Cyber Security for Europe

D3.5

Usable security & privacy methods and recommendations

Document Identification	
Due date	31st January 2020
Submission date	31st January 2020
Revision	1.0

Related WP	WP3	Dissemination Level	CO
Lead Participant	VTT	Lead Author	Kimmo Halunen (VTT)
Contributing Beneficiaries	VTT, CNR, KAU. KUL, UM, UPS-IRIT, UMU, GUF, UNITN	Related Deliverables	D3.1, D5.1

Abstract: This document presents the most relevant state of the art in usable security and privacy as well as usability related to these topics in the context of Cyber Security for Europe project. The document focuses on the most relevant use cases as identified in the demonstrators of this project. In the end, four recommendations are provided both for general use and in the context of use cases from CyberSec4Europe. We recommend the use of authenticated encryption whenever possible, early user involvement in the development of new security and privacy features, user modeling and tests for new features and the use of authentication methods that are secure and privacy-friendly. Also, future directions for research in these topics are provided. The main concern is to keep up with the changing user behavior and security and privacy technologies and threats.

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.

Executive Summary

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

This report presents an overview of the most relevant research on usability as it relates to security and provides some examples of usable security and privacy features. Because of sometimes conflicting requirements from usability, security and privacy, some tradeoffs are also presented. In addition, future research directions are discussed.

Based on the research and the expertise of the contributors, we provide four recommendations for improving usability in security and privacy technologies.

1. Use of authenticated encryption in the application layer or network layer communications whenever possible
2. Early user involvement should be ensured for new security and privacy features
3. User modeling and/or user tests should be conducted for new security and privacy features
4. Provide the users with authentication methods that are both secure and privacy-friendly

These can be applied both in the context of CyberSec4Europe project and in other areas, where the lack of usability is hindering security and privacy.

Future research topics include ways to bring new security and privacy features more easily to the developers of new technolgies and services and solving user authentication and digital identity problems in a way that is usable and also provides the necessary levels of security and privacy.

Document information

Contributors

Name	Partner
Kimmo Halunen	VTT
Manuel Cheminod	CNR
Matthias Beckerle	KAU
Luca Durante	CNR
Davy Preuveneers	KUL
Marko Kompara	UM
Célia Martinie	UPS-IRIT
Jorge Bernal Bernabe	UMU
Giuseppe Garofalo	KUL
Welderufael B. Tesfay	GUF
Sebastian Pape	GUF
Philippe Palanque	UPS-IRIT
Bruno Crispo	UNITN
Sandeep Gupta	UNITN

Reviewers

Name	Partner
Ahad Niknia	GUF
Jorge Bernal Bernabe	UMU
Alessandro Sforzin	NEC

History

0.01	2019-06-27	Kimmo Halunen	1st Draft
0.05	2019-10-17	Kimmo Halunen, Manuel Cheminod	2nd Draft
0.2	2019-10-31	Davy Preuveneers, Marko Kompara, Célia Martinie, Jorge Bernal Bernabe	3rd Draft
0.5	2019-12-17	All	4th Draft
0.6	2020-01-08	Kimmo Halunen, Davy Preuveneers, Giuseppe Garofalo, Welderufael B. Tesfay, Sebastian Pape	Final draft
0.7	2020-01-15	Kimmo Halunen, Philippe Palanque	Final version for review
1.0	2020-02-01	Ahad Niknia, Jorge Bernal Bernabe, Alessandro Sforzin, Kimmo Halunen	Final version after review

List of Contents

List of Figures

List of Acronyms

CTR	click-through rate
DID	Decentralized identifier
DP	Differential privacy
ECG	electrocardiogram
EEA	European Economic Area
ENISA	European Union Agency for Cybersecurity
ESM	Experience Sampling Method
EU	European Union
GAN	Generative adversarial networks
GAP	Generative adversarial privacy
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council, General Data Protection Regulation
GSM	Graphical Security Models
HTTP	Hypertext transfer protocol, a communication protocol
HTTPS	Hypertext transfer protocol secure, a communication protocol
LTS	Labelled Transition System
MFCC	Mel Frequency Cepstral Coefficients
MSR	Mission Success Rate
OTP	One time password
PCA	Principal Component Analysis
PET	Privacy enhancing technology
PGP	Pretty Good Privacy, an encryption tool
PII	Personally identifiable information
PIN	Personal Identification Number
SSI	Self-sovereign identity
SUS	System Usability Scale
TLX	NASA Task Load Index
TOR	The Onion router
ZKP	Zero knowledge proof

1 Introduction

Even the best security and privacy solutions will be effective only if they can be used by the end users correctly and without undue hindrance to the main tasks at hand. We would paraphrase the quote from Susan Dray[1] "If the user can't use it, it doesn't work" into "If the user can't use it, it is not secure". Thus, the usability of privacy and security solutions needs to guarantee a level of usability high enough so that user behavior will not jeopardize their benefits in terms of security and privacy.

Unfortunately, using these technologies is not always straightforward and, as an example, already in [1] many problems regarding the usability of the PGP encryption system have been pointed out. These usability issues can make it harder to reach the intended security and privacy goals. And follow up research has shown that the issue has persisted over the years [2], [3]. In the case of encryption, there have been many improvements that make end-to-end encrypted communications now available to large groups of people and that the majority of HTTP traffic is now encrypted HTTPS traffic. There are also other fields where security and usability have been improved such as user authentication, but still there are many open issues and a perfect solution does not yet exist. On the other hand, sometimes there are tradeoffs between usability and security or privacy meaning that a design solution favouring one property might require degrading another one [4], [5].

1.1 Security

Security is the main attribute that the different cybersecurity tools aim to provide for the system and its users. However, it is not always easy to define, what a secure system is. In addition, the different stakeholders (users, administrators, operators etc.) may have differing views of and objectives for security. Beyond, their behaviour is highly influenced by the perception of risks both in terms of probability of occurrence and impact [6].

Traditionally, information security has defined three main goals for security. These are *confidentiality*, *integrity* and *availability* [7]. By confidentiality they mean that the information is only accessible by the intended recipients of that information. Integrity means that the information has not been altered from sender to the recipient. Availability means that the information is accessible at the time it is needed.

Although modern information security differentiates more nuanced goals in addition to the three above, we can use them as the basic goals to which tools are aimed for. Furthermore, in this document we have the intended end user and usability as the focus. The end user can be a consumer of an everyday system, a system administrator or a decision maker. Thus, usability itself needs to be assessed for a wide variety of goals and actors.

1.2 Privacy

[1] https://worldofusability.wordpress.com/

The term “privacy” is used frequently in many everyday conversations. It is also discussed in political, philosophical, technical and legal discourse, especially when privacy issues are abundant.

However, there is not yet a unified definition of the concept and notion of privacy. This is primarily because privacy is dependent on context, cultural roots, individual as well as group preferences and perceptions. Regardless, there have been attempts to provide definitions. As such, Warren and Brandeis defined it as *”the right to be let alone”* [8]. Another well-known definition of privacy comes from [9] which reads as ... *“the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”*. Additionally, in the late 1990s [10] provided a more fine-grained definition of privacy; defining it as *“the ability of the individual to control the collection, retention, and distribution of information about herself”*. Also other discussion and definitions have been considered as in [11].

In the digital domain, privacy has often been reduced to meaning the use of encryption to protect the content of information that is stored or transmitted. This is a very narrow interpretation of privacy and today there is an understanding that privacy means also the protection of metadata related to communications, different decision made by algorithms that utilise user data and the overall surveillance of communications and even more recently our physical interactions through cameras and other sensors.

Achieving privacy in the digital domain is a very much ongoing research topic, with different tools and regulation coming up related to various use cases and in different regions and jurisdictions. Because data about users is considered valuable by many companies, there is also several „races“ where for example advertisers try to find ways to get information about users, the users apply ad-blocking software to protect their privacy (and in some cases security) and then websites applying ad-blocker-blockers and so on. Privacy protection mechanisms can also be present on the user interface itself before the information goes through the network as presented in Figure 1 which is an implementation of the Eigen space concept in [12].

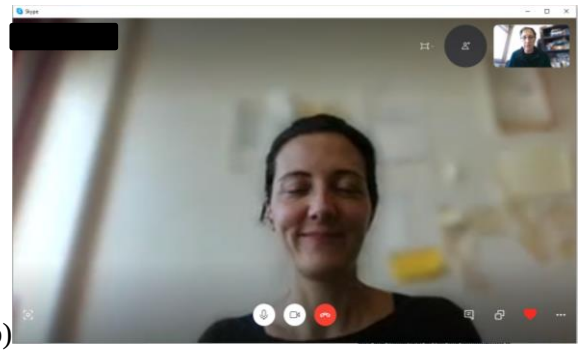
a)  b) 

Figure 1. Privacy partly preserved on Skype by fuzzing video stream background - a)screenshot not fuzzy, b) screenshot fuzzy

1.3 Usability

Usability is defined as *"the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"* [13].

