BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2021
http://excel.fit.vutbr.cz

Usability of Usable Security Guidelines from IT Professional Point of View

Katarína Galanská

Abstract

Balancing the security and usability has always been a challenge. Despite the importance of secure software, the security guidelines and standards are often too complicated, prone to error or time consuming. This non-equilibrium initiated the creation of the term usable security. For years it has been a common research problem. While the software should be developed with usability considerations of end users, security standards and guidelines used by IT professionals are not often given enough attention from the usability perspective. As the experts in the IT field are expected to have a higher level of knowledge, they often face very complex areas when trying to be compliant to particular security standard or follow specific guideline. This work presents the survey in the field of usable security, the aim of which was to evaluate the current awareness of the usable security across the people working in the software development. It discusses problems associated with the balance of the security and usability and devotes to design and implement an educational tool helping the newcomers in the IT field with making systems secure and usable. The aim is to introduce better understanding in certain areas of usable security, namely authentication, privacy, encryption and digital certificates.

Keywords: usable security, usability evaluation, authentication, encryption, digital certificates, privacy

Supplementary Material: Results of the Study

*xgalan02@stud.fit.vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

As the world is getting more connected, the need for secure and usable systems is increasing. Software vulnerabilities create huge risks of cyber crimes. Therefore, many organisations and institutes fight against malicious intent by creating security solutions, standards and guidelines which, if followed, provide the appropriate security level. Their importance is evident, however, more complex security solution does not necessarily lower the likelihood of the future attack. The centre of attention has been given to the security establishment and the most vulnerable part of the security supply chain, which is the human element, has not been given enough attention. The vulnerable factor can be the software architect creating a design, the developer implementing the system or end users performing security procedures not in appropriate way.

There are more and more security incidents due to insufficient usability of the software. Too complex decisions are often left in the hands of the end user. This issue has been the reason for creation of usable security field. Numerous recent incidents however showed that the cause can not only be end user but also software developers. Following different security standards or guidelines during the process of software development is more than crucial. The lack of usability can make even solid and robust standards prone to human error. Especially inexperienced programmers could benefit from direct help by using guidelines providing the basic advises for common problems.

When following a security guideline or complying to the specific security standard, there are factors that need to be considered. One of the most important ones are the amount of complexity, time consumption,

IT professional's knowledge or human convenience. In many cases, IT professionals must be more concentrated, accurate and have a perfect memory when completing their tasks. This highlights the need for not only secure guidelines and standards but also usable ones. The advancement of the security should come in hand with the increased usability [1]. The term usable security has been defined as security where the users are well aware of what security tasks they have and how to perform them. Nowadays, this definition can be extended to the IT professionals having awareness about appropriate security development. For example a programmer building an authentication for a system should not only satisfy the security requirements of the system. The developer should also think about the quality of a user's experience when interacting with the system.

While there are many security standards for secure development, the usability factor is not included in them and is considered as a secondary concern [2]. No existing standards provided by an institute for standardization process for usable security has been found. There are several security standards focusing on securing the software. The most of the guides for secure development focuses on the security perspective and the usability is still not fully incorporated [3]. The attempt of defining the guidelines for usable and secure development proposed a set of design guidelines for security management interfaces [4]. The paper focuses mainly on designing user interfaces for end users. This research's goal is to meet the challenges of providing the administrators of current interfaces enough detail without overwhelming them with too much information. The outlined principles define what should be done during the design phase of the interface by the IT professionals. However the guidelines do not exactly define how can they be addressed.

As the term usable security does not have such a long history, there are still multiple challenges to face. From the IT professionals perspective, the amount of research is insufficient. Many research papers are devoted to studying the usability of security solutions from users point of view. However, developers and IT professionals are usually not provided with standards or guidelines to help them reach the adequate level of security and usability. Several guidelines proposed only in a form of research papers carry multiple problems. They are often very general or not applicable. Some of them are not really evaluated or hard to use alongside with other security standards. As an implication from the insufficient research within this field, this work aims to speed up the process of gaining awareness of the usable security solutions by creating an educational aid.

Research in the area of usable security is lacking the IT professional's perspective. Improving the quality of usable security guidelines for architects, developers, testers and other people working in the development can result in an overall improvement of security. Many research papers showed that the developers are often a reason why the system has specific vulnerability. Not having enough information a adequate awareness can lead to poor security level of the system. Increasing the usability of the guidelines of IT professionals may result in increased usability of the end user and can mitigate a risk of unknowingly creating a vulnerability.

