T.R.
GEBZE TECHNICAL UNIVERSITY
GRADUATE SCHOOL

A SYSTEMATIC APPROACH TO MEASURE USABILITY AND SECURITY TRADE-OFF OF A GIVEN USER INTERFACE

İNCİ KARAMAHMUTOĞLU

A THESIS OF MASTER OF SCIENCE
DEPARTMENT OF COMPUTER ENGINEERING

ADVISOR: ASSOC. PROF. DR. MEHMET GÖKTÜRK

JULY 2024

T.R.
GEBZE TECHNICAL UNIVERSITY
GRADUATE SCHOOL

A SYSTEMATIC APPROACH TO MEASURE USABILITY AND SECURITY TRADE-OFF OF A GIVEN USER INTERFACE

İNCİ KARAMAHMUTOĞLU

A THESIS OF MASTER OF SCIENCE
DEPARTMENT OF COMPUTER ENGINEERING

ADVISOR: ASSOC. PROF. DR. MEHMET GÖKTÜRK

JULY 2024

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KULLANILABİLİRLİK VE GÜVENLİK DENGESİ ÖLÇÜMÜNDE SİSTEMATİK YAKLAŞIM

İNCİ KARAMAHMUTOĞLU

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMAN: DOÇ. DR. MEHMET GÖKTÜRK

TEMMUZ 2024

MASTER of SCIENCE JURY APPROVAL FORM

A thesis submitted by İnci KARAMAHMUTOĞLU, defended on 10/07/2024 before the jury formed with the 24/06/2024 date and 2024/32 numbered decision of the GTU Graduate Administration Board, has been accepted as a MASTER of SCIENCE thesis in the Department of Computer Engineering.

JURY

MEMBER (THESIS ADVISOR) : Assoc. Prof. Dr. Mehmet GÖKTÜRK

MEMBER : Prof. Dr. İbrahim SOĞUKPINAR

MEMBER : Asst. Prof. Dr. Onur DEMİR

APPROVAL

Gebze Technical University Graduate Administration Board

…..…/…..…/..…… date and ……/…….. numbered decision.

SIGNATURE/SEAL

To all my teachers and my family who brought me to this day.

ABSTRACT

Designing usable and safe interfaces has become a necessity in today's complex application structures. From the user's point of view, usability aims at simplifying the interaction with systems and at enabling operations to be carried out without spending too much physical and mental energy. The concept of security on the other hand aims to make applications more complex, with the main objective of making unauthorized access to systems impossible. At the same time, it aims to create a restricted system to make the operations that can be performed on the application and the application itself safe or more secure. Although the general view in the literature about the relationship between these issues is that they influence each other's performance in opposite directions and prevent each other from achieving the desired goals, these components should be evaluated together at all design stages in the application development process to maximize application performance.

Although there are no ready-made algorithms or rules that ensure a usable and secure user interface, these concepts can be expressed in terms of subjective approaches rather than mathematical expressions. Interface design and application development processes can vary depending on the designer's knowledge, perspective, experience and level of expertise in the field. The aim of this study was to make these issues more measurable by creating a conceptual and metric model. Therefore, as a result of the literature review, criteria were identified that can be effective in understanding a given interface as usable and secure by the user, and that can measure the usability and reliability level of that interface. The identified criteria were grouped by evaluating their supporting effect on the performance of the interface. The importance of these criteria was then determined by experts in the field of human-computer interaction and security, and the AHP method was used to identify the criteria that most influence the usability and security of a user interface. As a result of the study, an attempt was made to measure the level of usability and security of an interface using the characteristics that have the most impact on the user interface. This measurement was carried out by determining the position of the interfaces on a spatial plane whose dimensions are security and usability. In addition, this study creates a conceptual model as well as the metric model to guide the creation of systematic approaches to be carried out in the future. It is believed that under the guidance of this approach, the conflict between usability and security in user interfaces can be avoided and a balance between these concepts can be established. At the same time, this study will serve as a guide for software developers when creating a new application or making changes to an existing application during the application development phase.

Keywords: Usability, Security, User Interface, Human-Computer Interaction, Analytic Hierarchy Process, Metric Model.

ÖZET

Kullanılabilir ve güvenli arayüzlerin tasarlanması bugünün karmaşık uygulama yapılarında bir ihtiyaç haline gelmiştir. Kullanılabilirlik, kullanıcının bakış açısından değerlendirildiğinde sistemler ile etkileşimi kolaylaştırmayı, gerçekleştirilen işlemlerin çok fazla fiziksel ve zihinsel enerji harcamadan yapılabilmesini amaçlamaktadır. Güvenlik kavramı ise sistemlere yetkisiz erişimi olanaksız noktaya getirme ana hedefiyle, uygulamaları daha karmaşık hale getirmeyi hedeflemektedir. Aynı zamanda uygulama üzerinde gerçekleştirilebilen işlemler ile uygulamanın kendisini güvenli veya daha güvenli yapabilmek için kısıtlı bir yapı oluşturmayı amaçlamaktadır. Her ne kadar literatürdeki bu konuların birbiriyle ilişkisi konusundaki genel görüş, birbirlerinin performansını zıt doğrultuda etkilediği ve ulaşılmak istenen amaçların gerçekleştirilmesinde birbirlerine engel oluşturduğu yönünde olsa da uygulama performansını en üst düzeye çıkarmak için bu bileşenlerin uygulama geliştirme sürecindeki tüm tasarım aşamalarında birlikte değerlendirilmesi gerekmektedir.

Günümüzde kullanıcı arayüzünün kullanılabilir ve güvenli olmasını sağlayacak herhangi bir hazır algoritma veya kural kümesi bulunmamakla birlikte, bu kavramlar matematiksel ifadelerden çok sübjektif yaklaşımlar doğrultusunda ifade edilebilmektedir. Tasarımcının bilgi birikimine, bakış açısına, alandaki tecrübesine ve deneyimine bağlı olarak arayüz tasarımları ve uygulama geliştirme süreçleri değişiklik gösterebilmektedir. Bu çalışmada ise kavramsal bir model oluşturularak bu konuların daha ölçülebilir hale getirilmesi amaçlanmıştır. Bu sebeple verilen bir arayüzün kullanıcı tarafından kullanılabilir ve güvenli olarak kavranması için etkili olabilecek ve o arayüzün kullanılabilirlik ile güvenlik seviyesini ölçebilecek kriterler literatür taraması sonucunda belirlenmiştir. Belirlenen kriterler arayüzün performansını destekleyici etkisi değerlendirilerek gruplandırılmıştır. Daha sonrasında bu kriterlerin önem dereceleri İnsan-Bilgisayar Etkileşimi ve Güvenlik alanındaki uzmanlar tarafından belirlenerek AHP yöntemi yardımı ile bir kullanıcı arayüzünün kullanılabilirliğini ve güvenliğini en çok etkileyen kriterler belirlenmiştir. Çalışmanın sonucunda ise kullanıcı arayüzüne en çok etkisi olan karakteristik özellikler ile bir arayüzün kullanılabilirlik ve güvenlik derecesi ölçülmeye çalışılmıştır. Bu ölçüm, arayüzlerin konumunun boyutları güvenlik ve kullanılabilirlik olan bir düzlem üzerinde belirlenmesi ile gerçekleştirilmiştir. Ayrıca bu çalışma ile ileride gerçekleştirilecek sistematik yaklaşımların oluşturulmasına yön gösterme amacıyla metrik modelin yanı sıra kavramsal bir model de oluşturulmaktadır. Bu yaklaşımın rehberliğinde kullanıcı arayüzlerinde kullanılabilirlik ve güvenlik arasındaki çatışmanın önlenebileceği ve bu kavramlar arasında bir dengenin kurulabileceği düşünülmektedir. Aynı zamanda bu çalışma, uygulama geliştirme aşamasında yazılım geliştiricilerine yeni bir uygulama oluşturmada veya var olan bir uygulama üzerinde değişiklik gerçekleştirmede bir kılavuz görevi görecektir.

Anahtar Kelimeler: Kullanılabilirlik, Güvenlik, Kullanıcı Arayüzü, İnsan-Bilgisayar Etkileşimi, Analitik Hiyerarşi Prosesi, Metrik Model.

ACKNOWLEDGEMENTS

First of all, I would love to thank my supervisor Assoc. Prof. Dr. Mehmet GÖKTÜRK, who guided and supervised me in my academic progress with his valuable knowledge, help and support. I know that the time spent cannot be repaid in any way and it is priceless, for this reason, I would like to express my gratitude for his valuable time and for guiding me to take the right and good steps in this path. I would also like to thank all my teachers who have contributed to my academic journey in any way and who have trained and prepared me until today.

TABLE OF CONTENTS

LIST OF SYMBOLS AND ABBREVIATIONS

UI	:	User Interface
OS	:	Operating System
GUI	:	Graphical User Interface
HCI	:	Human-Computer Interaction
HCI-SEC	:	Human-Computer Interaction Security
PoI	:	Perception of Interactions
UX	:	User Experience
CLI	:	Command Line Interface
CD	:	Compact Disc
TCP/IP	:	Transmission Control Protocol/Internet Protocol
CAPTCHA	:	Completely Automated Public Turing Test to Tell Computers and Humans Apart
DoS	:	Denial of Service
SSH	:	Secure Shell
CCP	:	Cued Click-Points Password
PCCP	:	Persuasive Cued Click-Points Password
2FA	:	Two-Factor Authentication
SMS	:	Short Messaging Service
OTP	:	One-Time Password
SSO	:	Single Sign-On
GPS	:	Global Positioning System
AHP	:	Analytic Hierarchy Process
CI	:	Consistency Index
RI	:	Random Consistency Index
CR	:	Consistency Ratio

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Today's complicated lifestyle obliges us to stay connected with technology, and technological devices such as computers, tablets, and smartphones are essential parts of everyday life. Fortunately, these kinds of devices create opportunities to do time-saving and effective tasks since these are the main criteria of our hectic lives. Many specific purpose applications are released to the public to do such activities online. For example, money-transferring operations can be done in a few minutes by only using online banking applications without going anywhere physically. Nowadays, all applications have fancy, eye-catching user interfaces (UI) that create a layer of interaction between the user and the application. This structure is similar to the operating systems (OS) because the OS likewise stands between the hardware and software of the system. Therefore, users can communicate with an application through the user interface. Although user interfaces prepare the ground for ease, there are other sides, like intruders trying to convince the users to do unauthorized operations by using visual tricks or targeting UI vulnerabilities of the application [1]. Visual tricks can be used as a specific method, such as phishing attacks [2], which are used to gain information about users' credentials or private information without users' permission. Since finding vulnerabilities and applying all the stages that gather critical information about the system requires more in-depth work and effort, it is obvious that users can be targeted more easily by attackers. At this point, in addition to the usability factor of the application, security comes to the forefront.

While designing the user interfaces, the developers must consider both usability and security aspects at every stage since they directly impact the applications' success and performance. The common idea in the literature is that these two subjects conflict with each other and have a trade-off between them. However, if they are designed together based on some specific goals and structure, they can increase the performance of the system and go hand in hand.

The goal of usability is to design more convenient interactions from the user's viewpoint and ensure that the goal of the user can be reachable with little physical and mental effort. On the other hand, the objective of security is creating more complex structures to operate safe operations and make these kinds of systems more secure

within the aim of preventing unauthorized access. As intruders possess more detailed knowledge about the interface than a novice or regular user, security measurements or reinforcement operations to the system functions like a barrier against unauthorized activities.