Effectiveness corresponds to the capacity of the system to offer means to the users to achieve their goals. Task analysis and modelling correspond to the study of user tasks an activities and how interaction takes

place between users and the interactive systems. Effectiveness is thus usually assessed in term of coverage of the user tasks by the systems. If some goals or tasks are not feasible on a given system then its effectiveness is reduced and the users will have to find workarounds to perform their job.

Efficiency corresponds to the quantity of resources (e.g. time, effort, actions) consumed by the users when achieving their goals. The efficiency attribute of Usability can be computed using user evaluation through experimental settings and by measuring physical variables such as time needed to perform a task. This is usually called quantitative evaluation of efficiency and provides objective measurement. Qualitative evaluation can also be performed by asking users to provide subjective information such as workload perception. In that case, assessment is performed using questionnaires that are filled in by the users after the performance of the tasks. NASA Task Load Index (TLX) [14] is an example of such questionnaire for subjective self-assessment of workload by users. Despite these limitations, analysis of operators' tasks provides an efficient way for performing formative usability evaluation [15]. Indeed, efficiency correlates with tasks as the more tasks the user needs to do, the slower he/she will be and thus the less efficient. This measure is of course not as precise as usability tests, but it is a good way to evaluate the usability at an early stage in the system development and before the actual user interface is fully defined. However, task based assessment increases the coverage of user work [16] as usability test is mainly performed on few scenarios due to the fact that postprocessing of data gathered in the tests is extremely time consuming.

Satisfaction corresponds to the user's subjective perception of using the system and how pleasant it is to use it. The most common way to evaluate satisfaction is via standardized questionnaires such as SUS (System Usability Scale) [17].

1.4 Aim of the document

This document is part of CyberSec4Europe project and its research efforts in Work Package 3. This deliverable is one of the results from Task 3.6 which considers usable security and user-centric cybersecurity. The research activities in Task 3.6 aim to improve usability of security and privacy technologies in many fronts and the goal is to achieve progress in many of the future research directions and open questions identified in this document (see Section 6 for more details).

The aim of this document is to showcase the most important and relevant usable security and privacy methods and methods to improve usability in security and privacy technologies. From these a set of recommendations is formed. The recommendations are also linked to the demonstrators of this project from WP5 in order to help the designers and implementers of these demonstrators. Furthermore, some open questions related to the topics discussed in this document are provided. These can be used as a further input to the roadmap work in WP4 in relevant fields and as challenges to researchers working in these fields.

1.5 Structure of the document

This section gives a brief introduction and defines the basc concepts used in this document. The second section describes the state-of-the-art in relevant fields and gives background information on the topics of security, privacy and usability. The third section gives examples of usable security and usability in security and the fourth section similarly for privacy. The fifth section gives some notable tradeoffs as well as our

recommendations for usable security and privacy. The sixth section briefly discusses some important future directions and the seventh section gives a concise conclusion. In the end of this document an extensive list of references is given for the interested reader to find more detailed information on the topics discussed in this document.

2 State of the art and background

Usability has been a topic of study and practice in the fields of security and privacy for some time and there are results that form the foundation of our current knowledge base. The conference SOUPS (Symposium on Usable Privacy and Security) is the main forum for publication in that domain but most conferences in Human-Computer Interaction feature usable security sessions. Security-centered centered conferences such as IEEE DSN (Dependable Systems and Networks), SAFECOMP (Safety in Computing and Security) or IEEE SP (Symposium on Security and Privacy) regularly feature papers dealing with usability aspects of security mechanisms. This section briefly presents the most relevant results and how they relate to the research work in CyberSec4EU project.

2.1 Privacy and usability in user authentication

Biometric data embeds information about the user which enables (if user interface design of the authentication mechanism addresses usability concerns correctly) transparent and friction-less authentication. Despite being a more reliable alternative to traditional knowledge-based mechanisms, sharing the biometric template with third parties raises privacy concerns for the user. Recent research has shown how biometric traces can be used to infer sensitive attributes like medical conditions or soft biometrics, e.g. age and gender.

Mordini and Ashton [18] have performed an extensive study of medical pattern retainment in biometric templates: psychiatric conditions can be inferred from gait traces, chromosomal diseases can be accurately guessed from face images or fingerprints, while neurological pathologies have been associated to a broad range of behavioural biometrics. The same leakage potential holds true for electrocardiogram (ECG) signals [19], iris recognition [20] and other bio or behavio-metrics [21]. Similarly, soft biometrics like age, gender or race are linked to physiological or behavioural traits of the user.

The approaches to protect user's privacy divides into context-free and context-aware techniques. Context-free techniques, like differential privacy (DP), model worst-case adversaries regardless of his/her real capabilities and discarding relevant contextual information, i.e. about the problem to be solved. DP provides strong privacy guarantees, delivering a shrinking in data usefulness. Context-aware strategies, on the other hand, incorporate the retainment of task-specific utility by selectively adding noise where it matters. This advantage comes at the expenses of a formal characterization of the relationship between public variables, i.e. what we aim to share, and private variables, i.e. what we aim to protect, which is rarely available in practice.

Data-driven optimization has been recently proposed as a mean to achieve context-aware privacy. By exploiting recent advances in adversarial optimization, it is possible to model the joint distribution between shared and private variables. Generative adversarial networks (GANs) have been recently proposed as an effective tool to achieve this goal [22]. They model a min-max game between a generator and a discriminator, where the former tries to fool the latter in an iterative learning process. This concept has been first adapted to the privacy domain by Huang et al. who define the generative adversarial privacy (GAP) framework [23].

Morales et al. [24] recently proposed a method to reduce gender and race information in latent representations of face images. Their method is based on a modification of the triplet loss function, which is a commonly employed in face verification scenarios [25]. Malekzadeh et al. [26] have considered motion data and gait authentication in a different min-max optimization scenario: perturbing identity while preserving task-specific utility. Their classification task is activity recognition, which has been extensively studied in the gait literature in addition to being arguably a private variable. Osia et al. [27] investigates the use of Siamese networks for privatizing the user's identity while preserving gender classification accuracy. Besides the different learning goal, they focus on fine-tuning existing, pre-trained networks.

In general, the trade-offs between usability, privacy and security have been studied in the context of user authentication quite extensively. Bonneau et al. [5] propose a framework for evaluating different web authentication methods. Their framework considers aspects of usability, security and privacy and the evaluation of web authentication methods is provided using that framework. This has been extended by Halunen et al. [4] to cover a wider range of authentication methods and also to more accurately capture some attributes in user authentication. Some user authentication methods have used such frameworks to show how they improve from known state of the art e.g. in [28]. Recent field studies have also incorporated real-world analysis of current unlocking and behavior and users' perception of risk that influences these behaviors [29]. Such studies demonstrate that security mechanisms must also be evaluated involving methods and techniques from the Human-Computer Interaction domain in order to ensure acceptance [30].

2.2 Measuring Security and Privacy

Measuring security is hard since it can only be measured indirectly [31]. Additionally, it is often impossible to test all security requirements since security requirements often differ from traditional requirements in the way that the absence of an attribute is required (e.g. no buffer overrun, SQL injection) [32]. Even worse, the security of a system cannot be considered just by itself and the system's environment, the level of abstraction and the context affects the security of the system. As a consequence, security and security risk management depends, to a large degree, on modelling threats and attackers' behaviour. For organisations, this topic is mostly covered from a compliance perspective and there a hundreds of metrics to choose from, e.g. maturity level metrics of security controls which are mainly described in standards and rely on the security knowledge of security experts [33].

Similarly, the measurement of privacy, privacy risks and losses is hard. Several measurements for anonymity exist, such as the degree of anonymity based on entropy [34], [35], k-anonymity where the data of an individual cannot be distinguished from at least k-1 other individuals [36], [37] and differential privacy and its variations, where an observer cannot tell by the outcome of a computation if the information on a specific individual was used [38], [39]. Some results contain even more abstract concepts [40].

However, connecting these metrics with real world data and assurances is particularly hard. For example, it's hard to deal with probabilistic anonymity [41] respectively assurances. What does it mean for an individual if its identity is revealed with a certain probability? How can possibly privacy revealing information be found in unstructured text such as posts in social networks and how much information is needed to identify a user [42]? Furthermore many re-identification attacks deal with external data sources which they connect with an existing data set to identify users from a "anonymized" data set [37], [43]. Even without malicious behavior [44] has demonstrated that users identity of Netflix platform can be recovered

from datasets shared by the company in order to improve their recommender system [44]. These examples all demonstrate that in general it is hard to anticipate and measure privacy or the privacy loss caused by a data leakage or sharing.