This paper introduces better understanding in specific areas of usable security, namely authentication, encryption, privacy and digital certificates. It discusses the problems associated with the balance of security and usability. The paper carries out an survey based on theoretical research of the existing standards, guidelines and different material related to the term usable security. The results outlines the levels of IT professionals knowledge and awareness in this area. The evaluation reveals the methods IT experts use and the usability problems they face during developing security solutions. The obtained survey evaluation results are indicators of how usable current guidelines are, if there are any used, and to suggest possible modifications.

2. Methodology

The methodology for selecting which existing materials of usable security will be discussed followed the specific process. The research was oriented to the overall understanding of the field and defined challenges within the usable security. The process of specifying which articles will be examined was as follows. The first priority was searching for the keywords "usable security", "usability and security", "usable and secure" or "usability" and "security". The second priority has been the publish date. The articles published after the year 2017 were prioritized. The theoretical research provided the basis for the user study. The evaluation of the study of current awareness of IT professionals was based on the predefined hypothesis. The participants' answers were used to confirm or refute the defined statements.

3. Defining the Term Usable Security

The term of usable security has been a target of discussion in many research papers [5, 6, 7]. While this

term had no formal definition, it can be described as a field focusing on both security and usability. Based on the basic principles of these two areas the goal of usable security is to satisfy the security goals with the effectiveness and efficiency. If the usable security is in place, the user should have minimal inconvenience with the system. It should be hard for the end user to create a security incident by using the target system. A different study describes the usable security as the situation when the end people using particular software are aware of the security tasks and how to perform them [8]. The paper Usable Security Versus Secure Usability considers the aspects of security and usability and their competing characteristics [9]. It takes into account the ten characteristics defined in ISO/IEC 25010 and analyse their mutual influence [10]. The paper analyses the security and usability from two perspectives. The first one, *usable security* is within the paper defined as the method of how to develop functions secure access to the resources. An example is the CAPTCHA, that can not be properly discerned by the user, having an impact on the user, who then does not necessarily finish the procedure. The article highlights the need of taking this into account when developing the system. On the other hand *secure usability* has defined relationships with user interfaces with necessary level of security. An example for this approach would be a simpler Turing test, where the user has to only click on the check which is more usable for the users. However, there is higher likelihood that the security system will be passed by the software bot. This example represents an situation, where the usability came at the expense of security.

While the security area pursues the goal of ensuring the confidentiality, integrity non-repudiation, accountability and authenticity of information [10]. The usability area is officially defined by the ISO 9241-11 as in following definition [11].

> ”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.”

According to the ISO/IEC 25 010 security and usability can be represented as a set of characteristics1.

4. Existing Guidelines and Standards

While there are many security standards for secure development, the usability factor being considered as a secondary concern [2]. During the research no existing standards provided by an institute for standardization process for usable security has been found. There are several security standards focusing on securing the software.

Term	Characteristics
Security	confidentiality, integrity, non-repudiation, accountability, authenticity
Usability	appropriateness, recognizability, learnability, operability, user error protection, user interface aesthetics, accessibility accessibility

Table 1. Representation of Security and Usability According to ISO/IEC 25 010

National Institute of Standards and Technology (NIST) conducted a research on usable cybersecurity [12]. Their goal is provide guidance for the professionals creating policies, system engineers and security professionals. The guidelines should help to incorporate usability into the security decisions, processes and products. Their focus is given to specific areas as authentication, encryption, cybersecurity adoption and awareness, Internet of Things, phishing, privacy and user perceptions and behaviours. Their website serves as a signpost to accessing different research papers in these areas.

Various models for measuring the software usability has been summarized in the research paper Usability Meanings and Interpretations in ISO Standards [13]. The focus of the research has been given to standards ISO 9126 and ISO 9241. According to the study, experts and researchers have not yet agreed on the definition of the usability. An interesting outcome of the research is that while the professionals outside the standardization process can have a relevant understanding of usability measures, the standards may confuse them, what could lead to a failure of using these measures.

The problems that the field of cybersecurity usability is facing has already been reviewed [14]. The research outlined an general usability design guidelines. The paper proposed the list of guidelines that should be followed. However, the paper only proposed guidelines and did not evaluate their applicability to current security standards.

Hans-Joachim Hof presented guidelines to achieve the good security and usability in IT mechanisms [7]. The created set of nine design guidelines aims to help the developers with software development. The guidelines highlights following factors.

- Users should be able to use the system.
- Using the system with too many restrictions may

lead to the user trying to bypass the security mechanism.

