How to Educate an Organization in Working with Security Topics from a User Experience Perspective

Anna Dahlström and Felicia Gabrielii Augustsson

DEPARTMENT OF DESIGN SCIENCES
FACULTY OF ENGINEERING LTH | LUND UNIVERSITY
2023

MASTER THESIS

How to Educate an Organization in Working with Security Topics from a User Experience Perspective

Anna Dahlström
an7360da-s@student.lu.se

Felicia Gabrielii Augustsson
fe8534ga-s@student.lu.se

June 14, 2023

Master's thesis work carried out at
the Department of Design Science, Faculty of Engineering, Lund University.

Supervisor: Günter Alce, gunter.alce@design.lth.se

Examiner: Joakim Eriksson, joakim.eriksson@design.lth.se

How to Educate an Organization in Working with Security Topics from a User Experience Perspective

Published by
Department Design Sciences
Faculty of Engineering LTH, Lund University
P.O Box 118, SE-221 00 Lund, Sweden

Subject: Interaction Design MAMM01
Division: Ergonomics and Aerosol Technology
Supervisor: Günter Alce
Examiner: Joakim Eriksson

Abstract

In today's rapidly evolving society, the pervasive influence of technology has profoundly transformed various aspects of human life, presenting both unprecedented opportunities and critical security challenges. To mitigate the risks of data breaches, malicious attacks, and overall cyber threats, companies have taken proactive measures by providing education and training to their employees in the areas of cyber security and software security. However, these kind of educations are often considered unmotivating and are often skipped trough as quickly as possible, which is troubling since security is of great importance.

This master's thesis has therefore investigated how to educate an organization in working with security topics from a user experience perspective, to examine whether user centered design can aid in learning. Through the implementation of user research, which included a knowledge test, and the performance of a threat analysis, three specific security areas were identified. From the derived security areas an educational computer game was implemented, where each level focused on a security threat, keeping user experience and usability in mind when creating tasks.

By having two groups with ten participants in each, we let one group complete a traditional PowerPoint security education and one group play the game. Both groups took a knowledge test, consisting of various questions about security, immediately after completing the education as well as two weeks afterwards. This resulted in better results for the group who played the game. The final conclusion was not only that experience based on usability and gamification do aid in learning, but also that deeper learning concerning security also benefits from learning with the use of a digital, interactive tool compared to traditional learning.

Keywords: User centered design, threat analysis, security, experiential learning, gamification, interactive learning tool, the design process

Sammanfattning

I dagens snabbt föränderliga samhälle har teknologins inflytande djupt förvandlat olika aspekter av människors liv och medför både stora möjligheter och kritiska säkerhetsutmaningar. För att minska riskerna för dataintrång, skadliga attacker och övergripande cybersäkerhetshot vidtar företag proaktiva åtgärder genom att erbjuda utbildning och träning till sina anställda inom områdena cybersäkerhet och mjukvarusäkerhet. Dock anses dessa utbildningar ofta som oengagerande och oftast hoppas dessa över så snabbt som möjligt, vilket är oroande då säkerheten är av stor vikt i dagens teknikvärld.

Därför har denna masteruppsats undersökt hur man kan utbilda en organisation i att arbeta med säkerhetsämnen ur ett användarperspektiv för att undersöka om användarcentrerad design kan underlätta inlärning. Genom en användarundersökning, bestående av bland annat ett kunskapstest, och genomförandet av en hotanalys, identifierades tre specifika säkerhetsområden. Utifrån dessa säkerhetsområden implementerades ett datorspel i utbildningssyfte, där varje nivå fokuserade på ett säkerhetshot. Vid implementeringen var användarupplevelse och användbarhet i fokus.

Två grupper, med tio deltagare i varje grupp, genomgick varsin säkerhetsutbildning. En grupp genomförde en traditionell PowerPoint-baserad säkerhetsutbildning medan den andra gruppen spelade datorspelet. Efteråt genomförde båda grupperna ett kunskapstest, bestående av olika frågor om säkerhet. Tested gjordes både direkt efteråt, samt två veckor efter att utbildningen hade genomförts. Detta resulterade i en bättre prestation för gruppen som spelade spelet. Den slutliga slutsatsen var inte bara att erfarenheter baserade på användbarhet och gamification underlättar inlärning, utan också att djupare inlärning inom säkerhet även gynnas av att använda ett digitalt, interaktivt verktyg jämfört med traditionell inlärning.

Nyckelord: Användarcentrerad design, hotanalys, säkerhet, upplevelsebaserat lärande, gamifiering, interaktivt lärandeverktyg, designprocessen

Acknowledgements

We would like to thank Günter Alce for his astonishing support trough this master's thesis. Not only have he given us quick, relevant and thorough feedback but has also helped us when we had questions and worked as a sounding board for our ideas.

We would also like thank Erika Avenberg and Maria Ekström for their guaidance and viewpoints as Acme representatives. We would also like to say a big thank you for the opportunity of visiting the German office to futher substansiate this thesis.

To all participants and test persons, we are grateful for your participation and help. Without your contribution this study wouldn't have been possible.

Last, but not least, we would like to send a big thank you to all the people helping us trough our five years of studying, partying and crying. You know who you are!

Contents

Chapter 1
Introduction

The aim of this chapter is to give an insight of this thesis's background, research questions, and limitations. The fictional tech company Acme is described and explained to give an understanding about the organization. For this master's thesis some related work has been studied, within different fields to gain knowledge about methods, get inspired and create a stable foundation of what research questions already have been discussed.