On the other hand, from an individual user's perspective the measurement of security and privacy is ambiguous, i.e. since most users do not have a particular threat or attacker model in mind. Since the aim for this document is to showcase the most important and relevant usable security and privacy methods and methods to improve usability in security and privacy technologies, when we discuss about improving security, we have a more intuitive model of security and privacy in mind – fully aware that there is no one size fits all. Since for most users the decision is rather if they use a security method at all than which method to select (e.g. encrypt mails by PGP or S/MIME[2]), this consideration is sufficient for the purpose of this document. However, the user interfaces and related interaction techniques might have a huge impact on usability whatever security method is used.

[2] https://datatracker.ietf.org/wg/smime/about/

3 Examples of usable security and methods to improve usability in security

In the CyberSec4Europe project one task (Task 3.6) specifically considers technologies and methods to improve the usability of security and privacy technologies. Within this task there are seven assets that are developed in this project.

1. Guidelines for GDPR compliant user experience. Regulation and best practices review with focus on GDPR. Check a subset of local best-practices and identify requirements or issues with existing implementation.
2. HAMSTERS. Notation and tool to support: user task based design and development of user interfaces and user interactions, design and development of user training
3. PetShop. Notation and tool to support design and development of HMI (high-fidelity prototyping of user interfaces and user interactions).
4. EEVEHAC. EEVEHAC establishes an end-to-end encrypted channel that is 1) human authenticated and 2) visualizably encrypted.
5. TATIS. Enhanced open source threat intelligence sharing platform to share indicators of compromise in trustworthy manner on top of the MISP platform.
6. Tangible interactions for privacy management. This represent a solution to the problem of physical privacy in users' immediate physical environment that may arise through technological devices, or directly by other humans physically present around the user. This solution provides: 1) a waist belt to sense the environment around the user to detect people, objects and movements; 2) a wrist band that can vibrate to empatetically and actively warn the users in case a privacy threat is detected. This technology allows users to take immediate action when informed or automatically responds appropriately on the users' behalf, and learns continuously from user responses to understand their context and needs.
7. SYSVER. The tool supports security administrators of large distributed systems in the verification of correct implementation of the security policies in the actual system possibly affected by (software) vulnerabilities. When problems are detected, the tool leverages the detailed analysis results to investigate possible changes to apply in the system to correct the anomalies (conflict resolution).

These assets are described in more detail in the Deliverable D3.1.

In general, for improving the usability of security and privacy, it is important to understand the users' mental models about their needs and preferences for security and privacy. After that, this information has to be converted into technical means.

There are explicit and implicit ways of converting the information from the users' mental model into systems. Explicit conversion generally refers to direct user input. If a security decision has to be made, the information is presented to the user and the user is asked to make a decision. Implicit conversion of the users' mental model can be done if a sufficient technical representation of the users' mental model exists that then can be used to predict the users' decisions. Under this premise, decisions can be done automatically and potentially without bothering the user.

These user-representing models can be generated by gathering information about the user in the form of user studies and/or by observing the users behavior, i.e. analyzing former decisions and interactions of the user with hardware and software. The gathered information can, for instance, be used to train a machine-learning model that can be used to automate the decision making process. This approach is already widely used in software development and marketing to optimize the user experience[3], and influence consumer behavior by using the gathered information to show targeted ads. However, so far it is seldom used to optimize the security and privacy settings of users.

Both variants of converting the users' mental model into technical means have disadvantages.

The first, direct variant might be inconvenient for the user if the user has to make many decisions manually. Experience shows that in such cases users tend to quickly circumvent such inconveniences by deactivating security mechanisms, allow all accesses without checking for consequences, or mostly selecting the option that appears first, which easily leads to security and privacy problems.

The second variant, to automated decision-making based on a technical representation of the users' mental models, can lead to wrong decisions if the user model is flawed or if information about the user or the environment is missing. Even small errors can lead to wrong automated decisions with potentially impactful negative consequences for the users' security and privacy. In addition, the GDPR (Art. 15 I (h)) requires informing meaningfully about the logic involved in automated decision making, an therefore a right to explanation for data subjects about automated decision making has been derived. Transparency of the automated decision making process is important so that users understand what happens to their data. Moreover, pursuant to Art. 22 GDPR, data subjects have the "*right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"*. Hence, a fully automated process could therefore be in non-compliance with the GDPR. Therefore, this approach requires explicit consent and further privacy measures.

A promising compromise is to use technical representation of the users' mental model to generate meaningful defaults for the user and support the user making informed decisions by providing information that is more relevant. A possible idea to investigate is to make the decision process as easy as possible and potentially adaptive to the expertise and needs of each user. However, it is important to note that automating user activity usually comes with complex challenges harder to solve than designing a usable user interface. Automation surprises [45], lumberjack analogy [46] and complexity of automation [47] demonstrate that migration of tasks from users to systems remains a hard challenge highly intertwined with user interface design (as only part of the tasks are automated) [48]. Beyond, [49] has demonstrated that automation biases decision making processes.

[3] User Experience is a property, related to usability, that receives a lot of attention in the HCI domain. This property goes deeper into the users' perceptions and internal states (e.g. aesthetics, emotions, meaning and value, …). While user experience is being added to the ISO 9241 standard on Usability (in part 210), it goes beyond the work package on Usable Security. A list of six orthogonal attributes for User Experience can be found here [114] while academic and industrial resources can be found at http://www.allaboutux.org/.

In the context of CyberSecurity4Europe, to generate technical representation of the users' mental models and meaningful defaults, user studies in the form of interviews or statistical surveys for finding meaningful defaults as well as user segmentation studies can be conducted (see e.g. [50]). That and user data analyses are ways to understand what security and privacy settings users want to achieve and what kind of information they would need to make informed decisions. Understanding the users is the first step to make security and privacy decision-making a user centric process that satisfies and protects users without overstraining them.

3.1 Information visualization

The problem of usability in security spans over multiple aspects of the design and implementation of security mechanisms and tools. In particular, when we consider software tools that provide some kind of security analysis of a system, it is important to remark the usability of the results provided. The better a tool conveys its results the more easily and efficiently the user (system administrator) can evaluate and use them to improve the security of the system itself. In that domain, the focus is not on end-users anymore but on the tasks and work of security experts and managers.

Information visualization is a complex topic and it can both improve and hinder the usability and understanding of the system and the state of the system. A good visualization will give the relevant information to the user at a glance and a bad visualization will either give false information or present the information in a confusing or misleading way. IEEE society organizes a huge yearly event called VisWeek that gathers several conferences about information visualization (InfoVis), Visual Analytics (VAST) or Software Visualization (SoftVis).

There are also many different security related data that can be visualized for end users. Some are intuitive for example presenting the connections of a network with a graph (although the graph of a large network can become messy and hard to comprehend). Some less intuitive parts are for example visual cryptography [51], where cryptography is presented and applied in visual form. This type of presentation has some use cases e.g. [52]–[55], but it has not been researched a lot and has not gained wide adoption. Mostly because the encryption relies on XOR-variants, and thus the used keys can only be used once or a very low number of times [56].

3.2 The complexity and usability of Graphical Security Models

One way to deal with the evaluation of the security of large and complex systems is to leverage model-checking techniques to exhaustively analyze all the possible system state evolutions to identify those states that are not secure with respect to some metrics.

In this context, formal descriptions for the system model and the analysis results are required. A family of largely used models, especially for the description of the results, is the "Graphical Security Models" (GSM) family. This family includes, for instance, "Attack Graphs" and "Attack Trees". The problem with the exhaustive analysis is that the resulting graphs are often too complex and require some post-analysis to make them usable [57].

We consider here a specific example of a security analysis tool that performs formal analysis on a networked system and provides the results in the form of GSM. This tool is part of the CyberSec4Europe project's

asset portfolio, which has over 30 assets. Out of these there are six especially relevant in the scope of usable security and privacy.

The tool in question is the "Sysver" asset [58], it uses the formal description of a networked system and analyzes all the possible sequences of actions that an agent can perform leveraging his privileges and possible flaws in the configuration of the system resources. The raw result provided by the tool is a Labelled Transition System (LTS) where each state represents the state of the agent (his knowledge) and the transitions represent the actions that the agent can perform in any given state. This kind of information is checked against a security policy (access control list) to assess if the agent can actually perform all and only those actions that are allowed in the policy. In complex and large systems the resulting LTS size can quickly become a burden for the system administrator that should analyze it.