- The security mechanism should not interfere with the user task at any time.
- The efficiency of the system usage is also very important.
- If the user has to remember too many password it is less usable. The users may prefer to use existing account to authenticate.
- The security measures should be preconfigured on the system and the user should not face the important security decisions.
- The user feels secured when the system does not ask too many security related questions.
- The state off the system's security should be always visible.
- The system should predict that the user make mistakes and in the case of the failure of the security mechanism the software should guide the user to successful reparation of the system.
- The security mechanism should be consistent.

The research done as a master thesis by Markus Lennartsson identified common factors affecting the usability of security solutions [5]. The result of the thesis is a hierarchical model of aspects of usable security and their impact. The simplicity and time provided for the security procedure, as aspects, showed a significant impact of security.

The need of finding the trade off between the usability and security has resulted in a lot of research [15]. While many papers proposed different guidelines helping to reduce the gaps between these two factors, there are not fully applicable. Usable security guidelines could be found mostly in the form of research papers and they were often too general for the purpose of being useful for newcomers in IT.

On one hand, there has been a good amount of research done on the topic of usable security [16], however the focus has mostly been given to the end users and not to make things easier to the developer or IT professional. Security solutions getting more complex are creating a gap for further research of this field from professionals perspective.

5. Authentication as a Challenge of Usable Security

The growing use of the Internet brought the need of authentication of the user connected with many security measures, security testing and secure coding [17]. During the design, implementation and testing of these measures, the focus has been given to satisfy the security requirements. However, the data breaches and other security incidents happen mainly because of the misuse of these systems and procedures. This introduces a big problem for developers to implement a usable and security authentication.

The challenge in this authentication method is to figure out the trade-off between the usability and the security element [15]. Despite different efforts of the professionals on replacing the text password, people are still used to perform authentication through login and password [6]. Almost every service uses this method. The security and usability of this typical method has a huge importance from the perspective of possible data breach [18].

In recent years multi-factor authentication is becoming the more and more popular [19]. As many organisations are working with sensitive and personal information, the need for secure and usable authentication grows. A group of researches have done an experiment with one hundred of users, where each user was obligated to use to researcher's online banking to create a payment [19]. The actions of the users have been recorded. The users were able to authentication using the secure device, card reader and using their fingerprints. Users faces various visible security design flaws and warning messages. Based on their actions, the researchers were able to determine that the authentication process is not sufficient to meet the needs of end users. The research is working in progress but it was already able to show the insufficiency of the system's usability.

Biometric authentication has a big advantage to the user [20]. The biometric information cannot be forgotten. Despite multiple advantages of this method of authentication, there can be usability and security issues. The conducted survey resulted in a valuable result for the field of usable security. One of the main usability problems was the slow response of the system. For example slow face detection when unlocking the smart phone. Another defined problem was the lack of convenience. The example of inconvenience could be aligning the device for successful recognition. The important fact is that the usability factor was one of the most important factors in users' decision making to use or not to use the system.

6. Encryption as a Challenge of Usable Security

One of the challenges within the field of usable security is the data encryption [2]. It is the most widely used method for authentication and access control. As nowadays personal and sensitive data are all the time being transferred though the internet, the organisations

need to comply to the security standards in order to secure their data. The requirements for data encryption are increasing and the algorithms for encryption are changing together with key lengths and key management. This can be affecting the usability of these techniques.

The paper evaluating the usability of PGP 5.0 defined the usability for security as four characteristics of the software [8]. The security software is usable if the users are aware of the tasks performed using the software and the information how to do so. The users need to feel comfortable working with the software and can not make any errors that could harm the system's security. The research focuses on the problematic properties of security as unmotivated users, who take security as the secondary goal. A part of these properties represents also the abstraction property, where the author highlights the fact that the security policies, usually included in computer security management, are by the developers taken for granted. These policies define the access to resources and should be considered during software development. Another problems mentioned in the paper are the lack of feedback or security awareness leading to high-cost mistakes. This study takes into account the fact that human participation in the security processes is considered as the weakest link property. The conclusion showed the failure of standard interface design. Two thirds of the people educated in the email sending were not able to send it correctly signed and encrypted. They showed the need of creation and educational software to educate users to be able to manage their security.

Recent research reviewed the users' attitudes toward disk and file encryption [21]. The result of the researchers' survey showed the IT professionals awareness of the encryption tools could be increased.

