a prototype of a cybersecurity solution, product, or service secure-by-design. In addition to being developed with an eye on security and privacy, the demonstrators will also be compliant with important EU directives and regulations, such as PSD2 and the GDPR.

The work activity oversees the demonstrators' design and development. Over the course of the project's first year, we identified several use cases that serve as the basis of the demonstrators. Our first report *Requirements Analysis of Demonstration Cases Phase 1* (D5.1) describes them and analyses their requirements; it presents the results of many discussions with stakeholders and industry partners of each selected sector. The report served as input to the *Research and Development Roadmap* (D4.3), as well as to the initial set of research guidelines and technologies (*Common Framework Handbook 1* D3.1) – also known as assets – that the demonstrators will integrate into their implementations.

CyberSec4Europe's report *Specification and Set-up Demonstration case Phase 1* (D5.2) builds upon the work of our first deliverable by further specifying the use cases of each demonstrator and presenting a preliminary overview of how the demonstrators plan to increase the cybersecurity resilience of their respective sectors. Whereas we initially focused on identifying their requirements and describing their importance in the context of the selected sectors, this new report concentrates on formalising the use cases' workflows and their interactions defining the shape of the demonstrators.

Jigsaw puzzles are a useful analogy to understanding the relationship between a demonstrator and its use cases. In a jigsaw puzzle, interlocking pieces are put together to produce the complete picture. In our work activity, the use cases are the interlocking pieces and the demonstrator is the picture we want to assemble. With this analogy in mind, our report is the instruction manual that shows how to put the pieces together to compose the picture.

It structures the presentation of the demonstrators in two parts: specification and set-up.

A demonstrator's specification formally analyses its use cases' workflow with step-by-step descriptions and diagrams. A demonstrator's set-up shows how its use cases come together to implement its designed functionalities, and explains how the demonstrator will work once its development is complete.

Finally, this report maps the demonstrators to the assets referred to above. This is not a theoretical exercise; a demonstrator maps to only those assets that it will integrate into its prototype during the development cycle. The collaboration between these two work activities is mutually beneficial: one produces assets (ie, technologies) that satisfy our demonstrators' requirements. Our work activity also ensures that innovative technologies are integrated into the demonstrators, thus proving that CyberSec4Europe's research is not only relevant to the Digital Single Market, but also effective in addressing cybersecurity issues in the corresponding sectors worldwide.

Alessandro Sforzin and Rahul Bobba
NEC Laboratories Europe GmbH
—
26 February 2021

From requirements to validation: demonstrating innovation in real world use cases

Cybersecurity is a critical pillar of the EU's digital strategy. It touches nearly every aspect of physical and digital infrastructures such as telecom, finance, healthcare, transportation and energy.

In December 2020, the European Commission presented its new cybersecurity strategy which highlighted the importance of research, innovation, and deployment to create a resilient, global and open cyberspace. Historically, Europe has leveraged cybersecurity tools and infrastructures which originated in the United States and were adapted to European systems and policies. It is time for Europe to become technologically sovereign and create its own world-class solutions and standards. CyberSec4Europe plays a key role in driving this strategy by advancing cybersecure technologies through collaboration between universities, research institutes, and industry.

One of CyberSec4Europe's key contributions to the challenges of this ambitious goal is to design and develop a set of innovative, real world demonstrator use cases in the areas of open banking, supply chain, privacy-preserving identity management, incident reporting in the financial sector, maritime transport, medical data exchange and smart cities. A demonstrator is a prototype of a cybersecurity solution, product, or service, secure-by-design. In addition to being developed with an eye on security and privacy, the demonstrators are also compliant with important EU legislation, such as PSD2 and the GDPR.

Since the project's inception over 24 months ago, we have produced three deliverables: the first analysed the requirements of each use case, identified the key actors and described their importance in the context of the selected sectors; the second defined the specification and set-up required for each use case demonstrator.

Our latest report, *Validation of Demonstration Case Phase 1* (D5.3), is a validation of each demonstrator according to a pre-defined set of criteria including technical performance and usability based on the requirements and specifications outlined in the documents above.

We employ two validation strategies: test cases and technology-based analysis. Test cases are inspired by software engineering best practices and consist of a description, workflow and test results. The technology-based analysis reasons that some requirements are met by the design of a demonstrator architecture or by its use of a certain technology.

We use quality indicators to pose questions to users and to capture their feedback. Quality indicators also cover the effectiveness and efficacy of the solution across multiple categories, such as integration and interoperability, documentation, usability, and testing and deployment. For each use case, a validation summary presents the outcome of the validation, including, for example, the percentage of requirements successfully validated.

This latest report is an important milestone as it concludes the first of two parallel cycles. As we move forward, we are scrutinising the lessons learned during the first cycle, analysing where we would like to make changes or improvements in planning the second cycle of requirements analysis, specification and validation.

Alessandro Sforzin
NEC Laboratories Europe GmbH
—
18 October 2021

Phase 2: the vertical demonstrator requirements revisited

CyberSec4Europe's report *Requirements Analysis of Demonstration Cases Phase 2* (D5.4), is the first report in the second phase of the project demonstrators' lifecycle.

In this second phase, our plans for the demonstrators are perfected with the feedback we received during the first cycle (*Requirements Analysis of Demonstration Cases Phase 1* (D5.1)). To this end, the report builds upon the requirements analysis in the first cycle by reviewing the use cases and requirements of each demonstrator.

Both these reports present the demonstrators' goals and importance in the context of today's cybersecurity landscape, with a particular focus on the European Union's market and citizenry. These two deliverables give an in-depth description of the demonstrators' foundations; that is, the use cases to be implemented to showcase the project's research and development work, and the requirements of these use cases.

What does 'requirements' mean? A requirement is a property or a functionality that a use case and its implementation must satisfy. We put the requirements into categories with different concerns, namely security and privacy, look and feel, usability, operational, maintainability and portability, and legal and regulatory. The final report in this cycle will focus on validating the use cases; that is, assessing to what extent their implementations met the requirements laid down in this latest report. Because a large part of CyberSec4Europe is conducting research, we also included requirements that may not be met by the end of the project but may help with defining its latest research and development roadmap.

Given that this report is by design an iteration of the previous requirements report, their content is similar. To help the reader better understand the changes we made, we added one section per demonstrator that highlights the updates to the use cases and requirements since the publication of the first iteration. Namely, we added, merged, deleted and rewrote requirements to reflect both the feedback we received during the first cycle and our own research and development activities. In a few cases, we did the same for the use cases. Of particular interest might be a new use case, titled *Cyber Threat Intelligence Sharing*, for the open banking vertical as a result of a new collaboration with the other pilots.

To conclude, this new report is an important deliverable for CyberSec4Europe, providing an in-depth overview of the demonstrator use cases and requirements for the seven verticals whose cybersecurity challenges the project is addressing.

Alessandro Sforzin
NEC Laboratories Europe
—
11 March 2022

Preparing the second round of commercial and application demonstrators

One of CyberSec4Europe's principal goals is to address today's European cybersecurity challenges across seven commercial and application areas: open banking, supply chain, privacy-preserving identity management, incident reporting, maritime transport, medical data exchange and smart cities.

The main benefit for EU citizens is for this collaboration between industry and academia to foster pragmatic research and development that will produce novel solutions to those challenges.

The demonstrator use cases are CyberSec4Europe's means of achieving this ambitious goal. A demonstrator is a prototype of a privacy and security-by-design cybersecurity solution to one or more real-world challenges. In addition to being developed with an eye on security and privacy, the demonstrators are also compliant with important EU regulations, such as PSD2 and the GDPR. The demonstrators cater to the complex requirements of the Digital Single Market, as well as the security of European citizens and society.

The primary activity for each use case – and there are usually several use cases for each sector – is the design and development of an appropriate demonstrator. These activities are divided in two parallel phases split equally over the course of the project, each delivering three reports. The first two phase 1 reports, on requirements analysis and specification and set up, describe the goals, workflows, and building blocks required for the demonstrators derived as a result of many discussions with stakeholders and industry partners.

CyberSec4Europe's latest report, the second in phase 2 of this activity, *Specification and Set-up of Demonstration Case Phase 2* (D5.5), builds on the previous work by finalising each demonstrator use case specification, and presenting an overview of how the demonstrators benefit their respective sectors.

It focuses on formalising the use case workflows and their interactions which define the shape of the demonstrators.

The report structures the presentation in two parts: specification and set-up. The specification of a demonstrator presents its workflow with exhaustive step-by-step descriptions. A demonstrator set-up shows how its promised functionalities were implemented, its software architecture and, in general, how it works. The deliverable also maps the demonstrators to the assets produced during our work with the separate research and development of the project's assets, indicating those that will be integrated into its development cycle.

Collaboration between these activities is mutually beneficial: one produces technology assets that satisfy the demonstrator requirements; whereas the demonstrator use cases ensure that CyberSec4Europe's innovative technologies are integrated into real-world, commercially-viable application scenarios.

Finally, because this latest report is a revision of the work carried out in the parallel phase 1 report, a section of the report reviews the work on the demonstrators up until today, describing the improvements made since the start of the second cycle of CyberSec4Europe, and highlighting lessons learnt and making recommendations for the future.

Maritime transport

Panayiotis Kotzanikolaou
University of Piraeus
—
15 May 2020

From ship to shore: securing maritime transport

This application demonstrator covers the maritime transport use case. The goal of each demonstrator is to 'put the correct pieces together' which are firstly described through concrete use cases.

The use cases

Although the security requirements of maritime transport are vast and cover multiple areas of cybersecurity controls, we have identified four concrete security services – use cases – that will be integrated and later demonstrated. These are based on the requirements analysis and the maritime transport research and development roadmap developed in earlier stages of the project.

1. Threat modelling and risk analysis for maritime transport services
We identified targeted threats and risks for maritime transport that include various other use cases, which describe all the distinctive phases, such as:

- critical maritime assets and services identification;
- vulnerability management;
- threat modelling and scenarios specification;
- maritime transport risk analysis;
- attack paths representation; and
- maritime transport risk management.

2. Maritime system software hardening
Applications used in the maritime domain, such as software running on a moving vessel, usually utilise legacy code which is hard to update and sometimes even harder to replace. An attractive option is software hardening, whereby a program is re-written in order to avoid memory-related vulnerabilities. Re-writing the code can be done either by re-compiling the source (where possible) or by reconstructing the binary. Note that this re-writing is focused on the security properties of software and not on its base functionality.

Hardening can be applied much more easily than a total replacement of the code.

3. Secure maritime communications
We examined the secure exchange of various types of information, including maritime-specific systems such as:

- VHF data exchange system (VDES) frequencies;
- automatic identification system (AIS) information;
- maritime mobile service identity (MMSI), time, ship position, speed, course etc;
- vessel voyage information (such as route plans and mandatory ship reports);
- maritime single window reporting information (such as ship certificates, log books, passenger lists and crew lists); and
- port to vessel information, such as weather reports, passenger lists or cargo manifestos.

4. Trust infrastructure for secure maritime communication
As various types of information are exchanged/transmitted between different maritime stakeholders and actors at sea and on shore, designing a specially crafted trust infrastructure is vital. However, it is not straightforward to set up and operate a typical public key infrastructure (PKI) solution, since there are constraints associated with the maritime transport domain. The communication bandwidth of ship networks have to be taken into account. For example, the SATCOM component of VDES is expected to become a bottleneck in ship communication, due to its low capacity. In addition, it is not uncommon for ships to sail for long periods of time without any Internet connectivity at all; and, as shipping is a low cost business, this imposes strict limitations on what solutions will be acceptable to the industry.

Here we will research those constraints and design and demonstrate a PKI service specifically adapted to fit the needs of the maritime domain.

The demonstrator set-up

Here is what the three demonstrators will illustrate:

(A) Threat modelling and risk analysis for maritime transport services using a web application utilising multiple modules to give a complete risk assessment process. The sequence of information insertion will ultimately lead to a complete asset map and informative output forms based on multiple risk assessment results.

(B) Maritime system software hardening firstly by enhancing the risk analysis framework realised in (A), and then hardening unsafe components used in (C).

(C) Secure maritime communications and trust infrastructure for secure maritime communication initially implementing the PKI service described in (A) and in the next phase will be extended to demonstrate the secure maritime communications.

For more information on this phase of all the demonstrators, detailed descriptions can be found in our report *Specification and Set-up Demonstration case Phase 1* (D5.2).

Panayiotis Kotzanikolaou and Eleni-Maria Kalograki
University of Piraeus

—

27 March 2021

The case for investing in resilient maritime transport infrastructures

Maritime transport is a dynamic sector which includes various interactions between physical and cyber systems operated by different stakeholders and users. It involves various processes and services such as docking of the ship, loading and unloading, ship navigation, ship-to-ship and ship-to-shore communications, pre-arrival notifications, to name just a few.

Such complex structures provide a vast attack surface, where many attack paths may occur due to various causes, ranging from software vulnerabilities, deliberate attacks or human errors. The incremental evolution of technology in accordance with the spread of automation and digitalisation on maritime transport operations has raised the need to look for strategies, methods and tools that can adequately secure the dynamic environment of maritime transport. This includes the involved operators, the critical information infrastructures (of ports and vessels) that function and their corresponding communications.

The identification of the current and near-term future cybersecurity challenges for the maritime transport sector are within the scope of the research roadmapping activities of CyberSec4Europe, along with the identification of the existing methods and tools that may assist researchers in meeting these challenges.

Challenges and opportunities

The complicated dual cyber and physical nature of the maritime environment raises a set of open issues concerning the effective and efficient handling of their security and safety issues. In this context, we have identified a set of research challenges and issues, regarding the distributed and interconnected nature of complex, inter-related maritime components, network and operating environments that need to be investigated:

Developing risk assessment and threat modeling techniques targeted at the maritime transport threat landscape

Existing maritime transport risk assessment methodologies could be enhanced with targeted threat models that capture the adversarial environment of maritime infrastructures such as ship and port facilities. The early identification of novel cyber-physical attacks and cascading attack paths against autonomous ships and port automation SCADA systems are typical examples of new cascading threats.

Security hardening for critical maritime systems

System security hardening is a challenging task in domains where it is hard to analyse and correct software errors. Maritime systems fall into this category, as they are based on non-standard devices, embedded systems, legacy applications, and so on. Therefore, developing efficient hardening techniques for maritime systems is an important research challenge.

Maritime communication system security and trust infrastructures

Maritime communications involve data exchange between ships, ports, remote control centres, vessel traffic services, search and rescue and so on, each of which have different technical and environmental constraints. For example, ships cannot depend on landline communications, while search and rescue communication services require the prioritisation of communication channels in case of emergencies. Setting up and operating efficient trust infrastructures for such an environment is also an open challenge, since typical public key infrastructures require high bandwidth and real time communications for certificate verification, which may not be efficient for the ship environment.

Securing autonomous ships

Autonomous ships are characterised by the increasing deployment of interconnected cyber-physical systems. To this end, a comprehensive requirements elicitation process requires a security assessment to incorporate safety aspects.

Increasing the resilience of maritime infrastructures

Since resilience suggests properties like infrastructure redundancy and robustness, it is implicit that building resilient infrastructures comes with an increase in cost. An interesting problem is balancing infrastructure resilience and cost optimisation. As the recent pandemic has reminded us, the maritime transport sector is a critical sector for many vital activities such as the delivery of medicine and supply chain operations.

A major challenge is ensuring the resilience of critical maritime systems which should continue to provide a minimum service level during or after a cyber/physical threat, and should also quickly adapt and recover from such unwanted events.

As the EU is one of the key global players in maritime transport, the development of resilient and cost-effective maritime infrastructures is a clear opportunity for Europe.

More information on the research and development roadmap for the maritime transport sector but also for the other verticals examined within CyberSec4Europe can be found in the report *Research and Development Roadmap 1* (D4.3).

Medical data

Jérémy Decis
Dawex Program Manager
—
26 May 2020

How sharing information and data contributes to hinder the spread of Covid-19 and its economic impacts

The world is facing, with Covid-19, a unique and unprecedented health crisis in terms of its magnitude, gravity and speed of propagation, creating a huge disruption in the global economy, impacting the operation of millions of businesses and the life of billions of citizens. Since the beginning of the Covid-19 crisis, health organisations across the world, under the initiative of the World Health Organisation, have started to investigate the cases behind the development of the virus in order to curb its spread.

Facilitated access to data, as well as the co-ordinated effort of all economic stakeholders at a public and private level worldwide, is key to winning this war against the virus. To hasten the resolution of this unprecedented global health crisis and mitigate the economic fallout and the repercussions on all businesses, data must circulate between organisations easily, securely and rapidly.

At this time of crisis, it is important to remember that we may all have some means of helping in a positive way. CyberSec4Europe partner Dawex has launched the Covid-19 Data Exchange initiative, a privacy-respecting exchange platform of non-personal data essential for healthcare professionals and organisations who are at the front line in providing care, conducting research, ensuring transports and logistics of critical equipment, and saving lives. A whole ecosystem participating in the exchange of data, and testing data anonymisation, encryption and other services being carried out in the pilot in the resolution of this crisis could contribute to the global effort to beat the virus and restrain its economic impact.

The Covid-19 Data Exchange review

The Covid-19 Data Exchange is an easy-to-use platform, allowing its participants to securely source, publish and exchange non-personal data with public and private organisations from multiple sectors aiming to stop the virus's progression and its economic impact.

The Data Exchange technology enables users to remain in full control of the data they share, with whom they share it, and to keep track of all data flows.

The platform acts as a trusted third-party where users benefit from multiple governance features providing maximum security, traceability and confidentiality. Data is exchanged in full compliance with regulations, leveraging blockchain technology to ensure the integrity of licensing contracts in private or open data mode. Only strictly vetted participants are granted access to the platform to ensure strict confidentiality and relevance of the data exchanges.

To broadly open up the platform access to the maximum of countries and avoid any infringement of respective privacy regulations, participants are not authorised to create data offerings containing personal data on the Covid-19 Data Exchange.

On the Covid-19 Data Exchange

- Scientific communities can access vast amounts of data from all around the world, including data sources that are not easily available.
- Hospitals and other healthcare operations can have access to cutting-edge yet easy-to-use tools to publish and share field non-personal data with a large global community.
- Many other stakeholders having a direct impact on the resolution of this crisis can find and exchange valuable data. Amongst them are specialised equipment manufacturers and distributors, governmental agencies or public services, banks, insurance, retailers, transport and logistics organisations.
- Various types of non-personal data can be exchanged including, but not limited to, statistical data, research data, anonymised raw data, tests results, equipment sourcing and inventory data, social and sentiment data, and many other types of data (open data or private data).

With everyone working together, we will prevail against the virus, its economic impact and come through this stronger than ever.

Juan Carlos Pérez Baun
Atos Spain
—
8 October 2020

Enabling trust and preserving privacy when sharing medical data

The medical data exchange use case is the second of CyberSec4Europe's seven application demonstrators.

The main challenges to be addressed when sensitive data is shared between different actors are how to:

- preserve the privacy of data owners;
- increase trustworthiness to ensure the willingness of the different actors to share sensitive data;
- ease the use of the data exchange platforms;
- comply with the current regulations.

The different services that are planned to be offered by the data exchange platforms are:

- preserving user privacy techniques, such as anonymisation and encryption tools;
- increasing trust in the data exchange platform by providing strong user authentication by using an eID-based eIDAS network, and decentralised user access to the platform based on self-sovereign identity;
- improving user experience including data assessment and data sampling tools.

During the development of the demonstrator, the regulatory aspects of the GDPR and eIDAS will be considered as will the object of research.

With these aims in mind, three different use cases were identified to address these challenges and demonstrate the use of the services described.

- Sharing sensitive health data through an API: analytics are performed on the aggregated personal and health data collected by the data providers from different sources. The data is protected by using privacy-preserving techniques.
- Sharing sensitive health data through files: anonymisation and privacy-enhancing technologies are used to anonymise the files uploaded to the data exchange platform by the data providers who have received personal and health data from a data source, preserving data subject privacy. The data providers upload the files on the data exchange platform, including a set of related metadata.
- Enhancing the security of on-boarding and accessing the data exchange platform: increasing the security of the on-boarding process and facilitating secure access to the platform is envisaged by the provision of a secure mechanism for the online registration process, using eIDs issued by Member State authorised organisations. Decentralised access using a verifiable credential based on eIDAS authentication, and the validation of this verifiable credential by the data exchange platform is to be attempted using distributed ledger technology.

The lessons learnt during the development of the medical data exchange demonstrator and the use of the indicated privacy-preserving technologies will help address the oncoming challenges, not only in the health domain but also in other business domains.

Juan Carlos Pérez Baun
Atos Spain
—
11 May 2021

Privacy challenges when sharing sensitive medical data

European Commission Vice-President Margrethe Vestager recently tweeted 'data is not oil: it is a renewable resource that can be pooled, shared and re-used … we want to enable businesses to make the most of data – while securing that we can trust that we are protected from misuse.' Nowhere is it more vital to apply that sentiment than in the data generated in our healthcare systems.

According to *Forbes,* more than 2.5 quintillion (2.5x1018) bytes of data were created each day during 2018; 463 exabytes of data per day (463x260) are expected in 2025. In healthcare alone, the huge amount of health data and medical records generated is growing faster than in any other sector and is estimated to reach around 10 petabytes each year (10x250).

Wearables alone generate massive amounts of data each second, while hospitals and primary healthcare centres collect huge amounts of records every day. Additionally, the number of medical imaging tests, blood and genetic tests is constantly increasing.

Generating value through sharing

This enormous volume of stored data can be used to improve the health of our communities and its value increases when shared with others. By bringing data providers and data consumers together in a single place, a medical data exchange platform can sharply increase the value of this data, not least in the cross-border exchange of data, due to the increase in cross-border business. Overall, the big data health market is expected to have a compound annual growth rate (CAGR) of 36%.

The main asset to protect is the health data generated by data providers. The health data collected is generated by a number of sources: wearable health devices that collect a user's personal health and exercise data; patient devices that collect medical data; diagnostic image devices; online diagnostic tools; medical research; clinical trials; pharmaceutical research etc.

The health system overall can be significantly improved when this medical data is shared through a data exchange market platform among health stakeholders who are:

- data producers, such as:
  - hospitals, primary healthcare centres, health clinics, clinical analysis laboratories, private health institutions
  - doctors and patients, as health data providers

- data consumers, such as:
  - research institutions, health authorities, governmental agencies,
  - the pharmaceutical industry, drug agencies, insurance companies

The data exchange platform provides data consumer access to data shared by the data providers. Conversely, a lack of data-sharing can have a negative impact on the development of computer-based solutions. This negative impact affects areas such as imaging-based machine learning technologies which are able to:

- simulate surgical treatments or device implants,
- automatically detect pathological lesions; and
- cross-reference imaging findings with other patient data for highly personalised clinical predictions.

As the health data generated by data producers is of a personal nature, it is protected and not provided to data consumers.

Only the associated metadata that is closely related to health data can be displayed and browsed on the data exchange marketplace. It is not only health data that needs protection: apart from sensitive medical data, any associated personal data as well as the personal data from the different data exchange stakeholders, the data providers and data consumers, must also be protected. Moreover, a suitable technology and infrastructure are also essential requirements for developing the data-sharing process in a secure way. Hence, the security and privacy of health information must be assured, not only during data storage, but also during the exchange and/or sharing processes.

The data required for developing and testing these systems exists today in large quantities inside hospital firewalls, but it cannot be accessed without jeopardising patient privacy and exposing institutions to severe legal implications. The GDPR has established a much needed legal framework that sets clear boundaries for compliant data exchanges and provides clear guidance to economic players, finally framing biomedical data-sharing within legal boundaries and opening the possibility for trading such data under different classifications and corresponding legal agreements. The issue still to be resolved is the need for a robust and scalable solution to enforce privacy and security requirements in a way that efficiently meets the strong demand for health data.

How CyberSec4Europe is addressing the challenges

The CyberSec4Europe medical data exchange demonstrator use case leverages an existing data exchange marketplace (Dawex) and is tackling these challenges and contributing to the setting up of a trusted and secured data exchange platform in Europe for medical data.

The management and access to this sensitive data on data exchange platforms need to be appropriate in terms of quality, security and privacy. The medical data exchange platform must assure the integrity and reliability of the data. Additionally, only permitted users will get access to the platform where the data or metadata is stored. Also, the data must be protected at any moment when transiting between parties. Moreover, during the sharing process user data privacy must be preserved at every moment. Furthermore, in order to engage new users to the platform being willing to share and consume data, both the data consumers and data providers must interact with the exchange platform in a user-friendly way. Finally, the platform must comply with current data protection legislation ensuring that the rights of users are protected. These measures will prevent any third party from accessing user data, providing a secure and smooth use of the medical data exchange platform.

The main challenges being addressed in the medical data exchange demonstrator use case when personal and sensitive data such as medical records are identified are to:

- Preserve user privacy
- Assure secure access to data
- Provide a trusted environment where data providers and data consumers can share sensitive data
- Assure end-to-end data integrity
- Improve the user experience
- Apply innovative tools to comply with data protection regulations, principally the GDPR
- Boost the use of data exchange platforms among all stakeholders

To meet these challenges, CyberSec4Europe is carrying out the following activities:

Implementing and operating an anonymisation tool
The Data Anonymization Service (DANS), an asset for addressing the security and privacy challenges, is provided as a service which can be deployed at the data provider premises, offered as an additional service by the marketplace or on a third-party infrastructure. DANS is also provided as a library to be directly integrated into the data provider system, making it easy to adopt an anonymisation process.

Designing and implementing a cryptographic tool
The Functional Encryption to Medical Data (FE2MED) asset is a privacy-preserving tool which provides data integrity and confidentiality. An end-to-end encryption protocol is established in order to avoid a cloud provider from reading user data: only the appropriate authorised consumers can access the data or the result of any analytics process.

Using security tools and trust mechanisms
It is envisaged that strong authentication mechanisms will be adopted for accessing the data shared by the exchange platform. The use of Member State-issued eIDs leveraging the eIDAS network for the authentication process will increase user trust in these exchange platforms.

Exploring a user-centric approach
The adoption of a self-sovereign identity (SSI) platform would provide an alternative decentralised access to the data exchange platform.

Following regulatory guidelines
Research activities are being carried out on regulatory aspects and tools for complying with the GDPR and eIDAS regulations.

Not surprisingly, Covid-19 has generated a large amount of data across the world and in order to provide a positive response to the urgent need for global co-operation on many aspects of the pandemic, Dawex launched the Covid-19 Data Exchange platform which will be leveraged by the medical exchange data demonstrator. The tools and mechanisms for creating a trusted, secure and data privacy-preserving exchange platform are being applied on the Covid-19 Data Exchange platform.

The Covid-19 crisis has boosted the development of innovative tools for tracing and controlling the pandemic, but several aspects such as privacy, security and strategy must be considered in order to reach the expected objectives.

The project's roadmapping work carried out a SWOT analysis which shows the current situation of the medical data exchange domain in the EU regarding user data-sharing while preserving privacy, trustworthiness, security and complying with regulations. It shows that homogeneity in health data regulations worldwide would help to facilitate the use of health records which could in turn become a key factor for fighting against pandemics, while increasing citizen trust in any data exchange platforms used.

Dealing with these challenges should be of high importance in the near future, as an increasing volume of sensitive records are being generated by the digital economy. Trusted data exchange platforms will increase European digital sovereignty but in order to do so they need to seriously consider how to return control of the data associated with personally identifiable information to individual users through the adoption of self-sovereign identity through distributed ledger technology.

A more detailed description of the results of the Medical Data Exchange demonstrator work can be found in the two reports, *Validation of Demonstration Case Phase 1* (D5.3) and *Research 'and Development Roadmap 2* (D4.4).

Smart cities

Marco Angelini and Vincenzo Savarino
Engineering Ingegneria Informatica

—

19 June 2020

The security and privacy tale of three smart cities

A fundamental aspect of smart cities is the generation, analysis and sharing of large quantities of data. Smart city technologies capture data about people and places to all forms of privacy, and day by day they drastically expand the volume, range and granularity of the data being collected and processed. However, this smart city process puts individual privacy at risk, and reduces individual trust.

Taking into account this aspect, the smart cities demonstrator will move around personal data exchange among citizens and other city stakeholders, mainly the municipalities, as key players in the delivery of public services and citizens' data management.

The smart cities demonstrator involves a technical provider, Engineering Ingegneria Informatica S.p.A, academics from University of Murcia and University of Porto, a research centre, Consiglio Nazionale Recerche (Italy), a local public administration, Commune di Genova, and a smart cities' network, Open and Agile Smart Cities, who are working together to:

- put in place and operate a consent-based infrastructure to support a platform for sensors and other urban data; and an infrastructure for personal data exchange and reuse in public services, in compliance with the GDPR;
- set up an open innovation cycle that will drive city stakeholders from a cybersecurity risk and needs assessment to the identification of the related solutions (ie, cybersecurity services). Risk assessments will be applied at an individual and organisational level.

The main outcome of the activities working towards the smart cities demonstrator is the enablement of a novel ecosystem capable of fostering business models based on personal data exchange and usage in smart city and public services. At the same time it should properly manage the related cybersecurity risks and regulatory compliance to increase user confidence and to pave the way for a smart city cybersecurity competence centre.