To achieve the aim of enhancing the performance and satisfaction of the application, finding a balance between security and usability is a key point when designing systems. Unfortunately, standard design models in this area consider these subjects separately and treat them as add-on operations [3]. The common approach is that if there is a usable interface, then the security measurements can be implemented on top of this system; or otherwise can also be possible. The secure user interfaces can also be made usable by applying usability features to that system. However, this causes the interface does not felt natural or work well by the user's perspective.

1.1. Motivation and Research Gap

The missing part or difficulty of this research area is that neither security nor usability is easy to measure and there are no specific rules, mathematical applications or ready algorithms that will ensure that the graphical user interface (GUI) or the whole application itself becomes usable and secure enough [4]. This makes it inevitable that there is a need to create a conceptual and metric model so that this model is able to bring security and usability into a measurable structure of a given UI. In addition to this, this framework can create a guideline for developers when they create a new application or update an existing one by following the steps of the model and benefitting from the intuition of this research.

The definition of metric and conceptual model that determines the position of a given user interface in a multidimensional security and usability spatial plain is the aim of this study. Suppose somehow the security and usability can be aligned and balanced by preparing the environment so that they synergistically improve. In that case, the performance of the application can be maximized, and this is the targeted contribution of the defined model by the end of the study. Since the user interface can be defined as usable and secure only if it is perceived in this way by the user, the opinion of the user cannot be underestimated. Therefore, users' perceptions are prominent when creating a model and will create the baseline of this study.

1.2. Organization

In this literature, related works with security & usability relation, authentication related aspects and perception of interactions with mental models are explained in Section 2. After this, the methodology of this study is described in detail in Section 3. Finally in Section 4, conclusions and future work comments are added.

2. RELATED WORKS

Although usability and security areas are inside computer science, they include and consider multiple disciplines like human psychology, human-computer interaction (HCI), cognitive science, information security, and anthropology. In this research, studies related to usability and security subjects are organized into three main sections, focusing on the concepts of usability & security relation, an analysis of authentication-related aspects, and perception of interactions (PoI) & mental models.

2.1. Security & Usability Relation

With the development of technology and the inclusion of technology-related devices in everywhere of our lives, various kinds of disciplines and terminology started to emerge, such as browsers, users, and user experience (UX) in everyday language. To these words usability can be given as an example, and the definition of usability is providing convenience to users in the computer science aspect when they want to reach a goal by using the applications. In the 1970s, the User Interfaces (UI) started to be used by users to interact with computers, and the first personal computer running through an UI, known as “Lisa” from Apple, was created in 1983 [5].

[1] underlines the inevitability of growth in the HCI area with the presentation of GUI, which creates pleasing-to-eye and more straightforward computer display features. Due to the fact that humans have interacted regardless of what the computer interface alike from the invention of the first machines, the area of Human-Computer Interaction (HCI) has emerged as one distinct field of computer science in the 1980s [6]. This discipline’s fundamental approach is placing the user at the centre of every step in terms of the application design process and making them key figures. Research

studies in this area try to understand users' objectives (effectiveness), the speed with which goals are achieved (efficiency), and users' satisfaction with the system within a specified context [7]. During that period, different common issues were being to be addressed instead of asking questions and trying to find out the answers considering security-related subjects since it introduces difficulties to the universe of HCI. As part of these efforts, researchers focused on exploring methods for converting command-line interfaces (CLIs) into graphical user interfaces (GUIs), adjusting newly designed input devices to existing structures, and enhancing the efficiency of extracting information from compact discs (CDs).

The emergence of the concept of security is an inevitable part of since the Internet becoming a part of our lives. The history of the Internet endures to 1969 when the ARPANET network was constructed. This network is seen as the origin of the Internet; however, it was only useable for some specific ranges that can communicate with each other through separate computers. Therefore, after realizing the convenience and benefits of this network, as expected, it wanted to be expanded to a broader distance. Additionally, since communication can be done by following specific rules or grammar, computers also use some protocols to communicate among themselves, and the TCP/IP, which was constructed in the 1970s, is one of them. With this network communication protocol, the globalization of information transmission within different structures and distances that are larger between them become possible. The moment the Internet subject is expanded, users with various skills and knowledge of security topics will start to be involved and be part of this technological advancement. The information exchange on the network was initially without encryption and transmitted through the network as plain text so that the intruder could access the whole communication without any extra effort. The only security threat in the 1980s is physical hazards [6]. Additionally, at that time and now, security is not the users' primary goal [8] since it is a complex subject and increases the cognitive load of the user. In other words, the focus of the users is to reach the goal by getting the job done conveniently.

As a result of security comes up to the forefront in the 1990s, the security-related applications started to appear in the late 2004s. The evaluation of HCI to HCI-SEC is another consequence of the emergence of security, and in this research area both security and usability started to be considered rather than only usability. HCI-SEC

began to explore questions and try to find out answers to those topics such as the design process [9] and structure of warnings and implementation of alternative authentication mechanisms. It is obvious that users experience the application and face with security related problems mainly through the user interface [1]. Therefore, SANS start to review and examine the concept of flaws that involves human factors and social engineering concepts in addition to only software-based vulnerabilities in 2003 [10].

Table 2.1 shows the relevant studies of the security and usability field and core incidents in this area, which can be seen through the timeline. To increase and reach a high usability and security level, experts in HCI and security follow different methods and approaches. Based on the literature review, it can be seen that in the beginning, two common approaches were applied to find an equilibrium between security and usability [3]:

• making adaptations based on usability features to secure systems so that they become usable and,

• implement security principles to systems that are labeled as user-friendly.

Unless these approaches are modified, they may lead to further issues, such as the lack of natural and seamless experience feedback from the user since these criteria are applied as an add-on approach. Additionally, due to the constraints, there could be an insurmountable threshold in terms of the performance of the application. In the end, because these approaches do not achieve the expected results and create an opportunity to reach better performance, the user-centered design approach (ISO 9241-210:2019 [11]) is proposed [12]. The user-centered design approach requires regular monitoring of users and ensures that applications are updated according to user feedback based on their needs and preferences [13].

Looking at other studies that do not follow these two mentioned approaches; it becomes apparent that the evaluation of usability and security concepts is often limited to specific content. For instance:

• One notable study [14] has successfully identified and determined the levels of importance of security and usability concepts in the context of online banking, which is a critical area of application. This study's findings provide valuable insights into the interplay between these two concepts.

• In online shopping applications, the requirements of usability and security concepts have been formulated by considering mobile design principles [15], and the strengths or weaknesses of usability and security principles have been determined periodically (between 2000 and 2018) [16].

• Electronic voting systems [17] aim to balance usability and security components by comparing different voting systems.

The ignorance of the relationship between security and usability, regardless of positive or negative correlation, could be linked to the difficulties they impose on each other. HCI is a research area that requires constant interaction with users, but on the other hand, security experts prefer mere coding due to it has no relation with human psychology. However, this approach divides these two research areas with sharp boundaries, which will decrease the efficiency of the system. In addition to these difficulties, since these concepts are not functional and cannot be directly measured, it becomes difficult to conduct research in these areas [6].

The relation between usability and security can be shown and described with some common implementation examples and by explaining usage of them.

• CAPTCHA: One example of the balance between usability and security is the CAPTCHA software that developed in the early 2000s. In general, the aim of the CAPTCHA software is to minimize intentional or unintentional DoS attacks on heavy-use websites and applications that are caused by massive, rapid, automated service requests [8]. The properties of CAPTCHA which includes both usability and security aspects are identified in [18]. Based on that, usability includes how efficient and convenient a CAPTCHA can be when it is decoded by human beings, and the security perspective indicates the difficulty to solve a CAPTCHA for the computer or computer-based intelligence. From this point, it can be seen that the aim of security is to strengthen a part that requires interaction with the user, however, these reinforcements can be burden on the users. Therefore, to provide a secure and usable user interface to the user, the balance between these subjects needs to be created.

• Telnet command [19]: The telnet command is CLI command that provides efficient access to systems remotely. However, it is clear-text protocol and this means all data can be read without any effort by the sniffer. This will be critical when you pass some private information through the network such as password, username, and

credit card information. Therefore, to prevent such thing addition to telnet command the SSH can be used. It is more complex and difficult for novice user to understand and apply, but it will provide more secure communication since all data is encrypted.

• Authentication: The detailed explanation about authentication and passwords are given in Section 2.2.

Table 2.1: Usability and security relationship timeline.

1969	ARPANET
1970	The Emergence of the Concept of the User Interface (UI) - TCP/IP Protocol
1980	Human-Computer Interaction (HCI)
1983	"Lisa" Made by Apple
1990	The Emergence of the Concept of Security - Internet
1996	*User-Centered Security [12]*
1998	*Apple Human Interface Guidelines [5]*
2003	*Security and Human Computer Interfaces [1]* - *A Multi-level Defense Against Social Engineering [10]*
2004	Release of Security Related Applications - *Aligning Usability And Security [3]*
2005	*Design Principles And Patterns For Computer Systems That Are Simultaneously Secure And Usable [6]* *Are Usability and Security Two Opposite Directions in Computer Systems [19]*
2006	Vulnerabilities Caused by People
2007	*The Role Of Security, Privacy, Usability And Reputation In The Development Of Online Banking [14]*
2009	*A Methodology For Designing Information Security Feedback Based On User Interface Patterns [9]* *- ISO 9241-210:2010 [11]*
2010	*When Security Meets Usability: A User-Centric Approach On A Crossroads Priority Problem [8]* - *Security And Usability: Analysis And Evaluation [7]*
2014	*A Perception Oriented Approach For Usable and Secure Interface Development [4]*
2015	*User-Centric Security [13]*
2016	*Design Of Usable Interface For A Mobile E-Commerce Website [15]* - *Usability Analysis of the Specific Captcha Types [18]*
2019	*A Review Of Usability And Security Evaluation Model Of ECommerce Website [16]* *- Alerting Users About Phishing Attacks [2]*
2023	*Usability And Security Of Electronic Voting Systems [17]*

2.2. An Analysis Of Authentication-Related Aspects

In the most basic sense, authentication means introducing the user to the system and deciding whether the user has the right to access confidential information that lies inside the system. The simplest way to provide the identity of the user to the system is using password-based authentication systems because the implementation of this mechanism is easy [20]. By using the password concept, the usability and security relation can be stated and explained.

Security dictates hard-to-guess passwords, while usability dictates easy-to-remember passwords [8]. From the user's perspective, this means remembering complex passwords. Additionally, these days, the increasing number of websites means that one person can have multiple memberships on multiple websites [21], and this situation leads to the need to remember multiple different complex passwords by the user. Although the security of the passwords is increasing by using complex passwords, since there is no operation to balance the usability, the user-friendliness of the passwords is decreasing. Therefore, to reduce the burden of remembering so many passwords, research about balancing usability and security on authentication mechanisms needs to be considered.

After the expansion of the user profile, authentication gained importance and this subject started to take up a lot of space in the security area. By the emergence of the password concept, existing authentication methods have been updated or new methods have been introduced to align usability and security such as

- introducing a "dot" mechanism and,
- instead of using text-based passwords using graphical passwords.

In "dot" representation, when user starts to type the password, each symbol appears as a dot on the interface and since this can cause deletion of all the password because of a mistyping, the "dots" appear in a delay and people can see what they typed [22]. Due to the difficulty of remembering and typing the alphanumeric passwords the graphical authentication mechanisms are created like PassFaces, PassPoints, Cued Click-Points Passwords (CCP), and Persuasive Cued Click-Points Passwords (PCCP). Graphical password schemes can be grouped into three general categories: recognition, recall, and cued recall. Recognition is the easiest for human

memory whereas pure recall is most difficult since the information must be accessed from the memory with no triggers. Cued recall falls between these two as it offers a cue which should establish context and trigger the stored memory [23].

