



Cyber Security for Europe

D3.16

Security Requirements and Risks Conceptualization

Document Identification	
Due date	30 November 2021
Submission date	30 November 2021
Revision	1.0

Related WP	WP3	Dissemination Level	CO
Lead Participant	VTT	Lead Author	Latvala Outi-Marja (VTT)
Contributing Beneficiaries	GUF, UMU, UNITN, CNR, KAU, KUL, POLITO, UCD, UM, UPS-IRIT, VTT	Related Deliverables	D3.5, D3.7, D3.10, D3.17

Abstract: This document presents the research results on usable security and privacy, and on usability of different security solutions, that were acquired in the context of Cyber Security for Europe project. This report highlights relevant research questions organized into three themes of privacy, security requirements and designing security for the human user. In this task the partners have developed the usability aspects of their assets. We have organized the assets into three layers according to their relationship with the user. To conclude this report we collected common observations and recommendations from the research results.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement.



The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

Usability is an important ingredient of security and privacy solutions. If the technically more secure system is cumbersome and makes the main task at hand more difficult, a regular user will likely prefer an easier, unsecured option.

In this report we present our research results on usable, human-centred cyber security. The research can be divided into three themes: data privacy and protection, eliciting and fulfilling security requirements and enhancing the human understanding of security solutions. The assets that have been part of this research can also be categorised into a three layer structure: assets that analyze the user or the usability of other tools, assets that are used directly by the users for a specific purpose and assets that advise the user in their main task.

The results of our research include the following.

- We found ways to make data protection impact assessment easier.
- We described guidelines for adopting a privacy-preserving identity management solution in a user-friendly manner.
- We introduced different ways to elicit security requirements
- We proposed a framework to characterize the adaptive authentication problem and support the engineering of adaptive authentication systems.
- We utilized modelling to analyze the impact of security mechanisms on usability, and used threat modelling techniques to analyse security.
- We showed how results of exhaustive formal analysis can be presented in a more user friendly way.
- We implemented a proof-of-concept communication system using human understandable cryptography.
- We presented ways to advise users on authentication methods and how to compare them.

Overall, the use of visualizations and modelling is advisable when designing new secure solutions. They can benefit both the developers of new technologies and services as well as the final users of the products.

Document information

Contributors

Name	Partner
Outi-Marja Latvala	VTT
Manuel Cheminod	CNR
Sebastian Pape	GUF
Welderufael B. Tesfay	GUF
Matthias Beckerle	KAU
Simone Fischer-Hübner	KAU
Davy Preuveneers	KUL
Alzubair Hassan	UCD
Liliana Pasquale	UCD
Boštjan Kežmah	UM
Marko Kompara	UM
Jesús García Rodríguez	UMU
Rafael Torres Moreno	UMU
Célia Martinie	UPS-IRIT

Reviewers

Name	Partner
João Resende	C3P
Liina Kamm	CYBER

History

Version	Date	Authors	Comment
0.01	2021-03-16	Outi-Marja Latvala	Outline created
0.02	2021-06-21	Sebastian Pape	Initial content, formatting fixes
0.1	2021-09-03	Outi-Marja Latvala	ToC revision
0.11	2021-09-18	Davy Preuveneers	Update on content
0.12	2021-09-20	Célia Martinie	Update on content, organizing subsections
0.13	2021-09-20	Marko Kompara	Update on content
0.2	2021-09-29	Outi-Marja Latvala	Abstract and Summary
0.21	2021-09-29	Sebastian Pape	SotA, improvements on content
0.3	2021-10-03	Davy Preuveneers	Minor edits throughout document
0.31	2021-10-04	Welderufael B. Tesfay	Added content
0.4	2021-10-04	Jesús García and Rafael Torres	Finalized content, minor edits throughout document

0.41	2021-10-05	Liliana Pasquale and Alzubair Hassan	Added content
0.5	2021-10-13	Outi-Marja Latvala	Rewrote Introduction, rearranged section 4
0.6	2021-10-15	Outi-Marja Latvala	Conclusion, Summary, Abstract, titles, fixes
0.7	2021-10-21	Outi-Marja Latvala	Started migration to Word
0.8	2021-10-25	Outi-Marja Latvala	Figures, Tables, Abbreviations. Preparing for 1 st internal review.
0.81	2021-10-26	Outi-Marja Latvala	Merged last minute additions
0.82	2021-10-26	Célia Martinie	Corrected figure numbering issues in section 4.1
0.83	2021-11-05	Outi-Marja Latvala	Review comments check, some restructuring, Action points added
0.84	2021-11-08	Outi-Marja Latvala	Merging changes from several partners after reviews
0.85	2021-11-11	Welderufael B. Tesfay	Added introduction and SOTA to Sec 2.3 & Sec 4.6
0.9	2021-11-15	Outi-Marja Latvala	Edits before 2 nd review
0.91	2021-11-17	Sebastian Pape	Reworked 3.1 and 4.5
0.92	2021-11-19	Sebastian Pape	Reworked 3.2
0.93	2021-11-32	Outi-Marja Latvala	Final edits on conclusions and figures
1.0	2021-11-30	Ahad Niknia	Final check, preparation and submission

Table of Contents

1	Introduction.....	11
1.1	Aim of our Research.....	12
1.2	Document Structure.....	14
2	Data Privacy and Protection.....	15
2.1	User-Friendly Privacy-Preserving IdM.....	15
2.1.1	State of the Art.....	15
2.1.2	Challenge Beyond the State of the Art.....	16
2.1.3	Privacy-Preserving IdM for the User.....	16
2.2	Selecting Relevant Risks to Be Considered in a DPIA.....	17
2.2.1	State of the Art.....	17
2.2.2	Challenge Beyond the State of the Art.....	18
2.2.3	Identifying Implausible Risks.....	18
2.3	Explainable Default Privacy Setting Prediction.....	28
2.3.1	State of the Art.....	28
2.3.2	Challenge Beyond the State of the Art.....	29
2.4	Summary.....	29
3	Tools to Elicit and Fulfill Security Requirements.....	31
3.1	Serious Games to Prevent Social Engineering.....	31
3.1.1	State of the Art.....	31
3.1.2	Challenge Beyond the State of the Art.....	31
3.1.3	Systematic Scenario Creation for HATCH.....	32
3.1.4	Legal assessment for HATCH.....	33
3.1.5	CyberSecurity Awareness Quiz.....	33
3.2	Input Data for Security Risk Assessments.....	34
3.2.1	State of the Art.....	34
3.2.2	Challenge Beyond the State of the Art.....	35
3.2.3	Selection of a Secure Cloud Computing Provider.....	36
3.2.4	Empirical Analysis of Practitioners' Assessment Capabilities.....	36
3.3	Privacy Notifications.....	37
3.3.1	State of the Art.....	38
3.3.2	Challenge beyond State of the Art.....	38
3.3.3	Summary of Key Results.....	38
3.3.4	Implications for the Design of TETs.....	39
3.4	Adaptive Authentication.....	41

3.4.1	State of the Art	41
3.4.2	Challenge Beyond the State of the Art.....	41
3.4.3	Requirements, Authentication Methods, Contextual Factors, and Decision Techniques	42
3.4.4	Adaptive Authentication System Activities.....	45
3.5	Summary.....	45
4	Enhancing the Human Understanding of Security Solutions	47
4.1	Analyzing Usability and Security at Design Time	47
4.1.1	State of the Art	47
4.1.2	Challenge beyond the State of the Art	47
4.1.3	A Generic Multi-Models Based Approach for the Analysis of Usability and Security at Design Time 48	
4.2	Utilizing Human Capabilities in Cryptography.....	51
4.2.1	State of the Art	51
4.2.2	Challenge Beyond the State of the Art.....	52
4.2.3	A Novel Human Authenticated Communication Channel with Visualizable Encryption.....	52
4.3	Formal Verification and Visualization of Security Policies	54
4.3.1	State of the Art	54
4.3.2	Challenge Beyond the State of the Art.....	54
4.3.3	Formal analysis and complexity reduction to support usability.....	54
4.4	Analyzing Security, Privacy and Usability Trade-offs in Multi-factor Authentication	56
4.4.1	State of the Art	57
4.4.2	Challenge Beyond the State of the Art.....	58
4.4.3	Authentication Knowledge Framework	58
4.5	Understanding Users' Privacy Concerns.....	60
4.5.1	State of the Art	60
4.5.2	Challenge Beyond the State of the Art.....	61
4.5.3	Augmented Reality.....	61
4.5.4	Privacy Enhancing Technologies.....	63
4.6	Analysis, Presentation and Understanding of Privacy Policies	66
4.6.1	State of the Art	66
4.6.2	Challenge Beyond the State of the Art.....	67
4.6.3	Analyzing Privacy Policies	67
4.7	Summary.....	68
5	Conclusion.....	69
6	References	71

List of Figures

Figure 1: Overview of the assets' relationship to the users.	12
Figure 2: DPIA risk assessment example with identified implausible risks.	19
Figure 3: Steps of the systematic scenario creation.	32
Figure 4: Derived scenario for a consulting company.	32
Figure 5: Relation between HATCH, PROTECT and CyberSecurity Awareness Quiz.....	33
Figure 6: Player's user interface for the CyberSecurity Awareness Quiz.	34
Figure 7: Overview of our approach for secure cloud service provider selection.	37
Figure 8: Visualisation of the experiments' scenario.	37
Figure 9: Results of the practitioners' assessments for each control; red circles indicate the median of the practitioners' answers; green rectangles indicate the scenarios' maturity levels.	37
Figure 10: Adaptive authentication system activities.	45
Figure 11: Example of task model describing user actions to log in.	48
Figure 12: Example of an attack tree for a keyboard login authentication mechanism.....	49
Figure 13: Example of a task model with representation of threats and effects.	50
Figure 14: The AuthGuide wizard for MFA configuration and requirement validation.	59
Figure 15: Mockup for the vignette-based survey.	62
Figure 16: Research model for contextual factors of privacy concerns.....	62

List of Tables

Table 1: Mapping the assets and other research into layers and themes.....	14
Table 2: List of potential risks, with non-applicability criteria.....	23
Table 3. Summary of the results of the vignette-based online survey	63
Table 4. Qualitative results for PET usage.....	64

List of Acronyms

<i>2</i>	2FA	Two-factor Factor Authentication
<i>A</i>	AC	Access Control
	AHP	Analytical Hierarchy Process
	APCO	Antecedents - Privacy Concerns - Outcome
	API	Application Programming Interface
	AR	Augmented Reality
<i>B</i>	BLE	Bluetooth Low Energy
<i>C</i>	CAIQ	Consensus Assessment Questionnaire
	CCA	Chosen Ciphertext Attack
	CFIP	Concern for Information Privacy
	COBIT	Control Objectives for Information and Related Technologies
	CPA	Chosen Plaintext Attack
	CSA	Cloud Security Alliance
	CSP	Cloud Service Provider
	CWA	The German Corona-Warn-App
<i>D</i>	DLT	Distributed Ledger Technologies
	DPIA	Data Protection Impact Assessment
<i>E</i>	EEVEHAC	End-to-end Visualizable Encrypted and Human Authenticated Channel
	ESARA	Enterprise Smartphone Apps Risk Assessment
<i>G</i>	GDPR	General Data Protection Regulation
<i>H</i>	HAKE	Human Authenticated Key Exchange Protocol
	HAMSTERS	Human-centered Assessment and Modelling to Support Task Engineering for Resilient Systems
<i>I</i>	IAM	Identity and Access Management
	IdM	Identity Management
	IoT	Internet of Things
	IoV	Internet of Vehicles
	ISMS	Information Security Management System
	ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
	IUIPC	Internet Users' Information Privacy Concerns
<i>K</i>	KPI	Key Performance Indicator
<i>M</i>	MAC	Message Authentication Code
	MAPE-K	Monitor-Analyze-Plan-Execute over a shared Knowledge
	MFA	Multi-factor Authentication
	ML	Machine Learning

<i>N</i>	NLP	Natural Language Processing
<i>O</i>	OTP	One-time Password
<i>P</i>	PAKE	Password Authenticated Key Exchange
	PET	Privacy Enhancing Technology
	PIN	Personal Identification Number
	pp-IdM	privacy-preserving Identity Management
	PSI	Privacy sensitive information
<i>R</i>	RBAC	Role-based Access Control
	RFID	Radio-frequency Identification
	RP	Relying Party
<i>S</i>	SME	Small and Medium-sized Enterprises
	SMT	Satisfiability Modulo Theories
	SSI	Self-Sovereign Identity
	SVM	Support Vector Machine
<i>T</i>	TET	Transparency Enhancing Tool
<i>U</i>	UAN	User Authentication Number
	UX/UI	User Experience / User Interface
<i>W</i>	WTP	Willingness To Pay

1 Introduction

Security is often described as a combination of confidentiality, integrity and availability (the CIA triad). In day-to-day life, these are necessary but insufficient qualities for a secure system. Usability is an important attribute to all security solutions, 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.

In this report we present several usability solutions that are motivated by the need to empower users to make sensible security choices. We have researched methods on 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.

To take a broader perspective of the contributions of T3.6 we refer to the global architecture of WP3, which was described in D3.12 *Common Framework Handbook 2*. The research and assets of T3.6 are divided between two building blocks of the global architecture (see Figure 3 of D3.12):

- the usable tools and consent block from the user domain
- the usable dashboards, UI and tools block from the administrative plane

This report follows two previous deliverables produced in T3.6, D3.5 *Usable Security & Privacy Methods and Recommendations*, and D3.7 *Usability Requirements Validation*. The former presented a state of the art of the most relevant research on usability in relation to security and privacy. The latter reviewed the most important research and methodologies proposed to validate usability requirements. Additionally, this deliverable is followed by D3.17 *Integration to Demonstration Cases*, where we will discuss the way T3.6 assets have been integrated or may integrate with WP5 demonstration cases.

The purpose of this report is to provide a more focused view on three main themes: data privacy and protection, solutions for fulfilling security requirements, and analysing and illuminating security for the benefit of users. We present the state of the art for the individual topics and how the work conducted in this task expands on it, e.g., which challenges are solved or previous research gaps are filled.

Our research themes:

I: Privacy

II: Fulfilling security requirements

III: Understandable security solutions

1.1 Aim of our Research

In this task the focus of research and development of assets is on the users and usability. Several assets are developed in neighbouring tasks as well, so in this deliverable we provide the results that relate to the usability of those assets. We also present other research conducted in this task that relates to usability of security solutions.

The assets can be divided into three groups according to their relationship with the user. In Figure 1 we present these groups as the user layer, the guidance layer and the analysis layer. In the user layer the assets are directly used by either a layperson or a professional to achieve a goal, like authenticating themselves to access a service. In the guidance layer the user is still choosing to interact with the asset, but the purpose of the user is to learn something; these assets try to advise or influence the user, so that they can perform other tasks more securely. For example, when the user is trying to perform a data protection impact assessment (DPIA), they can consult the prepared DPIA template. The analysis layer is slightly different compared to the other two. It contains assets that analyze or model the actions of the user or the usability of other security solutions. Visualizations are used to make security information more understandable.

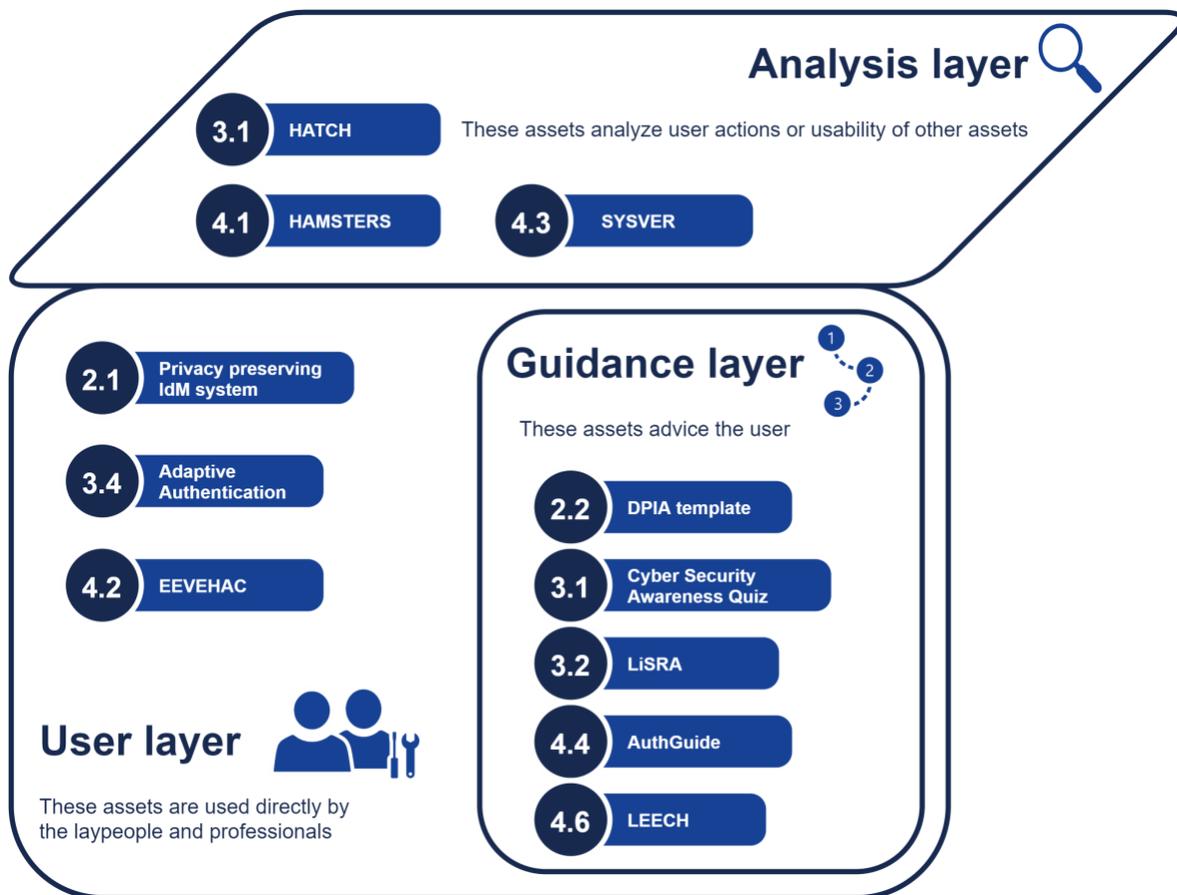


Figure 1: Overview of the assets' relationship to the users.

From the research conducted on and with these assets we can also identify three main themes. Firstly, we have the theme of *privacy*. Processing of personal data is a necessary step in many modern services. From the point of view of businesses, it is important to be in compliance with regulations, e.g., the General Data Protection Regulation (GDPR). A previous deliverable in the project (D3.6) proposed a solution to help users perform a DPIA. The proposed template included a long list of potential risks users would have to evaluate and address during their assessment. Here we try and define ways in which to shorten that list of potential risks based on the specific circumstances surrounding the processing of personal data.

Moreover, from the point of view of the citizen it is important to have knowledge and options on the ways their personal data can be used. This requires tools that enable the decision (i.e., privacy-enhancing tools so that there is a real possibility for managing personal information during interactions), but also that those tools are adapted to user preferences, or they will be dismissed by users in favour of more convenient (but privacy-harming) solutions. In the context of this project, we have attempted to answer the following questions regarding privacy and personal data:

- How to adjust or minimise the list of potential GDPR related risks based on personal data used and its processing?
- How to implement privacy preserving identity management solutions and the corresponding policies so they are user-friendly (quick and concise)?
- How to present privacy policies in a way they are easily understandable by users?
- What are the most important antecedents for privacy concerns with regard to privacy enhancing technologies and augmented reality?

The second theme covers the research on *security requirements*. Validation of security requirements has been discussed previously in D3.7, therefore in this report we present tools for eliciting and fulfilling them. The guiding questions for our research were:

- How can serious games with the focus to protect the user against social engineering attacks be adapted specifically to the target audience?
- How reliable are practitioners' assessments of security controls?
- How can existing data be used to assess the security of cloud service providers?
- What are the contextual factors and the requirements related to adaptive authentication?
- How do the contextual factors and the requirements inform the adaptive authentication system activities?

The third theme is about enhancing the *human understanding* of security solutions. We have studied how to make security solutions more user friendly, and how to present security information to a user in a clear and understandable manner. The tools to achieve these goals include modelling, visualizations and development of suitable frameworks. The nature of assets falling under this theme has allowed for collaborative research as well: the asset HAMSTERS has been used to model and analyze the usability of the asset EEVEHAC. The research questions behind the development of assets in this theme include:

- How to analyze, at design time, the potential security threats on user tasks and their potential effect?
- How to make cryptography more understandable and intuitive to use for humans?

- How to provide complex analysis results in a usable, graphical, way?
- How to advise or reassure users to use a particular method (e.g., multi-factor and biometric authentication)?
- How to compare usability and security of different authentication mechanisms, and how to justify trade-off when these properties are conflicting?

In Table 1 we have provided a mapping of different assets and other research results from all partners to the asset layers and to the research themes. The items are organized in the order they are presented in this report. To conserve space, the table uses labels *user*, *guidance* and *analysis* for the asset layers, and *privacy*, *requirements* and *human* for the research themes.

Table 1: Mapping the assets and other research into layers and themes.

Partner	Asset	Non-asset research	Asset layer	Theme	Section
UMU	Privacy-preserving IdM		User	Privacy	2.1
UM	DPIA template		Guidance and User	Privacy	2.2
GUF		Privacy settings prediction	Guidance and User	Privacy	2.3
GUF	HATCH		Analysis	Human	3.1
GUF	CyberSecurity Awareness Quiz		Guidance and User	Human	3.1
GUF	LiSRA		Guidance and User	Human	3.2
KAU		Privacy notifications	User and Guidance	Requirements	3.3
UCD	Adaptive Authentication		User	Requirements	3.4
UPS-IRIT	HAMSTERS		Analysis	Human	4.1
VTT	EEVEHAC		User	Human	4.2
CNR	SYSVER		Analysis	Human	4.3
KUL	AuthGuide		Guidance and User	Human	4.4
GUF		Privacy concerns	Analysis	Human and privacy	4.5
GUF	LEECH		Guidance and User	Human and privacy	4.6

1.2 Document Structure

This report presents the research conducted on the user and usability aspects of our assets, as well as other related research, over the duration of the project. The results are divided into three main Sections according to the themes discussed above: Data Privacy and Protection, Tools to Elicit and Fulfill Security Requirements, and Enhancing the Human Understanding of Security Solutions. The Conclusion section closes this deliverable with recommendations and future research directions.

2 Data Privacy and Protection

This section focuses on the theme of privacy and the processing of personal data. We take into account two different positions on this subject. On the one hand, the users need tools that enable their control over which and how their data will be shared. The usability of these tools will be a (or even *the*) key factor for their success. On the other hand, any business must be in compliance with regulations like GDPR. The service providers are similarly in need of usable solutions to ensure the privacy of their customers.

In this Section we present the results of three research endeavours from different perspectives on improving usability to enhance data privacy and protection. Firstly, we have studied the way security and privacy properties of products affect its usability and user adoption of the product. Secondly, we present a way for facilitating the application of one of the most relevant aspects for achieving and evaluating compliance in terms of data processing, i.e., the data protection impact assessment. Thirdly, we present a middle point solution, where the service providers predict privacy settings for the benefit of the user, but the users can still change the settings to their liking.

2.1 User-Friendly Privacy-Preserving IdM

One of the verticals of the CyberSec4Europe project is focused on privacy-preserving identity management. Throughout various deliverables and work packages of the project, we have discussed research on the challenges identified and addressed for this topic, as well as the assets adjacent to it. One of the key points identified in these discussions is the lack of adoption of existing privacy-enhancing technologies, and how one of the main reasons has been their poor usability.

In this section, we focus on the privacy-preserving identity management asset. In other deliverables, we have described the technical aspects of the asset, its place in the current landscape and how it is applied to various of the pilots developed within the project. Here, we tackle a specific aspect of the research on this asset: what are the user needs for usable privacy-preserving identity management and how can we apply and improve the asset to cover those needs.

2.1.1 State of the Art

Examining the state of the art identity management (IdM) solutions discussed in D3.5 (section 4.2) and D3.11 (section 3.2.2), we can discern two groups regarding usability/privacy. Federated (single sign-on) solutions like OpenID [1] or SAML [2] have won over users because of their convenience and ease of use and convenience. However, they have glaring privacy issues, especially with respect to identity providers. On the other hand, solutions that focus on privacy and security like Idemix [3] have failed to gain traction because of their poor usability (in terms of complexity of use and understanding, as well as performance). The recent trend towards Self-Sovereign Identity (SSI) [4] claims to empower users' control, but solutions do not tackle the issue of helping them do the management (which can be cumbersome) and are usually based on hard-to-understand technologies like distributed ledgers. Thus, the challenge that arises and we try to address is implementing privacy-preserving identity management solutions and the corresponding policies so that they are user-friendly.

2.1.2 Challenge Beyond the State of the Art

The work done in this task of CyberSec4Europe goes beyond the state of the art to offer users privacy-preserving and secure identity management with minimal trade-offs of usability. Security and privacy features have been added while lessening their impact on users. For instance, the role of identity provider has been distributed, but this is hidden from the user in day-to-day interactions by the client application, which offers common functionality APIs (e.g., authentication, registration, account management etc) while masking the complexity. Also, the results of user studies have been taken into account to create an application environment which tackles user issues with privacy-preserving solutions, such as cumbersome procedures (e.g., accepting/managing policies), different perspectives on usability/privacy trade-offs, or trust in their operations (both the IdM solution and service providers).

2.1.3 Privacy-Preserving IdM for the User

In this section, our work is connected to one of the assets in WP3: the privacy-preserving identity management (IdM) system based on the distributed identity provider introduced in the H2020 project OLYMPUS. In this work package, we are empowering the pp-IdM system by integrating it with distributed ledger technologies (DLTs), taking advantage of immutability and its ability to provide a complete transaction history unlike traditional databases, to improve auditability and trustworthiness. Users will only need to know about the immutability property to understand how we are applying DLTs to improve trust (ensuring entities do not fail to meet “promised” behaviours). We also integrate with eIDAS for creating solid links between citizens' physical and digital identities. In addition, as part of this specific Task 3.6, we are developing a mobile application that includes UX/UI techniques that improve usability of the system (and, in general, privacy aware systems with access policies).

