BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF INFORMATION TECHNOLOGY
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF INTELLIGENT SYSTEMS
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

USABILITY OF USABLE SECURITY GUIDELINES FROM IT PROFESSIONAL POINT OF VIEW

POUŽITELNOST POKYNŮ PRO POUŽITELNOU BEZPEČNOST Z POHLEDU IT PROFESIONÁLA

MASTER'S THESIS
DIPLOMOVÁ PRÁCE

AUTHOR **Bc. KATARÍNA GALANSKÁ**
AUTOR PRÁCE

SUPERVISOR **Mgr. KAMIL MALINKA, Ph.D.**
VEDOUCÍ PRÁCE

BRNO 2021

Brno University of Technology
Faculty of Information Technology

Department of Intelligent Systems (DITS) Academic year 2020/2021

Master's Thesis Specification

Student:	**Galanská Katarína, Bc.**
Programme:	Information Technology
Field of study:	Information Technology Security
Title:	**Relevance of Usable Security Guidelines from IT Professional Point of View**
Category:	Security

Assignment:

1. Study existing guidelines, standards and other materials related to the area of usable security.
2. Carry out a survey to investigate the current state of IT professionals awareness of usable security guidelines (test their knowledge of guidelines and methods they use).
3. Based on obtained results, evaluate applicability of existing materials and suggest modifications for their improvement.
4. Design and create educational aids that make this area more accessible for newcomers. Cover the most important areas (passwords and authentication, encryption, cybersecurity adoption, user characteristics).
5. Evaluate impact of created aids on IT professionals awareness of usable security area.

Recommended literature:

- https://www.diva-portal.org/smash/get/diva2:1440015/FULLTEXT01.pdf
- https://www.computer.org/csdl/magazine/co/2020/02/08996098/1hmvFwV0yty
- https://academic.oup.com/cybersecurity/article/5/1/tyz014/5681668
- https://link.springer.com/chapter/10.1007/978-3-030-50309-3_41
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7676139

Requirements for the semestral defence:

- Items 1 to 3.

Detailed formal requirements can be found at https://www.fit.vut.cz/study/theses/

Supervisor:	**Malinka Kamil, Mgr., Ph.D.**
Consultant:	Homoliak Ivan, Ing., Ph.D., UITS FIT VUT
Head of Department:	Hanáček Petr, doc. Dr. Ing.
Beginning of work:	November 1, 2020
Submission deadline:	May 19, 2021
Approval date:	November 11, 2020

Abstract

Balancing the security and usability has always been a challenge. Despite the importance of securing 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 introduces the study of current awareness in area of usable security. The work consists of carried out survey, analysis of the existing usable security guidelines and proposes a educational aid in order to address the issues raised by the research. The evaluation of the education aid showed a positive impact on the IT professionals awareness.

Abstrakt

Vyvážení bezpečnosti a použitelnosti bylo vždy výzvou. Navzdory důležitosti zabezpečení softwaru jsou bezpečnostní pokyny a standardy často příliš komplikované, náchylné k chybám nebo časově náročné. Tato nerovnováha iniciovala vznik pojmu použitelné bezpečnosti. Po celá léta to byl běžný výzkumný problém. Zatímco softvér by měl být vyvíjen s ohledem na použitelnost koncových uživatelů, bezpečnostním standardům a směrnicím, které používají IT profesionálové, není z hlediska použitelnosti často věnována dostatečná pozornost. Vzhledem k tomu, že se od odborníků v oblasti IT očekává vyšší úroveň znalostí, často čelí velmi složitým oblastem, když se snaží vyhovět konkrétním bezpečnostním standardům nebo dodržovat konkrétní pokyny. Tato práce představuje studium současného povědomí v oblasti použitelné bezpečnosti. Práce sestává z provedeného průzkumu, analýzy stávajících použitelných bezpečnostních pokynů a navrhuje vzdělávací pomůcku k řešení problémů, které výzkum přinesl. Hodnocení vzdělávací pomůcky ukázalo pozitivní dopad na povědomí IT odborníků.

Keywords

usability, security, usable security, authentication, encryption, privacy

Klíčová slova

použitelnost, bezpečnost, použiteľná bezpečnost, autentizace, šifrování, soukromí

Reference

GALANSKÁ, Katarína. *Usability of Usable Security Guidelines from IT Professional Point of View.* Brno, 2021. Master's thesis. Brno University of Technology, Faculty of Information Technology. Supervisor Mgr. Kamil Malinka, Ph.D.

Rozšířený abstrakt

Úvod

S tím, jak se svět propojuje, roste potřeba bezpečných a použitelných systémů. Zranitelnosti softwaru představují obrovská rizika kybernetických zločinů. Proto mnoho organizací a institucí bojuje proti zákeřným záměrům vytvářením bezpečnostních řešení, standardů a pokynů, které, pokud budou dodrženy, zajistí odpovídající úroveň zabezpečení. Jejich význam je evidentní, avšak bezpečnější řešení nemusí nutně snižovat pravděpodobnost budoucího útoku. V dnešní době jsou bezpečnostní opatření stále složitější. Střed pozornosti je věnován zabezpečení samotného zařízení. Nedávné výzkumné práce ukazují, že nejzranitelnější částí bezpečnostního dodavatelského řetězce je lidský prvek. Zranitelným faktorem může být softwarový architekt vytvářející design, vývojář implementující systém nebo koncoví uživatelé provádějící bezpečnostní postupy nesprávným způsobem.

Použitelná bezpečnost se nevztahuje pouze na zkušenosti koncových uživatelů. Měla by představovat celý proces vývoje bezpečnostního produktu od vytvoření až po použitelnost pro koncového uživatele. Může to zahrnovat návrh, vývoj, konfiguraci, údržbu produktu atd. Týká se to například věcí, jako organizace funguje a používá zásady a procesy, jakož i faktorů, které ovlivňují přístup lidí k jejich práci a zachování kybernetické bezpečnosti při práci.

Staré bezpečnostní produkty často selhaly, protože použitelnost nebyla považována za stejně důležitou prioritu návrhu. Bezpečnost a použitelnost není možné přidat hned po vývoji technologie, ale měly by být nedílnou součástí procesu navrhování produktu od samého začátku.

Tato práce si klade za cíl nastudovat současný stav použitelných bezpečnostních pokynů, standardů a dalších materiálů a zkoumat současný stav povědomí IT profesionálov o těchto materiálech. Práce provádí průzkum založený na teoretickém výzkumu stávajících standardů, pokynů a různých materiálů souvisejících s pojmem použitelné bezpečnosti. Vzhledem k zaměření na IT profesionály jsou účastníky průzkumu profesionálové pracující ve vývoji softwaru. Aby byli výsledky studie co nejkvalitnější a nejpestrejší, účastníci jsou z různých oblastí IT. Výsledky nastiňují úrovně znalostí IT profesionálů v této oblasti. Výsledky odhalují metody, které IT odborníci používají, a problémy s použitelností, kterým čelí při vývoji bezpečnostních řešení. Získané výsledky vyhodnocení průzkumu jsou indikátory použitelnosti současných pokynů, pokud jsou použity, a navrhují možné úpravy.

Popis řešení

Získané výsledky průzkumu byly dále analyzovány. Výsledek průzkumu poskytl informace o stávajících pokynech a standardech používaných IT profesionály. Celkové výsledky ukázaly, že polovina účastníků ani nevěděla o termínu použitelnost zabezpečení a jenom 15 procent účastníků tvrdilo, že používá standardy nebo pokyny, pokud jde o použitelnú bezpečnost.

Vyhodnocení těchto pokynů, norem a dalších materiálů, které byly výsledkem vykonaného průzkumu, ukazuje na nedostatečnost použitelnosti. Jedinými standardy, které účastníci zmínili, jsou normy ISO / IEC 2700x, které jsou zaměřeny na definování ovládacích prvků pro systém řízení informací (ISMS). Pokyny, které účastník uvedl, že použí-

vají, jsou zaměřeny na konkrétní oblast IT. Například Průvodce testováním OWASP vede vývojáře k tomu, aby ověřili zranitelnost svých webových aplikací. Výsledek analýzy poskytuje možné úpravy pro jejich zlepšení, konkrétně zahrnuje více případových studií nebo příkladů z reálného světa. Ostatní materiály mohou být příliš složité a obtížně čitelné. Podle analýzy předchozí studie bylo možné definovat požadavky na vzdělávací pomůcku. Navrhovaný software je webová aplikace, jejímž cílem je zvýšit povědomí uživatelů čtením o vybraných oblastech v rámci použitelné bezpečnosti a vyplněním kvízů. Účelem navrhované aplikace je pomoci nově příchozím lidem v oblasti IT a zpřístupnit oblast použitelné bezpečnosti. Důraz je kladen na konkrétní oblasti, jako jsou problémy v rámci opětovného ověřování, nedostatek použitelnosti v oznámeních o ochraně osobních údajů nebo zneužití kryptografických API. Vybrány jsou oblasti, kde může nedostatek použitelnosti vést k obrovskému nárůstu bezpečnostního rizika.

Výsledky práce

Výsledek průzkumu poskytol informace o současném stavu povědomí IT profesionálů a jejich znalostech nástrojů v oblasti použitelné bezpečnosti. Výsledek naznačil nedostatek povědomí, neexistující standardy a nepoužitelné nástroje. Podrobná analýza nástrojů, které účastník používá, postrádá rozsah nebo skutečnost, že by měly být pro vývojáře zacíleny. To zahájilo analýzu toho, co by mohlo zvýšit povědomí lidí pracujících v oblasti IT o problémech použitelnosti a vybraných výzvách v oblasti použitelné bezpečnosti.

Navrhovaný software je webová aplikace, jejímž cílem je zvýšit povědomí uživatelů čtením o vybraných oblastech a vyplňováním kvízů. Zaměření je specificky věnováno výzvám v oblastech, jako je soukromí, ověřování nebo kryptografické API. Tyto oblasti byly vybrány, protože jejich zneužití může vést k obrovskému nárůstu bezpečnostních rizik.

Dopad implementovaného softwaru se hodnotí provedením uživatelské studie, kde uživatele jsou lidé pracující ve vývoji softwaru. Cílem studie bylo zjistit, zda existuje dopad na povědomí o použitelné bezpečnosti účastníků. Studie se zúčastnilo celkem 6 lidí, kteří poskytli kvalitativní zpětnou vazbu. Celkové výsledky ukazují pozitivní dopad na povědomí účastníků.

Závěr

Špatná použitelnost a bezpečnost je často považována za velkou nevýhodu počítačových systémů. Teoretický výzkum stávajících standardů, pokynů a principů týkajících se oblasti použitelné bezpečnosti z pohledu IT profesionálů ukázal nedostatek existujících materiálů.

Vzhledem k nedostatečnému množství stávajícího výzkumu byla navržena studie formou průzkumu. Tento průzkum byl navržen v souladu s výsledky teoretického výzkumu. Hlavní důraz je kladen na zkoumání současného povědomí IT odborníků a jejich znalostí současných standardů, pokynů nebo metod.

Výsledky průzkumu byly dále analyzovány a poskytli informace o stávajících pokynech a standardech používaných IT profesionály. Celkové výsledky ukázaly, že polovina účastníků ani nevěděla o pojmu použitelné bezpečnosti a jenom 15 procent účastníků tvrdilo, že používá standardy nebo pokyny, pokud jde o použitelnú bezpečnost.

Vyhodnocení těchto pokynů, norem a dalších materiálů ukazuje na nedostatečnost použitelnosti. Výsledek analýzy poskytuje možné úpravy pro jejich zlepšení, konkrétně

včetně více případových studií nebo příkladů z reálného světa. Jiné materiály mohou být příliš složité a obtížně čitelné.

Na základě analýzy předchozí studie bylo možné definovat požadavky na vzdělávací pomůcku. Navrhovaný software je webová aplikace, jejímž cílem je zvýšit povědomí uživatelů čtením o vybraných oblastech a vyplňováním kvízů. Důraz je kladen na konkrétní oblasti, jako jsou problémy v rámci opětovné autentizace, nedostatečná použitelnost v oznámeních o ochraně osobních údajů nebo zneužití kryptografických API. Vybrány jsou oblasti, kde může nedostatek použitelnosti vést k obrovskému zvýšení bezpečnostního rizika.

Dopad implementovaného softwaru byl hodnocen provedením uživatelské studie, kde účastníky byli lidé pracující ve vývoji softwaru. Výsledky ukázaly, že vzdělávací pomůcka pomohla účastníkům porozumět vybraným výzvám v oblasti použitelné bezpečnosti. Vytvoření vzdělávací pomůcky tedy sloužilo lidem pracujícím na vývoji softwaru k dosažení výše uvedeného cíle.

Tato práce byla prezentována na konferenci ExcelFIT a byla publikována výzkumná práce k první části této práce. Nasazená aplikace je plně nasazená a veřejně dostupná.

Usability of Usable Security Guidelines from IT Professional Point of View

Declaration

I hereby declare that this Masters's thesis was prepared as an original work by the author under the supervision of Mgr. Kamil Malinka, Ph.D. I have listed all the literary sources, publications and other sources, which were used during the preparation of this thesis.

.....
Katarína Galanská
May 19, 2021

Acknowledgements

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

Contents

Chapter 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 secure solution does not necessarily lower the likelihood of the future attack.