To address smart city security and privacy objectives, several use cases were identified covering the following functionalities:

- Supporting urban data functionality
- Empowering citizens with their data
- Sensor data-sharing and processing
- Assessing exposure to social engineering by simulating phishing attacks on a service provider's target groups
- Performing a cyber risk assessment, evaluating a service provider's cyber maturity level and estimating the probability and impacts of cyber attacks
- Eliciting cybersecurity needs and selecting solutions

The demonstrator set-up

A specific characteristic of a smart city environment is the variety of the infrastructure, with multiple devices and levels of smartness. The demonstrator set ups of Murcia, Porto and Genova will focus on implementing and putting into operation in each of their specific contexts the use cases described above.

The Murcia smart city consists of a FIWARE platform that gathers data provided by hundreds of sensors and other data sources, such as parking providers or public transportation companies. With this demonstrator, we are extending the security and privacy aspects of the existing platform by implementing the self-sovereign privacy-preserving identity management system (SS-PPIdM), that will accommodate the registration of users to the smart city ecosystem, taking into consideration their preferences regarding privacy and how their personal data is to be shared and used for identification by the different services registered as part of the smart city project.

Porto currently has a laboratory testbed that combines diverse physical sensors and multiple computing devices with heterogenous resource capabilities. Its purpose is to map a wide range of application scenarios and use cases, including video and audio surveillance, noise, humidity, temperature, luminosity and motion detection, to name just a few. In this demonstrator, Porto will study how current data anonymisation and privacy-preserving techniques perform for achieving individual and citizen privacy.

The Genoa municipality is currently redesigning both system architectures and administration processes, aiming to improve both the efficiency and security of internal and external services. The goal of this demonstrator is to improve the systems and processes of the municipality that handle, manage and protect citizen data. To this end, we are assessing the current security level of the infrastructure, improving the technical skills of data officers and managers and centralising the management of privacy consents and data processing records.

For more information on this phase of all the demonstrators, detailed descriptions can be found in the report *Specification and Set-up Demonstration case Phase 1* (D5.2).

Marco Angelini
Engineering Ingegneria Informatica
—
7 April 2021

Get smart: securing the future of digital cities

Today, an increasing number of people worldwide live and work in cities. Consequently, creating liveable environments in which people and businesses can thrive has become one of today's most pressing issues: the way we all use the time and space available, the environment and resources at our disposal determines the quality of our life and forms the basis for the sustainability of our existence in the medium and long term.

For that reason, many cities and metropolitan areas are embracing the smart city concept: that is, adopting a more efficient management of services, and turning cities into enablers of innovation, economic growth and well-being, but also making them safe, dynamic and inclusive.

Building citizen trust in multi-application digital solutions

Over the past few years, automation in our everyday environments has noticeably increased. Smart devices that are capable of regulating everything from the water in large-scale facilities to the temperature in our homes have started to proliferate and will continue to do so in the future. As the associated sensors and actuators monitor and control significant parts of our everyday lives, they are bound to be considered by cyber attackers as potential targets. To address this challenge, smart cities are being forced to implement the appropriate mechanisms to provide their citizens with a safe and secure environment, assuring them of privacy and data protection-by-design and full control of how their personal data is processed.

To this end, it is important to identify measures, approaches and technical solutions that support responsible smart cities and stakeholders in the entire process of privacy and data protection, from risk assessment to solution elicitation and enforcement.

Digital solutions, supported by locally-generated data, are capable of providing high-quality services both to the public and to businesses. These solutions incorporate smart urban mobility, energy efficiency, sustainable housing, digital public services and civic-led governance. To gain public trust for such systems, data must be used responsibly via digital platforms, and their quality, security and privacy must be ensured.

Smart city attacks can happen at least at two levels, requiring different kinds of tools and approaches:

- Individuals, principally citizens and civil servants, require tools related to social engineering, phishing, data ownership and possibly training.
- Businesses and other organisations, including public authorities and third parties, require tools related to risk assessment, predictive analysis, and mitigation activities, according to the existing legislation on data protection and privacy.

Developing trustworthy federated platforms

The desired transformation process needs all levels of government together with organisations and networks of cities and communities of all sizes, with strong co-operation through multi-level governance and co-creation with citizens. To do this, a first step is needed: the smart city enablers' adoption. The role of these enablers is to connect consumers and producers, enabling a federated publication of context data, allowing service providers to find and use data from city and third-party sources while preserving data sovereignty.

The variety of services, systems and applications behind most smart city initiatives usually share servers and resources. Thus, the platform needs to tie different protections together and ensure that there are no privacy leaks at any point. Additionally, a security platform should be deployable across the many disparate systems that comprise the smart city environment, maintaining the required level of trust. Finally, it should support on-premises, IaaS (infrastructure as a service), SaaS (software as a service) and hybrid cloud environments, to ensure that no device or server remains unconnected.

Addressing the challenges

As part of its roadmapping activity, CyberSec4Europe has identified a series of challenges with associated research goals to the fulfilment of its vision for secure smart cities, some of which it wishes to address over the remainder of the project. Among these are the following:

- Trusted digital platform enabling citizen-centric services delivered seamlessly for all citizens, with the caveat that it will only work if citizens perceive it to be trustworthy ie, it must guarantee the protection of personal data
- Cyber threat intelligence and analysis platform. Information sharing, active defence and automation methods should be integrated into the smart city platform by developing efficient methods to create, disseminate, and consume threat intelligence in a standardised, usable and legal way. To make the solutions effective, automation should be considered, and solutions integrated into business workflow, governance and structure control.
- Cyber response and resilience of the overall framework, governance and business of smart cities will benefit from a higher security level if response measures and resilience to cyber threats are made an essential part of smart city design in terms of volume, velocity and variety of networked traffic.
- Cyber competence and awareness programmes focussed on improving knowledge about possible risks and hardware/software attacks, as well as techniques such as encryption, anonymity and access control. Both training software engineers about possible security vulnerabilities and current technical solutions and informing end-users about the security and privacy risks they could face and the correct security behaviour they should apply.

➔ Privacy-by-design solutions are a must when new public services use citizen data, particularly with the requirement to be GDPR compliant, meaning:

- proactive privacy protection rather than post violation remedial action;
- privacy as the default setting, privacy embedded into the design;
- full functionality with full privacy protection through the entire data lifecycle;
- visibility and transparency as well as respect for user privacy.

In parallel, data minimisation approaches should be considered as a best practice for the adoption of privacy-by-design.

➔ End user trusted data management encompasses approaches to gain citizens' trust in the collection and processing of data that concerns them:

- Assuring transparency
- Managing consent and control
- Implementing auditing and accountability procedures

Beyond the end of the project

It is almost inconceivable to imagine beyond the next two to three years how cities will adapt to the transformatory visions being laid down today, given the speed with which they are currently evolving. However, we are confident that the roadmap, together with the accompanying strategies and solutions, provided by CyberSec4Europe will help stimulate the growth and development of digitally robust cities in Europe and beyond in the 21st century.

For more on the roadmap for smart cities and the other six verticals, please read our report *Research and Development Roadmap 2* (D4.4)

Finance

David Goodman
Trust in Digital Life
—
30 July 2020

Share your fraud

Today financial fraud is global. As bank strategies are focused on digitalising critical processes like opening a bank account or adding a transfer beneficiary to a bank account, it has become very easy for hackers to carry out fraudulent transactions from their living rooms within a short period of time and without their physical identity being fully exposed. Moreover, they can attack several banks without having to change their mode of operation, given that today banks don't share information on frauds that have been effective and any associated data.

Finally, with new applications of technologies like Instant Payment which provide bank users with real time money transfer services, it is even more difficult to fight fraud, as banks don't have any time delay in which to carry out recalls in case of fraudulent transactions.

This demonstrator is the first step in the implementation of a trust network aimed at providing banks with a channel to share and exchange critical information about effective frauds, leveraging the latest online open banking services. First, by making such sharing possible, banks should be able to improve their ability to detect and react in real time to cases of fraud. For example, if a bank which had detected a transfer fraud were able to share with other banks the information about the IBAN implied in the transfer, these banks could take this information into account as soon as possible to prevent the fraudster from using this IBAN to carry out other fraudulent transactions.

The security aspects of PSD2, including the introduction of strong customer authentication (SCA), help the fight against fraud, leveraging identity theft techniques. Nonetheless, the majority of financial losses are due to successful modes of fraud operations for which user authentication is inadequate.

The demonstrator set-up

For the first release of the demonstrator we are focussing on two scenarios associated with sharing fraud information.

Means of payment fraud: A customer interacts with her bank to establish an account which then provides ready access to cash and credit. Ironically perhaps, the customer is either the individual or the representative of a criminal organisation intent on defrauding as many financial institutions as possible in a number of different ways.

From the perspective of the bank or merchant, this is a bona fide customer, who has opened an account and is carrying out everyday transactions, only to get unmasked as a fraudster after the fraud is detected.

The bank is represented by a fraud expert who carries out due diligence on the account request through know your customer (KYC) procedures and provides the mechanisms for the customer to get access to cash and credit facilities. The banks or financial institutions being targeted are the ones to incur financial loss and loss of brand credibility. Typically, if a fraudster is successful with one bank or financial institution, he or she will move on to attack another.

'Credit renegotiation broker fraud: A fraudster is an individual or representative of a criminal organisation (and who, depending on their mode of operation, could also be another bank customer) who interacts with an unsuspecting bank customer in order to get the necessary credentials/documents to defraud the customer.

The customer who is the target of the fraud has a pre-existing arrangement with a credit company which is a passive recipient of credit facility requests unaware that they are fraudulent (because they don't have the means to be informed). In addition, a bank also acts as the recipient of ill-gotten monies from the fraudster that the customer eventually seeks reimbursement from.

The demonstrator will be extended in the next phase of the project with more scenarios, intervention/detection mechanisms and potentially additional actors.

An open banking API architecture

This set of use cases involves six different scenarios associated with attacks on a bank's internal systems by a hacker or a malicious user who tries:

- to gain illegal access to the system,
- to tamper with customer data,
- to gain unauthorised access to information,
- to access customer data through API vulnerabilities,
- to access customer data by injecting code into a client-side application,
- to compromise a service with access to an internal API.

The scenarios described are plausible for all European banks and third-party service providers that have an economic interest in the network architecture. In particular, banks are able to easily connect other APIs in the market in order to extend their service offerings by introducing native plug-and-play FinTech solutions. Through embracing the Open Banking API economy, banks are able to further enhance and transform current offerings – increasing their appeal to existing and prospective customers alike. However, Open Banking APIs can also create a threat for banks, as they enable Fintech firms to tap into a bank's financial data. For example, a Fintech start-up may decide to use a bank's 'Customer Data API' in order to build a mobile application where customers budget their finances, manage their debt, and get real-time investment and financial advice through chat. The majority of traditional banks do not offer such debt and real time finance management services.

This means that by opening up their API, the bank has enabled the Fintech to fulfil this existing gap and drive a wedge between the bank and the customer.

The demonstrator set up

In the demonstrator we show how the Open Banking API Architecture platform can overcome the security issues associated with:

- an unauthorised user
- unauthorised access
- unauthorised use
- a man-in-the-middle attack
- the misuse of a user interface
- privilege escalation
- integrity/confidentiality compromise
- API misuse.

In each of the six scenarios mentioned earlier, the attacker is first able to get access to a bank's system or exploit some vulnerabilities against the platform non-compliant with security requirements; we then show how the attacker can be blocked by the application of appropriate countermeasures.

Laura Colombini Intesa Sanpaulo Group Services, **Vanesa Gil Laredo** BBVA Group and **Susana González Zarzosa** Atos Spain

—

16 February 2021

Prototyping an incident reporting platform

Cybersecurity is of paramount importance in protecting the Digital Single Market which is mirrored in the evolution of EU legislation. With the objective of increasing cybersecurity readiness and awareness, the current EU legal framework specifies the need to comply with requirements for mandatory incident reporting to different supervisory authorities. These requirements are particularly strong in the critical financial sector.

Currently, there are no cross-sector standards defined for mandatory incident reporting and each supervisory authority, both at EU and national levels, defines the relevant impact assessment criteria, thresholds, timing, dataset, procedures and means of communication that it requires to be followed. All these different criteria and patterns cause fragmentation in the overall incident reporting operation for the affected financial entities and have to be managed along the critical path of managing the incident itself. This implies time-consuming reporting processes for the incident management and reporting teams, and can even lead to potentially faster propagation of cyber threats.

Additionally, in the overall context of incident reporting, there is increasing importance given to co-operation and threat intelligence data-sharing among all the different stakeholders to improve the capacity and resilience of the European cyber environment and to give more efficient and quick answers to new cybersecurity threats.

Objectives

CyberSec4Europe's goal in this area is to provide a platform that enables financial institutions to fulfil the mandatory incident reporting requirements according to the different procedures and methods specified by the applicable finance-related legislation and initiatives, such as PSD2 and the ECB Banking Supervision cyber incident reporting framework. This incident reporting platform will address the common need for standardised and co-ordinated co-operation in cybersecurity communication, and could also pave the way towards public and private co-operation in reaching the common goal of enhanced cyber resilience across Europe and beyond.

The two main categories of stakeholders are those entities who will be affected by, or who have an economic, technical, political or legal interest in the incident reporting process and, as a consequence, in this platform. As described in the report, *Requirements Analysis of Demonstration Cases Phase 1* (D5.1):

- Financial institutions are forced by different legislation and initiatives to report to different supervisory authorities on cyber incidents. It is worth highlighting that under different regulations a single financial institution could represent several subjects at the same time, each with specific requirements. For example, as TARGET2 participants, significant institutions (ECB SSM), payment service providers (PSD2), operators of essential services (NISD), personal data processors/data controllers (GDPR), or trust service providers (eIDAS).
- EU/national supervisory authorities are responsible for the different reporting requirements and receiving the corresponding reports. Each regulation/framework imposes a concrete and corresponding authority.

With this purpose in mind, we are working on a first prototype of an incident reporting platform that will cover incident events from the collection of data related to a detected security incident up to the generation of the mandatory reports to be sent to the competent authorities. We have defined three use cases to validate the different phases of the incident reporting workflow:

- data collection, enrichment and classification,
- managerial judgement,
- data conversion and reporting preparation.

Progress in the development of the platform will be reported in the project's demonstrator use case reports during the remainder of the project.

Benefits

Ultimately the incident reporting platform will benefit both sets of stakeholders listed above by facilitating the collection of security incident information, the actual reporting of the incident as well as compliance with the requirements of the supervisory authorities. For the financial institutions in particular, it will facilitate internal collaboration by providing a centralised tool available across organisational departments. In the wider fight against cyber attacks, the incident reporting platform will promote a collaborative approach to incident reporting and foster co-operation in enhancing cyber resilience, potentially beyond the financial sector.

Susana González Zarzosa Atos Spain, **Vanesa Gil Laredo** BBVA Group, **Laura Colombini** Intesa Sanpaolo, **Jani Päijänen**, JAMK University of Applied Science, **Wouter Joosen** KU Leuven and **Ivan Pashchenko** University of Trento

—

3 June 2021

Research challenges on incident reporting in the financial sector

Several research challenges emerge from the need to report cyber and operational security incidents detected in financial institutions to different national and supranational supervisory authorities in order to be compliant with the increasing number of directives and regulations that affect the financial sector.

In the second revision of the roadmapping work carried out in CyberSec4Europe, an analysis of the strengths, weaknesses, opportunities and threats in this area, as well as an analysis of the impact that Covid-19 and the green dimension on incident reporting have helped to identify and address these research challenges.

Not only is the financial sector highly regulated, but the current cyber incident reporting frameworks are also highly fragmented and create increasing complexity as well as additional regulatory and operational burdens for financial institutions, with the need to report:

- to different authorities and supervisors,
- with different taxonomies, thresholds, timing, templates and information requirements; and
- at different local, national, European and industrial levels.

This situation is adding costs and unnecessary overhead in the management of incidents and can lead to different threats, such as diverting resources from where they are most needed after a cyber incident occurs, limiting the impact of the incident and increasing the risks.

Consequently, there are three distinct research challenges identified:

- To overcome the lack of harmonisation of procedures which arises from this need to comply with multiple regulations and supervisory authorities. There are some open-source and commercial tools to support different tasks performed in the incident management process. However, off-the-shelf technology is not yet available to reduce effort and complexity and to improve the incident management and reporting procedures that need to be followed.
- To facilitate the collection and reporting of incident and/or data leaks which emerge during this process of gathering all the information required about a security incident, and the preparation of reports in an easy and timely way.
- To promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and overall cyber resilience. This challenge arises from the need for better co-operation among public and private entities to fight against cyber attacks and enhance cyber resilience. It would also connect with the long-standing tradition of collaboration that the EU has established amongst different stakeholders in the financial sector; namely, an awareness of the willingness to collaborate and the added value that this collaboration and orchestration brings.

The impact of Covid-19

Although there are no indicators that the financial or banking sector has faced an increased number of cybersecurity incidents since the outbreak of Covid-19, there are some reports, as published by Interpol and Europol, confirming that, during the course of the pandemic, cyber criminals have made a major shift from targeting individuals and SMEs to attacking major corporations and critical infrastructures. In addition, the number of cybersecurity incidents as a result of the quick transition from on-premises to remote working has suffered a significant overall increase. A key finding from the Interpol report is that malicious domains registrations increased by 569 per cent in the month from February to March 2020. Europol emphasises that not reporting cases to law enforcement agencies will obviously hamper any efforts, as important evidence and intelligence from different cases can be missed. Europol also reports that in the European Money Mule Action (EMMA 6) operation, only a few Covid-19-related cases were reported.

Embracing the green dimension

The European Green Deal, an ambitious plan put forward by the European Commission to green the European economy, has also had an impact on incident reporting solutions.

Current incident reporting processes involve generating reports, which almost always are printed on paper. Printed reports could be replaced by an environment-friendly digital platform for mandatory incident reporting which would reduce the need for wood and the pollution emissions associated with paper manufacturing. Such a digital solution would not only reduce pollution, but also provide additional functionality such as aggregation and data visualisation as related to cybersecurity incidents.

How CyberSec4Europe is addressing the challenges

To meet those research challenges identified, the following activities are being carried out by CyberSec4Europe:

- Definition and development of:
  - a mandatory incident reporting workflow for the financial sector
  - a data model for collecting the information required for the mandatory incident reporting in the financial sector
  - a common severity event classification procedure in the financial sector
- Design and deployment of a prototype of incident reporting platform, integrating open-source tools (such as The Hive and Cortex) with assets implemented in the project to cover the different stages in the incident reporting process. The platform will be also connected with threat intelligence data-sharing platforms through MISP.

- → Implementation of tools for:
  - workflow enforcement and reporting. The Atos Incident Reporting Engine (AIRE) has been integrated with the open-source incident management and response tool The Hive for the enforcement of the financial incident reporting workflow, support for managerial judgement and the preparation of the reports that need to be sent for mandatory incident reporting according to different regulations.
  - threat intelligence data-sharing. The three assets integrated in the platform to improve trustworthiness and reliability for threat intelligence data-sharing using MISP and the qualification of indicators of compromise to improve actionability are:
    - Trustworthy APIs for enhanced threat intelligence sharing (TATIS),
    - Reliable cyber-threat intelligence sharing (Reliable-CTIs) and
    - Threat intelligence integrator (TIE)

Further reading on the latest incident reporting and CyberSec4Europe's other roadmapping activities can be found in the report, *Research and Development Roadmap 2* (D4.4)

Supply chain security

Prabhakaran Kasinathan
and **Martin Wimmer**
Siemens AG

—

16 October 2020

Ensuring the security and integrity of supply chains

As end-users we all want and need to be sure about the quality and origin of the goods we consume, whether it's the food on our plates or essential commercial products such as smartphones or cars. Ensuring the quality and reliability of these goods becomes even more important for a society's critical infrastructure, when the goods are complex components such as power generators which are produced and integrated by multiple sub-contractors. It is self-evident that a reliable and secure supply chain is essential.

In addition, not only must non-compliance with standards be prevented, but also, when such violations occur, they must be detected so that the responsible parties can be held liable.

CyberSec4Europe addresses some of these requirements by developing novel approaches to model supply chains, using innovative technologies such as blockchain for the tracking and tracing of supply chain resources (eg, parts and materials). Our approach brings several advantages:

- the ability to model and validate a supply chain process efficiently before deploying it in the real world.
- replacing common paper-based audit trails by means of a digitised equivalent.
- avoiding out-of-band communications and sharing of information with a platform that records and tracks supply chain information.
- the reduction of costs and time needed for handling disputes; and
- replacing a centralised trust model with a distributed trust architecture, where single entities alone will not have the power to manipulate and change any information.

CyberSec4Europe is focusing on two concrete use cases:

1. dispute resolution, specifically in the context of retail, and
2. compliance and accountability in distributed manufacturing.

The security components and concepts developed – which will be showcased in the demonstrators – contribute to:

- reducing the likelihood of conflicts in distributed supply chain scenarios and, in case they occur, lowering the time and efforts needed to resolve them.
- monitoring and enforcing adherence to a company's processes and guidelines as well as compliance with legal regulations.

Dispute resolution for retail supply chain

This use case focuses on the management and reconciliation of disputes in the retail supply chain. A dispute may arise when a supplier sends a certain quantity of goods to a purchaser to fulfil an order. Let us consider a scenario where a purchaser has placed an order for a certain product quantity with a supplier. When the shipment arrives at the purchaser's warehouse, the purchaser notices a discrepancy in the received product quantity. As the shipment contains a lesser quantity than what was ordered, the purchaser raises a dispute. The reason for the discrepancy is that the supplier had to redirect some of the product quantity to another purchaser who had a higher priority. Resolving this dispute is a costly and time-consuming process and is disruptive to both the purchaser and the supplier.

The underlying blockchain platform of the demonstrator supports fast and effective conflict resolution. All the transactions between the supplier and purchaser are recorded on the blockchain. In particular, any discrepancies such as a change in product quantities are recorded on the blockchain and visible to all the transacting parties. In this case, the supplier creates a transaction, recording the reduced quantity of goods that are being delivered to the purchaser. This change, ie, the reduction of the delivery quantity, is immediately visible to the purchaser. To address the discrepancy, the supplier sends the remaining goods in a following shipment and, again, records this transaction on the blockchain.

Without a blockchain, the enterprise resource planning (ERP) systems of the purchaser and supplier are updated separately creating inconsistencies. If these systems are siloed, a reconciliation is not possible, and the transacting parties need to raise disputes to resolve the issues. A blockchain offers a consistent view of the transaction status for all the business stakeholders. This unified view leads to a lower incidence of disputes in case of supply chain discrepancies, and, if disputes do arise, then the resolution time is reduced.

Compliance and accountability in distributed manufacturing

This use case focuses on the compliance and accountability of the supply chains associated with the manufacturing of the main components in power generation stations, such as power transformers. Their design and production might take up to one or two years. Yet, any malfunctioning of such components, which could require their replacement, may impact the availability of the electricity grid in the affected region for months or even years. Therefore, this scenario addresses the challenges that large manufacturers face when producing goods via complex and distributed processes. These include not only the tracking and monitoring of the location, movement, and availability of parts, but also their quality and compliance.

Generally, compliance in manufacturing implies adherence to technical and corporate requirements, as well as legal regulations and industry standards. In order to prevent or minimise disruptions, we are researching and developing frameworks to detect the inclusion of poor-quality components or counterfeits in end-systems. Additionally, the developed mechanism can be used to determine who is responsible for non-compliant parts or resources.

The frameworks are used to model the manufacturing and compliance workflows and enforce the workflows on the actors involved. The workflow participants execute the workflow and record the resulting actions on a blockchain which provides immutability via cryptographically chained transactions and non-repudiation via transactions signed using public key infrastructure (PKI) identities. Thus, the blockchain helps manufacturers enforce compliance and standards, monitor and trace the resources in real-time, and, in case of an error, manufacturers can detect the root cause of problems with the help of the blockchain.

Demonstrator set up

An essential characteristic of distributed supply chains is that different stakeholders – such as manufacturers, suppliers and sub-contractors – collaborate and contribute to the provisioning of certain goods. In case of disputes, additional actors like independent consultants or expert witnesses will get involved to solve conflicts. The demonstrator developed for this use case will employ the following:

- A web interface allowing the supply chain participants to execute a supply chain business process (or a workflow) modelled and implemented using a Petri net-based approach. The workflow represents the state and conditions that the participant needs to fulfil at a particular moment to proceed to the next step in the workflow. The main benefit of the developed framework is that compliant supply chain processes can be modelled, verified, validated and enforced. The framework includes several components such as Petri net tools, a Petri net-based workflow execution engine and the corresponding smart contracts deployed on a blockchain.
- An immutable audit log based on distributed ledger technology, showing that any interaction in a supply chain context, like the delivery of goods with the corresponding assurance of the quality of goods (in the form of a bill of delivery), will be logged in a distributed ledger. The benefit of a distributed ledger is that information is accessible by all relevant stakeholders which provides a high level of transparency and fairness to partners. If needed, confidential information can be kept secret (eg, manufacturing process details and recipes) and made accessible only to trusted authorities in the case of dispute handling procedures.

In the case of conflicts, smart contract-based dispute resolution procedures can be triggered. The smart contracts used for dispute handling check the history of transactions, verify constraints and store their results on the blockchain. These smart contracts are well-defined and agreed between the various partners interacting in a distributed supply chain, so that the rules of enforcement are transparent to all.

For further information on this demonstrator use case, see our report *Specification and Set-up Demonstration case Phase 1* (D5.2).

Rodrigo Roman
and **Cristina Alcaraz**
University of Malaga

—

12 February 2021

Addressing the cybersecurity challenges of global supply chains

When we think about supply chains, we might visualise various images such as a large fleet of trucks traversing our countries, and ships sailing the seas full of containers. Yet the reality of supply chain networks is much more complex.

They are comprised by multiple tiers of public and private stakeholders (eg, manufacturers, suppliers, integrators, end consumers, supervisory agencies) engaged in the production, integration and distribution of products – which can be physical (eg, a photovoltaic plate), digital (eg, a smart grid software component) or a combination of both.

Such a complex global ecosystem requires the use of multiple information technologies (IT) and operational technologies (OT), which facilitate the management and co-operation between all stakeholders. However, this increasing complexity of supply chains makes the protection of each of its elements extremely difficult.

In fact, the number and impact of attacks that specifically target supply chains (eg, data breaches, service disruptions and manipulation of products) is on the rise.

For this very reason, one of the goals of the CyberSec4Europe project is to create a security-oriented roadmap that not only outlines the most important challenges related to the security of supply chains, but also describes the methods, mechanisms and tools that should be researched and developed.

Challenges and opportunities

Although it is impossible to achieve perfect cybersecurity resilience against supply chain threats, we must strive to create an environment where operations are performed in a secure and private way, where vulnerabilities are minimised, and where attacks are promptly discovered and managed. In order to achieve this goal, we must address the following major challenges:

- Detection and management of supply chain security risks
- Existing supply chain risk management (SCRM) strategies could be enhanced with automated, context-based risk assessment approaches, which could make more accurate decisions and provide better protection against unforeseen situations and new threat vectors.
- Security hardening of supply chain infrastructures, including cyber and physical systems

Beyond the integration of traditional security mechanisms within IT/OT networks, it is necessary to implement distributed detection, continuous monitoring and incident management systems, where multiple stakeholders can exchange sanitised threat intelligence information to adequately react against global events.

Security and privacy of supply chain information assets and goods
All stakeholders must access and exchange multiple types of information assets and goods. It is then necessary to deploy secure and private systems that not only provide a digital profile for all actors and products, but also automatically register and share supply chain events while streamlining compliance requirements and clearance processes.

Management of the certification of supply partners
Certification processes improve trust between supply chain partners, as they ensure that all services are working as intended and that all products have their advertised features. In order to improve such processes, it is necessary to provide automated mechanisms that not only can analyse standard requirements and partner infrastructures, but also can continuously monitor for compliance with standards and recommendations.

In addition, the recent pandemic has reminded us that the security of the supply chain is of paramount importance for both Europe and the world: fake medicines, unavailable services, and buggy or tampered software are only the tip of the iceberg that could cripple the delicate web of the global supply chain. We see here a clear opportunity for Europe to move in, promoting a global approach and a supply chain security standardisation effort.

More information on the research and development roadmap where not only supply chain but also other verticals are discussed can be found in our report *Research and Development Roadmap 1* (D4.3)

Privacy-preserving identity management

Stephan Krenn
AIT

—

23 November 2020

An education in preserving privacy

Secure user authentication and sharing of personal data are core activities in an increasingly interconnected world. Over the last few decades, multiple mechanisms realising this task have been developed, ranging from password-based authentication over biometrics and multi-factor authentication to online identity providers. However, while giving sufficiently high security guarantees for many application domains, most approaches do not pay sufficient attention to the users' privacy, leading to over-identification and insufficient protection of the users' personal data.

Another piece of the application use case puzzle is a demonstrator on privacy-preserving identity management as illustrated in an educational context – although the techniques and ambition are equally applicable in many other processes and scenarios.

One of the challenges, for instance, among existing solutions is that they often do not allow a user to selectively disclose personal attributes while keeping other data secret. As an example, when authenticating to a movie streaming service, it is necessary to prove that one owns a valid account and is old enough to watch a certain movie. It might not be necessary to reveal one's full identity or even one's precise date of birth. Similarly, when requesting a senior discount, there is no need to reveal one's full identity – proving one's age is sufficient.

Alternatively, solutions allowing for such minimal disclosure of information are typically using an online identity provider which vouches for the correctness of a user's claim. However, in such cases the online identity provider typically learns a full metadata profile about the user, as it is actively involved in any authentication process.