Supporting this task, we have results from in-depth user interviews carried out in the OLYMPUS project to people of all levels of education and ages from 20 to 67, selected through an external recruiting bureau. Topics included general feelings on online security and information sharing, physical ID-cards and misuse and identity theft, and also specifically related to the considered IdM solution. These user interviews were based on the idea of being able to use the system as a general identification method to access different services, even in physical exchanges (e.g., being over 16 to participate in paintball matches). Particularly, the scenario proposed in the interviews was proving that the age of the user being is over 18, having that they have a specific nationality and/or proving that they possession of a valid driving license.

From the answers of the target group, we can surmise some general trends on what people want from these kinds of systems to consider it as being better than other alternatives. People value privacy with different intensities, but almost all would choose a privacy-aware system over a common one if it did not affect their common usage or habits. In that sense, depending on the balance between usability and privacy, users are more likely to favour one aspect over the other. For all participants, usage of a system heavily depended on how widespread its adoption was. With that in mind, we take into account their answers to develop guidelines and goals for doing the necessary processes in a user-friendly manner.

First, perception of *smoothness of operation* is very important for users. This also involves the time spent in cryptographic operations, but it is even more relatively important to make user interactions flow easily. In relation to this, users often found actually having to review and accept same(ish) policies multiple times or for similar service providers *too laborious*. Thus, including options to ease this process (e.g., remember policy acceptances, establishing preferences) would be welcomed. However, “edge cases”, i.e., people with stronger privacy concerns and who are not deterred by extra hassles, have to be considered. As an aside,

verifiers also benefit from simpler processes. In the solution, they only have to do setup once (which is mostly handled automatically). Also, in physical exchanges, checking a complex policy with multiple predicates (e.g., age over sixteen) becomes an uncomplicated process where the verifier only has to check that the validation was successful (could be as easy as a green/red icon) instead of taking an ID and manually checking every predicate (e.g., mental computations from date of birth).

Users sometimes found cryptographic principles too complex and did not bother to understand them, preferring to place their *trust* in the organizations involved over the soundness of the solution. Information on the principles behind the solution should be accessible if users want to make that decision, but not in the front of the application. Also, this concept can extend to services accessed. As we have deployed a DLT solution where information about identity and service providers can be published, we can do some evaluation on how they are behaving and establishing trust levels that are shown to users before interaction.

2.2 Selecting Relevant Risks to Be Considered in a DPIA

The deliverable *D3.6 Guidelines for GDPR Compliant User Experience* as part of the CyberSec4Europe project provides the readers with guidelines on understanding and applying General Data Protection Regulation (GDPR) requirements. One of the main contributions of the deliverable is a data protection impact assessment (DPIA) template, designed to help data controllers to perform the assessment themselves when one is required by the GDPR. The template is designed predominantly for use by small and medium organisations that do not have specialised personnel and/or where hiring outside help would present a significant expense.

One of the main tasks of a DPIA is identifying and assessing the risks to the rights and freedoms of individuals. The DPIA template provides data controllers with a pre-prepared list of potential risks that originate from the GDPR requirement (Table 8 in D3.6) and similar privacy frameworks from around the world, from which data controllers can select risks that are relevant to them and add further risks that are specific to their circumstances. The same table is then used to specify the probability and severity of identified risks and finally calculate the risk value. This extensive list of risks is something that adds a lot to the usability of the tool (especially for the controllers that are not familiar with identifying relevant risks, like might be found in smaller organisations) and is something that distinguishes the template from other free DPIA tools/templates (for alternative solutions see deliverable D3.11).

However, the list of potential risks in the original template is quite long, with 121 potential risks distributed among fourteen different categories. Therefore, the intent is to establish a way to reduce the potential risks data controllers performing a DPIA with the help of the template provided in the D3.6 have to consider. The result would cut down on time identifying relevant risks from the list of potential risks, consequently simplifying the procedure, making it more user-friendly and consistent among users of the method. While working on a model to streamline the number of relevant risks, we also intend to revise and add some more potential risks to the list.

2.2.1 State of the Art

Performing a data protection impact assessment is a major challenge in complying with the GDPR. To alleviate this, many solutions were have been presented. We have discussed related DPIA templates and

guides in D3.11 (Section 3.1.1) and mentioned some additional ones in D4.4 (Section 5.5.1.6). The biggest challenge within DPIA is the assessment of risks.

2.2.2 Challenge Beyond the State of the Art

The main advantage of the work done so far in CyberSec4Europe for the performance of DPIAs, is the list of potential risks. Such a list is not included in any of the other solutions, and as far as we are aware, there is no other work identifying potential risks to be addressed in a DPIA. The pre-prepared list makes it easier, especially for users who do not often perform DPIAs, to not leave out any relevant risks. In this deliverable, we expand on this advantage, further differentiating the produced DPIA template from other similar solutions. To improve the usability of the predefined list of risks, we propose exclusion criteria, by which the user can identify risks that are not relevant for their use case and, in turn, decrease the amount of work that needs to be done in the assessment. In the future, the European Data Protection Board or the national data protection authorities could endorse one or more such solutions (if they do not already have their own, like France's supervisory authority CNIL¹) to signal to the users that using a solution like that is safe and compliant with their and GDPR requirements.

2.2.3 Identifying Implausible Risks

The method we have used for reducing the work of recognising potential risks is based on the fact that depending on the types of personal data, how the data are processed, and why the data are processed, not all risks from the list provided in the D3.6 always apply or, to put it more accurately, the probability of them occurring is basically negligible. We have therefore noted some of the data processing situations (i.e., those that are not dependent on the interpretation, argumentation, or circumstances of why and how the personal data is processed) where some of the risks are not relevant for that particular set of circumstances. We have also updated the list of potential risks with some smaller changes to already existing risks and some new risks.

An example of the complete table to be used in a DPIA is presented in Figure 2. The pictured table holds each individual risk, with its probability, severity, and the combined risk level before any measures are taken. Next in the table are any notes that are relevant to the specific risk within this DPIA. We will use this field (when applicable) to explain why some risks are not relevant to the current DPIA. The next information in the table is the measure that we have taken to reduce the probability or the severity of the risk, and finally, there is information on the probability, severity, and the final risk level, after the measures to reduce the risks have been applied. This risk should never exceed a medium level; otherwise, you cannot proceed with the implementation of your solution (or processing of this data) until you have consulted your Data Protection Authority and they have allowed you to carry on.

The lower section of Figure 2 presents the example of a situation where a pair of risks are not applicable for the given DPIA. In such a case, the probability of a risk happening is basically non-existent. We mark it as not applicable (i.e. N/A). Even if an event has very severe consequences, the risk level associated is low because the event will never happen. Even if the resulting risk level is low, it is important to document this in the DPIA and explain why this is the case. We can do this in the field for notes. We propose some of these explanations further on.

¹ <https://www.cnil.fr/en/privacy-impact-assessment-pia>

Nr. RISK	BEFORE MEASURES			NOTES	MEASURE	AFTER MEASURES			
	PROBABILITY	SEVERITY	RISK			PROBABILITY	SEVERITY	RISK	
COMULATIVE VALUE			high					medium	
1 Choice and consent			high					low	
1	There is no legal basis for processing	low	high	medium	Through thorough analysis, we found that the processing, the purpose and the types of personal data are determined by law	Professionals (clerk) signed a "Data Protection Statement"	low	medium	low
2	The legal basis is not properly selected	low	high	medium	Through thorough analysis, we found that the basic foundation is the law, which also determines the details of processing	Professionals (clerk) signed a "Data Protection Statement"	low	medium	low
3	Use of legitimate interest by public authorities in the performance of their tasks	medium	high	high	We use a legitimate interest	Professionals (clerk) signed a "Data Protection Statement"	low	medium	low
● ● ●									
56	The portable data received by an individual are not machine-readable	N/A	high	low	There is no right to data portability due to the processing of data under the law.		N/A	medium	low
57	The portable data received by an individual is incomplete	N/A	high	low	There is no right to data portability due to the processing of data under the law.		N/A	medium	low
● ● ●									

Figure 2: DPIA risk assessment example with identified implausible risks.

We have prepared a numbered list of statements from 1 to 8 (where statement 2 is further divided into parts from *a* to *d*). These statements serve as the criteria to identify non-applicable risks in the adapted list of potential risks (Table 2). Each statement is also followed by a short text giving some more information and/or explaining the position of the original statement. Included is also a note that the users can use in their DPIA to explain why a certain risk has such a low probability (i.e., is not applicable) and consequently has a low overall risk level even without applying any preventative measures.

To reduce the number of applicable risks in the table, users should look at statements 1-8 and establish whether each of the statements applies to them. When a statement holds true for the DPIA they are preparing, they can mark the probability of the risks that are marked with the number of the applied statement in the last column of Table 2 **Error! Reference source not found.** as N/A (as was shown in Figure 2). Even though the risks are not applicable to a given situation, it is important to still keep the risks in the list and not just remove them because this shows that they were not missed in the assessment but were considered, and a conscious decision was made on why they are not applicable to the given circumstances. It is also worth

noting that when answers to the statements that were used to mark risks as not applicable, the risks and their impact should be reevaluated.

We have also updated the list of potential risks (Table 2) from the original presented in D3.6, with some smaller changes to already existing risks (they are marked with a * before their sequential number) and some new risks (they are marked with a + before their sequential number). We have added 5 new risks for the new total of 126. The new risks are mostly more specific and replace previous risks that were more generic. The eight statements can, in total, be applied to 59 different risks in the list. An example, where all the statements apply to a specific DPIA, results in an almost 47% reduction of relevant risks from the full list of 126 potential risks (Table 2).

Below are the eight statements to use when deciding the applicability of risks, followed by the improved list of potential risks (Table 2) together with information on which statements can make each of the risks not applicable.

1. You do NOT require the users to give their consent for the processing of their personal data. You use one of the other lawful bases for processing.

Possible bases for the processing of personal data are defined in Article 6 of the GDPR. In addition to consent, they include contract, compliance with a legal obligation, vital interests, task in public interest, or legitimate interests.

Note: We do not use consent as a base for processing.

2. You have a legal obligation to process the personal data, you are doing it for reasons of public interest, or the processing is in vital interests of the data subject.

The GDPR allows for some exceptions to the individuals' rights to erasure of data, portability of data, right to object to the processing of their data, and right to restrict processing²:

- a) *Legal obligation: Data subjects do not get the rights to erasure, portability, to object to processing, and to restrict processing³.*

Note: Data processing is compelled under legal obligation.

- b) *Public interest (e.g., public health, scientific, statistical or historical research purposes): Data subjects do not get the rights to erasure, portability, and to restrict processing (but not commercial purposes)⁴.*

Note: Data processing is done in the public interest.

- c) *Vital interests (is essential for the life of the data subject or that of another natural person): Data subjects do not get the rights to portability and to object to processing.*

Note: Data processing is in vital interest to individuals.

²<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#what>

³https://www.termsfeed.com/blog/gdpr-lawful-basis-legal-obligation/#The_Gdpr_S_Lawful_Basis_For_Processing

⁴<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/>

- d) *Data is needed to exercise the right of freedom of expression⁵(e.g., news report): Data subjects do not get the right to erasure.*

Note: Data is used under the right of freedom of expression.

Right to object is also more restricted when processing personal data for scientific or historical research, or statistical purposes; however, this only applies if appropriate safeguards are in place and the lawful basis for processing is a public task where it is necessary for the performance of a task carried out in the public interest⁶.

3. You do NOT use automated decision making or profiling of users using personal data. *Article 22 of the GDPR puts restrictions on decisions based solely on automated processing, including profiling, which produces legal or similarly significant effect for the data subject. Such automated decision making or profiling can be used only when:*
- *it is necessary for the entry into or performance of a contract; or*
 - *it is allowed by the Union or domestic law applicable to the controller which also lays down safeguards for the data subject; or*
 - *it is based on the data subject's explicit consent.*

Note: Personal data is not used to make automated decision making or profiling.

4. You do NOT have or require a Data Protection Officer (DPO). *The controller and the processor must appoint a Data Protection Officer if:*
- *They are a public authority or body, except for courts acting in their judicial capacity;*
 - *Their core activities consist of tasks that by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or*
 - *Their core activities consist of processing on a large scale of special categories of data (Article 9) or data relating to criminal convictions and offences (Article 10).*

Note: We are not a public entity and our activities do not require us to appoint a DPO.

5. You do NOT have third-party processors or are a joint controller. You are the sole processor of personal data. *The controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*

⁵https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_en

⁶<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/>

A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Joint controllers are two or more controllers which jointly determine the purposes and means of processing. Controllers are not joint controllers if they are processing the same data for different purposes. Joint controllers shall, in a transparent manner, determine their respective responsibilities for compliance with the obligations under GDPR, in particular as regards the exercising of the rights of the data subject. Regardless of the distribution of the responsibilities, the data subject may exercise his or her rights with any of the controllers.

Note: We are not a joint controller or use third-party processing.

6. You do NOT archive personal data for purposes in the public interest, for scientific or historical research purposes, or for statistical purposes.

GDPR (Article 89) allows for some derogations or exceptions for some of the rights and obligations of processing personal data. These most commonly apply to archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Note that this does not mean such data does not have to be subject to appropriate safeguards. Often it is not the nature of archives but the mission of the institution that holds them that determines whether the exemption can be applied⁷.

Note: Data is not archived for purposes in the public interest, for scientific or historical research purposes, or for statistical purposes.

7. You have a legal obligation to process personal data.

One can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation. It is still mandatory to document and justify the decision to use this legal basis, and show that the processing of personal data is necessary for compliance with legal obligations.

Legal obligation as a basis for the processing of personal data does not mean that there must be a legal obligation specifically requiring the specific processing activity. It is sufficient if the purpose of processing is to comply with a legal obligation that has a sufficiently clear basis in either common law or statute⁸.

Note: Processing of personal data is done to meet legal obligations.

8. You do NOT process the personal data of children.

⁷https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf

⁸<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/>

Sometimes It can be difficult to know whether you are processing children's data (especially online). If you cannot positively determine whether your data subjects are children, you should take one (or more) of the following routes⁹:

- *Design your data processes as if you are certain you process children's data.*
- *Put in place appropriate/proportionate deterrence from children participating and providing their personal data.*
- *Take appropriate actions to enforce age restrictions.*
- *Implement an up-front age verification system.*

Note: We definitively do not process data of children.

Table 2: List of potential risks, with non-applicability criteria.

1 Choice and consent	Not Applicable
1 There is no legal basis for processing	
2 The legal basis is not properly selected	
3 Use of legitimate interest by public authorities in the performance of their tasks	
4 The conditions for consent are not clear	1
5 The terms of consent are not separated by purpose	1
6 An individual is unlawfully coerced into consent in an incompatible relationship with another lawful ground	1
7 Consent is not clearly different from other matters	1
8 Consent is not in clear and simple language	1
9 The consent may not be revoked at any time by an individual	1
10 Consent is not as easy to revoke as to give	1
+11 Consent for children has not been obtained from holders of parental rights	1, 8
12 Risks related to the processing of children's personal data	8
2 Determination of lawful purpose and limitation of use	
13 The purpose of the processing is not specified	
14 The purpose of the processing is not explicit or clearly defined	
15 The purpose of the processing is not legal	7
16 The retention period is not set	
17 Use of data for another purpose than the purpose for which it was collected	
18 Excessive data volume for processing (minimum data volume not used)	

⁹<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be/>

19	Retention period exceeded	
20	The processing method does not guarantee the security of personal data	
21	There is no protection against tampering or illegal processing	
22	There is no protection against unintentional loss or destruction of personal data	
23	There is no protection against accidental data corruption	
24	Risks related to automated decision making	3
25	Risks related to profiling	3
+26	Different ages of consent between Member States have not been considered	8
+27	Processing special categories of personal data without meeting any of the specific conditions in Article 9 of the GDPR	
3 The life cycle of personal and sensitive information		
28	Extension of retention period with no legal basis	
29	Failure to extend the retention period, where there is a legal basis or at the request of the individual	
30	Undefined procedures of the individual's request after verification if the controller processes data	
31	Undefined procedures of the individual's request for access to data processed by the controller	
32	Undefined procedures for individual's requests after restriction of processing	2a, b
33	Undefined procedures for individual's requests after data deletion	2a, b, d
34	Undefined procedures of the individual's request for data portability	2a, b, c
35	Undefined procedures in case of an individual's objection	2a, c
36	Improper implementation of procedures in case of an individual's request to verify that the controller is processing data	
37	Improper implementation of procedures in case of individual's request access data processed by the controller	
*38	Improper implementation of procedures in case of an individual's request for restriction of processing	2a, b
39	Improper implementation of procedures in case of an individual's request for deletion of data	2a, b, d
40	Improper implementation of procedures in case of an individual's request for data portability	2a, b, c
41	Improper implementation of procedures in case of the objection of an individual	2a, c
*42	Unnecessary processing of special categories of personal data	
43	The implementation of information systems and the design of processes do not take into account data protection by default and by design	
44	No data protection impact assessment has been produced	
4 Punctuality and quality		
45	The information is incorrect	

46	An individual's data is not updated when the individual changes it	
47	In the case of data change, not all data of the individual is updated	
48	Undefined procedures in case of an individual's request for rectification of data processed by the controller	
49	Improper implementation of procedures when requesting an individual to correct data processed by the controller	
5 Openness, transparency and informing		
50	The information is not transparent to the individual	
+51	The information is provided in a way adjusted for children.	8
52	Information presented to the individual is not uniform for all controllers and processors	5
53	Ways to exercise the rights of the individual are not given in a comprehensive and clear manner	
*54	Required information is not provided to an individual when obtaining personal data	
55	Inaccurate informing of an individual when information is not obtained from an individual	
6 Participation of individuals		
56	The portable data received by an individual are not machine-readable	2a, b, c
57	The portable data received by an individual is incomplete	2a, b, c
58	The decision made by automatic decision-making is final	3
*59	Automatic listing of an individual's data is definitive	
60	For the joint controllers, the agreement does not clearly set out all the rights and obligations of each of the controllers	5
61	The content of the joint controller's agreement is not accessible to the individual	5
62	There is no designated contact point for the individual	
63	The contract unlawfully restricts the exercise of individual rights to certain controllers	5
64	There is no designated data protection authority	
65	The contact details of the Data Protection Officer are not accessible to the individual	4
7 Responsibility		
66	There is no defined procedure for determining whether the processing of personal data for other purposes is legal	7
67	The tasks and responsibilities of the Data Protection Officer are not clearly defined	4
68	There is no defined procedure for consulting the supervisory authority in light of the results of the privacy impact analysis	
8 Security measures		
69	There are no documented security policies for protecting personal information	

*70	There is no documentation of personal data processing for purposes other than the purpose for which they were collected	
71	Organisational measures for the protection of personal data are not clearly defined	
72	There are no clearly defined technical measures for the protection of personal data	
73	Organisational measures to protect personal data are not sufficient	
74	Technical measures to protect personal data are not sufficient	
75	Organisational measures to protect personal data are not being implemented	
76	No technical measures are in place to protect personal data	
77	There is no regular check on security controls	
78	Organisational controls for the protection of personal data are not clearly defined in contracts with processors	5
79	Technical control contracts for the protection of personal data are not clearly defined in contracts with processors	5
9 Monitoring, measuring and reporting		
80	The Data Protection Officer does not guarantee the implementation of privacy impact assessments	4
81	The Data Protection Officer does not check compliance with the regulations	4
82	The Data Protection Officer does not educate employees	4
83	The Data Protection Officer does not cooperate with the supervisory authority	4
84	No reporting regarding the correction of personal data is introduced	
85	No reporting regarding the deletion of personal data is introduced	
86	There is no documented content reporting on an individual's personal information	
87	Reporting on the transfer of individual data to third parties is not introduced	5
88	Copies of personal data provided as part of the right to data portability have been preserved longer than the retention period	2a, b, c
89	No triggers have been identified to produce a privacy impact analysis	
90	There are no policies in place to design and maintain records of processing activities	
91	Recipients of personal data are not identified	
10 Prevention of damage		
92	Guidelines for determining the legality of processing have not been established	7
93	Consequences of further processing of personal data for individuals have not been determined/analysed	
*94	There is no adequate safeguard for decision making based on special categories of personal data	3
95	There is no guarantee that the exercise of an individual's right will not adversely affect the rights and freedoms of others	
+96	Pseudonymised personal data is not considered personal data	
97	No rules and procedures have been put in place to minimise the harm to an individual when archiving in the public interest	6

98	No rules and procedures have been put in place to minimise harm to an individual for the use of their personal data in historical and scientific research purposes	6
99	No rules and procedures have been put in place to reduce harm to an individual for statistical use of their personal data	6
11 Supplier / third party management		
100	No outsourcing management policies are in place	5
101	Outsourcing arrangements do not contain sufficient guarantees that adequate organisational measures are in place to protect personal data	5
102	Outsourcing arrangements contain sufficient guarantees that adequate technical measures are in place to protect personal data	5
103	Sufficient restrictions and rules for hiring sub-contractors have not been applied	5
104	Procedures and duration of processing are not specified in the agreement with the processors	5
105	The purpose and type of processing is not specified in the agreement with the processors	5
106	The types of personal data subject to processing are not specified in the agreement with the processors	5
107	The types of individuals whose personal data are subject to processing are not specified in the agreement with the processors	5
108	In agreement with the processor, not all 8 obligations are specified as per Article 28 paragraph 3 of the GDPR	5
109	The agreement with the processor does not specify the obligation and the procedure for reporting incidents	5
110	There are no requirements for the processor to outsource his work	5
111	There are no procedures in place to ensure that processors comply with the requirements of the controller	5
112	There are no procedures in place for the employee of the controller to comply with the requirements of the controller	
12 Management of incidents		
113	Procedures for notifying the supervisory authority of incidents have not been established	
114	Procedures for notifying individuals of violations are not specified	
115	The content of the notice is not specified in accordance with the regulations	
13 Built-in security and privacy		
116	Privacy and security policies do not respect the rights of the individuals	
117	Privacy and security policies do not respect the freedoms of the individuals	
118	Privacy and security policies do not take into account the legitimate interests of the individuals	

*119	Automatic procedures (with legal or similarly significant effect on individuals) do not involve manual human intervention	3
120	No policies have been put in place to assess the nature, extent, context and purposes of the processing of personal data	
121	An impact assessment on an individual is not an input to the requirements for designing information solutions	
122	Harm reduction for an individual is not an integral part of the process of creating information solutions	
14 Free movement of information and legal restriction		
123	No procedures for validating binding business rules have been defined	
124	No data transfer procedures are defined at the request of other persons	
125	Data transfer procedures to a third country are not defined	5
126	No data protection procedures are in place for their transmission	
* This risk has been slightly updated since D3.6.		
+ This risk has been added and was not in the original D3.6.		

2.3 Explainable Default Privacy Setting Prediction

This section covers the the state of the art and our contributions to exisiting works in default privacy setting preferences prediction using machine learning.

2.3.1 State of the Art

Acquisti and Grossklags [5] showed in an experiment that when users confirm privacy policies and choices, they often have lacks of knowledge about appropriate technological and legal forms of privacy protection. This is further evidenced in Pollach's [6] experimental findings which state that ordinary users are oftentimes not familiar with technical and legal terms related to privacy.

Kolter and Pernul [7] emphasized the importance of privacy preferences and proposed a user-friendly, P3P-based privacy preference generator. This tool is applicable on online service providers and it included a configuration wizard and a privacy preference summary. Similary, Biswas [8] proposed an approach focused on privacy settings preferences. The authors proposed an algorithm to detect the conflicts in privacy settings, specifically, between user preferences and application requirements in smart phone ecosystems.

Furthermore, Fang et al. [9] have proposed a privacy wizard for social networking sites. The wizard is aimed at automatically configuring a users' privacy settings with minimal effort required by the user. Authors built the wizard with an underlying observation that ordinary users conceive their privacy preferences based on an implicit structure. The wizard asks the users a limited number of carefully chosen questions, which are then used to predict the users preferences. Although, similar work is presented, our approach discussed below, is applicable to general online services, while theirs is limited in scope (i.e., used to restrict privacy of friends in social media, namely, Facebook). Additionally, Tondel [10] proposed a conceptual architecture for learning privacy preferences based on the decisions that users make in their interactions on the web. Authors reiterate that predicting of privacy preferences has the potential to protect user's privacy without requiring users to have a high level of knowledge or willingness to invest time and effort in their privacy preference setting options. Guo and Chen [11] proposed an algorithm to optimise privacy configurations

based on desired privacy level and utility preference of users. Authors require users to set up a privacy preference levels.

2.3.2 Challenge Beyond the State of the Art

Privacy-by-design and privacy-by-default are, among other concepts, the anchors of the General Data Protection Regulation (GDPR). As such, the regulation stipulates that service providers must consider privacy preserving features from the onset. However, often times, privacy settings are difficult to comprehend for ordinary users. Moreover, setting appropriate privacy preferences is a cumbersome if not an overwhelming task for users. To ease this process of setting optimal default privacy settings, machine learning approaches have recently gained traction.

As such, we have proposed a series of approaches to support the user in choosing privacy-friendly default settings. In our first endeavor in this arena, we proposed [12] a novel mechanism that provides individuals with a personalised privacy-by-default setting when they register into a new system or service. The system uses a machine learning mechanism that infers users' contexts and preferences by asking a limited number of questions. In particular, it has two schemes, namely the prediction and clustering schemes. In the prediction scheme, a user is asked five questions related to privacy setting preferences before signing up to a new system. The system then predicts the answers of the other 75 questions related to privacy setting preferences. This scheme is based on the uses of support vector machines (SVM) to predict users' personalised settings. The second scheme implemented an additional layer that includes clustering.