Nowadays, the security measures are becoming more and more complex. The centre of attention has been given to the security establishment. Recent research papers show that the most vulnerable part of the security supply chain is the human element. 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 is still a not enough focus on the usability of the system during the software development. Moreover, there is not as many consideration from the IT professional point of view as it is from the users perspective. 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. 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 usability aspect.

Balancing the usability and the security in the IT industry has always seemed to be a challenge. Based on this issue the term usable security became known as a common research problem. The security and usability context is frequently studied for over a decade. While an comprehensive security is desired from any software, it is also often being considered at the end of the development, which can obstructs the usability. Moreover the security

strengthening may undermine the usability. For a long time the security and usability were considered to be a competing goals. The field of usable security has different perspective. There are existing research papers focusing on the topic on usability and security from the user's point of view . Regarding to the human element as the most vulnerable, creating more usable security functions can improve the overall security.

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 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 thesis aims to study the current state of the usable security guidelines, standards and other materials and investigate the current state of IT professionals awareness of these materials. The thesis carries out an survey based on theoretical research of the existing standards, guidelines and different material related to the term usable security. As the focus is given to the IT professionals, the participants of the survey are professionals working in software development. In order to receive the most quality feedback, the participants are from different field of IT. 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.

The outcome of the survey provides the information about the current state of IT professionals awareness and their knowledge of the tools within the usable security field. The result indicated the lack of awareness, no existing standards and inapplicable tools. The detailed analysis of the tools participant use are lacking the scope or the fact that they should be targeted for the developer. This initiated the analysis of what could raise the awareness of people working in IT field about the usability issues and selected challenges within the usable security field.

The proposed software is a web application aiming to increase users' awareness by reading about selected areas within usable security and completing quizzes. The focus is specificaly given to challenges within areas such as privacy, authentication or cryptographic API. These areas have been selected because their misuse can lead to a huge increase of security risks.

The impact of the implemented software is evaluated by conducting a user study, where the user are people working in software development. The aim of the study was to determine whether there is an impact on participants' usable security awareness. A total of 6 people participated in the study and provided the qualitative feedback. The overall results shows the positive impact the the participants awareness.

The document is further structured in eight chapters. The next chapter 2 is dedicated to specifying the methodology of this thesis. A part of this chapter defines the current state of the art and highlight the reason behind the research. Another goal is to define the thesis questions are then evaluated in last chapter.

The third chapter focuses on the characteristics of usability and security. Discussed is not only the end user's perspective but the importance is given to the IT professional's point of view. It summarises the current state of standards, guidelines and other materials

on usable security. The last section of the chapter is dedicated to selected challenged of usable security and case studies within them.

The chapter number 4 covers the study on the selected group of IT professionals. The main goal of this chapter is to investigate their current awareness of existing standards, guidelines and other materials related to usable security. The user study is dedicated to the first thesis question. Another goal is to perform an evaluation of the results from the study and aims to evaluate the guidelines, standards and frameworks used by participant in order to satisfy the usable security requirements. The main objective is to evaluate the applicability of selected tools. Moreover, this part also suggest possible modification of selected guidelines in order to make them more applicable.

The fifth chapter is devoted to the analysis of requirements for the educational aid. At first the importance of educating people included in software development is explained and then the chapter introduces the specific requirements for the application. The technical design is

The chapter number six introduces the selected areas of usable security with the focus on the usability issues connected to them. For each area, the consequences of the misuse are given together with the case study. These challenges represents an example of the content provided by the educational aid.

Next chapter deals with the implementation of the proposed tool. Each of the implemented modules is explained in details together with the third party packages. At the end of the chapter, the process of deployment is outlined.

The final part discusses and evaluates the impact of created tool on the IT professionals. The evaluation is based on the user study, where the users are people working in the software development cycle. The results shows the positive impact on participants and discusses the concrete outcomes of this thesis.

Chapter 2

Aims and Methodology

2.1 Methodology

The methodology of this thesis is based on the examination, evaluation and analysis of existing standards, guidelines and other materials for usable security. The emphasis was given to the IT professionals' perspective. For this purpose, both literature and online resources will be used, dealing with materials providing IT professionals with a guide for usable and secure software development. A part of this thesis is a survey, which has a goal to determine the current state of IT professionals' awareness within the field of usable security. Based on the research and the results of following study, the applicability of the existing guidelines, standards and other materials is evaluated. The evaluation builds a basis for the design of a web application, serving as the educational aid. The design of the educational aid, its functionality and possible usage is described in detail together with chosen areas of usable security, where there is a need to raise awareness. The second round of user study is designed to evaluate the awareness of the users of the application. The study is included within the application in a form of the questionnaire, and exists for each selected area of usable security. The participants are asked to fill the questionnaire before and after reading the guideline. The impact for participating users from IT field is evaluated from the results of people asked to use the application.

2.2 State of the Art

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 the research paper 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.

2.3 Thesis Questions

To satisfy mentioned expectations the following research question are raised:

1. What is current state of IT professionals awareness of usable security guidelines?
2. Can a developed educational aid help to raise higher awareness of usable security?

Chapter 3

Theoretical Research on Usable Security

The theoretical research reviews the literature relevant to this study. This chapter introduces the term usable security and security guidelines, standards and different materials within this area. Discussion of the relevance of the usable security guidelines and standards is mostly focused on the IT professional's perspective. The research concludes with the definition of the current challenges in this field.

3.1 Definition of the Usable Security

The term of usable security has been a target of discussion in many research paper [32, 20, 25]. While this term had no formal definition, it can be described as an 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. 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 [55].

A quote that can be seen on different Information Security Stack Exchange describes common approach to the security during the software development. Many research papers results agree that the security is often a secondary concern [3, 23]. The quote is formulated in following way:

> „Security at the expense of usability, comes at the expense of security."

3.1.1 Characteristics of Security and Usability

The paper Usable Security Versus Secure Usability considers the aspects of security and usability and their competing characteristics [22]. It takes into account the ten characteristics defined in ISO/IEC 25 010 and analyse their mutual influence [27]. The paper analyse 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 would be 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 [27]. The usability area is officially defined by the ISO 9241-11 as in following definition [28].

> „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 characteristics as shown on table 3.1. The factors of usability can be seen also on the figure 3.1.

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

Table 3.1: Representation of Security and Usability According to ISO/IEC 25 010

3.1.2 A Research on Usable Security for End Users

According to the latest research, the users are still often confused or overwhelmed by the security solutions [52]. They are not well aware of what to do to keep themselves and the technology they use safe. National Institute of Standards and Technology (NIST) carried out a research that identified particular aspects that can be one of the reasons why the users are still frustrated. Firstly, they receive too much information which leads to them not being sure of what to do or how to do it. Secondly, when the users face too many security software, like antivirus, firewalls and similar. This software usually runs different checks and can overwhelm the user.

The paper „Is Usable Security an Oxymoron?" introduces the term *security fatigue* as an psychological state reached by a person when the decision in the security field is too complex [52]. This shows that currently existing software often provide very low level of usability. Insufficient usability on the end user side may can be a result of a significant impact of complexity.

3.1.3 A Research on Usable Security for Developers

While in the recent years significant number of research papers occurred has been given to studying the usability factors of security for the end user, not enough focus has been given to the developers and IT professionals [35, 48, 25, 42]. Too complex solutions can overwhelm not only the end user but also the developer [23, 3].

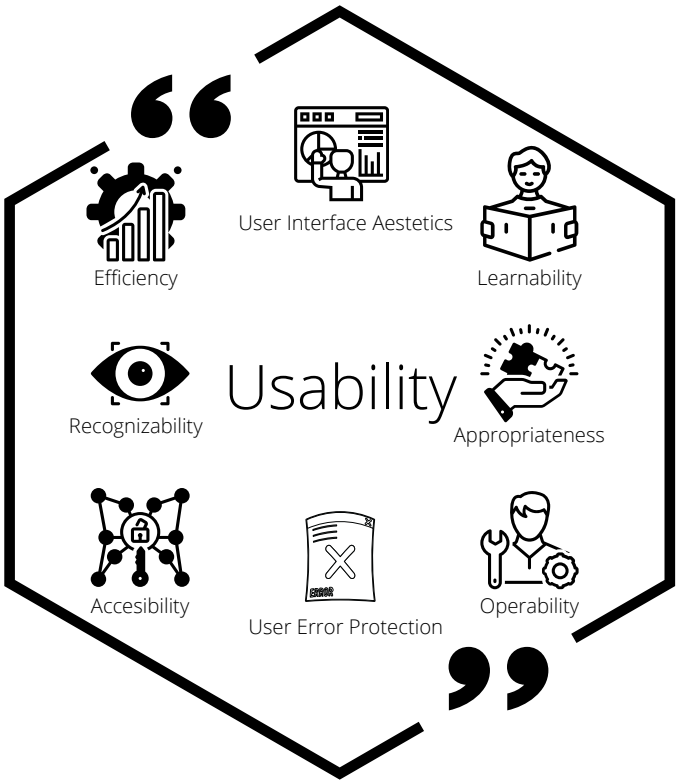

Figure 3.1: Usability characteristics

According to the paper „Developers are not the Enemy“ most of today's IT security incidents are caused by the usability problems [23]. The security guideline's security solutions may seem overly complicated for the user who wants to comply with them. The security mechanisms have a tendency to be time consuming and prone to errors. These are the factors showing the importance of why the balance of security and usability needs to be put in place.

According to the study on the usability of security API, the most of the security mistakes are done by the developers and not by the end users [23]. The small amount of research done on usable security for developers results in not guided developers and the security solutions not implemented in usable way. One of the found papers presents different ways how to improve the support for developers, e.g. usable security libraries or better testing tools.

The guidelines provided to the developers should consider the usability of the security solutions [32]. Although there are research done on the topic of usability of security solutions for the users, developers are still not well aware of the impact of lower usability level to the security.

A recent paper studying the impact of copy and pasting the code from Stack Overflow found out that out of 1.3 million Android applications, about 15% has contained code from Stack Overflow related with security [17]. From these selected applications about 97% contained an insecure code. This shows that programmers use code snippets found on the Internet. The worst part concluded from this research is that they do so without really understanding the code. The research was focused on the code snippets related to android

application security. The result of this paper was the automated processing for evaluation of parts of code posted on Stack Overflow.

The results of a recent research examined the degree of security integration in each stage of software development life cycle(SDLC). As a part of this research a interview study in multiple different topic was conducted. The questions asked about general developments activities, attitude towards security, security and testing processes and overall security awareness. Total of 13 participants filled the questionnaire. The results divided the participants in two distinct groups. The first group A considered security in the most of the stages of SDLC. On the other hand, the second group B barely considered security at all in any of the stage of SDLC. As the overall outcome of this research, the author discussed how is security prioritized in each stage of the SDLC. The following table 3.2 represents the important practices from the research. The A represents the first group of developers who consider the security as an important factor and the B represents the second group who consider the security as secondary concern.

Group	Stage	Practise
A,B	Design	Security is not considered.
B		The consideration of security is adhoc.
A		Security design is very important.
A,B	Implementation	Security is mostly a priority.
A,B		Developers are expected to be aware of the security perspective.
A,B		For smaller group of developers the security is not a priority.
B		Security can be taken for granted.
B		Developers misuse frameworks.
B		Not all developers have security knowledge.
B		Developers' perception on security is no accurate.
A,B	Testing	Developers do not do security testing.
A		For some developers the security is a priority.
A		Security is not absolutely dismissed.
B		Security testing is feature driven.
A	Code Analysis	Security is mostly a priority.
A		Security is a secondary concern.
B		The code analysis is performed rarely, the security analysis never.
B		No awareness of analysis tools.
A	Code Review	Considered as formal process that includes security.
A		Considered a checkpoint before the formal review.
B		Security is not considered.
B		Minimal consideration of security.
A	Post-development Testing	Security is a priority.
A		Used to discover security vulnerabilities.
A		Final approved given by testers.
B		Security is not considered.
B		Testing plan includes a security factor.
B		Security testing is feature driven.
B		The consideration of security is adhoc.
B		Security testing is externally driven.

Table 3.2: Developers' consideration of security in SDLC stages

3.2 Approaches to Software Development

During its development, each SW goes through several phases, which are described by the model SW life cycle. An example is e.g. waterfall or agile model. The models deal mainly with the development and possibly the time after the development, but already typically does not address the security aspect. Therefore, several approaches to integration have emerged security processes into the development model. In this chapter, the most important approaches will be introduced and compared.

3.2.1 Existing Approaches

OWASP CLASP extends existing SW development so that security is taken into account from the very beginning. It seeks to achieve this through structured, repeatable and measurable activities. It consists of five high-level views. These show how the individual CLASP components interact and how to apply them to development. Seven Best Practices that can be compared to the MS SDL phases. Twenty-four Activities corresponding to activities from the World Cup SDL. In addition, resources that help project managers, in particular, understand how to plan and implement CLASP activities. Finally, Taxonomy, which is a high-level classification, divided into several classes. This makes it easier to assess and respond to security vulnerabilities in your code.

A detailed document on the integration of security processes into SW development was also issued by NIST. The document should meet the security requirements summarized in the document and others. For each phase, references to extending NIST documents are also mentioned. At the beginning, it contains an overview of typical development methodologies, with the caveat that it is only aimed at a waterfall model for simplicity. Nevertheless, the presented activities should be applicable anywhere. A table with all the key roles and the description of their responsibilities is also very useful.