The usability of this kind of security tool is strictly related to the usability of its results. Large and complex graphs are difficult to analyse by a human operator. Of course, some kind of automatic reasoning and analysis are possible but, in some way, this would “bypass” the human administrator and this is not always desirable, To mitigate this problem and to move improve the usability of this approach, some techniques are possible, based on the construction of “abstract” and simplified views of the complete results. In particular, two techniques have been used in the proposed asset. Firstly, an abstract view of the overall check of the LTS against the policy is provided in form of a simple table where each possible operation (transition in the LTS) is evaluated and flagged as an error if not allowed in the policy. This kind of summarized view hides the complexity of the complete LTS and allows the system administrator to focus on the errors that require some fixing [59].

When the details about a specific error are required, the tool leverages a second post-analysis technique to simplify the LTS. While the LTS includes all the possible sequences of actions that an agent can perform, the simplified LTS includes only the minimal sequences that allow the agent to perform a specific action [60]. This greatly simplifies the task of the system administrator when he/she needs to find fixes for the errors. Moreover, this technique allows the tool to perform some automatic reasoning and to propose configuration changes that can fix the errors to the administrator [60].

3.3 User Authentication

Biometrics are nowadays a popular form of user authentication due to their ease of use, robustness and uniqueness compared to traditional knowledge-based systems, such as PINs and passwords. Especially on smartphones, the use of fingerprints and face authentication to unlock the device is becoming more prevalent. Moreover, the wide availability of mobile sensors allows for the deployment of near frictionless multi-modal user authentication systems.

Behavioral biometrics [61] are a particular kind of authentication factor that verify the identity of users by the way they behave. They operate in the background in a continuous manner while the user interacts with an application. Typical examples of behavioral biometrics are keyboard dynamics [62] and mouse movements [63], and voice biometrics [64]. Sensor based gait recognition is also explored as a solution for unobtrusive user authentication [65]–[68]. Despite being less robust than well-established biometrics, motion data takes advantage of body worn sensors that are widely implemented in modern devices and require little to no effort by the user. By enabling continuous user authentication, gait authentication is a

natural candidate for multi-modal settings, i.e. combining different types of biometric authentication factors. In this way, we can not only improve the accuracy of the user authentication system, but also strengthen the system against forging and spoofing attacks, while offering a user-friendly experience.

However, as soft biometrics like age, gender or race are linked to physiological or behavioural traits of the user, misuse of biometric templates may lead to severe privacy leakages for the user [21]. Previous work [18]–[20] has already shown the presence of sensitive data in biometric traces, including medical conditions and soft biometrics. In the case of gait based user authentication, Van hamme et al. [69] demonstrated the feasibility of age and gender estimation from gait traces in the frame of the OU-ISIR Wearable Sensor-based Gait Challenge: Age and Gender (GAG 2019) competition. The ever-improving resilience of continuous authentication systems based on accelerometer and gyroscope measurements, as well as other sensors, clashes with the lack of a comprehensive assessment in terms of sensitive data leakage, demanding for techniques to protect a user's privacy against sensitive inferences.

3.4 Encryption of Communications

One area where recent advances has been made to improve the security (and arguably also privacy) of users is in the encryption of communications. As mentioned in the introduction, correctly using encryption methods to protect communications was seen as hard from usability perspective [1]. Some recent advances have made such end-to-end encrypted (E2EE) messaging a commonplace and easy to use experience for hundreds of millions or even billions of users.

The important technology behind this development is the Signal protocol by Open Whisper Systems[4]and the Signal application[5]. When WhatsApp adopted this technology to provide E2EE messaging for their users, it signaled a major change in the encryption landscape of communications between individuals. Of course, there are many other applications that now provide similar protection of communications and even Facebook is said to be contemplating adding E2EE messaging to their Messenger application[6]. In [70] the authors provide a great overview on the topic of secure messaging. These examples show, that it is possible to achieve great security benefits, without affecting user experience in any meaningful way. Thus, this is a prime example for usable security.

This development has caused some discomfort in some law enforcement circles and there have been demands for weakening E2EE by the FBI, politicians from US, Australia and in the EU based on terrorist threat or the abuse of children. However, this weakening would make the wider public much less safe and only marginally help in catching the wrongdoers. This has been well argumented in [71] by many of the leading cryptographers.

E2EE is not the only field where additional security can be achieved through encryption. Network traffic (especially HTTP traffic) has been largely unencrypted until some recent developments. This means that a

[4] https://open-whisper-systems.readme.io
[5] https://www.signal.org
[6] https://www.theverge.com/2019/1/25/18197222/facebook-messenger-instagram-end-to-end-encryption-feature-zuckerberg

lot of the content included in our browsing has been unsecured. However, recent developments have produced website developers easy tools to make their sites run HTTPS, the encrypted version of HTTP. The Let's Encrypt -project provides an easy way to secure your website and their statistics show a remarkable increase in HTTPS adoption[7]. Again, this shows that easy to use tools have a huge impact on the adoption of a technology. HTTPS has been available for a long time, but the setting up of a certificate and all other setup for the encryption has been hard for the administrators.

For the end users, many browsers offer functionality that will enforce HTTPS is used in browsing whenever possible[8]. This makes the user experience very smooth also for the end users of web. Of course this type of encryption brings some side effects and the user may be prompted with a security warning (e.g. because a certificate has expired. There is research showing that users tend to ignore such warnings and thus can be exposed to phishing etc. [72]

Overall, these examples show that the original problems presented in [1] and others obstacles related to usability of encryption can be mitigated and overcome. This then provides the users with more security in their communications.

[7] https://letsencrypt.org/stats/
[8] https://www.eff.org/https-everywhere

4 Examples of usable privacy and methods to improve usability in privacy

This section presents some relevant examples of usable privacy and usability in relation to privacy.

4.1 GDPR compliant user experience

Regulation (EU) 2016/679 of the European Parliament and of the Council or more commonly known as General Data Protection Regulation (GDPR) [73] is a legal framework that sets guidelines for the collection and processing of personal information. This is arguably the most significant change in data privacy regulation in the last few decades. The regulation applies across the entire European Union (EU) and European Economic Area (EEA) region. However it's reach is actually much larger as the primary principle behind the GDPR is that it views personal data as the property of the individual/natural person, and it therefore applies to anybody storing personal information about citizens in Europe (with some exceptions, like personal use and others), including companies on other continents.

The regulation was designed to give the citizens of the EU and EEA greater control over their personal data and ensure that their information is being adequately protected. According to the GDPR, personal data is any information related to a person such as a name, a photo, an email address, a computer IP address etc. For any entity that processes personal data and does not comply with the regulation, the GDPR stipulates harsh fines. In turn, the companies processing personal data have put a lot of effort into compliance with the GDPR requirements. However, like any other legislation, and even more so as the GDPR is meant to be a framework, the nuances of the regulation are often complex. This steams from the differences how the holders of data interpret the regulation and how the European courts interpret it, and what each of the parties consider appropriate ways of implementing the given regulation. While big companies can afford to hire staff to make sure any processing of personal data, they do is compliant with the regulation, this is much harder for smaller companies to achieve.

For this reason, as part of the asset development in the CyberSec4Europe project, we propose to establish GDPR Guidelines that will collect and present in a simple and understandable way the specific points of the GDPR regulation and provide best practices and what solutions (local) supervisory authorities, European Commission and ultimately the European Court of Justice, consider to be appropriate or how they interpret the regulation itself. The final interpretation of the GDPR is within the jurisdiction of the European Court of Justice. However, the opinions of the supervisory authorities are also very relevant as they are responsible for investigations of non-compliance, the corrective powers they hold and their knowledge of local (member state) specific legislation. This work is conducted in the CyberSec4Europe project and is part of the asset portfolio of the project. However, detailing these best practices is beyond the scope of this more general document.

GDPR Regulation is meant to ensure appropriate security mechanisms are used to protect personal data, but even more importantly, it sets rules about when and for what purpose personal data can be used. Effectively this means that data holders cannot freely use the collected personal data without legal or contractual basis or explicit consent from the data owner. A big part of this is the idea of data transparency that the Regulation has also imposed. Data transparency gives each natural person an ability to know what personal data each

specific controller or processor has on them and for what purposes they are being used. This information must be conveyed in a concise, transparent, intelligible and easily accessible form, using clear and plain language. In addition to giving this information to the users, this also brings the issue of their data privacy to the attention of the users. In addition, since the regulation requires the information to be presented in a simple manner the effect is an improved usability in privacy. However, how data controllers and processors achieve this and other GDPR requirements can be, as we have mentioned before, anything but simple. The GDPR Guidelines will help simplify the understanding of the GDPR Regulation, which will improve the implementation of the regulation, and the final result will result in better usability in privacy.

When talking about usable security the focus is often in the individual or an average user. In this case, the primary beneficiary of this collection of information on good GDPR related practices are smaller and medium sized controllers and processors of personal data. They (and everybody else for that matter) will be able to freely access a curated collection of information regarding the necessary GDPR requirements and possible methods of achieving them. The given recommendations would therefore allow their user an easier way to check and ultimately achieve compliance with the GDPR Regulation. Even though the primary beneficiaries of the GDPR Guidelines are the personal data controllers and processors, individuals will also be able to take advantage of the final product. They will be able to educate themselves about their rights and about methods that controllers and processors that hold their data have to employ when protecting their data. Having a well-educated consumer base ultimately also forces the service providers to produce better services, further improving the privacy of personal data.