In the second approach in this direction of research aimed at easing the tediousness and complexities involved in understanding and changing privacy settings, we considered the effect of users' settings preferences and personal attributes (e.g., gender, age, and type of mobile phone) on the prediction accuracy [13]. Models built on users' privacy preferences have shown an overall increase in the accuracy of the scheme. However, user attributes, such as gender and age, do not show a significant effect on the accuracy of the system. Therefore, service providers could minimize the collection of user attributes and based the prediction only on users' privacy preferences.

While conducting a series of studies in the problem domain, we observed that the users have little idea as to how the algorithms were generalizing their predictions. Thus, the need to have a transparency and explainability features become paramount. Hence, we enhanced the default privacy setting prediction approaches with an explainability feature [14]. Compared to the approaches introduced above, this approach presents an improved feature selection, increased interpretability of each step in the model design and enhanced evaluation metrics to better identify weaknesses in the model's design before it goes into production. This feature achieves the aim of providing users an explainable and transparent tool for default privacy setting prediction which users easily understand and are therefore more likely to adopt and use.

2.4 Summary

The section presents the results of three research efforts on improving usability to advance data privacy and protection. The first study details the way some properties that are tied to providing privacy and protection and dictate the usability of a product affect the end user's choice to use the product. For instance, the perception of smoothness was identified as a key element for identity management tools. Also, there was an emphasis on the need to consider privacy/usability trade-offs, from users that are mostly concerned with

comfort to people that want to have as much control over privacy as possible. Overall, this research was tied directly to user experience and how they perceive usability.

The second study is the complete opposite: It improves the usability for the service providers when they are ensuring the privacy and protection of end users' data. End users never have to know or see these steps, and it makes no difference to their experience. The third study splits the difference between the first two. By adjusting the service provider's way of setting up users' privacy preferences, they directly affect the user experience. If the predictions are good, users never have to do anything, while if the predictions are not to the users' taste, they can still change them. The end result is improved usability for end users because they are spared the hassle of setting up their security preferences.

When discussing security and privacy requirements from the service provider point of view, one of the more well-known requirements that also received a lot of attention from media and businesses is the GDPR. DPIA is required under the GDPR and its purpose is to identify and minimise personal data protection risks by systematically analysing the processing of personal data. Moreover, privacy-by-design and privacy-by-default are fundamental concepts in the GDPR that direct the development of new products and services from the onset. In this Section we have provided ways to address the requirements of the regulation in a usable manner.

3 Tools to Elicit and Fulfill Security Requirements

This section is focused on the theme of security requirements. We present here approaches on eliciting these requirements and research on fulfilling different requirements.

3.1 Serious Games to Prevent Social Engineering

Social engineering is defined as a technique that exploits human weaknesses and aims to manipulate people into breaking normal security procedures [15]. As discussed in the deliverable D3.10 *Cybersecurity Outlook I* it is expected that machine learning techniques surface as new powerful tools in the social engineering area [16] while defenders still have a lack of tool support [17].

3.1.1 State of the Art

Schab et al. examined the psychological principles of social engineering and which psychological techniques induce resistance to persuasion applicable for social engineering [18]. Based on the identified gaps [19], the serious game HATCH [20] is proposed to foster the players' understanding of social engineering attacks. When playing HATCH, players attack personas in a virtual scenario based on cards with psychological principles and social engineering attacks. While personas are by definition imaginary, they provide a realistic descriptions of stakeholders, or in this case employees, who have names, jobs, feelings, goals, and certain needs [21]. This way players can learn about the attackers' perspectives, their vulnerabilities and get a better understanding of potential attack vectors. Serious games are more entertaining and engaging than traditional forms of learning and have demonstrated a potential in industrial education and training disciplines [22].

However, HATCH can not only be used for training purposes but also to elicit security requirements to prevent social engineering [23]. Instead of the virtual personas, players describe social engineering attacks on their colleagues (realistic scenario). Since players know their colleagues, no persona descriptions are necessary and players can exploit their knowledge about processes in their work environment, i.e., about how to cut through the red tape and informal ways of handling tasks. Thus, at the end of the game a list of potential attacks can be investigated by the IT department.

Based on the derived security requirements it is possible to adapt the organization's security policies. Since security policies are documents often unread by the users, the serious game PROTECT was developed to train users in behaving according to the organization's security policies [24]. PROTECT is the further development of PERSUADED [25] with the improvement of making the game more configurable. Both games are digital card games where players have to defend against attacks with the correct defences in solitaire like game type. Special cards allow users to peek on the card pile and avoid attack cards where they do not hold the corresponding defences.

3.1.2 Challenge Beyond the State of the Art

Similar to awareness campaigns, the scope of serious games such as HATCH should be as specific as possible to the target audience [26]. Thus, there is the challenge to create virtual scenarios specific to the players' working environments. Furthermore, playing HATCH in a realistic environment might put sensitive

data of the players at risk, thus a legal assessment is needed to evaluate in which cases the game can be played without hesitation.

Another challenge is to address the attackers' adaption of attacks. Naturally, the time span from discovering new types of attack, adapting the security policies and training the players in the new security policy is too long to be an effective tool. During the process of improving the security policies, the attacker might already have changed their attack theme.

3.1.3 Systematic Scenario Creation for HATCH

We have addressed the requirement of adapting the underlying virtual scenarios for HATCH. For that purpose, we propose a systematic approach based on grounded theory (cf. Figure 3 and Figure 4 [27]) similar to the approach introduced by Faily and Flechais [21]. By conducting interviews with relevant stakeholders, systematically coding the answers, and grouping the codes, different properties for the personas can be derived [27]. We have evaluated the approach by building a virtual scenario for consultant companies. The approach worked well and we obtained a reasonable scenario. However, the approach was quite time consuming, thus we propose further research in lightweight approaches which allow the creation of appropriate scenarios with less effort.

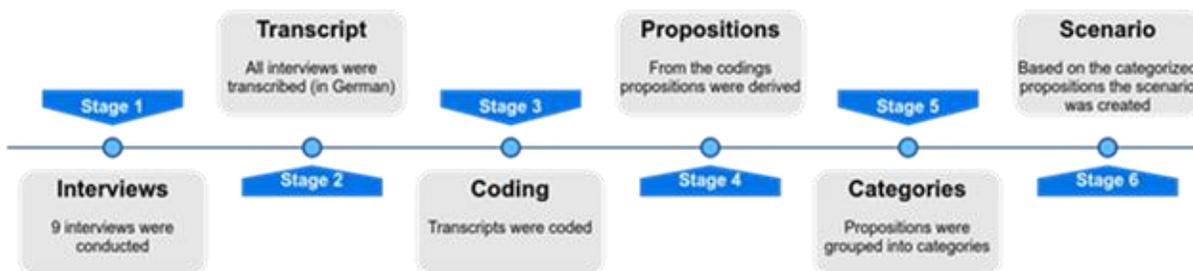


Figure 3: Steps of the systematic scenario creation.

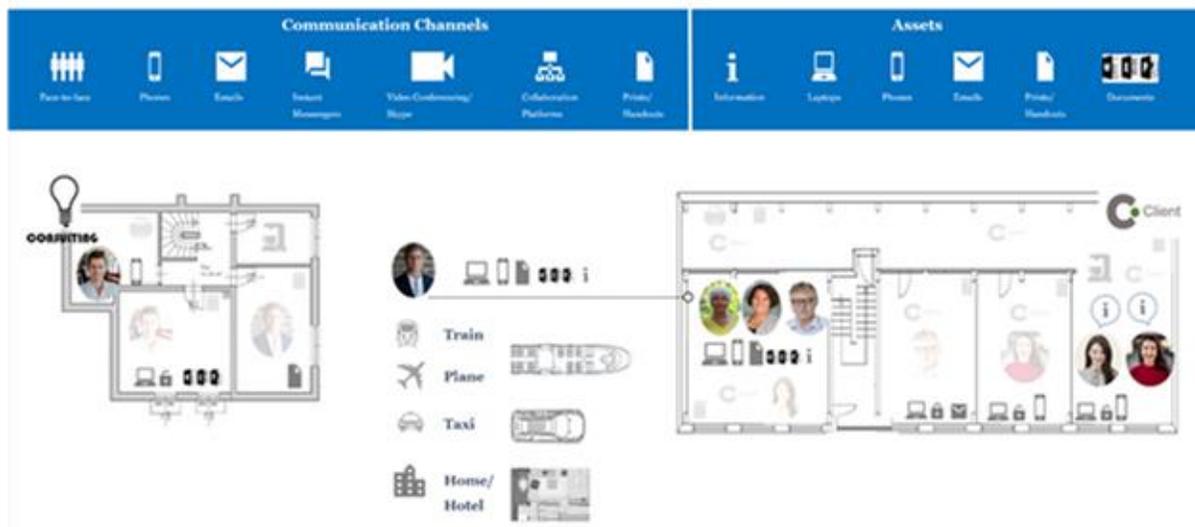


Figure 4: Derived scenario for a consulting company.

3.1.4 Legal assessment for HATCH

When playing HATCH with a realistic scenario, the employees' personal information might be at risk if players use it to describe their attacks. Legal requirements demand a careful consideration of when the game can be used. Therefore, we provide a legal analysis of the requirements to use HATCH for threat elicitation [28]. The main outcome is that the virtual scenario may be used without hesitation while the realistic scenario should only be used for threat elicitation.

While the assessment was specifically investigating HATCH and one would need to do a legal assessment for each considered serious security game before playing it in an official context, some general conclusions can be drawn. The most important question arising is if employees' personal characteristics are subject to the game. If they are, the organisation needs a justification why a more gentle type of training without considering the employees' personal characteristics is not appropriate. This could be the case if the organisation wants to conduct a threat analysis, for example because there already have been some incidents or the organisation is specifically exposed social engineering attacks and wants to mitigate that.

3.1.5 CyberSecurity Awareness Quiz

Since attackers adapt their attacks based on recent events, e.g., such as the COVID-19 pandemic [29], and naturally security policies can not be adapted too often and fast enough, it is also important to raise the employees' awareness about recent attacks or attack variations. For that purpose, we propose a CyberSecurity Awareness Quiz [30] which allows to add new content without too much effort. The cascade of games and how the CyberSecurity Awareness Quiz relates to HATCH and PROTECT is shown in Figure 5 [31] and has also been integrated in the TREAT-ARREST¹⁰ project's cyber ranges platform [32]. Figure 6 shows the user interface for the players. We also proposes a process for the timely development of new

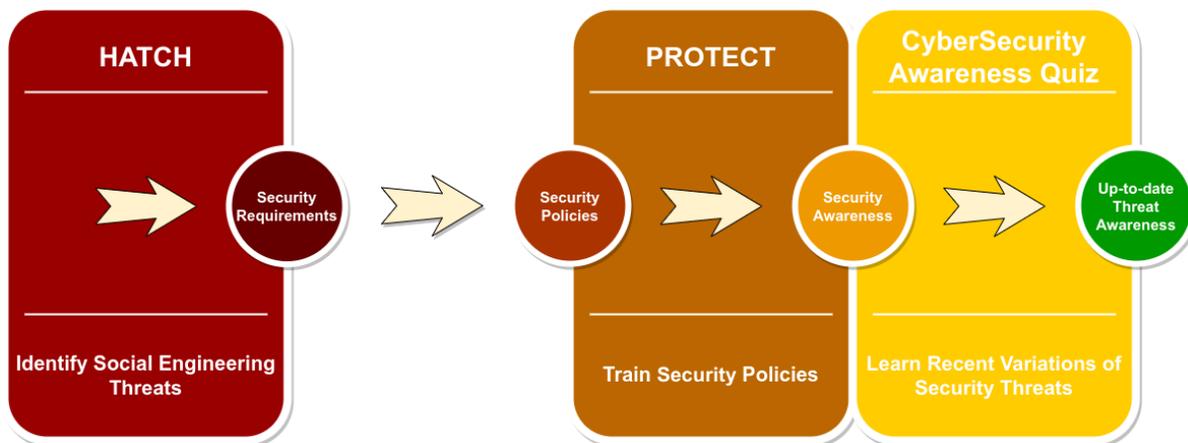


Figure 5: Relation between HATCH, PROTECT and CyberSecurity Awareness Quiz.

¹⁰ THREAT-ARREST was an EU-funded project (grant agreement No 786890) aiming to develop an advanced training platform incorporating emulation, simulation, serious gaming and visualization capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk cyber systems and organizations to counter advanced, known and new cyber-attacks.

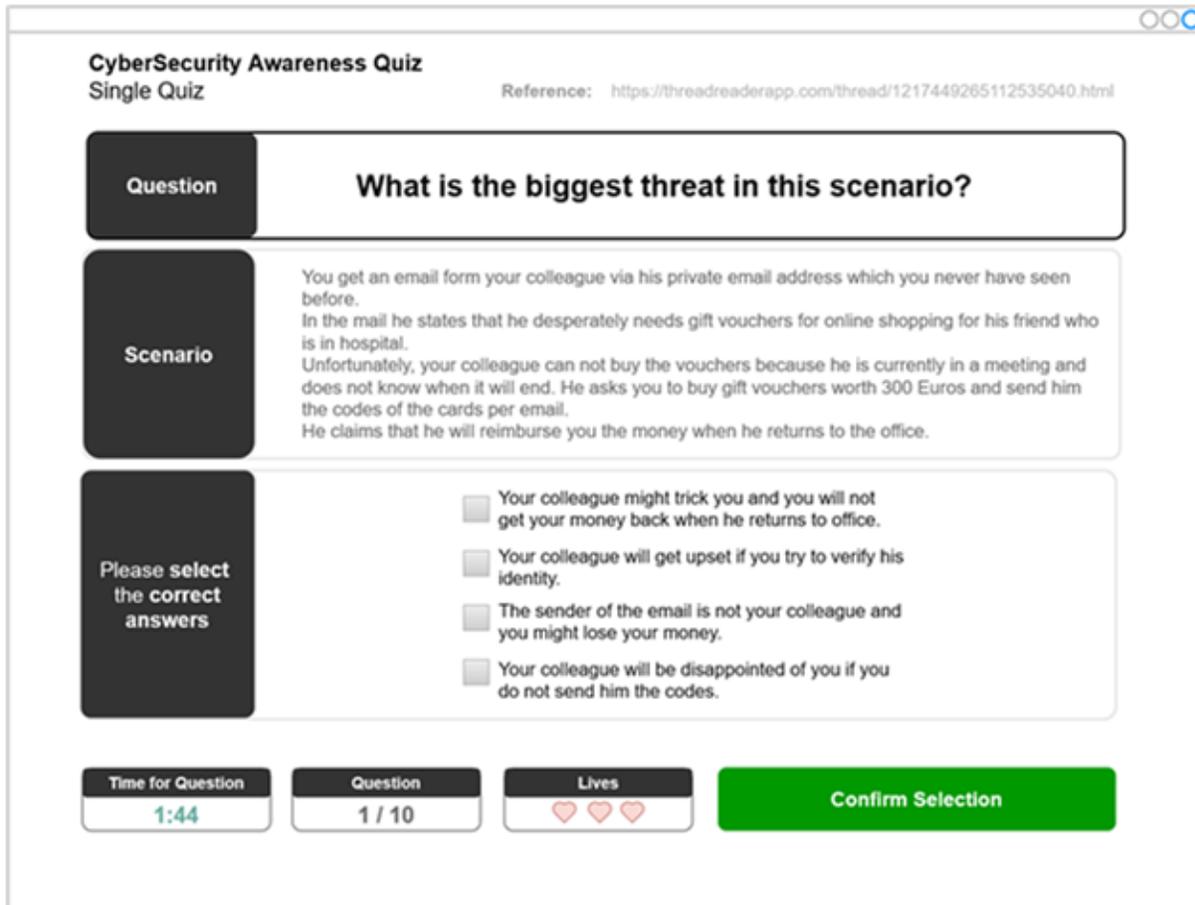


Figure 6: Player’s user interface for the CyberSecurity Awareness Quiz.

questions based on recent attacks. For that purpose, several relevant news feeds and websites are used as input. If adequate attacks are identified questions on the attack are derived along with correct and incorrect answers. The quiz content editor may then group selected questions to form a quiz or select all questions matching a certain keyword. In future work we intend to investigate by user studies if the implementation is also perceived as lightweight by the players and if players perceive the game suitable for occasional playing.

3.2 Input Data for Security Risk Assessments

One common challenge for security risk assessments is to get the data for the assessment and to assess its quality. We propose a method to assess security risks for cloud service providers (CSPs) which makes use of public available data and also discusses how to process the data to be usable for the suggested approach. Furthermore, we investigated the quality of maturity level assessments for security controls.

3.2.1 State of the Art

In the last ten years cloud computing has developed from a buzz word to the new computing paradigm on a global scale. Computing power or storage capacity can be bought and consumed flexibly and on-demand, which opens up new opportunities for cost-saving and data processing. However, it also goes with security concerns as it represents a form of IT outsourcing.

Stankovic and Pape [33] provide a qualitative in-depth examination of companies' attitudes towards security in the cloud. They investigated how security concerns manifest as a decisive factor in cloud provider selection using information gathered from interviews with eight practitioners from German companies. The underlying problem of service selection has been widely investigated both in the context of web services and cloud computing. Most of the works adopt different techniques to comparing and ranking CSPs such as genetic algorithms [34], ontology mapping [35], [36], game theory [37] and multi-criteria decision making [38], but did not consider security as an evaluation criteria.

There are specific approaches to support cloud customers with the security assessments, e.g. Bleikertz et al. [39] propose a systematic analysis of attacks and parties in cloud computing to provide a better understanding of attacks and find new ones, but many of them are not focussed on ranking. Only few works consider security as a relevant criteria for the comparison and ranking of CSPs [40], [41], [42], [43], [44], [45], [46], but none of them provided a way to assess and measure the security of a CSP in practice.

Information security risk assessment frameworks support decision-makers in assessing and understanding the risks their organisation is exposed to. Naturally, all of these frameworks require some input data on security practices which can be very challenging to gather. In general, frameworks require information on the organisation's security practices and organisational characteristics and combine that data with domain-specific information (e.g., attack scenarios for a specific domain or importance of those controls) to assess the organisation's security level.

One of these frameworks, LiSRA [47], is a lightweight, domain-specific framework based on attack-trees. Users provide a self-assessment [48] of the organisation's maturity level of ISO/IEC 27002 security controls via a web-based platform [49]. Results are illustrated in a comprehensible way so that decision-makers can intuitively understand what the metrics indicate [50]. The framework was evaluated with German energy providers, since along with other requirements the German critical infrastructure programme required them to implement information security management system [51], [52]. Another framework [53] is based on the analytic hierarchy process, and combines priorities for the different ISO/IEC 27002 security controls with their maturity to derive a security assessment. It was evaluated with real data from the eCommerce domain from a large international media and technology company [54].

Both frameworks have in common that domain experts initially provide domain specific information on the importance of different security controls which is then combined with information from the users about the maturity of these security controls. The latter is often done based on some maturity levels such as COBIT maturity levels.

3.2.2 Challenge Beyond the State of the Art

The challenge in defining an approach to select a secure CSP consists of not only proposing a method of comparison but also including a method how to get the data needed for the comparison of CSPs. Closest to solving that challenge is the work from Patiniotakis et al. [44] who refer to the Cloud Security Alliance's (CSA) registry of cloud service providers, but do not elaborate how this data should be used.

Maturity models are a widely used concept for measuring information security. The idea is to systematically evaluate the maturity of security-relevant processes in an organisation. Maturity models thus play a central role in the conception of information security management systems. Some industries, for instance, the

German automotive industry, have even established security maturity levels as the de facto standard for measuring information security. However, the quality of security maturity level assessments has not been sufficiently investigated yet.

3.2.3 Selection of a Secure Cloud Computing Provider

To the best of our knowledge all existing approaches for cloud provider selection lack a source of input data or the description how it should be used for the proposed approach. Therefore, we propose an approach [55] which makes use of a self-assessment questionnaire named Consensus Assessment Questionnaire (CAIQ) by the the Cloud Security Alliance (CSA). The questionnaire consists of a set of questions that providers should answer to document which security controls their cloud offerings support.

We first conducted an empirical study to investigate if comparing and ranking the security posture of a cloud provider solely based on CAIQ's answers is feasible in practice. Since the study revealed that manually comparing and ranking cloud providers based on the CAIQ is too time-consuming, we designed an approach that semi-automates the selection of cloud providers based on CAIQ (cf. Figure 7 [55]). The approach uses the providers' answers to the CAIQ to assign a value to the different security capabilities of cloud providers (step 1). Tenants have to map their security requirements to categories and prioritize them (step 2). With that input, our approach uses an analytical hierarchy process to rank the providers' security based on their capabilities and the tenants' requirements (step 3). Our implementation shows that this approach is computationally feasible. The most time consuming step is the assessment of the providers' answers, but it only needs to be done once as the results can be reused in further security comparisons.

3.2.4 Empirical Analysis of Practitioners' Assessment Capabilities

The aim of our study was to analyse to what extent security managers can accurately assess the maturity levels of security controls. To verify the quality of maturity level assessments, a case study was conducted where security experts assessed a subset of the ISO/IEC 27002 security controls for a hypothetical scenario using the COBIT maturity levels [56]. Additionally, ex-post interviews have been conducted with several study participants to verify some of the hypotheses developed during the previous analyses.

For the case study, a hypothetical infrastructure, including security measures and processes, of a small company was presented to the participants (cf. Figure 8 [56]). The description of the scenario was systematically constructed to represent predefined maturity levels for a number of the scenario's security controls. The participants' task was then to assess the maturity levels for these controls, and also to provide a rationale for their decision. These data build the basis for a quantitative and qualitative analysis on the quality of their assessments. The results show that many security experts struggled with the task and did not perform well (cf. Figure 9 [56]). However, we discovered professional characteristics that have a strong significant effect on the assessment capabilities, i.e., practitioners with security certificates had better assessment results. Moreover, the experts' self-perception was overly optimistic when asked to assess their performance. A weak negative correlation was found between the practitioners' performance and their estimated performance, also known as Dunning-Kruger effect.

Furthermore, various types of additional support could be identified that might help practitioners to make more reliable assessments in practice. Those include discussions of the assessments between two or more assessors, catalogues of measures fulfilling the security controls or training courses specifically on the assessment task. The practitioners need support to carry out high-quality assessments.

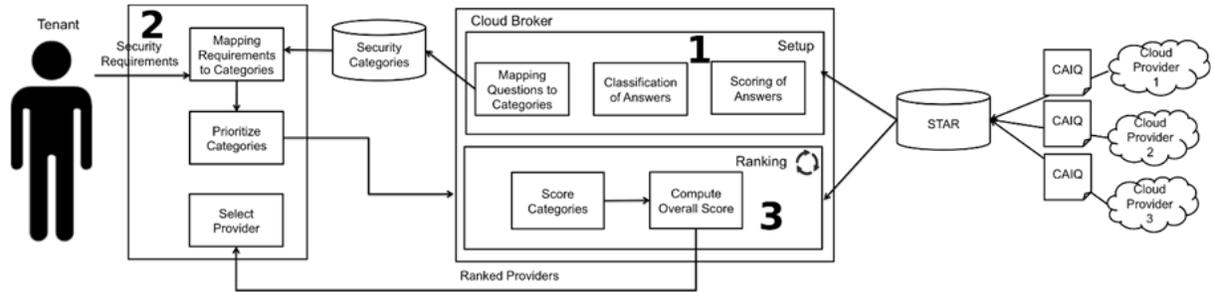


Figure 7: Overview of our approach for secure cloud service provider selection.

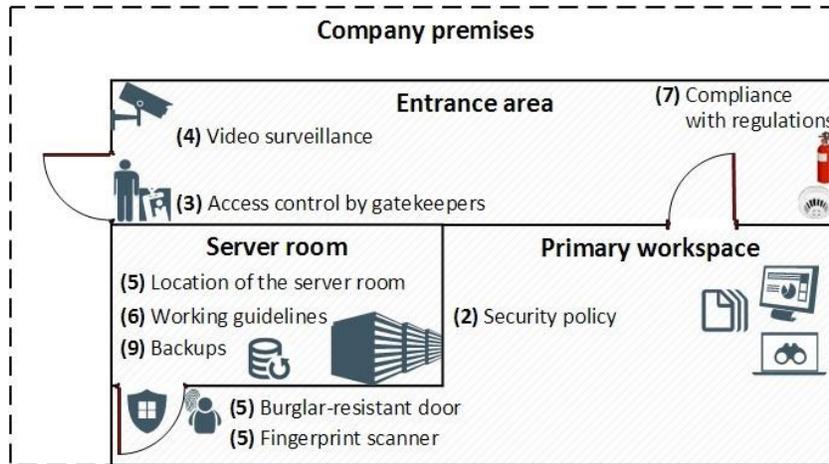


Figure 8: Visualisation of the experiments' scenario.

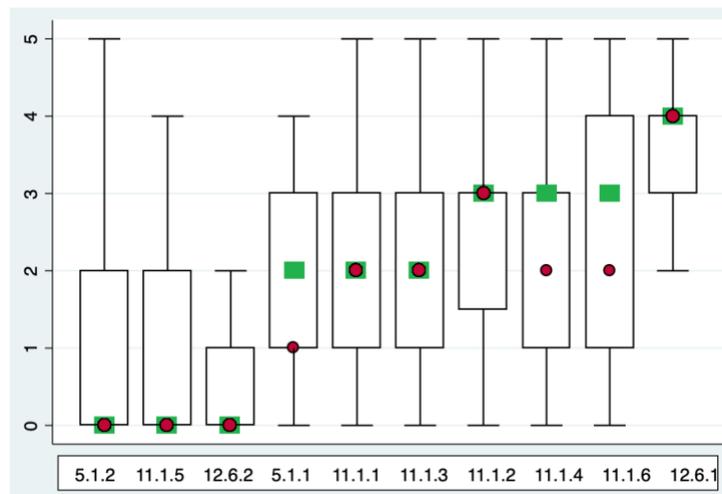


Figure 9: Results of the practitioners' assessments for each control; red circles indicate the median of the practitioners' answers; green rectangles indicate the scenarios' maturity levels.