In the early 2000s, touch screen mobile phones started to emerge and introduced another challenge in identification mechanisms. [24] mentions difficulty and slowness of virtual keyboards and compares it with physical ones. Therefore, rather than using text-based passwords the graphical passwords are implemented and as a password, user can start to select from multiple images. Although, in this way the memorability problem can be solved, it starts to danger security part. On the other hand, CCP is a click-based graphical password, and it offers both improved usability and security [23]. Rather than selecting an image, in click-based graphical passwords [25] user needs to be select points from images. However, this method is also not able to prevent creation of patterns. As a solution, rather than freely selecting secret points and creating hotspot areas like drawing a line or common letters by using given images, PCCP [26] limits the selection area and lead users to select random positions since creating randomness reduces predictability. In the mid 2000s, Two-Factor Authentication (2FA) mechanisms were implemented to reduce the password complexity on the user side but create a barrier on the attacker side [27]. For instance, in SMS-Based 2FA after typing username and simple password user will get a SMS to his/her phone number which includes a code to access authenticated areas [28].

To decrease the cognitive load of passwords to the human brain, Single Sign-on Authentication (SSO) and dynamic passwords like One-Time Passwords (OTP) are introduced. Users need to memorize every username and password for per system. Human memory has limitations and people start to remember less over time. By using SSO, the user can be able to authenticate herself/himself to multiple places through one website like Google and this leads to tie together multiple passwords to the same password [29]. Therefore, rather than remembering multiple passwords, the user can remember one complex password to access multiple websites and with this method both the usability and security have been improved. Unlike static passwords, in OTP the generated passwords can be used only once based on the limitations [30]. For instance, in time-based OTP, the user must use generated password in limited time. By this way, burden to remembering all the passwords are decreased since the OTP will be generated by a system and given to the user when the user wants to access a system.

2.3. Perception of Interactions (PoI) & Mental Models

[31] identifies perception as a major part of human intelligence and considers it as key component to understand human behavior. In addition to this, it states that incoming data will be evaluated by the perception to create a response as a behavior. In the usability and security perspective PoI is important, since how users give shape to the UI of the application in their mind affects everything. For instance, it influences the deciding mechanism of the user and by this way user can trust or not trust the system based on characteristic of user interface like color of the web page, used language and its tone.

Perceptions can be affected by many factors such as biases, computer experience or the education level of the user [32]. For instance, automation bias leads to feeling trust or accepting without questioning the generated result by machines/computers and this can be lead following GPS mechanisms even they lead user into a lake. As an example in the concept of security and usability, this bias might take shape as believing generated warnings and links by the intruder that seem as generated by the system. Another factor can be the type of loss [32] which means making mistakes may lead to financial loss or information loss and if the loss amount or effect is affordable according to this, the confidence of the user may change. In addition to the type of loss, users that have more experience in a given UI or with computer may feel familiar to systems and this may naturally create a trust to those systems. Therefore, the users may perceive elements of the UIs based on their trust level. HTTPs indicator can be given as an example of such a situation. For example, the user can think the website is completely secure by looking at the small lock symbol on the left side of the URL that represents only the protocol is secure. Also, the user will not notice the red indicator, which shows system does not use any secure protocol to transfer the information through network, because of other information that draws user's attention in UI.

Like perception affected by many factors, it can also affect users in different manner and can cause various behaviors. The person who is labeled as an online grocery shopper will have a different perception from the gamer since it needs more attention and there is payment phase. When perception changes, it may create different mental models and mental states. [33] defines models as abstractions or simplifications

of a given system. Since they are not the exact representations of something, they may lead or inspire the user incorrectly. Let us say in login page the one UI element is changed with releasing an update to that webpage. This situation can cause errors that are made by the user since their mental model does not represent the present model. To sum up, mental models and PoI influences how the user identifies the given user interface. It can be secure, usable or both secure and usable but without paying attention to those subjects the usability and security of the system cannot be decided.

Users represent the user interfaces (UI) in their mind based on their perception which is called mental models. The relation of mental model and perception is shown in Figure 2.1. For example, if all yellow buttons in the system represent a submission operation of input fields and with an update to the system the button's shape and color are changed then the performance of the system will be affected directly. Another example can be the representation of warnings to the user on the interface, its' origin and research comes from real world's traffic signs [34]. Therefore, it may create a comfort zone and familiarity by catching some traces from the real world.

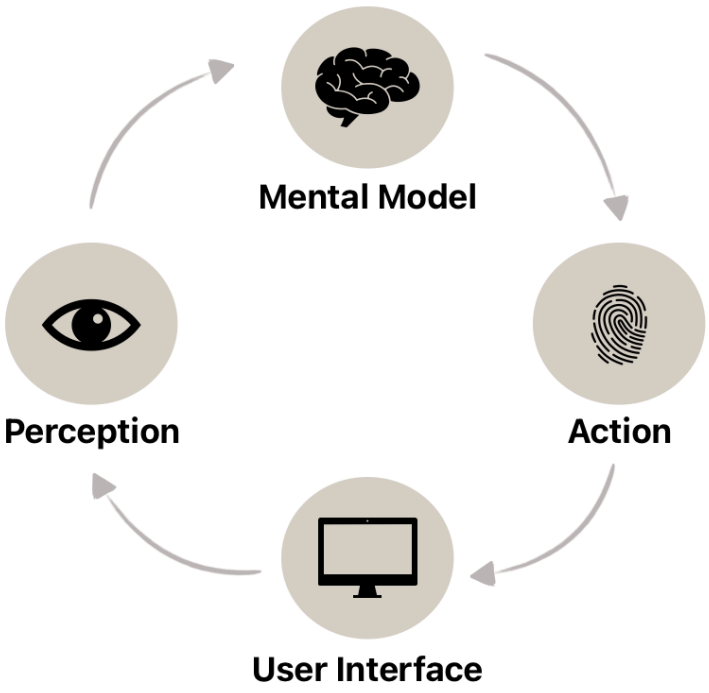


Figure 2.1: Perception of interaction (PoI) and mental model relation.

3. METHODOLOGY

Since no set of rules makes every user interface secure and usable, and these subjects are not functional enough to be measured easily, another method should be designed, which is constructing a framework using a heuristic approach. All the carried-out processes of creating this framework to give some intuition about the security and usability measurement of a given user interface are explained and can be seen from Figure 3.1.

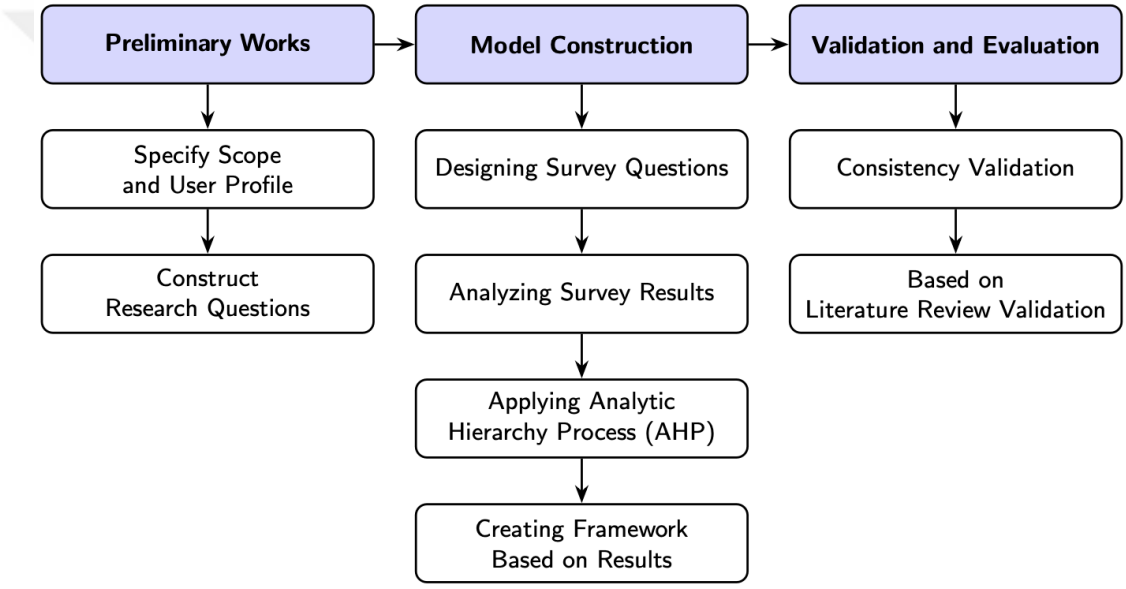


Figure 3.1: Structure of the study.

3.1. Preliminary Work

This study focuses on an average user profile who wants to authenticate through a login page of a given user interface. The meaning of average includes:

- familiarity with interacting with computers,
- having beginner level of security and usability knowledge,
- having accounts on different kinds of web applications on the Internet and
- using technological devices regularly.

In addition, almost all web applications have an identification process, which requires login operations to be performed through login user interface pages. Therefore, login pages are selected as the focus of this study.

At the beginning of the process, the research questions that need to be asked through this study are determined and can be seen in Table 3.1. These questions can be collected under two main sub-topics: perception and mental model-related questions, security and usability-related questions. Throughout this study, those questions will be tried to be answered.

Table 3.1: Research questions of the study.

Perception and Mental Model Related Questions
How users perceive the user interface when they interacting with it?
Which personal characteristics and environmental circumstances affects the users perception?
How the behavior of users be affected after constructing a mental model about the web application?
Usability and Security Related Questions
What are the properties of a web application that is perceived as secure by the user?
What are the distinguishing features of a web application that is perceived as user-friendly?
What are the key attributes of a web application that users find both easy to use and secure?

3.2. Model Construction

Research questions draw the lines of the study and define all processes that need to be carried out. These stages can be represented as four main sub-headings: designing survey questions, analyzing survey results, applying AHP, and finally creating framework.

3.2.1. Designing Survey Questions

At the beginning of the study, a literature review is carried out to systematically determine the key features of usable and secure applications. After evaluating the current baseline requirements for efficiently convenient and safe user interface design of any general application, these attributes are defined. These characteristics are the minimum necessities that specify an interface as reliable and usable user interface. In

total, 33 different factors related to security and usability are determined in the end. From Table 3.2, the names of the characteristics, definitions, and related literature review can be observed.

After identifying the all characteristics in the literature, these attributes are grouped together according to how they affect the user interface. This classification of factors resulted as four different groups:

- only usability related factor group,
- only security related factor group,
- both usability and security enhancing factor group,
- trade-off between usability and security factor group.

The meaning of each category and their corresponding characteristics can be viewed in Table 3.3. To give a more detailed explanation to each of these groups, for the first two groups, it can be said that modifying some of these elements will only affect the user-friendliness or reliability of the user interface. Under these conditions, these factors will only impact on the level of usability and on the security of the application separately. These scenarios may not have the desired effect on the performance of the system, and in this case, a different route may be selected. At best, modifying a given factor (tightening, updating, improving, strengthening, etc.) may improve both usability and security together, or at worst, there will be a negative correlation between the two subjects.

In the end of this process, by using these factors and factor groups that obtained through literature reviews, survey questions which expected to be answered by experts in human-computer interaction field and security are constructed. This survey consists of seven main sections, have created by using Google Forms and all questions & sections can be observable from Appendix-A.

- The first part contains demographic questions and personal experiences related to security and usability such as primary field of work, level of experience with usability and security, and previous experiences about problems that they are face to face within these areas.

Table 3.2: Characteristic features of usable and secure applications.