NIST divides the waterfall SW development model into five phases:

1. Initiation
2. Development/Control
3. Implementation
4. Maintenance
5. Closing.

Each phase initially contains a brief explanation of what will take place in it. Subsequently, the so-called control gate, which is a summary of important milestones that must be met at a given stage, and finally a detailed description of all security activities. In addition, each activity again contains a detailed description, expected outputs, dependencies on other activities and a description of who will be affected by the activity. Finally, for each phase, a clear diagram of the progress of activities is shown with a description of the important components.

Cisco also offers its own approach to developing secure SW. The official website states that it is applicable to a variety of operating systems, both for waterfall and agile development methods. It is also compatible with ISO9000 certification requirements.

Cisco SDL(CSDL) includes six key phases: Product Security Requirements, Third Party Security, Security Design, Security Coding, Security Analysis, and Vulnerability Testing. The phases cover a similar circuit as the other approach. OF

3.3 Study of Existing Standards, Guidelines and Other Materials

3.3.1 Methodology

The methodology of this thesis is based on the examination, evaluation and analysis of existing standards, guidelines and other materials for usable security. The emphasis was given to the IT professionals' perspective. For this purpose, both literature and online resources will be used, dealing with materials providing it professionals with a guide for usable and secure software development. A part of this thesis is a survey, which has a goal to determine the current state of IT professionals' awareness within the field of usable security. Based on the research and the results of following study, the applicability of the existing guidelines, standards and other materials is evaluated. The evaluation builds a basis for the design of a web application, serving as the educational aid. The design of the educational aid, its functionality and possible usage is described in detail together with chosen areas of usable security, where there is a need to raise awareness. The second round of user study is designed to evaluate the awareness of the users of the application. The study is included within the application in a form of the questionnaire, and exists for each selected area of usable security. The participants are asked to fill the questionnaire before and after reading the guideline. The impact for participating users from IT field is evaluated from the results of people asked to use the application.

Theoretical research 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.

3.3.2 Standards for Usable Security

Security standards are security techniques that enable organizations to take action to minimize attacks on computer networks. The reason behind creation of such techniques is an increasing need to keep stored data safe. With growing dependence on digital systems, cyber threats and attacks are on the rise.

While there are many security standards for secure development, the usability factor being considered as a secondary concern [37]. 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.

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 a research paper Usability Meanings and Interpretations in ISO Standards [2]. The focus of the research has been given to standards ISO 9126 and ISO 9241. The result of the study indicates that the usability definition has not been synchronized within experts and researchers. 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.

3.3.3 Guidelines and Principles for Usable Security

The most of the guides for secure development focuses on the security perspective and the usability is still not fully incorporated [42]. The attempt of defining the guidelines for usable and secure development proposed a set of design guidelines for security management interfaces [11]. 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.

The problems that the field of cybersecurity usability is facing has already been reviewed [35]. 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 [25]. The created set of nine design guidelines aim 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 to many password it is less usable. The users may prefer to use existing account to authenticate.
- The security measures should be pre-configured 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 [32]. The result of the thesis is a hierarchical model of aspects on usable security and their impact. The simplicity and time provided for the security procedure, as aspects, showed a significant impact of security.

3.4 Current Challenges of Usable Security

This section is devoted to the selected current challenges of usable security. The areas are chosen according the the study of recent research done in this field [12, 10].

3.4.1 Passwords and Authentication

The growing use of the Internet brought the need of authentication of the user connected with many security measures, security testing and secure coding [39]. During the designing these measures, implementing and testing them 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.

According to the the research studying the design process for usable security and authentication developers are often not provided with guidance for creating the usable and secure software design [39]. The paper Design Process for Usable Security and Authentication Using a User-Centered Approach presented different models, which can make the development easier, however it also highlighted the need for more research in order to achieve better balance between the security and the usability.

The importance of the systems usability has been presented by many research papers [32, 25, 11]. The incorporation of usability into the security features still seems to be an issue [39]. The research introduced authentication goals as part of the requirements for usable security improvement. One of the listed goals was the need for effective and secure authentication with at least one resource. Another goal requires the user to be able to remember the authentication process easily. The steps that need to be taken could not be too complex and hard to remember.

Identification by Username and Password

The challenge in this authentication method is to figure out the trade-off between the usability and the security element [43]. Despite different effort of the professionals on replacing the text password, people are still used to perform authentication through login and password [20]. 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 [48]. Recently, a research introducing the practical recommendations for more usable and secure passwords was published. The aim of the paper is to evaluate multiple combinations

of minimum length, minimum strength and different blocklist requirements. The outcome of the research are concrete recommendations for creating password policies. According to the paper, the recommendations takes into account the balance between the usability and the security. Experiments explored three types of password requirements and showed that increasing the password length may not only have a negative impact on the usability but also does not increase the strength of the password. In case of blocklists, experiments outlined the need for checking the password against about 10^5 most common passwords. The checking process should be done using a fuzzy matching algorithm. In case of minimum strength policies, the experiments resulted into a recommendation to limit password creation with 12 characters within at minimum one character class and the password can not be guessable in less then 10^{10} guesses. In another words, the password can not be weaker than 10^{10} guesses.

Related experiments

In recent years multi-factor authentication is becoming the more and more popular [8]. 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. The actions of the users have been recorded. The users were able to authentication using the secure device, card reader and using their fingerprints. Based on the actions, the researchers were able to determine if the authentication that the process is not sufficient to meet the needs of end user. 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 [33]. The „password“ can not 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.

The research paper „A Study on Usability and Security of Mid-Air Gesture-Based Locking System“ proposed a new mid-air based gesture authentication [19] . The interesting part is that they evaluated the new method in accordance to the Multi-Criteria Satisfaction Analysis as shown on the figure 3.2.

Re-authentication

The process of re-authentication overall improves the security of the application [56]. This approach is more and more used in nowadays' systems and helps to mitigate the risk of impersonation attack. Making the user to re-authenticate after a defined time period makes sure that there is the right user using authenticated account. From the usability perspective it can bring a significant amount of annoyance to the user. The lack of re-authentication brings the risk of stealing another persons identity. A study including more than 5 hundred participants showed that the users are happy with getting the verification code in both subject and body of the email [56].

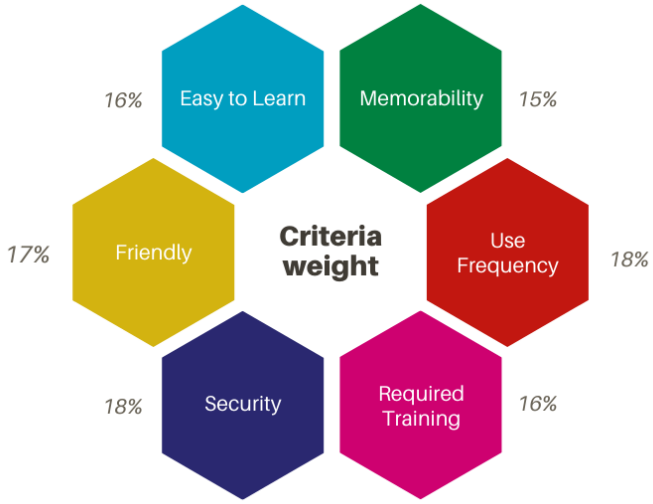

Figure 3.2: Criteria weight for mid-air gesture based authentication

3.4.2 Encryption

One of the challenges within the field of usable security is the data encryption [37]. It is the most widely used method for authentication and access control. As nowadays personal and sensitive data are daily 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 [55]. 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 [4]. The result of the researchers' survey showed the IT professionals awareness of the encryption tools could be increased.

Email Encryption

The analysis of email encryption from the usable security perspective identified a room for improvement [25]. 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 [25]. 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.

3.4.3 Digital Certificates

When establishing any connection over the Internet, e.g. browsing the web or sending an email, a large amount of information travels through the network [13]. They are sent by the client, e.g. an Internet browser, and a server, eg. the one running the website we want to visit. The information includes virtually all the content the user sees on the website, but also actions the user does. Since there are a number of other network elements in the network between the client and the target server, it is necessary to secure the connection between the main participants in this communication. Otherwise, someone could eavesdrop on it, or even pretend to be one of the original participants in the communication.

This is taken care of by protocols called Transport Layer Security (TLS) or Secure Socket Layer (SSL) [41]. They are a cryptographic protocols that authenticate data transfer between servers and users. Using these 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 cause by developers [21]. 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 [6]. 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 [15]. The studies introduced the challenge for creating a effective SSL warning messages which would mitigate many software vulnerabilities.

The focus within the research of SSL certificates in terms of usable security has been given to SSL Warnings [46]. The research called 'On the Challenged in Usable Security Lab Studies' investigated the effectiveness of SSL warnings. The study was conducted on 100 participants. During the experiment the participants faced the security decision to proceed the SSL Warning or not. 43 % of participants would leave the web site, 28 % would proceed

if the site would not contain sensitive data, 14 % would ignore the warning and 15 % would react somehow else.

3.4.4 Privacy

Data is very important for the businesses proving services. That is why storing personal data by web merchants is now very common [20]. The EU General Data Protection Regulation (GDPR) defines many security requirements for storing confidential data [1]. 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. There must me an explicit description of the fact, if the data are confidential or shared to 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 [16]. 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.

3.5 Summary

The research focused on exploring the term usable security. The biggest focus has been given to investigate the current state of standards, guidelines and principles to the area of usable security. The result of the research showed the absence of existing standards. The chapter reviewed multiple studies related to this field and current challenges the usable security and highlighted a selection of current challenges within this field.

The influence of the developer on the software security is significant and therefore the usability issues they face must be addressed [58, 29]. Existing guidelines for usable security can be found only in the form of research papers. However, their focus is usually given to the end user's perspective. Considering the existing guidelines there is still a gap for further study. The applicability of proposed existing guidelines has not been evaluated. Moreover, there has not been enough research done on the IT professional's point of view.

The need of finding the trade off between the usability and security has resulted in a lot of research [43]. 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 [7], 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.

Chapter 4

Usable Security Study of the Current State of IT Professionals' awareness

Theoretical research in the previous chapter defined the meaning of usable security and identified several areas along with the challenges this areas face. Therefore, the basis for the study has been provided. The results of the theoretical research showed a lack of existing guidelines for software development with regard to security and usability.

The following study aims to verify the information obtained and confirm the defined hypotheses. The aim of the study was to determine the direction of further work in this area. If the veracity of the hypotheses is confirmed and IT professionals are not very aware of the applicable security, it is necessary to provide them with relevant instructions that will further help them increase not only the security but also the usability of the software being developed. On the other hand, if the people involved in the software development are aware of the usable security, the goal will be to find out what methods they use in their work when performing their tasks.

Due to the first thesis question this chapter outlines the user study performed in order to evaluate the current awareness of the usable security across the people in IT industry. The focus is given to the IT professionals current awareness, their knowledge about guidelines, principles, methods and best practises. The participants 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 design of the educational aid that would be helping newcomers starting with usable and secure IT development.

4.1 Hypotheses

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

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

2. The usability of security solutions is usually considered as the secondary concern.

3. The efficiency of security mechanisms are more important than restrictions determination for end user.

4. Participants believe ensuring visibility of current state of system's security does not interfere with the users' tasks.

The first hypothesis is meant to examine IT professionals' current awareness. The hypothesis that is counting on them considering the usability as secondary issue is based on previous research, where this fact has been already studied within the developers by various research papers [3, 23]. However, this hypotheses have not been examined within wider perspective. The last two hypotheses are based on the proposed guidelines [25]. The study should be able to clarify the current state of participants' awareness.

4.2 Scope of the Study

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.

4.3 Data Collection

Data collection procedure in this survey consisted of online questionnaire, as it is one of the most common way of gathering data from the selected group of individuals Questions of the survey were designed so it is possible to determine the current state of usable security. Survey questions also intended to gather information about the methods of usable security IT professionals use when performing their tasks. The full questionnaire can be found in the appendix A. The survey results were designed to it is possible to fulfill or disprove the proposed hypotheses. The survey consists of three main parts. The first one serves as a demographic distribution where the participants state their level of education, the stages of software development they are part of together with the experience level. Participants were also asked if they are working in the security field. Second part is dedicated to investigation of their awareness of the term usable security and related materials. The last section of the survey tries to examine the methods IT professionals use to satisfy the usable security requirements when performing their tasks.

4.4 Limitations of the Study

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.

4.5 Results 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 4.2 shows the phrases the professionals work in.

The participants were asked what standards they use in three different areas. The first question targeted only the security factor and they participant were asked for security standards, guidelines and other materials they use. The majority of participants listed at least one item. The second question aimed to find out if the participant follow particular guideline to address the usability. Only three people answered to use some guideline or tool, from which two of the respondents developed the tool themselves. The last question about guidelines and standards targeted specifically the usable security. The majority of respondents have responded with the statement of not using any guidelines. Four of the respondents defined standards and guidelines they use. These standards, tools and framework will be evaluated in the next section. An interesting correlation found in the responses is that participants who stated to work in the design phase of software development do not use any standards to satisfy the usable security requirements. Another finding is that all of the people using the guidelines work in the maintenance phase of the software development cycle and three of them work also in deployment phase.