3.3 Privacy Notifications

Privacy notifications facilitate transparency by providing users with situational awareness about the processing of their personal data and can, as part of transparency enhancing tools (TETs), provide important building blocks for privacy-preserving identity management systems enabling data subjects to make informed decisions.

3.3.1 State of the Art

Usability aspects of transparency enhancing tools (TETs) have mainly been studied for privacy notices that are presented to users *ex ante* [57], i.e., before they disclose personal data. A survey of *ex post* TETs, which enhance transparency of the processing of data after they have been disclosed, is provided by [58]. Our work researches the usability of *ex post* privacy notifications, which is a special form of communication for enhancing *ex post* transparency.

Other related work on *ex post* privacy notifications are for instance provided by [59] and [60] targeting Android app permission settings, and the usability of a feedback mechanisms for contextual messaging, which notifies users whenever a querier requests access to their personal data related to her working context or location [61]. However, their work addresses other application areas and a smaller set of notifications than analysed by our work.

Wu et al. [62] researched the impact of the design of security notifications on users' perceived security. They observed that “app users routinely ignore security notifications” and that mobile security notifications that are disruptive may cause irritations. These results motivate us to investigate user preferences for privacy notifications and their signaling modalities that will be meaningful for the users, will not be ignored or be perceived as disruptive, and will thus facilitate usable transparency.

3.3.2 Challenge beyond State of the Art

The research reported in this section extends our previous work [63] investigating the structural clustering of privacy notifications based on content into the three classes or privacy notifications: privacy breach notifications, notifications about privacy consequences, and privacy tips that provide customised recommendations aimed at enabling users to improve their privacy. Our study addresses the following research questions:

- To what extent do users find different types of privacy notifications useful?
- To what extent do cultural context, demographics, usage characteristics, the option for intervenability, as well as the type, timing, and modality of privacy notifications serve as determinants that help predict suitable notification settings for users of m-health services?

3.3.3 Summary of Key Results

For eliciting determinants of notification settings in the context of personal health tracking, we conducted two online surveys including English-speaking (C_{Eng} : $n = 154$) and German-speaking (C_{Ger} : $n = 150$) participants to elicit determinants of notification settings in the context of personal health tracking. Results of our study are published in Murmann et al. [64] and extracted from this article below with an emphasis on design requirements and guidelines for transparency enhancing tools (TETs) that we could derive.

We found evidence for the perceived usefulness of privacy notifications, and for concordant predictors in terms of when and how users prefer to be notified about personal data processing in 12 scenarios related to

personal health tracking. The results of our study provide quantitative evidence that determinants exist for customising privacy notifications. The determinants surface in the form of cultural context, demographics and predisposition, and in that the participants' right to intervene in the processing of their personal data affects their choice to be notified. Moreover, the results indicate that the participants of two online surveys appreciated receiving privacy notifications to help them improve their privacy. Analysing when, how, and what scenarios they preferred to be notified about provides us not only with insight about their notification preferences, but also yields a two-fold segmentation that subdivides scenarios into high- and low-priority notifications.

Based on the elicitation of the respondents' notification preferences, we are able to infer a series of design guidelines for usable TETs that facilitate transparency by harnessing privacy notifications. Our research was conducted in the usage context of fitness tracking. As people perceive health data as more sensitive than other types of data [65], our results on notification preferences may differ from other application areas.

Nonetheless, we found that determinants for privacy notification settings exist for a specific context, which leads us to believe that such determinants can also be found for different contexts. Moreover, some of our findings on cultural differences are also backed up by research on cultural communication and thus seem to be generally valid. Further research will be required to verify to what extent preferences for privacy notifications apply in general, or how they differ from application contexts other than fitness tracking.

A majority of participants found notifications useful and the perceived usefulness correlated with the request for notification. Most preferred immediate delivery. Notification based on email was chosen most frequently followed by system notification and pop-up. In general, participants who preferred to be notified were also more likely to choose immediate delivery, a wide variety of notifications, as well as more salient signalling.

Scenarios had a noticeable impact on the decisions of C_{Eng} . For C_{Ger} , it was still noticeable for notification request and timing, but not so much for modalities. We found a two-fold segmentation that clusters scenarios into whether respective notifications warrant high- or low-priority delivery. Finally, intervenability had a weak impact on scenarios related to breaches (B1 - B4) and consequences (C1 - C4).

Moreover, our findings show also that C_{Eng} was less concerned and found privacy notifications less useful than C_{Ger} , which can be explained by Hofstede's cultural comparison findings [66] showing that the UK in contrast with German speaking countries has a low score on uncertainty avoidance, and hence, UK citizens are higher risk takers who feel more confident with ambiguity than German speaking Europeans.

3.3.4 Implications for the Design of TETs

Drawing on our findings, on legal requirements and on findings from the literature, we infer the following requirements in the form of qualitative guidelines regarding the design of usable ex post TETs employed in fitness tracking scenarios.

Default settings: The positively attributed valuations of our participants' request for notification across all 12 scenarios indicate that the default practice of a TET should be to send the privacy notification in question. To avoid spamming users with notifications they may not be interested in, receiving tips would be optional. This would implement default-on/opt-out, which is in line with the data protection by default principle stipulated in GDPR Art.~25. All notifications should be delivered immediately via email.

Selectable profiles: Selectable bundles of settings could consist of profiles that represent either high- or low-priority scenarios. Notifications classified as high-priority might, for example, be delivered immediately, whereas the delivery of low-priority scenarios, e.g., tips, could be postponed until the evening. As our results show that scenario-specific differences existed for modalities (emails, pop-ups, and system notifications) among C_{Eng} but hardly for C_{Ger} , culture-specific profiles should further be considered. As vibration, audio and LED were hardly chosen as signalling modalities, they should per default not be included in profiles.

Fine-grained customisation: The diversity of the responses of C_{Eng} in contrast to C_{Ger} suggests that there are cultural differences in regard to how far users benefit from fine-grained customisation. TETs might therefore enquire users about their future plans when the TET is first put into operation, and suggest further customisations 'on the fly' once a change of the user's usage pattern is detected [67], [68]. Approaches based on machine learning, such as suggested by Liu et al. [59], might accommodate initial preferences and culture-specific profiles, recommending adaptive changes towards different profiles depending on a user's behavioural pattern. With a machine-learning-based customisation based on culture-specific profiles, users with different cultural backgrounds may be guided differently to change to suitable culture-based profiles while using the system.

Archiving: Since email was the predominant modality across all scenarios, we hypothesise that our participants considered privacy notifications important enough to warrant post processing and archiving. The notion of storing messages is congruent with what Murmann designates a means of 'preventing user errors' [68], such as when a notification is accidentally dismissed, or when users want to refer back to messages at a later time.

Guidance: Intelligible facts will be required to facilitate transparency and to enable data subjects to make informed decisions [69]. A considerable proportion of the respondents did not specify how intervenability affected their request for notification. Hence, brief descriptions may not suffice to clarify the potential consequences of taking action in response to receiving notifications. TETs should therefore not only point out facts but also provide suitable secondary clarification on request. Customised guidance will help accommodate the needs of users with different backgrounds and levels of knowledge. To avoid imposing unnecessary cognitive load on users, secondary information could be implemented as multilayered information [70].

Intervenability: TETs have the potential to guide users in exercising their right of intervenability. However, our findings indicate that the concept of intervenability and the options it entails are not common knowledge. Moreover, a recent Eurobarometer survey [71] showed that about one third of EU citizens are not familiar with their legal rights stipulated by the GDPR. In addition to providing clarity about the facts of how personal data have been or will be processed, TETs may therefore provide users with actionable choices that enable them to make follow-up decisions based on the information at their disposal [72], [73]. Receiving customised advice about suitable options, the follow-up steps required, and the consequences that will arise when taken, may enable users to weigh up individual options against each other [74]. Respective advice may also provide the insight necessary to weigh up these options against not to acting at all.

Data protection by design and default: It is worth mentioning that personal information conveyed by privacy notifications needs to be protected in compliance with Art. 25 GDPR. This means that personalised privacy notifications related to sensitive medical data (such as "XYZ could learn that you have a high risk

of diabetes”) should, at least per default, not be conveyed via pop-ups or audio messages. Users may not have full control over who else in their proximity might learn about such facts. Such messages should instead be framed in general terms (such as “XYZ could profile your health status. More details can be retrieved here”) and provide a link or button to secondary information. This motivates a multilayered design that facilitates transparency by revealing details on request [70].

3.4 Adaptive Authentication

In this section, we discuss the state of the art on adaptive authentication, the contextual factors and the requirements related to adaptive authentication, and how do the contextual factors and the requirements inform the adaptive authentication system activities.

3.4.1 State of the Art

An adaptive authentication system monitors contextual factors and behavioural features of its users to identify changing security risks. The system can decide to enforce an authentication method to mitigate the security risks and maximise user convenience [75], [76], [77]. For example, Hayashi et al. [78] associate a risk level with the location from where a user requests access (home, work, other). They change the authentication method adopted depending on the user’s current location. If the user tries to access a service/resource from a previously unknown location, they are required to provide additional credentials (e.g., pin, password). Security risks can also be brought by changes in user habits. For example, Gebrie and Abie [79] consider the change in users’ daily routines (e.g., walking, eating, sleeping) monitored using wearable devices, to calculate the risk score of an access request. They link the risk score to an abnormal activity and adapt the authentication method accordingly. Similarly, Bakar and Haron [80] analyze the historical records of the users’ behaviour profile (e.g., login time, location, browser type) and associate a trust score to behaviour changes. If the trust score is higher than a given threshold, the user is asked to provide additional credentials to access the required service/resource.

Continuous authentication [81], instead, refers to the activities performed after a user has authenticated successfully, to ensure that the session continues to be held by the legitimate user. It also aims to ensure that the user experience is maximized, for example, by reducing the frequency with which a user is required to re-authenticate. A continuous authentication system usually monitors the user behaviour (e.g., applications usage, pressure on touch screens) to identify security risks arising after a user authenticates successfully. For example, Karanikiotis et al. [82] monitor the users’ gestures (e.g., swipes) on a mobile device. If the user exhibits abnormal gestures, s/he is classified as an illegitimate user and the mobile device is locked automatically. However, this approach is not suitable when a legitimate user is simply performing a new behaviour. In such a situation, continuous authentication should be combined with adaptive authentication. For example, Jorquera et al. [83] uses machine learning to identify whether the owner of a mobile device is legitimate depending on their application usage statistics. The system considers the usage statistics falling in the possibly normal category to learn new behaviours, and triggers re-authentication if the authentication level score falls in one of the anomalous categories.

3.4.2 Challenge Beyond the State of the Art

Previous work on adaptive authentication [76], [77] provides limited guidance on how adaptive authentication systems can be built systematically. Thus, a number of open issues still remain:

- which requirements are relevant to an adaptive authentication system,
- how contextual factors can affect the feasibility of authentication methods,
- and how different authentication methods can affect satisfaction of the requirements.

Although previous work on adaptive systems has considered context-driven adaptation (e.g., [84], [85], [86]), it has not taken into account how context can affect the priority of the requirements and the feasibility of authentication methods. Also, authentication is highly personal, and users' preferences and privacy requirements can affect adaptation decisions.

3.4.3 Requirements, Authentication Methods, Contextual Factors, and Decision Techniques

To know what are the contextual factors, and requirements related to adaptive authentication, we reviewed previous work on adaptive authentication to elicit the main aspects to be considered when building an adaptive authentication system: requirements, authentication methods, contextual factors, and decision-making techniques.

Requirements: The requirements of an adaptive authentication system are mainly related to security, privacy, usability, and performance. The majority of the adaptive authentication systems (e.g., [87], [79], [80], [88], [89], [75], [78], [83], [90], [91]) that we examined adapt the authentication method as a result of a changing security risk. For example, De Silva et al. [75] link specific changes in the user profile (e.g., location, browser type, mouse behaviour, keystroke patterns) to changes in the security risk. When a high-security risk is detected, a stronger authentication method (e.g., two-factor authentication) is enforced. Daud et al. [89] link the user's login attempts to the security risk based on contextual factors, such as the IP address, location, type of browser, and the operating system. In case of an increased risk, this approach applies penalties, for example, it can adopt 2- or 3-factor authentication, it can block authentication for a given period of time, or blacklist a user. Although it has not been considered in previous work on adaptive authentication, an important requirement is authenticity.

Some approaches surveyed, especially those based on user behaviour and using physiological credentials, aim to satisfy *privacy* requirements, particularly anonymity and untraceability [92], [93], [94], [95]. For example, Xi et al. [94] propose an adaptive anonymous authentication protocol in a V2R topology based on a cryptographic technique called verifiable common secret encoding. This technique uses the cryptographic keys of the communicating users to hide their individual identities. The authentication protocol can also adapt at runtime depending on the level of anonymity required by the users.

Because authentication can be performed by humans, it is also crucial to consider *usability* requirements. These mainly aim to maximize the quality of the user experience during authentication. Usability has been mainly considered in terms of ease of use, for users having different behaviors [83], abilities [96], and ages [97]. Other work [98] has considered usability in terms of transparency, i.e., the system should provide users with explanations justifying why it changed the required authentication method. Usability is also commonly expressed in terms of efficiency and effectiveness of the authentication methods [99]. More precisely, *efficiency* is related to the speed of the authentication method. For example, Jorquera et al. [83] minimize the number of authentication credentials to improve efficiency. Effectiveness is related to the error rate that an authentication method can be prone to. This can be related to the memorability of the credentials (e.g., using a password that is difficult to remember can be ineffective) and also to environmental factors (e.g., noise type and level, lighting level, or temperature) [100]. Other work [90], instead, aims to maximize

satisfaction of the *user's preferences*, by allowing a user to select an authentication method for specific applications. This can be relevant when users prefer stronger authentication techniques in specific contexts: work, personal account, and financial [101].

Authentication Methods: The authentication methods that have been used in previous work have optional and mandatory authentication features. It is mandatory to choose a credential type [102], such as something you know (e.g., password, OTP), something you have (e.g., smartcard, token), something you are (e.g., face, iris, fingerprint), or two-factor authentication (e.g., select two credentials). The credential type affects the level of automation. For example, iris and face recognition have the highest level of automation, since they require the minimum input from the user. Fingerprint-based authentication has a medium level of automation since it requires the user to actively scan his/her finger. Password-based authentication has a low level of automation since it requires the user to remember and input a password. Some authentication features, such as credentials renewal [103], [98] and cryptography type [94], [102], are optional. Others require specific devices to be performed [101], [90] (e.g., smartcard-based authentication requires a reader). Representing the features of an authentication method can help express its impact on the satisfaction of the requirements.

Contextual Factors: We group contextual factors depending on whether they affect 1) the security risk and the adaptive authentication requirements or 2) the feasibility of authentication methods.

- Security risks and requirements
 - *Assets Sensitivity* refers to the criticality of data or applications to which access is requested. Asset sensitivity can increase the priority of security requirements and also affect security risks. Thus, some approaches (e.g., [90], [104]) adapt the authentication method depending on the sensitivity of the data to be accessed.
 - *Location* refers to the place where a user is authenticating and can have an impact on the security risks. Several approaches have proposed to ask the user for additional credentials, if s/he attempts to access services/resources from an unusual location [80], [88], [89], [105].
 - *Network Topology* can affect the security risk. Previous work [95] suggests to change authentication method depending on the attacks that can exploit the topology of the network a node is currently connected to.
 - *Time* refers to the moment when authentication is performed and can also affect security risks [80], [88], [89]. For example, if a user tries to access an asset in odd times (e.g., outside the working hours) s/he can be asked to provide additional credentials during authentication [80], [88] or can be subjected to penalties (e.g., being blocked for some hours or permanently) [89].
 - *User Role* (e.g., manager VS regular employee [106]) can affect the security risk. Arfaoui et al. [91] require the nodes of an Internet of Things (IoT) network to adopt an authentication method depending on their role (e.g., IoT gateway, context manager, data consumer) and also depending on additional contextual information (e.g., location, time, emergency situation, normal situation).
 - *Movement of the Nodes* refers to the movement of the nodes within a network. For example, in an IoV (Internet of Vehicles) network nodes can change their position, requiring authentication to be performed rapidly. Fayad et al. [107] proposed an adaptive

authentication approach where nodes of an IoT network can store their authentication information on the blockchain. This allows authentication to be performed even when the authenticating nodes do not belong to the same network.

- *User Preferences* refer to users favoring specific authentication methods to others [100], [90], [108], [80], [88]. Considering user preferences during adaptive authentication can increase satisfaction of usability requirements.
- Feasibility of authentication methods
 - *Authentication Devices* refer to the devices (e.g., phone, camera, reader) available to perform authentication. For example, some authentication methods (e.g., RFID) require additional devices (e.g., reader) [109]. In other situations, limited-resources devices may not be able to support authentication methods that are computationally intensive (e.g., cryptography-based authentication) [83].
 - *Proximity* refers to the user's distance from a device and can indicate possession of the device [110]. For example, two-factor authentication can be enabled by sending a PIN to the device a user is close to.
 - *Device Position* refers to the relative position of a device w.r.t. its owner (e.g., held on hand or in the pocket). For example, face recognition is not feasible if the device is held in the pocket. Frequent changes of the device position can make gait-based authentication infeasible [111].
 - *Network Quality* can affect feasibility of authentication methods (e.g., cryptography-based authentication) that can have overheads in the communication network. For example, in IoV the use of a network with limited bandwidth can cause delays and even lead to fatal accidents [95].
 - *Environmental Conditions* refer to conditions, such as lighting and noise level. For example, Wojtowicz and Joachimiak [100] propose a system that avoids selecting authentication methods that may not be effective in certain environmental conditions. For example, face recognition and voice recognition are avoided when the lighting level is low and the noise level is high, respectively.

Although we have identified relationships between contextual factors and requirements, existing adaptive authentication approaches have only focused on specific contextual factors relevant to the considered application domain.

Decision-Making Techniques: Various decision-making methods have been used in previous work on adaptive authentication. For example, machine learning has been used to learn the features characterizing the user's behaviour and the power consumption of the devices [111], [112], [90], [75], [83], [79], [78]. Rule-based reasoning has been used to adjust the authentication method based on the security risk [113], [80], [114], [115], [89], [104], [100]. Optimization methods have been used to select an optimal authentication method depending on environmental conditions [100], [116]. However, these techniques have only considered the impact of a small set of contextual factors on the feasibility of the authentication methods. Also, they have not considered how different authentication methods can affect requirements that are different than security.

3.4.4 Adaptive Authentication System Activities

In this section we show how we can use the requirements, authentication methods, and contextual factors to inform the adaptive authentication system activities using the MAPE-K loop. As shown in Figure 10, we use the main pillars of adaptive authentication (requirements, authentication methods and contextual factors) to represent and maintain at runtime the knowledge that is used to configure the activities of the MAPE-K loop [117]. The contextual factors can bring security risks and affect priority of the requirements. They can also make certain authentication methods infeasible. Authentication methods, instead, can mitigate security risks and contribute to the satisfaction of the requirements. During monitoring and analysis, the adaptive authentication system should, respectively, monitor contextual factors and analyze the security risks. During planning, it should identify a feasible authentication method that a) minimizes security risks and b) maximizes the satisfaction of the requirements considering their trade-offs. During execution, the adaptive authentication system should enforce the selected authentication method.

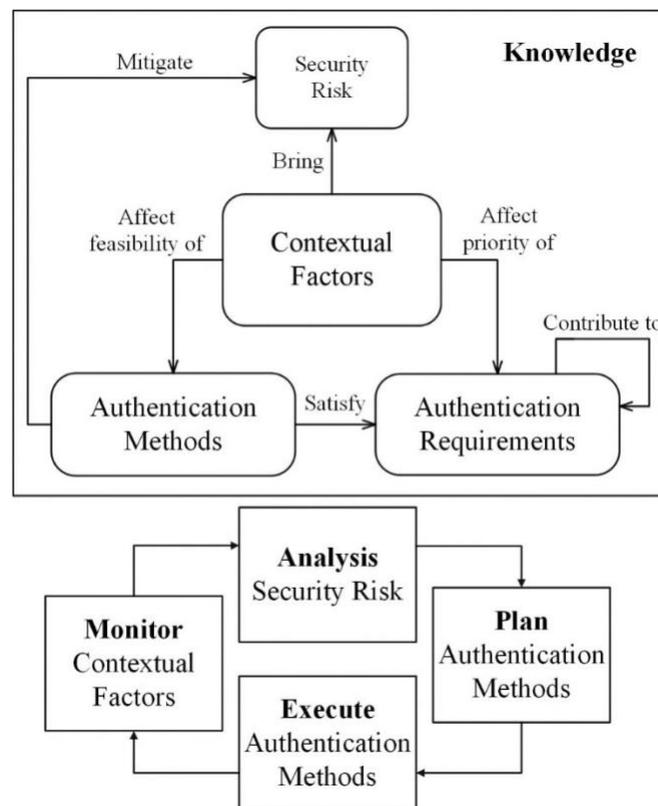


Figure 10: Adaptive authentication system activities.

3.5 Summary

In this section we have showcased different discovery tools or approaches for security requirements. First, we presented a way, in which security games, that are usually developed for training purposes, can be used to elicit security requirements. Security policies can be improved based on the requirements found.

However, because reading a policy is usually an unpopular activity, we propose additional serious games for training the policy and to enhancing the security awareness of employees.

Second, we discussed how to get data for security risk assessments and how to assess its quality in the context of cloud service providers. The security controls of CSPs and the priorities of tenants were used to rank the providers in a semi-automatic process. Furthermore, we studied how well the security managers are able to assess the maturity levels of security controls. The reliability of the assessments can be improved with, e.g., peer discussions or special training.

Third, we also found evidence for the perceived usefulness of privacy notifications, and for predictors on when and how users prefer to be notified about personal data processing. The cultural and personal predispositions of a user affect the customization of these notifications. From these results we can infer a series of design guidelines for usable TETs.

Finally, we proposed an adaptive authentication framework. Authentication is highly personal, and users' preferences and privacy requirements can affect adaptation decisions. Our framework, informed by previous research, characterizes the adaptive authentication problem and supports the engineering of adaptive authentication systems. Although we identified relationships between contextual factors and requirements (security and usability), existing adaptive authentication approaches have only focused on specific contextual factors relevant to the considered application domain. We demonstrated how it can inform the activities of the MAPE-K loop, upon which adaptive authentication systems are built.

4 Enhancing the Human Understanding of Security Solutions

This section discusses the third research theme of the task. We present ways to analyze and model user behaviour and the usability of products or services. We build frameworks for enhancing usability of security solutions. There are also examples on visualizing security to the user in order to empower them to make the right, i.e., secure, choices.

Our research was directed towards amplifying the awareness of the user on security. In addition to the more general analysis and modelling research we also 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.

4.1 Analyzing Usability and Security at Design Time

Security mechanisms are designed to protect users' assets by preventing a straightforward access to them, thus adding complexity to the user interaction with the system and ultimately degrading the system usability and, in particular the users' performance [118]. Designers and engineers of interactive systems thus require techniques and tools to analyze both usability and security when designing a security mechanism.

4.1.1 State of the Art

Despite of a large literature, very few works propose generic methods that can be used to compare diverse types of security mechanisms and systematically assess the trade-offs between security and usability. Alshamari [119] highlights the recurrent conflicts between usability and security. That author proposes a generic model of process to identify these conflicts between usability and security at design time, and to select a strategy to handle them using a decision support system for eliciting requirements. Other works employ inspection methods to analyze the effect of security mechanisms on the usability of an interactive system. Braz et al. [120] propose a set of heuristics and an inspection method for the analytical evaluation of the effects of security mechanisms on the system's usability of the system. Alarifi et al. [121] propose a structured inspection model dedicated to the analysis of usability and security of e-banking platforms. Bonneau et al. [122] propose a set of heuristics for comparing usability and security benefits between several authentication techniques. Such inspection methods and heuristics provide support to compare security mechanisms and to make tradeoffs during design. However, these approaches cannot ensure an exhaustive coverage of all possible user actions with the system and they might fail in detecting problems related to specific scenarios. Ben-Asher et al. [123] propose an experimental environment to collect systematically any possible user behavior facing security mechanisms. They propose to use the output of user tests run in the experimental environment to explore possible tradeoffs between security and usability for the system under design. That approach can help to identify usability problems and issues with security mechanism within tasks performed by users during the experimental phase. As such, the logistics required to run the user test limits the coverage of the study to a small subset of tasks that are possible within the system.

4.1.2 Challenge beyond the State of the Art

Security mechanisms may interfere with users' goals and tasks by adding articulatory activities, which affect each dimension of usability. The main challenge is to build a generic method that integrates systematic identification of user activities and main threats covered by the security mechanisms. This is needed in order

to enable the comparison of diverse types of security mechanisms and to systematically assess the trade-offs between security and usability.

4.1.3 A Generic Multi-Models Based Approach for the Analysis of Usability and Security at Design Time

Tasks models can be used to systematically analyse the impact of security mechanisms on usability, as well as how they can be used along with threat modelling techniques to analyse security [124]. First, the systematic identification of potential security threats on user actions and the effects of authentication mechanisms on user tasks requires the description of:

- user actions: a threat can arise from a type of user action, e.g., drawing a gesture password on a tactile screen is subject to smudge attacks whereas typing a password on a keyboard is subject to the key logging attack,
- their temporal ordering and/or temporal constraints: a threat can arise from the specific ordering of user actions, e.g., the user takes too long to input a pass-word,
- the information, knowledge and objects being manipulated during these actions: a threat can arise from an information, knowledge or object that the user has lost, forgotten or misused, e.g., a credit card lost in a public space.