No	Factor Name	Factor Description	Related Literature
1	Ease of Learning	Users who use the user interface for the first time should quickly adapt to the interface.	[1], [5], [6], [7], [15]
2	Task Efficiency	After learning the system, the user can be able to use the system to reach a goal with an acceptable amount of time or steps.	[6], [7], [15], [20]
3	Effectiveness	The user should be able to achieve their intended goals through the interface.	[7], [20]
4	Ease of Remembering	After a while, without using an interface, all the basic tasks should not be learned all over again. In addition to this, the secrets that are used for security operations should be memorized with ease.	[6], [7], [15]
5	Error Prevention and Recovery	The user interface should minimise the errors and if somehow an error is occurred the system should be able to recover from it.	[1], [5], [6], [15]
6	Subjective Satisfaction	Users should enjoy and be satisfied with their interactions with the user interface. In addition, since transactions that can be associated with security are not the user's first priority, such transactions should not be a burden to the user; on the contrary, they should be presented as encouraging transactions.	[1], [5], [6], [7], [15]
7	Accessibility	The user interface should be designed as universal which means that it should consider all user profiles and situations including disabilities.	[6]
8	Consistency	The meaning of the user interface or the actions designed to interact should be clear and consistent throughout the application.	[1], [6], [15]
9	Feedback and Feed-forward	The system should provide information such as what is going on and what will be the result of intended action.	[5], [6], [15]
10	Efficient Navigation	If the user interface needs navigation operations then these functionalities should be well-organized.	[9]
11	Customization	User interfaces should be customizable or adjustable so that users feel confident and comfortable.	[5], [15]
12	Minimal Cognitive Load	Only relevant information should be displayed, and the user should not be overwhelmed. Additionally, the security-related information should be shown to the user if necessary.	[1], [5], [6], [9], [15]
13	User-Centered Design	User interface design should always take users' needs into account.	[6]
14	Task Focus	Goals of the user should be prioritized and easily manageable.	[8]
15	Responsive Design	The application should be able to adjust itself to various different technological devices.	[15]
16	Familiarity	The patterns inside the user interface should bear traces from the real world so that it will create familiarity.	[1], [5], [6], [7], [15]
17	Simple and Natural Dialog	When it is necessary to establish a dialogue with the user, simple words should be chosen, and technical terms should be avoided.	[1], [6]
18	Knowledge and Skill	The user interface should consider the users' different levels of knowledge and skill types.	[7]
19	User Control	The control of the application should be given to the user.	[1], [15]
20	Input Validation	The user interface should check the validity of user inputs if there are any input fields.	[21]
21	The Principle of Least Surprise	The user expectancy and the system's provided behaviour should be matched.	[6]
22	The Principle of Good Security Now	Update the security features and do patch operations of the system in a regular basis so that system can always be up-to-date.	[6]
23	Attention	Security related operations should not be interrupted easily.	[7]
24	Vigilance	Users should be in alert mode to detect anomalies on the system.	[7]
25	Motivation	User motivation affects security-related transactions. Here, motivation means what the user can lose due to any security vulnerability in the application and the factor that motivates the user.	[7]
26	Visibility of System Status	The internal status and active security precautions of the system should be seen by the user.	[9], [15]
27	Trust	Degree of a trust of the user can be determined by the user interface.	[1], [9], [17]
28	Integrity	Integrity means that the information on the user interface is accurate and not altered. The system should be transparent and do verification of information operations.	[17]
29	Confidentiality	Information on the user interface should be seen by only authorized users. If there are any personal data, the privacy of them should be considered and operations should be observable in a way that who performed actions.	[17]
30	Availability	The actions on the web application should be done in an acceptable amount of time. Additionally, the system need to be capable of scale and perform in high-demand.	[17]
31	Non-repudiation	All steps on the user interface should be traced and cannot be denied.	[17]
32	Authentication	Authentication makes sure that operations can be done by valid user. In addition to this, there should be an unique identifier for each user.	[17], [21]
33	Least Privilage	Only users authorized in the role-authority matrix should be able to access any area of the application.	[22]

• Security related questions are asked in section two and this part consists of questions such as primary loss types, necessity of input validation, and consequences of delay.

• In the next part, corresponding questions are asked to determine the priority of characteristics of usable user interfaces. These questions include topics about universal design, convenient navigation, and responsivity of the interface.

• Ease of remembering, consequences of using words or symbols that have different meanings, and the characteristics that create trade-off and positive correlation between usability and security are measured by questions that are in the fourth section.

• In the next two sections consist of comparison between characteristics with visual and verbal aids.

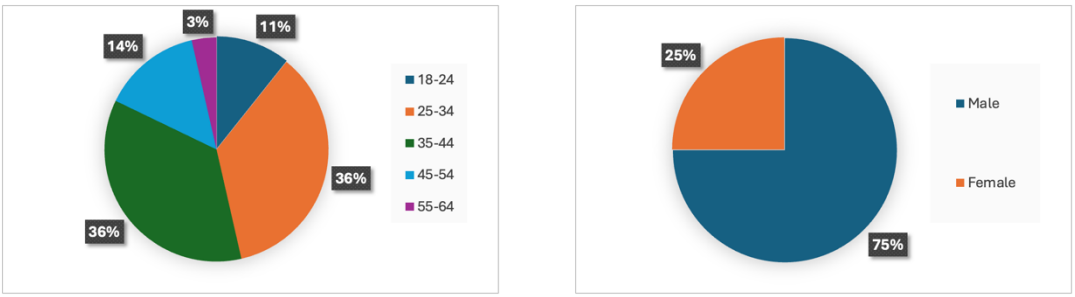
• Finally, the last section takes additional or optional feedback from the expert.

Table 3.3: Factor groups.

Factor Group Name	Group Definition	Related Factors	Total
Only Usability Related Factor Group	This group consists of factors that only affects the usability level of the user interface.	1, 2, 3, 7, 10, 15	6
Only Security Related Factor Group	This group consists of factors that only affects the security level of the user interface.	20, 21, 22, 23, 25, 28, 29, 30, 31, 33	10
Both Usability and Security Enhancing Factor Group	These factors create positive correlation between security and usability of the user interface.	4, 5, 6, 8, 9, 12, 13, 16, 17, 18, 26, 27	12
Trade-off Between Usability and Security Factor Group	These factors create negative correlation between security and usability of the user interface.	11, 14, 19, 24, 32	5

3.2.2. Analyzing Survey Results

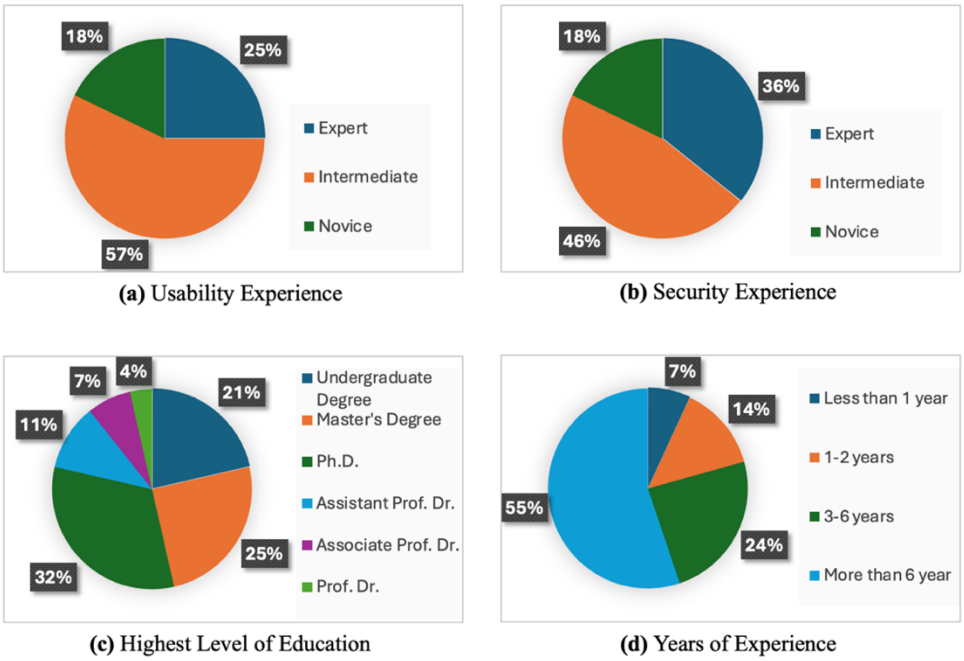
The survey questions focus on people who specialize in human-computer interaction and/or cybersecurity, and for this reason the survey is sent to people whose main area of expertise is in these areas. In this section, instead of data that can be used for AHP, other additional information taken from the experts is evaluated such as demographic distribution of the respondents, personal knowledge to do some estimation about the replies, awareness and level of experience in usability and security. In addition to these examples, all feedback given at the end of the survey and some virtual and verbal comparison questions of characteristics included in the questions in Sections 5 and 6 are analyzed.



(a) Respondent's Age Group Distribution **(b)** Respondent's Gender Distribution

Figure 3.2: Demographic distribution of respondents.

The responses that include demographic and personal experience can be observed in Figure 3.2 and Figure 3.3, respectively. In addition to this, all the surveys are conducted anonymously, and no personal information is collected. Most of the respondents are in the age group of 25-34 and 35-44, male, and have a doctorate (Ph.D.) degree. If we look at the experience side, the majority of the people have more than 6 years of experience in the area they specialize in and have an intermediate level of knowledge about User Experience (UX) and/or the security field.



(a) Usability Experience **(b)** Security Experience

(c) Highest Level of Education **(d)** Years of Experience

Figure 3.3: Personal experience distribution of respondents.

In addition to the questions that is related to usability and security experience, an attempt was made to use the heuristics of the survey taker to determine the security and usability characteristics. Two different approaches are followed to achieve this goal:

• Asking respondents about three different characteristics for both usability and security before showing them to any factors identified in this research study,

• After obtaining the prioritization level of about 33 characteristics from the respondents, in the feedback section, which is the last section, the additional factors that are wanted to be included, if any, is asked about.

Table 3.4: The characteristics of usability and security before the prioritization.

Usability Characteristic Name	Percentage Rate	Security Characteristic Name	Percentage Rate
Ease of Learning	%20.33	Authentication	%25.92
Minimal Cognitive Load	%11.86	Integrity	%24.07
Efficient Navigation	%10.16	Confidentiality	%12.96
Task Efficiency	%8.47	Least Privilege	%7.40
Subjective Satisfactory Consistency Feedback and Feed-forward Responsive Design	%6.77	The Principle of Good Security Now The Principle of Least Surprise Input Validation	%5.55

The results can be seen from Table 3.4. While in terms of usability the most important and indispensable feature is the ease of learning, in terms of security it is seen as the authentication. After considering all the responses 8 new characteristic is determined in addition to the 33 characteristics and its potential factor groups with definitions to support further research studies can be observable from Table 3.5.

In addition to this, when we look at the question that asks the security and/or usability issue that the respondent faced with we can see that the most usability problems are related with Efficient Navigation (26.3%), Responsive Design (21%), Familiarity (10.5%), Minimal Cognitive Load (10.5%), and Availability (10.5%). On the other hand, in security side issues are mostly related with doing operations without permission from the user (33.3%) and Input Validation (16.6%), Authentication (16.6%), Integrity (16.6%), and Consistency (16.6%). These results show the proportions of the respondents that encountered with any problem and explained the problem that they faced with in the given question. Therefore, those who have not face with any problem are not included in the shown rate.

Table 3.5: Additional characteristics for usability and security.