1.1 Background

The digital revolution is growing at an immense speed and extent. The ever growing number of devices, data and interactions with technology open the world to new possibilities. However, this is true for malicious attackers as well. The costs of data breaches and attacks are expected to reach a value of about $10.5 trillion every year by 2025, a 300 percent increase from 2015 levels [1]. The situation acts as a threat towards both individuals and companies, with organisations world wide spending about $150 billion in 2021 on cyber security, growing by approximately 12.4 percent each year [1].

It is clear to see that security and safety is a growing, urgent area of concern for organisations world wide. Although software services and systems can provide a good base layer of security, the human part of interactions is an important aspect not to overlook. For security systems and protocols to work as intended, and subsequently live up to the level of security they claim, they need to be used, and used correctly. This is based on the adoption that the user understands *how* and *why* they should use the security procedures in question. According to Verizons yearly Data Breach Investigations Report[43] of 2022, 82% of the thousands of analyzed breaches involved the human element, including social attacks, errors and misuse [43]. These numbers are frightening, yet they speak a clear language. Educating employees when it comes to security is of the outmost importance to secure the well being of both individuals and a company as a whole.

Based on this situation, we want to investigate how one can educate an organisation in regards to security, and use a user centered design method to ensure an enjoyable user experience that promotes learning. This will be done by creating a security based and interactive game to aid learning. By extracting common game elements and drivers that are motivating

within games we will create a capture the flag (CTF) based solution where the users will learn about critical security topics.

1.2 Acme

Acme is originally a fictional corporation used in cartoon movies and has since then been used when a company name is needed without advertising/promoting a specific company. However, in this report it will be the name of the company at which we are conducting our thesis, which wishes to remain anonymous. In this case Acme is a global tech company with around 400 000 employees world wide, of which around 300 of them are based in Lund. The team in which this master's thesis was conducted mainly consist of technically proficient people, most of them being software developers and does not work with security issues on a daily basis.

1.3 Purpose and Goals

For this master's thesis we have a set of goals and research questions. As previously mentioned, the main concept of this master's thesis is to investigate how one can educate an organisation within security using a user centered design, and we have therefore listed a few goals to aid us in that work. The research questions helps in defining the scope of the research and keeps the investigation on track.

1.3.1 Overall Goals

- Create a solid knowledge based on relevant literature in regards to the subject of security, usability and learning
- Analyze security risks at a global tech company
- Perform user research
- Create at least one conceptual design and lo-fi prototype
- Create a hi-fi prototype and iterate it
- Test all prototypes and evaluate during iterations
- Summarise, compare and evaluate our findings

1.3.2 Research Questions

- Which are the biggest software security risks at a global tech company?
- How can a user experience based on usability and gamification aid in learning?
- How can you achieve a higher level of learning with the use of a digital, interactive tool compared to traditional learning in regards to software security?

1.4 Global Goals

All United Nations Member States adopted, in 2015, a Sustainable Development agenda for 2030 [36]. It consists of 17 goals for peace and prosperity for the world's population, and the planet and its future. This includes ending poverty, improving health and education, reducing inequality and promoting economical growth, but also working on stopping climate changes.

The ambition for this master's thesis is to improve the security education throughout employees work life. This corresponds well to goal no 4 *Quality Education*, which is shown in figure 1.1. This goal promotes lifelong learning opportunities for all [35]. Cyber security is in constant advancement and is something that needs to be taught on a regular basis. Further, we also cover *Industry, Innovation and Infrastructure* including building resilient infrastructure, promoting inclusive and sustainable industrialization and fostering innovation [34], which can be seen in figure 1.2. Another hope is to inspire innovations regarding education, making it more motivating and fun to learn. Moreover we want to show that one can learn security topics by playing a game and hopefully pave the way for new and similar ideas.

Figure 1.1:
Global goal no 4

Figure 1.2:
Global goal no 9

1.5 Limitations

For this thesis there are a few limitations that has to be taken into consideration. Since Acme is a world wide tech company there are many different system in use, making it difficult to analyze all potential threats to all systems in the scope for this master's thesis. Therefore, we have chosen to focus on Microsoft Teams and Outlook, which are used globally by all teams at Acme. Moreover, since it is a tech company, almost all teams are using some kind of version control platform, and in this case it will be Bitbucket. However, the exact platform is not of significance, since it is the usage of such a platform and what threats it enables, that will be analyzed. Further, for the scope of this thesis, not all threats that will be found will be taken in to consideration. Not only because of the time limit to create the educational game, but also to be able to focus on specific aspects to ensure the quality and depth of those areas.

Which threats that will be taken into consideration, and how these will be derived will be further explained and discussed in section 3.3.

Throughout this report we will refer to our solution as a game. However, we will develop a solution where we will use gamification, i.e. apply game elements to, in this case, a security education, and will not develop a game per se. However, to make it easier and more clear for readers throughout this report, the solution will be referred to as a game.

1.6 Related Work

Yonemura et. al. [45] used gamification as a method to measure the outcome from comprehensive security training compared to security games in regards to security skills by educating Operational Technology security on college students using a game based on Gamification theory. The aim of the game was to, in a fun way and short period of time, teach the basics of cyber security. Yonemura et. al. came to the conclusion that gamifying security education makes it possible for engineers to practice the countermeasures to similar security incidents that could occur in real life [45].

Yet another study that is of relevance for our work is Li and Zhao's study [29]. Not only are they bringing up current information about educational games but has also come to the conclusion that the balance between education and playfulness is the key to a successful educational game [29].

