Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D9.24

CyberSec4Europe summer schools 3

Document Identification	
Due date	31/10/2022
Submission date	31/10/2022
Revision	1.0

Related WP	WP9	Dissemination Level	Public
Lead Participant	DTU	Lead Author	Alberto Lluch Lafuente
Contributing Beneficiaries	DTU, AIT, UMA, UMU, KUL	Related Deliverables	D9.7, D9.16

Abstract: This document presents the deliverable “D9.24 CyberSec4Europe summer schools 3”. It describes the contributions made by the CyberSec4Europe project to summer schools in the third period of the project.

Executive Summary

One main goal of Task 9.3 "Spreading of excellence" of the CyberSec4Europe project is the dissemination of project results through several channels. This deliverable presents one of the key sets of activities carried out to contribute to achieving this goal, in particular the dissemination among the new generations of researchers and professionals through summer and winter schools[1]. This deliverable provides a detailed overview of the schools that CyberSec4Europe partners used to disseminate information about the project and its results in the third period of the project.

Goals. One of the main overall goals of CyberSec4Europe is to disseminate the latest research from the project and to provide training based on it. Project activities aimed at achieving such a goal are being conducted in several areas and, especially, in WP9. Indeed, WP9 has, among others, the following objectives:

> [Obj. 9.1] Maximise dissemination of the project results to a wide audience of researchers and technologists within the relevant cybersecurity communities and initiatives. Run dissemination as a necessary step before and during exploitation
>
> [Obj. 9.2] Promote the project achievements and results taking strategic and targeted measures for communicating the education and training cybersecurity framework and the service infrastructure to all potential users, including the media.
>
> [Obj. 9.3] Spread excellence and guidance on best practices in next generation industrial and civilian cybersecurity technologies, applications and services

The project has several target groups for such dissemination and training efforts that include professionals, educators, students and researchers, both in the public and private sectors. A key target group are young professionals and researchers from the EU and beyond, who will form the basis of the new generation of experts in cybersecurity. Reaching them is fundamental to ensuring the widespread and long-term impact of the results of the project beyond the project lifetime. Indeed, summer and winter schools often give rise to new international networks of professionals bound by a unique learning and social experience. Moreover, schools are an excellent vehicle to connect experienced researchers and professionals with the younger generation from all across the world, thereby ensuring knowledge transfer among the generations, worldwide. Overall, schools are a key instrument to meeting the three objectives of WP9 mentioned above, as well as the general goal of spreading excellence.

The schools. To ensure a successful dissemination of CyberSec4Europe's results, the partners of the project decided to aim at getting actively involved in both well-established, reputed schools as well as in newly created ones. Such efforts resulted in CyberSec4Europe partners providing significant contributions to several schools, ranging from active involvement in the organisation of the schools to teaching of individual lectures or modules. Preliminary efforts in this direction were presented in D9.7[2] and D9.16[3]. The present deliverable reports on new school activities that took place in the third period of the project.

[1] Following academic conventions, the term "summer school" sometimes includes also "winter schools".
[2] CyberSec4Europe summer schools 1, available at https://cybersec4europe.eu/wp-content/uploads/2020/08/D9.7-CyberSec4Europe-summer-schools-1.v1.0-Submitted.pdf
[3] CyberSec4Europe summer schools 2, available at https://cybersec4europe.eu/wp-content/uploads/2022/02/D9.16-CyberSec4Europe-summer-schools-2-v1.0_submitted.pdf

Details about how CyberSec4Europe partners contributed to the schools, and about which specific CyberSec4Europe results were disseminated, are described in detail in the deliverable. In particular, each school is described in its own dedicated chapter where we provide the following information:

- **Name of the school:** The full name of the school.
- **Website (URL):** The URL of the school.
- **Dates:** The dates when the school took place.
- **Location:** The location where the school took place.
- **Organiser:** Who was the main organiser of the school.
- **Main audience category:** Who the audience of the school primarily was.
- **Description:** A short description of the school.
- **Speakers, lecturers and topics:** Who the speakers and lecturers were and what topics they covered.
- **Teaching material:** Links to teaching material.
- **Picture:** Photograph taken at the event.
- **Number of attendees:** How many people attended the school.
- **CyberSec4Europe involvement:** How CyberSec4Europe was involved.
- **Conclusion:** The main success and outcome of contributing to the school.