No	Factor Name	Factor Description	Potential Group No
1	Ease of Use	The design of the user interface is based on creating convenience from the perception of the user.	1
2	Speediness	Whilst a fast user interface is a usability requirement, it can be slow due to constant security checks.	4
3	Eye-catching Design	The user interface needs to catch the attention of the users.	1
4	Documentation	All user interface functionality must be documented from both the developer and user perspectives.	3
5	Sustainability	Both the usability and security aspects of the application must be sustainable, so that it can be used over the long term with minimal effort and cost.	3
6	Attack Surface Minimization	To avoid security vulnerabilities, the attack surface of the application needs to be minimised.	2
7	Confirmation	Confirmation from the user is required for critical and important operations to prevent errors and breaches in the system.	4
8	Foresight	The system must be able to predict potential situations that may occur in the application.	3

In the last to sections the visual aid questions try to determine the effect of the absence of a particular feature, whilst the verbal comparison questions measure which criteria are more desirable or necessary for the user interface than the other. In addition, the choices and preferences of the respondents are explained in the Table 3.6.

On the other hand, if we looked at the verbal questions that compare two different characteristic that seen close to each other or hard to differentiate, it can be seen that between Trust and Customization, Navigation and Efficiency, Familiarity and Satisfaction; the Trust, Efficiency and Familiarity is seen as the dominant characteristic.

Additionally, there is a question about the characteristics known as Motivation Loss which is designed to determine the risk factor that most affects the user. For this reason, the respondents were asked to choose in order the three most important risk factors from among the different ones. All the types of risk that most motivate the user and increase attention when using the user interface are listed below:

- First Risk Type: Financial Loss
- Second Risk Type: Loss of Data
- Third Risk Type: Personal Information Loss

Table 3.6: Visual comparison question results.

Characteristic Name	Design 1	Design 2	No Difference	Explanation
Minimal Cognitive Load	%89.3	%3.6	%7.1	This question measures the burden the user interface places on the user. The first design is simple and minimalist, whereas the second interface distracts the user by providing a lot of information.
Feedback and Feed-forward (I)	%7.1	%42.9	%25	By providing feedback on the cursor position, this question attempts to detect the user's attention. The second design provides feedback to the user whereas the first design does not.
Familiarity	%3.6	%71.4	%25	In this question the first design includes a keyword that is unfamiliar to the novice user, such as primary key instead of username.
Simple and Natural Dialog	%67.86	%21.42	%10.72	The first user interface design gives feedback on the password that chosen by the user user with a simple dialogue like 'Please enter a stronger password', but the second has a security-related term that may be difficult for the average user to understand.
Input Validation	%42.86	%42.86	%14.28	This question is designed to determine the behaviour of users who pay attention to feedback about input fields, such as the second design reveals information about the password or username for the attacker.
Feedback and Feed-forward (II)	%92.80	%3.6	%3.6	This question is related with password meters, the first design guides the user with more detailed feedback while the second design only gives information about the weakness.

3.2.3. Applying Analytic Hierarchy Process (AHP)

Analytic Hierarchy Process is a decision-making framework, it compares each alternative in pairwise manner and then prioritizes them by creating a hierarchy [35]. The importance of criteria decreases as you move down the hierarchy, so the root will contain the alternative that can influence the determined problem the most. In addition to this, at the end of the AHP, the consistency of the problem and alternatives can be interpretable. Since our chosen factors for the general problem are not mathematical subjects and cannot be compared by using calculations, AHP is selected to analyze each factor in this study. The phases of the AHP can be observed from Table 3.7.

AHP helps to understand the problem and instead of finding the correct solution, it finds the most appropriate or optimized one [36]. In this phase, the form results from the previous stage are going to be used for determining the importance of each criterion. In the end, factors that are most related to the level of security and usability of the user interface are expected to be determined.

In this phase of the study, there were questions in the survey to identify the priority of the 33 characteristics determined. For this reason, the 7-point Likert scale is used, with 1 representing 'Slightly important' and 7 representing 'Extremely important'. After obtaining the results from the survey respondents, separate importance scores are calculated for each characteristic and these importance percentages of characteristics are shown in Table 3.8 in descending order. The most important characteristics is defined as 'Integrity', whilst 'Customization' has the least priority.

Table 3.7: AHP application process.

1) Problem Definition and Determine Criteria	Decide the problem and select all the criteria that related with this problem.
2) Specify Order of Importance	Define priorities of each criteria by using form results for this operation.
3) Conduct Pairwise Comparison	Compare each pair separately and create a matrix based on results that shows all the priorities.
4) Calculate Overall Priority	By using generated matrix calculate total importance for each criteria and create hierarcy.
5) Check Consistency	After obtaining the overall results, check the consistency of it. If the consistency value is smaller than 0.10 then generated results are acceptable.
6) Identify the Best Option	Create a final decision based on the generated results.

In this way, the second stage of the AHP application process is successfully completed by specifying the order of importance priority. Then by using these priorities, a comparison matrix is generated to conduct a pairwise comparison between each characteristic. After this for calculating the overall priority, the following steps are conducted:

• Square of the matrix is taken,

• Calculated row totals,

• By using the sum of the row totals the priority vector is calculated which is weights,

• In the end, the top 15 criteria that affects the usability and security of the user interfaces are detected which can be observable from Figure 3.4.

From Figure 3.4 it can be seen that there are:

- 6 – both enhancing criteria,
- 4 – usability only,
- 4 – security only and,
- 1 – trade-off criteria.

Therefore, as expected, this shows that the focus needs to be on these types of characteristics to balance and increase the performance of the application by giving more attention and doing research on these characteristics.

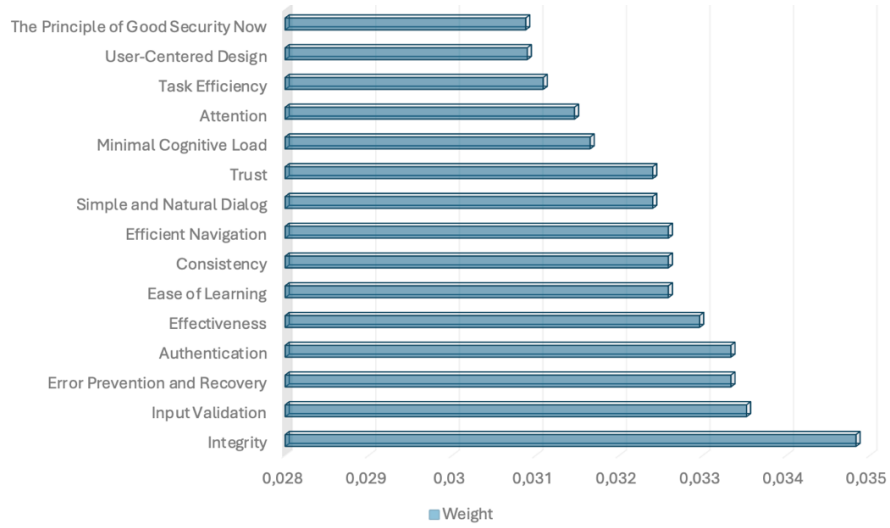


Figure 3.4: Top 15 characteristics that important for usable and secure application.

3.2.4. Creating Framework Based on Results

User interfaces can be described and shown in a spatial plane that has the dimensions of usability and security. To create such a space, the characteristics and identified priority levels are used. The y and x axes represent the security and usability levels of the given interface, respectively. The spatial plane will be constructed and designed with using only the determined top 26 features that have more than 80% priority. Therefore, all user interfaces will be compared using the same factors and plotted in the same spatial plane. For creating the spatial plane, there is a need for describing for hypothetical user interfaces:

- Imaginary both secure and usable user interface ($I_{optimal}$),
- Imaginary only secure user interface (I_{secure}),
- Imaginary only usable user interface (I_{usable}),
- Imaginary not secure and usable user interface($I_{not-optimal}$).

These user interfaces represent 4 different points in the created spatial plain which is shown on the Figure 3.5. On the spatial plain each imaginary user interface can be located on the corners which is represented as (1, 1) – Both Secure and Usable, (-1, 1) – Only Secure, (1, -1) – Only Usable, and (-1, -1) – Not Secure and Usable. To determine the position of a user interface on this created plane and compare them with each other, somehow the representation of these interfaces need to be created. The representation ($I_{example}$) and formula for determining position (W_{total}) of an interface is given below where the weight of each characteristic is represented as w_i, and c_i shows the priority level of that characteristics. These weights need to be determined as decimal points, which are between 0 and 1, by the experts or regular feedback from the user.

$$I_{example} = (w_1.c_1\ , \dots , w_n.c_n)$$

$$W_{total} = w_1.c_1 + \ \dots + w_n.c_n$$

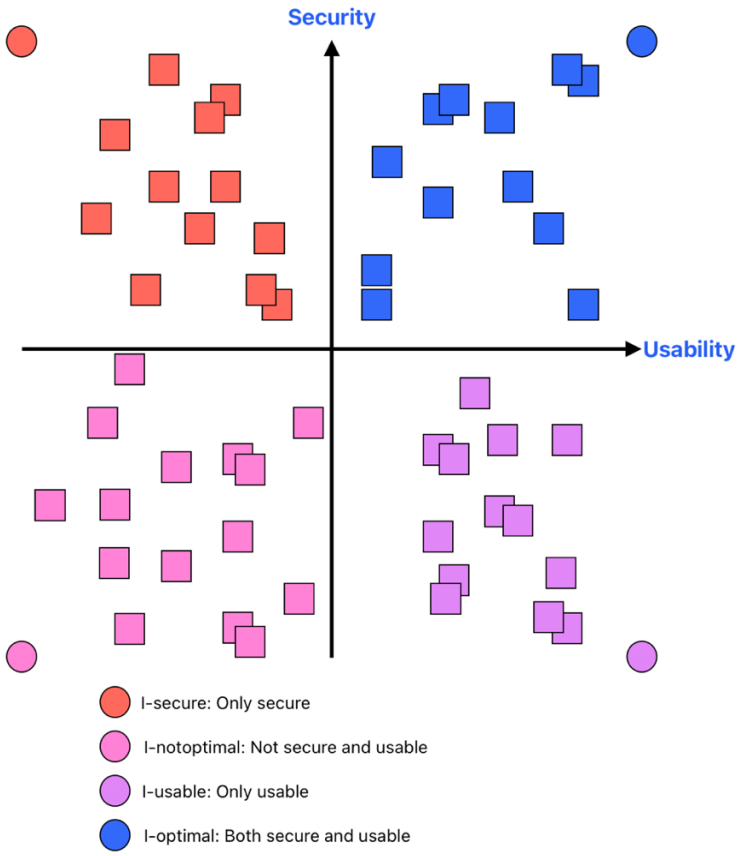


Figure 3.5: The spatial plane that has usability and security as dimensions.

The value of W_{total} is calculated based on its determined priority levels of the user interface with the aid of AHP results. Then, the obtained value will determine the position of the user interface in created space.

It can be seen that from Table 3.8, there exist 8 only security-related, 6 only usability-related, 11 both security and usability related, and 1 trade-off characteristics in the most important 26 characteristics. For trade-off characteristic, we need to use a flag that determines which feature (usability or security) is more affected. By using this information for each characteristic that are given an spatial plane which has dimensions of security and usability. All locations of interfaces can be observable from Figure 3.5. Each location on this figure can be represented as where u is the usability and s the is the security value of given point, respectively. For instance, if the characteristic is related with both usability and security then it will affect both u and s values.

$$p = (u, s)$$

Table 3.8: Priority of characteristics.