Task modelling is a technique for identifying and representing this required information. We selected the HAMSTERS task modelling notation [125] as it provides all of the required notation elements listed here above. HAMSTERS (Human-centered Assessment and Modelling to Support Task Engineering for Resilient Systems) is a tool-supported task modelling notation for representing human activities in a hierarchical and temporally ordered way [125]. The HAMSTERS notation provides support for representing a task model, which is a tree of nodes that can be tasks or temporal operators (Figure 11) presents a

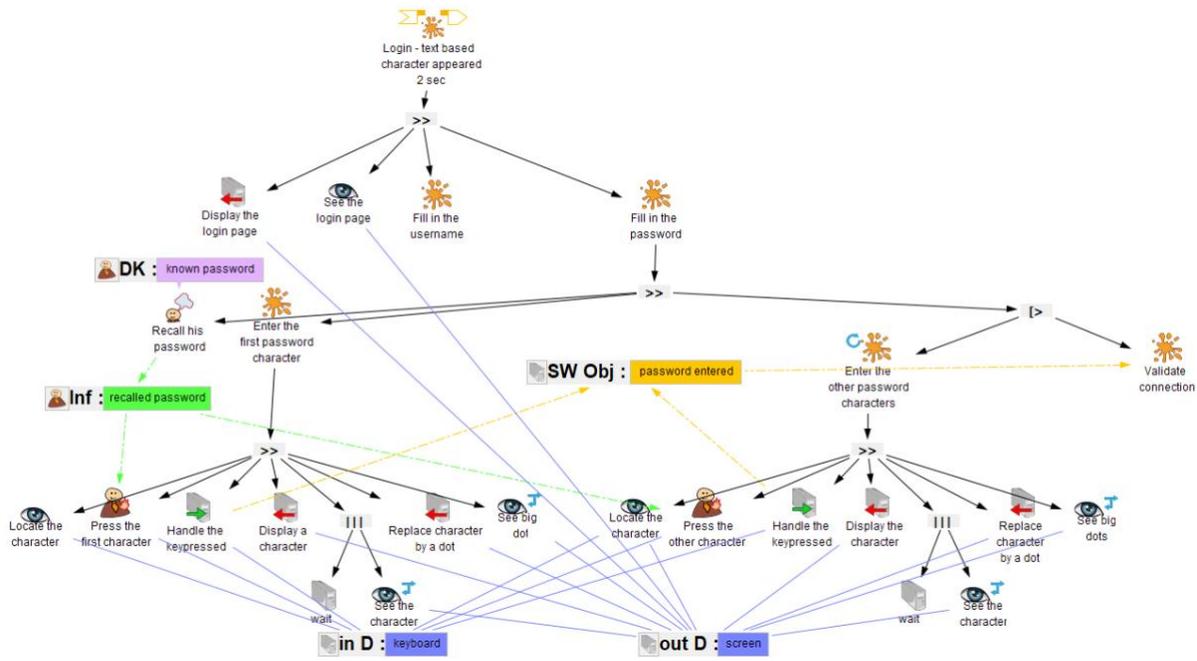


Figure 11: Example of task model describing user actions to log in.

HAMSTERS task models describing the user's actions to login). The top node represents the main goal of the user, and lower levels represent sub-goals, tasks and actions. Task types are elements of notation that enable to refine and represent the nature of the task as well as whether it is the user or the system who performs the task. In addition to elements of notation for representing user activities and their temporal ordering, HAMSTERS provides support to represent data (e.g., information such as perceived amount of money on an account, knowledge such as a known password), objects (e.g., physical objects such as a credit card, software objects such as an entered password) and devices (e.g., input devices such as a keyboard, output devices such as a screen) that are required to accomplish these activities.

Moreover, the systematic identification and representation of threats and effects of threats require a description of user actions and all possible threats that are not directly related to the user actions (e.g., network, electronic components...). Such information is essential to design and implement mechanisms to avoid or to mitigate the threats [126]. We selected attack trees to address security aspects as they are major tools in analyzing the security of a system [126].

Figure 12 presents an attack tree for a keyboard login authentication mechanism. They can be decorated with expert knowledge, historical data and estimation of critical parameters as demonstrated in [127]. Attack tree notation is a formal method to describe the possible threats or combination of threats to a system. B. Schneier [128] provided a first description of an attack tree, where the main goal of the attack is represented by the top root node and where the combinations of leaves represent different ways to achieve that goal. In the original notation, OR nodes refer to alternatives of attacks to achieve the attack whilst AND nodes refer to combination of attacks. Nishihara et al [126] proposed to extend the notation with potential effect of attacks and with a logical operator, SAND to represent constraints in the temporal ordering of combined attacks.

In order to identify and represent explicitly the security threats and effects related to user tasks and to their interaction with the security mechanisms, we have extended the HAMSTERS task model notation [124]. New elements of notation are: threat, effect of a threat, and the relationships between tasks, threats and

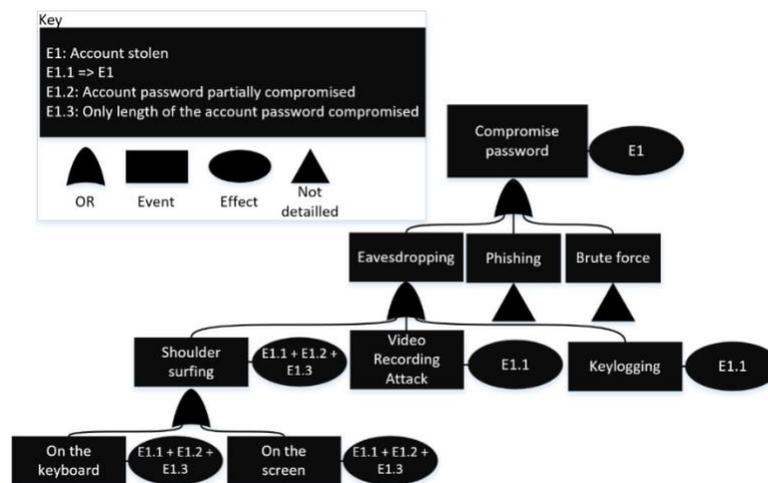


Figure 12: Example of an attack tree for a keyboard login authentication mechanism.

4.2 Utilizing Human Capabilities in Cryptography

It is a great challenge to present the security state of cryptographic operations, e.g., if a protocol has been executed correctly and without interference from malicious actors, to the user in an understandable way. Currently, the expectation is for the user to place blind trust in the digital communication system they need for everyday tasks. In this section we present an experimental proof-of-concept system, in which the user is involved in the different cryptographic processes. They can influence and oversee the communication and see the effect of interference from malicious actors. The intention is to build trust in the system by allowing the user to have agency in it.

4.2.1 State of the Art

Cryptography is a major building block of the modern digital society. However, it is realized with mathematical operations and represented in ways that are not readily accessible to human users, thus they are left out of the process of establishing trust. The seamlessness and user friendliness of human-machine interactions has been a topic of interest for both researchers and industry for a long time, but cryptography has not enjoyed much development in this direction. In this section we present the highlights of existing solutions, but there is a more thorough review on the topic available [129].

Modern cryptography is based on provable security: for a given cryptographic primitive or protocol there should be clearly defined security goals and proof. The security goals are supplemented with corresponding threat models. The proof, usually done by reduction, shows how and under what assumptions the proposed system achieves the goals. Naturally, any implementation of the system may have its own vulnerabilities and threats that were not covered by the original modeling, e.g., side-channel attacks using timing or power consumption. The current paradigm of provable security tends to leave the human users out of consideration when building the security models, which are based on the ubiquitous client-server model of communications. This model is of course perfectly adequate in machine-to-machine communications, but it cannot capture the human factor, which the user brings to the system.

There are a few notable exceptions for using human capabilities in cryptography, that have been studied in more detail. Firstly, there is *visual cryptography* [130]. A message is split into encrypted shares by a computer, and then a human user can decrypt the message by merely looking at the correctly positioned shares of the message. The message was a black-and-white image and the shares were printed on transparencies that were carefully stacked for decryption. Nowadays, there are several extensions to the original scheme, e.g., for using color images or rotation to encrypt more items into one share. Different kinds of visual cryptography schemes have been compiled and compared in surveys before, e.g., [131] and [132]. However, in most of the systems transparencies can at most be used once which may lead to usability issues [133] and requires a new security model [134].

Next, there is also the concept of *visualizable encryption*, which extends the normal CPA (chosen plaintext attack) and CCA (chosen ciphertext attack) adversarial models and respective security games more towards systems, where also the human behaviour and interaction with the different devices is taken into account [135]. The authors show that it is possible to construct CPA- and CCA-secure visualizable encryption schemes from respective regular encryption schemes together with secure hash and MAC functions. However, the system only implements symmetric encryption, which requires a key exchange between the

server and the user device. This key exchange is not defined to have any human verifiable or visualizable components.

Hashes are an important cryptographic building block. However, when the need to compare hash values arises, it is difficult for users to compare meaningless character strings. *Hash visualization* was proposed as a solution to this problem [136] and a survey of different techniques [137] was later published.

There are also different kinds of authentication methods of users, devices and computations that involve the user somehow. In these schemes the goal is that human users can verify the result of the authentication (e.g., device pairing) in a simple way. An analysis of some of these methods can be found in [138].

Many of the methods above do not have a security proof or the human element is not clearly present in the proof. There are, however, protocols for secure human authentication, e.g., [139] and [140].

Finally, a theory on *human computable functions* that could be utilized in cryptography has been proposed [141]. These ideas have been utilized in the context of password authentication [142], [143], but not more generally in cryptography. In comparison to the visual options discussed earlier, human computation schemes require more effort from the users, which is a major drawback for this approach.

4.2.2 Challenge Beyond the State of the Art

Even though there has been research on certain aspects and approaches of human-friendliness of cryptographic systems, there is a lack of complete systems that involve humans for the establishment of the whole communication pipeline. To fill this gap, we present EEVEHAC, the End-to-end Visualizable Encrypted and Human Authenticated Channel.

4.2.3 A Novel Human Authenticated Communication Channel with Visualizable Encryption

EEVEHAC is a system aiming to set up a secure channel between a human user and a server. Our implementation comprises two parts: first, a human authenticated key exchange protocol, based on [140], and second, a visual encrypted channel, based on [135]. HAKE protocol is used to authenticate the user. In our implementation, this protocol results in a 4-digit code, which is used to create encryption keys necessary in the visual channel phase. The reason for including the HAKE protocol in our system is to engage human users in the protocol and thus make the system more reliable and understandable from the human point of view.

Our HAKE protocol is based on a story and a mapping between colors and numbers. In the registration phase, the user gets a story, a mapping and a user number. All these are user-specific, meaning the same colors are in use for every user, but the colors correspond to different numbers for different users. The story is collected by picking up random words picked from a word database in a grammatically correct way. The user is able to swap certain words in the created sentences in the story generation phase. The user number is used to identify the user.

In the HAKE part, the server sets challenges to the user by picking one clause from the story, changing one word from it to another, random word, and then coloring all words in that clause with different colors. On the screen of their personal device, the user sees two clauses of this kind, and two additional clauses, which do not have anything to do with the story. The user must detect familiar clauses and spot the changed words in them. They then memorize which digits correspond to the colors of these words, count the sum of these

numbers and type modulo 10 of this sum to the device. This is repeated four times, resulting to a 4-digit UAN code. If both the user and the server calculated the same UAN code, the user is authenticated and encryption keys for the latter part can be successfully exchanged.

For the encrypted visual channel, EEVEHAC implements EyeDecrypt [135]. The system consists of three parts: a server, an untrusted device (that could be used in a public space) and user's trusted device (a smartphone). Having previously completed the HAKE protocol, the user and the server have matching keys to encrypt and decrypt data as well as to authenticate the data sent by the server.

The server sends encrypted data to the untrusted device, which then displays the encrypted data in the GUI as QR codes. The untrusted device does not have the keys to decrypt the data. The user uses their smartphone to scan the GUI and when the application detects all QR codes visible on the screen simultaneously, it decrypts the data and shows it to the user on top of the camera feed. If the data has been corrupted, the user will be able to notice it as the application cannot decrypt the data properly. Also, the position of the QR codes in the GUI is taken into account and the application will notice if the order of the QR codes is not correct.

A threat analysis of EEVEHAC was presented in [144], in which we considered the HAKE and EyeDecrypt phases separately first and then analysed the whole system. The first main threat concerning the HAKE protocol was denial of service, which could happen by, e.g., stealing the user's device. The second main threat was breaking the HAKE protocol and thus stealing encryption keys used in the latter phases. This could happen by eavesdropping the user during the authentication phase and conducting mathematical inference. Our UAN protocol did not provide very good security level towards this scenario. Some improvements to address this problem could be obtained by moderate changes in the protocol.

Since EEVEHAC implements the whole EyeDecrypt scheme, we assume that security proofs presented in [135] hold for EEVEHAC as well. For the visual channel, denial of service is naturally a threat, and can happen by, e.g., destroying the public device. When the user is using the visual channel in a public space, shoulder surfers can be assumed to be able to see the encrypted data and the user's inputs on the public device. Because the decrypted data is only shown on the smartphone screen, trying to see it is much more difficult for a shoulder surfer. If EEVEHAC was implemented on, e.g., smart glasses, shoulder surfing would be even more difficult.

An analytical modelling of usability of the visually encrypted part of EEVEHAC was conducted using HAMSTERS, see Section 4.1. Adding to that, we conducted usability tests with a small group of test persons not familiar with the system. All the test persons were given instructions about using EEVEHAC and they were asked to conduct registration to the service, human-understandable authentication and QR code scanning.

In our test setting, the users registered to the service on a laptop and then used a smartphone to execute the HAKE protocol and read QR codes on the screen of the laptop. During and after using the system, our test persons gave qualitative comments about usability of EEVEHAC. The HAKE protocol was considered most difficult and only one of the four test persons managed to conduct it successfully. The visually encrypted part was considered relatively easy, even though lighting conditions affected the performance of the smartphone when reading QR codes.

The most striking problem with the HAKE protocol was that it was considered laborious and complex. On the other hand, none of the test persons were willing to use several minutes to practice the protocol, even though all human-authenticated schemes are based on the assumption that the users spend some time to practice it. Thus, motivating people to devote their time to this kind of protocols remains a problem.

4.3 Formal Verification and Visualization of Security Policies

One common problem in the usability of security analysis tools, is the effective representation of information and analysis results. This is particularly true when the tool performs some form of exhaustive analysis that usually results in large and complex outputs. One of such case is addressed in this section where we consider the problem of formal analysis of policies in complex systems and the representation of its results. In particular, we focus on access control policy verification in large heterogeneous systems.

4.3.1 State of the Art

Policy-based management is a critical aspect to consider when dealing with the security of any computer system, computer network or device. A reliable policy system is necessary to ensure the correctness and consistency properties of the overall dynamic system. The scope of policy analysis is quite broad [145] and spans over computer network management and access control mechanisms. The former involves network policies that defined the requirements that a communication networks must satisfy, both in terms of performance, of functionalities and security. The latter mainly focus on specifying which subjects (either users, processes or applications) can access which resources (either physical or cyber). In case of a complex system where heterogeneous subjects can access different types of resources, the policy analysis is particularly important to discover potential *anomalies* in the policy definition or its implementation [146]. In the field of access control, this is particularly relevant as anomalies could result from a specific implementation of access control mechanisms or by the combination of different access control systems. However, in most of the policy analysis approach available in literature, the focus is on a specific aspects such as firewall rules, or embedded security mechanisms in operating systems or specific applications (e.g., database management systems). Such type of analysis is, of course, necessary to provide a solid foundations for any higher level complex system. However, it is not sufficient to address the problems with modern distributed systems where different types of subjects and mechanisms can interact in unexpected ways. To ensure that the performed analysis is able to take all the possibilities into account, an exhaustive analysis approach should be preferred. To obtain this result, in our contribution we leverage a formal analysis approach based on the models of the system components.

4.3.2 Challenge Beyond the State of the Art

The challenges we highlight here are twofold: From one point of view, we need to overcome the limitations of classic access control analysis approaches by considering complex interactions in high-level system components. On the other side, we need to provide a solution that is actually usable by system administrators, hiding the complexity of formal analysis results [147].

4.3.3 Formal analysis and complexity reduction to support usability

In large and heterogeneous network systems, where many different agents operate on system resources, the definition and implementation of security policies is of utmost importance. In particular, to provide a clear indication of who can access to which resources, specific access control policies have to be identified. One of the most widely used access control model is the role based access control (RBAC) one. In this model, users are assigned to roles, and roles are provided with permissions. A permission identifies an object (a

resource of the system) and an operation that can be performed on it. This abstract model must be then implemented in the low-level configurations of the security mechanisms provided by the nodes of the actual system. In the general case, it is not possible to assume that a centralized access control system is available that is able to configure each node. This is particularly true, for instance, for industrial control systems, where the heterogeneity of the devices used (in terms of configurability and capabilities) requires a finer approach to the evaluation of the available security mechanisms. In fact, some types of devices are not able to locally provide access control mechanisms and rely on proxies or gateways able to overcome this limitation. In such complex systems, the verification of the correct implementation of access control policies is a difficult task. One possible solution to this verification process problem has been proposed in the SYSVER asset, where, starting from the preliminary work in [148], a formal analysis approach based on models of the system and all its components, has been followed.

The required models include the description of the system from both the physical and cyber points of view. From the physical point of view, the model includes the physical locations and placement of the physical devices, as well as configuration of the physical security mechanisms used (e.g., doors that can be opened by physical or logical keys). From the cyber point of view, instead, the model also includes the network topology and the configuration of network devices (such as switches and firewalls) and the configuration of all the services provided by physical and virtual nodes. The final ingredient is the model of the users/agents, with their initial location and knowledge (e.g., passwords, keys).

With this level of details it is possible to perform an exhaustive formal analysis, based on model checking, to build the list of every possible sequence of actions that any user can perform in the system, to verify which resources are accessible, in which way. In this approach, we build, for each user, a single automaton where each state represents the state of the user (his physical location and his current knowledge) while the edges are labelled with the action that the user was able to perform (operations on objects). The final set of such actions is then compared to the desired security policies (in terms of assigned permissions to users) and any discrepancy is marked as a flaw in the implementation. This kind of result is sufficient to assess the presence of errors but is not enough to understand the causes and the possible remediation.

For each user, instead, the corresponding automaton includes all the information needed to understand how the user was able to trigger specific forbidden operations, in one or more of his states. However, due to the exhaustive nature of the performed analysis and the complexity of the model used, these automata are large and complex and not directly usable by a human operator. The system administrator, in fact, must understand the problem and must be supported in finding a possible solution. In this approach, we recognize that these problems are in fact, related to the usability of the technique as any powerful enough security tool is useless if its results are not meaningful and manageable by a human operator. To overcome these issues, we followed two approaches: on one hand we worked on reducing the size and complexity of the produced automata maintaining the same amount of information, on the other hand we leveraged this simplified structure to provide an automatic synthesis of possible fixes to the configuration of the nodes involved in the identified flaws.

To reduce the complexity of the automata without losing information we developed an algorithm to transform each automaton in its minimized form, by deducing, from the complete graph, the dependencies between the events, represented as a logical formula between triggered events and their set of preconditions

that must be satisfied. The process is based on a traversal procedure that for each automaton (a graph) collects all the possible alternative *minimal* paths that lead to each event. A brute force approach, based on the complete enumeration of all these paths, is not feasible. To avoid this problem, we included a pruning algorithm able to cut portions of the graph while visiting the graph. The final result can be represented both as a minimal automaton and as a logical formula showing the dependencies among preconditions and subsequent events. The former is a convenient representation that is more readable by the system administrator, while the latter is easier to analyse looking for solutions to the identified flaws. In particular, the representation as a logical formula enables to find all the possible changes in the configuration of the system (affecting the preconditions of the events) that, in some way, prevent the users from triggering forbidden events (operations).

This kind of representation is clearly more useful and more effective to understand *how* potential security policy violations can happen in the system. Another problem related to the usability of such results is that the security administrators cannot simply change elements in the system so as to break violation paths because they could also break legitimate sequences of actions that the users must be able to perform in the system. To help the security administrators solving this problem, we also leveraged the obtained logical formulation of the system so as to define two sets of logical constraints. One set is composed by formulas that must be always satisfied (representing the actions that the users must be able to perform) and the other set representing formulas that must be falsified (that is users must be blocked from reaching a policy violation). With these two sets, we leveraged an SMT (Satisfiability Modulo Theory) solver to provide the security administrators with possible (partial) solutions to the logical formulas that prevents the system to from breaking while blocking unwanted events. Of course, depending on the scenario considered, it is not always possible to find a solution that satisfies both sets of constraints and in this case, the SYSVER tool provides partial solutions or simply suggests to relax some of those constraints. In this way, an iterative usage of the tool could help the administrators in reaching an acceptable solution.

This approach is useful to security administrators, such as the ones operating at the user layer in the reference scenario, to better grasp the meaning and relevance of security policies potential violations and to act accordingly.

4.4 Analyzing Security, Privacy and Usability Trade-offs in Multi-factor Authentication

Two-factor authentication (2FA) and multi-factor authentication (MFA) [126], [127] are effective security measures to reduce the impact of breaches caused by stolen credentials and credential stuffing attacks. Yet, setting up an adequate multi-factor or multi-modal authentication strategy configuration remains a disconcerting job due to the non-trivial trade-offs between security, privacy and usability. For example, risk-based MFA implementations that leverage contextual factors-such as current and previous IP addresses, locations of the end-user, or browser fingerprints [151], [152], [153] can assist the relying party (RP) to estimate the risk and initiate step-up authentication actions. However, the same context factors are exploited as web-based fingerprints for online tracking, and hence harm the privacy of the user [154]. Furthermore, they may be rendered obsolete when new versions of contemporary web browsers implement countermeasures against such tracking.

Authentication specifications and protocols like FIDO2, WebAuthn and CTAP provide support for web browsers to authenticate users with public key cryptography, where the private key on the client is protected

by a hardware security key or a mobile device implementing biometric authentication (e.g., fingerprint verification). While passwordless authentication sounds convenient from a usability point of view, the adoption of biometric authentication is stagnant. Previous research [155] on passwordless authentication has demonstrated that usability concerns remain.

Additionally, from a security perspective, the RP offering WebAuthn authentication, must trust the client to implement adequate security measures, e.g., the biometric factor implementation on a mobile phone, used to unlock the private key. When the client uses face or fingerprint authentication, the RP may not know the false positive rate (i.e., a security concern) and false negative rate (i.e., a usability concern) of each biometric factor on every mobile device. Unforeseen circumstances of use can also challenge the security of the solution. For example, in 2019 the 'Face Unlock' feature of Google's Pixel 4 was confirmed to work even when asleep¹¹, and the use of gel-based screen protectors was also reported¹² to fool fingerprint authentication. Last but not least, even if end-users comprehend the privacy benefits of their biometric templates never leaving their mobile device, they may not grasp the extent to which biometric factors can be subject to the above vulnerabilities.

4.4.1 State of the Art

This section reviews relevant related works and the state-of-the-art solutions on multi-factor authentication, including adaptive and continuous authentication. The goal of reviewing these works is, to illustrate the complexity of understanding the security, privacy and usability trade-offs from the perspective of the different stakeholders, i.e., security administrators and end-users.

Dasgupta et al. [116] discussed adaptive multi-factor authentication strategies as a combination of the calculation of the trustworthiness of different authentication factors, and an adaptive strategy for selecting authentication factors based on their calculated trustworthiness, performance, surroundings and more. It combines a variety of biometric and non-biometric authentication factors, and also avoids repeated selections of the same set of factors in successive re-authentications to reduce the chance of establishing recognizable patterns. The solution was compared with the FIDO and Microsoft Azure MFA frameworks in a user study, and the proposed solution was found to be better. While the usability of the solution was evaluated, the perceived impact on the user's privacy was not assessed. Wang et al. [156] analyzed 5 MFA solutions based on smart cards, passwords and biometrics, and they specifically investigated security failures of their deployment in multi-server environments under the assumption of various threat models (or adversary models). They found critical security and privacy issues in each of them, including vulnerabilities against stolen-verifier attacks, insider attacks, failing to provide forward secrecy, and the loss of user anonymity.

Many security and authentication guidelines, such as websites of governmental agencies¹³ strongly encourage the use of 2FA and MFA, though often only from an end-user perspective to recommend how to

¹¹ Google Pixel 4 Face Unlock works if eyes are shut (2019), <https://www.bbc.com/news/technology-50085630>

¹² Samsung: Anyone's thumbprint can unlock Galaxy S10 phone (2019), <https://www.bbc.co.uk/news/technology-50080586>

¹³ Safeonweb, Use two-factor authentication (2020), <https://www.safeonweb.be/en/use-two-factor-authentication>

better protect online accounts. Other reports, such the NIST Special Publication 800-63B [157] on “Digital Identity Guidelines: Authentication and Lifecycle Management” offer detailed technical requirements at different authenticator assurance levels, and with consideration of usability and privacy. While those reports are typically targeted towards security administrators, the latter have to consider not only the security, privacy and usability trade-offs of their MFA implementation, but also the degrees of freedom they are willing to offer to end-users to further customize the MFA experience to their personal preferences. Those trade-offs and their impact on the actual implementation and deployment are less straightforward.

Klieme et al. [158] presented FIDOnuous that builds upon the WebAuthn standard to support continuous authentication. While WebAuthn enables user-friendly passwordless authentication, as well as strong authentication methods with biometrics, it fails to detect an attack after a successful login. The authors propose a WebAuthn extension that uses an Android-based authenticator communicating over Bluetooth Low Energy (BLE), such that the relying party and the authenticator can continuously exchange authentication verifications. While the authors did not evaluate any specific continuous or behavioral authentication method, their simulation demonstrates the practical feasibility of the integration with WebAuthn. From a privacy perspective, the risk assessment is carried out on the client, and no sensitive behavioral information is shared with the relying party. From a security point of view, the strength of the continuous authentication depends on the accuracy of the authentication methods used and their robustness against threats, such observation, spoofing and replay attacks by an active adversary.

Karegar et al. [159] studied user perceptions on the widely deployed fingerprint recognition on smartphones, often used to unlock the device or to authenticate against remote applications. More specifically, they investigated in an online survey how 100 individuals think that fingerprint recognition works and this in contrast to PIN codes, as well as privacy and possible other issues with this biometric authentication factor. They compared the attitudes of users and non-users. Their user study demonstrated amongst others that even participants reporting a higher level of knowledge in security do not necessarily have a good perception about access to fingerprint patterns and PIN codes of mobile apps.