Ambitions

To meet these challenges, the main ambitions of CyberSec4Europe's pilot on privacy-preserving identity management are:

- → minimise the disclosure of personal data when sharing information in online identity management scenarios, including metadata
- → ensure that users have full control over their information and which data is revealed to whom
- → give formal authenticity and integrity guarantees for all data revealed to the verifier
- → support service providers to comply with legal regulations such as the GDPR

Learning to use ABC

In order to achieve these goals, the core technology will be an anonymous credential systems (or attribute-based credentials (ABCs). This cryptographic technology allows a user to receive a signature on her attributes (say, name, birth date, nationality) and then later to selectively disclose parts of this information (birth date etc) to a service provider, while blanking out all other information (ie, name, nationality).

Standard digital signatures are invalidated as soon as a single bit of the signed data is changed. ABCs still give the receiving party cryptographic authenticity guarantees on the revealed information, while fully protecting the user's privacy. In addition, the user may decide to only prove that she is eligible for a discount without revealing her full birth date. This can even be done in a way that gives high metadata privacy guarantees, as authentications performed by one user cannot be linked to another – unless the user explicitly consents to linkability during the authentication session.

Certified job applications

CyberSec4Europe will demonstrate this technology in the educational domain. Specifically, the pilot will allow users to receive digital certificates for passed courses and degrees from their university department. The users may then use these certificates in a privacy-preserving way in different contexts. For instance, students may prove that they have a university degree in a first formal round of a job application phase, without having to reveal the full name stated on the degree (eg, in cases where applications are handled in a semi-anonymised way in order to avoid a gender-bias). Or students may prove to public authorities that they earned a sufficient number of ECTS (European Credit Transfer and Accumulation System) points during the last semester in order to be eligible for some student allowance, without having to reveal the specific grades and courses taken.

The first phase of the pilot, covering the fundamental functionalities, will be executed over the next few weeks. The lessons learned regarding functionality, usability, and scalability will be taken into consideration for the further development and second piloting phase to be executed in 2022.

Antonio Skarmeta
University of Murcia
—
21 January 2021

CyberSec4Europe's roadmap for privacy-preserving identity management

In most identity management scenarios, there are different interests at play. Users are characterised by the different attributes that make up their identity. Service providers must verify that users comply with the necessary conditions to access services. These requirements may simply involve the knowledge of the typical username and password combination or include more sensitive data such as the user's age or location.

There is a growing concern that citizens, businesses and the EU Member States are gradually losing control of their data, their capacity for innovation, and their ability to shape and enforce legislation in the digital environment.

The final goal of CyberSec4Europe's research on privacy-preserving identity management (pp-IdM) is to provide a set of advanced mechanisms that can be integrated in various scenarios, in order to provide additional protection and privacy features to end-users, organisations and infrastructures. Thanks to the provided tools, European systems will be able to perform authentication and authorisation processes with strong trust, while enforcing user privacy.

To this end, the pp-IdM research team has performed an analysis of the topic, resulting in a description of the EU's strengths/weaknesses/opportunities/threats in relation to privacy and identity management with the identification of several key challenges:

(1) GDPR and eIDAS impact interoperability,
(2) Unlinkability and minimal disclosure,
(3) Password-less authentication,
(4) System-based credential hardening,
(5) Distributed oblivious identity management,
(6) Privacy preservation in blockchain, and
(7) Identity management solutions for IoT scenarios.

The following briefly describes why these challenges have been considered.

During authentication, more information than intended may be revealed by a user to a service provider, or the information revealed to multiple service providers may be pooled to create a more complete picture of the user's identity than expected (2). Also, a malicious or compromised issuer can track user activity which may lead to breaches of privacy (identity data is revealed) or even to identity theft or forgery (5). Lastly, it is necessary (and/or desirable) to conform to existing regulations regarding privacy while keeping in mind the possible interoperability issues (1).

However, protecting the user from malicious (or compromised) actors is not the only challenging matter. Other risks come from the software tools that are used or the possible misuse by the user himself. For example, the most widespread method for authentication is the use of username plus password. While the method itself can be secure, in practice it leads to possible breaches because of weak or reused passwords and offline attacks (3). Also, when cryptographic materials like certificates or credentials are involved, they become assets that must be protected so they do not put the user's identity at risk (4). Lastly, as new scenarios and technologies arise, they must be either protected, as in the case of IoT scenarios, or taken advantage of to achieve privacy-enhancing solutions, like blockchain (6).

So far, the work done has resulted in the development of roadmaps that delineate the research efforts for tackling these challenges. The first phases of work have already been completed and focused on through the analysis of the different issues (eg, a comparison of different existing solutions or requirements analysis).

Also, first steps in developing the solutions have been taken, like the design of architectures for the systems that will be proposed, a definition of GDPR guidelines or first reference implementations of the components and their evaluations.

The latest results of CyberSec4Europe's work on roadmapping privacy-preserving identity management are available in our report *Research and Development Roadmap* (D4.4).

2.3
Roadmapping

CyberSec4Europe defined a common cybersecurity research and innovation roadmap – also referred to as a research priority list – which clearly identified the short, medium- and long-term priorities and provided the strategic direction to be addressed by the European Cybersecurity Competence Centre and Network.

Our roadmapping work had a dual goal which was to identify the research directions that the application demonstrator domains needed to focus on in their day-to-day, short- and medium-term work as well as the cybersecurity challenges for the broader community to address.

By reaching out beyond the project, we interacted with researchers, practitioners, other research projects, European organisations and EU agencies, mobilising relevant partners and contributing to and leading several roadmapping activities. We also played an instrumental role in the roadmapping task force which developed a set of research priorities along with supporting material that are considered important for years to come.

Finally, the roadmapping community summarised its views for the future in a 'Blue Book' that contains our future horizon roadmap and outlines not only research priorities but also lists the major challenges that need to be addressed, such as, "Make smartphones secure" or "Provide online the same levels of privacy people have offline".

David Goodman
Trust In Digital Life
—
2 December 2021

Roadmapping – a cybersecurity strategy for Europe

A key aspect of the original call for proposals, which led to the funding of the four pilot projects including CyberSec4Europe, was the implementation of a common cybersecurity research and innovation roadmap – also referred to as a research priority list.

The motivation for and significance of this roadmap is that it should clearly identify the short-, medium- and long-term priorities to be addressed by the European Cybersecurity Competence Centre and Network, that is now being put in place under the direction of the European Commission. It will provide the strategic direction not only for the Horizon Europe and Digital Europe funding programmes but also for the work of ENISA, Europol and other EU agencies and bodies.

CyberSec4Europe's response to this directive is to publish a yearly research and development roadmap which aims to explore emerging threats and prioritise research directions, mainly in the areas of the seven verticals associated with the project: open banking, supply chain security assurance, privacy-preserving identity management in higher education, incident reporting in finance, maritime transport, medical data exchange and smart cities. The first roadmap published in 2020 focused on outlining the cybersecurity research areas associated with these verticals and establishing the most important priorities and challenges in the following 12-month and 24-month periods and by the end of the project.

Now in its third iteration, the contribution associated with each vertical has expanded to providing a 'big picture', a scene setter for the scope of the business and/or technology area being addressed. Although the vertical sectors being reviewed are also the subject of the project demonstrators, the scope of the roadmapping exercise goes beyond those individual use cases. For each vertical, questions are asked as to what is at stake and what could go wrong – and consequently what needs to be protected and hence identifying where possible who the attackers might be. In this latest report, we also look at what were the major incidents that took place over the last 15-20 years. With some of the verticals, the technology under the spotlight is sufficiently new that it hasn't attracted any significant attacks, although we can only assume that this is just a matter of time.

The meat of the report looks at identifying and categorising the main cybersecurity challenges, also summarised in a detailed SWOT (strengths, weaknesses, opportunities and threats) analysis. The five to six challenges are analysed, both in terms of relevance to the 'big picture' as well as the mechanisms and tools needed to address them.

Mindful of current events beyond the 'normal' purview of cybersecurity, the report also takes a look at specific topics of global concern: the impact of – and on – Covid-19 and other health issues, the green dimension as well as the vertical's influence on addressing climate change issues. Equally relevant are the insights provided on what impacts there may be pertaining to democracy. Each vertical is asked to highlight sector specific dimensions, which in one case included Brexit!

Now that the project is entering its final phase, the objectives each vertical would like to see accomplished are set out in three new periods: by the end of the project, by 2025 and, hardest of all given the pace of changes in technology and cybersecurity, by 2030.

The overall report concludes with a survey of other current cybersecurity roadmaps – from the other three pilot projects, ENISA and Europol, all of which have fed into the comprehensive approach taken in the EU Cybersecurity Strategy for the Digital Decade which focuses on the following ten areas:

- Resilient infrastructure and critical services
- Building a European Cyber Shield
- An ultra-secure communication infrastructure
- Securing the next generation of broadband mobile networks
- An Internet of Secure Things
- Greater global Internet security
- A reinforced presence on the technology supply chain
- A cyber-skilled EU workforce
- EU leadership on standards, norms and frameworks in cyberspace
- Co-operation with partners and the multi-stakeholder community
- Strengthening global capacities to increase global resilience

According to some, a distinguishing feature of roadmapping is the use of structured visual representations both to communicate and articulate strategic thinking. With that in mind, the roadmapping focus group, composed of representatives from the four pilots plus ECSO (that first came together in June 2020) produced a distinctive visualisation of a common research roadmap which can be supported by the entire community. After consultations with the JRC (Joint Research Centre) and DG CONNECT, the group has created a set of research priorities which will eventually find their way onto the Cybersecurity Atlas website. Although the focus group delivered its first input during the summer of 2021, it is envisaged that the bulk of its activities will happen over 2022, reaching its pinnacle during the second semester of 2022.

The prioritised focus areas are ranked in no particular order and are seen as most notable yet non-exhaustive.

- Governance and capacity building (collaborative networks, education and training, certification)
- Trustworthy ecosystems of systems (secure platforms of platforms, infrastructure protection)
- Disruptive and emerging developments (secure quantum technologies, secure AI systems, personalised protection)
- Trust building blocks (holistic data protection, AI-based security, systems security and security management, secure architecture for next generation communication)

As expected, these focus areas are generally intertwined with each other. Also, the current scope of the group's work does not yet cover research priorities with respect to specific vertical sectors, an additional dimension that will be addressed in future releases.

It is gratifying to realise that the EU's early objectives to create a common cybersecurity roadmap generated by the wider community are slowly but surely coming together.

For further reading see our report, *Research and Development Roadmap 3* (D4.5).

3

Education, tools and standards

CyberSec4Europe addressed the need to ensure the provision of educational courses to provide a sufficient number of highly skilled cybersecurity engineers, scientists and other specialists, who will have the necessary tools and appropriate standards to develop solutions to future industrial, scientific, societal and political cybersecurity-related challenges.

3.1
Cybersecurity skills and capacity building

Are European universities providing adequate courses in all areas of cybersecurity? Or are there much-needed cybersecurity skills being neglected? CyberSec4Europe identified and prioritised the cyber skills needed, alongside investigating existing cybersecurity curricula at university level.

Our setting of an education and training framework and related instruments provided support for continuing education and lifelong learning in the area of cybersecurity for a wide audience, including university students, professionals and the general public.

It was organised to demonstrate the effectiveness of the governance models and the full transfer of the pilot results to the future Centre's operations. Transferability stands on the definition of learning objectives and competences, required to develop and enhance cybersecurity skills for different profiles and roles, which are based on international knowledge taxonomies.

We specified knowledge units and curricula, training and awareness to achieve such objectives and competences and set activities to apply and test such competences. We implemented a CyberSec4Europe education strategy for citizens, students and professionals through the creation and promotion of the CyberSec4Europe brand and the guidelines and procedures to produce and consume content from platforms developed in the activity on tools and infrastructure.

We did not aim to produce all possible content required to implement the specified educational and training programmes, but instead to set and run its platforms as a capability-building instrument open to external sources and third-party material outside the consortium (if they meet guidelines and quality standards), to allow the programme to be bootstrapped in the future beyond the project.

Alberto Lluch Lafuente
Technical University
of Denmark

—

14 February 2020

Addressing the shortage of cybersecurity skills in Europe

The European Union needs to ensure that sufficient highly-skilled engineers, scientists and other cybersecurity specialists are educated to be ready to support and lead solutions to current and future industrial, scientific, societal and political cybersecurity-related challenges. But how well is the EU doing in this area? Are European universities educating students in all areas of cybersecurity? Or are much-needed cybersecurity skills being neglected?

One of the aims of CyberSec4Europe is to identify and prioritise the cyber skills needed at university level, and to investigate existing cybersecurity curricula. As a first step towards such a goal, the project report *Education and Training Review* (D6.2) presents a review of existing European university MSc cybersecurity programmes.

The review is based on a survey of more than a hundred MSc programmes at participating universities in EU Member States. The heads of studies or other senior members at these universities were contacted through the extensive CyberSec4Europe partner network and using existing education maps in cybersecurity, such as the one provided by ENISA.

The survey uses well-understood terminology for cybersecurity knowledge topics and skills drawn from existing cybersecurity curricula frameworks, such as the *ACM Cybersecurity Curricula* and *NIST's NICE Cybersecurity Workforce Framework*. Based on the analysis of the survey data collected, the summary focuses on pinpointing the cybersecurity skills that are either sufficiently or insufficiently covered by individual Member States and the EU as a whole.

Our main findings identify a set of cybersecurity knowledge areas and topics that are insufficiently covered by the surveyed education programmes and countries. We believe that our findings, together with European initiatives like the JRC taxonomy, the Cybersecurity Atlas, and the new edition of the ENISA cybersecurity map, can be a good starting point for the identification and prioritisation of the cyber skills needed in the European Union, and that those skills should be promoted to enrich cybersecurity education programmes. The apparent lack of focus on topics related to system retirement, security- and privacy-by-design is critical as the use of legacy and third-party software and systems, possibly produced outside the EU, and their dismantling and replacement poses challenges to security and privacy that require specialised training and skills.

Simone Fischer-Huebner
Karlstad University

—

14 January 2021

CyberSec4Europe and CONCORDIA organise survey on MOOC certification

The two cybersecurity pilot projects, CyberSec4Europe in co-operation with CONCORDIA, have jointly organised a survey on the certification of MOOCs as part of an investigation regarding the future of MOOCs in cybersecurity and the value of a possible related certification.

Massive Open Online Courses or MOOCs are frameworks that provide online, accessible collaboration and learning spaces where learners can participate in a training course, interact with other students, complete assignments etc. MOOC courses still contain the basic characteristics of traditional courses (eg, training material, instructors, participants etc) without having to be subject to traditional constraints (eg, location, participation etc)

Although 2012 was named 'The Year of the MOOC', the year 2020 and the Covid-19 crisis have given an unprecedented rise in MOOC participation. For example, three MOOC providers (Coursera, edX, and FutureLearn) registered as many new users in April 2020 as in the whole of 2019.

The sheer volume is staggering. There were 32.7 million new users registered across four platforms during 2020 representing a 120% increase on the number of registrants in 2019. With hundreds of MOOCs currently available, the industry is expected to grow at a rate of at least 40% over the next seven years.

MOOCs have been implemented for a variety of subjects, one of which is cybersecurity. Given the existing cybersecurity skills gap in Europe, the role of such MOOCs is increasingly significant and is attracting widespread attention. With MOOC utilisation undergoing such hype driven by the numerous provided solutions, this survey aims to identify whether there is a need for further standardisation of (cybersecurity) MOOC implementations and whether a possible certification scheme would provide added value to the learner, the offering institution or any other interested party.

The closing date for responding to the survey was 8 February 2021. Participation was completely voluntary. Demographic and other personal data was used in pseudonymised form for the research purpose of collecting and analysing opinions on quality criteria of MOOCs and MOOC certification and processed in compliance with the GDPR. The data controller was Karlstad University.

Anni Karinsalo
VTT Technical Research
Centre of Finland

—

13 November 2021

A better view on the cybersecurity professional education

There is an urgent requirement to improve European cybersecurity skills and competences which starts by addressing the availability of relevant education programmes, the lack of which poses a grave risk for all stakeholders in European society.

CyberSec4Europe's report *Design of Education and Professional Framework* (D6.3) reviews the most common cybersecurity-related professional frameworks and analyses the challenges and requirements for quality professional cybersecurity education courses and proposes several framework taxonomies and methodologies in support of providing professional cybersecurity programmes.

A credible education programme builds on identifying the particular skills and competences, and at what level, as required in various cybersecurity-related roles.

This can be achieved by prioritising the cyber skills needed for security professionals in general. Furthermore, it is feasible to assess how educational, customisable cybersecurity programmes for professionals can be built in the light of already existing industry programmes. This requires designing a methodology for this particular process, and implementing the related capabilities required to run such programmes.

The report establishes a framework for cybersecurity professional categories, and a scale for assessing the skills and skill levels for each category. The end goal is to provide good educational resources for those wanting to learn about cybersecurity, and some form of criteria that people can present as evidence of their qualifications for cybersecurity-related employment positions. The framework is based on that defined by CyberSec4Europe, and on other common frameworks that have been proposed in the field of cybersecurity. To enhance the framework applicability and build relevant and wide-ranging job profiles for the framework, four specific use cases with twelve scenarios are presented.

The skills required in each of these scenarios are evaluated from which related job profiles are derived. Then the average cybersecurity skill level for each profile required in each of the scenarios is evaluated according to a four-step skill rating scale. From the scenario evaluations, the report concludes that the most needed skills in such scenarios are data integrity and authentication, access control, secure communication protocols and usable security and privacy. Less often required skills are in the areas of cryptanalysis, design, component procurement and system thinking. In general, most scenarios require a multitude of broad cybersecurity skills.

Even though skill requirements related to the scenarios represent a particular point of view, some general conclusions can be drawn. Because the variance of required skills can differ vastly depending on the role, general cybersecurity programmes targeted to a certain work environment might be useful to some extent. However, to efficiently add value, there is need for a well-justified and customised skills education for a certain professional group.

Also, an analysis of a scenario of this kind, in the form of a standard and easily comparable table framework, may help point to the breadth of skills needed. The framework can help visualise highly relevant cybersecurity skills that can be difficult to discover otherwise. For instance, when considering a cybersecurity education offering in general for IT professionals, usability skills might often be overlooked in favour of technical skills, even though an awareness of usable security and privacy is required in many of the scenarios at an advanced level.

In addition, this kind of illustration reveals overlapping education needs and may help combine different target groups when arranging cybersecurity education.

In the future, we aim to validate our work with a wider audience, using a targeted survey. Our aim is to ensure that the evaluations via our framework help organisations resolve what kind of skills education would be most beneficial for their professionals.

3.2
Open tools and infrastructures for certification and validation

To support cybersecurity education, testing, and certification, CyberSec4Europe delivered a number of tools such as Cyber Sandbox Creator – a versatile tool for creating lightweight virtual labs – and tested them in real time including in a series of cyber range exercises.

Our work targeted open cybersecurity tools and infrastructures for two types of users – end-users and security professionals involved in cybersecurity certification and validation.

The set of open-source tools and operating systems in the *Open tool portal* forms a secure and usable desktop environment for two defined end-user types – beginner and intermediate – with different levels of security/privacy skills and knowledge. Those with no experience at all may have moderate general IT skills and can install applications and undertake basic settings according to instructions. Others with moderate security/privacy skills and knowledge could be keen to explore relevant tools and applications further and willing to undertake advanced settings under instruction.

The whole project evaluated multiple candidate open tools in each of the categories, and we provided specifications of ideal candidate traits and test evaluations for each individual tool category.

The *Open tools for professional use* section on the portal presents and describes five expert tools that we developed. The main tool is the Cyber Sandbox Creator – a virtual lab (cyber range) for open-source tools education and research, successfully tested both with universities and companies in several European countries.

Beyond core tool development and testing, we organised and provided tools for two multi-national cyber range exercises (flagships) and also examined the role of certification for cybersecurity and its implementations.

Jan Vykopal
Masaryk University
—
2 December 2020

Supporting cybersecurity education, testing and certification with Cyber Sandbox Creator

The need for educational training of cybersecurity experts is growing rapidly. In 2019, the (ISC)² Cybersecurity Workforce Study estimated there are 291,000 unfilled cybersecurity jobs in Europe: an amount that has almost doubled since 2018. To address this gap, we need to educate new specialists and provide tools that would allow specialists to fulfil their work tasks efficiently.

To support cybersecurity education, testing, and certification, we have delivered Cyber Sandbox Creator – a versatile tool for creating lightweight virtual labs. Cyber Sandbox Creator builds isolated lab environments for cybersecurity training, experimentation, or testing based on user input.

The lab environments can be then distributed to individuals and small and medium organisations. Key benefits of the created labs are:

- Lightweight design. The lab can be hosted on a standard PC or laptop and used with zero additional costs. The only limit is the available system resources of the host PC.
- The lab can be hosted at any standard hosting operating system: Windows, Linux, and Mac OSX.
- The lab uses proven and open-source components and best practices.

We have tested the lab at at Masaryk University to prepare and configure custom environments for cybersecurity training of our students. Students were provided with the created lab and completed their tasks there or worked on their thesis projects. We have recently provided Cyber Sandbox Creator to instructors at the Slovak Technical University in Bratislava, who will follow this approach.

Another use case is now being tested by a medium-sized company from the Czech Republic, which simulates its industrial control system in the lab environment created with Cyber Sandbox Creator.

Cyber Sandbox Creator uses the same format for the definition of a virtual environment (sandbox) as KYPO Cyber Range Platform. That means users can save time and costs for developing and testing their sandboxes locally at their computers before deploying them to a fully-fledged cyber range platform. We also piloted this use case and thus demonstrated a successful operational federation of Cyber Sandbox Creator and KYPO Cyber Range.

We have released the first prototype of Cyber Sandbox Creator as open-source and look for early adopters from other institutions who would like to try their use cases and provide feedback.

If you are interested, check out our public project repository and e-mail us at svabensky@fi.muni.cz.

David Goodman
Trust in Digital Life
—
27 April 2022

Introducing SURFACE – a support framework for certification

CyberSec4Europe is proud to introduce its development of SURFACE, a support framework for certification that provides an integrated approach for the process of certifying and rectifying Internet-based products and solutions based on a range of current contrasting but complementary certification schemes.

The borderless nature of infrastructures such as the Internet of Things (IoT) and cloud computing, and the associated threats involved means that any vulnerability or security incident in one country can have disastrous consequences across the European Union.

A vulnerability can easily affect more than one system and can be propagated very quickly. While Europe is leading large initiatives to guarantee the security of these systems, such as the Cybersecurity Act 2019, it is still not yet clear how to deal with vulnerability dependencies in such a complex environment.

The certification of products and services helps to systematically test and assess the security targets, and the certificate provides a degree of assurance to consumers. However, there are very many different standards and protection profiles out there to choose from and the results are often not easy to comprehend by someone not involved in the process. Moreover, the assurance reports and resulting certificates present the information as free text, and are, therefore, difficult to process automatically. The dependencies on other products and certificates are static and, when something happens to the connected certificate, the issue is often not propagated.

Hence, the rationale for the development of SURFACE, an integrated approach for the process of certifying and rectifying. SURFACE brings together solutions from the EUCC scheme, the ECSO meta-scheme, the ARMOUR methodology and NIST SP 800-137. We have combined the solutions in such a way that they complement each other at different steps. The ECSO meta-scheme allows the integration of certification schemes or standards. The ARMOUR methodology supports SURFACE in establishing the context, testing and communication of the result processes. NIST SP 800-137 supports continuous monitoring for patches or updates. SURFACE supports incremental certification, which reduces the cost and time taken for recertification. SURFACE uses the EUCC guidelines throughout the process starting from the selection of assets to the recertification process. Hence, it is in accordance with articles of the Cybersecurity Act.

SURFACE also takes advantage of the cybersecurity certificates information and the MUD (manufacturer usage description) files to manage security dependencies and provide mitigations. This way the dependencies can be traced when a new threat is discovered. On the one hand, the certificate indicates certified subcomponents that the system has, and on the other hand, the MUD file indicates the connections with other services not certified or not considered in the certificate. Knowing the affected services, we can apply fast mitigations before a patch or update is released by the manufacturer.

SURFACE also provides a template for a structured certification report which will make the result more easily analysable and helps discover dependencies between certificates. If a new vulnerability occurs and a certificate is revoked, other affected certificate holders can automatically be notified.

If you're interested in more details of how SURFACE could improve the robustness of your systems or infrastructure to new threats, the CyberSec4Europe report, *The Role of Certification and its Implementations* (D7.7) has more information.

Vaclav Matyas
Masaryk University
—
27 June 2022

CyberSec4Europe – open tool portal

The recently published *Open Tool Portal* presents two groups of open tools that are of interest to both security experts and users with little or medium experience in security tools and technologies.

Open tools for professional use

This portal section presents five expert tools developed within the project, described briefly in the sections that follow. The main tool is the Cyber Sandbox Creator (CSC) – an open-source tool for building lightweight virtual laboratories for cybersecurity education, testing and certification. Since February 2020, CSC has been used in practice numerous times and has been continuously improved to address the needs of a broad range of users. We identified six target user roles that can benefit from the tool: educator, trainee, researcher, developer, specialist, and auditor. CSC is referenced in a CyberSec4Europe report, *Virtual lab for open-source tools education and research* (D7.2), and was also accompanied in another report, *Common virtual lab with open-source tools for research and development* (D7.4), where it was integrated with parts of the expert tools described in the following sections. To create a virtual lab environment, a knowledgeable user first writes a sandbox definition: semi-structured text files describing virtual machine parameters and configuration of network topology. Then, CSC uses these files as input to generate an intermediate definition for Vagrant and Ansible. Finally, the result is distributed to regular users, who execute CSC to instantiate the actual virtual lab.

The sec-certs set of tools downloads, processes, and analyses security certificates issued under Common Criteria and NIST FIPS 140-2 schemes and turns these into computer-searchable and analysable datasets. As a result, the following and other questions can be answered:

- What chips are impacted by flaw found in certified library X?
- Which certificates are relevant for my certified product Z?
- What products are affected by specific common vulnerabilities and exposure (CVE) vulnerability?
- What devices were analysed for timing side-channel leakage?
- Is ECC 521-bit curves supported?
- What are the trends of whole certification ecosystem regarding the archival rate, achieved security levels, usage of protection profiles and others?

The certification reports are the most detailed publicly available documents, yet currently available as PDF reports in non-standardised format with only some metadata extracted (eg, FIPS140-2 extracts referenced certificates). The sec-certs downloads source documents (as PDF reports describing certified configuration and security target, CSV and HTML with additional metadata) and extracts relevant information using regular expressions created for specific areas like certificate references, cryptographic algorithms, security assurance levels and many others. The information extracted is stored in open format (JSON) and further used to analyse certificates, map them to other sources like a CVE vulnerability database and construct aggregate visual presentation available at seccerts.org. The sec-certs tools also allow the users to process all data locally including additional own, non-public documents.

SCRUTINY is then a set of tools allowing users to verify that all devices (eg, cryptographic smartcards) match the expected forensic profile to detect chips of different revision, malfunctioning or even a counterfeited one.

RTT toolset provides and easy-to-use assessment of the randomness properties of data generated by a truly random data generator (eg, physical TRNG) or pseudo-random generator (eg, AES ciphertext, PRNG).

The fifth set of tools provides for exhaustive implementation testing of existing RSA and ECC implementations and verifies that the required security-relevant checks like known invalid inputs tested (EC point not on curve, invalid curve parameters...) are performed. Automatic analysis of library output artefacts (generated keys, side-channel leakage...) is collected and any deviances (even if not directly exploitable) from the common behaviour are searched for and detected. A black-box analysis is performed, allowing for analysis also on the closed, proprietary devices.

The typical use-case scenarios are:

- Automatic testing during development (eg, continuous integration).
- Initial thorough analysis of a specific card or library.
- Generation of behavioural forensic profiles for later comparison of the libraries including the closed, proprietary ones.

Tools for end-users

This section of the portal presents a set of carefully selected open-source tools and operating systems, forming a secure and usable desktop environment for the two defined user types – beginner and intermediate users. CyberSec4Europe evaluated multiple candidate open tools in each of the categories, and we provide specifications of ideal candidate traits and test evaluations for each individual tool category. The portal for both can be found on the CyberSec4Europe website under Our Results.

Jani Päijänen
JAMK University of Applied Sciences

—

8 January 2021

CyberSec4Europe maps European cyber ranges: training against cyber attacks

European cyber ranges and their features have been studied by JAMK University of Applied Sciences. The comprehensive survey is the first of its kind in Europe.

Thirty-nine reported European cybersecurity training environments – cyber ranges – were found in the study. The most cyber ranges reported by country are in Finland, seven in total. Finnish cyber ranges can be found at JAMK's Cyber Security Research, Development and Training Center (JYVSECTEC), VTT, the University of Tampere, Turku University of Applied Sciences, Rugged Tooling Oy and two actors who remain anonymous. There are four similar environments in Sweden, three in Germany and Greece and the rest are evenly distributed across Europe.

According to the study, cyber ranges were mainly used by companies and public organisations, as well as by students in engineering bachelors and masters degree programmes. Companies and organisations use environments to develop staff skills and to develop business continuity and resilience to cybersecurity incidents. Cybersecurity exercises in training environments range from short-term exercises to multi-day national cyber-disorder exercises. Organisations from different countries participate in international co-operation exercises.