Further, there are also work that suggest that security within organizations has to be enhanced. Leache [27] claims that as a result of poor security education that bore its audience, many threats to a organisation are internal and are caused by employees or users [27].

These sources of related work are of interest for our study, partly since some of them lies close to this master's thesis work, but also since relevant methods are presented which we could use in our own work.

Chapter 2
Theoretical Background

The aim of this chapter is to give the reader a foundation of theories that has been used throughout this thesis, to ensure that the user has a knowledge base of relevant subjects, concepts and terms. Three main focus areas will be presented throughout the chapter; software security & and threats, gamification & learning, and design theory.

2.1 Threat Modeling

Threat modeling is the process of identifying, communicating and understanding potential threats and mitigations [10]. A threat model is a way to represent aspects that might harm the security of a system and is used to improve the security of that system [12]. Threat modeling can be completed on various kinds of systems, among software applications, networks, and Internet of Things devices.

In more detail, a threat model generally includes a description of the subject to be modeled to get a deeper understanding of the system. From that, potential threats, attack goals, and aspects that could be challenged in the future are distinguished. Not only does threat modeling identify threats but also which threats that are more likely and what impact they might have on the system [11]. From those threats, security requirements that are of importance for the system are defined which finally results in what action could be made to mitigate threats [11]. Moreover, threat modeling allows for informed decision-making and possible security improvements to the design of the system.

There are several different tools and frameworks that could be used for threat modeling. For this thesis the STRIDE and DREAD models were used to not only define security requirements and potential actions based on threats, but also to gain understanding of how big of an impact the threats were. STRIDE has been criticised [28], especially for being cross-correlated, meaning that some of the threats STRIDE process imply each other. Diverse threat modeling are not necessary contradictory and thus can multiple models be applied to the same organisation [11]. Therefore, we have decided to use both STRIDE and DREAD to cover more aspects in this threat assessment, and this choice of method will be further discussed in the chapter 7.

2.1.1 STRIDE

STRIDE was developed by Microsoft security engineers Loren Kohnfelder and Praerit Garg in 1999 [25]. STRIDE is an acronym and stands for **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service (DoS), and **E**levation of Privilege [19]. These threats originates from the properties they violate; authenticity, integrity, non-repudiation, confidentiality, availability and authorization [41]. For each kind of threat the ambition is to discover what potential breaches exists, what could happen and what actions could be taken to mitigate the threats. Each STRIDE attack is described in more detail below, based on Shostack's *"Threat Modeling: Designing for Security"*.

Spoofing is to pretend to be someone other than yourself. An attacker can for example spoof a person by gaining access and taking over a person's account. It is also possible to spoof files by creating new and changing already existing files and let those files "pretend" to be real and valid files.

Tampering is to modify a system's components to change the systems behaviour or create damage. Tampering can be anything from changing data in a document or modifying a database to changing a configuration file.

Repudiation is when a person denies their actions or take no responsibility for what they have done. This can for example be that someone claims not to have clicked on something, or didn't receive a certain email.

Information Disclosure concerns allowing people to access information to which they are not authorized to access. A process can leak memory addresses and permissions to certain data can be set improperly.

Denial of Service (DoS) is an attack which hinders non-malicious users to use a resource. This can be done by absorbing all the CPU or memory, sending too many requests to the resource to slow down the system or consume all the network resources.

Elevation of Privilege is when a person or program gains access and permissions to a system to which they are not authorized. For example, a user could execute code as an admin, or allow a person without privileges to run code.

Analyzing different parts of a system from the six threats will aid in finding potential breaches and what effects they could have.

2.1.2 DREAD

DREAD is a quantitative threat model [14], and alike STRIDE is also used for risk assessment [28]. DREAD is also an acronym and stands for **D**amage Potential, **R**eproducibility, **E**xploitability, **A**ffected Users, **D**iscoverability [11]. Each of these categories are analyzed and potential risks are rated on a scale from one to three. Below are each category briefly described.

Damage Potential analyzes how much damage an attack could possibly cause [11]. This is done to understand the potential harm the threat is causing [11].

Reproducibility identifies how easy it is to replicate an attack [14]. It specifies if the attacker is able to create an attack that affects the systems every time, or are there more misses than hits when launching the attack [28].

Exploitability determines how much effort and resources that is needed to initiate the attack [14, 11, 28]. If the attacker can do it anonymously and still get access, the exploitability is high.

Affected Users is decided from estimating the number of users that is exposed to the threat [14, 11]. If all users of a system is affected by an attack the number of affected is high, and if only a few are affected it is considered to be fairly low [28].

Discoverability considers whether it is easy for an attacker to detect security breaches or whether it is required to know the system in detail to find potential vulnerabilities in the infrastructure [14, 11, 28].

Table 2.1: Table showing grading criteria for each category in DREAD [30]

	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

From the grading criteria in table 2.1, the threat is graded from one to three. The grades from the five criteria are then summarized and will result in a total grade ranging from five to fifteen. If the grades fall in the range of 5-7 it is considered as a low risk, if it is between 8-11 it is a medium risk, and if it results in 12 or higher it is a high risk. David LeBlanc means that it can be hard to distinguish how to grade one criteria if there are only small differences between the grades [28]. When concluding the DREAD analysis it will be kept in mind that the grading is based on a human estimation and can include subjective differences.