4.4.2 Challenge Beyond the State of the Art

When setting up multi-factor authentication in contemporary and state-of-practice identity and access management (IAM) platforms, the security administrator is typically faced with a large number of configuration options. The implications of the choices made on the overall security, privacy and usability of the MFA solution are not always understood in advance. This is also a concern for end-users, and the lack of understanding may jeopardize the onboarding of MFA.

4.4.3 Authentication Knowledge Framework

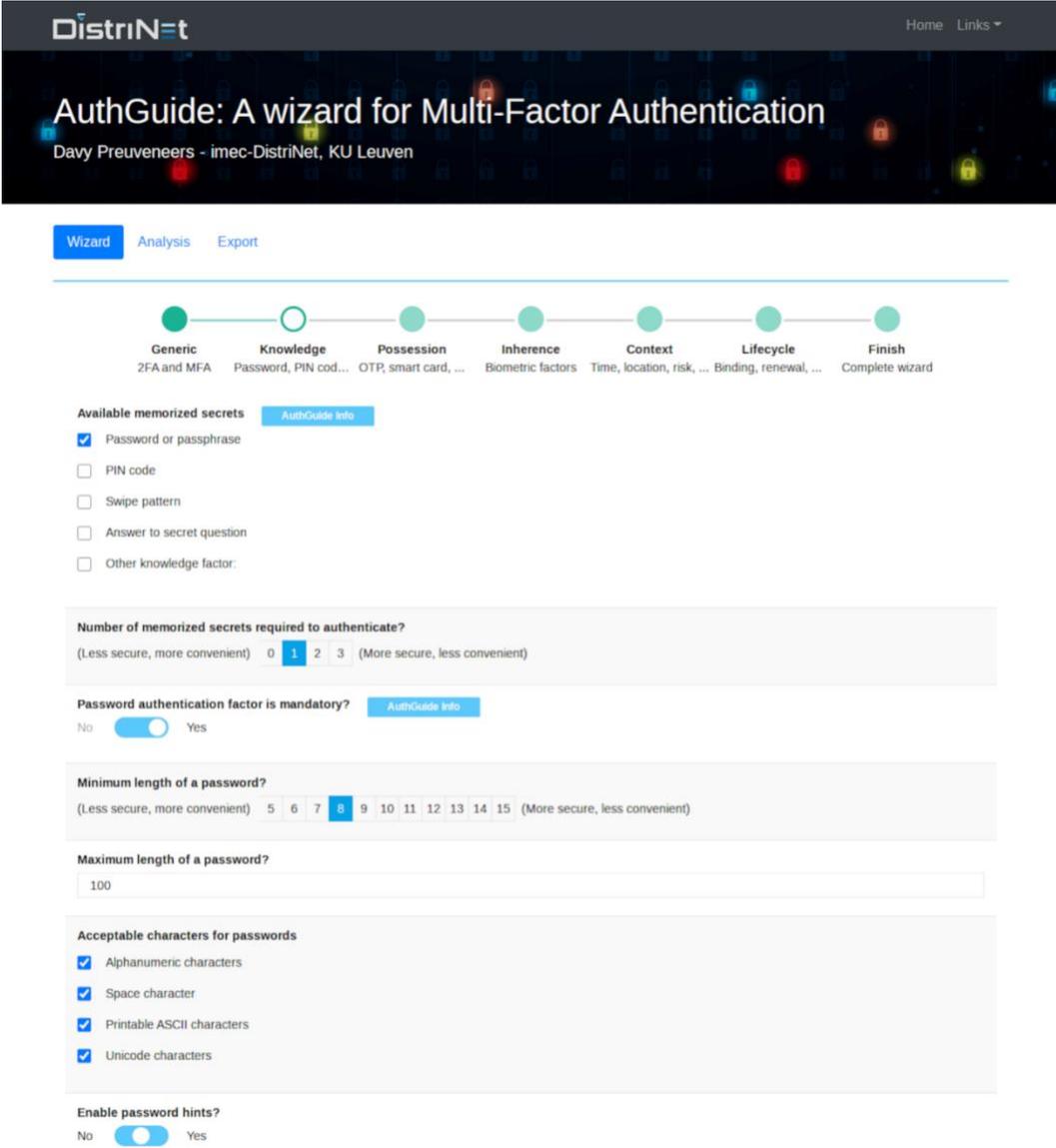
To create a better understanding of the challenges and corresponding security-privacy-usability trade-offs, we present AuthGuide, an authentication knowledge framework that:

- Embeds a body of knowledge to inform about the trade-offs of MFA,
- Analyzes the risk of the customization flexibility granted to the end-user,
- Raises the level of abstraction to simplify the configuration of MFA.

The main use case of AuthGuide is security administrators configuring their IAM platforms by mapping individual options in AuthGuide onto a specific IAM workflow of authentication steps for registration and login. Such a workflow may consist of mandatory and optional steps depending on whether the use of certain

authentication factors is compulsory. To configure MFA for different platforms, AuthGuide generates a custom specialized script that supports the security administrator with deploying the MFA solution. Additionally, AuthGuide provides security administrators and end-users a breakdown of various security, privacy and usability requirements and trade-offs.

The purpose of AuthGuide is not to improve the strength, efficiency or accuracy of any particular authentication factor, but rather to analyze (1) the security, privacy and usability implications of different authentication factors, (2) their combination in an MFA configuration, and (3) the consequences of granting some flexibility on authentication factor selection to the end-user. AuthGuide is inspired by the NIST set of technical requirements [157]. Our AuthGuide solution relies on them to evaluate the assurance level of MFA implementations, as well as their impact on security, privacy and usability. It does so by validating each and



The screenshot shows the AuthGuide wizard interface. At the top, the title is "AuthGuide: A wizard for Multi-Factor Authentication" by Davy Preuveneers - imec-DistriNet, KU Leuven. The interface is divided into sections for configuration and validation.

Wizard Progress: A horizontal progress bar shows seven steps: Generic (2FA and MFA), Knowledge (Password, PIN cod...), Possession (OTP, smart card, ...), Inherence (Biometric factors), Context (Time, location, risk, ...), Lifecycle (Binding, renewal, ...), and Finish (Complete wizard). The "Knowledge" step is currently active.

Available memorized secrets: A list of secret types with checkboxes:

- Password or passphrase
- PIN code
- Swipe pattern
- Answer to secret question
- Other knowledge factor:

Number of memorized secrets required to authenticate? A range selector from 0 to 3. The value "1" is selected. (Less secure, more convenient) to (More secure, less convenient).

Password authentication factor is mandatory? A toggle switch is set to "Yes".

Minimum length of a password? A range selector from 5 to 15. The value "8" is selected. (Less secure, more convenient) to (More secure, less convenient).

Maximum length of a password? A text input field containing "100".

Acceptable characters for passwords: A list of character sets with checkboxes:

- Alphanumeric characters
- Space character
- Printable ASCII characters
- Unicode characters

Enable password hints? A toggle switch is set to "Yes".

Figure 14: The AuthGuide wizard for MFA configuration and requirement validation.

every configuration option selected by of the security administrator with respect to the “SHALL” and “SHOULD” requirement notations and conventions (including the negative forms), the degrees of freedom for customization granted to the end-user, as well as influences of external elements beyond control of the security administrator of an IAM and/or end-user.

AuthGuide manages the list of configuration options per authentication factor, the mapping onto SHALL/SHOULD requirements, and any dependencies across the choices and requirements. Currently, it manages 73 configuration options in the wizard that are mapped onto a subset of the SHALL/SHOULD requirements, and that are conditionally exposed in the wizard depending on previously selected options. It also checks for violations against the 3 authentication assurance levels in NIST Special Publication 800-63B [157]. The specification covers many more requirements than what AuthGuide can actually verify. As such, AuthGuide is not a full compliance analysis tool as it does not check the implementation-specific details or requirements. Additionally, if certain configuration options can be further tweaked by the end-user, AuthGuide evaluates both a best-case and a worst-case configuration scenario. As such, AuthGuide can not only inform the user about security-privacy-usability trade-offs of individual configuration options, but also about trade-offs for configurations as a whole.

Figure 14 depicts the web-based wizard interface to configure the multi-factor authentication configuration and carry out the security, privacy and usability trade-off analysis. In [160], we provide a more detailed analysis of the strengths and benefits of AuthGuide.

4.5 Understanding Users’ Privacy Concerns

In this Section we present research that relates to the privacy concerns of regular users. We discuss two different scenarios: the use of augmented reality applications and the use of privacy enhancing technologies.

4.5.1 State of the Art

One popular model in the privacy literature that tries to explain privacy concerns of online users is based on the Internet Users’ Information Privacy Concerns (IUIPC) construct by Malhotra et al. [161]. Their research targets involve a theoretical framework and an instrument for operationalizing privacy concerns (IUIPC) as well as a causal model for this construct. Malhotra et al. model privacy concerns of users with a second-order construct consisting out of three main constructs: information collection, control, and awareness of privacy practices. Several factors such as cultural differences [162] or different legislation between countries [163] are assumed to have decisive impact on individuals’ privacy behavior. A re-assessment with Japanese respondents recently confirmed most parts of the IUIPC model for Japan [164] and provides an overview of the models’ replications up to 2020 [165].

Besides IUIPC, another instrument to measure information privacy concerns is the concern for information privacy (CFIP) by Smith et al. [166] which was restructured by Stewart and Segars [167] in 2002. CFIP measures the privacy concerns of individuals with regard to organizational privacy practices and consists of four dimensions: collection, unauthorized secondary use, improper access, and errors. Recent applications show that the CFIP construct is still valid and reliable [168]. Since CFIP and IUIPC overlap in the collection dimension, combined they include six dimensions which are the most popular dimensions in the existing literature [169]. Even though Malhotra et al. showed that IUIPC explains more of the variance in a person’s willingness to transact than CFIP, CFIP seems to be still more widely used [170], [171].

4.5.2 Challenge Beyond the State of the Art

Our research efforts on understanding the users' privacy concerns are split into two subsections: augmented reality (AR) (Section 4.5.3) and privacy enhancing technologies (PETs) (Section 4.5.4).

Augmented reality gained much public attention after the success of Pokemon Go in 2016, and has found application in online games, social media, interior design, and other services since then. It is highly dependent on various different sensors gathering real time context-specific personal information about the users to offer them services. Often the collection of sensor data is combined with machine learning approaches to infer information. Using a plethora of sensors, in particular the camera, causes more severe and new privacy threats compared to other technologies. In order to ensure users' privacy and foster market adoption of privacy-friendly augmented reality systems, these threats have to be investigated as long as augmented reality is still shapeable.

Non-technical work on PETs mostly focuses on usability studies and does not primarily focus on user acceptance issues such as privacy concerns, trust and risk beliefs of PET users. For example, Lee et al. [172] assess the usability of the Tor Launcher and propose recommendations to overcome the found usability issues. Benenson et al. [173] investigate acceptance factors for anonymous credentials. Among other things, they find that trust in the PET has no statistically significant impact on the intention to use the service. For our research on Tor and JonDonym, we found different results.

4.5.3 Augmented Reality

Our work builds on a user study with German Pokémon Go users, where we investigated technology acceptance factors based on the UTAUT2 model by Venkatesh et al. [174]. These results imply that AR applications, besides needing to be easily integrable in the users' daily life, should be designed in an intuitive and easily understandable way [175]. We also investigated privacy concerns and the privacy behavior of users. The results indicate that the majority of the active players are concerned about the privacy practices of companies, know about risks and might take actions to protect their privacy, but deliberately trade-off their information privacy for the utility generated by playing the game [176].

Furthermore, we also investigated the effect of childhood brand nostalgia as a mediator and could show it (positively) influences the intention of users of playing the game through altering beliefs concerning Pokémon [177]. We followed this line of work by empirically testing one exemplary extraneous factor within the 'enhanced APCO model' (antecedents – privacy concerns – outcome). Specific empirical tests on such biases are rare in the literature which is why we proposed and empirically analyzed the extraneous influence of a positivity bias. In our case, we could show that the bias is induced by childhood brand nostalgia towards the Pokémon franchise [178].

For further investigations, we designed a vignette-based online experiment to investigate influencing factors of privacy concerns related to a hypothetical mobile augmented reality app. Furthermore, we investigated whether individuals associate higher privacy concerns with augmented reality by manipulating the description of the app (cf. Figure 15 [179]). Thereby, we want to better understand the attitude formation process related to augmented reality and the relation to privacy concerns. After a pretest with 91 German smartphone users [180], we have run the online vignette-based survey with 1100 smartphone users.

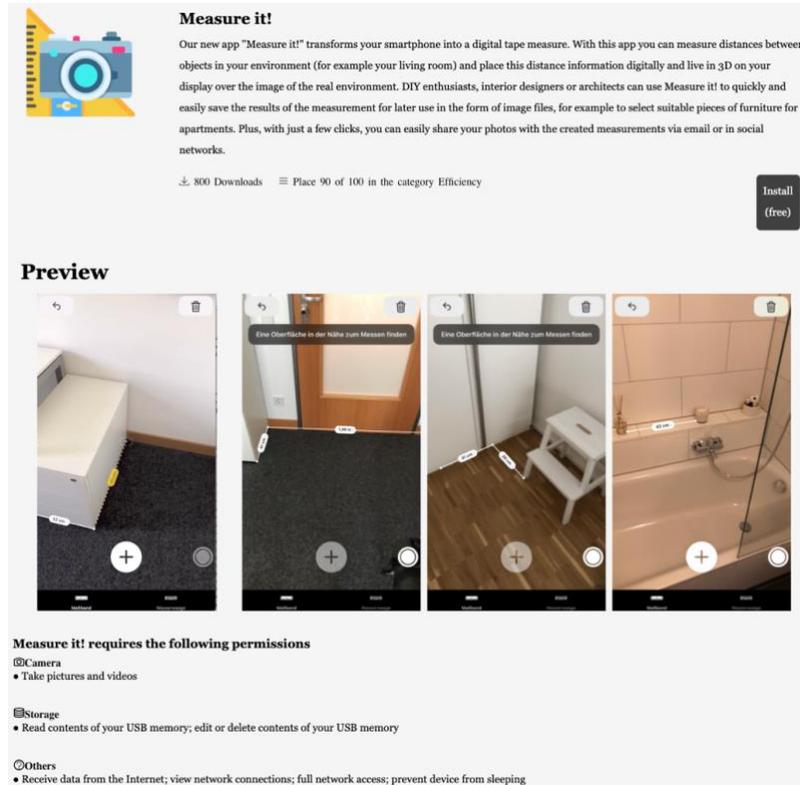


Figure 15: Mockup for the vingette-based survey.

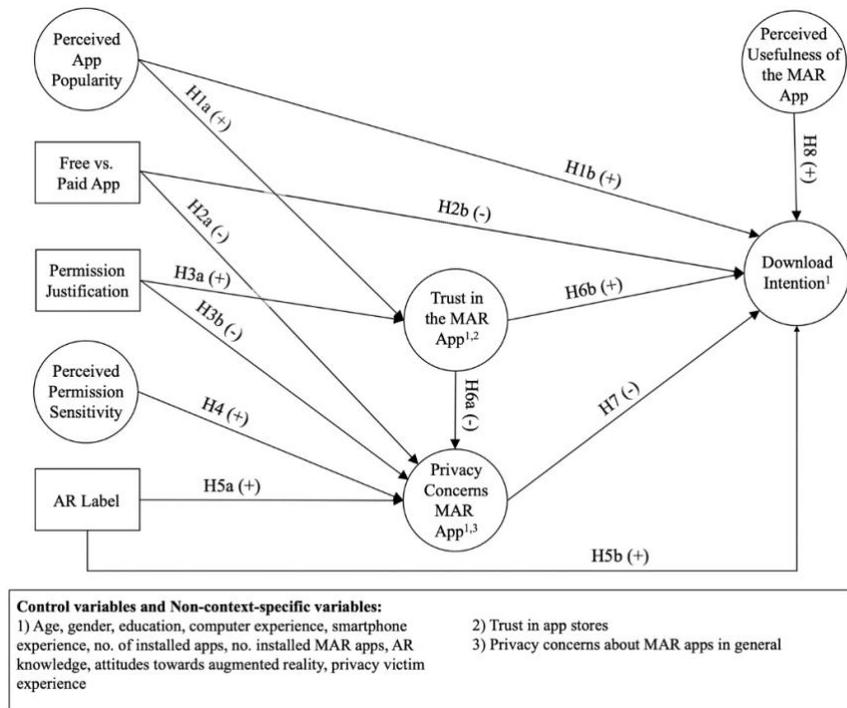


Figure 16: Research model for contextual factors of privacy concerns.

research model shown in Figure 16. The model is based on the framework of contextual integrity by Nissenbaum [181]. Contextual integrity aims at providing a systematic account for understanding user expectations regarding privacy and for showing causes of moral outrage in case of perceived violations of individuals' privacy.

Table 3 shows the hypothesis along with their results. In summary, we used the widely known APCO model from the privacy literature and augmented it with the framework of contextual integrity as a starting point to figure out contextually relevant factors which determine privacy concerns in our chosen context. We showed the relevance of two other contextual factors for the context of mobile augmented reality apps (app price and the augmented reality label). We contribute to literature by developing one of the first models which explains factors influencing privacy concerns related to mobile augmented reality apps. We also presented a new structure of permissions for MAR apps which could be conceptually applied to other types of augmented reality (e.g., smart glasses), too. By that, we contribute to the large stream of research on permissions and propose a new way of thinking about permissions according to the contextual information they represent [179].

Table 3. Summary of the results of the vignette-based online survey

	Hypothesis	Result
H1a	Perceived app popularity positively influences the trust in the app.	✓
H1b	Perceived app popularity positively influences the intention to download the app.	✓
H2a	The price of the MAR app negatively influences privacy concerns related to the MAR app if the app is not free.	✗
H2b	The price of the MAR app negatively influences the intention to download the MAR app.	✓
H3a	Permission justifications positively influence trust in the app.	✗
H3b	Permission justifications negatively influence privacy concerns related to the app.	✗
H4	Perceived permission sensitivity positively influences privacy concerns related to the app.	✓
H5a	The AR label of the MAR app positively influences privacy concerns related to the app.	✗
H5b	The AR label of the MAR app positively influences the intention to download the app.	✗
H6a	Trust in the MAR app negatively influences privacy concerns related to the app.	✓
H6b	Trust in the MAR app positively influences the intention to download the app.	✓
H7	Privacy concerns related to the MAR app negatively influence the intention to download the app.	✓
H8	The perceived usefulness of the MAR app positively influences the intention to download the app.	✓

4.5.4 Privacy Enhancing Technologies

Due to an increasing collection of personal data by internet companies, and several data breaches, research related to privacy has gained importance in the last years in the information systems domain. Privacy

concerns can strongly influence users' decision to use a service. The Internet Users Information Privacy Concerns (IUIPC) construct is one operationalization to measure the impact of privacy concerns on the use of technologies. However, when applied to a privacy enhancing technology (PET) such as an anonymization service, the original rationales do not hold anymore. In particular, an inverted impact of trusting and risk beliefs on behavioral intentions can be expected. We show that the IUIPC model needs to be adapted for the case of PETs. In addition, we extend the original causal model by including trusting beliefs in the anonymization service itself as well as a measure for privacy literacy. A survey among 124 users of the anonymization service Tor shows that trust in Tor has a statistically significant effect on the actual use behavior of the PET. In addition, the results indicate that privacy literacy has a negative impact on trusting beliefs in general and a positive effect on trust in Tor [182].

Today's environment of data-driven business models relies heavily on collecting as much personal data as possible. One way to prevent this extensive collection, is to use PETs. However, until now, PETs have not succeeded in larger consumer markets. In addition, there is a lot of research determining the technical properties of PETs (e.g., for Tor) but the use behavior of the users and, especially, their attitude towards spending money for such services is rarely considered. Yet, determining factors that lead to an increased willingness to pay (WTP) for privacy is an important step to establish economically sustainable PETs. We argue that the lack of WTP for privacy is one of the most important reasons for the non-existence of large players engaging in the offering of a PET. The relative success of services like Tor corroborates this claim since this is a service without any monetary costs attached. Thus, we empirically investigate the drivers of active users' WTP of a commercial PET – JonDonym – and compare them with the respective results for a donation-based service – Tor. Furthermore, we provide recommendations for the design of tariff schemes for commercial PETs [183].

We conducted an online survey with 265 users of the anonymity services Tor and JonDonym (124 users of Tor and 141 users of JonDonym). The results are summarized in Table 4. We use the technology acceptance model as a theoretical starting point and extend it with the constructs perceived anonymity and trust in the service in order to take account for the specific nature of PETs. Our model explains almost half of the variance of the behavioral intention to use the two PETs. The results indicate that both newly added variables are highly relevant factors in the path model. We augment these insights with a qualitative analysis of answers to open questions about the users' concerns, the circumstances under which they would pay money and choose a paid premium tariff (only for JonDonym), features they would like to have and why they would or would not recommend Tor/JonDonym. Thereby, we provide additional insights about the users' attitudes and perceptions of the services and propose new use factors not covered by our model for future research [184], [184], [185]. Table 4. Qualitative results for PET usage shows the results of our qualitative analysis by grouping the discovered concepts and distinguishing between concepts which specifically relate to Tor or JonDonym or are common to both. For each of the concepts relevant quotes are provided.

Table 4. Qualitative results for PET usage

Concepts	Subconcepts	Common to both PETs	Specific Subconcepts for Tor	Specific Subconcepts for JD
Statements about technical issues	PET design	Feature requests (Tor.1, Jon.1)	Malicious exit nodes (Tor.2)	Location of mix cascades (Jon.2)
	Compatibility	Accessibility of web-sites (Tor.3, Jon.3)		

	Usability	Documentation (Tor.4, Jon.4) Ease of use (Tor.5, Jon.5) Missing knowledge to use it correctly (Tor.6, Jon.6)		
	Performance	Latency (Tor.7, Jon.7, Jon.8)		
Beliefs and perceptions	Anonymity	Concerns about deanonymization (Tor.8, Jon.9) Reason of use (Tor.9, Jon.10)		Size of the user base (Jon.11)
	Consequences	Fear of investigations (Tor.10, Tor.11, Jon.12)	Beliefs about social effects (Tor.13, Tor.14)	
	Trust		Trust in the community (Tor.12)	Trust in technology (Jon.13)
	Substitute technologies	Best available tool (Tor.15, Jon.14)		Tor as reference technology (Jon.3, Jon.8, Jon.11)
Statements about economical issues	Costs			Lower costs, other pricing schemes (Jon.15)
	Payment methods			Easy, anonymous payment options (Jon.15)
	Use cases		Circumvent censorship (Tor.16)	Willingness to pay in certain scenarios (Jon.16, Jon.17)
Tor.1	<i>TCP support for name resolution via Tor's DNSPort...</i>	Jon.1	<i>Larger number of Mix Cascades, more recent software, i.e., preconfigured browser, faster security updates</i>	
Tor.2	<i>Many exit nodes are run by governmental intelligence organisations. Exit notes can collect unencrypted data.</i>	Jon.2	<i>First and last server of the mix cascade should not be located in the same country</i>	
Tor.3	<i>It can't be used on all websites; therefore it is of limited use to me</i>	Jon.3	<i>Unlike Tor, JonDonym is not blocked by some websites. (Google for example among others)</i>	
Tor.4	<i>Easy to understand instructions for users with different levels of knowledge.</i>	Jon.4	<i>Clearer explanations and instructions for JonDoFox</i>	
Tor.5	<i>Tor protects privacy while on the web and is easy to use.</i>	Jon.5	<i>Easy to use, outside the mainstream like Tor</i>	
Tor.6	<i>An unexperienced user may not understand the technical limitations of Tor and end up losing [...] privacy</i>	Jon.6	<i>Privacy is less than expected because of wrong configuration settings</i>	
Tor.7	<i>Increased latency makes the experience painful at times</i>	Jon.7	<i>[...] even if it is quite slow without a premium tariff</i>	

Tor.8	<i>It may fail to provide the expected level of anonymity because of attacks which may not even be known at the time they are performed (or commonplace)</i>	Jon.8	<i>[...]sometimes it's a little bit too slow, but compared with Tor[...]</i>
Tor.9	<i>It is a key component to maintaining one's privacy when browsing on the Internet.</i>	Jon.9	<i>Defeat of your systems by government agencies.</i>
Tor.10	<i>Tor usage "stands out"</i>	Jon.10	<i>It provides a minimum level of personal data protection and online safety.</i>
Tor.11	<i>[...] having a cop boot at my door because of Tor.</i>	Jon.11	<i>Tor is better due to having a much larger user base. More users results in greater anonymity</i>
Tor.12	<i>An end user needs to trust the network, the persons running Tor nodes and correct implementations [...]</i>	Jon.12	<i>By using the service, am I automatically marked by intelligence authorities as a potential terrorist, supporter of terrorist organizations, user [...] for illegal things?</i>
Tor.13	<i>Only social backlash from people thinking that Tor is mostly used for illegal activities.</i>	Jon.13	<i>How can I trust Jondonym? How can Jondonym proof that servers are trustworthy?</i>
Tor.14	<i>For the same reason I don't hang out in brothels, using Tor makes you look like a criminal</i>	Jon.14	<i>It appeared to be the least worst option for anonymisation when I researched anonymisation services</i>
Tor.15	<i>While not perfect, Tor is the best option for reliable low-latency anonymization</i>	Jon.15	<i>Fair pricing, pre-paid is an easy payment option.</i>
Tor.16	<i>It can be used as a proxy / VPN to get past censorship</i>	Jon.16	<i>For use it in a country where it's difficult surf the net</i>
		Jon.17	<i>If I would use the computer for work-related tasks</i>

4.6 Analysis, Presentation and Understanding of Privacy Policies

This section covers the analysis, presentation and automatic summarization of privacy policies. It covers the state of the art and technologies provided beyond the existing work.