Summary. Overall, this set of schools, together with the set of schools reported in D9.7 and D9.16, constitutes a significant step towards the achievements of the above-mentioned goals of the project. In total, CyberSec4Europe reached out to, through these schools, more than 700 attendees in the scientific community, a main target group. The schools reported here were hosted at several locations in Europe (Italy, Luxemburg, France, Belgium, Slovenia, Greece, Switzerland, Czech Republic, Germany) and beyond (Brazil and Madagascar). Some of the schools were organised in collaboration with the SPARTA and CONCORDIA pilots. Lastly, we think it is also worth mentioning that, in addition to spreading CyberSec4Europe results, some of the schools resulted in outcomes that are currently being integrated with the activities and results of the project.

Document information

Contributors

Name	Partner
Alberto Lluch Lafuente	DTU
Andreas Viktor Hess	DTU
Stephan Krenn	AIT
Javier López	UMA
Manuela Kos	AIT
Jesús García Rodríguez	UMU
Davy Preuveneers	KUL
Wouter Joosen	KUL
Carmen Fernández Gago	UMA

Reviewers

Name	Partner
Christine Jamieson	Trust In Digital Life Association
Antonio Lioy	Politecnico di Torino

History

Version	Date	Authors	Comment
0.1	2022-09-16	The Authors	1st Draft
0.2	2022-10-05	The Authors	2nd Draft
1.0	2022-10-31	Ahad Niknia	Final check, preparation and submission

Table of Contents

List of Figures

List of Tables

1 FOSAD 2022

1.1 Name of the school

21st International School on Foundations on Security Analysis and Design (FOSAD 2022)

1.2 Website (URL)

https://sites.google.com/uniurb.it/fosad/home/fosad-20https://sites.google.com/uniurb.it/fosad/home/fosad-2022

1.3 Dates

29 August 2022 - 2 September 2022.

1.4 Location

The school was held as a hybrid event with physical location at Bertinoro (Italy).

1.5 Organiser

University Residential Centre of Bertinoro.

1.6 Main audience category

Scientific community and early-stage researchers, mainly PhD students and MSc students.

1.7 Description

Security in computer systems and networks emerged as one of the most challenging research areas. The International School on Foundations of Security Analysis and Design (FOSAD) has been one of the foremost events established with the goal of disseminating knowledge in this critical area. The main aim of the FOSAD school is to offer a good spectrum of current research in the foundations of security - ranging from programming languages to the analysis of protocols, from cryptographic algorithms to access control policies and trust management - that can be of help to graduate students and young researchers from academia or industry who intend to specialise in the field.

FOSAD is held annually at the University Residential Centre of Bertinoro. From the first event in 2000 until its 21st edition in 2022, FOSAD has attracted all these years more than 1000 participants and almost 200 lecturers from all over the world. The school programme alternates monographic courses given by well-known experts in the security community. Moreover, FOSAD encourages presentations by those participants who intend to take advantage of the audience to discuss their current research topic. Many of the young speakers of the FOSAD open sessions are now appreciated researchers and professors.

For the 2022 edition, the school was supported by two of the four EU Cybersecurity Competence Networks pilots, **CyberSec4Europe** and **SPARTA**. Both of them emphasised the crucial role of education for cybersecurity, proposing new educational and training programmes and new methods of teaching.