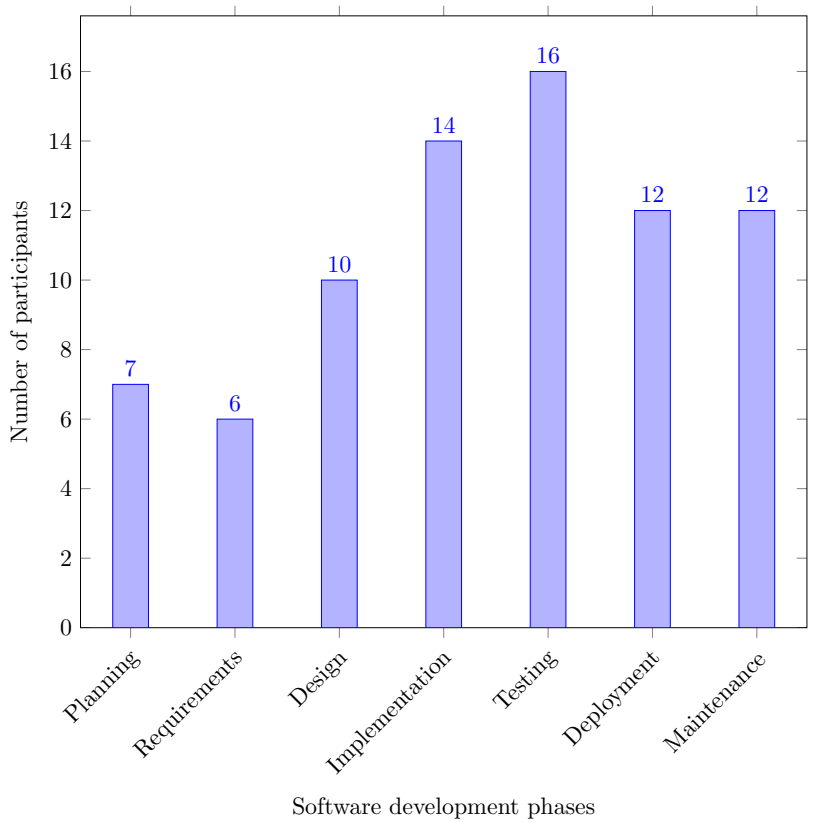

Figure 4.1: Distribution of software development phases participants work in

Professionals who participated in this survey have different experience in the IT industry. The following table 4.2 shows the distribution of years of experience within the IT field.

The results if the survey indicates the correlation between the amount of standards and guidelines used while performing the tasks and the yeas of experience in the field.

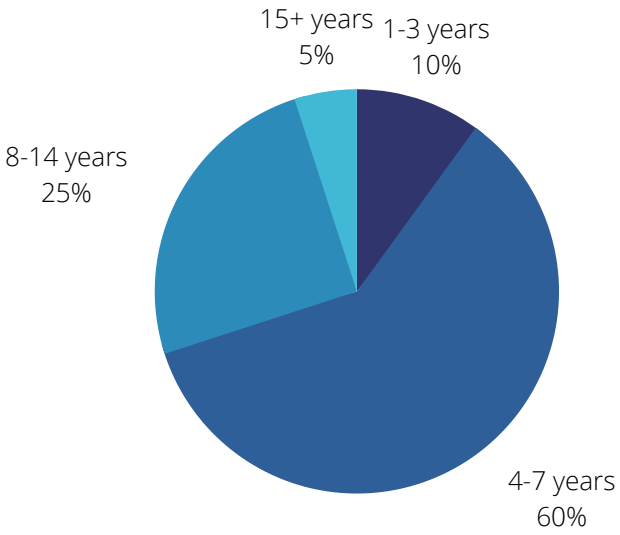

Figure 4.2: Work experience in the IT industry

One 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 4.3 shows the overall percentage of participant that have or have not heard of this term. According to the results, the participant working in the security field are more aware of the usable security than the participant unrelated to the security field.

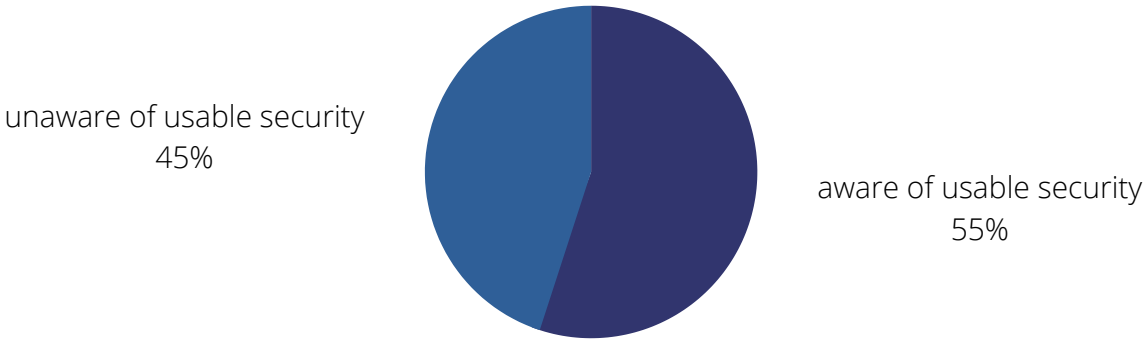

Figure 4.3: Awareness of the term usable security

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.

From only three participants using tools to increase usability, the tools mentioned only address specific areas of usable security. For example a guide to ensure usable security of web applications.

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. According to the results, the people who do not have methods in place to satisfy the usable security requirement work in almost all phases of software development cycle and are not focused on just one or two phases.

4.6 Applicability Evaluation of Existing Tools and Materials

The following chapter discusses the tools and materials listed by respondents during the survey. The main focus is given to the applicability evaluation of these tools and guidelines and determination if they can be used to reach better security and usability within the software development phase.

4.6.1 Tools and Materials According to the Respondents

COBIT

The first mentioned framework participant stated as the form of guideline they use is the framework Control Objectives for Information and Related Technology (COBIT) created by the international association ISACA for IT Governance [14].

It is a set of practices that should enable the achievement of the organization's strategic goals through the efficient use of available resources and the minimization of IT risks. The methodology is primarily intended for auditors and managers. The main advantages include a wide scope across the entire organization. The focus is not only on information and communications technology (ICT), but also on audits and controls. COBIT tends to create a comprehensive system of rules that can cover other systems, such as ITIL, TOGAF, ISO, and which will fit into the comprehensive framework of the methodology that covers them from a functional point of view.

From the usable security security perspective and the developers point of view, COBIT is not a framework that could be used by developers. As mentioned earlier, the framework is main target are the managers and auditors.

ISO/IEC Standards

Almost the third of the respondents stated that they use the ISO/IEC 2700x standards [26]. ISO 27001 Information Security Management Systems: ISO 27001 sets specific standards for information security for use by data centers and other organizations. One of the key parts of ISO 27001 is the introduction of controls and control objectives - an integral part of any risk management plan. These controls cover everything from human resources policy to encryption standards. In summary, they reflect a set of best practices for managing information security at the organizational level.

ISO/IEC 27001 is an international standard for the management of information security management systems (ISMS) but it is not focused on the users and developers in terms of providing them guidelines for usable security. The standard provide useful information that can help with ensuring the security of the system. However the document is very complex

and comprehensive and not really addressing the usability issues the developers often face. Moreover, these standards are not free and publicly available to all IT professionals.

OWASP Testing Guide

Many respondent work in the testing phase of the software development claimed to use the OWASP Testing Guide as their guideline to address security issues [18]. The purpose of this guide is to cover the most common security vulnerabilities that arise when developing web applications, as well as to show how to test those vulnerabilities. This guide, developed by the OWASP organization, has become a wiki, allowing people to contribute to its development and make it easier to update. It also contains components from other projects such as the OWASP Developers Guide and the Code Review Guide. The main focus is given to the guides addressing the issues of web application or mobile applications. The guides have a very good form and are easy to read. They offer real world examples of how the issues could be addressed.

The only downside of this guide is the narrower focus on web and mobile application and the guidelines are not offered for different areas of software development.

Burp Suite

The versatile Burp Suite is standard tool for every penetration tester [54]. This tool has also been mentioned by respondents working in the testing phase of the software development cycle. In addition to the basic functionality, which is to allow exploration and change of communication between the web browser and the server (local proxy), it also contains useful modules such as an intruder, (de)encoder or automatic vulnerability scanner. Burp Suite is very clear, working with it is intuitive and modularity allows its extension with other functionalities.

Overall Burp Suite serves the purpose to make the security more accessible to developer. The tool is considered as a very usable guide that satisfies many usability and security issues developers can face. However the scope of this tool is limited to web applications.

OSSTMM

The Open Source Security Testing Methodology Manual (OSSTMM), mentioned by two respondents, is a publicly available open-ended security testing methodology that tests so-called bottom-up security [24]. The methodology has become an international open standard.

The main purpose of this paper is to provide a scientific methodology for the accurate characterization of security through its positive and accurate testing. The manual can be adapted for most information system audits, penetration tests, ethical hacking, security and vulnerability assessments, or other security audits. And as a second, no less important sense of the manual, the author considers it as a kind of guideline or outline, which when the auditor follows, will achieve a certified OSSTMM audit.

According to the latest research this manual's methodology and principles is being criticized to not be a usable tool [5] because of the inability to guide the users.

MITRE ATT&CK

MITRE is a non-profit organization which has a to solve problems so that the digital information is more secure [53]. Among other things, we also use the knowledge database known

as MITRE ATT&CK (short for Adversarial Tactics, Techniques, and Common Knowledge). It is a platform that gathers and categorizes the different types of strategies, techniques, and procedures used by cyber-attackers. The platform helps companies find weaknesses in their own cyber defense.

4.7 Summary

This section summarizes the most important findings from the respondents answers about their awareness and tools they use to satisfy the security and usability requirements. The results of the survey showed that more that almost the half of the developers and IT professionals are not aware of the usable security. Only the half of the participant were able to define tools they use to ensure the security factor. The guidelines addressing the usability have not been discovered. According to the analysis of the tools, the only usable tools found were the OWASP Testing Guide and Burp Suite which are the tools used mostly for securing the web applications. They provide the user with an examples of how to avoid particular security or usability issued however and are easy to read. However they do not address the whole software development cycle.

The other previously described guidelines serves well for various security challenges, however there are reasons why the mentioned tools are not enough for the field of usable security such as, insufficient scope or they are not targeting the developers as the users of these guidelines. This opens space for an improvement. As the developers are not well aware of the challenges within the usable security, there is a need to providing them with the basic knowledge of the current issues and the steps guiding them to solve them. More about the requirements for educating the IT professionals and providing them with sufficient materials are discussed in next chapter.

Chapter 5

Analysis and Design of Educational Aid

The analysis in the previous chapter discussed the current state of IT professionals awareness together with the applicability of existing guidelines, tools or other materials they use in the field of usable security. A survey was conducted among professionals, where the aim was not only to find out their awareness but also to find out what methods, standards and tools they use for this purpose.

The main shortcomings include the absence of existing standards, the lack of research in this area and the inapplicability of existing guidelines. This part of the diploma thesis will deal with the solution of these shortcomings.

The evaluation of the survey highlighted the need to provide developers with basic guidelines on how to properly develop software with a respect to the usable security. The study confirmed that IT professionals do not have sufficient awareness of usable security or are aware of this area, but do not have the guidelines and tools to help them take into account development factors. Therefore, there is a need to make this area more accessible for newcomers.

Because of the results of the survey and the previously mentioned issues, it would be beneficial to educate the newcomers in the usable security field. As there are no existing standards and official guidelines that could educate them on how to work correctly in terms of security and usability. However, the developers could be educated by raising their awareness in current challenges within this field. The main focus of the proposed tool is provide them the information about such challenges and make the educational process understandable and concise.

The tool aims to increase the awareness of people coming to the field of IT. The theoretical research has identified interesting areas in terms of applicable security. The areas that are a part of the newly proposed challenges are selected on the basis of the largest number of studies found in the given areas as these areas represent the biggest challenges within this field. The following section describes the use cases serving to address these requirements.

5.1 Application Use Cases

In order to address the requirements for the application, the following use cases needs to be provided to the community of people working in the software development. The main use

case of the developed tool is obvious the user visits the page, chooses the area in which he or she wants to learn, clicks on the end node of the mental map, reads about selected area of usable security and then take a quiz. Another use cases are described in following list.

- Before the first use of the application, the user need to register. After filling the register form and providing information such as username, e-mail and password, the profile is created and the newly created user can sign in with created username and password.
- After the first log in, the new user can undertake the initial preliminary quiz in order to determine the initial awareness in the area. The application contains two groups of the quizzes. The first group are the preliminary quizzes serving the user to determine the current general awareness in the field of usable security. And the second group of quizzes are associated with particular challenge defined within the application.
- The users can read challenges and go through the selected areas of usable security. Each challenge provides the user the overview of the topic, the consequences of ignoring the usability, case study and following principles, standards or guidelines.
- To enhance the educational process, each challenge provide the link to associated quiz which can be taken after reading about the challenge. However, the list of all quizzes can be viewed by clicking on the menu tab `Quizzes`.
- Another use case is to list all the challenges within the application by click on the tab `Challenges` in the menu. The challenges can be then filtered by inserting the keyword in the search field.
- The home page is used to visualize the selected areas of usable security and to help the user see the connections between the areas. Moreover, the usability is enhances by enabling the user to click on the end nodes of the map and redirecting them to specific set of challenges.

5.2 User Interface design

When designing the user interface, it is necessary to take into account the most important aspect of application development, namely the intuitive, simple and clear control, which How does this tool want to differentiate itself from the current possibilities of education dealing with the same issues. From the learner's point of view, the application will be divided into 4 thematic units: Homepage, Guidelines, Quizzes and About. Links to these units will form the application menu. They are described in more detail in the following subsections.