4.2 Usability in Identity and privacy management for decentralized systems

The concept of privacy embraces the right given to citizens to Control and manage their personal data at any time, ensuring user self-determination, as defined in the European GDPR [73]. Privacy as Control can be implemented through Privacy Enhancing Technologies (PET), ensuring selective and minimal disclosure of credentials and personal attributes using, for instance, Anonymous Credential Systems [74] such as Idemix [75], which employs ZKPs (zero knowledge proofs) to reveal the minimal amount of information to the verifier (usually a service provider), even without disclosing the attribute value itself. However, current Anonymous credential systems implementations such as Idemix are complex and difficult to manage by final users.

Identity Management based on Self-Sovereign identities systems [76] (SSI) focuses on providing a privacy-respectful solution, enabling users with full control and management of their personal identity data without needing a third-party centralized authority taking over the identity management operations. Thus, citizens are not anymore data subjects, instead, they become the data controller of their own identity. This is, they can determine the purposes, and ways in which personal data is processed, as they manage directly their personal data during their online transactions. There are already proposal for privacy-preserving SSIs [77] but not yet applied in blockchain. Blockchains bring many advantages encompassing provenance, accountability, traceability and transparency of the transactions stored in the ledger. However, non-technical people might find difficulties to deal with the privacy-control and management in distributed systems and ledgers, due to its complexity [78], [79]. SSI can be applied through blockchain, which facilitates the governance of the SSI system, increasing the performance to Internet scale and enabling the accessibility of identities to everyone. Blockchain enables sovereignty as users can be endowed with means to transfer

digital assets, including user decentralized identifiers (DID) [80], DID documents, identity attributes, verifiable claims and proofs of identity [6] (including ZKPs), to anyone privately, without rules in behind.

In this context, as part of the SSI system functionalities, configuring and selecting the personal attributes to be included in a claim - to meet the requirements imposed by the service provider (i.e. verifier) - might be also cumbersome and not privacy-friendly. Thus, protocols/ specifications and their corresponding appealing front-end apps for blockchain are needed to automate the data release/consent/selection of blockchain verifiable claims [81] and management of DID Documents and data [80], and in general, to deal with end-user privacy management.

To deal with these privacy usability aspects, the asset *SelfSovereign-PPIdM* (Self-sovereign privacy-preserving IdM in blockchain) being designed in this project, is tackling the Identity and privacy-management bearing in mind usability recommendations. Thus, users will be able to configure their privacy-policies for sharing personal data in the blockchain, access to services and give consent, in a user-friendly way, while doing it as much automated as possible. It embraces the best ways to visualise privacy management for users accessing and sharing personal information and assets through blockchain when using "Verifiable Credentials", and best ways of authorization and privacy policies needed to indicate which specific personal information can be shared in a transaction, complying with minimal disclosure principle. Besides, this asset will deal with access control policies and manage their personal data, to indicate which data can be accessed by whom, in in a particular context, through blockchain, using verifiable credentials and Decentralized Identifiers.

4.3 Usability in selected use cases of this project

Usability is a critical factor that influences end-users to use particular security or privacy mechanism. We present some important considerations that account for the growing significance of usability in systems such as online banking, supply chain security assurance, privacy-preserving identity management, maritime transportation, medical data exchange, and smart cities, which are the demonstrator cases in the Cyber Security for Europe project. The subsections below relate to some of the many requirements identified in the deliverable D5.1 Requirements Analysis of Demonstration Cases Phase1 of CyberSEc4Europe project. For the sake of brevity, we have not included the full list of requirements and do not reference these in full in this document.

- Usage easiness is an intrinsic characteristic that impacts end users' decisions to go for a security and privacy mechanism. Usability aids to determine the effort required by users to interact with a system, their performance in terms of time and errors but also their satisfaction (that might contradict performance measures as in [12]).
- Many critical sectors, e.g., banking and finance, transport, smart offices, etc., require users to adhere to prescribed security and privacy guidelines to maintaining and safeguarding them from adversaries. At the same time, they consolidate the security, privacy, and safety of their legitimate users. Usable security can aid to overcome the inadvertent (or even deliberate) undermining of security by end-users (like writing down their password on a post-it next to their computer screen).
- Sometimes, usability enhances user experience, skills, and attitudes in using a security or privacy mechanism, thus, achieving the various usable security goals. In other cases (for instance in games), increasing user experience will require degrading usability (to increase challenge and thus users' reward

when reaching the goal). Identifying design solutions that align multiple properties remains a great challenges in the field of HCI [82].

4.3.1 Error Reporting

For critical systems like online banking and supply chain security assurance, which are two demonstrator use cases in the CyberSec4Europe project (see D5.1 for details), the usability of errors and security breaches reporting mechanism must consider: 1) completeness of the errors or security breaches reported to end-users, and 2) how easily the end-users can interpret the errors or security breaches presented to them by the system.

Reeder et al. [83] performed a study of web browser security warning behavior using the Experience Sampling Method (ESM) that includes a survey of over 6000 Chrome and Firefox users in situ to gather reasons for adhering or not to real warnings. They concluded that warning designers to address all the specialized issues by examining contextual factors and a wider variety of users' concerns, rather than through one-size-fits-all improvements, to improve warning adherence and user comprehension. Good et al. [84] tested short summary notices in contrast to long, legalistic license agreements. Moreover, suggested reducing information overloading that significantly improves the usability of error reporting.

One example of error reporting are HTTPS certificate error warnings that protect users against network attacks by alertly them promptly [85]. However, spurious HTTPS warnings could be problematic resulting in poor user experience, hinder the adoption of HTTPS, and people get habituated to ignore messages. Authors suggested many of these problems could be mitigated by building more actionable warnings in the browser or investing in other client-side engineering solutions.

Felt et al. [86] mitigated HTTPS authentication warnings avoidance by lower click-through rate (CTR) because (a) they consider it is safer to err on the side of caution, and (b) they believed that low CTRs will encourage developers to adopt valid SSL certificates.

4.3.2 Verifiable Credentials

Verifiable credentials are also a part of several use cases in the CyberSec4Europe project, e.g., Privacy-preserving identity management and banking use cases. Studies have shown that conventional authentication schemes, i.e., knowledge-based schemes or token-based schemes, possess many security and usability issues [87]. From the security perspective, knowledge-based authentication schemes are vulnerable to common attacks such as guessing-, shoulder-surfing-, or dictionary-based attacks[9] [88], [89]. Similarly, token-based authentication schemes are vulnerable to common attacks such as side-channel, denial-of-service, real-time phishing or coercion attacks [90]–[92]. From the usability perspective, users face difficulty to manage numerous PINs/passwords, and complex passwords add cognitive load on users [93]–[95]. In the case of smart-tokens, they can be easily shared or misplaced [87]. Lastly, it is worth mentioning that these schemes do not necessarily authenticate the users but authorize anyone who enters the correct PIN/password, OTP or smart token number.

[9] see for example https://capec.mitre.org for more details on the attack types

Biometrics including both physiological and behavioral could be utilized for designing next-generation user authentication solutions for critical systems. Biometric traits such as a face, fingerprint, voice, handwritten signature, keystroke/touch dynamics, and hand-movements can be easily acquired owing to the availability of cost-effective sensors.

Wang et al. [96] proposed a privacy-preserving edge computing-based face verification system for user authentication. They employed secure nearest neighbor scheme and secret sharing is used for protecting the privacy of face information. For smart devices and smart homes, voice assistants become an easy interface to interact with applications or connected appliances. Chang [97] presented a two-layer authentication method to protect voice assistants and maintain their usability. They employed user voiceprint and challenge-response protocol to authenticate a legitimate user and granting access to the ecosystem. At the same time, resist replay attacks by asking the user to respond to the pre-configured challenge within 5 seconds.

Proteus, proposed by Gofman et al. [98], is a bi-modal biometric verification system based on face and voice features, for smart devices that can be useful for securing access in critical systems. This scheme extracts principle components using Principal Component Analysis (PCA) and Mel Frequency Cepstral Coefficients (MFCC) from face and voice modality, respectively, to construct a bi-model system. Gupta et al. [99] proposed a multimodal biometric-based authentication scheme, DriverAuth, that exploits face, text-independent voice, and swipe to ensure the safety and security concerns of the customers using on-demand rides and ride-sharing transportation.