No	Factor Name	Related Factor Group	Priority
28	Integrity	Only Security Related Factor Group	94.89%
20	Input Validation	Only Security Related Factor Group	91.32%
5	Error Prevention and Recovery	Both Usability and Security Enhancing Factor Group	90.81%
22	The Principle of Good Security Now	Only Security Related Factor Group	90.81%
32	Authentication	Trade-off Between Usability and Security Factor Group	90.81%
3	Effectiveness	Only Usability Related Factor Group	89.79%
1	Ease of Learning	Only Usability Related Factor Group	88.77%
8	Consistency	Both Usability and Security Enhancing Factor Group	88.77%
10	Efficient Navigation	Only Usability Related Factor Group	88.77%
17	Simple and Natural Dialog	Both Usability and Security Enhancing Factor Group	88.26%
27	Trust	Both Usability and Security Enhancing Factor Group	88.26%
12	Minimal Cognitive Load	Both Usability and Security Enhancing Factor Group	86.22%
23	Attention	Only Security Related Factor Group	85.69%
2	Task Efficiency	Only Usability Related Factor Group	84.69%
13	User-Centered Design	Both Usability and Security Enhancing Factor Group	84.18%
26	Visibility of System Status	Both Usability and Security Enhancing Factor Group	83.67%
30	Availability	Only Security Related Factor Group	83.67%
31	Non-repudiation	Only Security Related Factor Group	83.67%
16	Familiarity	Both Usability and Security Enhancing Factor Group	82.65%
15	Responsive Design	Only Usability Related Factor Group	82.14%
18	Knowledge and Skill	Both Usability and Security Enhancing Factor Group	82.14%
4	Ease of Remembering	Both Usability and Security Enhancing Factor Group	81.63%
7	Accessibility	Only Usability Related Factor Group	81.63%
9	Feedback and Feed-forward	Both Usability and Security Enhancing Factor Group	81.63%
21	The Principle of Least Surprise	Only Security Related Factor Group	81.12%
29	Confidentiality	Only Security Related Factor Group	80.61%
14	Task Focus	Trade-off Between Usability and Security Factor Group	79.59%
25	Motivation	Only Security Related Factor Group	76.53%
33	Least Privilege	Only Security Related Factor Group	76.53%
6	Subjective Satisfaction	Both Usability and Security Enhancing Factor Group	70.91%
24	Vigilance	Trade-off Between Usability and Security Factor Group	65.30%
19	User Control	Trade-off Between Usability and Security Factor Group	63.26%
11	Customization	Trade-off Between Usability and Security Factor Group	61.73%

3.3. Validation and Evaluation

To validate and evaluate this research, the two different validation approach is conducted: consistency validation which applied for the AHP results that obtained in Section 3.2.3 and based on literature review validation. The second approach concludes a heuristic approach and includes comments that obtained from literature review.

3.3.1. Consistency Validation

To check the correctness and consistency of the AHP application process, consistency ratio calculation process explained by Saaty [37] is used. After creating a pairwise comparison matrix, let's call it M, using this matrix eigenvalues and eigenvectors of this matrix are calculated. Then from these values, the highest magnitude is selected to find out the principal eigenvalue shown as λ_{max}. This value is used for the determination of the consistency index (CI). Therefore, the CI is calculated according to the given formula, where n represents the total number of characteristics:

$$CI = \frac{\lambda_{max} - n}{n - 1} \tag{3.1}$$

This CI value is used with random consistency index (RI) in the calculation of the consistency ratio (CR). The RI can be obtained based on the average CI value that is reached in generally with given size n. After deciding RI, the CR is calculated by finding the ratio of CI and RI and this value needs to be smaller than 0,1 to say that the AHP result is consistent for this problem and characteristics.

$$CR = \frac{CI}{RI} \tag{3.2}$$

When we apply all processes to this research and determined characteristics with its priority value, the consistency index is calculated as 0,0082 and then CR value becomes 0,0005 which is less than 0,1 where RI is used as 1.59 for n equal to 33. Therefore, the application of AHP for this research is approved as consistent.

3.3.2. Based on Literature Review Validation

By taking into account the reviewed literature, it can be seen that the 10 topmost appeared characteristics and their priority rank after survey are as given below in order:

- Ease of Learning – 7
- Subjective Satisfaction – 30
- Minimal Cognitive Load – 12
- Familiarity – 19
- Task Efficiency – 14
- Error Prevention and Recovery – 3
- Trust – 11
- Feedback and Feed-forward – 24
- Consistency – 8
- Ease of Learning – 22

From this point of view, it can be said that the usability and security focus of the literature is not distributed efficiently in terms of usability related characteristic number and number of security characteristics.

4. CONCLUSION AND FUTURE WORK

In this study, two disciplines, known as security and usability, explained in terms of conceptual and heuristic metric model which puts these subjects into spatial plain that is two dimensional and describes the level of the security and usability of the given user interface. In this way they can correlate with each other positively and guide programmers or designers in these fields so that they can upgrade an existing interface, or they can create it from scratch more effortlessly. Therefore, in this way they can predict and foresight the features to focus on. Finding a balance between security and usability characteristics provides a better structure and performance.

Since there is no such algorithms or rulesets that when we apply them so that it guarantees to provide secure and usable user interfaces, characteristics or factors from literature and reviewing from experts make more measurable these subjects and

create intuition. With the guidance of this systematic approach, the trade-off between security and usability of a given user interface can be prevented.

In future work, the additional characteristics that identified by the HCI and security experts at the end of the survey can be also considered and used in further research. Additionally, when creating spatial plane instead of randomly generated user interfaces the real ones can be used. Also, created conceptual, metric model and described characteristics can be validated by using real time analysi

REFERENCES

[1] J. Johnston, J. H. P. Eloff, and L. Labuschagne, 'Security and human computer interfaces', *Comput Secur*, vol. 22, no. 8, pp. 675–684, 2003, doi: 10.1016/S0167-4048(03)00006-3.

[2] G. Desolda, F. Di Nocera, L. Ferro, R. Lanzilotti, P. Maggi, and A. Marrella, 'Alerting Users about Phishing Attacks'.

[3] 'Usability and Security', 2004. [Online]. Available: www.computer.org/security/

[4] M. Göktürk and İ. Şişaneci, 'LNCS 8520 - A Perception Oriented Approach for Usable and Secure Interface Development', 2014.

[5] *Apple human interface guidelines : the Apple desktop interface.* Addison-Wesley, 1987.

[6] C. University, 'Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable', 1987.

[7] R. Kainda, I. Flechais, and A. W. Roscoe, 'Security and usability: Analysis and evaluation', in *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 2010, pp. 275–282. doi: 10.1109/ARES.2010.77.

[8] C. A. Fidas, A. G. Voyiatzis, and N. M. Avouris, 'When security meets usability: A user-centric approach on a crossroads priority problem', in *Proceedings - 14th Panhellenic Conference on Informatics, PCI 2010*, 2010, pp. 112–117. doi: 10.1109/PCI.2010.17.

[9] J. Muñoz-Arteaga, R. M. González, M. V. Martin, J. Vanderdonckt, and F. Álvarez-Rodríguez, 'A methodology for designing information security feedback based on User Interface Patterns', *Advances in Engineering Software*, vol. 40, no. 12, pp. 1231–1241, 2009, doi: 10.1016/j.advengsoft.2009.01.024.

[10] D. Gragg, 'A Multi-Level Defense Against Social Engineering', 2002.

[11] ISO/IEC, 'Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems, ISO/IEC 9241-210:2019.', 2019.

[12] M. Ellen, Z. Z. Org, and R. T. Simon, 'User-Centered Security'.

[13] D. Feth, 'User-Centric security : Optimization of the security-usability trade-off', in *2015 10th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering, ESEC/FSE 2015 - Proceedings*, Association for Computing Machinery, Inc, Aug. 2015, pp. 1034–1037. doi: 10.1145/2786805.2803195.

[14] L. V. Casaló, C. Flavián, and M. Guinalíu, ‘The role of security, privacy, usability and reputation in the development of online banking’, *Online Information Review*, vol. 31, no. 5, pp. 583–603, 2007, doi: 10.1108/14684520710832315.

[15] P. Paškevičius and R. Damaševičius, ‘Design of Usable Interface for a Mobile e-Commerce System’.

[16] N. A. Bt Mohd and Z. F. Zaaba, ‘A review of usability and security evaluation model of E-commerce website’, in *Procedia Computer Science*, Elsevier B.V., 2019, pp. 1199–1205. doi: 10.1016/j.procs.2019.11.233.

[17] S. Aouragh, F. Kalinowski, K. Boudaoud, and K. B. Usability, ‘Usability and security of electronic voting systems’, p. 10, 2023, doi: 10.48545/advance2023-fullpapers-1_3ï.

[18] D. Brodić and R. Janković, ‘USABILITY ANALYSIS OF THE SPECIFIC CAPTCHA TYPES’.

[19] K. Rozinov, ‘Are Usability and Security Two Opposite Directions in Computer Systems?’

[20] A. Conklin, G. Dietrich, and D. Walz, ‘Password-Based Authentication: A System Perspective’, 2004. [Online]. Available: www.microsoft.com,

[21] D. Florencio and C. Herley, ‘A large-scale study of web password habits’, in *16th International World Wide Web Conference, WWW2007*, 2007, pp. 657–666. doi: 10.1145/1242572.1242661.

[22] L. F. Cranor and S. Garfinkel, *Security and Usablity: Designing secure systems that people can use.* 2005.

[23] V. Moraskar, S. Jaikalyani, M. Saiyyed, J. Gurnani, and K. Pendke, ‘International Journal of Computer Science and Mobile Computing Cued Click Point Technique for Graphical Password Authentication’, 2014. [Online]. Available: www.ijcsmc.com

[24] C. Katsini, M. Belk, C. Fidas, N. Avouris, and G. Samaras, ‘Security and usability in knowledge-based user authentication: A review’, in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Nov. 2016. doi: 10.1145/3003733.3003764.

[25] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, ‘User interface design affects security: Patterns in click-based graphical passwords’, *Int J Inf Secur*, vol. 8, no. 6, pp. 387–398, 2009, doi: 10.1007/s10207-009-0080-7.

[26] M. Swathi, M. V. J. Reddy, and I. Mtech, ‘Authentication Using Persuasive Cued Click Points’. [Online]. Available: www.ijert.org

[27] A. S. Albesher, ‘Reviewing the Usability of Web Authentication Procedures: Comparing the Current Procedures of 20 Websites’, *Sustainability (Switzerland)*, vol. 15, no. 14, Jul. 2023, doi: 10.3390/su151411043.
[28] S. Ma *et al.*, ‘An empirical study of SMS one-time password authentication in android apps’, in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2019, pp. 339–354. doi: 10.1145/3359789.3359828.

[29] A. Bakry, H. Ahmed, and M. S. Thesis, ‘Balancing Security and Usability in Web Single Sign-On’, 2020.

[30] S. Mamoudou and W. Al-Khateeb, ‘An Overview on Authentication Approaches and Their Usability in Conjunction with Internet and Mobile Applications’, 2014. [Online]. Available: www.ijera.com

[31] D. L. Huang, P. L. P. Rau, and G. Salvendy, ‘Perception of information security’, *Behaviour and Information Technology*, vol. 29, no. 3, pp. 221–232, May 2010, doi: 10.1080/01449290701679361.

[32] D. Cooper, ‘Psychology, Risk and Safety: Understanding how personality & perception can influence risk taking’, *Journal of the American Society of Safety Engineers; Professional Safety*. 2003.

[33] L. F. Cranor and N. Buchler, ‘Better together: Usability and security go hand in hand’, *IEEE Secur Priv*, vol. 12, no. 6, 2014, doi: 10.1109/MSP.2014.109.

[34] L. F. Cranor, ‘A Framework for Reasoning About the Human in the Loop’.