Homepage

The initial page that the user will see the map of selected challenges within the usable security area. The challenges are structured within the mind map. A mind map is a graphical arrangement of words, concepts, and images that allows the user to mark and identify dependencies and connections that are often not completely obvious at first glance. The map serves for easy orientation in the offered areas of education. Each end node in the map contains a link to a specific guideline, which is linked with the label of the end node.

After a user logs in, the menu on the homepage displays one more element, which is a link to quizzes and a user's profile.

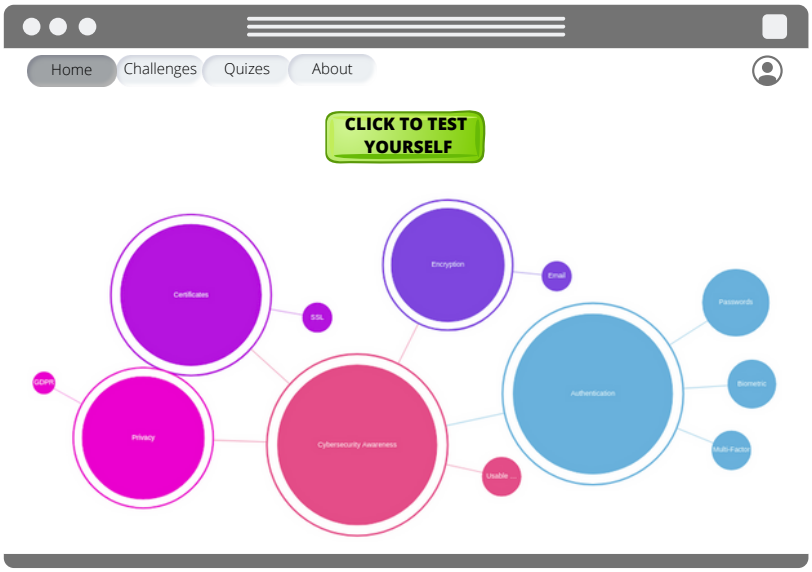

Figure 5.1: Homepage Design

Profile

The profile page provides the user with basic functionalities for managing the user account. The user is able to change the password, change name or password. Moreover the profile page presents the user with the results of quizzes done by currently logged in user. This keeps the user aware about the improvements he or she did. The results assigned to concrete user and concrete quiz.

Challenges

The main part of the application in terms of educating IT professionals is the page that presents the current challenges in the field of usable security. The main objective is to provide information about selected areas about which the IT professionals should be aware. Each challenge provide the overview of the problem, research or area. After that, when the reader is aware of the background of the topic, the application provide the information about possible consequences which should define the reason why it is important to gain awareness about the problem. Followingly, the user can read about case study which should represent a study or a research in this area and its outcome. After reading a case study the reader should be aware of the usability issue within selected area. Each challenge includes a standards, guidelines or principles existing for chosen area. At the end of the challenge, the user can find relevant references to research, standard or other materials used to create the challenge.

In order to make the challenges easy to read, the goal is to make them concise. The brief and comprehensive information should provide the reader the basis to take a quiz in order to test gained knowledge.

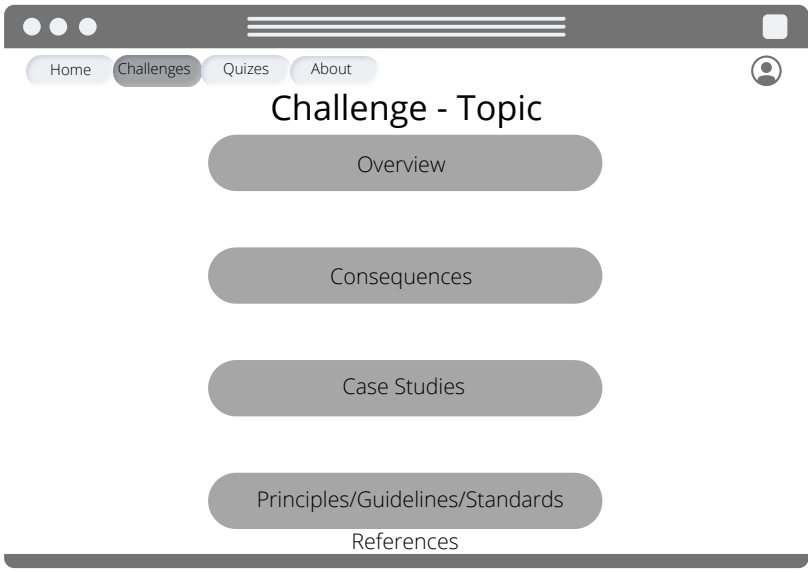

Figure 5.2: Design of the Challenge

Quizzes

As one of the goals of the thesis is to provide the IT professionals with educational aid, the application is design the way their users can evaluate gained awareness by taking the quiz. As mentioned before, each challenges is connected with particular quiz, which asks the user questions about currently gained knowledge.

The user can be redirected to the quiz page in two ways. The first way is to click on the link on the challenge page after reading the challenge content. However, even when not recommended, it is possible to list all the quizzes and take any of the quizzes any time. The quiz contains question related to the challenge, that is why it is recommended to do the quiz after the reading. After submitting the questionnaire, the user receives the feedback for each of the questions. The feedback includes the information about answer given by the user and correct answer, that should have been selected.

Preliminary Quizzes

The application offers five preliminary quizzes which are not related no any concrete usable security challenge. However the questions are designed to address the usability factors in software development. The first quiz address the overall usable security awareness of the participant. This quiz consists of 6 questions with one correct answer per question. After submitting the quiz, the user receives the feedback which answers were correct or not. In case of incorrect answer, the explanation of correct choice is provided. The next two quizzes are focused on the design and evaluation phase of the software development. The last preliminary quiz asks about the usable security principles and guidelines.

About

The about page consists of be a welcome text and a short description of the applications' functionalities. By reading the provided information the user gains knowledge of how to use the application and how the educational process is designed.

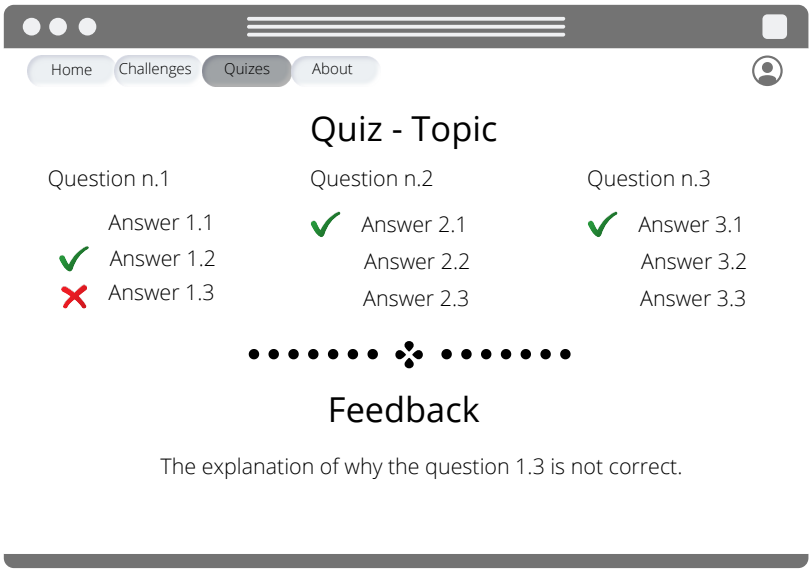

Figure 5.3: Design of the Quiz

Moreover, the page provides information about the master project, its objectives and link to publically available code. A part of the page is also the information about the research paper connected to this thesis and link to the publication.

5.3 Application requirements

Usable security requires effort beyond the design of user-friendly interfaces to secure tools [44]. As users behaviour has a big impact on organisational assets, users, including designers and developers, need the education. This part of the work deals with the design of an educational tool for IT professionals, which will help raise their awareness and thus ensure more secure software development. The goal is to raise the awareness of newcomers to the IT field and educate them about important factors in usable security. The proposed educational aid aims to educate the user about selected important areas which according to the research presents the biggest security risk. The person who devotes time and familiarity with the tool should be able to understand the selected areas within this field.

As mentioned in the research section, there are really many solutions to the problem of creating tests. However, there is no free tool that would provide the basis for studying the usable security with quizzes that are based on the selected areas, the users of this application studies. Furthermore, it is desirable that the application is capable to organize the wide area of usable security thematic units and keep everything in one place. The target group of the proposed application should be mostly newcomers to he IT but also people who works in the IT field and have no awareness about provided content. The core elements for improving the users' awareness are shown on the figure 5.4.

5.3.1 Functional Requirements

Some of the above requirements are more detailed in the following sections. In the following subsections, the entire software system is designed in detail. The result then serves as a basis for implementation phase.

Figure 5.4: Core elements for improving users' awareness

Providing basic Information about the System

The system should provide a basic and comprehensive overview of information about reporting and the application itself. This report should be available to everyone, regardless of registration and authentication.

Registration in the System

Within the application the user should be able to easily register in the system. The user must fill it out information such as name, email and password. These information of identity is then used to correlate the results from the quizzes with specific user.

Authentication

The system will allow two types of access control. You are not required to log in to the system when viewing selected areas used for education. Passing quizzes, questionnaires and the rating, however, is tied to the identity of the user. To enter this part of the system, it is essential to perform user authentication.

Access to the System by Username and Password

Logging in to the system should be performed exclusively by e-mail and password. This ensures that the access data is unique and easy to remember. This prevents the possibility of two accounts with the same login details.

Update of User Data

The user should be able to update personal data and access them in the system at any time.

User roles within the Application

The user after registration should be automatically assigned a user role in the system, which may be changed only by the administrator. Each role has certain rights and restrictions in the system.

User Rights

The user will have certain rights and permissions in the system with regard to the user role. Users can only work with their records, while the administrator has access to all records.

Creation of new Challenges and quizzes

This is the basic functionality of the entire application. The administrator will be able to create challenges and quizzes. In contrast, an ordinary user should be only allowed to read the challenges and see quizzes in order to evaluate gained awareness, however, the user have no right for editing the content.

Provide quizzes to Allow Users to Test Their Gained Knowledge

The system should provide quizzes for all selected areas according to the provided guidelines. During the learning, there is a need for self-testing, i.e. the need to test themselves from the material they have just read. As a result of this need, the proposed tool should not only provide the guideline but also validate the impact of reading the guideline. The most fundamental requirements for that application are therefore:

Provide the User the Feedback from Each Quiz

After taking the quiz, the user should be provided with the feedback. The user should be aware of which answers were answered correctly and in case the user made a mistake, the feedback should include an information about what was the correct answer.

Quiz Results Evaluation

The user should be allowed to view the evaluation of the quiz attempts related to his or her identity. The evaluation shows all the results of the quizzes the user took in the order in which they were taken. According to this view, the user is able to see the improvement in his or her skills.

About the Application

The user should provided with the information of the application usage. The about page should guide users to properly work with the application, including the schema of the challenges and the purpose of the quizzes and the feedback they provide.

Accessibility of the Application

Given the target group the last application's requirement is a price. The proposed application should therefore be available for free for all users that are willing to raise their usable security awareness.

Chapter 6

Selected Challenges for Educational Aid

6.1 The Importance of Developer Training

The training of the developers is considered the foundation of secure software development. Thanks to continuous education, developers know all aspects of creating secure code and know that there are high demands on the development of secure products.

6.2 SSL Error Codes

Overview

Secure Socket Layer (SSL) is a common protocol to encrypt data in transit. Unfortunately, developers have difficulty using these protocols correctly. This usable security challenge demonstrates broken validation of SSL certificates. The root cause of this challenge are the API of SSL implementations, which confuses developers with insufficient error messages.

Providing guidelines for usable and secure digital certificates is tremendously important. Without digital certificates, a user has no basis to determine if the website is trustworthy or not. This guideline will provide the information about the problem of error codes in cryptographic API.

Consequences

- Untrustworthy CA issuing certificates may result in man in the middle attack.
- Ignoring untrustworthy certificate may lead to data information disclosure.
- Ignoring critical extensions that cannot be processed may result in unauthorized use of the certificate.

According to [47] there are several risks included:

- application outages caused by expired TLS server certificates
- hidden intrusion, exfiltration, disclosure of sensitive data, or other attacks resulting from encrypted threats or server impersonation

- application outages or attacks resulting from delayed replacement of large numbers of certificates and private keys in response to either certificate authority compromise or discovery of vulnerabilities in cryptographic algorithms or libraries

Case Study

Securing the network traffic using SSL is a complex task that might be difficult for developers who are not security oriented [57]. This initiated the creation of APIs that encapsulate the underlying complexity of this protocol and are easier to understand and implement, eg. OpenSSL, JSSE or GnuTLS [51].

When the user access a web page, it is usually possible to see the lock symbol and the SSL certificate [57].

This can be seen when everything is as it should be. However, when there is a problem with the SSL, the user sees following error:

From the user's perspective, the message can be good enough to be understood as it tries to explain in simple terms where the problem is. It also includes an advanced error code, that can help the developer to find out more about the error.

The problem occurs when the developer wants to validate the certificate. Usually following command would be used:

```
openssl verify certificate.pem
```

What the developer now sees is the error 34 with text „unhandled critical exception". According to the [57] the developers often have no idea of this error's meaning and start to google the term „ssl unhandled critical extension".

Figure 6.1: Insufficient documentation of SSL API

Recommendations

1. The risk should be presented clearly together with the consequences of acceptance of not being compliant [9].

2. The steps defining how to avoid the risk should be presented.

3. Provide the explanation of the warning as well as the explanation of the potentially wrong decision users are about to make. The amount of information provided to the users should empower them to make the right decision.