2.2 Further Threats and Attacks

STRIDE and DREAD do not cover all potential threats and attacks. Not all threats and attacks are of interest, due to the limitations and scope of this master's thesis. However, in this sections a few more possible attacks are described.

2.2.1 Social Engineering

Social engineering is defined as

> *...the 'art' of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated [16].*

It is hence a term to describe malicious activities achieved trough human interactions. Examples of social engineering are baiting, scareware and phishing. However, one of the most common social engineering threats are phishing, which is described in the following paragraph.

2.2.2 Phishing

Phishing is a type of social engineering where the attacker sends spoofed emails [33]. The aim is to gain personal information from the user. The attacker could send an email to a user with a link to a website that looks legitimate, deceiving the user into visiting the fake website and entering the user credentials. The attacker collects the users credentials from the illegitimate website which the attacker can use to gain access to the original website. Phishing is a type of spoofing. The attack is illustrated in figure 2.1.

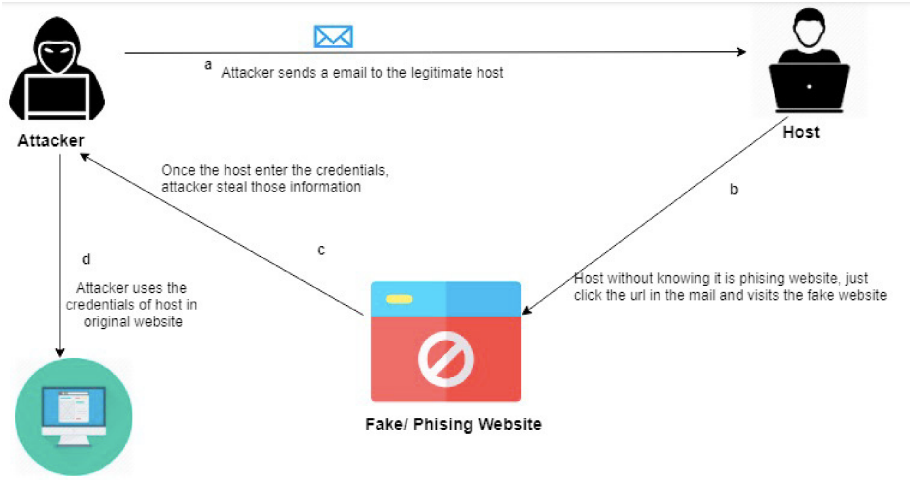


Figure 2.1: Phishing attack [33]

2.2.3 Man-in-the-middle Attack

Man-in-the-middle attack is a cyber attack where a malicious person listens in on, and potentially alters, the communication of two parties who think they are communicating directly with each other [8]. The man in the middle can for example make individual connections with the two parties and pretend to be the person they intend to communicate with, while the man in the middle actually controls the entire communication between them all [44].

2.3 Learning and Gamification

One of the theories within the field of educational learning is experiential learning. This theory describes learning from the viewpoint of experience, and how we from experience form knowledge. Since we want to create a gamified experience for users with the goal to educate them, we believe this theory is relevant for our work. Further, the section will present the gamification design which is human-focused, in contrary to function-focused design [23].

2.3.1 Experiential Learning

In 1984 David A. Kolb published *Experiential learning: experience as the source of learning and development* [26], in which he presents his theory about experiential learning. The theory is closely related to the work of three previous approaches to learning as described by Kolb; The Lewinian model of Action Research and Laboratory training, Dewey's model of Learning and Piaget's model of Learning and Cognitive Development, and serves as a differentiation to more classical perspectives of learning based on behavioral and rational idealist epistemology theories [26]. Experiential learning emphasize the role of experience in regards to learning, focusing on the importance of subjective experiences and consciousness rather than acquisition and recall. Despite this, Kolb points out;

> *It should be emphasized, however, that the aim of this work is not to pose experiential learning theory as a third alternative to behavioral and cognitive learning theories, but rather to suggest through experiential learning theory a holistic integrative perspective on learning that combines experience, perception, cognition, and behavior.*

Furthermore, Kolb presents main characteristics of experiential learning. He describes ideas as something that is constantly formed and re-formed by our experiences, and concepts are derived from this constant modification, resulting in learning. Hence, learning represents our historical record, not knowledge about the future. The knowledge that a person derives is then continuously tested in the experiences of the person. This also suggests that learning is a tension- and conflict-filled process, where knowledge is achieved by confrontation between four modes within the theory of experiential learning. To effectively learn, one needs four kinds of abilities; concrete experience abilities (CE), reflective observation abilities (RO), abstract conceptualization abilities (AC), and active experimentation (AE) abilities. The first ability is to be able to involve oneself entirely, openly, and with no bias in new experiences (CE). The second is to be able to observe and reflect on experiences from many perspectives (RO). Third is the ability to create concepts that transform observations into logically sound theories (AC), and lastly one must be able to utilize these theories for decision-making and problem-solving (AE). The circular relationship between these four modes can be viewed in figure 2.2.