1.8 Speakers, lecturers and topics

The full program of this year edition is available at https://sites.google.com/uniurb.it/fosad/home/fosad-2022/program?authuser=0 CyberSec4Europe contributed to the organisation of FOSAD 2022 as UMA and CNR are part of the scientific committee. Also, CyberSec4Europe supports the school. In addition, CyberSec4Europe contributed with the following talks in the PhD forum:

Lecturer (Partner)	Topic
Laouen Fernet (DTU)	How to verify privacy automatically
Simone Bussa (POLITO)	Formal verification for Cyber-Physical Systems
SystemsDaniele Bringhenti (POLITO)	Automating security configuration in virtualized computer networks

Table 1: Cybersec4Europe talks at the PhD forum of FOSAD 2022.

1.9 Teaching material

Teaching materials for some of the lectures are available at

https://sites.google.com/uniurb.it/fosad/home/fosad-2022/program

1.10 Picture

Figure 1: FOSAD 2022 group picture.

1.11 Number of attendees

The summer school had 32 attendees.

1.12 CyberSec4Europe involvement

UMA and CNR were involved in the summer school. Javier Lopez (UMA) is a member of the Scientific Committee as well as some members of CNR. This summer school contributed to successfully achieving some of the objectives of WP9. WP9 is devoted to dissemination and outreach, therefore all activities that are carried out in order to reach certain audiences (young researchers in this case) are related to this WP – in particular tasks T9.2 and T9.3 which are devoted to outreach in general and summer schools in particular.

1.13 Conclusion

CyberSec4Europe keeps a continual presence in this school by being part of the organising committee, supporting it and by the attendance of PhD students of CyberSec4Europe partners.

2 IFIP Summer School on Privacy and Identity Management 2021 and 2022

2.1 Name of the school

IFIP Summer School on Privacy and Identity Management

2.2 Website (URL)

- General links:
  - https://ifip-summerschool.org/
  - https://ifip-summerschool.github.io/
- The 2021 edition can directly be reached under:
  - https://ifip-summerschool2021.uni.lu/
- A permanent link for 2022 is not available, however, the website will be archived and maintained as a subsite of the general webpage.

2.3 Dates

IFIP Summer School 2021: 16-20 August 2021
IFIP Summer School 2022: 30 August-2 September 2022

2.4 Location

2.4.1 IFIP Summer School 2021

The school was planned to be held in Esch-sur-Alzette (LU), but was then held as a fully virtual event due to the ongoing spread of Covid-19, and the associated uncertainties.

2.4.2 IFIP Summer School 2022

Similarly to the year before, the 2022 edition of the summer school was held as a virtual event due to the uncertainties due to the pandemic. It was originally planned to be held in Brunswick, Germany.

2.5 Organiser

The conference series is held in cooperation with the International Federation for Information Processing (IFIP), an international, non-governmental, and non-profit organisation for researchers and professionals working in the field of computing to conduct research, develop standards and promote information sharing.

In particular, the conference series is a joint effort among the following IFIP Working Groups:

- WG 9.2: Social Accountability and Computing,
- WG 9.6/11.7: Information Technology Misuse and the Law,
- WG 11.6: Identity Management, and
- SIG 9.2.2: Special Interest Group on Framework on Ethics of Computing.

2.5.1 IFIP Summer School 2021

The conference General Chair was:

- Stefan Schiffner (University of Luxembourg),

while the PC Co-Chairs were:

- Ina Schiering (Ostfalia University of Applied Sciences),
- Michael Friedewald (Fraunhofer ISI), and
- Stephan Krenn (AIT Austrian Institute of Technology).

2.5.2 IFIP Summer School 2022

In 2022, the conference' General Chairs were:

- Ina Schiering and
- Andreas Weich (Leibniz Institute for Educational Media | Georg Eckert Institute),

while the PC Co-Chairs were:

- Felix Bieker (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein),
- Joachim Meyer (Tel Aviv University), and
- Sebastian Pape (Goethe University Frankfurt).

2.6 Main audience category

The target audience of the IFIP Summer School series is twofold.

Firstly, the summer school is aimed at early-stage researchers. It offers them a platform to present research goals (including, potentially, work in progress), receive feedback from an experienced program committee, discuss ideas and build an interdisciplinary network in the field of privacy and identity management. Furthermore, young researchers without their own contribution are also welcome at the event.