Tolosana et al. [100] proposed a signature verification architecture based on the number of lognormal from the Sigma LogNormal writing generation model that is adapted to the signature complexity for security purposes. Additionally, they performed an exhaustive comparative analysis of both stylus and touch scenarios for smartphones and tablets.

Buriro et al. [101] proposed a bimodal authentication scheme that exploits users' touch-typing and hand-movements transparently, while the users access their sensitive applications by inserting an 8-digit PIN/password. Similarly, DialerAuth authenticated users based on touch-stroke timing-differences and hand micro-movements for 10-digit PIN/password [102]. These solutions can be seamlessly integrated into existing sensitive applications that incorporated pin or password to authenticate their users. Unarguably, both solutions offer flexibility to users to enter random alphanumeric digit and authenticate them based on their touch-typing and hand-movements, thus, enhancing the overall usability of the system.

4.3.3 Users' Data Privacy

Also data privacy is part of many use cases of our project. Users' data (e.g., personal information, health data, biometrics, etc.) leakage in digital systems is a widely known issue fostering a strong need for privacy preservation. A study revealed that many medical, health, and fitness applications collect high-risk data (including financial information, full name, health information, geo-location, date of birth and zip code). 50% of these applications sent personally identifiable information (PII) over the internet without any encryption, whereas 83% of these applications store data locally on the device without encryption [103].

According to Rui and Yan [104] privacy protection methods can be evaluated by determining the Mission Success Rate (MSR). Further, privacy disclosure in network transmission can be solved by enhancing the

non-invertibility, revocability, and unlinkability of data. Sui et al. [105] proposed a secure-fusion based biometric authentication method that involves key extraction for mixing the user's biometrics and a reference subject's biometrics to be fed into an existing biometric system to generate a BioCapsule for authentication.

4.4 Privacy in communications

The privacy of communications is not only important for protecting the content of the communications but also for protecting the metadata (the who, when and where) of the communications. This cannot be solved by only encrypting the content with E2EE (see section 3.4).

The Onion router (TOR) is one example how this problem of metadata has been tackled at the network. The usability of TOR is fairly good, but there are many complexities and methods that can undermine the privacy protections it provides e.g. browser fingerprinting methods in browsers [106].

The metadata of our communications is collected many times by the platforms user employ in their communications (e.g. Facebook). This social graph and its properties can be used to make very accurate inferences about the users attributes and habits. In communications there exist solutions that do not gather metadata. One example of this is Signal, which does not store excessive metadata of user communications. One example of tracking different messaging solutions and their properties is the (unfortunately now out of date) EFF privacy scorecard[10]. For current advice reader could visit the Surveillance Self-Defence website[11]

[10] https://www.eff.org/pages/secure-messaging-scorecard
[11] https://ssd.eff.org

5 Tradeoffs, compromises and recommendations

Better usability should go hand in hand with better security and privacy, but sometimes there are tradeoffs and the need to compromise between the three of them. In this section, we present some of the existing tradeoffs and compromises that have been made. This can then be seen also as possible research directions for future work.

5.1 Security

From user authentication perspective some tradeoffs can be seen from [4], [5]. It is clear that not one method can offer all the possible usability and security (or privacy, for that matter) benefits. What is still unclear is which combinations can achieve this. It is also evident that many end users are willing to choose better usability and user experience even if other options offer better security (or privacy) in many cases.

5.2 Privacy

One tradeoff between usability and privacy can be seen with the TOR system. The usability of TOR is fairly good and after installation the browsing experience is quite straightforward. The privacy of the user is protected by the TOR network in many cases. Although the use of TOR improves the privacy of the user, it is sometimes not possible to use it to browse all the websites that the user wants. Furthermore, the use of TOR can be seen as suspicious activity and in some cases access to TOR has been restricted by governments [107].

Another example trade-off in privacy is the “informed consent” that is used in several contexts e.g. the cookie policies enforced by many websites. Although this gives user some control over the use of their information, the default option is usually to allow the use of all possible cookies and functionalities. The process of disabling these is many times fairly cumbersome and sometimes has to be enforced by the user every time they visit a specific website. Thus there is a usability trade-off to this privacy feature.

5.3 Recommendations

To reach more usable security and privacy enhancing systems, we have provided a short list of recommendations. Some of these are general and some are directed towards specific use cases such as user authentication.

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

   The use of authenticated encryption protects both the integrity of the communications as well as the privacy of the content. There are many available tools to achieve this and these can be applied in a vast majority of use cases, where communication over network is done. The impact to the end-users is minimal, when this is done right and when user needs, user knowledge and user work is carefully identified at design time.

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

User Centered Design (UCD) approaches [108] advocate the involvement of the end users in the early stages of the development process (e.g. via brainstorming sessions and work analysis). Beyond, UCD promotes multiple iterations at design time to gather user feedback on concrete artifacts such as mockups and paper prototypes [109]. User interfaces and user interactions that are the front end of security and privacy mechanisms should follow UCD processes to ensure that usability is considered from the very beginning and not too little too late, as this was the case for software applications in the past [110].

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

As mentioned in the earlier chapters, collecting the information on users is not a straightforward task and both automated and other approaches have their shortcomings. However, it is not possible to improve the usability of new privacy and security technologies, if no effort to that end is made. Thus, there should be some way to test and/or model the users in the security and privacy systems. User research methods should thus be used throughout the design, development and assessment of security mechanisms.

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

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

6 Future directions and open questions

There are many open questions that need to be solved in the fields of usability, usable security and usable privacy. It is worth noting that the survey conducted by ENISA (European Union Agency for Cybersecurity) found user-centric security practices and tools as one of the key topics in the future development of cybersecurity.[111]

One key aspect is to make these topics more visible to the developers of new systems. When new methods to improve security and privacy are developed, these should be accessible to developers. This way they can be incorporated into the new technologies that will establish our digital society in the coming decades. Similarly, developers of security mechanisms should be aware of methods, techniques and tools to support design and development of usable designs.

From user authentication perspective finding a method that adheres to all the usability, security, privacy, scalability and economic requirements is still a very much open research question. In communications, protecting the content of the data transmitted over networks seems to be well on its way to becoming the norm. There, the open question is how to protect also the privacy of the communications when metadata is considered. In digital identity, the way to provide anonymous, pseudonymous, and more user-centric identity is currently a very interesting area of research, with new proposals coming frequently. This is also a problem that needs to be solved in order to reach a better digital society for us all.

As mentioned earlier, usability, security and privacy are likely to bring conflicting aspects to the design. This aspect is not new as similar concerns are well known for the usability of dependability mechanisms [112]. Holistic methods should thus ensure that usability, security and privacy objectives are met by the design and researcher must identify means to make explicit the conflicts and to rationalise their design decisions following design rationale approaches as in [113].

7 Conclusion

Providing recommendations on usability in fields such as security and privacy is a difficult task. Much of the relevance of the recommendations is based on the context where the user is and the different risks the user might encounter in her current task. Thus there are only four recommendations that we can give based on the current research and the different use cases demonstrated in the CyberSec4Europe project. These are Use of authenticated encryption in the application layer or network layer communications whenever possible; Early user involvement should be ensured for new security and privacy features; User modeling and/or user tests should be conducted for new security and privacy features; Provide the users with authentication methods that are both secure and privacy-friendly.

Although there is a great deal of research on the subject of usability and also related to usability of security and privacy, there are still many open questions. In addition, all three concepts, usability, security and privacy are constantly evolving. This means that the ways in which users interact with systems and their expectations of security and privacy are not constant and solutions that work today may be obsolete in a short while.

In conclusion, we can state that usability should not be taken lightly in the development of security and privacy technologies. It should be integral to the design and evaluation of different new methods and it should be present in the roadmaps for future cybersecurity technologies.

8 References

[1] A. Whitten and J. D. Tygar, "Why Johnny Can' t Encrypt : A Usability Evaluation of PGP 5 . 0," in *Proceedings of the 8th USENIX Security Symposium*, 1999, pp. 169–184.

[2] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland, "Why Johnny Still Can ' t Encrypt : Evaluating the Usability of Email Encryption Software," pp. 3–4.

[3] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons, "Why Johnny Still , Still Can ' t Encrypt : Evaluating the Usability of a Modern PGP Client."

[4] K. Halunen, J. Häikiö, and V. Vallivaara, "Evaluation of user authentication methods in the gadget-free world," *Pervasive Mob. Comput.*, vol. 40, 2017.

[5] 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 *Security and Privacy (SP), 2012 IEEE Symposium on*, 2012, pp. 553–567.

[6] B. Merdenyan and H. Petrie, "Perceptions of Risk, Benefits and Likelihood of Undertaking Password Management Behaviours: Four Components," in *IFIP Conference on Human-Computer Interaction*, 2019, pp. 549–563.

[7] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. dependable Secur. Comput.*, vol. 1, no. 1, pp. 11–33, 2004.