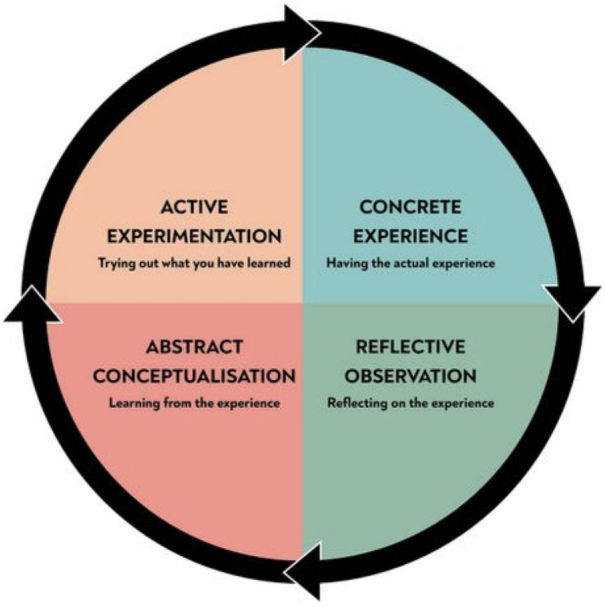


Figure 2.2: Kolb's cycle of experiential learning

Furthermore, experiential learning is a holistic approach to the human learning mechanism, taking into account both thinking, feeling, perceiving and behaving. Kolb views learning as **the** basic process of human adaption, making it the foundation for more specialized adaptions such as problem solving, decision-making and attitude changes. When learning is viewed as a holistic and adaptive concept, it highlights learning as a lifelong, continuous process. Experiential learning describes knowledge as the result of a transaction between objective social knowledge, the collective knowledge from previous human experience, and

the individuals subjective personal knowledge, gained from life experiences. Hence, Kolb explains, we must understand learning to understand knowledge, and understand knowledge to understand learning. Since the relationship between learning and knowledge are so tightly connected, both an epistemological and psychological approach is needed to understand these concepts [26].

Kolb sums up his theory in the definition;

> *(Experiential) learning is the process whereby knowledge is created through the transformation of experience.*

He states that this definition highlights multiple important aspects of the theory. It puts the emphasis on the process of adaptation and learning as opposed to content or outcomes, and focuses on knowledge as a transformation process, continuously being recreated. It also states that learning transforms both subjective and objective experience, and that one must understand learning to understand knowledge, and vice versa [26].

2.3.2 Gamification

Gamification refers to extracting motivating components from games and applying them to real-world problems and situations, and thus the human motivation is emphasised [23]. The main idea of gamification is not only to motivate people to learn, but it is also suggested that it promotes learning, engagement and the ability to solve problems [42]. Different types of games can be gamified, such as war games, simulations games, serious games and Alternate Reality (AR) games [24]. For this thesis gamification of a simulation and serious game will be in focus.

Simulation game reflects real world situations and can be used for education [24]. This type of game has been used in areas such as financial management, accounting, marketing and sales to improve performance within those fields. The hope for this master's thesis is to gamify and simulate a situation where an employee of Acme could learn new skills.

Serious game is developed for educational purposes, and is not developed purely for entertainment [24]. A serious game applies the motivational advantages to train and teach its users, and can for example be used by corporations for educational purposes. This is of relevance for this master's thesis where one of the main goals is to teach the subject of security.

2.3.3 Capture the Flag Games

Capture the Flagm (CTF) is, within the area of computer security, an exercise in which "flags" are purposely hidden in applications and/or hardware. The player's task is to retrieve flags by finding the weak spots in the security of the system in question [21]. Capture the Flag games usually uses a website or program to submit answers, flags or secrets to advance in the game. However, the actual actions or game elements often take place outside from the CTF web page. An example is where the player is asked to find a secret within the computers file system, application or webpage, and when the secret is found it is entered in to the CTF web page.

Root the Box is an open source framework based on a CTF functionality [13]. The framework is adaptable and combines a game-like environment with tasks based on real life security risks in order for the users to learn about realistic scenarios. The framework is built using mainly Python, Javascript and HTML [13].

2.3.4 The Octalysis Framework for Gamification

The Octalysis Framework for Gamification is designed by Yu-kai Chou, and its main purpose is to help create fun games [23]. Chou suggests eight Core Drivers that motivates people and has from them created the Octalysis Framework to use when designing games. Each driver is described in more detail below, according to Chou's description, and can be viewed in figure 2.3.

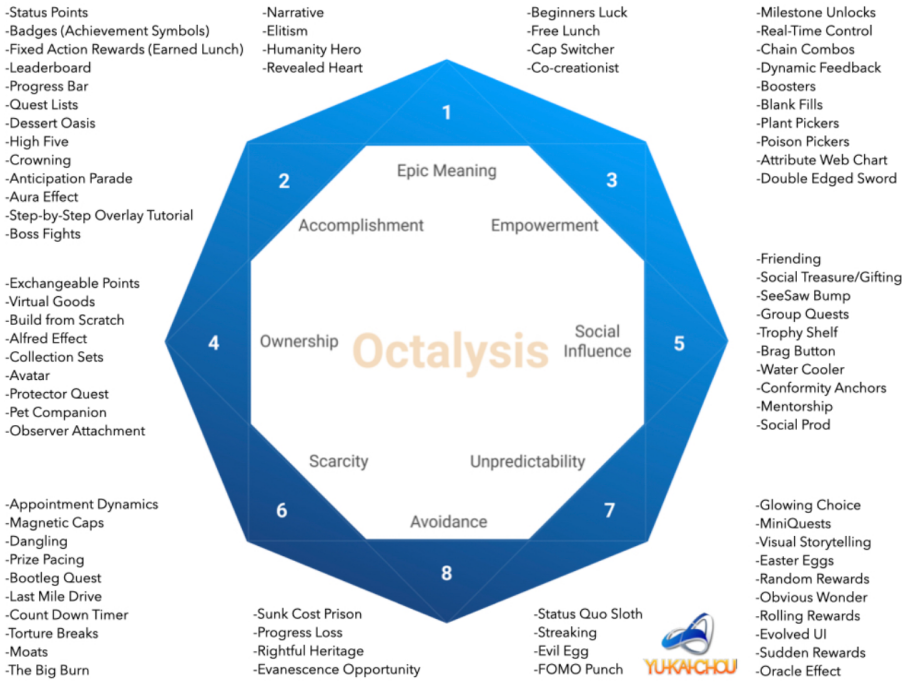


Figure 2.3: The Octalysis Framework for Gamification [23]

Epic Meaning & Calling is when players of a game think they are doing something greater than them self to help a community, e.g contributing to Open Source projects. This driver is also connected to beginners luck where a people believe they have abilities that others do not, motivating them to continue playing the game.