4.6.1 State of the Art

By applying Natural Language Processing (NLP) and Machine Learning (ML) techniques, Costante et al. [186] proposed a method for evaluating the completeness of privacy policies. In this approach the authors show that a privacy policy is said to be complete if it contains descriptions which should be explained in privacy policies, such as how to deal with cookies. Their research is based on The Organization for Economic Cooperation and Development (OECD) guideline, and the Safe Harbor Framework documents. Even though this work was conducted pre-GPDR, it provides an important motivation for our research presented below.

Furthermore, Guntamukkala et al. [187] present an automated approach for assisting users to evaluate online privacy policies based on completeness. In this work, authors define completeness to the presence of 8 sections in an online privacy policy that have been recognized as helpful in establishing the transparency of a privacy policy. Authors used a machine learning-based approach to predict a completeness score for the

privacy policy which is then used by the user to assess the risk to their privacy. Zimmeck and Bellwin [188] developed Privee – a software architecture for analyzing privacy policies which authors state that it has promising avenue for facilitating the notice-and-choice principle by accurately notifying.

Gluck et al. [189] have previously shown that the use of condensed and standardized privacy notices has a positive effect on user’s awareness of privacy practices.

Zaeem et al. [190] developed PrivacyCheck, a free Chrome browser extension that utilizes the data mining models to summarize any HTML page that contains a privacy policy. PrivacyCheck is readily applicable on any online privacy policy. Authors mention that over 400 independent Chrome users are currently using PrivacyCheck.

In summary, different approaches have been implemented to support users in understanding privacy policies. However, we note that none of these approaches had considered the GDPR as basis to build the benchmarks. Moreover, in our approach outlined below, we follow a risk-based assessment of privacy policies.

4.6.2 Challenge Beyond the State of the Art

Service providers are required to inform their users as to how they collect, store and process personal data. The de facto means of communicating these practices remains to be through privacy policies. However, most privacy policies are incomprehensible and largely unreadable. As a consequence, most users do not bother to read them.

4.6.3 Analyzing Privacy Policies

Different approaches have been proposed to support users in making them easily grasp privacy policies. As such, machine learning and natural language processing techniques have become popular lately. To this end, we propose PrivacyGuide [191], [192], a machine learning based privacy policy bench marking tool which also takes the users regulatory rights into account. Similar approaches have been proposed to support users in default privacy preference setting [193], and unintended disclosure of privacy sensitive information [194]. PrivacyGuide follows a risk-based analysis of privacy policies. It also considers eleven aspects from the GDPR as a basis to analyze and bench mark the privacy policies. It has been applied to different use-cases such as augmented reality apps [195], in which it demonstrates promising applicability.

As a continuation of work on an assessment framework for privacy policies of Internet of Things Services which is based on particular GDPR requirements [196], we propose another tool named Leech, a serious game developed in a students' project for learning about the contents and structure of privacy policies so that users get a rough understanding of what to expect in privacy policies. Leech is an adventure game and the player has to solve quests to complete the game. Two of the tasks are implemented as a mini game to allow more complexity. Two pre-tests led to promising results and we intend to quantitatively evaluate the game in the next step by investigating players' online privacy literacy, demographics, values on privacy policies, actions within the game, and their in-game experience. [197]

4.7 Summary

In this Section we presented several different tools that can enhance a user's understanding of security. We proposed a generic method for systematically analyzing the usability of security mechanisms of a product or service in order to better assess the trade-offs between security and usability. Balancing the needs for ease-of-use and security is revisited with the tool for configuring multi-factor authentication: the options offered to the security administrator are usually plentiful and it is often difficult to know their implications for privacy, security and usability. We presented a solution that can guide both the professional and private user around these hurdles. We also analyzed access control policies in complex, heterogeneous systems using formal methods. The results of such analysis are typically large and unwieldy, thus there was a need to enhance usability with automation and visualization.

We also examined the different aspects of human capabilities in relation to cryptography. Based on our findings we implemented an experimental proof-of-concept communication channel in which the user performs simple cryptographic operations. They were most happy with the part of the system that only required visual perception and no mental effort. Usability of this visual perception task was analyzed with the modelling tool also presented in this section.

To conclude this Section, we provided our reports on enhancing the usability of privacy tools. We discussed the user's privacy concerns relating to AR applications and PETs. We also showcased two tools for helping users understand privacy policies.

5 Conclusion

In this deliverable we have presented the most current research on human-centered cyber security that was conducted within this project. The driving force for most of our research has been to give regular and professional users the tools and information they need to make secure choices in their day-to-day lives, and to do that in an understandable and easily approachable manner.

The research presented here was divided into three themes. For the first theme of privacy and data protection, we have looked at opportunities for reducing the number of potential risks to assess in a data protection impact assessment. We showed how to, prior to the assessment, identify risks that are not relevant to a DPIA. This reduces the amount of work and makes performing a DPIA easier.

We also described guidelines for adopting a privacy-preserving identity management solution in a user-friendly manner, with special focus on management of access policies. From this, we can highlight the importance of perception of smoothness, consideration of multiple stances on privacy/usability trade-offs and enabling trust on the components.

For the second research theme on eliciting and fulfilling security requirements we have presented several tools and other designs. We showed how to use security games to discover security requirements in order to improve security policies, and how to acquire data for security risk assessments and how to gauge its quality. Privacy notifications and their perceived usefulness was discussed and we were able to infer a series of design guidelines for usable transparency enhancing technologies. We also proposed a framework to characterize the adaptive authentication problem and support the engineering of adaptive authentication systems. We elicited a set of challenges for the community to address in future research on adaptive authentication, and suggest that these challenges could be generalised to other user-facing security controls.

The third theme of enhancing the user's understanding of security solutions included several different kinds of research endeavours. First of all, we demonstrated how tasks models can be used to systematically analyse the impact of security mechanisms on usability, as well as how they can be used along with threat modelling techniques to analyse security.

Secondly, we implemented a proof-of-concept communication system using human understandable cryptography. The aim of involving human capabilities and oversight for each step was achieved, but the system is still very immature: according to our threat and usability analyses, it cannot compete with regular authentication methods and communication channels.

Next, we have shown how approaches based on exhaustive formal analysis could result in unmanageable results. However, we can improve the usability of this approach by manipulating complex graphs into focused views.

Finally, we have studied the ways to advise users on authentication methods and ways to compare them. For this purpose, an authentication knowledge and configuration framework called AuthGuide was developed. It increases the user's awareness about security, privacy and usability trade-offs. The tool supports the configuration of multi-factor authentication and analyzes such configurations with respect to the NIST SP 800-63B guidelines.

The common refrain in the conclusions above is that the ease of use is an important design consideration for security solutions. One would be wise to try, for example, modelling their system to ensure its usability at an early stage of development. Visualizations are also important for making the human user understand abstract cyber security concepts more easily. And of course, the more experimental ideas of human understandable cryptography proved not mature enough to stay secure and win over the users at the same time.

To conclude the work on T3.6 we are preparing D3.17 *Integration to Demonstration Cases*. We will show how most of the assets of T3.6 have been, or can be, integrated into demonstration cases from WP5. Moreover, a unified smart campus scenario is also developed in D3.17 in order to showcase the interplay of our assets.

6 References

- [1] D. Recordon and D. Reed, “OpenID 2.0: A Platform for User-Centric Identity Management,” in *Proceedings of the Second ACM Workshop on Digital Identity Management*, 2006, pp. 11–16, doi: 10.1145/1179529.1179532.
- [2] J. Hughes and E. Maler, “Security assertion markup language (saml) v2.0 technical overview.” 2005.
- [3] J. Camenisch and E. Van Herreweghen, “Design and Implementation of the *Idemix* Anonymous Credential System,” in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 21–30, doi: 10.1145/586110.586114.
- [4] C. Allen, “The path to self-sovereign identity.” 2017.
- [5] A. Acquisti and J. Grossklags, “Privacy and rationality in individual decision making,” *IEEE Secur. & Priv.*, vol. 3, no. 1, pp. 26–33, 2005.
- [6] I. Pollach, “What’s wrong with online privacy policies?,” *Commun. ACM*, vol. 50, no. 9, pp. 103–108, 2007.
- [7] J. Kolter and G. Pernul, “Generating user-understandable privacy preferences,” in *2009 International Conference on Availability, Reliability and Security*, 2009, pp. 299–306.
- [8] D. Biswas, “Privacy policies change management for smartphones,” in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, 2012, pp. 70–75.
- [9] L. Fang, H. Kim, K. LeFevre, and A. Tami, “A privacy recommendation wizard for users of social networking sites,” in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 630–632.
- [10] I. A. Tondel, Å. A. Nyre, and K. Bernsmed, “Learning privacy preferences,” in *2011 Sixth International Conference on Availability, Reliability and Security*, 2011, pp. 621–626.
- [11] S. Guo and K. Chen, “Mining privacy settings to find optimal privacy-utility tradeoffs for social network services,” in *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Conference on Social Computing*, 2012, pp. 656–665.
- [12] T. Nakamura, S. Kiyomoto, W. B. Tesfay, and J. Serna, “Personalised Privacy by Default Preferences,” 2016.
- [13] T. Nakamura, W. B. Tesfay, S. Kiyomoto, and J. Serna, “Default privacy setting prediction by grouping user’s attributes and settings preferences,” in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, Springer, 2017, pp. 107–123.
- [14] S. Löbner, W. B. Tesfay, T. Nakamura, and S. Pape, “Explainable Machine Learning for Default Privacy Setting Prediction,” *IEEE Access*, vol. 9, pp. 63700–63717, 2021.
- [15] M. Papadaki, S. Furnell, and R. C. Dodge, “Social Engineering: Exploiting the weakest links,” *Eur. Netw. & Inf. Secur. Agency (ENISA), Heraklion, Crete*, 2008.
- [16] D. Canavese *et al.*, “Cybersecurity outlook 1,” 2020.

- [17] K. Beckers, D. Schosser, S. Pape, and P. Schaab, “A Structured Comparison of Social Engineering Intelligence Gathering Tools,” in *Trust, Privacy and Security in Digital Business - 14th International Conference, TrustBus 2017, Lyon, France, August 30-31, 2017, Proceedings*, 2017, pp. 232–246, doi: 10.1007/978-3-319-64483-7_15.
- [18] P. Schaab, K. Beckers, and S. Pape, “A systematic Gap Analysis of Social Engineering Defence Mechanisms considering Social Psychology,” in *10th International Symposium on Human Aspects of Information Security Assurance, {HAISA} 2016, Frankfurt, Germany, July 19-21, 2016, Proceedings.*, 2016.
- [19] P. Schaab, K. Beckers, and S. Pape, “Social engineering defence mechanisms and counteracting training strategies,” *Inf. Comput. Secur.*, vol. 25, no. 2, pp. 206–222, 2017, doi: 10.1108/ICS-04-2017-0022.
- [20] K. Beckers, S. Pape, and V. Fries, “{HATCH}: Hack And Trick Capricious Humans -- A Serious Game on Social Engineering,” in *Proceedings of the 2016 British {HCI} Conference, Bournemouth, United Kingdom, July 11-15, 2016*, 2016.
- [21] S. Faily and I. Flechais, “Persona cases: a technique for grounding personas,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011, pp. 2267–2270.
- [22] J. C. K. H. Riedel and J. B. Hauge, “State of the art of serious games for business and industry,” in *2011 17th International Conference on Concurrent Enterprising*, 2011, pp. 1–8.
- [23] K. Beckers and S. Pape, “A Serious Game for Eliciting Social Engineering Security Requirements,” in *Proceedings of the 24th IEEE International Conference on Requirements Engineering*, 2016, doi: 10.1109/RE.2016.39.
- [24] L. Goeke, A. Quintanar, K. Beckers, and S. Pape, “{PROTECT} - An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks,” in *Computer Security - {ESORICS} 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers*, 2019, vol. 11981, pp. 156–171, doi: 10.1007/978-3-030-42051-2_11.
- [25] D. Aladawy, K. Beckers, and S. Pape, “{PERSUADED:} Fighting Social Engineering Attacks with a Serious Game,” in *Trust, Privacy and Security in Digital Business - 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5-6, 2018, Proceedings*, 2018, vol. 11033, doi: 10.1007/978-3-319-98385-1_8.
- [26] M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber Security Awareness Campaigns: Why do they fail to change behaviour?,” *CoRR*, vol. abs/1901.0, 2019.
- [27] V. Hazilov and S. Pape, “Systematic Scenario Creation for Serious Security-Awareness Games,” in *Computer Security - {ESORICS 2020} International Workshops, {DETIPS}, {DeSECSys}, {MPS}, and {SPOSE}, Guildford, {UK}, September 17-18, 2020, Revised Selected Papers*, 2020, vol. 12580, doi: 10.1007/978-3-030-66504-3_18.
- [28] S. Pape and D.-K. Kipker, “Case Study: Checking a Serious Security-Awareness Game for its Legal Adequacy,” *Datenschutz und Datensicherheit*, vol. 45, no. 5, pp. 310–314, 2021.
- [29] T. Saleh, “CovidLock Update: Deeper Analysis of Coronavirus Android Ransomware.” 2020.
- [30] S. Pape, L. Goeke, A. Quintanar, and K. Beckers, “Conceptualization of a CyberSecurity Awareness Quiz,” in *Computer Security - {ESORICS} 2020 International Workshops MSTEC*, 2020, vol. 12512,

- pp. 61–76, doi: 10.1007/978-3-030-62433-0_4.
- [31] S. Pape, “Requirements Engineering and Tool-Support for Security and Privacy.” 2020.
- [32] L. Goeke, S. Pape, and G. Tsakirakis, “THREAT-ARREST serious games v2,” 2021.
- [33] S. Pape and J. Stankovic, “An Insight into Decisive Factors in Cloud Provider Selection with a Focus on Security,” in *Computer Security - {ESORICS} 2019 International Workshops, CyberICPS, SECPRE, SPOSE, ADIoT, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers*, 2019, vol. 11980, pp. 287–306, doi: 10.1007/978-3-030-42048-2_19.
- [34] G. F. Anastasi, E. Carlini, M. Coppola, and P. Dazzi, “QBROKAGE: A Genetic Approach for QoS Cloud Brokering,” in *Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on*, 2014, pp. 304–311.
- [35] L. D. Ngan and R. Kanagasabai, “OWL-S Based Semantic Cloud Service Broker,” in *Web Services (ICWS), 2012 IEEE 19th International Conference on*, 2012, pp. 560–567.
- [36] K. M. Sim, “Agent-Based Cloud Computing,” *Serv. Comput. IEEE Trans.*, vol. 5, no. 4, pp. 564–577, 2012.
- [37] P. Wang and X. Du, “An Incentive Mechanism for Game-Based QoS-Aware Service Selection,” in *Service-Oriented Computing*, vol. 8274, Springer Berlin Heidelberg, 2013, pp. 491–498.
- [38] R. Karim, C. Ding, and A. Miri, “An End-to-End QoS Mapping Approach for Cloud Service Selection,” in *Services (SERVICES), 2013 IEEE Ninth World Congress on*, 2013, pp. 341–348.
- [39] S. Bleikertz, T. Mastelic, S. Pape, W. Pieters, and T. Dimkov, “Defining the Cloud Battlefield -- Supporting Security Assessments by Cloud Customers,” in *Proceedings of IEEE International Conference on Cloud Engineering (IC2E)*, 2013, pp. 78–87, doi: 10.1109/IC2E.2013.31.
- [40] S. Sundareswaran, A. Squicciarini, and D. Lin, “A Brokerage-Based Approach for Cloud Service Selection,” in *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on*, 2012, pp. 558–565, doi: 10.1109/CLOUD.2012.119.
- [41] N. Ghosh, S. K. Ghosh, and S. K. Das, “SelCSP: A Framework to Facilitate Selection of Cloud Service Providers,” *Cloud Comput. IEEE Trans.*, vol. PP, no. 99, p. 1, 2014, doi: 10.1109/TCC.2014.2328578.
- [42] P. Costa, J. Lourenço, and M. da Silva, “Evaluating Cloud Services Using a Multiple Criteria Decision Analysis Approach,” in *Service-Oriented Computing*, vol. 8274, Springer Berlin Heidelberg, 2013, pp. 456–464.
- [43] S. K. Garg, S. Versteeg, and R. Buyya, “SMICloud: A Framework for Comparing and Ranking Cloud Services,” in *Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on*, 2011, pp. 210–218, doi: 10.1109/UCC.2011.36.
- [44] I. Patiniotakis, S. Rizou, Y. Verginadis, and G. Mentzas, “Managing Imprecise Criteria in Cloud Service Ranking with a Fuzzy Multi-criteria Decision Making Method,” in *Service-Oriented and Cloud Computing*, vol. 8135, K.-K. Lau, W. Lamersdorf, and E. Pimentel, Eds. Springer Berlin Heidelberg, 2013, pp. 34–48.
- [45] E. Wittern, J. Kuhlenkamp, and M. Menzel, “Cloud Service Selection Based on Variability

- Modeling,” in *Service-Oriented Computing*, vol. 7636, C. Liu, H. Ludwig, F. Toumani, and Q. Yu, Eds. Springer Berlin Heidelberg, 2012, pp. 127–141.
- [46] S. M. Habib, S. Ries, M. Mühlhäuser, and P. Varikkattu, “Towards a trust management system for cloud computing marketplaces: using CAIQ as a trust information source,” *Secur. Commun. Networks*, vol. 7, no. 11, pp. 2185–2200, 2014, doi: 10.1002/sec.748.
- [47] C. Schmitz and S. Pape, “LiSRA: Lightweight Security Risk Assessment for Decision Support in Information Security,” *Comput. & Secur.*, vol. 90, 2020, doi: 10.1016/j.cose.2019.101656.
- [48] C. Schmitz, A. Sekula, S. Pape, V. Pipek, and K. Rannenber, “Easing the Burden of Security Self-Assessments,” in *12th International Symposium on Human Aspects of Information Security & Assurance, {HAISA} 2018, Dundee, Scotland, August 29-31, 2018, Proceedings.*, 2018.
- [49] J. Dax *et al.*, “Das SIDATE-Portal im Einsatz,” in *State of the Art: IT-Sicherheit für Kritische Infrastrukturen*, S. Rudel and U. Lechner, Eds. Neubiberg: Universität der Bundeswehr, 2018, pp. 145–150.
- [50] C. Schmitz, A. Sekulla, and S. Pape, “Asset-centric analysis and visualisation of attack trees,” in *Graphical Models for Security - 7th International Workshop, GramSec@CSF 2020, Boston, MA, USA, Virtual Conference, June 22, 2020, Revised Selected Papers*, 2020, vol. 12419, pp. 45–64, doi: 10.1007/978-3-030-62230-5_3.
- [51] S. Pape, C. Schmitz, D.-K. Kipker, and A. Sekula, “On the use of Information Security Management Systems by German Energy Providers,” in *Presented at the Fourteenth IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, 2020.
- [52] J. Dax *et al.*, “IT Security Status of German Energy Providers.” 2017.
- [53] M. Schmid and S. Pape, “A structured comparison of the corporate information security,” in *{ICT} Systems Security and Privacy Protection - 34th {IFIP} {TC} 11 International Conference, {SEC} 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings*, 2019, pp. 223–237, doi: 10.1007/978-3-030-22312-0_16.
- [54] M. Schmid and S. Pape, “Aggregating Corporate Information Security Maturity Levels of Different Assets,” in *Privacy and Identity Management. Data for Better Living: {AI} and Privacy - 14th {IFIP} {WG} 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19-23, 2019, Revised Selected Papers*, no. 576, M. Friedewald, M. Önen, E. Lievens, S. Krenn, and S. Fricker, Eds. Springer Boston, 2019, pp. 376–392.
- [55] S. Pape, F. Paci, J. Juerjens, and F. Massacci, “Selecting a Secure Cloud Provider: An Empirical Study and Multi Criteria Approach,” *Information*, vol. 11, no. 5, 2020, doi: 10.3390/info11050261.
- [56] C. Schmitz, M. Schmid, D. Harborth, and S. Pape, “Maturity Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners’ Assessment Capabilities,” *Comput. & Secur.*, vol. (to appear, 2021, doi: 10.1016/j.cose.2021.102306.
- [57] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, “A Design Space for Effective Privacy Notices,” in *Proc. of the Symposium On Usable Privacy and Security*, 2015.
- [58] P. Murmann and S. Fischer-Hübner, “Tools for Achieving Usable Ex Post Transparency: A Survey,” *IEEE Access*, vol. 5, 2017.
- [59] B. Liu *et al.*, “Follow My Recommendations: A Personalized Privacy Assistant for Mobile App

- Permissions,” in *Proc. of the Symposium On Usable Privacy and Security*, 2016.
- [60] H. Almuhiemedi *et al.*, “Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging,” in *Proc. of the ACM Conf. on Human Factors in Computing Systems*, 2015.
- [61] G. Hsieh, K. P. Tang, W. Y. Low, and J. I. Hong, “Field deployment of IMBuddy: A study of Privacy Control and Feedback Mechanisms for Contextual IM,” in *Proc. of the Int. Conf. on UbiComp*, 2007.
- [62] D. Wu, G. D. Moody, J. Zhang, and P. B. Lowry, “Effects of the design of mobile security notifications and mobile app usability on users’ security perceptions and continued use intention,” *Inf. \& Manag.*, vol. 57, no. 5, 2020.
- [63] P. Murmann, D. Reinhardt, and S. Fischer-Hübner, “To Be, or Not to Be Notified -- Eliciting Privacy Notification Preferences for Online mHealth Services,” in *Proc. of the Int. Conf. on Information Security and Privacy Protection*, 2019.
- [64] P. Murmann, M. Beckerle, S. Fischer-Hübner, and D. Reinhardt, “Reconciling the What, When and How of Privacy Notifications in Fitness Tracking Scenarios,” 2021.
- [65] E.-M. Schomakers, C. Lidynia, D. Müllmann, and M. Ziefle, “Internet Users’ Perceptions of Information Sensitivity -- Insights from Germany,” *Int. J. Inf. Manag.*, vol. 46, 2019.
- [66] G. Hofstede and G.-J. Hofstede, *Lokales Denken, globales Handeln: Interkulturelle Zusammenarbeit und globales Management*. Deutscher Taschenbuch Verlag, 2006.
- [67] J. Angulo, S. Fischer-Hübner, E. Wästlund, and T. Pulls, “Towards Usable Privacy Policy Display and Management,” *Inf. Manag. \& Comput. Secur.*, vol. 20, no. 1, 2012.
- [68] P. Murmann, “Eliciting Design Guidelines for Privacy Notifications in mHealth Environments,” *Int. J. Mob. Hum. Comput. Interact.*, vol. 11, no. 4, 2019.
- [69] F. Schaub, R. Balebako, and L. F. Cranor, “Designing Effective Privacy Notices and Controls,” *IEEE Internet Comput.*, vol. 21, no. 3, 2017.
- [70] Art. 29 Data Protection Working Party, “Guidelines on Transparency under Regulation 2016/679, WP260 rev.01.” 2018.
- [71] EU Commission, “Special Eurobarometer 487a -- The General Data Protection Regulation,” 2019.
- [72] S. Egelman, L. F. Cranor, and J. Hong, “You’ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings,” in *Proc. of the ACM Conf. on Human Factors in Computing Systems*, 2008.
- [73] S. Patil, R. Hoyle, R. Schlegel, and others, “Interrupt Now or Inform Later? Comparing Immediate and Delayed Privacy Feedback,” in *Proc. of the ACM Conf. on Human Factors in Computing Systems*, 2015.
- [74] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri, “Bridging the Gap in Computer Security Warnings: A Mental Model Approach,” *IEEE Secur. \& Priv.*, vol. 9, no. 2, 2011.
- [75] H. De Silva, D. C. Wittebron, A. M. R. Lahiru, K. L. Madumadhavi, L. Rupasinghe, and K. Y. Abeywardena, “AuthDNA: An Adaptive Authentication Service for any Identity Server,” in *2019 Int. Conf. on Advancements in Computing*, 2019, pp. 369–375.