Industry-specific systems, often related to critical infrastructures such as industrial and process automation, IoT environments, and logistics, have been modelled for several environments. Few environments have been modelled from the perspective of realistic Internet use. Somewhat surprisingly, the study found that traditional office and computer network infrastructure systems were under-represented in cyber ranges. It was noticeable that the international vocabulary related to cyber practice and training environments is inconsistent.

The possibilities for co-operation in the cybersecurity environment were explored through interviews. The technical capacity for concerting cyber ranges was perceived as challenging, but collaboration is necessary. The technical federation of cyber ranges enables participants to have a more comprehensive and realistic training experience. In order to interconnect or technically federate cyber ranges, a requirements specification was developed, which enables the composition of several different environments into a single training environment. Interconnection is possible with both open-source and commercial products.

"The idea behind the requirements specification is to make it easier for companies and organisations to participate in more extensive cybersecurity exercises. The entity offers its users features that one operator would not be able to offer" according to Juha Piispanen, JAMK's expert, who prepared the definition.

The connection method created on the basis of the definition was tested in January 2021, when a two-day cybersecurity exercise, Flagship 1, was organised at JAMK's IT Institute.

It was the first of its kind and required no previous experience, being open to representatives from CyberSec4Europe partners.

During Flagship 1, participants were provided with guidelines concerning a fictional organisation they would be working for. With the available documentation, participants were able to examine and analyse a cyber attack and seek to mitigate the damages. The short duration of the exercise provided an interesting challenge: one of the key questions is what to expect participants are able to learn in a complex learning situation in such a short time.

In the exercise, the fictional organisation's internal and external communication representatives were alerted. The recent cybersecurity attacks in Finland and abroad have shown that communication is usually a duty of non-technical employees. A detected successful cyber attack not only concerns the targeted organisation, but also an organisation's ecosystem and its stakeholders who need to receive timely updates on the attack and its aftermath. With the now-piloted exercise, attendees should gain a good understanding of how a team could collaborate and communicate during an incident response.

The technology behind Flagship 1 is based on Realistic Global Cyber Environment (RGCE), a cyber arena developed in JAMK's cybersecurity research, development and training centre, JYVSECTEC. The platform development started in 2011 and the first national cyber exercises were held in 2013. Since then, RGCE has been used in various realistic cybersecurity exercises and in masters level cybersecurity education at JAMK.

In Flagship 1 an open-source SD-WAN interconnection requirement specification is proven. It is used for interconnecting various cyber range internal and external services and endpoints. The implementation is based on a requirement specification, documented in Part B of CyberSec4Europe's *Report on existing cyber ranges, requirements* (D7.1) A report on the experience and lessons learnt during the exercise will be published and made generally available.

Jani Päijänen
and **Juha Piispanen**
JAMK University of Applied Sciences

—

29 October 2021

Cyber range federation – the real benefits

The ICT landscape in organisations and companies is complex. Rarely do organisations plan, commission, operate or decommission their infrastructure themselves, but outsource the function to one or more service partners or rely on 'as-a-service' kind of delivery model for software, hardware, and ICT-infrastructure. Such multi-vendor delivered end-user services require a skilled workforce to manage and lead the whole operation, whilst keeping running costs low and quality high, especially with respect to cybersecurity.

As a result, organisations and companies which have understood their high dependence on technology, although not managing it themselves, have taken the precautionary step of training their employees and service partners in the anticipation of potential cyber incidents by using cyber ranges.

Individuals can be educated in many aspects of real-world cyber-attacks and cybersecurity good practices through training exercises and research on cyber ranges. These technical environments are connected to a network, running software on a hardware platform, or simulating a modern data centre running virtualisation software. Some cyber ranges contain cyber-physical elements, such as medical devices and patient simulators. Cyber ranges that are realistic, running the commodity software and services found in an office, and having business domain specific capabilities, found for example in a factory facility or a healthcare unit, can provide an immersive and realistic exercise experience for the participants. By attending a realistic cyber exercise, participants might even face real malware or ransomware they may encounter in their work. An organisation participating in a cyber exercise develops their employees' skills thus improving its preparedness for cyber incidents and ensuring business continuity after a cyber attack.

Developing and operating a cyber range requires investment in labour costs, hardware procurement, software licences, facilities rental and electricity, to name a few. Developing and operating a cyber range also requires a skilled workforce, as technology itself cannot fulfil the needs and expectations a cyber range owner has set.

To relieve the pain of investing in the development of cyber ranges, and to maximise the operating hours, cyber ranges can be interconnected or technically federated. In a technical federation, cyber ranges may cross-use federated cyber range capabilities, features and capacity, offering a single venue to end-users. Thus, federated cyber ranges can use the capabilities and features already available in a cyber range, without making additional investments. The lifespan of a technical federation may be temporary or permanent, depending on the needs of the cyber range operators, their end-users and the contracts that have been negotiated.

In the recent CyberSec4Europe report, *Evaluation report on integration demonstration* (D7.3), only open-source software solutions to implement cyber range technical federation were identified and evaluated. One solution met the set requirements (identified in our earlier report, *Report on existing cyber ranges, requirements* (D7.1), and was demonstrated in our Flagship cybersecurity exercise. For the cyber exercise, two use cases were implemented:

1. Federating a commercial Amazon AWS cloud component into a cyber range
2. Creating a federation network for end-users joining the cyber exercise

Both implemented use cases were seamless to the end-users. In the demonstration, network traffic was tunnelled in the federation network through the public Internet between the participants' commissioned workstations and exercise network, and between the exercise network and Amazon AWS.

The participants in the demonstration event were simultaneously located in 16 EU Member States. The feedback that the cyber exercise conductor received from the participants was highly positive, indicating that not only did the perceived cyber range technical federation perform well, but also the contents of the exercise met or exceeded expectations.

The demonstrated open-source software-only solution performed with high throughput, low latency and low CPU usage, as monitored by the cyber exercise conductor from the exercise network. The tested solution is estimated to be production-ready to be used in cross-border cyber exercises. The benefit of software-only open-source solutions is that no investment in hardware or software licences is required to establish a cyber range technical federation.

However, a skilled workforce to plan and implement a federation network is required.

Jani Päijänen
JAMK University
of Applied Sciences
—
16 March 2022

Flagship 2: The successful second cybersecurity exercise hosted by CyberSec4Europe

Flagship 2, the second CyberSec4Europe cybersecurity exercise conducted in January 2022, consolidated the high quality of standards previously set by Flagship 1. In addition to representatives from CyberSec4Europe, Flagship 2 also engaged a highly motivated external community of cybersecurity enthusiasts, serving as clear evidence of a pressing market need for this type of educational facility.

The two-day cybersecurity exercise was designed, orchestrated and post-analysed by JAMK University of Applied Sciences – one of two CyberSec4Europe Finnish partners.

As with its predecessor, the Flagship 2 exercise was designed as a learning experience, built on the Flagship 1 narrative, that demanded no previous technical cybersecurity expertise from its participants. However, Flagship 2 included for the first time an open track, offered in parallel to the CyberSec4Europe partners' track:

- Participants in the open track ('the analysts' activity') analysed samples exported from the exercise environment and reported their findings to the exercise using a dedicated self-hosted open-source Capture The Flag (CTF) platform. Analysts worked alone, without any instructions on how to analyse the samples.
- Participants in the partners' track ('the exercise') played the role of employees of a critical infrastructure provider, a fictional Italian train operator. The employees detected operational anomalies which they had to investigate. This revealed an active threat actor in the environment, who had penetrated the train operator's network and had modified the on-train firmware which was guarded by a trusted platform module. The exercise participants followed the attack path, cleared the environment and detected the initial weakness that allowed the threat actor to penetrate the network.

For the exercise, the technical environment was a realistic global cyber environment (RGCE), ie, a cyber arena that contains several cybersecurity training environments or cyber ranges. This included a new environment that simulated a railway operator's IT and OT infrastructure, several networks providing, for example, on-premise data centre and traffic control systems, office and other common networks and services.

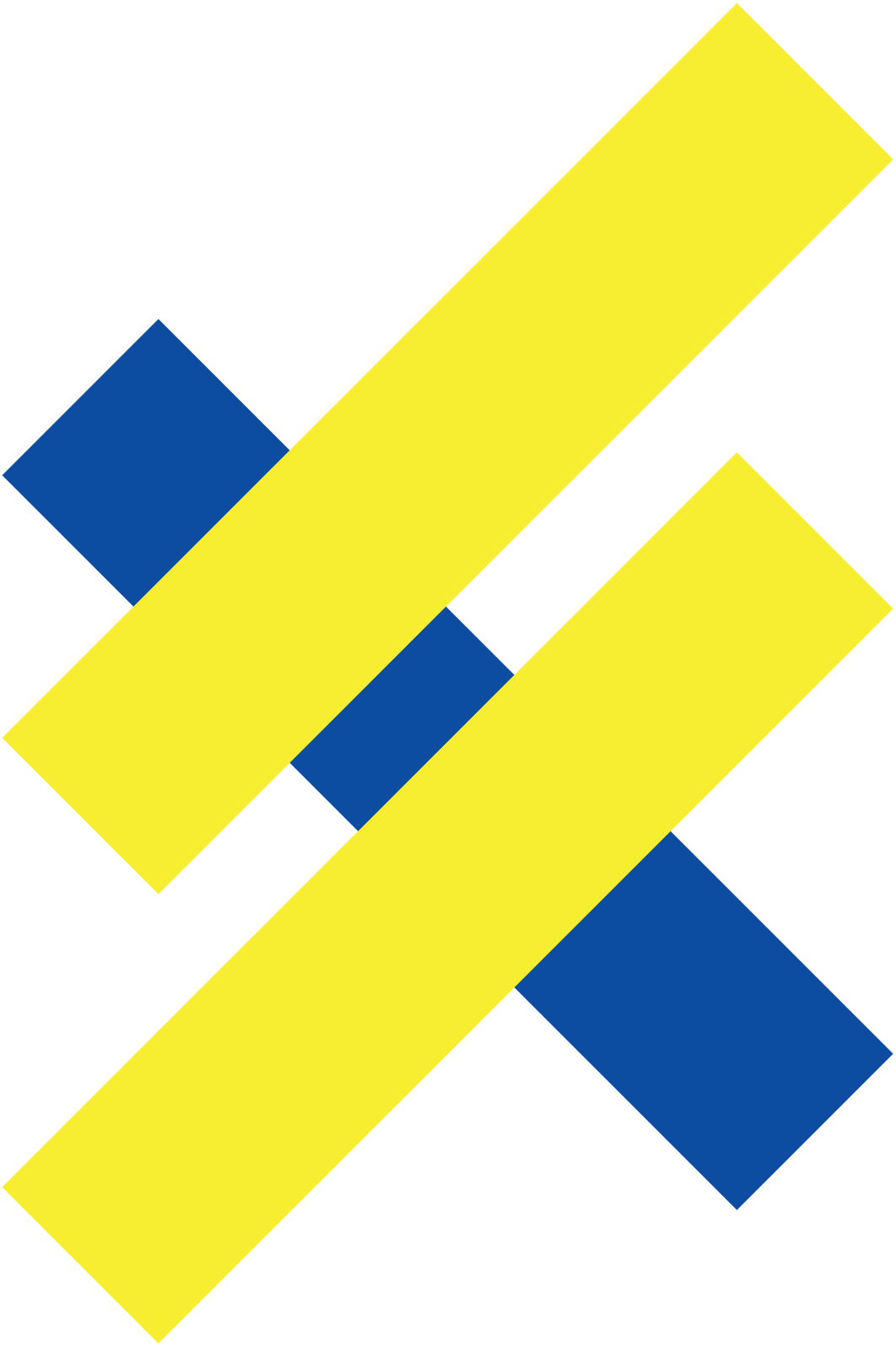
For the analyst activity, participants were sent an email containing login information to an open-source capture the flag platform instance, which was commissioned to the premises of JAMK for this purpose. The email contained a URL to the technical support platform, which was hosted by TU Delft. To work on this, the analyst workstation was a prepared virtual machine containing Kali Linux with additional analyst tools pre-installed. The analyst workstation was created by Masaryk University using the Cyber Sandbox Creator.

Post-exercise surveys gathered responses from the 19 CyberSec4Europe participants. Gender analysis revealed 24% female participants, making Flagship 2 representative of the current (still to be improved) gender balance in technical IT fields. Moreover, all participants gave highly positive feedback, reporting that they:

- found the exercise beneficial,
- acquired new cybersecurity-relevant content through their participation,
- would recommend the Flagship 2 exercise to others.

A total of 43 participants provided answers to the survey questions concerning the two days of the analysts' activity. Statistics revealed different degrees of skill, from junior to high-performing specialists, and also IT professionals with no previous experience in analyst workshops. This is evidenced by the number and time distribution of incorrect answer submissions: in total, 337 submissions were deemed incorrect and 185 correct, with a roughly uniform distribution on the number of correct submissions per challenge (there were six challenges in total). The conclusion is that, even though the difficulty of the activity was balanced, the degree of skill of the participants was not: while some submitted all correct answers at once at the end of the exercise, others had to submit several responses to each challenge before getting it right.

The conductor of the analysts' activity estimated that, based on the received feedback and from what we have concluded from the statistics, the analyst activity was certainly in demand. So, all in all, the active participation and high number of submissions from the analyst activity reveals a pressing need for such realistic technical cybersecurity exercises in the IT sector.



3.3
Standardisation

Standardisation is an important stepping stone in popularising and disseminating new technologies, helping to unify the terminology and models related to their deployment and use. CyberSec4Europe's contribution to developing standards was significant with our participation in a number of the major standards development organisations (SDOs), which are currently developing projects, aspects of which are cybersecurity related.

Throughout the project we maintained contact and collaborated with standards developing organisations (SDOs) with the aim of linking the technical work of the project to standards.

In addition to maintaining contacts with the (European) SDOs and the relevant cybersecurity committees, this work links the technical work of the project to standards and standards to the project and, in so doing, assessing the appropriateness of the existing standardisation procedures for the cybersecurity goals. We also compiled a matrix that maps more than one hundred existing standards from different standards development organisations to different application areas and research questions.

Liina Kamm
Cybernetica
—
6 March 2020

A mapping of cybersecurity standards and research challenges

International standardisation (eg, in ISO/IEC, but also CEN/CENELEC and ETSI) is one channel for technology dissemination for all kinds of organisations in the world. Companies and governments are coming together to contribute their best practices and agree on interoperability, compliance and certification.

Global technology companies are active in pushing their terminology and technological concepts into standardisation processes. The European technology companies, including the cybersecurity industry, should engage in the same practice, especially as through European collaboration by multiple Member States there will be more impact in such activities.

Even though standardisation is a long-term strategy with no immediate return on investment, it will be instrumental in ensuring that European companies grow in size to compete on the global market.

Researchers are envisaging the future with new technologies that promise a cleaner environment, better security, more efficient work and better health. Through research activities, R&D forms the best practice for the future for both leading edge and existing technologies.

Thus, engaging in standardisation is a channel for global dissemination of research concepts. A standardised concept may be used by governments, companies and other organisations worldwide, disseminating EU research results. While it may not immediately be a source of citations or additional research funding, standardisation of results will also inspire new research on the same topics, increasing impact over a longer period.

There are twofold benefits of the mapping of cybersecurity standards and research challenges. Even though experts in cybersecurity are aware of the existence of standardisation and standards in their fields, it is not a trivial task to have an adequate overview of all the standard projects that could be relevant to each topic. The CyberSec4Europe report, *Project Standards Matrix* (D8.2) presents a mapping of the project verticals and research challenges to privacy and cybersecurity standards from ISO/IEC, CEN/CENELEC and ETSI.

The report has been compiled foremost to direct the attention of project partners to the standards and technical reports that could be relevant in their vertical or research topic so that they can more quickly find the necessary information.

On the other hand, all of the pilot competence centres include many capable specialists whose expertise can be a great benefit to the standardisation projects that are still being developed. CyberSec4Europe can contribute the research results and insights that have been gathered throughout the project to the standards that are under development. Many CyberSec4Europe partners are also involved in standardisation activities, so this can be another way of approaching disseminating the results of the project and ensuring that leading edge research reaches standardisation projects.

Liina Kamm
Cybernetica

—

13 April 2020

Why security standards are important

Conformance with established standards and best practices is essential for increasing the protection baseline in cybersecurity. Many organisations lack personnel experienced in the domain and, therefore, have a hard time adopting new approaches and techniques.

Education is an important component, but in-depth knowledge is hard to transfer. Thus, certification methodologies that distil certain best practices into structured, easy-to-apply guidelines have an important role in the proliferation of cybersecurity innovation.

That said, the compacted nature of certification may also have its downsides. For example, the ROCA case in 2017 involved a serious vulnerability in the national eID cards of Estonia and the eID cards of Slovakia, which had to revoke 760,000 and 300,000 certificates, respectively. This vulnerability was found in cards where the chips were certified according to the well-established Common Criteria methodology with an assurance level mandated by European regulation.

While it is currently unclear how the vulnerable system was able to receive a certificate, we see that development in the certification domain is needed for multiple reasons. Firstly, while Common Criteria is flexible, it does not have protection profiles or security targets for everything. The expectation in Common Criteria use is that, once the innovation reaches maturity, customers and technology vendors assemble to come up with the common points of reference for certifying.

However, this is a limitation for new technologies that may not find adoption due to the lack of certification. This is especially the case for quickly evolving technologies like IoT (the Internet of Things). It is not the intention to sidestep due process and reduce security requirements of technologies. Instead, we need to consider new methodologies that contain considerations for new techniques.

Inspired by this, we set out to identify frameworks that allow us to describe and compare the security properties of new technologies in the IoT domain. In our report, *Framework and Toolset for Conformity* (D3.8), we have identified the ARMOUR methodology for IoT devices as a suitable approach.

It allows us to support other CyberSec4Europe tasks by analysing technologies, system designs and implementations to determine whether the combination of cybersecurity technologies in use achieves the desired security goals, allowing it to compare different systems. We also present a prototype tool that can be used to automate and simplify the use of the ARMOUR methodology, speeding up its use.

Liina Kamm
Cybernetica
—
28 October 2020

CyberSec4Europe's recognition by ISO/IEC

Standardisation is an important stepping-stone in popularising and disseminating new technologies, helping to unify the terminology and models related to their deployment and use. It simplifies procurement by both governments and businesses and is expected to grow the market in the long run.

Some standards have become almost brand names, such as:

- the ISO/IEC 27000/27700 series on Information Security Management Systems
- the ISO/IEC 11770 family on key management
- the ISO/IEC 24760 family on identity management; and
- the ISO/IEC 29100 privacy framework.

All these standards were developed in subcommittee 27 "Information security, cybersecurity and privacy protection" of the ISO/IEC Joint Technical Committee 1 "Information technology" (ISO/IEC JTC 1/SC 27).

Hence, in 2019 CyberSec4Europe decided to apply for a liaison relationship with two SC27 Working Groups:

- WG 2 Cryptography and security mechanisms; and
- WG 5 Identity management and privacy technologies

This initiated an intensive process including an analysis of CyberSec4Europe's constitution by the ISO Central Secretariat, an assessment of CyberSec4Europe's competencies by both WG 2 and WG 5 as represented by Stephan Krenn (Austrian Institute of Technolgy) to WG 2 and Liina Kamm (Cybernetica) to WG 5 and, based on this, letter ballots by both SC 27 and JTC 1.

Just in time for the September meetings of the SC27 WGs, this process was concluded successfully and CyberSec4Europe was approved as a liaison partner, meaning that now CyberSec4Europe members can engage with both WGs. Liina Kamm and Stephan Krenn were accepted as CyberSec4Europe Liaison Officers with Liina chiefly responsible for managing the process.

As Liina explained:

> *"Now CyberSec4Europe and its members can keep themselves up-to-date on the newest developments in international standards and can directly give valuable input and feedback to ongoing standardisation projects, making use of the competencies and results of CyberSec4Europe."*

Due to Covid-19 the recent SC 27 WG meetings were held online, otherwise they would have been held in Warsaw hosted by the National Institute of Telecommunications, which nevertheless hosted an impressive hybrid conference on *"The Future of Standards in Cybersecurity"*.

Multiple standardisation efforts are underway in SC 27 that relate to topics relevant to CyberSec4Europe. For example, WG 2 is working on standardising secure multiparty computation mechanisms based on secret sharing (ISO/IEC WD 4922-2); whereas WG 5 is creating a user-centric framework for the handling of personally identifiable information (PII) based on privacy preferences (ISO/IEC CD 27556.2) and a framework for privacy-enhancing data de-identification (ISO/IEC WD 27559).

At CyberSec4Europe we are certain that our experts can contribute to these and other relevant ongoing standardisation projects. The next subcommittee and working group meetings will take place online in April 2021.

Liina Kamm
Cybernetica
—
12 March 2021

StandICT launches the EUOS – European Observatory for ICT Standardisation

On March 9, StandICT.eu announced the launch of the EUOS – European Observatory for ICT Standardisation.

The goal of this new platform is to monitor ICT standardisation and to provide an accurate and up-to-date coverage of ICT standards on different topics. In addition, the EUOS provides a place for ICT experts to meet and collaborate with others on standardisation.

The EUOS has two main functionalities:

1. **Discussion groups** – a collaborative, networking space to provide users to join the conversation with other ICT members by starting new discussions on relevant ICT topics, creating technical working groups (TWG), creating and editing documents, setting up live chats, video calls or sharing calendar of events or simply valuable insights around the ICT standardisation arena, and
2. **Standards repository** – a library of the most relevant standards covering the pivotal ICT fields, continuously updated and integrated with user-friendly search functionality to allow smooth browsing.

Currently the technical working groups include blockchain, artificial intelligence, big data spaces, data interoperability, cybersecurity, smart cities, and trusted information, but more will be created as need arises.

CyberSec4Europe is happy to collaborate with StandICT. For our project, the standards repository is an invaluable collection of information, offering experts an overview of different standards from different standard development organisations in one location.

We encourage our experts to join the discussion groups to offer insights and disseminate the findings of the work we have done in our project, while bringing back valuable information from these groups.

Find out more about the EUOS by contacting StandICT (info@standict.eu) to see how you can get involved.

Marko Hölbl and
Marko Kompara
University of Maribor
—
9 September 2021

Making cybersecurity standards more accessible

Despite the immense amount of collaborative international effort that goes into developing robust and timely standards, there is a growing concern that this work is not being deployed as widely as it should. Notably, putting standards behind paywalls often negatively impacts the accessibility and outreach of the results to a wider audience, which has a detrimental impact on both standards experts and system developers. This applies generally but cybersecurity issues are particularly critical and need to be addressed swiftly.

Hence, CyberSec4Europe has been investigating how the situation could be improved. Firstly, we carried out an analysis using assessment criteria developed through discussions in the project, on documentation from a number of the major standards development organisations (SDOs) currently developing projects addressing aspects which are cybersecurity related.

The objective of this analysis was to allow cybersecurity researchers, policy makers and actors from the private sector in the EU to better understand the operation of these organisations and to facilitate the process of deciding which of them to collaborate or associate with. The intention is to encourage participation in such organisations and to speed up the development of cybersecurity standards.

More precisely, the assessment investigates eight standard organisations, selected to cover a wide range of governance models, based on a methodology that defines eight evaluation criteria – openness, impact, governance, maturity, stability, effectiveness and relevance, coherence and the development dimension.

Organisations with national representation following the UN model

CEN/CENELEC is a European standardisation organisation, operating within the framework of EU Regulation 1025/2012 that produces market-driven European standards (ENs) that serve the needs of business, industry, and other interested parties.

ISO/IEC JTC 1 is a joint technical committee working on information technology that is also a consensus-based, voluntary international standards group.

Organisations with member-based consortia with no national restrictions

ETSI is a European standards organisation, set up in 1988 by the European Conference of Postal and Telecommunications Administrations (CEPT) in response to proposals from the European Commission. It is also recognised as a regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services.

OASIS is a global, non-profit standards body founded in 1993 and now supported by organisations from around the world. The consortium behind OASIS works towards the development of open-source software and standards in very diverse ICT areas including cybersecurity, blockchain, cloud computing and IoT, among others.

HL7 (Health Level Seven International) was created in 1987 and has worked towards improving the electronic collection and exchange of healthcare data to improve the speed, quality, safety and cost of patient care.

National standardisation bodies

Bundesamt für Sicherheit in der Informationstechnik (BSI) – the Federal Office for Information Security - is a German federal agency responsible for the management of computer and communication security for the German government.

UNE is a private, non-profit organisation recognised by the Spanish public administration as the national standardisation body in Spain.

Common Criteria for Information Technology Security Evaluation (CC) is an international standard for computer security certification according to ISO/IEC 15408.

The analysis produced a set of key findings and recommendations on how to better integrate cybersecurity into the procedures of standardisation bodies, especially in the future European Cybersecurity Competence Centre.

Among the common findings, it was found that some organisations allow commenting on projects even if you are not a member, and many organisations have liaisons with other organisations, which is supposed to reduce duplication of work. In addition, not all organisations take into account the development dimension which is especially true for continental and national SDOs.

Finally, the main recommendation made to the European Union and Member States is that the results of the work of SDOs (standards, technical reports) should be made freely available to universities, independent cybersecurity researchers, SMEs, cybersecurity experts and other interested parties, as otherwise security research will be hindered. Putting standards behind paywalls often negatively impacts the accessiblity and outreach of the results to a wider audience. SDOs can follow a similar approach as ‘author’s copy’ to make their resources available for free on the website of the authors or editors.

4

Dissemination, communication and exploitation

CyberSec4Europe's work would only be partially realised if it did not communicate with multiple audiences across Europe those exploitable results and policy recommendations it created in its lifetime – not only through its website and other media – but through many scientific papers, seminars, conferences, summer schools and webinars.

A key aspect of every European research project is engaging with a target audience, in our case the wider cybersecurity community in Europe, to keep them abreast of how the project is faring, what its results are and what its future legacy to European society will become when the project is no more.

We approached this by designing a website that initially contained the bare bones of our work plans and ambitions and then gradually expanded its scope to incorporate new activities and connections.

The main goal of the project's dissemination activities was to ensure that the findings of the project as a whole reach and engage key stakeholders effectively. As well as maintaining an up-to-date listing of all our public deliverables and scientific articles, we also incorporated a calendar of project and industry events. In concert with the website, we maintained an active social media presence on Twitter and LinkedIn. To capture the breadth and depth of the project's outreach to wider audiences, we regularly reported on all the events, conferences, workshops and community interactions undertaken by project partners.

We were specifically charged with creating excellence as well as raising awareness about cybersecurity, and reported on our considerable number of contributions to the body of scientific publications as well as our involvement in driving and participating in summer schools focused on cybersecurity.

4.1
News and opinions

As with any modern day broadcaster, we published news and opinion pieces that would encourage contributors to promote new ideas and address challenging issues that would offer our audience new insights.

Throughout the lifetime of the project, from time to time we published news of announcements from the EU or highlighted significant initiatives and developments taking place across Europe with a long-term impact on the broad cybersecurity agenda that might go beyond the scope of CyberSec4Europe but nonetheless impacted our work. The plethora of news pumped out across the Internet, through social media and online news outlets, means that important news can often get buried and is effectively lost to many until it reappears at a later date. In cybersecurity, the pace of change and development is so fast, we cannot afford to wait!

In particular, the original objective of CyberSec4Europe was to pilot and support the proposed regulation to establish and operate a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre. The regulation passed into EU law in June 2021 which enabled us to support planning for the new Centre in Bucharest and the emerging national cybersecurity competence centres with the objective of advancing existing research in cybersecurity to secure the future of the Digital Single Market, with marketable solutions and services.

In addition, given the wealth of experts in the project, it is not surprising that many of them had opinions that were important to be aired. Conscious that some of the best ideas might not have a place in a project deliverable or a scientific article, our regular weekly news posts offered individuals the opportunity to challenge and, in some cases, provoke new ways of thinking about more general cybersecurity topics that might otherwise be taken for granted. Included here is a selection of their insights

Aljosa Pasic
Atos Spain
—
20 February 2020

The future shape of cybersecurity professional workforces in Europe

Gavin Belson is a bad guy from the HBO TV series, *Silicon Valley,* and his character is maybe inspired by some of the Internet giants' CEOs. One of his famous comments is about the "group of five", an observation on how software teams organise themselves and end up having different and complementary characters, which in Silicon Valley fiction is exemplified by a different cultural background or look.

In Europe, for the joint cybersecurity teams of the future, we might even go a step further, given the very diverse set of cultures, backgrounds and talent pools. Leaders, team players, eternal students, strong communicators, conservative guardians, technical gurus and "everybody's friends" might all be needed in a single team. Understanding human behaviour will help in risk assessment, especially when it comes to social engineering threats.

Persuasion and communication skills will be needed in approaching higher management and convincing them of the importance of a continuous investment in cybersecurity. Education appetite and curiosity is essential to remaining up to date. Strong situational awareness and analytical abilities, handling complexity, positive attitudes and stability, and many other human and social skills come to mind as well for cybersecurity experts. Technical knowledge, therefore, is only a part of what a cybersecurity professional team should have.

In the Atos opinion paper on *Digital Vision for Cybersecurity*, a lot of attention is given to the future of the cybersecurity workforce. To maintain a high calibre cybersecurity workforce, we need to create a common framework where academia, industry, law enforcement and the public sector all fit, and can all refer to or understand. The National Institute of Standards and Technologies (NIST), for example, published *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework* where they define seven categories, 33 speciality areas, 52 work roles and then mapped these to 1,007 tasks, 374 skills, 630 knowledge areas and 176 abilities. Europe might need to adapt it to its own context.