Secondly, the program is complemented by keynote lectures and workshops organised by experienced senior researchers, thereby complementing the early-stage result, and contributing to a lively exchange of ideas.

2.7 Description

Both, the 16th and 17th International IFIP Summer School on Privacy and Identity Management had to be held as a virtual event due to the COVID-19 pandemic.

As in previous years, the IFIP Summer Schools took a holistic approach to society and technology, and supported interdisciplinary exchange through keynote and plenary lectures, tutorials, workshops and research paper presentations. In particular, it aimed to bring together early-stage as well as senior researchers with technical, legal, regulatory, socio-economic, social or societal, political, ethical, anthropological, philosophical or psychological backgrounds. This interdisciplinary character of the work is fundamental to the school.

2.7.1 IFIP Summer School 2021

In 2021, the summer school was held in cooperation with three of the pilot projects CyberSec4Europe, SPARTA[4] and CONCORDIA[5]. Furthermore, the school was supported by the Forum Privatheit[6] and the EnCaViBS project[7].

2.7.2 IFIP Summer School 2022

In 2022, the summer school was supported by CyberSec4Europe, the Forum Privatheit, and the Leibniz ScienceCampus – Postdigital Participation – Braunschweig[8].

[4] https://www.sparta.eu/
[5] https://www.concordia-h2020.eu/
[6] https://www.forum-privatheit.de/
[7] https://encavibs.uni.lu/
[8] https://www.postdigitalparticipation.org/en/

2.8 Speakers, lecturers and topics

2.8.1 IFIP Summer School 2021

The full program is available at https://ifip-summerschool2021.uni.lu/programme/. CyberSec4Europe contributed with a workshop which was held in close collaboration with the H2020 OLYMPUS project[9], as well as a keynote speech:

Lecturer (Partner)	Topic
Jorge Bernal Bernabe (UMU), Jesus Garcia (UMU), Stephan Krenn (AIT), Vasia Liagkou (CTI), Antonio Skarmeta (UMU) and Rafael Torres (UMU)	Privacy-Preserving Identity Management
Sebastian Pape (GUF)	Challenges for Designing Serious Games on Security and Privacy Awareness

Table 2: CyberSec4Europe lectures at IFIP Summer School on Privacy and Identity Management 2021.

2.8.2 IFIP Summer School 2022

The full program can be found on the conference's website. In 2022, CyberSec4Europe contributed with a workshop:

Lecturer (Partner)	Topic
Jesús García-Rodríguez (UMU), David Goodman (TDL) and Stephan Krenn (AIT)	Privacy-Preserving Industry Applications - From Research to Industry

Table 3: CyberSec4Europe lectures at IFIP Summer School on Privacy and Identity Management 2022.

2.9 Teaching material

2.9.1 IFIP Summer School 2021

The post-event proceedings, including the student contributions, summaries of workshops and tutorials, have been published by Springer, and are available at https://link.springer.com/book/10.1007/978-3-030-99100-5 .

Note that gold open access to all papers in this volume has been granted for a limited time period after the publication of the proceedings.

The contribution of Cybersec4Europe is available via green open access at https://zenodo.org/record/7095901.

2.9.2 IFIP Summer School 2022

At the time of writing this deliverable, the post-proceedings of the summer school were still under preparation, and are expected to appear in spring 2023. The possibility for a workshop summary is currently being analysed by the partners.

[9] https://olympus-project.eu/

2.10 Pictures

Figure 2: Audience at the 2021 workshop organised by CyberSec4Europe and OLYMPUS

Figure 3: Impressions from the 2022 workshop on "Research to Industry"

2.11 Number of attendees

In both years, about 50 registrations were received by the local organisers, and sessions were typically attended by 20-30 participants.

2.12 CyberSec4Europe involvement

The IFIP Summer School series has a long tradition and strong links with several CyberSec4Europe participants. For instance, Simone Fischer-Hübner (KAU), Kai Rannenberg (GUF), and Stephan Krenn (AIT) are permanent members of the school's steering committee. Also, consortium members frequently serve as General or Program Chairs (2021: Stephan Krenn (AIT), 2022: Sebastian Pape (GUF)), or as members of the program committee.