Special publication 1800-16 by NIST proposed TLS Server Certificate Management [47]. The research paper by Martin Ukrop and Lydia Kraus outlined a methodology for collecting a comprehensive data set of web browser security indicators and warnings [31].

6.3 Design of Privacy Notices

Overview

Signing up to new services requires users to provide private information. This situation is controlled by the EU General Data Protection Regulation(GDPR) [1]. According to the regulations organizations providing services must provide the user with adequate information and receive the consent from the user. The recent research shows only little change in the visualization of privacy notices about data handling.

Case Study

An exploratory study examined the current state of current design notices [30]. The focus has been given to human decision to agree or disagree with the terms.

Total of 88 participants were part of this study. The results show that people often feel like they do not have a choice and must agree with privacy policies. The participants lack the control when making the decision whether to agree or not.

Further research showed the connection between the notice's design and the effect on people's decision. In the second study, 36 participants faced 16 different pictures and had to define their feelings associated with the illustrations. The images were both positive and negative examples of privacy notices. The study defined which examples are human-positive.

The third study associated with this topic consisted of multiple steps. At first the participant filled an entry questionnaire, then performed interactive tasks, and again filled the questionnaire. The results of this research states that the current controls implemented in privacy notices lack the usability because of inconsistent design. The amount of needed clicks performed by the user or mandatory redirects often lower the usability.

Consequences

Privacy breaches may result in personal information disclosure and data collection. Users are concerned about their online information and how they lack control over its use.

Principles

1. The visual design of privacy notices influence the user's affective state.
2. People may feel more satisfied when they feel they are provided with control.
3. Users feeling about control can be increased with the design of the privacy notice.
4. Curiosity positively influences privacy comprehension.
5. Users should be provided with options to set individual preferences. Users should be allowed to make possible adjustments.

6.4 User's Awareness about Ransomware

Overview

Ransomware restricts users' access to their computer system or files. The program requires a ransom fee to restore access. The random is typically cryptocurrency payment. This type

of attack receives a lot of attention. A recent research carried out a survey on how users perceive risks and react to these kinds of attacks [45].

Consequence

Infection by a ransomware creates a risk of complete data loss or high financial costs for decrypting files.

Case Study

The classical paradigm to reaction to malware is defense-focused and reactive [45]. A recent research examined the user's reaction to ransomware. The respondents were provided the information about how the typical ransomware acts like, together with its basic characteristics.

During the study the respondents faced the situation when they were attacked by ransomware. Total of 1 180 participants were part of this study from which 14 percent of them reported that they faced ransomware in the past. The responses of the victims were independently reviewed and categorized under two regimes: a conservative or inclusive. The inclusive category includes the responded where based on the description it was possible to determine whether the attack has been ransomware. On the other hand in the conservative regime the respondents have not provided enough information for determination whether the attack has been ransomware.

The overall result of the study shows the importance between online behaviours or user's cybersecurity awareness with making better security decisions.

6.5 Users' Attitude towards Re-authentication

Overview

Reauthentication is the process of confirmation of a user's identity. It aims to determine whether the user who is currently accessing a particular resource is the same person as at the first authentication procedure. The process of re-authentication is often considered annoying by many users.

Consequence

The longer the user is authenticated without re-authentication the higher the risk of the attacker getting hold of the device within this time frame.

Case Study

Devices such as smartphones, which are commonly used nowadays enable users to access sensitive data directly on the device or in the cloud [34]. The use of these devices is based on explicit authentication methods, e.g. lock patterns, passwords, PINs or different biometric information.

Recent research examined the users' attitude to re-authentication methods. The reason for the users' annoyance mostly consisted of the unpredictability of re-authentication and the following interruption. The factor of negative users' attitude is also the lack of information about the current state of authentication and no control about the timing of the mandatory confirmation of the identity.

The research addresses this issue with a proposed long term indicator which serves as an informator of the current state of authentication for users along with the device confidence level which serves as an indicator of the timing for next re-authentication. These indicators allow the users to have the awareness of the current state and let them perform their tasks without being interrupted.

Moreover, the research proposed the voluntary re-authentication process which reduces the annoyance of the users.

6.6 Phishing Awareness and Education over Time

Overview

Perhaps all security experts agree that users are currently the weakest link in an organization's information security. This is not only because users generally do not like to read the guidelines and therefore do not follow their regulations, but also because they often like to experiment and thus commit a number of fundamental safety offenses. So how to effectively arrange for users to know and act on security rules? By constantly and consistently instilling basic safety rules and work habits.

Consequences

A person who designs, manages or uses information systems represents a vulnerability present in every information system. In cases where the organization's information systems are technically well secured, it is most worthwhile for a potential attacker to try to exploit the vulnerability in the form of a human. He has several options for that. Even some of them do not even require any technical skills. Examples include social engineering or espionage. Other threats arising from a lack of security awareness are a poor knowledge of the organization's rules and their intentional or unintentional violation. These include, for example, human error, unauthorized use of information systems, unsafe use of the Internet and e-mail, carelessness in handling information or improper administration of information systems.

Case study

A very recent study examined education programmes for security awareness [40]. The focus has been given to effectiveness over time and the determination of appropriate time interval between education. The study has been performed in an organisation of 409 employees.

The first research question examined the time period of the lasting effect of awareness after the on-site tutorial. The results showed that the difference of users' awareness before the on-site tutorial and 6 months was not so significant.

The second research question determined the most suitable measure serving as a reminder for participants to distinguish between phishing email and legitimate one. The study examined the impact of measures in form of text, video or interactive examples. The interactivity factor had better results, however only with slight difference to the effect of videos.

The third research question examined the time period of the effect of the reminder measures. Based on the result from the second question, the experiment serving to address this question excluded the text measures. Users were able to determine whether they receive a legitimate or phishing email after the period of 6 months

6.7 Password Managers

Overview

The password manager can help with memorization. It is a special program created to generate strong passwords by auctioning login details to an encrypted digital safe. It usually also offers browser extensions, which allow you to automatically fill in login forms after logging in to the administrator. The only thing a user needs to remember as a user is one master password. The password managers can differ. The following are two examples of password managers:

- Browser extensions, a key feature of the best password managers, is browser extensions. This is software that adds additional features to your browser. It makes it easier for you to use the Internet and at the same time protects your login details.
- Many of us log in to our accounts through applications, but many password managers only support web login. The better password managers also offer password management for applications.

The recent research highlights the need for increasing the usability of the design of these tools. Users from non technical backgrounds encounter even more issues connected with password managers.

Consequence

If password managers are not designed with needed usability factors, users might circumvent these inconveniences and use different less secure methods instead.

Case Study

Password managers are affected by several usability issues [38]. One of the issues is caused by the incorrect or incomplete mental models. Users are often unsure whether the system has correctly been activated. Users' understanding of the interaction with the system can be incorrect or incomplete.

A recent study explored factors in the adoption of password managers. The aims were to determine the effectiveness of their usage. A total of 30 interviews have been conducted, from which nine users worked in technical fields. The results of the interviews revealed that many users have very complex password strategies and several methods for password storage. The outcome of the study identified barriers such as users' confusion about the meaning of "remember me" option and the confusion about the source of password prompts.

6.8 API Blindspots

Overview

When it comes to security, developers often use Application Programming Interface (API) for cryptography. This interface provides them with easier access to the cryptography functions without having to access the raw data. The API can be easily misused or misunderstood which can result in an increase of security risk.

Case Study

A recent study examined the developers' ability to solve programming puzzles [36]. Each of the puzzles (code snippets) contained a code from Java APIs and simulated real world scenarios. These real-world related puzzles were designed in two types, with and without blindspots. The first type, with the blindspot, targeted one particular function of Java API, which is known to make the security implications to be understood by developers. The other type included the code which strictly follows the code security guidelines.

```
1  // OMITTED: Import whatever is needed
2  public final class SystemUtils {
3    public static boolean setDate (String date)
4        throws Exception {
5      return run("DATE " + date);
6    }
7
8    private static boolean run (String cmd)
9        throws Exception {
10     Process process = Runtime.getRuntime().
       exec("CMD /C " + cmd);
11     int exit = process.waitFor();
12
13     if (exit == 0)
14       return true;
15     else
16       return false;
17   }
18 }
```

Figure 6.2: Puzzle with Blindspot

The figure 6.2 above shows one of the puzzles with the blindspot. The developers were asked above the effect of calling the function *setDate()*. They had to choose between 5 statements and choose the correct one.

The first statement claims that if the function *setData()* is not given String value, an exception is raised. Another statement to choose claimed that return value from the function *waitFor()* is not well interpreted. One option declares that the application would crash after running this code.The last two options lay claims to the impact of function *setDate()* to not be able to change the date or be able to change the date and even do more than that.

The correct answer is the last one, correct inspection of the given code shows another method to be executed on line 10. Invoking the method with the argument *"10-12-2015 && shutdown /s"* would turn off the server. This defines the blindspot of the API and highlights the need for proper sanitization of the method. The study outcome indicates that the code snippets with blindspots have impact on the developers' ability to solve the puzzle.

Chapter 7

Implementation of the Educational Aid

This chapter deals with the actual implementation of the web application. It explains the technologies used, tools and principles that were used in creating the application. At the end of the chapter are real examples of using the system.

7.1 Choice of Technologies

Currently, the fastest and easiest way to create a new web application is to use an existing framework. The framework is a software structure that is used to support the creation of systems.

It can contain programs, libraries, design patterns, or best practices. The main goal of the framework is to facilitate and speed up the work of system development, as they often solve typical problems in the given area and developers can thus fully focus only on solving their task. The application logic of the system is created using the Python programming language together with the use of the Django framework and the MySQL database. Interactivity in the system is achieved using Javascript and jQuery. HTML5, CSS and Bootstrap take care of the design page of the application. Bootstrap also ensures system responsiveness.

7.1.1 Django

Django, a web framework written in Python, builds on the principles of maximum productivity and reusability. At its core, the Django application framework is simply a collection of libraries written in the Python programming language. Django loosely follows the MVC (Model-View-Controller) design pattern, but uses its own implementation logic.

The controller component is provided by the Django core itself, and most things are done in models, templates, and views, which is why Django is often referred to as the MTV application framework. MTV is described in as:

- M as Model - It is a representation of the data layer, so it contains everything related to the data itself. It consists of the base class Model, which provides automatic data conversion between the data model and the relational database. This technique is called object-relational mapping(ORM).

- T as Template - The template forms a presentation layer, it is a string of text whose the purpose is to separate the appearance of the document from the data itself. Templates define tags that determine how data is displayed to users.
- V as View - View covers the application layer, it is a connecting element between models and templates. Basically, these are functions that process HTTP1 requests and return an HTTP response.

Django follows a so-called „Don't repeat yourself" (DRY) principle. This means that each concept or piece of code should never appear more than once, so the emphasis is on code reproducibility. We can notice this, for example, on the modular system in Django. Each application built within Django is composed of several modules, which are called as applications in Django. Each application has its own interface and can be used across projects.

7.2 Modules

The implemented application consists of multiple modules. Each module is represents a logical entity of the application. This section aims to describe the details of each of the modules.

7.2.1 Challenges

The model of challenge consists of multiple attributes. The first attribute is the admin user, the author that created challenge. It also includes the title, topic, date of creation the challenge and the overview. To connect challenge with another associated models such as risks, case studies, principles and references, the associated models are related to the challenge with foreign keys. This creates 1 to multiple association between the challenge and mentioned models. Each challenge can be added, updated and deleted through the admin console. Moreover, the challenge can be visualised, added, updated and deleted within the application where each of these action has separate URL. While listing the challenges is a part of typical use case, the parameter `?q=query` has been implemented and serves to filter the result of the search of the challenges based on their title, or content of associated content within.

7.2.2 Quizzes

The quiz model is made up of the text fields name and the topic, number of questions and approximate time needed to finish the quiz. Another attribute is the required score to pass which serves as the threshold for passing or failing the quiz. The last attributes are the difficulty of the quiz and the foreign key defining the association with the challenge. The quizzes are accessible through general view where the user can list all quizzes or view the particular quiz with associated questions and answers. Before starting the quiz, the application provides the user with all attribute of the quiz in a modal windows and asks for validation to proceed to the quiz.

7.2.3 Questions

A quiz question consists of multiple answers, which are represented by the text fields. Each answer has attribute defining if the answer is correct or incorrect. Each answer has to be

associated with a specific question. Adding new questions does not have separate interface as it is done by admin on admin view and the admin stores the data into database file that is accessible for deployment. The question in quiz contains text data defining the actual question and the date of creation.

7.2.4 Results

The logged in users store their scores they reached on particular quizzes. This is done along connection between the user and associated quiz. The results consists of the obtained score, the user who took the quiz, and the name of the quiz taken. The results are listed in user profile view scaled from the most recent result to th oldest.

7.2.5 Users

The user profile is made up of `User` authentication model that is inherited from Django models. Each user can upload a custom profile image or the default picture is automatically assigned.

This module contains signal dispatchers which helps to allow decoupled applications get notified when actions occur elsewhere in the framework. Namely the creation and saving of the profile.

Newcomer on the website is able to register for free. The views contains the register form which represents the process of singing up and profile view, where the user is able to adjust personal information.