[8] S. D. Warren and L. D. Brandeis, "The Right to Privacy Harward Law Review," in *Ethical issues in the use of computers*, vol. 4, no. 5, Wadsworth Publ. Co, 1890, pp. 172–183.

[9] A. F. Westin, "Privacy and freedom Atheneum," *New York*, vol. 7, pp. 431–453, 1967.

[10] I. Goldberg, D. Wagner, and E. Brewer, "Privacy-enhancing technologies for the Internet," in *Proceedings IEEE COMPCON 97. Digest of Papers*, 1997, pp. 103–109.

[11] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European data protection: coming of age*, Springer, 2013, pp. 3–32.

[12] J. Coutaz, F. Bérard, E. Carraux, W. Astier, and J. L. Crowley, "CoMedi: using computer vision to support awareness and privacy in mediaspaces," in *Conference on Human Factors in Computing Systems: CHI'99 extended abstracts on Human factors in computing systems*, 1999, vol. 15, no. 20, pp. 13–14.

[13] I. O. for Standardization, *ISO 9241-11: Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs): Part 11: Guidance on Usability*. 1998.

[14] S. G. Hart and L. E. Staveland, "Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research," in *Advances in psychology*, vol. 52, Elsevier, 1988, pp. 139–183.

[15] D. Hix and H. R. Hartson, "Formative evaluation: Ensuring usability in user interfaces," 1992.

[16] A. Lecerof and F. Paternò, "Automatic support for usability evaluation," *IEEE Trans. Softw. Eng.*, vol. 24, no. 10, pp. 863–888, 1998.

[17] J. Brooke and others, "SUS-A quick and dirty usability scale," *Usability Eval. Ind.*, vol. 189, no. 194, pp. 4–7, 1996.

[18] E. Mordini and H. Ashton, "The transparent body: Medical information, physical privacy and respect for body integrity," in *Second generation biometrics: the ethical, legal and social context*, Springer, 2012, pp. 257–283.

[19] R. Matovu and A. Serwadda, "Your substance abuse disorder is an open secret! Gleaning sensitive personal information from templates in an EEG-based authentication system," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2016, pp. 1–7.

[20] American Academy of Ophthalmology, "Evidence Mounts That an Eye Scan May Detect Early Alzheimer's Disease," 2018. [Online]. Available: https://www.aao.org/newsroom/news-releases/detail/evidence-eye-scan-may-detect-early-alzheimers. [Accessed: 31-Oct-2019].

[21] A. Dantcheva, P. Elia, and A. Ross, "What else does your biometric data reveal? A survey on soft biometrics," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 3, pp. 441–467, 2015.

[22] I. Goodfellow *et al.*, "Generative adversarial nets," in *Advances in neural information processing systems*, 2014, pp. 2672–2680.

[23] C. Huang, P. Kairouz, X. Chen, L. Sankar, and R. Rajagopal, "Context-aware generative adversarial privacy," *Entropy*, vol. 19, no. 12, p. 656, 2017.

[24] A. Morales, J. Fierrez, and R. Vera-Rodriguez, "SensitiveNets: Learning Agnostic Representations with Application to Face Recognition," *arXiv Prepr. arXiv1902.00334*, 2019.

[25] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 815–823.

[26] M. Malekzadeh, R. G. Clegg, A. Cavallaro, and H. Haddadi, "Mobile sensor data anonymization," *IoTDI 2019 - Proc. 2019 Internet Things Des. Implement.*, pp. 49–58, 2019.

[27] S. A. Osia *et al.*, "A hybrid deep learning architecture for privacy-preserving mobile analytics," *arXiv Prepr. arXiv1703.02952*, 2017.

[28] R. Peeters, J. Hermans, P. Maene, K. Grenman, K. Halunen, and J. Häikiö, "N-Auth: Mobile authentication done right," in *ACM International Conference Proceeding Series*, 2017, vol. Part F1325.

[29] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *10th Symposium On Usable Privacy and Security (${$SOUPS$}$ 2014)*, 2014, pp. 213–230.

[30] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q.*, pp. 319–340, 1989.

[31] R. Böhme, "Security metrics and security investment models," in *International Workshop on Security*, 2010, pp. 10–24.

[32] S. Pfleeger and R. Cunningham, "Why measuring security is hard," *IEEE Secur. Priv.*, vol. 8, no. 4, pp. 46–54, 2010.

[33] M. Rudolph and R. Schwarz, "Security Indicators - A State of the Art Survey Public Report," *FhG IESE*, vol. VII, no. 043, 2012.

[34] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Privacy Enhancing Technologies*, 2002, pp. 41–53.

[35] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Privacy Enhancing Technologies*, 2002, pp. 54–68.

[36] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," 1998.

[37] L. Sweeney, "k-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowledge-Based Syst.*, vol. 10, no. 05, pp. 557–570, 2002.

[38] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of cryptography conference*, 2006, pp. 265–284.

[39] C. Dwork, A. Roth, and others, "The algorithmic foundations of differential privacy," *Found. Trends® in Theor. Comput. Sci.*, vol. 9, no. 3--4, pp. 211–407, 2014.

[40] K. Halunen and A. Karinsalo, "Measuring the value of privacy and the efficacy of PETs," *Proc. 11th Eur. Conf. Softw. Archit. Companion Proc. - ECSA '17*, pp. 132–135, 2017.

[41] X. Cai and Y. Gu, "Measuring anonymity," in *International Conference on Information Security Practice and Experience*, 2009, pp. 183–194.

[42] W. B. Tesfay, J. Serna, and S. Pape, "Challenges in Detecting Privacy Revealing Information in Unstructured Text.," in *PrivOn@ ISWC*, 2016.

[43] S. Pape, J. Serna-Olvera, and W. B. Tesfay, "Why open data may threaten your privacy," in *Workshop on Privacy and Inference*, 2015.

[44] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets [Netflix]," in *IEEE Symposium on Research in Security and Privacy, Oakland, CA*, 2008.

[45] E. Palmer, "Oops, it didn't arm-a case study of two automation surprises," in *Proceedings of the Eighth International Symposium on Aviation Psychology*, 1995, pp. 227–232.

[46] A. Sebok and C. D. Wickens, "Implementing lumberjacks and black swans into model-based tools to support human--automation interaction," *Hum. Factors*, vol. 59, no. 2, pp. 189–203, 2017.

[47] P. Palanque, "Engineering Automations: From a Human Factor Perspective to Design, Implementation and Validation Challenges," in *Proceedings of the ACM SIGCHI Symposium on Engineering Interactive Computing Systems*, 2018, p. 2.

[48] R. Bernhaupt, M. Cronel, F. Manciet, C. Martinie, and P. Palanque, "Transparent automation for assessing and designing better interactions between operators and partly-autonomous interactive systems," in *Proceedings of the 5th International Conference on Application and Theory of Automation in Command and Control Systems*, 2015, pp. 129–139.

[49] L. J. Skitka, K. L. Mosier, and M. Burdick, "Does automation bias decision-making?," *Int. J. Hum. Comput. Stud.*, vol. 51, no. 5, pp. 991–1006, 1999.

[50] P. Murmann, D. Reinhardt, and S. Fischer-Hübner, "To Be , or Not to Be Notified Eliciting Privacy Notification Preferences for Online mHealth Services," in *34th IFIP TC 11 International Conference, SEC 2019*, 2019.

[51] M. Naor and A. Shamir, "Visual Cryptography," *Adv. Cryptogr.*, pp. 1–12, 1995.

[52] O.-M. Latvala, C. Peng, P. Honkamaa, and K. Halunen, "" Speak , friend , and enter " - Secure , Spoken One-Time Password Authentication," in *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018, pp. 1–5.

[53] K. Halunen *et al.*, "Human Verifiable Computing in Augmented and Virtual Realities," 2017.

[54] A. G. Forte, J. A. Garay, T. Jim, and Y. Vahlis, "EyeDecrypt - Private Interactions in Plain Sight.," *IACR Cryptol. ePrint Arch.*, vol. 2013, p. 590, 2013.

[55] P. Lantz, B. Johansson, M. Hell, and B. Smeets, "Visual Cryptography and Obfuscation: A Use-Case for Decrypting and Deobfuscating Information Using Augmented Reality," in *Financial Cryptography and Data Security*, Springer, 2015, pp. 261–273.

[56] S. Pape, *Authentication in insecure environments: using visual cryptography and non-transferable credentials in practise*. Springer, 2014.

[57] 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.

[58] M. Cheminod, L. Durante, L. Seno, and A. Valenzano, "Semiautomated verification of access control implementation in industrial networked systems," *IEEE Trans. Ind. Informatics*, vol. 11, no. 6, pp. 1388–1399, 2015.