The analysis of email encryption from the usable security perspective identified a room for improvement [7]. The research paper on user-centric security discusses the usability factors in IT security. It claims that if the security features on the system fail, for example as email encryption, the error message should guide the user to import the certification with the steps of how to achieve it.

Hans Hof performed an analysis of the email encryption based on his own guidelines for usable security [7]. The process of encrypting of email communication is easy and there is not many complex tasks for users. However, before the email communication can be encrypted, the public keys has to be exchanged. The users usually do not get guidance for this process. The user often has to decide that certificates to trust.

7. Digital Certificates as a Challenge of Usable Security

When using web application, the system is using the SSL for traffic encryption. Using the certificates allows the users to send their data securely to the target server. In order to do that, the user needs to have installed certificate authority that can verify the websites' certificates. User can communicate only with the ones that are accepted by the authority.

In case that the unverified website wants to communicate with the user, the browser usually shows an error. This message can often be too complicated for the user to understand which can lead into the user adding the security exception.

Many vulnerabilities connected to SSL certificate are caused by developers [22]. The major cause lies in the API design and SSL libraries. Developers face low level security details and often do not use the libraries in correct way. The parameters may be misunderstood. The recent study revealed that 83% of vulnerabilities related to the SSL development are the result of the misuse of the cryptographic APIs [23]. Often even in case of fixing a bug the developers tend to create different vulnerability. The usage of these libraries is not usable. The security libraries should provide the IT professionals efficient way to use them ad try to avoid them accidentally creating vulnerabilities.

There are well known usability problem of SSL certificates as non adequate warning messages in browsers [24]. The studies introduced the challenge for creating a effective SSL warning messages which would mitigate many software vulnerabilities.

8. Privacy as a Challenge of Usable Security

Data is very important for the businesses proving services. That is why storing personal data by web merchants is now very common [6]. The EU General Data Protection Regulation (GDPR) defines many security requirements for storing confidential data [25]. As the organisations need to comply to the regulations, they need to provide a clear and concise privacy policy. This documents states how the users data are being collected, processed and handled. Moreover, the policy must include readable information whether the data are confidential or shared with third parties.

One of the challenges in the usable security field is related to privacy policies. The lack of usability in the documents is a known problem [26]. The unstructured text may lead to the misunderstanding of the user and the uselessness of the statement. The paper

”Privacy Policy – “I agree”?! – Do alternatives to text-based policies increase the awareness of the users?” demonstrated the influence of policy structure to the awareness of the users. The other alternatives to the text-based format showed a significant increase.

9. Study of the Current State of IT Professionals' Awareness of Usable Security

The theoretical research provided the basis for the study. The survey has been designed in order to evaluate the current awareness of the usable security across the people in IT industry. The focus has been given to the IT professionals current awareness, their knowledge about guidelines, principles, methods and best practises. The participants were asked to fill the survey are working in different part of the process of IT development. Their current awareness and experience could result in qualitative feedback in terms of security and usability. The feedback from participants will built the base for the educational aid helping newcomers starting with IT development.

The theoretical research outlined a specific hypothesis which will be evaluated based on the results of the survey. The hypothesis is meant to examine IT professionals' current awareness and is defined as follows.

- IT Professionals have heard the term usable security before. However, they are not well aware of the usable security standards and guidelines.

The scope of this study is limited to investigate the current state of usable security guidelines, principles and method from the IT professionals' point of view. Thus, the survey does not cover other fields of usable security where the impact is not dependent on the IT professionals.

10. Limitations of the Study of IT Professionals' Awareness of Usable Security

Due to the lack of prior research studies on the topic of usable security, it is possible that the survey will not clearly identify the gaps between the security and usability. Therefore, the survey is designed with the goal of identifying current awareness of IT professionals in the studied field. The primary goal is to examine, if people working in IT know how important is usability from the security point of view.

Another limitation of the research is the lack of access to the people. While the survey was meant to be performed as an interview, which tends to bring better results, the survey was carried out remotely using an online questionnaire. The survey was carried out in the organisation, which provides numerous security solutions.

11. Evaluation of the Study of IT Professionals' Awareness of Usable Security

A total of 20 participants working in a certain phase of software development took part in the survey. Almost half of the participants work in the field of security. The figure 2 shows the phrases the professionals work in.