From a work plan point of view, the summer school directly contributes to the objectives of WP9 by raising awareness of cybersecurity, bringing together experts from different domains, and supporting CyberSec4Europe beyond the consortium, thereby directly contributing to T9.3. Given the collaboration with SPARTA and CONCORDIA during CyberSec4Europe, and the active advertisement in, and

collaboration with, other H2020 projects such as KRAKEN or OLYMPUS, the summer school also contributes to the clustering activities envisioned in T10.1.

Given the main ambition of the summer school, there is also a strong relation to the topics covered by the research activities in WP3 and demonstrators in WP5. In particular, the overall ambition of the summer school on privacy and identity management is directly related to the ambition of T3.2 and T5.3.

2.12.1 IFIP Summer School 2021

More specifically, the IFIP Summer School on Privacy and Identity Management 2021 is linked to various tasks of CyberSec4Europe, such as:

- T3.2, demonstrated, e.g., by the session on "IoT and smart things" or the workshop co-organised by CyberSec4Europe,
- T3.6, demonstrated, e.g., by the sessions on "Informational self-determination" and "Knowledge imbalances", or
- T5.3, demonstrated by the workshop co-organised by CyberSec4Europe

2.12.2 IFIP Summer School 2022

For 2022, the link is, among others, given through:

- T3.4, demonstrated, e.g., by the session on "Privacy and Machine Learning",
- T3.6, demonstrated, e.g., by the session on "Privacy and User Perception",
- T3.7, demonstrated, e.g., by the session on "Data Protection Regulation", or
- T5.1, T5.3, and T5.7, demonstrated by the joint workshop on "Privacy-Preserving Industry Applications - From Research to Industry".

2.13 Conclusion

The IFIP Summer School on Privacy and Identity Management is directly related to CyberSec4Europe's overall ambitions in several ways. Firstly, the summer school aims to bring together researchers from different fields, backgrounds and seniority levels, thereby directly contributing to the objectives of strengthening Europe's cybersecurity capacities (Policy Objective 2) and establishing synergies between experts from different communities (Innovation Objective 2). Secondly, the contents of the summer school are directly linked to the project's vertical demonstrators, specifically T5.3 (privacy-preserving identity management), but also to those dedicated, for example, to open banking (T5.1) or smart cities (T5.7), which have very strong privacy requirements. Thirdly and finally, the school was also related to research activities from WP3, for example, regarding privacy-preserving technologies or blockchains (T3.2), or usable security (T3.6).

3 Future IoT Ph.D. School 2021

3.1 Name of the school

4th Future-IoT Ph.D. School 2021 – IoT Meets Cyber and Security

3.2 Website (URL)

https://school.future-iot.org/summerschool21/

3.3 Dates

29 November –3 December, 2021

3.4 Location

The school was held as a hybrid event with physical location at IRISA Laboratory (Campus Beaulieu), 263 Av. Général Leclerc, 35000 Rennes.

3.5 Organiser

The series is organised by IMT Atlantique and the Technical University of Munich as a flagship event of the German-French Academy for the Industry of the Future. The French-German series is kindly supported by the Deutsch-Französische Hochschule / Université Franco-Allemande.

3.6 Main audience category

Future-IoT.org connects academia and industry. Therefore, the series is in collaboration with leading industry partners from France and Germany including Airbus, ArianeGroup, Atos, AWS, elm.leblanc, Siemens, and several other industrial partners..

3.7 Description

The Internet of Things (IoT) connects a plethora of devices. It allows programmers to interact with the physical environment. This brings many fascinating challenges and opportunities but also risks.

The Future IoT Ph.D. School 2021focused on the fascinating world of the Industrial Internet of Things, the IoT that makes factories run. Students learned about many different aspects from device manufacturing over communication protocol and semantics to application management.