The professional workforce must consider not only the EU Member State context, but also organisational and scenario-specific situations. Cybersecurity experts in the police will likely have a different profile to a cybersecurity specialist in the hospital. Personality traits should fit the organisational cybersecurity context, although it is still a sensitive issue, often neglected or avoided. Cyber threats, for example, might be ambiguous, which result in different categorisation, labelling or structuring, depending on the cognitive or cultural bias of an individual. A well-balanced cybersecurity team must take this into account and should take care of levelling individual differences, when it comes to these bias-driven situations.

Europe-wide cybersecurity workforce development plans must confront, sooner or later, this diversity and complexity, as well as the cultural or technological legacy in some EU Member States. The same applies also to the future European Cybersecurity Competence Centre, Network and Community. This framework should acknowledge regional differences, organisational fitness and social capabilities. Assessing team performance in a constantly changing cybersecurity landscape is very difficult, but this is where CyberSec4Europe work can make important contributions.

Alessandro Mantelero
Politecnico di Torino
—
24 February 2020

The European paradigm of personal data and cybersecurity regulations

Reinforcing cybersecurity is a primary goal for Europe, but, from a legal standpoint, this result is not achievable through general regulation. Starting from the assumption that in Europe several Acts contribute to defining the cybersecurity legal framework, it is necessary to identify the various provisions which contribute to creating this legal and IT framework.

These legal requirements – such as those defined in the GDPR, the ePrivacy Regulation proposal, PSD2, eIDAS and the NIS Directive – entail the adoption of specific technical and organisational solutions which foster cybersecurity in Europe and make the EU a unique context for the development of data protection and cybersecurity-oriented technologies and practices.

A significant part of the analysis carried out in our research was therefore driven by defining the common security and data protection building blocks which characterise the EU regulatory patchwork. In this light, two of the main outcomes of the task concerning the legal and regulatory requirements are:

- an overview of the potential overlap concerning the existing legal obligations in the field of cybersecurity eg, notifications, certifications; and
- the outline of a general, comprehensive and cross-cutting map of legal obligations and procedures concerning cybersecurity.

The results of the comparison highlight that the GDPR, as well as the other regulations, provides a general framework, outlining the main principles for the use of data, also in terms of data security. In this sense, the general principles – such as data minimisation, storage limitation and data confidentiality, that are defined and stated in this regulation – shape the entire regulatory framework.

This common core has been defined through five main pillars, based on the obligations laid down in different articles of the GDPR, PSD2, eIDAS and the NIS Directive:

1. Risk-based approach: basically, an operational and security risk management framework, including adequate technical measures.
2. By-design approach: secure technologies-by-design and by-default must be provided.
3. Reporting obligations: specific procedures for reporting must be adopted.
4. Resilience: developing response and recovery plans is required by law.
5. Certification schemes: ad hoc certification schemes have been provided for by law.

In the light of the above, all the legal provisions mentioned, explicitly or implicitly, require the development of specific technologies for cybersecurity and data security.

The framework provided by these different legal sources is not a patchwork, but a co-ordinated harmonious model, in which similar technologies are required by different regulations to address issues related to the common core of these regulations.

This uniformity demonstrates the coherence that guides the whole approach adopted by the EU legislators in the field of data protection and cybersecurity, and undoubtedly provides a clear and unique framework for the development of a roadmap for the implementation of the network of national cybersecurity centres (NCCs).

Natalia I. Kadenko
and **Tobias Fiebig**
Technical University Delft
—
14 September 2020

Leadership, sovereignty, and security: why Europe should lead rather than follow

Recently, the Mozilla Corporation – the company behind the open-source browser Firefox – announced an unprecedented lay-off.

This lay-off concerns mostly the teams working on Rust, a new security-focused programming language, and Servo, a new web browser engine implementation. These decisions were chiefly driven by an attempt to monetise the Mozilla Corporation.

This could have a devastating effect on the browser ecosystem. While we like to think that there are many different browsers available for users to choose from – for example, Microsoft Edge, Google Chrome and the privacy browser Brave – these all tend to use the same underlying browser engine, Chromium, made by Google. This obviously gives tremendous power to Google: it gets to dictate and decide which standards and technologies are supported on the web, and how these are designed. At the same time, it also creates a monoculture, which – as not only the botanists among us know – is not good for the resilience of an ecosystem.

The big question now is: can the EU do something about it? And the answer is a resounding “yes”. We could undertake a European joint effort – much like the Airbus success story – by offering the laid-off team the opportunity to continue its development to create a European, secure, and open-source web browser providing a counterbalance of power to the Chromium engine, impacting the lives of billions, and making a real step towards cyber sovereignty within Europe.

As things go within Europe, we might want to look for companies that would want to monetise this product to be developed, do a multi-year public tender, and then try to get our digital Airbus to fly. However, there is one aspect that will prevent this proven – and in the case of Airbus very successful – process from taking off.

Unfortunately, this technology simply cannot be monetised easily (unlike a plane that can be sold) – it’s not a product. It is public infrastructure that should be provided by a public institution for the common good. The reason why Google pushed the Chromium engine is because they knew that they would co-monetise simply as a result of controlling the ecosystem. However, if we pay for this with public money, we should not try to monetise it as EU citizens would effectively be paying twice.

Furthermore, for the very same reason, we should not develop a public asset and then hand it over to one or more companies to profit from.

Hence, we suggest that we – within Europe – need an organisation that focuses on building and improving these fundamental infrastructure elements of an open Internet. We can do this carefully. It would also include relinquishing any notion of having backdoors to aid law enforcement and national interests (nobody would buy an Airbus A400M that comes with an EU-controlled bomb 'just in case'). And if we do this fast, we Europeans can change the world for the better. It is time for action.

Pasquale Annicchino
Archimède Solutions
—
2 November 2020

ENISA's latest report: the evolving cyber threat landscape

The threat landscape is becoming extremely difficult to map. Not only are attackers' developing new techniques to evade security systems, but threats are growing in complexity and precision in targeted attacks.

In October 2020, ENISA published the eighth edition of its review of *The Threat Landscape*, in a new more dynamic structure. The series of reports, which provide relevant insights on the evolution of cyber threats for the period from January 2019 to April 2020, was compiled with the support of the European Commission, EU Member States and the CTI Stakeholders Group.

The individual reports allow readers to focus on the information of particular relevance for their sector of interest or activity. This broad approach seeks to satisfy:

> *... different audiences and adopts different levels of technical language, depending on the domain and the importance of the topic for non-technical readers.*

The content of the report aims to be industry and vendor agnostic and ensures appropriate references and citations are listed. The approach taken was based both on in-depth desk research of openly available literature as well as interviews with members of the cybersecurity stakeholder community, which helped define the list of the top 15 threats and validate assumptions about trends and future challenges.

The reports are categorised as follows:

- Entry point providing a general overview of the threat landscape
- Strategic reports consisting of:
  - Sectoral and thematic threat analysis
  - Main incidents in the EU and worldwide
  - Research topics
  - Emerging trends
- Technical reports consisting of:
  - CTI overview summarising the most important topics relevant to the cyber threat intelligence community
  - ENISA's top 15 threats consisting of 15 reports, one for each of the top threats identified in 2019-2020, presenting for each a general overview, the findings, major incidents, statistics, attack vectors and corresponding mitigation measures.

The two main factors identified in the report as drivers for the threat landscape transformation were the coronavirus pandemic and the trend in advanced adversarial capabilities of threat actors. In particular, as far as the pandemic is concerned, the report underlines how Covid-19 forced large-scale adoption of technology to master a variety of critical aspects of the crisis, such as co-ordination of health services, the international response to the spread of Covid-19, adoption of teleworking regimes, distance learning, interpersonal communication, control of lockdown measures, teleconferencing and many others.

It also points out that in a short turnaround time, IT security professionals had to quickly respond to the challenges introduced by working from home arrangements such as enterprise data movements whenever employees use their home Internet to access cloud-based apps, corporate software, videoconferencing and file sharing.

The ten main trends observed during the reporting period are reviewed across all the reports:

1. Attack surfaces in cybersecurity continue to expand as we are entering a new phase of digital transformation.
2. There will be a new social and economic norm after Covid-19, even more dependent on a secure and reliable cyberspace.
3. The use of social media platforms in targeted attacks is a serious trend and reaches different domains and types of threats.
4. Finely targeted and persistent attacks on high value data (eg, intellectual property and state secrets) are being meticulously planned and executed by state-sponsored actors.
5. Massively distributed attacks with a short duration and wide impact are used with multiple objectives such as credential theft.
6. The motivation behind the majority of cyber attacks is still financial.
7. Ransomware remains widespread with costly consequences to many organisations.
8. Many cybersecurity incidents still go unnoticed or take a long time to be detected.
9. With more security automation, organisations will invest more in preparedness using cyber threat intelligence as its main capability.
10. The number of phishing victims continues to grow since it exploits the human dimension being the weakest link.

The overall conclusion is that with all the changes observed in the cyber threat landscape and the challenges created by Covid-19, there is still a long way before cyberspace becomes a trustworthy and safe environment for everyone.

But, the picture painted is not altogether gloomy: according to the findings of an EC 2019 survey, concerns about online privacy and security have already led more than nine in ten Internet users to change their online behaviour – most often by not opening e-mails from unknown people, installing anti-virus software, visiting only known and trusted websites and using only their own computers.

The report also offers relevant policy conclusions and recommendations, among which increasing the co-operation between policy makers and technologists is considered essential. From a CyberSec4Europe viewpoint, research and educational conclusions are of fundamental importance.

Among them:

- The EU should continue to invest in cybersecurity research and development with an emphasis on long-term and high-risk research initiatives.
- The EU should continue building capacity through investment in cybersecurity training programmes, professional certification, exercises and awareness campaigns.
- Multidisciplinary research in cybersecurity should be promoted and incentivised.

This report will contribute to the ongoing work of CyberSec4Europe and help our research teams to focus on the priorities identified by different stakeholders and policy makers. It is relevant reading for all those with an interest in cybersecurity developments.

Access to the report is available from ENISA's website.

Pasquale Annicchino
Archimède Solutions
—
1 December 2020

Overcoming the barriers to data-sharing In Europe

On 25 November the European Commission published its proposal for a new regulation on European data-sharing and governance, known as the Data Governance Act. The initiative is driven by the recognition of the role that data plays within the European digital economy and is the first in a set of measures in the European strategy for data which was adopted in February 2020.

The proposal includes measures:

- To increase trust in data-sharing, which is perceived by many stakeholders as a real priority in the data-driven economy
- On data intermediaries who will function as trustworthy organisers of data-sharing with regulatory intervention
- To facilitate data altruism, for both personal and non-personal data, and to develop a common European consent form
- To facilitate the re-use of datasets held in the public sector by businesses and citizens

The proposal also calls for the establishment of a European Data Innovation Board, a group of experts, chosen by the Member States and the Commission, who would act as an advisory body in promoting best practices for data-sharing.

Before the proposal goes for approval by the European Parliament and the Council of Ministers, several issues need to be addressed: such as co-ordination with other ongoing initiatives, such as the Digital Service Act package, and existing legislation, especially the General Data Protection Regulation.

Research projects and other stakeholders on data governance, cybersecurity and digitalisation were able to contribute to the effort of the EU institutions through a three month online consultation which elicited 806 contributions.

The setting up of a new European approach to data governance will facilitate data-sharing across sectors and Member States through common data spaces. The Act has the potential to drive the digital economy for the benefit of both businesses and citizens while also giving citizens control over their personal data and making companies more trustworthy.

Stephan Krenn
Austrian Institute of Technology
—
11 December 2020

Security through encryption and security despite encryption

Recently, a planned resolution by the Council of the European Union entitled *Security through encryption and security despite encryption* was leaked through various media.

The resolution acknowledges the benefits of strong cryptography security, yet it also states that:

> *... law enforcement is increasingly dependent on access to electronic evidence to effectively fight terrorism, organised crime, child sexual abuse.*

In order to support law enforcement agencies, the resolution asks for "lawful and targeted" access to encrypted data through competent authorities. In response to this resolution, the academic community has drafted an open letter to the EU institutions. The challenges of law enforcement agencies are indisputable. However, while not explicitly asking for encryption "backdoors", the Council's resolution suggests a "middle ground" of sufficiently secure cryptography, while still giving competent authorities access to encrypted data. The signatories to the letter explain that such a middle ground does not exist today – and most likely cannot exist. Any attempt to weaken encryption or to introduce other means for digital surveillance introduces a wide variety of risks, ranging from technical weaknesses in implementations all the way to potential violations of fundamental freedom rights.

The authors of the letter conclude by proposing a roadmap towards better capacity building for evidence in information and communication networks. They suggest an honest and open-minded dialogue between policy makers, law enforcement agencies, academic experts from all affected fields (eg, cryptography, digital forensics, fundamental rights, ethics, or procedural law), in order to avoid negative impacts of any deployed solution for cybersecurity in general as well as society as a whole.

At this point, more than 190 experts from various fields – cryptography, IT security, law (including Data Protection Acts) etc – have signed the letter. For many years, the European Union has been a pioneer of strong cybersecurity, fundamental human rights, and data protection. This position could be put at risk by premature decisions, made without broader consideration of all the consequences, to counter digital crimes.

The four pilot projects – CONCORDIA, CyberSec4Europe, ECHO and SPARTA – represent an embryonic European cybersecurity competence network of multi disciplinary research experts. This expertise could be tapped to obtain first inputs and to develop a way forward, in order to find the optimal balance between the needs of law enforcement and the security and fundamental rights of all European citizens.

Kai Rannenberg
CyberSec4Europe Co-ordinator
—
31 December 2020

From 2020 into 2021: CyberSec4Europe's year in perspective

Never before at the end of a year have I received as many good wishes for a "better" next year as this time. Obviously, 2020 was not a good year considering the criteria we are used to.

Almost everybody has been hit by the Covid-19 pandemic, some much harder than others. Most plans made at the beginning of 2020 could not be implemented as expected. Several had to be rewritten to preserve their goals or at least some of them. How did we fare in European cybersecurity and in CyberSec4Europe? Moreover, what does that mean for 2021 and beyond?

Clearly, most of our meeting plans had either to be shredded or thoroughly rewritten. We can be thankful, that the CyberSec4Europe public event on the evening of 24 February 2020 and the General Meeting around it had not been scheduled for two weeks later.

Then we would have been hit by a more or less spontaneous lockdown. On 24 February probably only our Italian colleagues, some of them hindered from travelling to Brussels already then, could possibly imagine the extent of the pandemic and its impact. The rest of us enjoyed a fruitful meeting with good results and an exciting live panel on governance and other issues regarding the Cybersecurity Competence Network. Moreover, we enjoyed the exciting atmosphere of an inspired post-panel reception hosted by the Hessen Representation in Brussels. It was a vibrant convocation of a cybersecurity community growing way beyond the CyberSec4Europe project partner representatives and looking forward to the next public event in July at the same place.

Then the pandemic hit. The Covid-19 page on the project website shows early reactions and answers based on progressed digitalisation of our work.

While first we hoped to do physical events again later in the year or at least some hybrid events, the events had to become virtual only. Virtual public events, like the public panel on 9 July and the CONVERGENCE event in December together with our fellow pilots, indeed showed that a major share of the existing community and additional people could gather – and did gather – to present and discuss the progress of the Cybersecurity Competence Centre and Network.

Moreover, we passed the first periodic review very successfully after hosting the virtual review meeting on a European-hosted open-source platform (the predecessor of the Big Blue Button that later served CONVERGENCE very well).

Maybe this review meeting was even the first organised in this way, but we definitely showed our commitment to European digital sovereignty, in that spirit, all the many deliverables, on governance, research, roadmapping, demonstrator use cases, capability building, certification, validation, standardisation, outreach and community building, were delivered despite the unexpected conditions and in high quality.

At the same time, the outgoing Croatian and incoming German EU Presidencies in trilogue with the Parliament and the Commission progressed negotiations towards an agreement between Council and Parliament, a major and welcome result given the need for more cybersecurity progress and hence the new entity. The Council web page has the final compromise text. In addition, the seat of the new centre was agreed: congratulations go to Romania, especially Bucharest, for their successful application.

So, work has not stood still, results have been produced but questions remain:

- Can we say that we achieved the same in virtual meetings and other gatherings that we would have done under the conditions of the "old normal"?
- Have we laid the basis for a thriving community improving European cybersecurity while preserving European values, eg, open and free dialogue?
- Will the new EU body have a strong soul?
- Will it exist in an EU, whose digital sovereignty is strong enough to shape the future? There are promising elements, but only the future will really tell.

Certainly, there is more work to do, especially for pilots such as CyberSec4Europe. The upcoming European regulation will need a lot of underpinning by:

- A lively community and ecosystem progressing the many initiatives to be co-ordinated by the Competence Centre and Network.
- An active centre in Bucharest profiting from a governance that now needs to be further developed based on the regulation.
- Pilot activities to try out the new opportunities.

Therefore, while a lot of work and achievements, especially considering the conditions, are behind us, more interesting work lies ahead, some of it to be done under lockdown conditions as we can see already now. Still one can profit from the deliverables and contributions by CyberSec4Europe, and the work will lead to more of them in 2021 including the first Flagship Challenge exercise on 12/13 January.

Eventually we will know how strong and robust the community will be. Its foundations had to be created under circumstances that were not friendly to live communities and yet triggered many efforts to overcome the new and unexpected challenges. Even if there would have been nothing else, that kind of resilience and effectiveness gives good hope for 2021 and the future of the Competence Centre and Network.

2020 was a difficult year for everyone and we came through it – together – with flying colours; and together we can look forward to interesting and exciting new challenges in 2021.

A happy, healthy and safe New Year to everyone!!

David Goodman
Trust in Digital Life

—

5 March 2021

Romania in the spotlight

On the evening of 24 February during its 2021 Winter General Meeting, CyberSec4Europe hosted an online panel discussion entitled *Establishing the competence centre in Bucharest and building the network.* Following an introduction from Marc Weinmeister, Secretary of State for European Affairs of the State of Hessen and Kai Rannenberg, Goethe University Frankfurt and co-ordinator of CyberSec4Europe, moderator David Goodman from Trust in Digital Life introduced the panellists:

- Miguel González-Sancho, Head of Cybersecurity Technology and Capacity Building, DG CONNECT, European Commission
- Ramona Nițǎ, Counselor Telecommunications, Cyber Security, Digital Internal Market, Postal Services, Permanent Representation of Romania to the EU
- Stelian Brad, President, Cluj IT Cluster and Professor, Technical University of Cluj-Napoca
- Monica Florea, Director of European projects, SIMAVI
- Virgil D. Gligor, Professor, Electrical and Computer Engineering, Carnegie Mellon University

The goal of the evening's discussion was to explore both how Europe proposes to achieve its cybersecurity objectives over the coming two to three years as well as its impact on the industrial and academic cybersecurity community across Romania – not only in Bucharest, but also in Cluj-Napoca, home to a vibrant technology community that includes ten universities.

Miguel González-Sancho introduced the topic with insights into how the setting up of the Centre is progressing.

During the evening of 9 December 2020, a decision was made by the European Council to locate the EU's much anticipated cybersecurity centre in Bucharest, which was ratified a few days later at the final trialogue meeting. The regulation itself – for a European Cybersecurity Industrial, Technology and Research Competence Centre – is expected to be formally adopted in April, although work has started already.

As proposed, the European Commission is to facilitate the setting up of the three levels referenced in the legislation: the Centre, the Network and the community. Work is ongoing in the administrative aspects which include finding a suitable building in Bucharest, making a hosting agreement between the Centre and Romanian authorities and there are numerous discussions taking place with other relevant parts of the Commission regarding financial arrangements, staffing and building issues. There is an awful lot to go through in setting up a new EU body, particularly one with responsibility for distributing EU funds! It comes with a lot of conditions and requirements, so that although all the parties involved are moving as fast as possible, it will take some time before the Centre is autonomous, although work will start well before that.

The second dimension are the Member States, represented by the National Co-ordination Centres, who together with the European Commission are partners of the Centre. The first step has been to set up a Governing Board which will be ultimately responsible for making all decisions – nothing can be achieved without it. Until the regulation is adopted, legal decisions cannot be made, so at present a 'shadow Governing Board' is being put in place with nominations for members being solicited from Member States.

Representatives will be chosen on the basis of cybersecurity expertise as well as experience in investments. Creating the atmosphere for the coming years is of course difficult without being able to meet in person. Decisions on the Director of the Centre and matters of strategy will be the responsibility of the Board. A key piece at this level, the role of the National Co-ordination Centres is vital as they will also be tasked with financial responsibilities.

Preparation of the work programmes relating to cybersecurity will be a job of the Centre, but already the Commission has prepared the programmes for Horizon Europe and Digital Europe for 2021/2022, both of which have strong cybersecurity components.

The third level is the community, where the pilots come into play alongside ECSO and ENISA, all of whom have extensive communities. The Commission is working hand-in-hand with them all to collect all the relevant inputs to be handed over to the Centre in the future.

The ultimate goal of the Centre is to create a common approach to decide about cybersecurity investments in Europe: these discussions will start already this year.

Ramona Nițǎ represents Romania in matters relating to cybersecurity in Brussels and is in a unique position to observe what is happening on the ground in Romania in addition to political and strategic decisions being made in Brussels, as well as the emerging relationship between Brussels and Bucharest. The setting up of the Centre is of major importance to Romania and there is already a task force in place that will ensure the logistical and administrative arrangements to enable the Centre to become operational as soon as possible. Romania is strong in technology through its industrial and academic community which has long been recognised internationally. The Centre will also open up opportunities for cost reduction of products and easier access to the investment community, providing a huge help to, for example, micro-enterprises. The Centre also represents competencies, which is of enormous importance for Europe, as well as a driver of collaboration between all stakeholders providing access to resources for researchers from academia and industry.

Although many may not have been aware previously, one of the compelling arguments for Bucharest's successful bid is that Romania has a strong digital mentality, a strong cybersecurity ecosystem and an excellent digital infrastructure: it is one of the best networked countries in Europe. Also Bucharest is one of the best cities in terms of connectivity, and boasts many major companies. In short, it is one of the best cities, not only in Europe, but in the world!

Stepping away from Bucharest, Stelian Brad is President of the Cluj IT cluster and a professor at one of the universities in Cluj-Napoca in north-west Romania. The cluster is of particular interest to CyberSec4Europe which has developed the concept of CHECKs – Community Hubs of Expertise in Cybersecurity Knowledge.

Cluj-Napoca has the largest community of IT experts outside Bucharest, but the biggest in terms of density: more than 20,000 IT specialists, with over 1,200 IT companies located in the city, including many enterprises operating worldwide, as well as the ten universities with more than 100,000 students. Cluj-Napoca works closely with Bucharest and other communities beyond Romania: a city of cluster initiatives with a strong culture of co-operation. To build up the Competence Centre will require a lot on the institutional side, in particular a network aligned to a common goal, an expertise which Cluj-Napoca can contribute to. An example of this being a recently formed national framework on distributed ledger technologies, the results of which can be shared through the Centre. There are also plans to set up a national initiative on cybersecurity which could be internationalised with links to Central and South America as well as Africa – another reason for basing the Centre in Romania.

As already indicated, the community is one of the most important pillars, and Cluj IT is driving innovation ideas for small businesses through the H2020 cyberGEIGER project.

The cluster is both an organisation and a network and could be a model for the operation of the Centre. It started from a bottom-up approach to change the paradigm from services to intellectual innovation, making competitors collaborate on certain initiatives to open new windows of opportunities which raised attention at a European level. The set-up of the administration and specific task forces is a major but vital challenge and comes down to a code of ethics and intellectual property synergies between companies.

Monica Florea has had a long-standing relationship with the Romanian IT sector with close connections to Brussels, from both a technical and business perspective, and has seen the role of the community in Romania grow over many years. As head of European projects of SIMAVI, a spin-off of SIVECO which covers a wide range of domains, Monica is engaged in research innovation projects and is involved in 30 Horizon projects in different fields and domains. Security is one of the largest of those domains, particularly on the application side in security-related projects in health, energy, border security, digital and visual intelligence and counter-terrorism, in which SIMAVI plays the role of co-ordinator, technology provider or integrator. The company is also involved in e-learning and e-training related to security, deploying augmented reality and games. As a company, SIMAVI/SIVECO is looking forward to opportunities to strengthen public-private collaboration as well as policy makers, academia and practitioners in cybersecurity through the Centre. Brussels has always been Monica's second home after Bucharest and she doesn't feel that there is a great distance between them.

If Bucharest is a long way from Brussels, Pittsburgh is even further away. Virgil Gligor also has his own unique perspective on the technology scene in Romania. He grew up in Romania but moved to the United States as a young man and although he has lived and worked there ever since, he has always maintained close professional links with Romania. He very much appreciates setting up the Centre in Bucharest, having once failed miserably (his words) in an attempt to set up something similar. It was not for lack of funding: it had been a political decision. There was interest in security in Romania, as elsewhere, in the early seventies, but only a few experts. But it was only at the turn of the millennium that things really took off everywhere in cybersecurity including in Romania.

Virgil's vision goes back to an anecdote about three axioms of *cyberinsecurity*.

- There will always be rapid innovation in information technology which always leads to *cyberinsecurity* – forever. Why? The three reasons for this are zero cost of entry in the business, zero regulation and zero reliability. People don't have the time to pay attention to the detail
- Zero days, no attacks
- Based on the above, there will always be adversaries.

Users don't need security all the time, platforms should offer feasible recourse against breaches of their system – all of this should be as usable as possible. In the future, we will have systems that cannot be attacked by individual hackers or nation states. We are now building systems that are unconditionally secure, that no amount of quantum computing can breach. What is the interest of the Competence Centre and Network in the United States? Plenty, many of the top experts in the US came from Europe. It doesn't matter that the Centre is in Europe or in Bucharest – it is more important that Europe found the political will to crystalise its objectives. A big success!

In conclusion, it's important that the Centre will be a vehicle for driving a vision but also, when the time is right, in co-operating beyond the borders of Europe. Cybersecurity is no longer a technical concern but, with the growing number of cyber attacks, it has become an eco-system. Establishing the Centre in Bucharest can act as a magnet for young people to get involved and carry out research in cybersecurity, as well as generating a lot of interaction across Europe, ultimately to a safe Europe for citizens and businesses. Europe is a leader in privacy but is secondary in security, and this initiative will strengthen Europe's ambition to establish digital capacity and digital sovereignty.

From all that was heard, the future of cybersecurity in Europe is in safe hands!

A recording of the event is also available on the CyberSec4Europe website.

David Goodman
Trust in Digital Life
—
22 April 2021

Europe lays down its rules for human-centric artificial intelligence

The European Commission today published its much-anticipated proposal for a set of guidelines, in the form of rules and actions which aim to turn Europe into the global hub for trustworthy artificial intelligence (AI). The combination of a legal framework together alongside a 2021 co-ordinated plan with Member States is intended to ensure the safety and fundamental rights of people and businesses, while strengthening uptake, investment and innovation in AI across the EU. New rules on machinery will complement this approach by adapting safety rules to increase users' trust in the new, versatile generation of products.

Building trust and mitigating risk

By emphasising that 'trust is a must', Europe is taking a clear lead in asserting the ethical norms that need to be associated in the use of AI technologies to counter public misgivings without inhibiting competition or innovation in the vast potential across all business and social sectors.

The European approach to AI, which will apply across all Member States, is based on identifying risk. Any AI system which can be considered a clear threat to the safety, livelihoods and rights of people will be banned. Significantly, this includes 'systems or applications that manipulate human behaviour to circumvent users' free will (eg, toys using voice assistance encouraging dangerous behaviour of minors) and systems that allow 'social scoring' by governments.'

Before they can be put on the market, high-risk AI systems will be subject to strict obligations that will focus on adequate risk assessment, traceability, detailed documentation, user-friendly information as well as high levels of robustness, security and accuracy. All remote biometric identification systems are included in this high-risk classification.

Other risk categories are 'limited' which simply require an advice warning for users; and 'minimal' covering most commercial AI systems for which no regulatory intervention is required.

A European Artificial Intelligence Board

A new European Artificial Intelligence Board is to be created to manage the implementation of these rules as well as to help stimulate development and to facilitate co-operation across the EU. This announcement comes in the wake of the European Strategy on AI in 2018 and the subsequent work and publications of the High-Level Expert Group on Artificial Intelligence (HLEG)

Next steps

The European Parliament and the Council will need to adopt the Commission's proposals in the ordinary legislative procedure which, once adopted as regulations, will be directly applicable across the EU. In parallel, the Commission will continue to collaborate with Member States to implement the actions announced in the Co-ordinated Plan.

David Goodman
Trust in Digital Life
—
1 July 2021

A trusted and secure digital identity for all Europeans

On 3 June 2021 the European Commission announced its proposal for a framework for a European Digital Identity which will be available to all EU citizens, residents and businesses in the EU. Citizens will be able to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phone. They will be able to access online services with their national digital identification, which will be recognised throughout Europe.

Very large platforms will be required to accept the use of European Digital Identity wallets upon the request of the user, for example to prove their age. Use of the European Digital Identity wallet will always be at the choice of the user.

Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age said:

> *"The European digital identity will enable us to do in any Member State as we do at home without any extra cost and fewer hurdles. Be that renting a flat or opening a bank account outside of our home country. And do this in a way that is secure and transparent. So that we will decide how much information we wish to share about ourselves, with whom and for what purpose. This is a unique opportunity to take us all further into experiencing what it means to live in Europe, and to be European.*

Thierry Breton, Commissioner for Internal Market, said:

> *"EU citizens not only expect a high level of security but also convenience whether they are dealing with national administrations such as to submit a tax return or to enrol at a European university where they need official identification. The European Digital Identity wallets offer a new possibility for them to store and use data for all sorts of services, from checking in at the airport to renting a car. It is about giving a choice to consumers, a European choice. Our European companies, large and small, will also benefit from this digital identity, they will be able to offer a wide range of new services since the proposal offers a solution for secure and trusted identification services."*

The European digital identity framework

Under the new regulation, Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (eg, driving licence, diplomas, bank account). These wallets may be provided by public authorities or by private entities, provided they are recognised by a Member State. The new European Digital Identity wallets will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data. With this solution they will have full control of the data they share.

The European Digital Identity will:

- Be available to any EU citizen, resident, and business in the EU who wants to use it.
- Be useable widely as a way either to identify users or to prove certain personal attributes, for the purpose of access to public and private digital services across the EU.
- Enable people to choose which aspects of their identity, data and certificates they share with third parties, and to keep track of such sharing. User control ensures that only information that needs to be shared will be shared.

To make it a reality as soon as possible, the proposal is accompanied by a Recommendation. The EC invites Member States to establish a common toolbox by September 2022 and to start the necessary preparatory work immediately. This toolbox should include the technical architecture, standards and guidelines for best practices.

Next steps

In parallel to the legislative process, the EC is working with Member States and the private sector on technical aspects of the European Digital Identity. Through the Digital Europe programme, the EC will support the implementation of the European Digital Identity framework, and many Member States have foreseen projects for the implementation of the e-government solutions, including the European Digital Identity in their national plans under the Recovery and Resilience Facility.

Member States should issue the new European Digital Identity wallets one year after entry into force of the new Regulation.

The aim is that, by September 2022, Member States agree on the toolbox to implement the European Digital Identity Framework to enable the EC to publish the toolbox in October 2022. Once the technical framework has been agreed, it will be tested in pilot projects.

Background

The EC's Digital Compass, a vision for Europe's digital transformation by 2030, sets out a number of targets and milestones which the European Digital Identity will help achieve. For example, by 2030, all key public services should be available online, all citizens will have access to electronic medical records; and 80% citizens should use an eID solution. For this initiative, the EC is building on the eIDAS regulation, the existing cross-border legal framework for trusted digital identities. Adopted in 2014, eIDAS provides the basis for cross-border electronic identification, authentication and website certification within the EU. About 60% of Europeans can already benefit from the current system.

However, there is no requirement for Member States to develop a national digital ID and to make it interoperable with ones from other Member States, which leads to high discrepancies in levels of implementation between countries. The current proposal will address these shortcomings by improving the effectiveness of the framework and extending its benefits to the private sector and to mobile use.

What is the European Digital Identity wallet?

Many citizens are already using digital wallets on their smartphones to store boarding passes when they travel or to keep their virtual bank cards for convenient payment. Under the new rules, European Digital Identity wallets, which will be available to everyone, are personal digital wallets allowing citizens to digitally identify themselves, store and manage identity data and official documents in electronic format. These may include a driving licence, medical prescriptions or education qualifications. With the wallet, citizens will be able to prove their identity where necessary to access services online, to share digital documents or simply to prove a specific personal attribute, such as age, without revealing their identity or other personal details. Citizens will at all times have full control of the data they share, and control which personal data they want to share, with online services. While public services and certain private services will be obliged to recognise the European Digital Identity, its security features make it attractive for all private service providers to recognise it for services that require strong authentication, creating new business opportunities.

How can I use my European Digital Identity wallet?

You will be able to use it to access both public and private online services in the EU, in particular those requiring strong user authentication. Examples of these could be accessing a bank account or applying for a loan, submitting tax declarations, enrolling in a university in your home country or abroad and many other things that you do with your normal means of identification.

Here are a few examples of how the European Digital Identity wallet could be used, once in place:

- **Use the Digital Identity wallet:** Peter has installed a personal digital wallet on his mobile phone. It has been provided by his home country, ensuring that the wallet has been issued to him personally. Peter's digital wallet allows him to download, store and use his basic personal data, a driving licence, a diploma and a bank card he used to carry around as physical cards in his physical wallet.
- **Prove your age:** Myra is in the queue to enter a nightclub and the security guard at the door asks for her ID. Instead of showing her physical ID card, she uses her European Digital Identity wallet. The security guard can verify she is over the legal age as Myra can choose to use her digital identity wallet to confirm her age without showing any other personal data.
- **Renting a car at an airport:** Sarah used to queue at the rent-a-car counter of the airport. She would have to wait for the car rental company to scan a copy of the passport or identity card, the driving licence, the credit card and sign all documents. With the digital identity this could be done without having to wait in the queue, even beforehand. Sarah will be able to head to the car park, pick up the car and drive to her hotel. The car rental company may either give her the key in the parking or else enable the car to be started via her mobile phone.
- **Identify to an online service to prove who you are:** Kurt has moved to a new country for work. To fulfil the need to register as a resident in the new country, he can use his European Digital Identity wallet. Kurt can also use his wallet to prove his identity for various online services in his new country of residence, such as to open a bank account, buy a SIM card for his mobile phone or subscribe to a public transport pass.

What is the added value compared to the current system?

The European Digital Identity wallets will be built on the basis of trusted digital identities provided by Member States, improving their effectiveness, extending their benefits to the private sector and offering personal digital wallets that are safe, free, convenient to use and protect personal data.

The existing eIDAS Regulation provides the basis for cross-border electronic identification, authentication and website certification within the EU but does not contain any obligation for Member States to provide their citizens and businesses with a digital identification system enabling secure access to public services, or to ensure their use across EU borders. Nor does it contain provisions regarding the use of such identification for private services, or with mobile devices. This leads to discrepancies between countries.

Some countries offer identification system to their citizens while other do not and, when they do, not all these systems can be used cross-border. Today, 19 notified eID schemes are used by 14 Member States, covering almost 60% of the EU-27 population but take-up is low, their use is cumbersome and business cases are limited. The EC will propose and agree with Member States on standards, technical specifications and operational aspects through an implementing act.

The coronavirus pandemic and the shift towards the use of digital services has shown that this has limitations that need to be addressed urgently.

A Joint European Cyber Unit

David Goodman
Trust in Digital Life
—
13 July 2021

On 23 June, the Commission laid out its vision to build a new Joint Cyber Unit to tackle the rising number of serious cyber incidents impacting public services, as well as the lives of businesses and citizens across the European Union.

Advanced and co-ordinated responses in the field of cybersecurity have become increasingly necessary, as cyber attacks grow in number, scale and consequences, impacting heavily Europe's security. All relevant actors in the EU need to be prepared to respond collectively and exchange relevant information on a 'need to share', rather than an only 'need to know', basis.

First announced by President Ursula von der Leyen in her political guidelines, the proposed Joint Cyber Unit aims to bring together resources and expertise available to the EU and the Member States to effectively prevent, deter and respond to mass cyber incidents and crises. Cybersecurity communities, including civilian, law enforcement, diplomatic and cyber defence communities, as well as private sector partners, too often operate separately. With the Joint Cyber Unit, they will have a virtual and physical platform of co-operation: relevant EU institutions, bodies and agencies together with the Member States will build progressively a European platform for solidarity and assistance to counter large-scale cyber attacks.

Background

The Covid-19 pandemic has increased the importance of connectivity and Europe's reliance on stable network and information systems and has shown the need to protect the whole supply chain. Reliable and secure network and information systems are particularly important for entities in the frontline of the fight against the pandemic, such as hospitals, medical agencies and vaccine manufacturers. Co-ordinating EU efforts to prevent, detect, deter, mitigate and respond to the most impactful cyber attacks against such entities could prevent the loss of life and attempts to undermine the EU's ability to defeat the pandemic in the swiftest possible manner. Moreover, strengthening the EU's ability to counter cyber attacks effectively contributes to advancing a global, open, stable and secure cyberspace.

Faced with the cross-border nature of cybersecurity threats and the continuous surge of more complex, pervasive and targeted attacks, it is incumbent on the relevant cybersecurity institutions and actors to increase their ability to respond to such threats and attacks by harnessing existing resources and co-ordinating efforts better.

No common platform

Despite the major progress achieved through co-operation between Member States on cybersecurity, most notably through the NIS Co-operation Group and the CSIRTs (Computer Security Incident Response Teams) network, there is still no common EU platform where information gathered in different cybersecurity communities can be exchanged efficiently and safely and where operational capabilities can be co-ordinated and mobilised by relevant actors. As a result, cyber threats and incidents risk being addressed in silos with limited efficiency and increased vulnerability. Furthermore, an EU-level channel for technical and operational co-operation with the private sector, both in terms of information sharing and incident response support, is missing.

Existing frameworks, structures and the resources and expertise available in Member States and relevant EU institutions, bodies and agencies provide a strong basis for a collective response to cybersecurity threats, incidents and crises.

However, a mechanism for harnessing existing resources and providing mutual assistance across the cyber communities responsible for network and information systems security, for combating cybercrime, for conducting cyber-diplomacy, and, where appropriate, for cyber defence in the event of a crisis does not yet exist. Nor is there a comprehensive mechanism at the EU level for technical and operational co-operation in situational awareness, preparedness as well as response, between all communities. Moreover, synergies with the law enforcement and intelligence communities should be achieved respectively through Europol and INTCEN (EU Intelligence and Situation Centre).

A Joint Cyber Unit

The importance of analysing the strengths, weaknesses, gaps and overlaps of the current EU cybersecurity architecture which has been created over recent years is clearly recognised at the highest levels. In consultation with Member States, the Commission, with the involvement of the High Representative of the Union for Foreign Affairs and Security Policy, has developed a concept for a Joint Cyber Unit as a response to this analysis and as an important component of the Security Union Strategy, the Digital Strategy and the Cybersecurity Strategy.

The four cyber communities

In cases of crisis, Member States should be able to rely on EU solidarity in the form of co-ordinated assistance, including from all four cyber communities ie, civilian, law enforcement, diplomacy and, where appropriate, defence.

The degree of intervention of participants from one or more communities may depend on the nature of a large-scale incident or crisis and, consequently, on the type of countermeasures required to respond to it. When confronted with cyber threats, incidents and crises, well-trained experts and technical equipment represent essential assets that can contribute to avoiding serious damage and bring effective recovery.

Therefore, clearly identified technical and operational capabilities, primarily experts and equipment, ready to be deployed to Member States in case of need, will be at the centre of the Joint Cyber Unit. Within that platform, participants will be in a unique position to nurture and co-ordinate such capabilities through EU Cybersecurity Rapid Reaction teams, while ensuring appropriate synergies with the already existing cyber projects conducted in the framework of PESCO (cyber defence-related projects launched under the Permanent Structured Co-operation).

The Joint Cyber Unit provides for a virtual and physical platform and does not require the creation of an additional, standalone body. Its setup should not affect the competencies and powers of national cybersecurity authorities and relevant EU entities. The intention is that the Joint Cyber Unit should:

- be anchored in MoUs between its participants.
- build on, and add value to, existing structures, resources and capabilities as a platform for secure and rapid operational and technical co-operation between EU entities and Member State authorities.
- bring together all four cybersecurity communities.
- provide a new impetus to the process started in 2017 with the Blueprint.
- further operationalise the Blueprint architecture and mark a decisive step towards a European cybersecurity crisis management framework where threats and risks are identified, mitigated and responded to in a co-ordinated and timely manner. By taking such a step, the Joint Cyber Unit should help the EU respond to current and impending threats.

Participants in the platform should have either an operational or supporting role.

- Operational participants should include ENISA, Europol, the CSIRTs network and the Commission, the European External Action Service (including INTCEN), the CSIRTs Network and EU-CyCLONe.
- Supporting participants should include the European Defence Agency (EDA), the NIS Co-operation Group Chair, the Council Horizontal Working Party on Cyber Issues Chair, and one representative of the relevant PESCO projects.

Since the Member States have operational capabilities and competences to respond to large-scale cyber threats, incidents and crises, the platform's participants should primarily rely on their capacities, with the help of relevant EU entities, to achieve their objectives.

A four-step implementation process

The objectives set out in the Recommendation are to be achieved through a four-step process:

- A preparatory process should start with the identification of relevant available EU operational capabilities and the launch of an assessment of the roles and responsibilities of participants within the platform.
- The development of the EU Incident and Crisis Response Plan, consistent with the Blueprint and the EU Law Enforcement Emergency Response Protocol, the roll-out of preparedness and situational awareness related activities, consistent with the Cybersecurity Act and the Europol Regulation, and the conclusion of the assessment on the roles and responsibilities of participants within the platform. The working group should present the results of that assessment to the Commission and the High Representative, which subsequently will share those results with the Council. The Commission and the High Representative should work together, in line with their respective competences, to draw up a joint report based on that assessment and invite the Council to endorse that report via Council conclusions.
- Following that endorsement, the Joint Cyber Unit will be made operational, with a view to completing the two remaining steps of the process.
- Participants should be able to deploy EU Rapid Reaction teams within the Joint Cyber Unit, along the lines of procedures defined in the EU Incident and Crisis Response Plan, leveraging both the physical and virtual platform and contributing to various aspects of incident response (from public communication to ex-post recovery).

Private sector stakeholders, including both users and providers of cybersecurity solutions and services, will be invited to contribute to the platform, allowing participants to improve information sharing and enhance the EU's co-ordinated response to cyber threats and incidents.

The role of ENISA

It is intended that the Commission, ENISA, Europol and CERT-EU should provide administrative, financial and technical support to the Joint Cyber Unit, subject to budget and human resource availability. In view of its reinforced mandate, ENISA is in a unique position to organise and support the preparation of the Joint Cyber Unit, as well as to contribute to its operationalisation. In line with the provisions of the Cybersecurity Act, ENISA is currently establishing a Brussels office to support its structured co-operation with CERT-EU. That structured co-operation, including adjacent offices, provides a useful framework to facilitate the creation of the Joint Cyber Unit, including the establishment of its physical space which should be made available to participants in case of need, as well as to staff from other relevant EU institutions, bodies and agencies.

The physical platform should be combined with a virtual platform composed of collaboration and secure information sharing tools. Those tools will leverage the wealth of information gathered through the European Cyber-Shield, including security operation centres (SOCs) and information sharing and analysis centres (ISACs).

Law enforcement procedures

The EU Law Enforcement Emergency Response Protocol for major cross-border cyber attacks gives a central role to Europol's European Cybercrime Centre (EC3) as part of the 'Blueprint' framework. That Protocol allows EU law enforcement authorities to provide a response to large-scale cross-border attacks of a suspected malicious nature on a 24/7 basis through rapid reaction and assessment, as well as the secure and timely sharing of critical information for the effective co-ordination of responses to cross-border incidents. The Protocol further elaborates on the collaboration with other EU institutions and EU-wide crisis protocols, as well as crisis co-operation with the private sector.

The law enforcement community, with the support of Europol when appropriate, is to contribute to the Joint Cyber Unit by taking the necessary steps within the full investigation cycle, in line with the requirements of the criminal justice framework and the applicable electronic evidence handling procedures. Europol has been providing operational support and facilitating operational co-operation against cyber threats since the inception of EC3 in 2013. Europol should support the platform according to its mandate and the intelligence-led policing approach, while leveraging all types of in-house expertise, products, tools and service of pertinence for the incident or crisis response.

The cyber diplomacy community

The EU cyber diplomacy community seeks to promote and protect a global, open, stable and secure cyberspace and to prevent, deter and respond to malicious cyber activities in this regard. In 2017, the EU established a *Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities* (Cyber Diplomacy Toolbox). This framework is part of the EU's wider cyber diplomacy policy. It contributes to conflict prevention and greater stability in international relations. It allows the EU and Member States, in co-operation with international partners where relevant, to use all Common Foreign and Security Policy (CFSP) measures, in line with the respective procedures for their attainment, to encourage co-operation, mitigate threats and influence current and potential future malicious behaviour in cyberspace. The cyber diplomacy community should co-operate under the Joint Cyber Unit by using and providing support in using the full range of diplomatic measures, notably as regards public communication, supporting shared situational awareness and engagement with third countries in the event of a crisis.

The cyber defence community

Within the cyber defence community, the EU and Member States aim to strengthen cyber defence capabilities and enhance further synergies, co-ordination and co-operation between relevant EU institutions, bodies and agencies, as well as with and between Member States, including as regards the Common Security and Defence Policy (CSDP) missions and operations. The community functions based on an intergovernmental governance at EU level, national military command structures and military, or dual-use capabilities and assets. In light of its different nature, specific interfaces with the Joint Cyber Unit should be built to enable information sharing with the cyber defence community.

Private sector engagement

Through the Joint Cyber Unit, participants should adequately integrate private sector stakeholders, including both providers and users of cybersecurity solutions and services, to support the European cybersecurity crisis management framework, with due regard to the legal framework for data-sharing and security of information. Cybersecurity providers should contribute to the initiative by sharing threat intelligence and providing incident responders to quickly expand the Unit's capacity to respond to large-scale attacks and crises. Users of cybersecurity goods and services, primarily those under the scope of the NIS Directive, should be able to seek help and advice through currently missing structured channels linked to EU-level information sharing and analysis centres (ISACs). The platform could also contribute to strengthening co-operation with international partners.

The role of the Commission

The Commission, primarily through the Digital Europe programme, will support the necessary investment to set up the physical and virtual platform, and build and maintain secure communication channels and training capabilities, as well as developing and deploying detection capabilities. In addition, the European Defence Fund could help fund key cyber defence technologies and cyber defence capabilities which would reinforce national cyber defence preparedness.

Tobias Fiebig, Max-Planck-Institut für Informatik and
Doris Aschenbrenner
Aalen University
—
2 August 2022

Burning down the house

We currently live in a world that is evaporating under the human-made climate emergency and countless other shifts we find ourselves in at the moment. The Internet of today will certainly be neither sustainable nor resilient in the future we appear to be heading towards.

This article is adapted from an original written by Tobias Fiebig, Max-Planck-Institut für Informatik, and Doris Aschenbrenner, Aalen University, who wrote down these thoughts in the form of '13 propositions', which are based on their research contributions published in the past, public discourse, and are rooted in system administration lore and their own experience as system administrators. They are intentionally bold, and the authors make no personal claim to originality or completeness.

Thirteen propositions on an Internet for a "burning world"

Proposition 1:
Operating systems require operators to execute care towards their system, their users and the infrastructure as a whole.
This is not so much about operating systems running on computers but more about the process of running and maintaining a system. If we want the Internet to be sustainable in our burning future, we have to reorient ourselves to actually doing the care-work necessary for keeping infrastructures running and addressing users' needs.

If we do that, digital infrastructure might give us an edge in surviving the future to come. If we don't start caring soon, it may very well become a liability (if it is not already) further dragging us down.

Proposition 2:
The centralisation of the Internet has been promoted by a lack of care.
The early Internet used to be a rather collaborative network, and that showed in the protocols developed for it. For example, initial visions of SMTP – the protocol underlying email – assumed open relays being the default, and DNS – as a UDP-based protocol – neglected the issue of spoofing.

Over time, the Internet has become more hostile – more of a 'for one's own benefit' focused place, where such features turned from useful to dangerous. Especially the abuse of DNS and similar protocols from the same era has given rise to large-scale denial of service (DoS) attacks.

DoS attacks are enabled by careless system administration, ranging from operators who leave, for example, DNS-based packet amplifiers readily connected to the Internet and allow spoofing addresses on their network, to vendors that roll out carelessly thrown together IoT devices, shipped with default credentials. It has become common to provide services and run infrastructure without taking responsibility and caring for its impact on others. If one does not fall victim to such a large-scale DoS attack, one has to hide behind the larger network of a major centralised cloud provider. And so we are all paying the price for carelessness in the form of centralisation, with all its implications.

Proposition 3:
There is a tension between privacy and security, pitting decentralisation vs. centralisation.
This point confounds several aspects of centralisation and cloudification. One part is that a major component of centralisation (and migrating to centralised cloud infrastructures) is the reduction of capital expenses in terms of institutionalised knowledge and operational expenses in terms of knowledge workers. Having a full team working on security makes a lot more sense at scale. The other part is that security is simply 'easier' for centralised environments like clouds.

This ultimately creates a choice between the devil and the deep blue sea. Either you allow a selected hypergiant to (technically be able to) read your emails, and their walled garden and ability to scale operations will keep your mail and you secure. Or you host your own system, and it may be less able to deliver your mail to others, or find it leaked due to a configuration mistake.

Proposition 4:
Centralisation and profit are inherently incompatible with care for infrastructures.
In our globalised economy, the idea is that people, especially corporations, naturally seek to maximise their profits and gains. For the purposes of this proposition, it is irrelevant whether this is a good or a bad thing.

Unfortunately, centralisation and profit are incompatible with care. Centralising infrastructure also means centralising control which means centralising power which in turn means that, all of a sudden, entities gain the ability to make decisions simply for their own benefit, disregarding the needs of others. This, quite obviously, can become suboptimal if we are talking about infrastructure others depend on.

In a profit-oriented world, it can become fiscally untenable to maintain sufficient care for a service/infrastructure and its users. To conserve their bottom line, corporations will discontinue services that users rely on, or apply support mechanics that cannot provide the care some users may need, or neglect maintenance of existing systems. Or, more bluntly put: to scale a system you sometimes have to make things the same that inherently are not.

For a profit-driven corporation, this is a rational decision, but it will mean a significant loss for users, no matter how mundane (your fancy home automation no longer working), unusual (you found love with a digital entity) or obviously essential (visual implants becoming obsolete) a service is.

When centralisation disappears

Centralisation is the continuous aggregation of infrastructure and content around a small number of hypergiants – Amazon, Meta, Apple, Microsoft and Google – with their large infrastructure-, platform- and software-as-a-service offerings.

As unimaginable as it may have been decades ago that one day Myspace would no longer be there, or, as hypothetical as it may have sounded in Wall Street in 2008 that Lehman Brothers might be gone in a matter of days, the idea of Amazon, Google, Microsoft, Apple or Meta (and for that matter, a set of several more hyper and micro-giants like Digital Ocean or Hetzner) simply disappearing can't be discounted.

Proposition 5:
We have to be prepared for hypergiants failing.

Small ripples can cause a hypergiant to ultimately tumble, and our burning world is sending out the first signals. Infrastructure supported by the exploitation of labour in a globalised world will not sustain itself forever.

Still, hypergiants and all those fancy tech companies that make up their heavily paying customer base have a thing for exploiting labour.

One of the big innovations that Uber, DoorDash, Amazon and others have found is a way around that concept of worker rights. You can be insanely more profitable if you don't have to bother with the costs of generations of societal development and social security.

Nevertheless, this will not work forever.

Workers realise that those mechanisms put in place – organising, unionising, strikes and labour fights — are there because they are useful, and are beginning to prove successful.

The question of why hypergiants fail and there are several possibilities and examples, and whether it is ultimately good for the Internet, is not essential. The important question is how we handle them disappearing, possibly suddenly, when the majority of websites contain fonts hosted by Google, for example; or run entirely on Amazon Elastic Compute Cloud (EC2).

If a hypergiant fails all of a sudden, we will have a lot of legacies and broken infrastructure. And, historically, legacy infrastructure is not something we are particularly good at dealing with.

Proposition 6:
Communities caring for local and distributed infrastructure are the future in a world falling apart.
Our world is changing and not necessarily for the better. This is a world where billions are displaced by heat and floods, and where the global north learns that climate change will ravage us all, no matter where we live. A world where there is no global supply chain to collapse anymore, and most long-range fibres just go … dark.

The question here is, of course, how dire our future will be.

In a ravaged and war-torn future with limited space for things to be peaceful enough for technology to function, "… we would still have *some* power available …".

That world is pretty much aligned with a rather 'solar punk' future, one where there is some power available, but it's not as abundant as now.

Naturally, despite having burned down, our world would remain littered with (dysfunctional) computers and network technology. That world would most likely be one where local communities commandeer these sets of technology and start to (re)build (potentially interconnected) networks (of networks). However, the focus would always be providing primary and useful services for local communities. Having local access to a knowledge database will be more important than, say, global communication.

With supply chains gone, keeping systems and networks running will also become difficult in terms of getting spare parts and replacements. This world will be about engineers finding ways for the benefit of their local community (again).

The task of 'making it run, even though the cloud controller is gone' will potentially be an essential occupation in the future. Local communities will (must) find ways to use technology and provide working services to survive.

Proposition 7:
The slow adoption of IPv6 hinders a re-decentralisation of the Internet.
The IPv4 address space is, for all practical matters, exhausted and unjustly distributed. With the Internet still being very much IPv4-centric – at least when it comes to the path outside of hypergiants – communities running their services still need IPv4 addresses to provide services.

If we want to redistribute the Internet, without further disadvantaging traditionally disadvantaged regions, rolling out more IPv6 is the only path forward.

Proposition 8:
In a burning world, functionality is more important than security, but remains trumped by safety.
Faced with a world burnt to its foundations – with an Internet fallen apart and hypergiants failed – the paradigms of what is important would shift dramatically. In such a scenario, the utility and functionality of systems would superimpose their security even more robustly than in the current world.

Security may end up being resolved by a social contract, along the lines of 'you won't break your power supply'. Therefore, in such a world, threat modelling would see a significant shift away from security threats from the larger Internet, and become a question of safety, akin to the question of 'What (physical) harm can be done (by outsiders) if it is not secure?' Ultimately, the physical safety (and survival) of local communities will have the highest importance.

Sustainability means simplicity

We really have a tendency to build complex systems. There are countless discussions about the explosion in the complexity of protocols; for example, the DNS Camel is certainly one of the most iconic illustrations of this issue.

Sometimes, this complexity comes in the form of AI systems. Sometimes it throws resources at concepts looking for solutions. Sometimes it's the issue of bloat on the web. Other times, we wonder where all the RAM went. Then there's the environmental issues associated with the footprint of large models, proof-of-work-based blockchain technology, and the piles of IoT waste. The examples are endless.

In the end, this all boils down to the joint responsibility that we have, as computer science people and ultimately those building these systems.

Proposition 9:
Systems that are too complex to be understood by a single person cannot be sustainable.

In a world burning down, it will be important to keep systems running. Systems may end up being isolated and small scale. They may depend on individual operators. They may depend on knowledge of how they are operated being easily transferable to another person.

To be sustainable in a burning world, systems will have to be run (and understood) by small teams and communities; and while automation is a necessity in an ever-growing and centralising Internet, its complexity might become a curse in an Internet that is supposed to survive in a burning world.

Proposition 10:
Systems should enable a better tomorrow and not burn the world even further.

With the wide availability of automation and support infrastructure – which, of course, has the good intention of enabling many people to build – the hunger for system resources steadily increases. Currently, we tend to create a growing ball of systems supporting other systems – abstracting something simple to be more complex. This, in turn, becomes embedded in how we build and design systems, adding layers and using more resources for the same functionality. This overall development has probably been brought to the extreme by Bitcoin and its proof-of-work siblings, churning through energy on a nation-state scale, while having no purpose except profit.

As such, it should be the responsibility of engineers to ensure that the systems they build contribute to a beneficial purpose and do not harm society or the environment by needless and redundant processing. The system's purpose should be tangible and reasonable in relation to the resource consumption of the system and serve the benefit of all instead of the profits of a few.

Proposition 11:
There are no technical solutions for social and societal problems.
A common theme in communities of engineers is that periodically, several tech-savvy people start to implement a complex digital system to solve a real-world social issue, usually in a way that also includes a touchscreen and/or a Raspberry Pi. Ultimately, that approach will suffer from limited adoption and the same issues as before, so a social solution will have to be found instead. If the community is very unlucky, the technical solution will also introduce new social problems. The insufficient solution inevitably stays in place, usually until the next generation of local nerds experiences this issue and repeats. In a nutshell: digitising a bad process won't result in a better process but in a digitised bad process.

The same 'solving social problems with technical solutions' reasoning is also applied to problems faced at the much larger scale of the Internet and society as a whole, inevitably with the same result. Sanctions and sovereignty.

For some weird reason, humans have an uncanny tendency to react to crises not with the appropriate unification and 'surviving together' response, but with an 'us' versus 'them' mentality.

With the 'neuland' of the Internet having been around for a couple of decades now, traditional leadership and governance people discovered this vast new area for themselves and their ideas.

Humans being humans, when confronted with something new, people will try to pattern match it to what they already know. The known terms for international politics are 'borders' and 'sovereignty', so this pattern matching gave us the new buzz-term 'digital sovereignty'.

This pressing issue in the policy arena is usually understood as 'ensuring that a state can exert policy on the (IT) systems used by its constituents, while ensuring that only their own policy is applied to them'.

The classic example of attempts to realise this with policy is most likely the ongoing discussion of the Trans-Atlantic Data Privacy Framework, that after various iterations replaced the EU-US Privacy Shield and Safe Harbor agreements. A similar, more technical, approach is Schengen Routing, which is an attempt to make sure packets from European users do not leave Europe.

What all these approaches have in common is that they dream of a cosy little Internet within the boundaries of individual nation states or sets of such. Europeans are usually quick to judge economies installing cryptographic backdoors and running national firewalls for censorship. Under the guise of either digital sovereignty or the pretence of protecting groups of vulnerable people they are also equally quick to flock to policies yielding the same results.

At this point, we do not want to pass judgement on these approaches, no matter where they take place.