Development & Accomplishment drives people into developing their intelligence within the field to try to overcome challenges. A leaderboard motivates people to continue fighting for the first place and hence also develop their competence to be the best.

Empowerment of Creativity & Feedback drives people since they are engaged in a creative process where they have to try different ways to be able to find a solution.

Further, this way people also receive feedback since they see what works and what doesn't work with different approaches.

Ownership & Possession is when people feel responsible for what they own and want to expand what they own and make it better. It drives people to collect pieces of a puzzle or customize their avatar to make it their own.

Social Influence & Relatedness includes all potential social elements e.g. mentorship, acceptance, social responses as well as competition. By comparing your work to a co-players you become driven to perform better than that player. This driver also includes the motivation of being able to relate to people, places and things.

Scarcity & Impatience is when you are longing for something you can't currently have. This can be projected in a game where you have to wait to be able to try again, or to get your reward.

Unpredictability & Curiosity engages the player of a game to think more of it, since they are unable to predict the future. This is not only a common element in games, but also in movies and books making people interested in what comes next.

Loss & Avoidance is the driver that makes people try to avoid bad things happening. This can for example be the avoidance of losing progress or dying in a game.
Chou states that it is not a necessity for a game to meet all these eight Core Drivers to be considered a good game. It is rather better to focus on a few and implement those well when designing games [23].

2.4 Design Theory

This section describes the theories and methods on which we will base our overall methodology. However, these theories will be used as a foundation for our work, and some slight modifications will be done to accommodate our overall goals and research questions, as well as the limitations of the study.

2.4.1 The Interaction Design Process

Interaction design is a term used to describe a large area of techniques, methods, and activities. The main purpose of the process of Interaction Design is to find requirements, create designs based on these requirements, build prototypes from the designs, and review them. The focus during all of these stages remain on the user and their needs and wants in regards to the product that is being designed. The process is iterated until a satisfactory product is achieved. These four areas can be referred to as the Four Basic Activities of Interaction Design [39], and are visualized in figure 2.4.

Discovering requirements for the interactive product. The first step is to gather information about the product that is to be developed. This involves gathering an understanding about the users of the product, their wants and needs, what value the product can bring the user, and in what context the interaction will take place. Examples of activities that can be performed during this step is different kinds of user research , for example surveys, and the creation of personas, see section 2.4.3. The result from this step makes up the foundation for upcoming design and development.

Designing alternatives that meet those requirements. The aim of this step is to suggest designs based on the produced requirements. This step includes both conceptual and concrete designs, where the former focuses on the overall abstract solution that the product offers, and the latter explores precise design alternatives in regards to colors, symbols, images etc. Examples of activities that can be performed during this step is Brainstorming and the creation of an Conceptual design, see section 2.4.3.

Prototyping the alternative designs so that they can be communicated and assessed. The prototyping activity seeks to materialize the designs that are previously created. One of the foundational principles of interaction design is user tests, and producing different types of prototypes is an efficient way to facilitate such tests. A prototype gives the user a feel for both the functionality and the design of a product. This can be done by simple prototypes made of paper that visualize the overall design, often referred to as lo-fi prototypes. Lo-fi prototypes have a low creation cost and can be sufficient in identifying problems in the early stages of design. In contrast to lo-fi prototypes there is hi-fi prototypes. Hi-fi prototypes are often created in the later stages of the design process, where the aim is to substantiate many aspects of the design, including functionality, navigation and visual design. A hi-fi prototype is often created by using some kind of software. Apart from the creation of lo-fi and hi-fi prototypes, one can also perform cognitive walkthroughs at this step, see section 2.4.3

Evaluating the product and the user experience it offers throughout the process. The purpose of an evaluating activity is to determine the usability and acceptance of a product, based on previously placed goals. This is not to be confused with tests that establish quality assurance for the product, although it contributes to the fullfillment of such tests [39]. An example of an activity that can be performed during this step is user testing, which can be performed via observations, interviews or surveys, see section 2.4.3.