The 2021 edition had the title “IoT meets Cyber and Security”. Software drives the critical infrastructures around us like water or energy supply, communication, transportation, banking, production, or healthcare. The focus of the Ph.D. school was on aspects of the software cyberspace, including cybersecurity.

3.8 Speakers, lecturers and topics

The full program is available at https://future-iot.org/category/summerschool/2021-iot-meets-cyber/ . CyberSec4Europe contributed with the following keynote talk:

Lecturer (Partner)	Topic
Prabhakaran Kasinathan (SIE)	Using Blockchain technology for Cybersecurity – “Can Blockchain help securing distributed IoT workflows?”

Table 4: CyberSec4Europe keynote at 4th Future IoT School, Rennes, France

3.9 Teaching material

Video recording of the live keynote talk is available at https://future-iot.org/2022/01/07/fiot-rec-prabhakaran-kasinathan-siemens-keynote-using-blockchain-technology-for-cybersecurity/

3.10 Picture

Figure 4: 4th Future IoT Ph.D. School – Picture taken from the URL: https://future-iot.org/2022/04/09/fiot-pic-4th-future-iot-photo-highlights-of-day-4/

3.11 Number of attendees

- 40 students from all over the world connecting to each other and working on real challenges
- 60+ online participants
- Live streaming over YouTube and LinkedIn

3.12 CyberSec4Europe involvement

Prabhakaran Kasinathan (SIE) was involved from CyberSec4Europe - WP5 and delivered a keynote.

3.13 Conclusion

The 4th edition of Future IoT Ph.D. school 2021 focused on different aspects of software cyberspace – the algorithms that move the things around us - including cybersecurity. The keynote addressed the importance of one of the emerging technologies “Blockchain” and its role in cybersecurity. Thus, the results of CyberSec4Europe have been disseminated to the next generation of cybersecurity experts in Europe.

4 NeCS – PhD Winter School 2022

4.1 Name of the school

NeCS PhD Winter School 2022

4.2 Website (URL)

https://necs-winterschool.disi.unitn.it/

4.3 Dates

17 - 21 January 2022

4.4 Location

Hotel Montana, Vason – Trento (Italy)

4.5 Organiser

University of Trento (UNITN)

4.6 Main audience category

The target audience of the NECS PhD Winter School is young researchers (mainly PhD students) and the wider scientific community.

4.7 Description

The European Network for Cybersecurity (NeCS) PhD School was launched as part of the NeCS Marie Curie training network, in response to the increasing need for highly qualified experts in cybersecurity. The School addresses the issues of training and development of talented junior researchers as indicated in the European Cybersecurity strategy and highlighted in the EC's Digital Agenda.

For the 2022 edition, the School is supported by the four most important EU initiatives in this area: the Cybersecurity Competence Networks. They have been launched in 2019, within the H2020 framework, and include **CONCORDIA**, **CyberSec4Europe**, **ECHO** and **SPARTA**. All of them put emphasis on the crucial role of education for cybersecurity, proposing new educational and training programmes and new methods of teaching.

4.8 Speakers, lecturers and topics

The full program is available at https://necs-winterschool.disi.unitn.it/program/. CyberSec4Europe contributed with the following talk:

Lecturer (Partner)	Topic
Kai Rannenberg (GUF)	An overview of the Pilots project: CyberSec4Europe

Table 5: CyberSec4Europe lectures at NECS PhD Winter School 2022.

4.9 Teaching material

The lectures materials are available here: https://necs-winterschool.disi.unitn.it/lectures-material/

4.10 Picture

Figure 5: NECS PhD Winter School 2022 group picture.

4.11 Number of attendees

The Winter School had a total of 26 participants.

4.12 CyberSec4Europe involvement

CyberSec4Europe's involvement in the Winter School was as follows:

- UNITN was the organiser of the school.
- UMA was part of the steering committee.
- GUF presented CyberSec4Europe.