7.2.6 Third Party Packages

As the Django is third party framework it is part of the third party packages for python. These packages are stored in `requirements.txt` file. This file also contains dependent packages for Django but others that is the website using. Namely Django extensions like crispy forms, widget tweaks and Heroku, which is used for deployment purposes. As next package required by the Django framework is whitenoise package that simplifies the static file serving during deployment[1]. The last non prerequisite package but used also for deployment is gunicorn package that serves as WSGI HTTP server for Unix[2]. So the application can be either directly executed through `manage.py` script or indirectly using gunicorn services connected with `nginx` server[3].

7.3 Deployment

In order to be able to further evaluation of the application's impact on IT professionals awareness, the implemented application was deployed as public service. For such a purpose Heroku application was used. It is cloud based service that offers deployment of Github repositories with hooks or deployment using third party versioning systems through command line interface [49]. Deployed application is connected with Heroku database, where information are stored and retrieved. No further setup is needed and the application do not need to specify external entities that are connected. The deployment of Django applications has to follow official guideline where prerequisites are defined in `requirements.txt`

[1] `http://whitenoise.evans.io/en/stable/`
[2] `https://gunicorn.org/`
[3] `http://nginx.org/en/`

file. The file contains packages that have to be installed before deployment of the application. Another necessary prerequisite is the `Procfile` file which specifies steps needed to be performed in order to launch web service.

To have a consistent state of the database before deployment the data is stored in the `database.json` file that represents all the Django database models that are related with previously mentioned challenges, quizzes, case studies and others. The file contains created test user, described in more details in next chapter, serving for further evaluation of the application.

In order to perform a single deployment of an application through Heroku, the following commands need to be executed:

```
git push heroku <name-of-branch>
heroku pg:reset DATABASE
heroku run bash
// Now the user is remotely connected to Heroku
python manage.py migrate
python manage.py loaddata database.json
```

First command pushes all the changes to Heroku specified branch name. This branch is going to be deployed. However as the database could change it has to be reset with a second command. Next three commands perform initialization of the Heroku Postgre SQL database and load prepared data [50, 49]. The deployed application is available on [4].

7.3.1 Deployment Limitations

As the application' purpose is to educate and raise awareness in a usable security field it has to follow the rules of being secure itself. However the deployment runs in debug regime because of an ongoing issue in the *whitenoise framework* that is used by Django[5]. It is not a good security practice but for demonstrational purposes the application was deployed as follows to let users evaluate it.

[4] `https://edussec.herokuapp.com`
[5] `https://github.com/evansd/whitenoise/issues/274`

Chapter 8

Impact Evaluation of the Created Educational Aid

This chapter aims to evaluate the implemented education aid's impact on the IT professional's awareness. The impact on people working in the software development was measured by conducting a survey with a goal of receiving qualitative data. Unlike the first research which was conducted as an online questionnaire with a total of 20 participants, this survey aims to target smaller group of developers and interview them about their experience with the implemented tool. The evaluation process was performed in following steps:

1. The users were asked to take the one or more preliminary quizzes in order to determine the current state of their knowledge. One specific preliminary quiz was mandatory and the rest could be voluntarily taken.
2. The participants were guided to read about selected challenges and take the associated quizzes.
3. After completing previous steps, users were requested to fill the questionnaire which included questions about the application user interface.
4. A short interview was conducted in order to receive the qualitative feedback.

The methodology for the impact evaluations has multiple objectives. The first objective is to determine the level of current awareness of the participant. The result of the preliminary quiz can help the users identify the gaps in their knowledge. Based on the score, the participant are divided into two groups, the ones who passed the the preliminary quiz (GP) and the ones who failed (GF). The threshold defining the passing for the preliminary quizzes is the half of the possibly obtained points. In the second step of the evaluation process, the differences between the two groups are observed.

8.1 Participants

The chosen participant are a subset of participants selected for previous study. As this study is more based on qualitative feedback, the number of respondents is lower. A total of 6 IT professionals participated in the evaluation of the educational aid. For this purpose, six test user accounts were created to be able to access and collect their results of the

quizzes directly from the application database and to be able to match the particular quiz to particular person. Each participant was given username and password and the previously specified tasks. The time limit for each step has not been specified, however the maximum time for the whole test has been set to one hour including the interview at the end of the test. As the educational aid aims to serve the newcomers in the field of usable security, the participants chosen to the evaluation of application's impact have experience in IT in the scale from 1 to 3 years.

8.2 Preliminary Quiz

The application offers five preliminary quizzes, however only one has been defined as mandatory during the study. The selected quiz asks the participants about the usable security principles and guidelines. The aim is to determine whether the participant are aware of the usable security and whether, when facing the security decision, they consider also usability factor.

The selected quiz consists of 10 questions and asks about the basics of usable security. They deal with the principles of the visibility of system's security state, warnings, users' access to resource, granting authority, security decisions and the balance of usability and security. The application collects the overall score of the users for each quiz. The results of test users has been collected for this particular quiz. Some of the participants took the same quiz multiple times. In this case, only the fist attempt has been taken into account. The figure 8.1 shows the distribution of reached score in the quiz with a name *Usable Security Guidelines*.

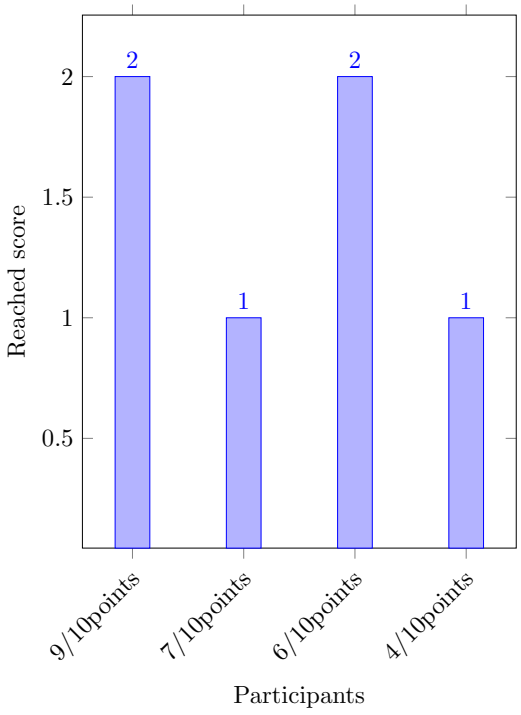

Figure 8.1: The distribution of reached score in preliminary quiz

8.3 Educational process

During the second step, participants were asked to read about selected areas and take the quizzes afterwards. In total, they were asked to read about 4 challenges, from which three of them were oriented on the developers and one of them was more concretely oriented on re-authentication. The following is the specified order of steps they received:

1. Follow the list of given challenges.
2. Read the challenge.
3. Take the quiz.

In order to make the evaluation more accurate, the users received a specific selection of challenges for this task. This helps with the differences in difficulty levels in provided content. The selection of challenges has been defined as follows. The first challenge taken aimed to educate the participant about the usability issues related to SSL validation errors. The second area was the re-authentication challenge, after that the participant learnt about blindspots in API and as the last challenge participants could raise their awareness about usability issues within static analysis tools.

The order of the challenges has not been defined. The important factor for evaluation was the existence of the score of each participant for the same quiz. The table 8.1 shows the distribution of obtained scores in each of the 4 quizzes related to 4 challenges for each test user.

User	Group	SSL errors	Re-authentication	API blind-posts	SAT usabil-ity
testUser1	GP	4/4	3/4	4/4	4/4
testUser2	GF	4/4	4/4	4/4	3/4
testUser3	GP	4/4	3/4	4/4	4/4
testUser4	GP	4/4	3/4	4/4	4/4
testUser5	GF	3/4	2/4	3/4	3/4
testUser6	GP	4/4	3/4	4/4	3/4
Results					
max		24	24	24	24
total		23	18	23	21
in %		95.8%	75%	95.8%	87.5%

Table 8.1: A distribution of the score participants gained during evaluation

8.3.1 Results

The most of the feedback of the participants has been collected through the interview after completing previous steps. The test users were asked about readability, understandability and overall feelings from the application. At the beginning of the interview, the users were requested to fill the questionnaire rating the application's user interface. The median of the overall rating can be seen on the table 8.2

The questionnaire has been filled during the interview session in order to receive more detailed feedback of what are the downsides and the upsides affecting the usability of the interface. A half of the participants were not fully satisfied with the quality of the

Question	Very Satisfied	Satisfied	Neutral	Not Satisfied	Unsatisfied
Considering your complete knowledge and experience about users' interface, how likely would you be to recommend a friend or colleague?		x			
How satisfied are you with quality of application?			x		
How satisfied are you with features of the application?		x			
How satisfied are you with challenges, it's description and design?		x			
How satisfied are you with application overall?		x			
How satisfied are you with difficulty of reading challenges?	x				

Table 8.2: Median of the evaluation of the application

application. The factor that has been most often pointed out was the inability to understand the connections visualized in the mind map.

During the interview, the participants were asked about the form of the challenge. If the amount of information provided was acceptable without arousing annoyance. One of the participants claimed that the provided challenges include insufficient amount of information for the reader. However, the majority rated the concise and briefly provided information as sufficient and enough to understand the given problem.

According to the table 8.1 there is not a big difference between the group GP and GF. Participant from both groups were able to pass the quizzes after reading about particular challenge.

According to the final interview, two of the participants stated that they had a problem to understand the key information in given challenge. However, they still declare to be positively impacted using the application. More than a half claimed a increase of their awareness in selected areas.

Overall the participants stated that the educational aid had positive impact on their awareness. One of the participant stated that the information provided are not needed to successfully complete his work tasks. On the other hand, he considers the educational aid as the good source of information for the ones who faces these challenges in their work.

Chapter 9

Conclusion

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 number of research focusing on the end users has been done in recent years. Examined 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. This survey has been designed in accordance to results of theoretical research. The main focus is given to examination of the current awareness of IT professionals and their knowledge of current standards, guidelines or methods. In total of 20 respondents participated in the study and were from different fields of IT. More than a half of participant were from the security sector.

Obtained results of the survey were further analysed. The outcome of the survey provided the information about the existing guidelines and standards used by IT professionals. Overall results showed that half of the participants were not even aware of the term usable security and less than a half of the participant claimed to use any standards or guidelines in terms of usable security. The evaluation of these guidelines, standards and other materials shows the insufficiency in applicability. The only standards the participants mentioned are the ISO/IEC Standards 2700x, which is focused on defining the controls for Information Security Management System(ISMS). The guidelines, the participant stated they use, are focused on specific area of IT. For example OWASP Testing Guide guides the developers to test the vulnerabilities in their web applications. The outcome of the analysis provides the possible modifications for their improvement, namely including more case studies or real world examples. Other materials may be too complex and difficult to read.

According the the analysis of the previous study it was possible to define the requirements for the educational aid. The proposed software is a web application aiming to increase users' awareness by reading about selected areas within usable security and com-

pleting quizzes. The purpose of the proposed application is to help the newcomers and make the area of usable security more accessible. The focus is given to specific areas such as issues within re-authentication, the lack of usability in privacy notices or misuse of cryptographic APIs. Selected are areas, where the lack of usability can result in an huge increase of security risk.

The impact of the implemented software was evaluated by conducting a user study, where the participants were people working in software development. The aim of the study was to determine whether there is an impact on participants' usable security awareness. The methodology of the evaluation of the impact was defined as follows. The participants were asked to fill the preliminary quiz in order to determine their current state of awareness in the field. Then, the participant were guided to read about four selected challenges and take quizzes associated with them. At the end of the study, the participant were asked to fill the survey rating the user interface of implemented educational aid and participate in short interview. During the interview, they were asked about the overall feelings from the educational process, the conciseness of the provided guidelines and overall impact on their awareness. The results showed that the education aid helped the participants to understand selected challenges within the field of usable security. The tool was considered to speed up the process of gaining awareness of the usable security solutions and knowledge of how to do it. Therefore, the creation of the education aid served to the people working in software development to achieve the previously mentioned goal.

This work has been presented on the conference ExcelFIT and the research paper addressing the first part of this thesis has been published. The implemented application is fully deployed and publicly available.

Bibliography

[1] *2018 reform of EU data protection rules*. Available at: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf.

[2] Abran, A., Khelifi, A., Suryn, W. and Seffah, A. Usability Meanings and Interpretations in ISO Standards. *Software Quality Journal*. november 2003, vol. 11, p. 325–338. DOI: 10.1023/A:1025869312943.

[3] Acar, Y., Fahl, S. and Mazurek, M. L. You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users. In: *2016 IEEE Cybersecurity Development (SecDev)*. 2016, p. 3–8. DOI: 10.1109/SecDev.2016.013.

[4] Al Ammal, H. and Aljasmi, L. Usability, Encryption, and the User Experience. *KnE Engineering*. october 2018, vol. 3, p. 71. DOI: 10.18502/keg.v3i7.3073.

[5] Albrecht, M. and Jensen, R. *The Vacuity of the Open Source Security Testing Methodology Manual*. November 2020. 114-147 p. ISBN 978-3-030-64356-0.

[6] Alhanahnah, M. and Yan, Q. Towards best secure coding practice for implementing SSL/TLS. In: *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2018, p. 1–6. DOI: 10.1109/INFCOMW.2018.8407011.

[7] Alshamari, M. A Review of Gaps between Usability and Security/Privacy. *International Journal of Communications, Network and System Sciences*. january 2016, vol. 09, p. 413–429. DOI: 10.4236/ijcns.2016.910034.