Proposition 12:
Internet sanctions: What once has been thought can never be taken back. The Internet will be falling apart.
The quote relates to a physicist's perspective on the probability of keeping one's own dangerous inventions – ultimately an analogy for nuclear fission – from the world. However, it is also relevant in terms of the Internet as technology and proposals with good intentions are developed.

A concrete example: In the wake of the war waged by Russia against Ukraine, members of the Internet community and several politicians called for a multistakeholder approach to 'Internet sanctions.' The authors of that open letter called for a multistakeholder mechanism that populates databases, which willing Internet participants can use to participate in sanctions against specific netblocks and domains, ideally by using existing infrastructure for blacklisting IP routes.

It has now been successfully demonstrated that state blocking of resources is possible. Therefore, we claim that this approach will be used again by policy makers. It will also put Internet sanctions on the diplomatic agenda, leading to a fragmentation of the Internet: 'Well, if you block A, we will block B.' 'Well, if you block B, we will just disconnect all of you.' And then they do.

Proposition 13:
Digital sovereignty is being used wrongly.
Given the state of our world, we also have to consider a much more fundamental meaning of sovereignty that is usually missed: the ability to (re)build and maintain one's infrastructure independent of another party. And this is something that continues to get harder and harder. In a burning world, it may be essential to have the 'know how' to keep systems running, widely spread, and locally available. And yes, this includes questions like open and publicly available, ideally, open-source software and documentation. Otherwise, computers may become rather expensive bricks – or worse!

Also, the policy aspect may even be secondary. In the end, it's about running systems, providing services and caring for users. Everywhere. As long as we can rebuild.

Conclusion

These '13 Propositions for a Burning World' are intended to ask people to start thinking about a resilient and sustainable Internet that should be run with care for its users and the infrastructure itself.

The propositions might be overly bold, lack concrete solutions and paint a disturbingly dire picture. However, given the state of the world, the authors claim that we are past the point of raising awareness and hiding behind 'that would never happen.' We can no longer risk staying complacent in the hopes for a better future. We have to talk about these issues now and find tangible solutions. The future will be bleak if we do not make it better, and whether the world goes down in flames or not, preparation is better than reaction.

Asked for an answer to the questions they raise, the authors' first gut reaction roughly translates to 'Computers were a mistake. Learn to ride a horse and grow your own food'. But that cannot be the answer, and engineers, whether they work on applications, systems, networks, routing or anything else in the digital sphere, have a responsibility to build a better world for everyone and to keep trying to make the world better, even if it looks bleak.

This material is based upon work partially supported by CyberSecurity4Europe. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of their host institutions or those of the European Commission

David Goodman
Trust in Digital Life

—

12 October 2022

Reasonable Security

'Reasonable security' is a subjective term that has to be understood objectively, striking the right balance between security and privacy to ensure the rights of individuals. Without clear guidance, you may be uncertain what reasonable security looks like. And uncertainty is unsettling. Most regulatory bodies have also struggled to define exactly what reasonable security means. Reasonable security should not just be interpreted as 'minimum security' – the objective is to protect individuals' personal data that you are responsible for.

Failing to provide reasonable data protection opens an organisation to potential findings of negligence in the case of a data breach. Beyond the potential monetary impact of fines and plaintiff awards, the independent judgment of a court or regulatory body that an organisation failed to provide reasonable security could cause existing and potential customers to take their business elsewhere. Irrespective of the above, you still failed to protect your customers'/employees' data from a breach.

The security principle

If it is any consolation, as you're grappling with what reasonableness means, it appears that the EU which spent years drafting and finally publishing the GDPR, was probably not 100% sure either in specifying how far to go with security.

For example, Article 32 of the GDPR states:

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement* ***appropriate*** *technical and organisational measures to ensure a level of security* ***appropriate*** *to the risk, ...*

Despite the vagaries of this statement, the recital tries to help us understand what to do:

... including inter alia as ***appropriate****:*

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

An appropriate level of security

None of the tips provided are straightforward and it's not 100% clear how to execute them in most organisational environments. The GDPR article goes on to explain further:

> *In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

The word 'appropriate' is used judiciously four times, suggesting that it is up to a data protection officer (DPO), or equivalent, to figure out what it might mean in any particular context.

Finding motivation

OK, you say, then it's up to me and my security experts to make the hard, grown-up decisions and negotiate with the CIO/CISO and other executives who may themselves have competing priorities.

The crunch comes when there is a data breach.

Even if you satisfy a court that you met the legal requirements on the grounds of reasonable security, the loss of your customers' data would have a severely detrimental impact on your business's reputation and the consumer-perceived safety of associating with your much treasured and protected brand. By understanding the bigger set of problems you're trying to solve, you'll get a decent measure of what is and what isn't important.

Where to begin

Malware, phishing attacks and human error cause most data breaches. So, it clearly makes sense to encrypt and redact all personal data to limit the exposure of sensitive data in applications. However, the procedures required are often inconvenient, cumbersome and difficult to implement, particularly email encryption in a busy work environment where response speed and agility are demanded or simply part of company culture. At the very least, you should have an active enforceable password management program that ensures that passwords are changed frequently and are strength-based, and that separate passwords are used for different systems. Imposing lockouts after a set number of unsuccessful login attempts or notifying users of suspicious activity may not be popular, but frankly it is necessary. Leaving no stone unturned requires ensuring the security of the application, database and operating system layers, endpoints and mobile devices, hypervisors and micro services, remote, local and wide area networks as well as data centres systems and backups.

The stakes are high

In July 2015, the Ashley Madison website experienced a data breach by a group of hacktivists (the Impact Team) that exposed the profile information of 36 million users. Ashley Madison charged customers that no longer wanted to be associated with the site $35 per person to delete their profile information. Rather than deleting these profiles, Ashley Madison moved the profile data from their active site into an unsecured database that was easy to exploit.

The Impact Team claimed to have stolen more than 300 GB of data and leaked millions of Ashley Madison's users' email addresses and damaging emails from the CEO's account.

The US Federal Trade Commission (FTC)'s complaint stated that, despite claims that the website was "100% secure," "risk-free," and "completely anonymous," the company "engaged in several practices that, taken together, failed to provide reasonable security to prevent unauthorised access to personal information on their network", concluding that "in truth and in fact ... [the company] did not take reasonable steps to ensure that AshleyMadison.com was secure."

The past, present and future

In addition, the growth in the number of intelligent and Internet-connected devices together with the emergence of 5G are introducing new data-driven and increasingly autonomous scenarios. For enterprises, that includes surveillance cameras as well as personal objects and devices that hackers could attack to gain further access into your network, systems and other vital resources. If that were not enough, we're not yet done with physical data assets – such as paper files – which are equally susceptible to attack and tampering which could lead to mischief and data leaks. Any hard copy sitting in an open room is a potential liability.

The future of reasonable security

The speed at which we are collecting data and evolving technology in combination with the exploitation of our supply chain makes "reasonable security" a moving target precariously positioned on a slippery slope. Reasonable security practices will depend on the circumstances and whether a business's decisions were sound in hindsight.

Documentation of a reasoned decision will give evidence that shows whether a business considered the risk and options and, for legitimate business reasons, may not have implemented a more robust solution.

The law is like a slow-moving tortoise, and the technology and adversaries are the hares. Laws are hesitant to clearly define what it means to act reasonably because

(1) the legislators are not cybersecurity experts, and
(2) by the time the law is published, the technology has changed so dramatically the law is outdated.

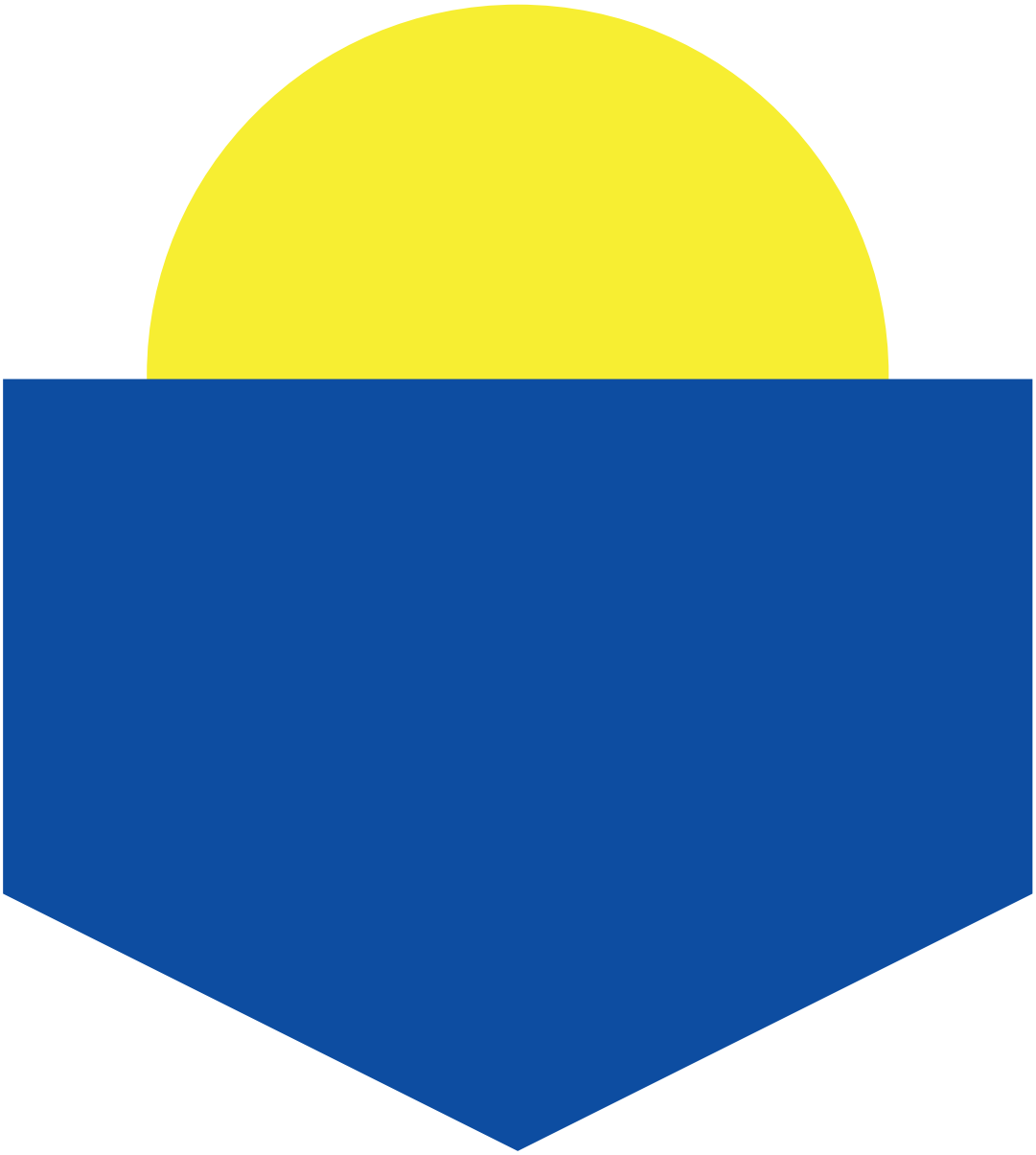
Conclusion

Risk management is at the heart of organisational governance and

is the cornerstone of security program development. Organisations confront infinite risk with finite resources, but not all risks are material, nor do all risks have a high probability of occurring. Reasonable security should anticipate which risks an organisation will likely confront and document its risk treatment strategy. Risks can be mitigated, insured against (transferred), accepted, avoided or a combination of these strategies, but risks should never be ignored.

There is no one-size-fits-all definition of reasonable security. All companies that hold personal data in trust should implement reasonable data protections to secure that data.

'Reasonable' is what the courts decide it is, depending on the facts at hand for the case before them. Regardless of precedent or regulator-defined rules, reasonable security is ultimately what your customer, partners and employees expect. An organisation's privacy leader's role is to work with a security leader to determine the right approach and work with them to uncover deficiencies and advocate for improvements where needed.



4.2
Scientific publications

During the lifetime of the project, CyberSec4Europe partners authored and co-authored over 150 published scientific papers, all of which are referenced on the project website with details of how to access the source publication.

We were specifically charged with creating excellence as well as raising awareness about cybersecurity and we reported on our considerable number of contributions to the body of scientific publications as well as our involvement in driving and participating in summer schools focused on cybersecurity.

The ambition of CyberSec4Europe was to achieve a high level of excellence by prioritising the publication of research results in the best top-tier journals and highly recognised conferences. Relevance to the area of the project and to European interests as well as the high level of academic recognition guided the submission policy of the project.

As well as maintaining an up-to-date listing of all our public deliverables, we published all the peer-reviewed scientific articles authored and co-authored during the lifetime of the project by CyberSec4Europe partners. Over 150 published scientific papers are referenced on the project website with details of how to access the source publication.

Needless to say, we cannot provide a summary of every paper written but we do offer an exemplar from a recent publication.

Elias Athanasopoulos
University of Cyprus
—
4 October 2022

Protecting servers from data breaches with Lethe

Nowadays, it is no news to hear that even high-profile web services, such as Yahoo, Dropbox, LinkedIn and Facebook, have been compromised and millions of passwords leaked. These data breaches are often detected several months or years after the attackers have exploited the services and posted, or even sold, their data online.

Honeywords, which are false passwords associated with each user account, provide an easy to set up and low overhead approach for detecting data breach incidents. A honeyword, which is visually similar to a user's real password, is intended to lure potential adversaries into selecting it to attempt to log into the user's account. However, using a honeyword to login sets off an alarm that an attempted data breach has been detected.

Since real passwords are now blended with honeywords, we need to store a list containing the index (position) of each user's real password for validating login attempts. However, this list is an Achilles' heel which, once compromised, renders honeywords no longer useful. Thus, for increasing the dependability of honeywords, such lists have to go!

Lethe (from the ancient Greek word "λήθη", which means forgetting) is a honeywords-based data breach detection framework that can operate without storing the real password for each user account. Lethe is based on two principles:

- By utilising machine learning technologies for generating honeywords that cannot be reproduced, even when given the same password as input, Lethe ensures that an attacker cannot reverse the model and subvert the security of the honeywords.
- The only one who knows the real password is the user who selected it in the first place: Lethe is not aware of the real password.
- Lethe records login events, but without storing the password used, and then replays those login events in another server offline. During this replay, Lethe can detect whether two different passwords were used for logging into a particular user account, in which case it signals a data breach alarm.

Full details of publication:

- Title: Lethe: Practical Data Breach Detection with Zero Persistent Secret State
- Authors: Antreas Dionysiou and Elias Athanasopoulos
- Publication: *Proceedings of the 7th IEEE European Symposium on Security and Privacy*, Genoa, June 2022
- Additional note: Distinguished paper award finalist

4.3
Events

As well as hosting and organising three annual concertation events and the summit conference, Momentum!, we hosted a number of lively public evening panel discussions and our consortium partners participated in and in some cases organised a wide range of external events. Our Insights webinar series gave researchers a channel to share their ideas with a wide audience from the European cybersecurity community.

The main goal of the project's dissemination activities was to ensure that the findings of the project as a whole reached and engaged key stakeholders effectively. As well as maintaining an up-to-date listing of all our public deliverables and scientific articles, we also incorporated a calendar of project and industry events. In concert with the website, we maintained an active social media presence on Twitter and LinkedIn. To capture the breadth and depth of the project's outreach to wider audiences, we regularly reported on all the events, conferences, workshops and community interactions undertaken by project partners.

The three annual concertation events involved all four pilot projects and European agencies, such as ECSO (European Cyber Security Organisation) and ENISA (the European Union Agency for Cybersecurity). They represented the most visible aspect of our work on community building beyond the project, involving significant collaboration and interaction with external entities. These are the European institutions and agencies, cybersecurity communities, ecosystem innovators, the other three pilot projects (CONCORDIA, ECHO and SPARTA) and other cybersecurity projects. Together they support a fully sustainable competence network and comprehensive integrated European cybersecurity ecosystem for the benefit of European industry, the European research community and ultimately that of the European citizen.

Over the course of the project, we expanded the project community inviting over 40 Associate partners to participate in our work as well as over 150 Friends of CyberSec4Europe to join our events and to keep abreast of our latest news. We actively collaborated with the other project pilots as well as ECSO in focus groups in the areas of communications, cyber ranges, education, governance, roadmapping and threat intelligence in the financial sector.

David Goodman
Trust In Digital Life
—
22 November 2019

CyberSec4Europe comes to Toulouse!

Cybersecurity For Europe 2019, the first of three annual CyberSec4Europe concertation events, brought together significant European cybersecurity stakeholders including representatives of all four pilot projects in Toulouse from 13-15 November. Hosted by the Occitanie Region at the seat of the regional council of Occitanie, the three days of collaboration, conversation and networking featured high-level participants from industry, academia, government from across the European cybersecurity competence network.

The event attracted around 150 participants comprising a comprehensive representation from the cybersecurity ecosystem and the stakeholder community, including but not limited to: the public sector (the European Commission, the Occitanie Region and ENISA), the private sector (large companies, SMEs), the research and academic community (from all over Europe), and civil society (NGOs, citizens advocacy organisations).

The first day provided an overview of the symbiotic perspectives on cybersecurity from local, national and European-level government agencies, including Miguel González-Sancho from the European Commission's DG CONNECT and Luigi Rebuffi, Secretary General of ECSO, the European Cyber Security Organisation. The conference was formally launched in the early evening by Kai Rannenberg from Goethe University Frankfurt, co-ordinator of CyberSec4Europe, who introduced Bertrand Monthubert, President of Occitanie Data, Renaud Vedell, from the French Ministry of the Interior and a video message from Mariya Gabriel, European Commissioner, Digital Economy and Society.

Delegates were then transported across town to a reception hosted by the Ocssimore association, where, after an introduction by Antoine Derain from Group BPCE who described the Ocssimore's implementation of the decision-making processes and policies proposed by the governance model, they had the opportunity to meet the contributors to the construction of the Toulouse pilot regional hub of the future European network of cybersecurity competence centres.

The second day consisted of two sets of panels. The morning sessions focussed on policy matters, looking at recommendations for research and innovation in cybersecurity followed by a discussion on governance. The afternoon sessions were more technical, examining first, good practices associated with data-sharing whilst handling different types of incident responses, followed by a panel addressing the broad subject of managing identities securely, from the perspectives of system protection as well as the preservation of individual privacy. After a recap session involving the moderators of the four panels, the conference attendees left to walk along the banks of the beautiful river Garonne to the Hotel Dieu Saint Jacques, a former hospital situated alongside the Pont Neuf, for dinner and some classic jazz.

The final day started with an inspirational keynote presentation from Pascal Andrei, the Chief Security Officer at Airbus in Toulouse, whose observations on the threat of cyber attacks, particularly to the supply chain, resonated with the audience.

The panel on the future of European cybersecurity presented visions of the security implications of emerging technologies alongside some hard-hitting realities relating to European strategic autonomy in cybersecurity. The final panel reflected back to the beginning of the conference in a conversation between the representatives from the four pilots who were each asked how they envisaged furthering inter-pilot collaboration over the coming months and what they admired the most about each other's project. At the conclusion of the three days, delegates came away, heads buzzing from what they'd heard and discussed and plenty of ideas for the next CyberSec4Europe concertation event in 2020!

Cybersecurity for Europe 2019 was organised locally by Université Paul Sabatier, and the Institut de Recherche en Informatique de Toulouse (IRIT), with the support of the Occitanie Region.

David Goodman
Trust in Digital Life
—
1 September 2020

Realising Europe's cybersecurity strengths and capacity for the 2020s

On 12 September 2018, the European Commission proposed a regulation establishing a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Co-ordination Centres. Its aim was to improve EU cybersecurity and resilience, enhance and strengthen the EU's cybersecurity capacity, stimulating the European cybersecurity technological and industrial ecosystem, as well as to co-ordinate and pool relevant EU resources. Two years later, key aspects of the proposal continue to be discussed among the major European institutions supported by the four pilot projects, including CyberSec4Europe.

The evening online panel discussion aimed to explore how the proposed Competence Centre and Network regulation will progress during the current German EU Presidency – and beyond.

The distinguished group of panelists were:

- Tamara Tafra, Counsellor for Cyber Issues, Permanent Representation of Croatia to the EU. She was Chair of the Horizontal Working Party on Cyber Issues during the recent Croatian Presidency.
- Rasmus Andresen, a Member of the European Parliament and Rapporteur for the Cybersecurity Competence Network Centre Regulation dossier.
- Miguel González-Sancho, Head of Cybersecurity Technology and Capacity Building, DG CONNECT, European Commission.
- Andreas Könen, head of Cyber and Information Security at the German Federal Ministry of the Interior, Building and Community.
- Juhan Lepassaar, Executive Director of ENISA.

The moderator was David Goodman from Trust in Digital Life Association.

The panel discussion opened with a high-level review on how the regulation proposal progressed at the Council during the Croatian Presidency which ended on 30 June. Despite the restrictions on face-to-face meetings from March to June, a mandate was agreed by Coreper on 3 June and negotiations with the Parliament started on 25 June, with only two open issues (the number of seats and voting rights). Through the incoming German Presidency, the ambition is to complete the trilogue and to have the regulation adopted by the end of 2020.

The Competence Centre

The Competence Centre is intended to be the main body managing EU financial resources dedicated to cybersecurity research under the two proposed programmes – Digital Europe and Horizon Europe – within the next multiannual financial framework (MFF) for 2021-2027.

- The primary role of the Competence Centre is to provide investment, identify priorities, both political and technical, pool resources and give support to Member States and the stakeholder community.
- The anticipated engagement of the Member States with the Centre could be in taking joint proposals to the Centre which would approach the EC to match the contribution of the Member States.
- The network that the Centre will support includes the stakeholders participating through the pilots as well as the communities associated with ECSO and ENISA. The Commission's Cybersecurity Atlas is already demonstrating how the broader community of cybersecurity experts will be built in practice.

The Advisory Board and the stakeholder community

- There are outstanding differences of opinion concerning the Advisory Board, whether to maintain the involvement of civil society, industry and science as an integral part of the structure of the Competence Centre; or to remove it, giving a bigger role to the European cybersecurity stakeholder community with more power to choose its own representatives.
- It is envisaged that ENISA will have an enhanced role, with several levels of co-operation with the Centre – structural, operational (including research area synergies, workshops etc) and a shared community.
- It was confirmed that the concept of CHECKs (Community Hubs of Expertise in Cybersecurity Knowledge), as proposed by CyberSec4Europe, is broadly supported.

Looking beyond 2020

- The establishment of the Competence Centre will be a step in the direction of giving Europe a stronger and better co-ordinated role in cybersecurity on the world stage than it has at present, leading to greater European sovereignty.
- Throughout the pandemic, everyone has spent more time online and become more keenly aware of cybersecurity issues, at both a micro and macro level, than ever before, making now a great opportunity to headline cybersecurity.

- One of the first things the Centre will do is to launch its first round of projects, the results of which we should be able to see next year.
- A concern was expressed as to whether the Centre will be pro-active, stimulating new products, proposing new legislation and driving standardisation – or 'just' a distributor of money to Member States, which are perceived as still prioritising the building of their own cybersecurity capacity, rather than encouraging more money to be invested in common European projects.

It was observed that however much we invest, it will always all come down to the actions of individuals, raising awareness and working on cyber hygiene, in order to protect us all.

David Goodman
Trust in Digital Life
—
18 December 2020

CONVERGENCE: When the legislation and the four pilots converged

In 2019 the European Union funded four innovative projects to pilot the proposed legislation on a European cybersecurity competence centre and network of cybersecurity expertise. As the legislation edges ever closer to approval by the European Parliament, the four pilot projects, CyberSec4Europe, SPARTA, CONCORDIA and ECHO, organised for the first time a single online collaborative event, CONVERGENCE, from 9-11 December 2020, that highlighted the joint progress made and brought together the most important people and organisations addressing cybersecurity in Europe.

The event opened on the evening of 9 December with welcome addresses from the four pilot co-ordinators followed by a panel discussion featuring four distinguished speakers who addressed the status and impact on the cybersecurity community of the new regulation:

- Rasmus Andresen, Member of the European Parliament, Rapporteur Cybersecurity Competence Network Centre Regulation
- Despina Spanou, Head of Cabinet of the Vice-President of the European Commission, Margaritis Schinas
- Andreas Könen, Head of Department Cybersecurity and Information Security in the German Ministry of the Interior
- Wojciech Wiewiórowski, European Data Protection Supervisor
- Miguel González-Sancho, Head of Unit Cybersecurity Technology and Capacity Building, DG CONNECT, European Commission

Over the next one and a half days each pilot demonstrated their achievements and results to date through videos, presentations, tools and panel discussions, and a series of focus group sessions showcased the co-operation between the pilots in key cybersecurity areas.

These sessions covered topics ranging from communications to cyber ranges, education and governance to roadmapping and threat intelligence, and also featured a session on the European Cybersecurity Atlas which launched in mid-December.

The Atlas is a first of its kind and will be an important support to the European Cybersecurity Competence Centre in Bucharest. Over 500 members of the cybersecurity stakeholder community registered for the online event from across Europe, North America and Asia Pacific.

This was the second in a series of three cybersecurity concertation events and the four pilots are already looking forward to the next one in a year's time, hopefully in person.

CONVERGENCE was hosted with the friendly support of the Representation of the State of Hessen to the EU.

David Goodman
Trust in Digital Life
—
18 May 2022

CyberSec4Europe in Venice

Over three days in early April, more than 500 privacy and security professionals gathered in the magnificent settings across the Ca' Foscari University campus close to the Grand Canal in Venice for the 2022 Privacy Symposium.

Sessions were organised to foster dialogue and co-operation among researchers from both sides of the Atlantic. National supervisory authorities presented and shared their lessons learnt and recommendations on topics such as privacy-by-design, cross-border data transfers, data breaches and 'legitimate interest' in practice.

CyberSec4Europe – research to innovation

Part of the programme was reserved for European research projects and to that end, representatives from CyberSec4Europe, an official partner of the Privacy Symposium, were invited to demonstrate the results of the project's work in developing privacy-aware software assets and the innovative approaches adopted by the vertical applications.

During the morning of 7 April, Antonio Skarmeta from the University of Murcia moderated a two-hour session – *Research to Innovation: Common Research Framework on Security and Privacy* – in which ten short presentations were given, ranging from 'Cybersecurity governance' to 'Privacy-preserving cyber threat intelligence sharing and enhanced intrusion detection'.

In the afternoon, David Goodman from Trust in Digital Life introduced another two-hour session – *Research to Innovation: Privacy-preserving Industry Application Innovations* highlighting the work carried out on roadmapping as well as the development of demonstrator use cases. Four of the seven application areas areas – open banking, higher education, medical data exchange and smart cities – presented their work with an emphasis on those aspects most relevant to privacy.

At the end of the day there was a joint session demonstrating *European Cybersecurity Collaboration in action* featuring representatives from both CyberSec4Europe and CONCORDIA who described common collaborative activities and innovative solutions envisioning new cybersecurity assets in the areas of cyber threat intelligence and financial incident reporting.

An international gathering

The Privacy Symposium is an international conference established to attract, present and discuss original and innovative research results and technology developments related to personal data protection and compliance with data protection legislation. This year it brought together legal and technology experts together with researchers, data protection authorities and privacy/security professionals to share their knowledge and to support international dialogue and co-operation.

In over 77 sessions more than 170 international top-level speakers took the floor from organisations including the OECD, the Data Protection Unit of the Council of Europe, the UN rapporteur on the right to privacy, the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), the data protection authorities (DPAs) of the United States, Japan, Canada, Brazil, Mexico, Italy, France, Germany, Spain, Belgium, Hungary, UK, Switzerland and others, as well as researchers on innovative technologies.

The keynote speakers included such luminaries as Dr Andrea Jelinek (President of the EDPB), Dr Guido Scorza (Italian Data Protection Supervisory Authority), Jane Horvath (Chief Privacy Officer, Apple), Catherine Lennmann (Swiss DPA), Julie Brill (Chief Privacy Office and Corporate Vice President, Global Privacy and Regulatory Affairs, Microsoft), Tommaso Stranieri (Partner, Deloitte Risk Advisory), Conor Hogan (Global Practice Lead on Privacy, BSI Group), as well as Vint Cerf, the so-called 'Father of the Internet'.

The EU's General Data Protection Regulation (GDPR) has triggered a chain reaction with many other jurisdictions around the world adopting their own regulations. At the same time, the process of digitisation has impacted all economic and societal sectors, generating an exponentially growing volume of personal data. There are many questions that arise in this context. For example, supporting the convergence of data protection requirements can only be achieved by close collaboration among and across distinct jurisdictions; and there are open questions about how to adopt data protection-by-design approaches with emerging innovative technologies such as AI, 5G/XG, distributed ledger technologies (DLT), extended reality (XR)/Metaverse, quantum computing, IPv6, IoT and Edge computing and more.

Challenges are constantly emerging – and will continue to do so for the foreseeable future – requiring original research results and innovative approaches. What became clear throughout this event was the strong desire by all privacy professionals present to collaborate at national, regional and global levels on resolving outstanding technical aspects and tackling issues related to compliance monitoring. The growing focus is illustrated by the many other high-quality events focused on privacy and data protection that appear somewhere in the world almost every week.

CyberSec4Europe is making a contribution to this effort, and it is to be hoped that its legacy will be reflected in next year's event in Venice!

David Goodman
Trust in Digital Life
—
2 June 2022

CONVERGENCE NEXT is here!