Some project partners such as CNR, University of Luxembourg and NEC Labs Europe were among the lecturers. The Winter School successfully contributed to achieving some of the objectives of WP9, particularly tasks T9.2 and T9.3, which are devoted to outreach and summer schools.

4.13 Conclusion

By being part of the organising committee, we could include in the program of this school topics eliciting cybersecurity and data governance. Also, Kai Rannenberg (GUF) presented the project to the participants of the Winter School.

5 Security and Privacy in the (golden) Age of AI 2022

5.1 Name of the school

Summer School on Security and Privacy in the (golden) Age of AI

5.2 Website (URL)

https://cybersecurity-research.be/summer-school-on-ai-security

5.3 Dates

5 September - 8 September 2022.

5.4 Location

The school was held at Campus Arenberg III of KU Leuven in Heverlee, Belgium.

5.5 Organiser

The organiser of this summer school is KU Leuven, with Wouter Joosen (KUL) and Davy Preuveneers (KUL) acting as the organising co-chairs.

5.6 Main audience category

Scientific community and early-stage researchers, mainly PhD students and MSc students.

5.7 Description

Any computer scientist, software engineer or information technology specialist will become a user and practitioner of artificial intelligence (AI) technology. Quite a number of the longstanding promises of AI, are nowadays being harvested in multiple application domains. This is not different for the broad area of Security & Privacy, obviously of critical importance in a world that has to be, more than ever, concerned about cybersecurity. Even though great progress has been achieved, much more is required. This obviously is an exciting setting for PhD candidates who target advanced research goals in Security & Privacy and in Machine Learning.

In short, there is a strong and exciting interplay between Security & Privacy and AI. On the one hand, specific S&P challenges, ranging from various types of anomaly detection (e.g. network intrusion, malware, data exfiltration attacks), spam and social engineering detection, to biometric authentication and user behaviour analytics, will benefit from novel research in AI, Machine Learning (ML) and Deep Learning (DL). On the other hand, ML solutions encounter challenges by adversaries: ML applications need strengthening for real world (malicious) operating environments. Last but not least, adversaries are exploiting the latest advances in ML and DL themselves to tweak their attacks (e.g. phishing campaigns, misinformation with deep fakes) and increase the likelihood that users become a victim of spoofing, fraud or identity theft.

We have invited and gathered a group of experts that will teach, reflect and challenge us all, by addressing major challenges in this versatile and rapidly evolving domain.

5.8 Speakers, lecturers and topics

The full program is available at https://cybersecurity-research.be/summer-school-program-ai

Lecturer (Partner)	Topic
Jesse Davis (KU Leuven)	Learning, Verifying, and Robustifying Additive Tree Ensembles

Michel Van Eeten (TU Delft)	Real World Security Data: Meaning, Acquisition & Impact
Fabio Rolli (University of Genova, University of Cagliari)	Adversarial Machine Learning: Fundamental Concepts and Common Misconceptions
Pavel Laskov (University of Liechtenstein)	Adversarial Examples in 5G Networks
Carlos Gañan (TU Delft)	Beyond ML association models: causal inference for cybersecurity in practice
Konrad Rieck (TU Braunschweig)	From Fun to Serious: Attacking Code Stylometry and Lessons Learned for Machine Learning in Computer Security
Lorenzo Cavallaro (University College London)	Trustworthy Machine Learning… for Systems Security
Emmanuela Orsini (KU Leuven)	Data Protection Frontiers: MPC, FHE and more
Yizheng Chen (University of California, Berkeley)	Learning Security Classifiers with Verified Global Robustness Properties

Table 6: Overview of all lectures at the "Security and Privacy in the (golden) Age of AI" summer school.

5.9 Teaching material

Teaching materials for the above lectures are made available to the attendees only.

5.10 Picture

Figure 6: Picture of the poster session of the "Security and Privacy in the (golden) Age of AI" summer school.

5.11 Number of attendees

The summer school had approximately 40 attendees.