[59] M. Cheminod, L. Durante, L. Seno, and A. Valenzano, "Analysis of access control policies in networked embedded systems: A case study," *2015 10th IEEE Int. Symp. Ind. Embed. Syst. SIES 2015 - Proc.*, pp. 69–78, 2015.

[60] 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.

[61] I. Deutschmann, P. Nordstrom, and L. Nilsson, "Continuous authentication using behavioral biometrics," *IT Prof.*, vol. 15, no. 4, pp. 12–15, 2013.

[62] F. Bergadano, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 367–397, 2002.

[63] A. A. E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," *IEEE Trans. dependable Secur. Comput.*, vol. 4, no. 3, pp. 165–179, 2007.

[64] H. Feng, K. Fawaz, and K. G. Shin, "Continuous authentication for voice assistants," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, 2017, pp. 343–355.

[65] C. Wan, L. Wang, and V. V Phoha, "A survey on gait recognition," *ACM Comput. Surv.*, vol. 51, no. 5, p. 89, 2018.

[66] M. De Marsico and A. Mecca, "A Survey on Gait Recognition via Wearable Sensors," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–39, 2019.

[67] D. Gafurov, "A survey of biometric gait recognition: Approaches, security and challenges," in *Annual Norwegian computer science conference*, 2007, pp. 19–21.

[68] T. Hamme, D. Preuveneers, and W. Joosen, "Improving Resilience of Behaviometric Based Continuous Authentication with Multiple Accelerometers," 2017.

[69] G. Garofalo, E. Argones Rúa, D. Preuveneers, W. Joosen, and others, "A Systematic Comparison of Age and Gender Prediction on IMU Sensor-Based Gait Traces," *Sensors*, vol. 19, no. 13, p. 2945, 2019.

[70] N. Unger *et al.*, "SoK: Secure Messaging," *2015 IEEE Symp. Secur. Priv.*, pp. 232–249, 2015.

[71] H. Abelson *et al.*, "Keys under doormats," *Commun. ACM*, vol. 58, no. 10, pp. 24–26, 2015.

[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 *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2008, pp. 1065–1074.

[73] G. D. P. E. U. Regulation, "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," *Off. J. Eur. Union*, vol. 59, pp. 1–88, 2016.

[74] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 2001, pp. 93–118.

[75] 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.

[76] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *Sovrin Found.*, vol. 29, 2016.

[77] J. B. Bernabe, M. David, R. T. Moreno, J. P. Cordero, S. Bahloul, and A. Skarmeta, "Aries: Evaluation of a reliable and privacy-preserving European identity management framework," *Futur. Gener. Comput. Syst.*, vol. 102, pp. 409–425, 2020.

[78] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for Blockchain: review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[79] J. B. Bernabe and A. Skarmeta, "Challenges in Cybersecurity and Privacy - the European Research Landscape," River Publishers, 2019, pp. 1–372.

[80] D. Reed, M. Sprony, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized Identifiers (DIDs) v0. 11 Data Model and Syntaxes for Decentralized Identifiers (DIDs). W3C." 2018.

[81] M. Sporny and D. Longley, "Verifiable claims data model and representations." Technical report, W3C, 2017.

[82] C. Fayollas, C. Martinie, P. Palanque, Y. Ait-Ameur, and others, "QBP notation for explicit

representation of properties, their refinement and their potential conflicts: application to interactive systems," in *IFIP Conference on Human-Computer Interaction*, 2017, pp. 91–105.

[83] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman, "An experience sampling study of user reactions to browser warnings in the field," in *Proceedings of the 2018 CHI conference on human factors in computing systems*, 2018, p. 512.

[84] N. S. Good, J. Grossklags, D. K. Mulligan, and J. A. Konstan, "Noticing notice: a large-scale experiment on the timing of software license agreements," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2007, pp. 607–616.

[85] M. E. Acer *et al.*, "Where the wild warnings are: Root causes of Chrome HTTPS certificate errors," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1407–1420.

[86] A. P. Felt, R. W. Reeder, H. Almuhimedi, and S. Consolvo, "Experimenting at scale with google chrome's SSL warning," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2014, pp. 2667–2670.

[87] S. Gupta, A. Buriro, and B. Crispo, "Demystifying authentication concepts in smartphones: Ways and types to secure access," *Mob. Inf. Syst.*, vol. 2018, 2018.

[88] C. Katsini, M. Belk, C. Fidas, N. Avouris, and G. Samaras, "Security and usability in knowledge-based user authentication: A review," in *Proceedings of the 20th Pan-Hellenic Conference on Informatics*, 2016, p. 63.

[89] G. Ye *et al.*, "Cracking Android pattern lock in five attempts," 2017.

[90] H. Choi, H. Kwon, and J. Hur, "A secure OTP algorithm using a smartphone application," in *2015 Seventh International Conference on Ubiquitous and Future Networks*, 2015, pp. 476–481.

[91] H. Sun, K. Sun, Y. Wang, and J. Jing, "TrustOTP: Transforming smartphones into secure one-time password tokens," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 976–988.

[92] B. Cha, N. Kim, and J. Kim, "Prototype analysis of OTP key-generation based on mobile device using voice characteristics," in *2011 International Conference on Information Science and Applications*, 2011, pp. 1–5.

[93] T. Bhattasali, K. Saeed, N. Chaki, and R. Chaki, "A survey of security and privacy issues for biometrics based remote authentication in cloud," in *IFIP International Conference on Computer Information Systems and Industrial Management*, 2015, pp. 112–121.

[94] L. Zhang-Kennedy, S. Chiasson, and P. van Oorschot, "Revisiting password rules: facilitating human management of passwords," in *2016 APWG symposium on electronic crime research (eCrime)*, 2016, pp. 1–10.

[95] S. Komanduri *et al.*, "Of passwords and people: measuring the effect of password-composition policies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011, pp. 2595–2604.

[96] X. Wang, H. Xue, X. Liu, and Q. Pei, "A Privacy-Preserving Edge Computation-Based Face Verification System for User Authentication," *IEEE Access*, vol. 7, pp. 14186–14197, 2019.

[97] Y.-T. Chang, "A Two-layer Authentication Using Voiceprint for Voice Assistants," 2018.

[98] M. I. Gofman, S. Mitra, T.-H. K. Cheng, and N. T. Smith, "Multimodal biometrics for enhanced mobile device security," *Commun. ACM*, vol. 59, no. 4, pp. 58–65, 2016.

[99] 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.

[100] R. Tolosana, R. Vera-Rodriguez, R. Guest, J. Fierrez, and J. Ortega-Garcia, "Exploiting Complexity in Pen-and Touch-based Signature Biometrics," *arXiv Prepr. arXiv1905.03676*, 2019.

[101] A. Buriro, S. Gupta, and B. Crispo, "Evaluation of motion-based touch-typing biometrics for online banking," in *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2017, pp. 1–5.

[102] A. Buriro, B. Crispo, S. Gupta, and F. Del Frari, "Dialerauth: A motion-assisted touch-based smartphone user authentication scheme," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, 2018, pp. 267–276.

[103] L. Ackerman, "Mobile health and fitness applications and information privacy," *Priv. Rights Clear. San Diego, CA*, 2013.

[104] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2018.

[105] Y. Sui, X. Zou, E. Y. Du, and F. Li, "Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method," *IEEE Trans. Comput.*, vol. 63, no. 4, pp. 902–916, 2013.

[106] G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz, "The web never forgets: Persistent tracking mechanisms in the wild," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 674–689.

[107] 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. to appear, 2020.

[108] D. A. Norman, "Cognitive engineering," *User centered Syst. Des.*, vol. 31, p. 61, 1986.

[109] M. Rettig, "Prototyping for tiny fingers," *Commun. ACM*, vol. 37, no. 4, pp. 21–27, 1994.

[110] K. Y. Lim and J. B. Long, "A method for (recruiting) methods: facilitating human factors input to system design," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1992, pp. 549–556.

[111] ENISA, "DIGITAL SOVEREIGNTY - Cybersecurity research directions for Digital Sovereignty in Europe," 2019.

[112] C. Fayollas, C. Martinie, P. Palanque, Y. Deleris, J.-C. Fabre, and D. Navarre, "An approach for assessing the impact of dependability on usability: application to interactive cockpits," in *2014 Tenth European Dependable Computing Conference*, 2014, pp. 198–209.

[113] X. Lacaze and P. Palanque, "DREAM & TEAM: a tool and a notation supporting exploration of

options and traceability of choices for safety critical interactive systems," in *IFIP Conference on Human-Computer Interaction*, 2007, pp. 525–540.

[114] M. M. Pirker and R. Bernhaupt, "Measuring user experience in the living room: results from an ethnographically oriented field study indicating major evaluation factors," in *Proceedings of the 9th European Conference on Interactive TV and Video*, 2011, pp. 79–82.