[35] T. L. Saaty and J. M. Katz, ‘How to make a decision: The Analytic Hierarchy Process’, 1990.

[36] A. Darko, A. P. C. Chan, E. E. Ameyaw, E. K. Owusu, E. Pärn, and D. J. Edwards, ‘Review of application of analytic hierarchy process (AHP) in construction’, *International Journal of Construction Management*, vol. 19, no. 5, pp. 436–452, Sep. 2019, doi: 10.1080/15623599.2018.1452098.

[37] T. L. Saaty, ‘A Scaling Method for Priorities in Hierarchical Structures’, 1977.

BIOGRAPHY

Inci KARAMAHMUTOGLU studied Computer Science Engineering Department at the Yeditepe University in Türkiye between 2018 and 2022. She graduated with a Bachelor's degree in Computer Science Engineering and after that she started a Master's Graduate School at Gebze Technical University in Türkiye in 2022. Additionally, she began working as a research assistant at the same university in 2023.

PUBLICATIONS AND PRESENTATIONS FROM THE THESIS

[1] I. Karamahmutoglu and M. Gokturk, "A Systematic Approach to Measure Usability and Security Trade-off," *2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Istanbul, Turkiye, 2024, pp. 1-4, doi: 10.1109/HORA61326.2024.10550727.

APPENDICES

APPENDIX-A: SURVEY QUESTIONS

Research Survey on Measuring the Balance of Usability and Security

Description of the Survey:

This survey is designed to gather information about participants' experiences, opinions, and intuition about the trade-off between the usability and security of a user interface (UI). The aim can be explained as determining the priority and perception of usability and security characteristics. In addition to this, your insights have a crucial role for not only shaping the research about balancing the usability and security relationship but also the future developments about user experience and reliability concepts.

Estimated Time and Privacy:

The questionnarie, which has 54 number of questions, will take about 30-40 minutes to complete. All answers will be taken anonymously and your personal information will not be shared anywhere.

Guideline:

- Please answer all questions based on your experience and intuition.
- In the end, take time to give additional feedback about the concept.

Contact Info:

If you have any concerns or questions about the survey, please contact with incikaramahmutoglu@gtu.edu.tr.

Thank you for your participation and time.

Section I - Demographic and Personal Experience Questions

Description:

This part is designed to estimate the personal knowledge, awareness, level of experience about usability and security subjects, and how this experience and intuition affected by given answers while creating statistic approach about the demographic distribution. These questions are general therefore, personal information that identifies you is not collected.

Estimated Time:

This part consists of *11 survey questions* and will last approximately 5-*10 minutes*.

1. Please select your age group. *

- ◯ 18 - 24
- ◯ 25 - 34
- ◯ 35 - 44
- ◯ 45 - 54
- ◯ 55 - 64
- ◯ 65 - 74
- ◯ 75+

2. What gender do you identify as? *

- ◯ Male
- ◯ Female
- ◯ Prefer not to say
- ◯ Other: _____

3. What is the highest level of education you have completed or your title? *

- ◯ Master's Degree
- ◯ Doctoral Degree (PhD)
- ◯ Assistant Prof. Dr.
- ◯ Associate Prof. Dr.
- ◯ Prof. Dr.
- ◯ Other: _____

3. What is the highest level of education you have completed or your title? *

- ◯ Master's Degree
- ◯ Doctoral Degree (PhD)
- ◯ Assistant Prof. Dr.
- ◯ Associate Prof. Dr.
- ◯ Prof. Dr.
- ◯ Other: _____

4. What is your primary field(s) of work or area of study? *

- ☐ Human-Computer Interaction
- ☐ Software Engineering
- ☐ Information Security
- ☐ Web Developer
- ☐ UX Designer
- ☐ Artificial Intelligence (AI)
- ☐ Computer Graphics
- ☐ Cybersecurity
- ☐ I am working as a developer at a company.
- ☐ Other: _____

5. What is your years of experience in this field? *

- ◯ Less than one year
- ◯ 1-2 years
- ◯ 3-6 years
- ◯ More than 6 year

6. Which of the following best describes the level of your user experience (UX) related knowledge in computer science? *

Choose ▾

7. Which of the following best describes the level of your security-related knowledge in computer science? *

Choose

8. When thinking about a user-friendly interface, what three criteria immediately come to your mind? (Please separate them with "-") *

Your answer

9. When thinking about a secure interface, what three criteria immediately come to your mind? (Please separate them with "-") *

Your answer

10. Have you ever experienced a security issue while using a web application? If yes, kindly provide details about the specific problem you encountered. If no, you can just type "No". *

Your answer

11. Have you ever experienced a usability issue while using a web application? If yes, kindly provide details about the specific problem you encountered. If no, you can just type "No". *

Your answer

Section II - Security Related Questions

Description:

In this section, security-related characteristics such as input validation and availability are covered. It aims to state the priority of given factors separately.

Estimated Time:

This part consists of *11 survey questions* and will last approximately 5-10 *minutes*.

12 (Input Validation). If the user interface contains a form that accepts user inputs, it should conduct input validation procedures. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

13 (The Principle of Least Surprise). The user expectancy and the provided security behaviour of the system should be matched. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

14 (The Principle of Good Security Now). The application should regularly monitor for emerging attack types and apply security patches as needed. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

15 (Attention). If a security-related operation requires user attention, it should not be easily disrupted by other operations. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

16 (Motivation). The user's motivation must be sufficiently high to determine the security issues within the provided user interface. In this context, motivation refers to the potential risks and losses involved. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

17 (Motivation). What type of loss primarily influences behavior of the user to be cautious while they are using an application? *

	Financial Loss	Motivation Loss	Loss of Data	Waste of Time	Intellectual Property Loss	Physical Property Loss	Personal Information Loss	Reputa Dama
1st Choice	○	○	○	○	○	○	○	○
2nd Choice	○	○	○	○	○	○	○	○
3rd Choice	○	○	○	○	○	○	○	○

18 (Integrity). When using any web application that gathers personal information, it's imperative to implement measures ensuring the use of secure encryption methods during data transmission over the network to maintain the integrity of this data. For example, verifying the reliability of its certificate and confirming the utilization of secure protocols like HTTPs. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

19 (Confidentiality). The customization of privacy and security settings within the application and control over visibility should be determined by the user to suit the preferences. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

20 (Availability). When conducting operations that require a sufficient level of security, such as financial transactions through online banking applications, the delay needs to be within an acceptable range. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

21 (Non-repudiation). The web application must log operations using digital signatures and timestamps to ensure non-repudiation. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

22 (Least Privilage). Access to any area of the application should be restricted based on the principle of granting the least privilege to the user. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

Section III - Usability Related Questions

Description:

The corresponding questions are only about usability characteristics such as convenient navigation. The goal of this part is to specify the priority of these factors to make a user interface user-friendly.

Estimated Time:

This part consists of *6 survey questions* and will last approximately 4-8 *minutes*.

23 (Ease of Learning). The application should be straightforward to use, allowing users to easily understand its layout and operational flow with minimal effort. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

24 (Task Efficiency). Once users get used to how to achieve their goals within a web application, they should be able to accomplish those goals within a reasonable amount of time compared to other similar applications. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

25 (Effectiveness). The interface should enable users to effectively achieve their intended goals. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

26 (Accessibility). The user interface should be designed to serve all individuals, including those with disabilities like color vision deficiency or visual impairment, ensuring accessibility and usability for everyone. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

27 (Efficient Navigation). In today's most user interfaces, navigation often involves traversing multiple pages to complete a task. As a result, the user interface should provide clear guidance throughout the process. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

28 (Responsive Design). The application should be designed to be compatible with various technological devices, ensuring adaptability. For example, it should seamlessly function on a smartwatch, mobile phone, or personal computer. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

Section IV - Both Usability and Security Related Questions

Description:

In this section, the focus is on exploring factors that measure both usability and security, acknowledging their potential interrelation.The purpose of this section is to determine the importance of the characteristics to make a system reliable and usable.

Estimated Time:

This part consists of *17 survey questions* and will last approximately 5-10 *minutes*.

29 (Ease of Remembering). Building blocks of the user interface need to be remembered easily even after a while without using it. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

30 (Error Prevention and Recovery). The user interface should minimize errors and guide the user through tasks without directly confronting them with errors. If somehow an error occured the system must recover from it. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

31 (Subjective Satisfaction). User interface give enthusiasm to the user and provide satisfaction during their interactions with it. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

32 (Consistency). The user interface must maintain consistency, ensuring that each word or symbol retains the same meaning throughout and avoids any ambiguity in its usage. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

33 (Feedback and Feed-forward). To establish a communication between user and ensure the visibility or comprehensibility of any interaction result, the system should provide signals and feedback to the user. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

34 (Minimal Coginitive Load). The user interface should present brief explanations and make efficient use of the entire screen to convey sufficient information to the user. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

35 (User-Centered Design). The user interface design needs to consider users and their requirements all the time. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

36 (Familiarity). The user interface should match with the real world and use familiar gestures, symbols, and icons. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

37 (Simple and Natural Dialog). As the majority of operations are technical from the user's perspective, dialogues between the application and user should be simple and easily understandable by all. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

38 (Knowledge and Skill). The user interface should be designed in a way that users from various level of knowledge and skills can use the application conveniently. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

39 (Visibility of System Status). In tasks with multiple stages, the user interface should visibly indicate completed stages and the user should receive updates on various aspects such as security issues and notifications. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

40 (Trust). The user interface should enhance the user's trust in the system. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

41 (Customization). The user should be able to adjust and personalize the user interface such as font-size, language, and color theme. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

42 (Task Focus). Users should be able to accomplish their primary goals without being disturbed by other tasks. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

43 (User Control). The control of the application should be given to the user. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

44 (Vigilance). The user interface should encourage users to remain vigilant and alert mode to detect any anomalies. *

	1	2	3	4	5	6	7	
Slightly important	○	○	○	○	○	○	○	Extremely important

45 (Authentication). The application should make sure that only valid users can access the system by implementing secure authentication mechanisms. *

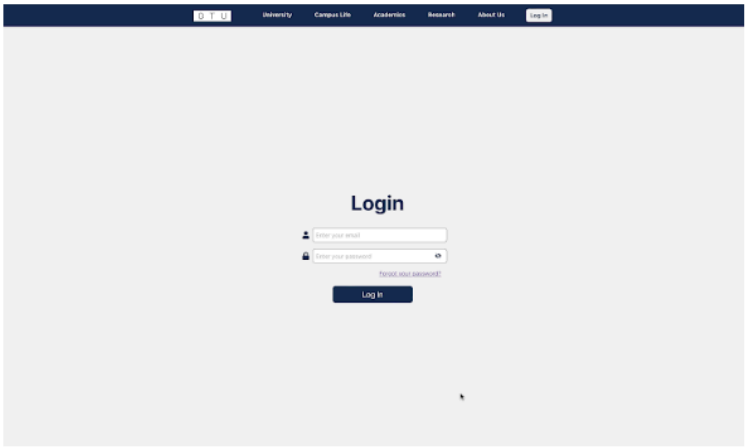
	1	2	3	4	5	6	7	
Sligthy important	○	○	○	○	○	○	○	Extremely important

Section V - Implemented Comparison Questions

Description:
Following two parts are created to compare characteristics of usability and security with visual and verbal aids, respectively. The objective is to gain insight about the absence of the characteristic and how it affects the interface.

Estimated Time:
In total, there are 6 *survey questions* and will last approximately 4-8 *minutes*.