[8] Althobaiti, M. M. and Mayhew, P. Usable security of authentication process: New approach and practical assessment. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. 2015, p. 179–180. DOI: 10.1109/ICITST.2015.7412083.

[9] Bauer, L., Bravo Lillo, C., Cranor, L. and Fragkaki, E. *Warning Design Guidelines*. CMU-CyLab-13-002. CyLab, Carnegie Mellon University, february 2013. Available at: https://www.cylab.cmu.edu/research/techreports/2013/tr_cylab13002.html.

[10] Caputo, D., Pfleeger, S., Sasse, A., Ammann, P., Offutt, J. et al. Barriers to Usable Security? Three Organizational Case Studies. *IEEE Security & Privacy*. september 2016, vol. 14, p. 22–32. DOI: 10.1109/MSP.2016.95.

[11] Chiasson, S., Biddle, R. and Somayaji, A. Even Experts Deserve Usable Security: Design guidelines for security management systems. In:. 2007.

[12] Choong, Y.-Y., Dawkins, S., Furman, S., Greene, K., Haney, J. et al. *NIST Usable Cybersecurity* [online]. 2021 [cit. 2021-12-27]. Available at: `https://csrc.nist.gov/Projects/usable-cybersecurity/media`.

[13] Dastres, R. and Soori, M. Secure Socket Layer (SSL) in the Network and Web Security. *International Journal of Computer and Information Sciences*. october 2020, vol. 14, p. 330–333.

[14] De Haes, S., Van Grembergen, W., Joshi, A. and Huygh, T. COBIT as a Framework for Enterprise Governance of IT. In: *Enterprise governance of information technology*. Springer, 2020, p. 125–162.

[15] Fahl, S., Harbach, M., Perl, H., Koetter, M. and Smith, M. Rethinking SSL development in an appified world. In:. November 2013, p. 49–60. DOI: 10.1145/2508859.2516655.

[16] Faurie, P., Moldovan, A. and Tal, I. 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)*. 2020, p. 1–6. DOI: 10.1109/CyberSecurity49315.2020.9138857.

[17] Fischer, F., Böttinger, K., Xiao, H., Stransky, C., Acar, Y. et al. Stack Overflow Considered Harmful? The Impact of Copy Paste on Android Application Security. In: *2017 IEEE Symposium on Security and Privacy (SP)*. 2017, p. 121–136. DOI: 10.1109/SP.2017.31.

[18] Foundation, O. *OWASP Testing Guide 4.0*. Publication. OWASP Foundation, April 2014.

[19] Gao, B., Kim, H. and Divya Udayan, J. A Study on Usability and Security of Mid-Air Gesture-Based Locking System. In: Peter, J. D., Alavi, A. H. and Javadi, B., ed. *Advances in Big Data and Cloud Computing*. Singapore: Springer Singapore, 2019, p. 313–325. ISBN 978-981-13-1882-5.

[20] Garfinkel, S. and Lipford, H. R. 2014.

[21] Georgiev, M., Iyengar, S., Jana, S., Anubhai, R., Boneh, D. et al. The most dangerous code in the world: validating SSL certificates in non-browser software. In:. October 2012, p. 38–49. DOI: 10.1145/2382196.2382204.

[22] Gordieiev, O., Kharchenko, V. and Vereshchak, K. Usable Security Versus Secure Usability: an Assessment of Attributes Interaction. In: *ICTERI*. 2017.

[23] Green, M. and Smith, M. Developers are Not the Enemy!: The Need for Usable Security APIs. *IEEE Security & Privacy*. 2016, vol. 14, no. 5, p. 40–46. DOI: 10.1109/MSP.2016.111.

[24] Herzog, P. *OSSTMM - The Open Source Security Testing Methodology Manual*. ISECOM, 2010.

[25] Hof, H.-J. User-Centric IT Security - How to Design Usable Security Mechanisms. In:.

[26] ISO Central Secretary. *ISO/IEC 27001 - Information Security Management*. Standard. International Organization for Standardization, 2013.

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

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

[29] Kirlappos, I. and Sasse, A. What Usable Security Really Means: Trusting and Engaging Users. In:. June 2014, vol. 8533, p. 69–78. DOI: 10.1007/978-3-319-07620-1_7. ISBN 978-3-319-07619-5.

[30] Kitkowska, A., Warner, M., Shulman, Y., Wästlund, E. and Martucci, L. A. Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, August 2020, p. 437–456. ISBN 978-1-939133-16-8. Available at: https://www.usenix.org/conference/soups2020/presentation/kitkowska.

[31] Kraus, L., Ukrop, M., Matyas, V. and Fiebig, T. Evolution of SSL/TLS Indicators and Warnings in Web Browsers. In: *27th International Workshop on Security Protocols (SPW 2019)*. Springer International Publishing, 2020, p. 267–280.

[32] Lennartsson, M., Kävrestad, J. and Nohlberg, M. Exploring the Meaning of "Usable Security". In:. August 2020, p. 247–258. DOI: 10.1007/978-3-030-57404-8_19. ISBN 978-3-030-57403-1.

[33] Luca, A. D., Hang, A., Zezschwitz, E. V. and Hussmann, H. 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.

[34] Mecke, L., Rodriguez, S. D., Buschek, D., Prange, S. and Alt, F. Communicating Device Confidence Level and Upcoming Re-Authentications in Continuous Authentication Systems on Mobile Devices. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, August 2019, p. 289–301. ISBN 978-1-939133-05-2. Available at: https://www.usenix.org/conference/soups2019/presentation/mecke-confidence.

[35] Nurse, J., Creese, S., Goldsmith, M. and Lamberts, K. Guidelines for usable cybersecurity: Past and present. In:. October 2011, p. 21 – 26. DOI: 10.1109/CSS.2011.6058566.

[36] Oliveira, D. S., Lin, T., Rahman, M. S., Akefirad, R., Ellis, D. et al. API Blindspots: Why Experienced Developers Write Vulnerable Code. In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD:

USENIX Association, August 2018, p. 315–328. ISBN 978-1-939133-10-6. Available at: https://www.usenix.org/conference/soups2018/presentation/oliveira.

[37] Payne, B. and Edwards, W. A Brief Introduction to Usable Security. *Internet Computing, IEEE*. june 2008, vol. 12, p. 13–21. DOI: 10.1109/MIC.2008.50.

[38] Pearman, S., Zhang, S. A., Bauer, L., Christin, N. and Cranor, L. F. Why people (don't) use password managers effectively. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, August 2019, p. 319–338. ISBN 978-1-939133-05-2. Available at: https://www.usenix.org/conference/soups2019/presentation/pearman.

[39] Realpe Mu noz, P., Collazos, C. A., Granollers, T., Arteaga, J. Muñoz and Fernandez, E. B. Design Process for Usable Security and Authentication Using a User-Centered Approach. In: *Proceedings of the XVIII International Conference on Human Computer Interaction*. New York, NY, USA: Association for Computing Machinery, 2017. Interacción '17. DOI: 10.1145/3123818.3123838. ISBN 9781450352291. Available at: https://doi.org/10.1145/3123818.3123838.

[40] Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R. et al. An investigation of phishing awareness and education over time: When and how to best remind users. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, August 2020, p. 259–284. ISBN 978-1-939133-16-8. Available at: https://www.usenix.org/conference/soups2020/presentation/reinheimer.

[41] Rescorla, E. *The Transport Layer Security (TLS) Protocol Version 1.3* [Internet Requests for Comments]. RFC 8446. RFC Editor, August 2018.

[42] Rice, T., Brown White, J., Ozmore, T. S. N., Carlage, N., Poland, W. et al. Fundamental Practices for Secure Software Development, Third Edition. In:. 2018.

[43] Sahar, F. Tradeoffs between Usability and Security. *International journal of engineering and technology*. 2013, p. 434–437.

[44] Sasse, A. and Flechais, I. Usable Security: Why Do We Need It? How Do We Get It? In:. January 2005.

[45] Simoiu, C., Bonneau, J., Gates, C. and Goel, S. „I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, August 2019, p. 155–174. ISBN 978-1-939133-05-2. Available at: https://www.usenix.org/conference/soups2019/presentation/simoiu.

[46] Sotirakopoulos, A., Hawkey, K. and Beznosov, K. On the Challenges in Usable Security Lab Studies: Lessons Learned from Replicating a Study on SSL Warnings. In: *Proceedings of the Seventh Symposium on Usable Privacy and Security*. New York, NY, USA: Association for Computing Machinery, 2011. SOUPS '11. DOI: 10.1145/2078827.2078831. ISBN 9781450309110. Available at: https://doi.org/10.1145/2078827.2078831.

[47] Standards, N. I. of and Technology. *Securing Web Transactions: TLS Server Certificate Management*. NIST SPECIAL PUBLICATION 1800-16. Washington, D.C.: U.S. Department of Commerce, 2020.

[48] Tan, J., Bauer, L., Christin, N. and Cranor, L. 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.

[49] Heroku. *What is Heroku?* 2021 [cit. 2021-05-12]. Available at: `https://www.heroku.com/about`.

[50] Postgres. *PostgreSQL: The World's Most Advanced Open Source Relational Database*. 2021 [cit. 2021-05-12]. Available at: `https://www.postgresql.org/`.

[51] The OpenSSL Project. *OpenSSL: The Open Source toolkit for SSL/TLS*. April 2003. `www.openssl.org`.

[52] Theofanos, M. Is Usable Security an Oxymoron? *Computer*. 2020, vol. 53, no. 2, p. 71–74. DOI: 10.1109/MC.2019.2954075.

[53] Thomas, B. E. S. D. P. M. K. C. N. A. G. P. C. B. *MITRE ATT&CK™: Design and Philosophy*. The MITRE Corporation, July 2018.

[54] Wear, S. *Burp Suite Cookbook: Practical Recipes to Help You Master Web Penetration Testing with Burp Suite*. Packt Publishing, 2018. ISBN 1938581164.

[55] Whitten, A. and Tygar, J. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: *USENIX Security Symposium*. 1999.

[56] Wiefling, S., Patil, T., Dürmuth, M. and Lo Iacono, L. Evaluation of Risk-based Re-Authentication Methods. august 2020.

[57] Wijayarathna, C. and Arachchilage, N. A. G. Why Johnny can't develop a secure application? A usability analysis of Java Secure Socket Extension API. *Computers & Security*. 2019, vol. 80, p. 54–73. DOI: https://doi.org/10.1016/j.cose.2018.09.007. ISSN 0167-4048. Available at: `https://www.sciencedirect.com/science/article/pii/S0167404818304887`.

[58] Wurster, G. and Oorschot, P. C. van. The Developer is the Enemy. In: *Proceedings of the 2008 New Security Paradigms Workshop*. New York, NY, USA: Association for Computing Machinery, 2008, p. 89–97. NSPW '08. DOI: 10.1145/1595676.1595691. ISBN 9781605583419. Available at: `https://doi.org/10.1145/1595676.1595691`.

Appendix A

Questionnaire for Developers

A.1 Demography

1. What is your current job position?
   (a) software architect
   (b) programmer
   (c) tester
   (d) other: .....
2. How many years of experience in IT do you have?
   (a) 1 to 3 years
   (b) 4 to 7 years
   (c) 8 to 15 years
   (d) 15 and more years
3. Do you work in the field of IT security? If yes, how many years of experience do you have?
   (a) yes
   (b) no
4. What areas of IT do you work in? You can choose multiple options.
   (a) web applications
   (b) IoT applications
   (c) mobile applications
   (d) hardware
   (e) others: .....

A.2 Security

1. Were you given specific security criteria that needs to be met?
   (a) yes
   (b) no
2. Do you use any security standards, guidelines, tools or other materials? If yes, what standards, guidelines, tools or other materials do you use?
   (a) yes: .....
   (b) no

A.3 Usability

1. Were you given specific usability criteria that needs to be met?
   (a) yes
   (b) no
2. Do you use any usability guidelines or tools? If yes, what guidelines or tools do you use?
   (a) yes: .....
   (b) no

A.4 Usable Security

1. Have you ever heard the term usable security?
   (a) yes
   (b) no
2. How do you improve you skills related to security and usability. You can choose multiple options.
   (a) self improvement
   (b) training at work
   (c) certifications
   (d) others: .....
3. Do you find security criteria and usability criteria as competing factors?
   (a) yes
   (b) no
4. Are you aware of any standards, guidelines or other related materials on usable security?
   (a) yes: .....

(b) no

5. Which standards, guidelines or other related materials on usable security do you use?

   (a) .....

   (b) none

6. Do you think that security is in development considered as a secondary concern?

   (a) yes

   (b) no

A.5 Methods within Usable Security

1. What methods ensure usability consideration in designing, developing or testing security solutions? E.g. direct communication with the end user, given detailed specification.

   .....

2. What is the basis for determining restrictions for the end user? E.g. antivirus scanning every input on the same website over and over could lead to the user turning the checks off.

   .....

3. What is the basis for determining limitations for users security decisions? E.g. user can not send unencrypted message containing sensitive data, however user can agree that the data is being processed

   .....

4. According to what methods is the system designed and implemented so that the security mechanisms do not interfere with the tasks of the user? E.g. security warnings appearance during the users' tasks.

   .....

5. How is the effectiveness of using the system evaluated? E.g. considering the time consumption of security mechanisms.

   .....

6. How is the usability considered during designing and implementing authentication process? E.g. creating a prototype and using users feedback.

   .....

7. What methods are used for ensuring the visibility of current state of system's security? E.g. web browser showing the secure connection.

   .....