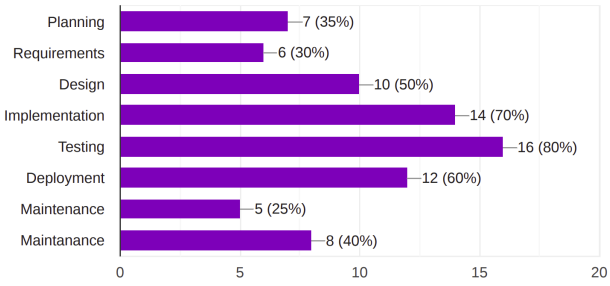

Figure 1. Distribution of software development phases participants work in

Professionals who participated in this survey have different experience in the IT industry. The following figure figured on table 2 shows the distribution of years of experience within the IT field.

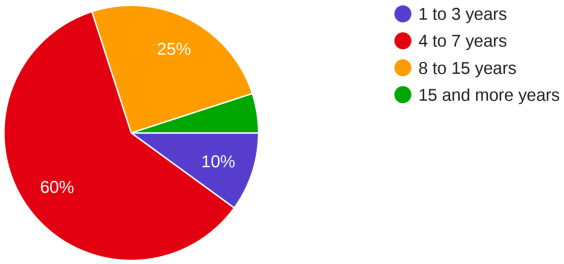

Figure 2. Work experience in the IT industry

The first part of the questionnaire was devoted to the current awareness of security. Almost a half of participants have never heard the term usable security before. The figure 3 shows the percentage of participant that have(yes) or have not(no) heard of this term.

Half of the participants confirmed that they are not given security criteria to be meet in their work when performing their tasks and 55% of the participants do not get the usability criteria in order to perform their task with respect to usability factor.

Only three of the participants defined that they use tools to increase usability. However, these tools only address specific areas of usable security. The OWASP has been mentioned as a guide to ensure usable security of web applications.

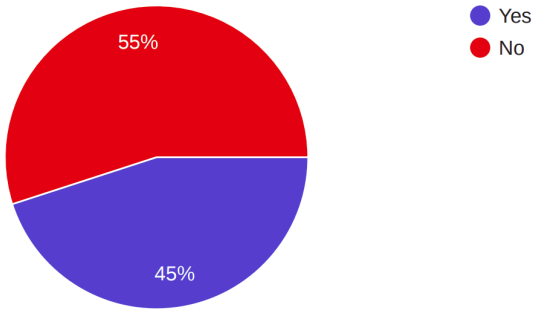

Figure 3. Awareness of the term usable security

One part of the survey was devoted to the methods IT professionals use to develop usable and secure software. The outcome of the survey showed that there is a lack of tools available.

An interesting result of the questionnaire is that more than half of the respondents see security and usability as competing factors. 60% of respondents consider security as a secondary concern.

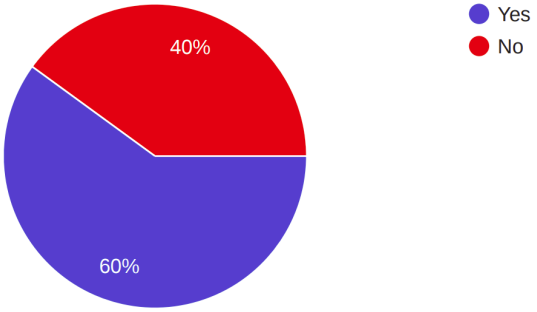

Figure 4. Security as a secondary concern

12. Conclusions

Poor usability and security is often considered as a big disadvantage of the computer systems. The theoretical research of existing standards, guidelines and principles related to the area of usable security from the IT professionals perspective showed the lack of existing materials. While there are many security standards and guidelines for IT professionals, there is a lack of guidance for usable security. The general standards for software development from common institutes for standardization has a significant impact on the security. However, they are more focused on the security aspect and do not take the usability fully under consideration.

According to the research, human factor is considered as the weakest link in the security processes. This highlights the need for making the security solutions more usable. Significant research focusing on the end users has been done in recent years. These papers focus on ensuring the usable security of the security mechanisms they use. Providing the IT professionals the appropriate guidance to create such a solution could increase the overall security.

Due to a insufficient amount of existing research, a study of usable security in form of a survey has been designed and carried out. This survey has been designed based on the basis provided by the theoretical research. The main focus is given to examination of current awareness of IT professionals and their knowledge of current standards, guidelines or methods. A study aims to distribute the participants demographically, examine their awareness and find out about the standards, guidelines and different materials they use.

The evaluation of the study of IT professionals' current awareness confirmed the hypothesis that people working in IT are not aware of usable security or are aware of the term usable security, but they are not aware of any tools for this purpose.

The result of this paper is a carried out survey for IT professionals and the evaluation the current situation that indicates the form of guidance would increase the awareness of usable security within the professionals and what could help the newcomers from their beginning.