CyberSec4Europe, CONCORDIA, ECHO and SPARTA are hosting CONVERGENCE NEXT, a three-day event from 1-3 June at the Hessen Representation in Brussels. It follows in the tradition set in the first CONVERGENCE event on 9-11 December 2020 which successfully presented results and demonstrations from the four pilot projects and the collaborative focus groups.

CONVERGENCE NEXT is focussing on the future of the community, the European Cybersecurity Competence Centre (ECCC) and looking at the key issues for cybersecurity in the future. This event is not to be missed if you are interested in European cybersecurity issues. High-level representatives from EU institutions will discuss the role of the ECCC and that of the wider stakeholder community in the next stages.

The first day sets the scene with a review of how we got to where we are today from the perspectives of the four pilots, ECSO and EARTO. One session will investigate the key explorations on how the wider cybersecurity community should be governed in the future in the context of the ECCC and the national competence centres.

The proceedings conclude with an evening panel discussion, moderated by Kai Rannenberg, CyberSec4Europe co-ordinator, featuring representatives from the European Parliament, the ECCC, the European Commission, ECSO and the German national cybersecurity competence centre. This will be followed by an evening social event.

The next day dives into more of the detailed results of the work of the pilots over the last three years with a focus on research and innovation, highlighting the work carried out by the pilots, individually as well as jointly, on cybersecurity roadmapping and industrial demonstrator use cases.

The last day moves from where we've come from and what we've been doing to look at the sustainability of the community and expanding the impact of the momentum created by the pilots. A focus will be on the vital role education and capacity building play as well as how this contributes to the evolution of the European cybersecurity ecosystem. The conference will finish with a panel discussion involving more of the key stakeholder representatives who will be asked the simple intriguing question, "What Next?". No doubt, given the uncertain times we live in, we all look forward to hearing the answers.

You can catch up on CONVERGENCE NEXT from the video of the conference on the project website.

David Goodman
Trust in Digital Life

—

15 September 2022

What can Member States expect from their cybersecurity communities?

On 14 September, CyberSec4Europe hosted an evening panel discussion on 'What can Member States expect from their cybersecurity communities?' at the Representation of the State of Hessen in Brussels. This followed a highly productive afternoon when several National Coordination Centre (NCC) representatives participated in a joint workshop.

Alongside the European Cybersecurity Competence Centre (ECCC), the NCCs are the other dimension in the emerging European cybersecurity landscape. Mirroring the ECCC's initiatives and policies in the Member States, each NCC has a key role to play in building strong relationships with the existing and emerging stakeholder communities, the experts and researchers in industry, SMEs and knowledge institutes who drive the work of securing European society's institutions, infrastructure and digital economy.

The event opened with welcomes from Martin Friedrich Reinhardt, Head of Unit, Affairs of the Hessian Ministry of the Interior and for Sports and Kai Rannenberg, Goethe University Frankfurt and CyberSec4Europe co-ordinator, who introduced the panellists.

- Cristian Iordan is project manager at the Belgian NCC, which is hosted by the Centre for Cybersecurity Belgium and has been active since February 2022.
- Christian Hartlage is an advisor at the Federal Office for Information Security (BSI) which since December 2021 has been the central contact point for the German NCC, a joint platform for co-operation among four federal ministries – Economic Affairs and Climate Action, Defence, the Interior and Community as well as Education and Research.
- Katarzyna Prusak-Górniak is vice chair of the Governing Board of the ECCC and cyber attaché at the Permanent Representation of the Republic of Poland to the EU
- Allard Kernkamp, from the Netherlands Enterprise Agency, explained how the Netherlands NCC was set up in March 2022.

With occasional questions from the audience, the panellists explored community expectations, agreeing that the task of the NCCs is to address what their communities want to do, and to find ways to enable them to be successful, sharing information, learning from each other and, in the process, establishing and maintaining mutual trust and value.

We also learnt that, while ENISA responds to cyber incidents, the ECCC is responsible for funding the Digital Europe programme with potential opportunities for joint funding and accessing other cybersecurity funds.

Moderator Kai Rannenberg concluded the meeting reflecting that we are at the beginning of a new dawn, and it is evident that there is the right spirit in place for success in the long term.

4.4
Raising SME awareness

We examined several approaches to supporting the huge, disparate group of SMEs achieve an acceptable level of cybersecurity awareness commensurate with their levels of resource and skills set to advance the European single digital market.

The competence, awareness and risk perception of users and small businesses are critical dimensions of cybersecurity, while the enhanced understanding of the potential severity of the impact arising from digital vulnerabilities, particularly in supply chains, significantly improves the societal posture against threats at a personal and professional level.

99% of companies in the EU are SMEs (small- to medium-sized enterprises), roughly 25 million businesses, of which 93% are micro-SMEs with under 10 employees. In the context of this enormous number of SMEs, a dominant feature of the European economy, we investigated the distinctive issues facing raising awareness of cybersecurity best practices with the goal of implementing adequate cybersecurity measures. Additionally, we analysed the landscape of the myriad cybersecurity awareness materials available, both commercially and free of cost.

We concluded by interviewing numerous organisations across different countries that provide support to SMEs and made a set of proposals to tackle the communication gap that still exists. As part of this overall exercise, we looked at the effectiveness of awareness programs as well as some of the challenges facing supply chains involving potentially vulnerable SMEs.

Sunil Chaudhary
Norwegian University
of Science and Technology
—
13 November 2020

SME cybersecurity awareness

The use of information and communication technologies across enterprises increases continuously, as it enables the development of new business models and the improvement of operational and commercial activities. Nevertheless, this practice introduces new vulnerabilities, which require the deployment of suitable countermeasures, to be treated in order to prevent their exploitation by various threat agents.

Larger organisations possess both the resources and often the maturity to establish the required mechanisms for continuous monitoring and enhancement of holistic cybersecurity programs. However, small and medium-sized enterprises (SMEs), more often than not, lack both the resources and the incentives to prioritise this practice. At the same time, they constitute a significant portion of the European economy, both numerically and in terms of revenue.

As the European digital value and digital supply chains increase in complexity and cross border/market dependencies, the impact and spillovers of each cybersecurity incident become more severe. Furthermore, prior studies have shown that numerous security breaches occur due to negligence or ignorance of the personnel within an organisation and that often attackers structure malicious actions by exploiting one or more human factor weaknesses. Maintaining a secure and resilient posture is a continuous process for every organisation, requiring a balanced focus on people, technologies and processes.

It is well known that as the operating environments become more complex, and the corresponding guidelines proliferate, it is getting increasingly difficult, especially for SMEs, to keep track, invest in and apply the required solutions. Although digitalisation is one of the main drivers for development, the return on investment for security, which it is even possible to model, is not directly evident for decision makers.

However, the cost of cyber incidents is clear to all: more than 60% of cyber attacks are aimed at SMEs, and 60% of those SMEs which have been victims of cyber attacks do not manage to recover and end up shutting down operations within six months.

The principal objective for each organisation should be to establish a cybersecurity culture that must be initiated and maintained at the strategic level and propagated downwards towards operations, within both the organisations themselves and the supply chains in which they participate. CyberSec4Europe's goal in this area is to advance the state of the art by developing novel security awareness conceptual models, monitoring and enhancement methods with international applicability.

Our focus is to analyse and identify efficient measures and methods for the continuous enhancement of societal security awareness, referring to private usage of digital technologies, human aspects of information security, professional practice and competence development.

Furthermore, we seek to investigate suitable measures to raise cybersecurity awareness across industry and society by establishing the value of new, integrated, secure and trust-aware services, with particular focus on SMEs, and the cybersecurity vulnerabilities that these SMEs may face and introduce into supply chains. Read more in our report *SME cybersecurity awareness program 1* (D9.6).

Sunil Chaudhary
Norwegian University
of Science and Technology

—

16 April 2021

Measuring the effectiveness of cybersecurity awareness programmes

Cybersecurity awareness intends to prepare the audience for cyber risks and threats so as to make cybersecurity best practices or cyber hygiene occur to them automatically while performing personal and professional tasks. This is a continuous and long-term process that requires regular reviews and evaluations to measure its effectiveness. The results also act as critical factors in indicating whether an awareness programme is relevant for the intended audience and optimised for a particular organisation. Based on this feedback, the awareness programme can be improved and updated.

The effectiveness of a cybersecurity awareness programme is dependent on features like its ability to comprehend evolving and emerging cyber threats, advancements in technology, and shifts in an organisation's business missions and priorities as well as the usability of awareness material and its delivery channels in terms of the relevance of topics and the quality of the content.

Factors widely used to measure the effectiveness of a cybersecurity awareness programme include assessing its reachability and touchability (ie, the ability to reach and impact an audience) as well as monitoring improvements in an audience's cybersecurity competencies, attitudes, and behaviour through its participation in awareness programmes.

To achieve this analysis, one or multiple qualitative and quantitative methods are used, such as conducting surveys, assessment tests and interviews of the participants, observing the participants' behaviours, and analysing system and log data.

The existing review and evaluation approaches are mostly limited to what factors to measure and how to measure them. Unfortunately, they often do not consider when to take a measurement (ie, before, during, or after the programme implementation) and for whom each factor is measured. For example, conducting assessment tests before and after the awareness programme can provide results that can be assumed to be due to the awareness programme; whereas conducting interviews at regular intervals helps to identify areas where people may need further support. Likewise, the meaning of effectiveness may vary according to the stakeholders involved. An audience may understand effectiveness in terms of how interesting and engaging an awareness programme is. Similarly, the cybersecurity awareness professional may perceive effectiveness in terms of reachability and touchability, as mentioned earlier.

Finally, the programme's sponsors may want to know what value the programme brings to the organisation to decide whether or not to further invest in the awareness programme. Therefore, the review and evaluation of cybersecurity awareness programmes should consider the needs of all the relevant stakeholders; obtaining results in their desired formats will assist in future decision-making and the ongoing sustainability of the programmes.

CyberSec4Europe's report, *Awareness effectiveness study* (D9.13), focuses on developing cybersecurity awareness review and evaluation metrics that address the limitations mentioned above and help to make the review and evaluation processes as inclusive, complete, and unbiased as possible. We believe that such metrics are necessary to effectively carry out continuous monitoring of and enhancements to cybersecurity awareness programmes. The report will be of value to anyone looking to design and evaluate a cybersecurity awareness programme.

David Goodman
Trust in Digital Life
—
21 May 2021

Developing SME resilience in Europe

On the evening of 5 May during its 2021 Spring General Meeting, CyberSec4Europe hosted an online panel discussion entitled, *Developing SME Cybersecurity Resilience in Europe*.

Following an introduction from Mark Weinmeister, Secretary of State for European Affairs of the State of Hessen and Kai Rannenberg, Goethe University Frankfurt and co-ordinator of CyberSec4Europe, moderator David Goodman from Trust in Digital Life introduced the panellists:

- Martin Übelhör, Head of Cybersecurity Industry and Innovation, DG CONNECT, European Commission
- Annika Linck, Senior EU Policy Manager, European DIGITAL SME Alliance
- Nicholas Ferguson, Trust-IT Services, Partner, CYBERWISER.eu; Project Co-ordinator, cyberwatching.eu
- José Francisco Ruiz, Atos Spain, Technical Co-ordinator, Cyber-GEIGER

The goal of the evening's discussion was to explore issues relating to developing SMEs' awareness of cybersecurity in order to improve resilience and responses to cyber attacks – an important aspect of the work of the new European Cybersecurity Competence Centre in Bucharest.

SMEs account for the majority of businesses worldwide and are important contributors to job creation, innovation, and global economic development. SMEs represent about 90% of businesses and more than 50% of employment worldwide, and similarly, in the European Union, 99% of enterprises are SMEs who provide two-thirds of private sector employment. In 2018, there were over 25 million SMEs in the European Union, employing 100 million people, of which 93% were micro-SMEs, defined as having 10 or fewer employees.

Given the size and limited resources of most SMEs, it's not surprising that SMEs are more vulnerable than larger enterprises to cyber attacks. However, without effective training and support, many SMEs are not sufficiently protected or able to recover from the impact of such attacks with, in many cases, dire consequences. All SMEs are busy building their businesses, what time or resource do they have to worry about cybersecurity?

Martin Übelhör introduced the topic with insights as to what the Commission plans are to help SMEs in terms of cybersecurity by quoting from an ENISA study from the end of 2020 on 250 SMEs in 25 Member States and went on to discuss the Commission's plans for SMEs.

Annika Linck noted that the European DIGITAL SME Alliance is a network of over 20,000 SMEs, comprising a variety of companies most of which, roughly 90%, are in the ICT sector. In 2019 it carried out a study looking at the hurdles inside organisations to the adoption of cybersecurity solutions. It was apparent that cybersecurity is perceived as a cost rather than something that brings immediate benefits.

Nick Ferguson was on the panel representing cyberwatching.eu and CYBERWISER.eu, both of which have developed strategies for SMEs and understands well how hard the challenge is in actually reaching SMEs. It is understandably very difficult to get SMEs interested in cybersecurity – sending an employee to get training on a topic which is seen as an extra is challenging.

José Francisco Ruiz participated as technical co-ordinator of the GEIGER project which evolved from an earlier three-year project, SMESEC. Both projects aimed at working with SMEs on cybersecurity: whereas SMESEC was oriented to technical aspects, GEIGER is focussed on both technical and awareness raising pillars. One without the other cannot be understood.

It is impossible to make an SME understand cybersecurity unless they understand why it is important. They see cybersecurity as something that consumes time, effort, people, resources, everything and it doesn't bring immediate benefits today. One very important aspect is to make SMEs understand how cybersecurity is beneficial for them.

It was clear that all the panellists were in agreement about the nature and vastness of the problem, how fragmented it is by language, digital maturity and wealth – added to which is the difficulty of reaching out particularly to micro-SMEs and getting them interested enough to see the benefits of a cybersecurity program. Working through intermediaries was touched upon several times and made a lot of sense as did the different roles at the supranational, national and regional levels. Without doubt there is a lot of work to be done. It is the responsibility of the cybersecurity community to create the momentum to get the right messages out to SMEs and also the general public which is equally important. It happens already in the offline world but as we get more immersed in the digital world, it is small businesses and citizens who need to be made aware of the dangers and the malevolent actors that exist.

Finally, we all look forward to meeting again, hopefully in person, when we can continue the discussion in an informal and convivial atmosphere. Both a full report and a recording of the evening panel discussion are available on the CyberSec4Europe website.

Selected CyberSec4Europe references:

- *SME cybersecurity awareness program 1 (D9.6)*
- *SME cybersecurity awareness program 2 (D9.11)*
- *Supply chain security recommendations 1 (D9.12)*
- *Awareness effectiveness study 1 (D9.13)*

Sunil Chaudhary
NTNU, Norway
—
13 June 2022

Multidisciplinary approach in cybersecurity awareness

Cybersecurity awareness (CSA) refers to being mindful of cybersecurity issues that affect one's personal and professional life. If properly conceived and implemented, this preventive measure can provide a reliable defence against cyber attacks and crimes. In reality, however, many CSA initiatives fail to yield the desired results.

One of the key reasons for CSA initiatives' failure is their limited grasp of awareness concepts. Awareness is commonly misunderstood as an act of sharing security information, traditionally on what to do and what not to do, with the target audience group. While providing information about security risks and threats with the target audience group is definitely necessary for building a conducive environment for change, it is unlikely that doing so alone will influence their security attitudes and behaviour.

In fact, getting people to act in a secure or recommended manner necessitates communicating the complex issues of cybersecurity in such a way that people understand the importance of information, then comprehend the information on how to respond appropriately, and finally develop a determination to act despite a variety of other demands of normal workflow. And such communication requires adopting and leveraging strategies and applications of multiple disciplines.

CyberSec4Europe's report *Awareness Effectiveness Study 2* (D9.18) implemented a multidisciplinary approach to elicit and analyse the relevant factors that can be used or required to address in order to enhance security attitudes and behaviour transformation. To accomplish that, this study explored research studies from different disciplines, namely,

- social psychology – eg, to understand the impact of cognitive biases, cultural biases and personal traits on security decision-making,
- behavioural economics – eg, to understand the impact of incentives on security decision-making,
- pedagogy – eg, to understand suitable learning materials, learning techniques, and effective evaluation for security purposes,
- usability and user experience – eg, to understand better usability and user experience to facilitate security decision making,
- framing theory – eg, to understand the influence of information presentation on security decision-making,
- communication theory – eg, to understand the communication phenomena necessary for effective delivery of security messages,
- the science of persuasion – eg, to understand persuasion mechanisms that can foster security learning and actions, and so on.

The findings of this study will be useful to CSA professionals, organisations, and individuals who want to design, develop, and implement CSA materials or programmes. The identified factors could assist them in designing appropriate awareness messages and conveying the messages effectively. Additionally, the information could be valuable for those who make requests for awareness designers, as well as anyone who analyses the efficiency of security measures already in place.

4.5
Exploitation, innovation and policy recommendations

CyberSec4Europe's legacy beyond the end of the project is demonstrated in the individual and joint exploitation and innovation assets and solutions, as well as a series of two-page policy briefs, incorporating recommendations to European institutions and others, derived from project explorations and investigations.

CyberSec4Europe's legacy beyond the end of the project can be seen in the results of the work carried out by all partners over the past four years.

We demonstrated this in two ways. In a series of reports, we highlighted the individual and joint exploitation and innovation plans, involving assets and solutions across the different project domains, ranging from, for example, maritime transport to the Flagship cyber range challenges. As CyberSec4Europe comprised diverse organisations – from software vendors, commercial businesses, universities, research institutes, SMEs, legal and consultancy firms to not-for-profit organisations – each type of partner evolved exploitation strategies in line with their own needs and opportunities.

This culminated in the presentation of the key exploitable assets and solutions at the project's final conference, Momentum!, held at the beginning of December 2022. This was also an opportunity to distribute a series of two-page policy briefs, incorporating recommendations to European institutions and others, derived from project explorations and investigations.

Evangelos Markatos
FORTH
—
5 October 2020

Recommending policies: how to make a difference

One of the roles of the emerging European Cybersecurity Competence Network which CyberSec4Europe is piloting is to provide effective policy recommendations to policy makers formulating policies that will shape the cybersecure future of Europe.

CyberSec4Europe partners provide policy recommendations as a result of attending workshops, conferences and diverse meetings under the auspices of organisations such as ECSO, ENISA, the European Data Protection Supervisor and others. Proactively, important elements of the work performed during the course of the project itself, particularly in the context of the roadmapping work, form the basis of what can shape proposals for the attention of EU policy makers:

- to support novel privacy-preserving technologies including data-sharing for Covid-19
- university curricula to provide more attention to certain cybersecurity topics including security-by-design and privacy-by-design
- to adopt integrated models for legal compliance and sanction avoidance
- to co-ordinate Member States on achieving cybersecurity sovereignty
- to continue to invest in novel solutions for cybersecurity threats
- to take leadership in the research and development of blockchain applications
- to consider secure 5G as a crucial enabler
- to adopt a common eIDAS-based trust framework for Member State digital identity trust schemes
- financial services institutions to adopt a privacy-preserving approach to sharing KYC data and IBAN information among banks and other financial institutions

Although each one of the above is worth exploring, we will focus on one.

Support privacy-preserving technologies including data-sharing for Covid-19

The recent pandemic uncovered a major problem: we need to find a way, directly or indirectly, to share location data in order to identify people who have come in contact with others infected with Covid-19. At the same time, such sharing of location data has to be carried out in a privacy-preserving way if we are not to set a precedent for the creation of a surveillance society, monitoring the movements and whereabouts of citizens at all times. The well-intentioned goal to stem the tide of the virus and protect a nation's health could end up creating the conditions for digital entrapment.

Hence, privacy-preserving contact tracing appears to be a contradiction, an impossible trade-off: having to know who an individual has had contact with without having to reveal the identities of who was in contact with whom. Data-sharing is an immensely powerful and now pervasive business process but with major societal impacts, not only during a time of emergency but in many everyday health, finance, educational and other scenarios.

Focus areas for support

Our recommendation is to proactively support the numerous European research centres working in this aspect of policy privacy-related identity management. To be more specific the areas to support are:

- Privacy-preserving data-sharing which could be used for other medical/health purposes, such as scientific processing, research, secondary processing, epidemiology etc.
- Privacy-by-design technological approaches. If privacy is not to become an afterthought, it should be included in the first design phase of solution or process creation.
- Privacy-enhancing technologies. Like it or not, when people go online they leave digital "crumbs" that can be used to follow them all over the Internet – and frequently they have no other choice. In order to communicate, we provide our IP address, to receive decent service from a web server, we accept cookies, and, to access an online service, we are subjected to device fingerprinting. Privacy-enhancing technologies can help users protect their IP address, protect their devices, and ultimately protect their identity from unwanted intrusion.

An ongoing process

The set of policy recommendations identified above are just the beginning of a process that will continue over the remaining months of the project – and beyond. All partners will be looking to extract the key ideas and principles from across the whole spectrum of activities in CyberSec4Europe and finding opportunities to present these ideas externally to help progress cybersecurity policymaking for years to come.

For more on CyberSec4Europe's initial set of policy recommendations, you are invited to read our report *Policy Recommendations* (D9.8)

We can be heroes

David Goodman
Trust in Digital Life
—
19 March 2021

The primary dictionary definition of the expression, 'to exploit', the one that most people are familiar with, is to take advantage of (a person, situation etc) for one's own ends – thus often used in the context of exploiting workers, colonial possessions etc.

In other words, activities that most of us would not wish to be knowingly associated with. In sharp contrast, 'an exploit' is defined as a heroic deed or feat as well as a brilliant or daring achievement, which is much more promising as aspirations go. Somewhere between the two, we have a further, final, *a propos* definition which is to make the best use of.

It is in this sense that all 43 CyberSec4Europe partners are requested to identify how they intend to exploit, both individually and collectively, the results of their work or the assets developed or enhanced during the course of the project.

This is a common requirement of all EU-funded projects, as it demonstrates to the Commission and other policy makers – as well as European taxpayers – the potential return on investment from the project in terms of the EU's strategic initiatives, which in the case of CyberSec4Europe is to strengthen the safety and security of European society.

Having said that, the series of three exploitation strategy reports, the first of which was published recently, is different from those of other H2020 projects, as CyberSec4Europe is expected to test and validate the procedures and operational setup for the better exploitation of cybersecurity research, which will later serve the Cybersecurity Competence Network and Centre. From an exploitation perspective, this presents a significant challenge in that CyberSec4Europe is a large-scale pilot exercise consisting of a wide-range of mini-projects that are held together through collaboration and a common cause and are equally diverse in terms of results.

The other challenge is that CyberSec4Europe comprises organisations, large and small from software vendors to corporate businesses, universities and research institutes, SMEs, legal and consultancy firms, and not for profit organisations, all of whom are expected to develop their own clear ideas on how to exploit their achievements and to contribute to their own exploitation goals, enabling implementation of the project results through various disciplines and stakeholder types.

To assist with achieving a degree of uniformity in their responses given this diversity, partners are offered a pre-defined set of headings to describe their plans and to maintain independently throughout the course of the project. The outcomes not surprisingly reflect the activities of the different types of organisations in the project, although it was also apparent that many organisations have not yet fully considered how they may leverage their participation in CyberSec4Europe.

It is realistic to expect many if not all partners to be more focused at the time of the next set of reports.

The joint collaboration was split between the five of the project segments:

- Governance, design and pilot
- From research and innovation to industry
- Education, training and tools
- Standardisation
- Communication and community building

In each of these sectors, we were able to point to outstanding achievements involving groups of partners working together. We also identified the sustainability strategy of the CyberSec4Europe framework in the context of building a network of competence centres in Europe beyond the completion of the project, in collaboration with the other three pilots and ECSO, the European Commission and the Competence Centre in Bucharest. For this we asserted that each of the pilot projects comprise three distinct sets of activities:

- Governance
- Technical activities
- Communications

Consequently, we split the project's sustainability strategy along these lines into three types of output, each of which are instruments used during the course of the project in order to achieve the sustainability of the project beyond its completion:

- Strategic input – management and governance design contributions
- Technical collaboration – participation in four focus groups
- Communications and networking – participation in a joint communication group as well as hosting two concertation events
- We also referenced innovation in the project, whether they be innovative products, solutions or services being developed during the course of the project, either from pre-existing assets introduced by consortium partners or developed from scratch. It was to be expected and was evidenced that the demonstration use cases were the most likely – but not the only – candidates for generating innovation assets that could be successfully exploited, commercially or otherwise, after the end of the project.

At this stage, there are no patents pending as a result of CyberSec4Europe activities, although it is clear that discussions are ongoing between several partners about commercialisation rights on assets developed during the project. We would expect to report more in this regard in future iterations of this report.

In conclusion, we acknowledge that this first report is going to be a living document over the rest of the project and to provide indicators of proposed next steps over the coming twelve months.

In a later report in this series, we will ask all partners to compare their organisation's initial expectations of how they would eventually benefit from participation in CyberSec4Europe with how their very advanced exploitation plans have (or have not) met those expectations. The insights gained from this exercise could inform how future collaborative activities are constructed.

Overall, the reflections on what we have achieved to date and what lies ahead demonstrate that, with confidence, we can be heroes, if not for ever and ever, certainly for more than one day.

Evangelos Markatos
FORTH
—
30 March 2022

The vital importance of blue sky research in cybersecurity

CyberSec4Europe recently published a new set of policy recommendations in the area of research for cybersecurity.

One of the most important recommendations in this report focuses on the issue of funding in Europe. The authors of the recommendations argue that although Europe invests significant amounts in cybersecurity research, most of the research funds are for short-term medium/high-TRL (technology readiness level) projects that allow practically no time to explore new and promising technologies. Without the proper environment to invent fundamentally new technologies, and to nurture them into fruition, Europe will be forced to import its cybersecurity technologies from overseas. Such a practice not only increases Europe's reliance on imported technology, but also significantly undermines its long-term sovereignty in the digital domain.

Indeed, it seems that fundamental ideas which have the opportunity to significantly change the world, usually need a lot of time to develop and reach a mature stage. In addition to time, such ideas also need space: a nurturing environment in which to grow, flourish, and find their place in the sun. Such an environment should be willing to take high risks in order to have a chance to reap high gains at the end.

Scientific evidence clearly supports the fact that fundamental ideas and technologies need a lot of time between their invention and the time they take to achieve a noticeable market share. For example, the mobile phone took 29 years to reach 20% market penetration; LED lights took 24 years; the Internet took more than 25 years, the ATM cards took 25 years, etc.

These are inventions that almost everyone in the developed world uses every day and possibly cannot properly function without. And, still, it took those amazing inventions almost three decades to get out of their nurturing environment and achieve a decent market share. It seems that the old proverb is true: "great things just take time". Time, indeed, is what most new cybersecurity ideas are deprived of in the current European setting.

Over the past few years, research funding in the area of cybersecurity follows a completely different approach with respect to time: it favours short-term projects with immediate market application, medium/high TRLs, and rapid market exploitation. This approach effectively deprives cybersecurity ideas from a nurturing environment: their environment is dwindling, the expectations are high and the ideas just cannot reach maturity.

To help researchers make fundamental long-term contributions in the area of cybersecurity, the authors make two clear research policy recommendations:

- Create an "EIC PathFinder" for cybersecurity: It is possible to form a collaboration between EIC Pathfinder or a similar research line and the research community to support blue sky research in the future challenges of cybersecurity.
- Restructure funding: A good architecture of European funding may consist of blue sky individual projects under the ERC (European Research Council), plus a large number of collaborative EIC Pathfinder projects in strategic areas of cybersecurity. These could also network the results stemming from the ERC, complemented by DARPA-like technological projects that would bring the most promising ideas that have most impact potential closer to the market. Essentially, by refocusing existing EU funding schemes, like the EIC Pathfinder and the ERC, we can accelerate the production of high-quality research in cybersecurity that can address Europe's cybersecurity needs for the future. For more information see our report, *Policy Recommendations 2* (D9.20).

Cyber
Security
for Europe

cybersec4europe.eu

CyberSec4Europe is funded by the European Union
under the H2020 Programme Grant Agreement No. 830929

ABI Lab
Archimède Solutions Sàrl
Atos Spain S.A.
Austrian Institute of Technology GmbH (AIT)
BBVA Group
Computer Technology Institute and Press “Diophantus” (CTI)
Comune di Genova
CONCEPTIVITY Sàrl
Consiglio Nazionale delle Ricerche (CNR)
Cybernetica AS
Dawex Systems
Engineering Ingegneria Informatica S.p.A
Foundation for Research and Technology – Hellas (FORTH)
Goethe University Frankfurt
Informatique Banques Populaires
International Cyber Investigation Training Academy (ICITA)
Intesa Sanpaolo S.p.A.
JAMK University of Applied Sciences
Karlstad University
KU Leuven
Masaryk University
NEC Europe Laboratories GmbH
Norwegian University of Science and Technology (NTNU)
Open & Agile Smart Cities vzw (OASC)
Politecnico di Torino (POLITO)
Siemens AG
SINTEF AS
Technical University Delft
Technical University of Denmark (DTU)
Timelex
Trust in Digital Life Association (TDL)
University College Dublin
University of Cyprus
University of Luxembourg
University of Malaga
University of Maribor
University of Murcia
University of Piraeus Research Center
University of Porto
University of Trento
University Toulouse III – IRIT
VaF, s.r.o.
VTT Technical Research Centre of Finland Ltd

CyberSec4Europe is funded by the European Union
under the H2020 Programme Grant Agreement No. 830929

cybersec4europe.eu