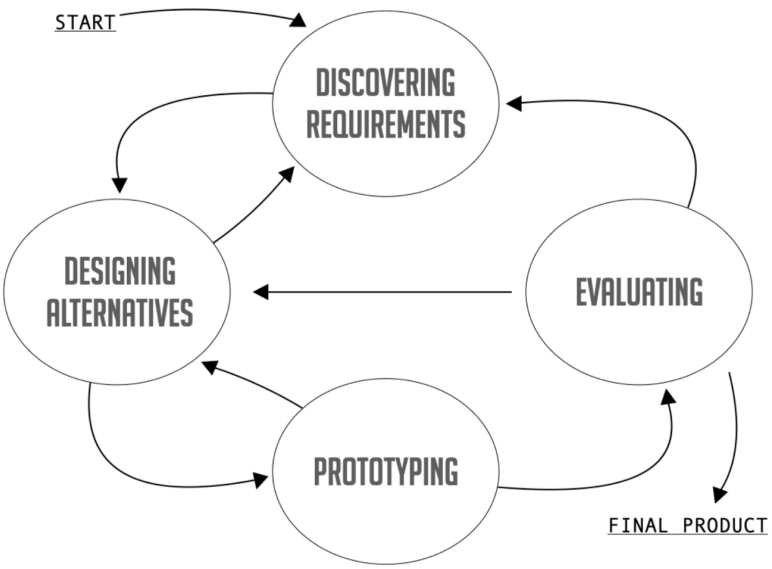


Figure 2.4: The simplified life circle of interaction design[39]

2.4.2 User Centered Design

User Centered Design (UCD) is founded on three main principles, formulated by John Gould and Clayton Lewis [17] in 1985 during the early stages of the creation of the field of Human Computer Interaction (HCI). The principles are; Early focus on users and tasks, Empirical measurement, and Iterative design. Together they form a basis on which useful and easy-to-use designs can be created [39].

The first principle, early focus on users and tasks, evolves around studying and understanding the users of the system. This is done by observing their characteristics by examining their behavior while performing tasks as well as the nature of these tasks. This involves using the users' tasks and goals as the main driving force of the development, and ensuring the system is designed to support these tasks in their natural context. The principle also includes the involvement of users throughout the entire design process, from the early creations of use cases and conceptual designs to final evaluations of the system. This means that all design decisions are based on the context of the users, their activities, and the environment in which they are executed.

Empirical measurement is the second UCD principle. This principle highlights the need to empirically investigate and evaluate users actions and reactions in all stages of the design process. When feasible, one should set up concise goals when it comes to usability and user experience in the early stages of development. These goals can then later serve as a guideline and deciding factor when making design choices, and act as a blueprint to evaluate empirical tests of the product during all stages of the process.

The third and last principle consists of iterative design. Based on the empirical measurements found during user tests, new designs are created that improves the usability issues that were highlighted during testing. The new design is then tested and evaluated again to see how the new fixes are perceived by the users. This loop is then repeated as many times as needed, resulting in an iterative process driven by feedback, searching for a user friendly design that meets the goals of the user.

Further, Dhandapani [9] states that software progress towards the point where the user can customize and assemble their own product, which then causes the UCD to be more crucial in product development. The two processes, UCD and software development, have to go hand in hand, according to Dhandapani. This is of relevance for our work since we are going to use the Root the Box framework where we are going to use software to build our own game, focusing on user experience.

2.4.3 Usability Strategies

This subsection will explain the different methods and techniques that will be used in this project in regards to producing and evaluating our solutions. This part of the report can preferably be used as a dictionary by readers not familiar with the concepts of interaction design and usability evaluation.

Surveys are one main way of performing usability evaluations, and are a proficient way of reaching many respondents. Surveys can be performed during all stages of the design process, but it can preferably be used to get an understanding of the user segment early on in the process. Surveys can be performed in many different ways such as online surveys and telephone interviews. They collect quantitative data that can result in useful statistics. However, the language use in surveys is very important, since one wants to make sure all users perceive the questions in the same way [22]. The construction of the questions within a survey can vary.

One common technique is to use Likert scales. A Likert scale is a scale where the participant rates their agreement or disagreement to a statement. Likert scales usually take the form of a five- or seven-point scale [22]. When designing a Likert scale, three main steps should be carried out. The first is to gather a collection of short statements about the product that is being tested, based on what you want to investigate. The statements should be of the character that one can agree or disagree with the statement. A brainstorming session can be one way of gathering such statements(see more at paragraph 2.4.3). Step two is to decide on a scale to use, including how many points the scale should have, if it should be continuous or discrete, and how it should be represented. The last step is to finalize what questions should be included in the questionnaire, and make sure they are clearly formulated [39].

One example of a concrete implementation of a Likert scale is the NASA Task Load Index (NASA TLX) [38]. NASA TLX was created by NASA as a way to measure the subjective workload assessments for different tasks involving interaction with human-computer interfaces. The survey originally consists of two parts. The first part consists of a survey with six different sub-categories, each having a statement and corresponding Likert scale for the user to answer. The second part of the survey is an individual weighting of the mentioned six sub-categories, where each one is compared to the others, and the most relevant aspect for the task is chosen and given a score of 1 if chosen, and a 0 if not. This weighting is then summarized for each individual sub-category and multiplied by the rating of each sub-category. The mean of all categorise is calculated to create an overall task load index for the task, resulting in a score from 0-100. However, many researchers today choose to only perform the first part of the NASA TLX to minimize the risk of measurement errors. When conducting a NASA TLX test, the test participants inherently introduces measurement errors to the results. The reproduction of these errors during the pairwise weighting and calculating of the

final score has been proven to reduce the reliability of the scale. Because of this, it is accepted to only perform the first part of the NASA TLX [4]. The scale was created by Sandra Hart for NASA in the 1980's, and is a generally accepted and tried method in many fields [38]. A picture displaying NASA TLX can be seen in figure 2.5.