- [76] K. A. A. Bakar and G. R. Haron, "Adaptive authentication: Issues and challenges," in *2013 World Congress on Computer and Information Technology*, 2013, pp. 1–6.
- [77] P. Arias-Cabarcos, C. Krupitzer, and C. Becker, "A survey on Adaptive Authentication," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–30, 2019.
- [78] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, "CASA: context-aware scalable authentication," in *Proc. of the Ninth Symposium on Usable Privacy and Security*, 2013, pp. 1–10.
- [79] M. T. Gebrie and H. Abie, "Risk-based adaptive authentication for Internet of things in smart home eHealth," in *Proc. of the 11th European Conf on Software Architecture: Companion Proc.*, 2017, pp. 102–108.
- [80] K. A. A. Bakar and G. R. Haron, "Adaptive authentication based on analysis of user behavior," in *2014 Science and Information Conf.*, 2014, pp. 601–606.
- [81] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics," in *Proc. of the 2017 ACM on Asia Conf on Computer and Communications Security*, 2017, pp. 386–399.
- [82] T. Karanikiotis, M. D. Papamichail, K. C. Chatzidimitriou, N.-C. I. Oikonomou, A. L. Symeonidis, and S. K. Saripalle, "Continuous Implicit Authentication through Touch Traces Modelling," in *2020 IEEE 20th Int. Conf. on Software Quality, Reliability and Security*, 2020, pp. 111–120.
- [83] J. M. Jorquera Valero *et al.*, "Improving the security and QoE in mobile devices through an intelligent and adaptive continuous authentication system," *Sensors*, vol. 18, no. 11, p. 3769, 2018.
- [84] A. Bucchiarone, R. Kazhamiakin, C. Cappiello, E. Di Nitto, and V. Mazza, "A context-driven adaptation process for service-based applications," in *Proc. of the 2nd Int Workshop on Principles of Engineering Service-Oriented Systems*, 2010, pp. 50–56.
- [85] G. Tamura, N. M. Villegas, H. A. Muller, L. Duchien, and L. Seinturier, "Improving context-awareness in self-adaptation using the DYNAMICO reference model," in *2013 8th Int Symposium on Software Engineering for Adaptive and Self-Managing Systems*, 2013, pp. 153–162.
- [86] L. Kulp, A. Sarcevic, M. Cheng, and R. S. Burd, "Towards Dynamic Checklists: Understanding Contexts of Use and Deriving Requirements for Context-Driven Adaptation," *ACM Trans. Comput. Interact.*, vol. 28, no. 2, pp. 1–33, 2021.
- [87] S. Gupta, A. Buriro, and B. Crispo, "Driverauth: A risk-based multi-modal biometric-based driver authentication scheme for ride-sharing platforms," *Comput. & Secur.*, vol. 83, pp. 122–139, 2019.
- [88] N. I. Daud, G. R. Haron, and S. S. S. Othman, "Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor," in *2017 IEEE Symposium on Computer Applications & Industrial Electronics*, 2017, pp. 152–156.
- [89] N. I. Daud, G. R. Haron, and D. Din, "Adaptive Authentication to determine login attempt penalty from multiple input sources," in *2019 IEEE Conf on Application, Information and Network Security*, 2019, pp. 1–5.
- [90] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive authentication: deciding when to authenticate on mobile phones," in *Presented as part of the 21st USENIX Security Symposium*, 2012, pp. 301–316.
- [91] A. Arfaoui, S. Cherkaoui, A. Kribeche, S. M. Senouci, and M. Hamdi, "Context-Aware Adaptive

- Authentication and Authorization in Internet of Things,” in *IEEE Int. Conf. on Communications*, 2019, pp. 1–6.
- [92] A. Hassan, A. A. Omala, M. Ali, C. Jin, and F. Li, “Identity-based user authenticated key agreement protocol for multi-server environment with anonymity,” *Mob. Networks Appl.*, vol. 24, no. 3, pp. 890–902, 2019.
- [93] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, “Adaptive privacy-preserving authentication in vehicular networks,” in *2006 First Int. Conf. on Communications and Networking in China*, 2006, pp. 1–8.
- [94] Y. Xi, K.-W. Sha, W.-S. Shi, L. Schwiebert, and T. Zhang, “Probabilistic adaptive anonymous authentication in vehicular networks,” *J. Comput. Sci. Technol.*, vol. 23, no. 6, pp. 916–928, 2008.
- [95] S. Sharma and B. Kaushik, “A survey on internet of vehicles: Applications, security issues & solutions,” *Veh. Commun.*, vol. 20, p. 100182, 2019.
- [96] R. Kainda, I. Flechais, and A. W. Roscoe, “Security and usability: Analysis and evaluation,” in *2010 Int. Conf. on Availability, Reliability and Security*, 2010, pp. 275–282.
- [97] J. Nicholson, L. Coventry, and P. Briggs, “Age-related performance issues for PIN and face-based authentication systems,” in *Proc. of the SIGCHI Conf on Human Factors in Computing Systems*, 2013, pp. 323–332.
- [98] S. Ruoti, B. Roberts, and K. Seamons, “Authentication melee: A usability analysis of seven web authentication systems,” in *Proc. of the 24th Int. Conf. on World Wide Web*, 2015, pp. 916–926.
- [99] E. Frøkjær, M. Hertzum, and K. Hornbæk, “Measuring usability: are effectiveness, efficiency, and satisfaction really correlated?,” in *Proc. of the SIGCHI Conf on Human Factors in Computing Systems*, 2000, pp. 345–352.
- [100] A. Wójtowicz and K. Joachimiak, “Model for aptable context-based biometric authentication for mobile devices,” *Pers. Ubiquitous Comput.*, vol. 20, no. 2, pp. 195–207, 2016.
- [101] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, “A usability study of five two-factor authentication methods,” in *Fifteenth Symposium on Usable Privacy and Security*, 2019.
- [102] A. Hassan, N. Eltayieb, R. Elhabob, and F. Li, “An efficient certificateless user authentication and key exchange protocol for client-server environment,” *J. Ambient Intell. Humaniz. Comput.*, vol. 9, no. 6, pp. 1713–1727, 2018.
- [103] D. Dasgupta, A. Roy, and A. Nag, “Toward the design of adaptive selection strategies for multi-factor authentication,” *Comput. & Secur.*, vol. 63, pp. 85–116, 2016.
- [104] J. Seifert, A. De Luca, B. Conradi, and H. Hussmann, “Treasurephone: Context-sensitive user data protection on mobile phones,” in *Int. Conf. on Pervasive Computing*, 2010, pp. 130–137.
- [105] R. J. Hulsebosch, M. S. Bargh, G. Lenzini, P. W. G. Ebben, and S. M. Iacob, “Context sensitive adaptive authentication,” in *European Conf on Smart Sensing and Context*, 2007, pp. 93–109.
- [106] D. Goel, E. Kher, S. Joag, V. Mujumdar, M. Griss, and A. K. Dey, “Context-aware authentication framework,” in *Int. Conf. on Mobile Computing, Applications, and Services*, 2009, pp. 26–41.

- [107] A. Fayad, B. Hammi, and R. Khatoun, “An adaptive authentication and authorization scheme for IoT’s gateways: a blockchain based approach,” in *2018 Third Int. Conf. on Security of Smart Cities, Industrial Control System and Communications*, 2018, pp. 1–7.
- [108] A. Forget, S. Chiasson, P. C. Van Oorschot, and R. Biddle, “Improving text passwords through persuasion,” in *Proc. of the 4th symposium on Usable privacy and security*, 2008, pp. 1–12.
- [109] B. Mbarek, M. Ge, and T. Pitner, “Self-adaptive RFID Authentication for Internet of Things,” in *Int. Conf. on Advanced Information Networking and Applications*, 2019, pp. 1094–1105.
- [110] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, “Ensemble: cooperative proximity-based authentication,” in *Proc. of the 8th Int. Conf. on Mobile systems, applications, and services*, 2010, pp. 331–344.
- [111] A. Primo, V. V. Phoha, R. Kumar, and A. Serwadda, “Context-aware active authentication using smartphone accelerometer measurements,” in *Proc. of the IEEE Conf on computer vision and pattern recognition workshops*, 2014, pp. 98–105.
- [112] Z. Cui, Y. Zhao, C. Li, Q. Zuo, and H. Zhang, “An Adaptive Authentication Based on Reinforcement Learning,” in *2019 IEEE Int. Conf. on Consumer Electronics-Taiwan*, 2019, pp. 1–2.
- [113] W. Xu, Y. Shen, Y. Zhang, N. Bergmann, and W. Hu, “Gait-watch: A context-aware authentication system for smart watch based on gait recognition,” in *Proc. of the Second Int. Conf. on Internet-of-Things Design and Implementation*, 2017, pp. 59–70.
- [114] I. You, J. D. Lim, J. N. Kim, H. Ahn, and C. Choi, “Adaptive authentication scheme for mobile devices in proxy MIPv6 networks,” *IET Commun.*, vol. 10, no. 17, pp. 2319–2327, 2016.
- [115] A. Mansour, M. Sadik, E. Sabir, and M. Azmi, “A context-aware multimodal biometric authentication for cloud-empowered systems,” in *2016 Int. Conf. on Wireless Networks and Mobile Communications*, 2016, pp. 278–285.
- [116] D. Dasgupta, A. Roy, and A. Nag, “Toward the design of adaptive selection strategies for multi-factor authentication,” *Comput. & Secur.*, vol. 63, pp. 85–116, 2016, doi: <https://doi.org/10.1016/j.cose.2016.09.004>.
- [117] J. O. Kephart and D. M. Chess, “The vision of autonomic computing,” *Computer (Long Beach. Calif.)*, vol. 36, no. 1, pp. 41–50, 2003.
- [118] A. Sasse, “Computer security: anatomy of a usability disaster, and a plan for recovery,” *Proc. CHI 2003 Work. HCI Secur. Syst.*, 2003.
- [119] M. Alshamari, “A Review of Gaps between Usability and Security/Privacy,” in *Int. J. Communications, Network and System Sciences*, 2016, vol. 9, pp. 413–429.
- [120] C. 10. Braz, A. Seffah, and D. M’Raihi, “Designing a trade-off between usability and security: a metrics based-model,” in *IFIP TC 13 INTERACT*, 2007, pp. 114–126.
- [121] A. Alarifi, M. Alsaleh, and N. Alomar, “A model for evaluating the security and usability of e-banking platforms,” in *Computing*, 2017, vol. 99, pp. 519–535.
- [122] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,” in *IEEE Symposium on Security and Privacy*, 2012, pp. 553–567.

- [123] N. Ben-Asher, J. Meyer, S. Möller, and R. Englert, “An Experimental System for Studying the Tradeoff between Usability and Security,” in *International Conference on Availability, Reliability and Security*, 2009, pp. 882–887.
- [124] N. Broders, C. Martinie, P. Palanque, M. Winckler, and K. Halunen, “A Generic Multimodels-Based Approach for the Analysis of Usability and Security of Authentication Mechanisms,” vol. 12481, pp. 61–83, 2020.
- [125] C. Martinie, P. Palanque, E. Bouzekri, A. Cockburn, A. Canny, and E. Barboni, “Analysing and Demonstrating Tool-Supported Customizable Task Notations,” *Proc. ACM Hum.-Comput. Interact.*, vol. 3, no. EICS, 2019.
- [126] H. Nishihara, Y. Kawanishi, D. Souma, and H. Yoshida, “On Validating Attack Trees with Attack Effects,” vol. 12234, pp. 309–323, 2020.
- [127] F. M., F. M., G. O., K. R., S. M., and T.-R. R., “Using Attack-Defense Trees to Analyze Threats and Countermeasures in an ATM: A Case Study,” *Pract. Enterp. Model.*, vol. 267, 2016.
- [128] B. Schneier, “Attack Trees,” 1999.
- [129] K. Halunen and O.-M. Latvala, “Review of the use of human senses and capabilities in cryptography,” *Comput. Sci. Rev.*, vol. 39, 2021, doi: 10.1016/j.cosrev.2020.100340.
- [130] M. Naor and A. Shamir, “Visual cryptography,” in *Workshop on the Theory and Application of Cryptographic Techniques*, 1994, pp. 1–12.
- [131] R. Bhatnagar and M. Kumar, “Visual cryptography: A literature survey,” in *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2018, pp. 78–83.
- [132] P. Punithavathi and S. Geetha, “Visual cryptography: A brief survey,” *Inf. Secur. J. A Glob. Perspect.*, vol. 26, no. 6, pp. 305–317, Nov. 2017, doi: 10.1080/19393555.2017.1386249.
- [133] S. Pape, *Authentication in Insecure Environments -- Using Visual Cryptography and Non-Transferable Credentials in Practise*. Springer Vieweg, 2014.
- [134] S. Pape, “Sample or Random Security - {A} Security Model for Segment-Based Visual Cryptography,” in *Financial Cryptography and Data Security - 18th International Conference, {FC} 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, 2014, pp. 291–303, doi: 10.1007/978-3-662-45472-5_19.
- [135] A. G. Forte, J. A. Garay, T. Jim, and Y. Vahlis, “EyeDecrypt—Private interactions in plain sight,” in *International Conference on Security and Cryptography for Networks*, 2014, pp. 255–276.
- [136] A. Perrig and D. Song, “Hash visualization: A new technique to improve real-world security,” in *International Workshop on Cryptographic Techniques and E-Commerce*, 1999, vol. 25.
- [137] H.-C. Hsiao *et al.*, “A study of user-friendly hash comparison schemes,” in *2009 Annual Computer Security Applications Conference*, 2009, pp. 105–114.
- [138] R. Nithyanand, N. Saxena, G. Tsudik, and E. Uzun, “Groupthink: Usability of secure group association for wireless devices,” in *Proceedings of the 12th ACM international conference on Ubiquitous computing*, 2010, pp. 331–340.

- [139] N. J. Hopper and M. Blum, “Secure human identification protocols,” in *International conference on the theory and application of cryptology and information security*, 2001, pp. 52–66.
- [140] A. Boldyreva, S. Chen, P.-A. Dupont, and D. Pointcheval, “Human computing for handling strong corruptions in authenticated key exchange,” in *Computer Security Foundations Symposium (CSF), 2017 IEEE 30th*, 2017, pp. 159–175.
- [141] M. Blum and S. Vempala, “The complexity of human computation via a concrete model with an application to passwords,” *Proc. Natl. Acad. Sci.*, vol. 117, no. 17, pp. 9208–9215, 2020.
- [142] S. Samadi, S. Vempala, and A. T. Kalai, “Usability of humanly computable passwords,” in *Sixth AAAI Conference on Human Computation and Crowdsourcing*, 2018.
- [143] J. Blocki, M. Blum, A. Datta, and S. Vempala, “Towards human computable passwords,” *arXiv Prepr. arXiv1404.0024*, 2014.
- [144] J. Hekkala, S. Nikula, O. M. Latvala, and K. Halunen, “Involving Humans in the Cryptographic Loop: Introduction and Threat Analysis of EEVEHAC,” in *18th International Conference on Security and Cryptography, SECURITY 2021*, 2021, pp. 659–664.
- [145] A. A. Jabal *et al.*, “Methods and Tools for Policy Analysis,” *ACM Comput. Surv.*, vol. 51, no. 6, 2019, doi: 10.1145/3295749.
- [146] F. Valenza, C. Basile, D. Canavese, and A. Lioy, “Classification and Analysis of Communication Protection Policy Anomalies,” *IEEE/ACM Trans. Netw.*, vol. 25, no. 5, pp. 2601–2614, 2017, doi: 10.1109/TNET.2017.2708096.
- [147] J. B. Hong, D. S. Kim, C.-J. Chung, and D. Huang, “A survey on the usability and practical applications of Graphical Security Models,” *Comput. Sci. Rev.*, vol. 26, pp. 1–16, 2017, doi: <https://doi.org/10.1016/j.cosrev.2017.09.001>.
- [148] M. Cheminod, L. Durante, L. Seno, F. Valenza, and A. Valenzano, “A comprehensive approach to the automatic refinement and verification of access control policies,” *Comput. & Secur.*, vol. 80, pp. 186–199, 2019, doi: <https://doi.org/10.1016/j.cose.2018.09.013>.
- [149] D. Dasgupta, A. Roy, and A. Nag, “Multi-Factor Authentication,” in *Advances in User Authentication*, Cham: Springer International Publishing, 2017, pp. 185–233.
- [150] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” *Cryptography*, vol. 2, no. 1, 2018, doi: 10.3390/cryptography2010001.
- [151] N. Andriamilanto, T. Allard, and G. Le Guelvouit, ““Guess Who?” Large-Scale Data-Centric Study of the Adequacy of Browser Fingerprints for Web Authentication,” in *Innovative Mobile and Internet Services in Ubiquitous Computing*, 2021, pp. 161–172.
- [152] P. Laperdrix, G. Avoine, B. Baudry, and N. Nikiforakis, “Morellian Analysis for Browsers: Making Web Authentication Stronger with Canvas Fingerprinting,” in *Detection of Intrusions and Malware, and Vulnerability Assessment*, 2019, pp. 43–66.
- [153] P. Eckersley, “How Unique Is Your Web Browser?,” in *Privacy Enhancing Technologies*, 2010, pp. 1–18.
- [154] C. F. Torres, H. Jonker, and S. Mauw, “FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting,” in *Computer Security -- ESORICS 2015*, 2015, pp. 3–19.

- [155] W. Oogami, H. Gomi, S. Yamaguchi, S. Yamanaka, and T. Higurashi, “Observation Study on Usability Challenges for Fingerprint Authentication Using WebAuthn-enabled Android Smartphones,” in *Symposium on Usable Privacy and Security (SOUPS 2020)*, 2020.
- [156] D. Wang, X. Zhang, Z. Zhang, and P. Wang, “Understanding security failures of multi-factor authentication schemes for multi-server environments,” *Comput. & Secur.*, vol. 88, p. 101619, 2020, doi: <https://doi.org/10.1016/j.cose.2019.101619>.
- [157] P. Grassi *et al.*, “Digital Identity Guidelines: Authentication and Lifecycle Management [including updates as of 03-02-2020].” Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2017, doi: <https://doi.org/10.6028/NIST.SP.800-63b>.
- [158] E. Klieme, J. Wilke, N. van Dornick, and C. Meinel, “FIDOuuous: A FIDO2/WebAuthn Extension to Support Continuous Web Authentication,” in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 1857–1867, doi: [10.1109/TrustCom50675.2020.00254](https://doi.org/10.1109/TrustCom50675.2020.00254).
- [159] F. Karegar, J. S. Pettersson, and S. Fischer-Hübner, “Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood,” in *Proceedings of the 13th International Conference on Availability, Reliability and Security, {ARES} 2018, Hamburg, Germany, August 27-30, 2018*, 2018, pp. 39:1--39:9, doi: [10.1145/3230833.3234514](https://doi.org/10.1145/3230833.3234514).
- [160] D. Preuveneers, S. Joos, and W. Joosen, “AuthGuide: Analyzing Security, Privacy and Usability Trade-Offs in Multi-factor Authentication,” in *Trust, Privacy and Security in Digital Business - 18th International Conference, TrustBus 2021, Virtual Event, September 27-30, 2021, Proceedings*, 2021, vol. 12927, pp. 155–170, doi: [10.1007/978-3-030-86586-3_11](https://doi.org/10.1007/978-3-030-86586-3_11).
- [161] N. K. Malhotra, S. S. Kim, and J. Agarwal, “Internet users’ information privacy concerns (IUIPC): The construct, the scale, and a causal model,” *Inf. Syst. Res.*, vol. 15, no. 4, pp. 336–355, 2004.
- [162] Y. Wang, G. Norice, and L. F. Cranor, “Who is concerned about what? A study of American, Chinese and Indian users’ privacy concerns on social network sites,” in *International conference on trust and trustworthy computing*, 2011, pp. 146–153.
- [163] K. Ishii and T. Komukai, “A comparative legal study on data breaches in Japan, the US, and the UK,” in *IFIP International Conference on Human Choice and Computers*, 2016, pp. 86–105.
- [164] S. Pape *et al.*, “Open Materials Discourse: Re-evaluating Internet Users’ Information Privacy Concerns: The Case in Japan,” *AIS Trans. Replication Res.*, vol. 6, no. 22, pp. 1–7, 2020, doi: [10.17705/1attr.00065](https://doi.org/10.17705/1attr.00065).
- [165] S. Pape *et al.*, “Re-evaluating Internet Users’ Information Privacy Concerns: The Case in Japan,” *AIS Trans. Replication Res.*, vol. 6, no. 18, pp. 1–18, 2020, doi: [10.17705/1attr.00061](https://doi.org/10.17705/1attr.00061).
- [166] H. J. Smith, S. J. Milberg, and S. J. Burke, “Information privacy: Measuring individuals’ concerns about organizational practices,” *MIS Q.*, pp. 167–196, 1996.
- [167] K. A. Stewart and A. H. Segars, “An empirical examination of the concern for information privacy instrument,” *Inf. Syst. Res.*, vol. 13, no. 1, pp. 36–49, 2002.
- [168] D. Harborth and S. Pape, “German Translation of the Concerns for Information Privacy (CFIP) Construct,” 2018.

- [169] W. Hong and J. Y. L. Thong, “Internet privacy concerns: An integrated conceptualization and four empirical studies,” *Mis Q.*, pp. 275–298, 2013.
- [170] F. Bélanger and R. E. Crossler, “Privacy in the digital age: a review of information privacy research in information systems,” *MIS Q.*, pp. 1017–1041, 2011.
- [171] B. Osatuyi, “Empirical examination of information privacy concerns instrument in the social media context,” *AIS Trans. Replication Res.*, vol. 1, no. 1, p. 3, 2015.
- [172] L. Lee, D. Fifield, N. Malkin, G. Iyer, S. Egelman, and D. Wagner, “A Usability Evaluation of Tor Launcher,” *Proc. Priv. Enhancing Technol.*, no. 3, pp. 90–109, 2017, doi: 10.1515/popets-2017-0030.
- [173] Z. Benenson, A. Girard, and I. Krontiris, “User Acceptance Factors for Anonymous Credentials: An Empirical Investigation,” *14th Annu. Work. Econ. Inf. Secur.*, pp. 1–33, 2015.
- [174] V. Venkatesh, J. Y. L. Thong, and X. Xu, “Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology,” *MIS Q.*, pp. 157–178, 2012.
- [175] D. Harborth and S. Pape, “Exploring the Hype: Investigating Technology Acceptance Factors of Pokémon Go,” in *2017 {IEEE} International Symposium on Mixed and Augmented Reality, {ISMAR} 2017, Nantes, France, October 9-13, 2017*, 2017, pp. 155–168, doi: 10.1109/ISMAR.2017.32.
- [176] D. Harborth and S. Pape, “Privacy Concerns and Behavior of Pokémon Go Players in Germany,” in *Privacy and Identity Management. The Smart Revolution - 12th {IFIP} {WG} 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers*, vol. 526, M. Hansen, E. Kosta, I. Nai-Fovino, and S. Fischer-Hübner, Eds. Springer International Publishing, 2017, pp. 314–329.
- [177] D. Harborth and S. Pape, “How Nostalgic Feelings Impact Pokémon Go Players - Integrating Childhood Brand Nostalgia into the Technology Acceptance Theory,” *Behav. {&} {Information Technol.}*, vol. 39, no. 12, pp. 1276–1296, 2019, doi: 10.1080/0144929X.2019.1662486.
- [178] D. Harborth and S. Pape, “Empirically Investigating Extraneous Influences on the ‘APCO’ Model - Childhood Brand Nostalgia and the Positivity Bias,” *Futur. Internet*, vol. 12(12), no. 220, 2020, doi: 10.3390/fi12120220.
- [179] D. Harborth and S. Pape, “Investigating Privacy Concerns Related to Mobile Augmented Reality Apps - A Vignette Based Online Experiment,” *Comput. Human Behav.*, vol. 122, 2021, doi: 10.1016/j.chb.2021.106833.
- [180] D. Harborth and S. Pape, “Investigating Privacy Concerns related to Mobile Augmented Reality Applications,” in *Proceedings of the 40th International Conference on Information Systems {ICIS} 2019, Munich, Germany, December 13-15, 2019*, 2019.
- [181] H. Nissenbaum, *Privacy in context*. Stanford University Press, 2020.
- [182] D. Harborth and S. Pape, “How Privacy Concerns, Trust and Risk Beliefs and Privacy Literacy Influence Users’ Intentions to Use Privacy-Enhancing Technologies - The Case of Tor,” *ACM SIGMIS Database DATABASE Adv. Inf. Syst.*, vol. 51, no. 1, pp. 51–69, 2020, doi: 10.1145/3380799.3380805.
- [183] D. Harborth, X. Cai, and S. Pape, “Why Do People Pay for Privacy?,” in *{ICT} Systems Security and Privacy Protection - 34th {IFIP} {TC} 11 International Conference, {SEC} 2019, Lisbon, Portugal*,

- June 25-27, 2019, *Proceedings*, 2019, pp. 253–267, doi: 10.1007/978-3-030-22312-0_18.
- [184] D. Harborth, S. Pape, and K. Rannenberg, “Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym,” *Proc. Priv. Enhancing Technol.*, vol. 2020, no. 2, pp. 111–128, 2020, doi: 10.2478/popets-2020-0020.
- [185] D. Harborth, S. Pape, and K. Rannenberg, “Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym (Poster),” in *SOUPS Poster*, 2021.
- [186] E. Costante, Y. Sun, M. Petković, and J. Den Hartog, “A machine learning solution to assess privacy policy completeness: (short paper),” in *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society*, 2012, pp. 91–96.
- [187] N. Guntamukkala, R. Dara, and G. Grewal, “A machine-learning based approach for measuring the completeness of online privacy policies,” in *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, 2015, pp. 289–294.
- [188] S. Zimmeck and S. M. Bellovin, “Privee: An architecture for automatically analyzing web privacy policies,” in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 1–16.
- [189] J. Gluck *et al.*, “How short is too short? Implications of length and framing on the effectiveness of privacy notices,” in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016, pp. 321–340.
- [190] R. N. Zaeem, R. L. German, and K. S. Barber, “Privacycheck: Automatic summarization of privacy policies using data mining,” *ACM Trans. Internet Technol.*, vol. 18, no. 4, pp. 1–18, 2018.
- [191] W. B. Tesfay, P. Hofmann, T. Nakamura, S. Kiyomoto, and J. Serna, “PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation,” in *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*, 2018, pp. 15–21.
- [192] W. B. Tesfay, P. Hofmann, T. Nakamura, S. Kiyomoto, and J. Serna, “I read but don’t agree: Privacy policy benchmarking using machine learning and the EU GDPR,” in *Companion Proceedings of the The Web Conference 2018*, 2018, pp. 163–166.
- [193] T. Nakamura, S. Kiyomoto, W. B. Tesfay, and J. Serna, “Easing the burden of setting privacy preferences: A machine learning approach,” in *International Conference on Information Systems Security and Privacy*, 2016, pp. 44–63.
- [194] W. B. Tesfay, J. Serna, and K. Rannenberg, “PrivacyBot: detecting privacy sensitive information in unstructured texts,” in *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, 2019, pp. 53–60.
- [195] D. Harborth, M. Hatamian, W. B. Tesfay, and K. Rannenberg, “A two-pillar approach to analyze the privacy policies and resource access behaviors of mobile augmented reality applications,” in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.
- [196] N. Paul, W. B. Tesfay, D.-K. Kipker, M. Stelter, and S. Pape, “Assessing Privacy Policies of Internet of Things Services,” in *{ICT} Systems Security and Privacy Protection - 33rd {IFIP} {TC} 11 International Conference, {SEC} 2018, Held at the 24th {IFIP} World Computer Congress, {WCC} 2018, Poznan, Poland, September 18-20, 2018, Proceedings*, 2018, pp. 156–169, doi: 10.1007/978-

3-319-99828-2_12.

- [197] S. Pape, A. Klauer, and M. Rebler, “Leech: Let’s Expose Evidently bad data Collecting Habits - Towards a Serious Game on Understanding Privacy Policies (Poster),” in *SOUPS Poster*, 2021.