Design 1

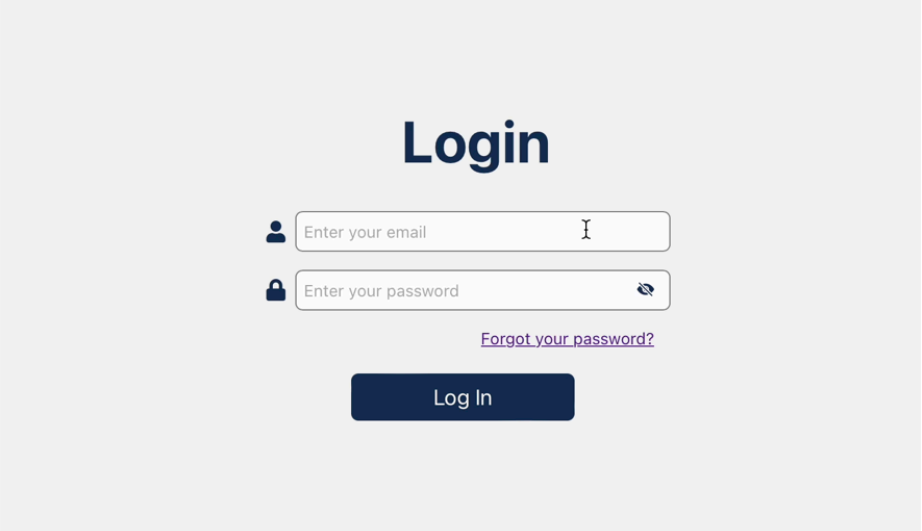


Design 2

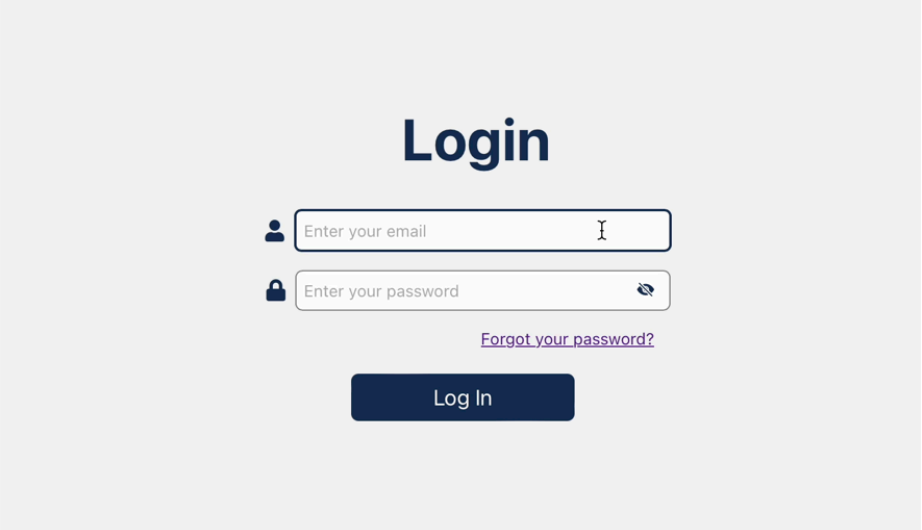
46 (Minimal Cognative Load). Please choose from the two designs that given above, selecting the one that you consider to be the better choice in terms of security and usability. *

- ◯ Design 1
- ◯ Design 2
- ◯ There is no difference between two design.

Design 1



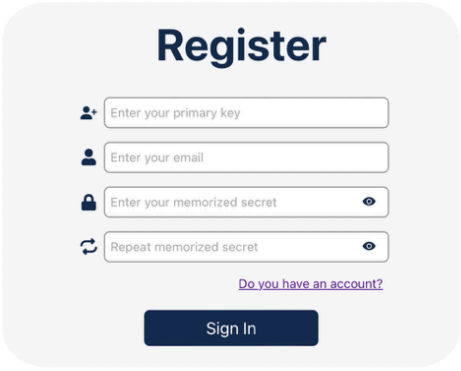
Design 2



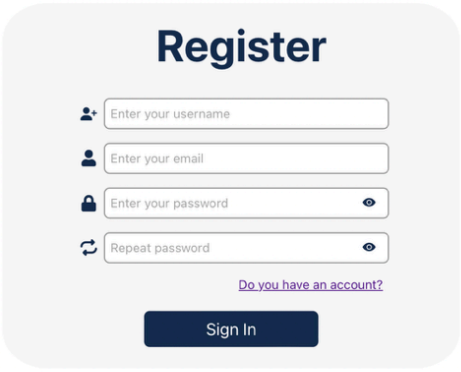
47 (Feedback and Feed-forward). Please choose from the two designs that given above, selecting the one that you consider to be the better choice in terms of security and usability. *

- ◯ Design 1
- ◯ Design 2
- ◯ There is no difference between two design.

Design 1



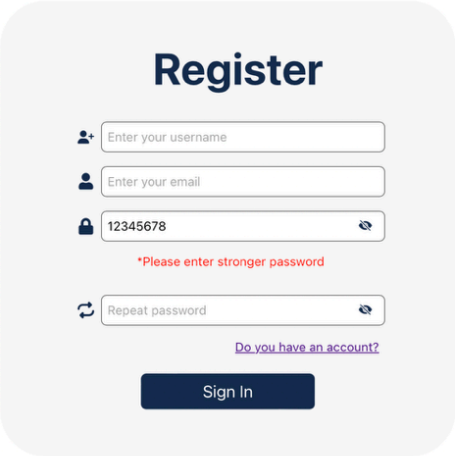
Design 2



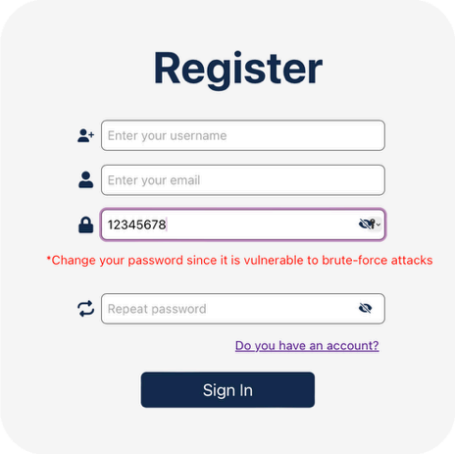
48 (Familiarity). Please choose from the two designs that given above, selecting the one that you consider to be the better choice in terms of security and usability. *

- ◯ Design 1
- ◯ Design 2
- ◯ There is no difference between two design.

Design 1



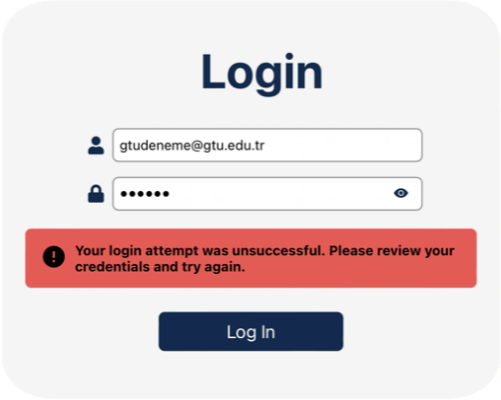
Design 2



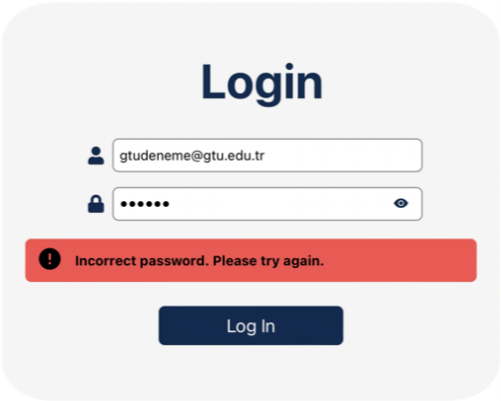
49 (Simple and Natural Dialog). Please choose from the two designs that given above, selecting the one that you consider to be the better choice in terms of security and usability. *

- ◯ Design 1
- ◯ Design 2
- ◯ There is no difference between two design.

Design 1



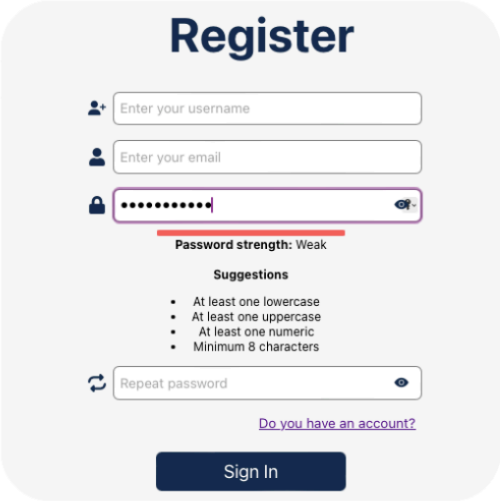
Design 2



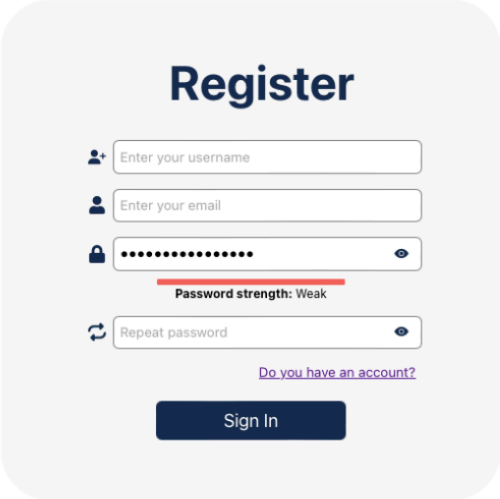
50 (Input Validation). Please choose from the two designs that given above, selecting the one that you consider to be the better choice in terms of security and usability. *

- ◯ Design 1
- ◯ Design 2
- ◯ There is no difference between two design.

Design 1



Design 2



51 (Feedback and Feed-forward). Please choose from the two designs that given above, selecting the one that you consider to be the better choice in terms of security and usability. *

- ◯ Design 1
- ◯ Design 2
- ◯ There is no difference between two design.

Section VI - Comparision Questions

Estimated Time:
In total, there are 3 *survey questions* and will last approximately 3-5 *minutes*.

52 (Trust - Customization). Creating a sense of uniqueness and capturing users' attention not only strengthens their bond with the application but also cultivates trust. While these criteria are interconnected, which do you perceive as more influential in terms of creating usability and security balance? *

- ◯ Trust
- ◯ Customization

53 (Efficient Navigation - Effectiveness). Clear instructions, such as micro-animations and navigation bars, effectively guide users toward achieving their goals. While these aspects are interconnected, which do you consider more significant in enhancing user experience? *

- ◯ Efficient Navigation
- ◯ Effectiveness

54 (Familiarity - Subjective Satisfaction). People tend to look for a sense of familiarity with interfaces that mirror their perception of the world. For instance, 3D illustrations offer a more interactive experience compared to flat surfaces, aligning with how individuals naturally perceive their environment. While both criteria are interrelated, which do you think more impactful in enhancing the user experience? *

- ◯ Familiarity
- ◯ Subjective Satisfaction

Section VII - Feedbacks

Description:

In this section, open-ended questions allow for feedback on the survey, as well as the opportunity to provide additional information that may influence the priority of characteristics related to usability and security.

Estimated Time:

It will last approximately 5 *minutes*.

1. Are there any additional characteristic of security that you would like to add? (If there is more than one characteristic, please separate them with "-")

Your answer

2. Are there any additional characteristic of usability that you would like to add? (If there is more than one characteristic, please separate them with "-")

Your answer

3. Did you encounter any difficulties throughout the survey?

Your answer

4. Please feel free to provide any additional feedback you may have. Your opinions are valuable to us.

Your answer