5.12 CyberSec4Europe involvement

Wouter Joosen (KUL) and Davy Preuveneers (KUL) are the co-organising chairs of the summer school. Many PhD students of their research group presented their work during the poster session. Jesse Davis (KUL, DTAI) and Emmanuela Orsini (KUL, COSIC) who are members of two other research groups at the same faculty of KUL, contributed two lectures. Additionally, Michel Van Eeten (TUD) and Carlos Gañan (TUD) gave two lectures at the event.

5.13 Conclusion

The first edition of the “Summer school on Security and Privacy in the (golden) Age of AI” has been a success. In spite of the COVID pandemic, we were able to organise this four-day program on-campus, in Heverlee (Belgium). For many of the researchers coming from abroad, this was their first international event during their PhD. It gave the PhD students the opportunity to jointly learn, discuss and target research results and research plans on how ML solutions contribute to improvements in Security & Privacy, and how to ensure the robustness of ML applications and techniques in a context of attacks and adversarial behaviour. Both the lectures and social events were well appreciated.

6 Security Testing and Verification 2022

6.1 Name of the school

Summer School on Security Testing and Verification

6.2 Website (URL)

https://cybersecurity-research.be/summer-school-security-testing-and-verification-2022

6.3 Dates

20 September - 22 September 2022.

6.4 Location

The school was held at Campus Arenberg III of KU Leuven in Heverlee, Belgium.

6.5 Organiser

The first edition of the Summer School on Security Testing and Verification was a joined effort between KU Leuven (KUL) and Vrije Universiteit Brussel (VUB).

6.6 Main audience category

Scientific community and early-stage researchers, mainly PhD students and MSc students.

6.7 Description

Nowadays, the need to secure software is of utmost importance. Cybersecurity attacks and abuses often exploit weaknesses in software implementations. As a community, we therefore need to create various security testing and verification techniques to contribute to a versatile solution space. Security testing and verification has become a subject of interest to many researchers. This summer school covers insights and state-of-the-art knowledge about multiple relevant subdomains. PhD students and researchers will thus get a broad overview, as well as an opportunity to dive deeper into their own areas of specialization.

6.8 Speakers, lecturers and topics

The full program is available at https://cybersecurity-research.be/summer-school-program

Lecturer (Partner)	Topic
Eric Bodden (Paderborn University)	ML-aided Static Application Security Testing: Current benefits and limitations
Mathy Vanhoef (KU Leuven)	Fuzzing Network Protocol Implementations
Amin Timany (Aarhus University)	A Formal and Foundational Approach to Program Verification for Safety and Security
Cristian Cadar (Imperial College London)	Testing Your Software with Dynamic Symbolic Execution
Fabio Palomba (University of Salerno)	Mining Software Repositories for Vulnerability Prediction: Lessons Learned, Challenges, and Recommendations
Riccardo Scandariato (Hamburg University of	Automated analysis of architectural security

Technology)	
Koen Yskout (KU Leuven)	Automated analysis of architectural security

Table 7: Overview of all lectures at the “Security Testing and Verification” summer school.

6.9 Teaching material

Teaching materials for the above lectures are made available to the attendees only.

6.10 Picture

Figure 7: Picture of the opening session of the “Security Testing and Verification” summer school.

6.11 Number of attendees

The summer school had approximately 75 attendees.

6.12 CyberSec4Europe involvement

Bart Jacobs (KUL) is one of the co-organising chairs of the summer school. Many PhD students of their research group presented their work during the poster session. Mathy Vanhoef (KUL) and Koen Yskout (KUL) gave two lectures at this summer school. Amin Timany and Riccardo Scandariato are both alumni of KUL, and now professors at other universities.

6.13 Conclusion

The first edition of the “Summer school on Security Testing and Verification” was organised as a four-day an on-campus event in Heverlee, and welcomed a high number of participants. They appreciated both the lectures as well as the hands-on sessions to gain insights in the areas of verification, security by design, static application security testing, dynamic application security testing, machine learning for cyber security, observing ecosystems of abuse. Additionally, the poster sessions gave the PhD students the opportunity to discuss their ongoing research.