The future aim of this research is to speed up the process of gaining awareness of the usable security solutions and knowledge of how to do it. The creation of the education aid that would be explanatory to the newcomers in IT will ensure the achievement of this goal. The goal will be reached by creating an education and explanatory aid.

Acknowledgements

Thanks to my supervisor Mgr. Kamil Malinka, Ph.D for his leadership and support. This paper would not have been possible without his technical advice and continuous encouragement.

References

[1] Claudia Acemyan, Phil Kortum, Jeffrey Xiong, and Dan Wallach. 2fa might be secure, but it's not usable: A summative usability assessment of google's two-factor authentication (2fa) methods. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 62:1141–1145, 09 2018.

[2] Bryan Payne and W. Edwards. A brief introduction to usable security. *Internet Computing, IEEE*, 12:13–21, 06 2008.

[3] Tony Rice, Josh Brown-White, Tania Skinnerand Nick Ozmore, Nazira Carlage, Wendy Poland, Eric Heitzman, and Danny Dhillon. Fundamental practices for secure software development, third edition. 2018.

[4] S. Chiasson, R. Biddle, and Anil Somayaji. Even experts deserve usable security: Design guidelines for security management systems. 2007.

[5] Markus Lennartsson, Joakim Kävrestad, and Marcus Nohlberg. *Exploring the Meaning of "Usable Security"*, pages 247–258. 08 2020.

[6] S. Garfinkel and H. R. Lipford. 2014.

[7] Hans-Joachim Hof. User-centric it security - how to design usable security mechanisms. 01.

[8] A. Whitten and J. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX Security Symposium*, 1999.

[9] O. Gordieiev, V. Kharchenko, and Kate Vereshchak. Usable security versus secure usability: an assessment of attributes interaction. In *ICTERI*, 2017.

[10] Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models. Standard, International Organization for Standardization, Geneva, CH, March 2018.

[11] Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. Standard, International Organization for Standardization, Geneva, CH, March 2018.

[12] Yee-Yin Choong, Shaneé Dawkins, Susanne Furman, Kristen Greene, Julie Haney, Kerrianne Morrison, and Mary Theofanos. Nist usable cybersecurity. online, 2021.

[13] Alain Abran, Adel Khelifi, Witold Suryn, and Ahmed Seffah. Usability meanings and interpretations in iso standards. *Software Quality Journal*, 11:325–338, 11 2003.

[14] Jason Nurse, Sadie Creese, Michael Goldsmith, and Koen Lamberts. Guidelines for usable cybersecurity: Past and present. pages 21 – 26, 10 2011.

[15] F. Sahar. Tradeoffs between usability and security. *International journal of engineering and technology*, pages 434–437, 2013.

[16] Majed Alshamari. A review of gaps between usability and security/privacy. *International Journal of Communications, Network and System Sciences*, 09:413–429, 01 2016.

[17] Paulo Realpe-Muñoz, César A. Collazos, Toni Granollers, Jaime Muñoz Arteaga, and Eduardo B. Fernandez. Design process for usable security and authentication using a user-centered approach. In *Proceedings of the XVIII International Conference on Human Computer Interaction*, Interacción '17, New York, NY, USA, 2017. Association for Computing Machinery.

[18] Joshua Tan, L. Bauer, Nicolas Christin, and L. Cranor. Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020.

[19] M. M. Althobaiti and P. Mayhew. Usable security of authentication process: New approach and practical assessment. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 179–180, 2015.

[20] A. D. Luca, A. Hang, E. V. Zezschwitz, and H. Hußmann. I feel like i'm taking selfies all day!: Towards understanding biometric authentication on smartphones. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015.

[21] Hesham Al-Ammal and Lamya Aljasmi. Usability, encryption, and the user experience. *KnE Engineering*, 3:71, 10 2018.

[22] Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov. The most dangerous code in the world: validating ssl certificates in non-browser software. pages 38–49, 10 2012.

[23] M. Alhanahnah and Q. Yan. Towards best secure coding practice for implementing ssl/tls. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–6, 2018.

[24] Sascha Fahl, Marian Harbach, Henning Perl, Markus Koetter, and Matthew Smith. Rethinking ssl development in an appified world. pages 49–60, 11 2013.

[25] Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation).

[26] P. Faurie, A. Moldovan, and I. Tal. Privacy policy – “i agree”?! – do alternatives to text-based policies increase the awareness of the users? In *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pages 1–6, 2020.