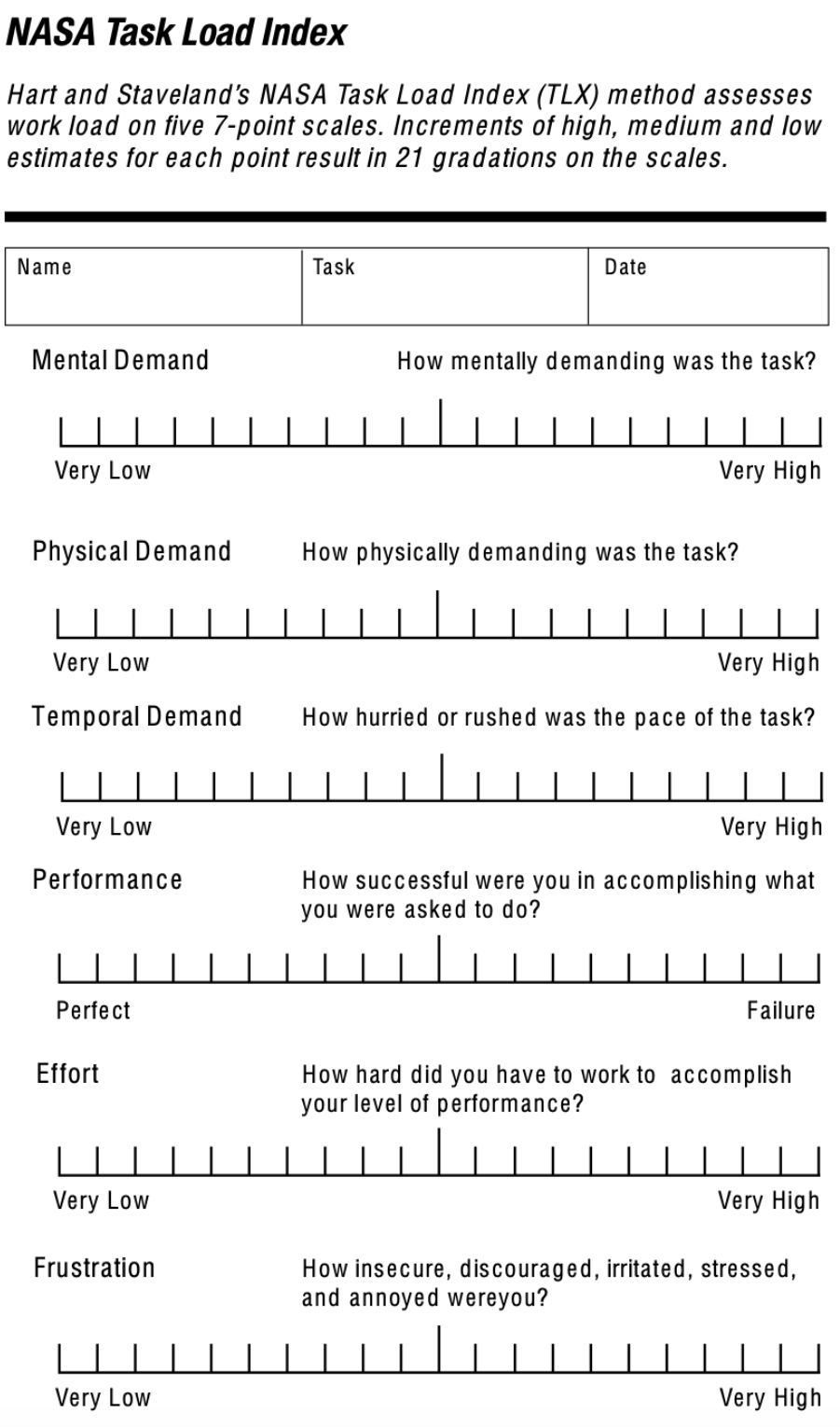


Figure 2.5: The official NASA Task Load Index

Table 2.2: User Experience aspects, desirable and non-desirable [39]

Desirable aspects		
Satisfying	Helpful	Fun
Enjoyable	Motivating	Provocative
Engaging	Challenging	Surprising
Pleasurable	Enhancing sociability	Rewarding
Exciting	Supporting creativity	Emotionally fulfilling
Entertaining	Cognitively stimulating	Experiencing flow
Undesirable aspects		
Boring	Unpleasant	
Frustrating	Patronizing	
Making one feel guilty	Making one feel stupid	
Annoying	Cutesy	
Childish	Gimmicky	

User Experience Goals To help shape the User Experience, user experience goals can be produced. The goals can be sorted into wanted and not-wanted aspects of the user experience. These goals can later be used as a tool to measure the outcome of the chosen design, and see if the goals are met. Examples of such goals can be seen in figure 2.2.

Observation can be an effective way of studying the interaction between user and product. This can be done in many ways; directly in the real life setting of the product, in a controlled test environment or via recordings of the interaction. The purpose is to carefully study the way a user interacts with the product, including their experience and behavior. It can be performed during all stages of the design process, and with many different purposes, including exploratory, assessing requirements, validating a design or comparing different solutions [39]. To support the observer during testing, a test plan with a test protocol can be used, see paragraph 2.4.3. Observations can also work well as a compliment to other evaluation methods.

Interviews can be seen as a conversation between the interviewer and the user, but with a purpose. The goals is to get information from the user that can help the designers in any way. The shape of the interview depends on what type of interview it is. There are four main types; unstructured, structured, semi-structured, and group interviews(also called focus groups). An unstructured interview is loosely controlled by the interviewer, and resembles a normal conversation. On the other side of the spectrum is structured interviews, where the interviewer closely follows a predetermined set of questions for the user to answer. Semi-structured interviews land in between these two poles, where the interviewer does have prepared questions for the user, but have some wiggle room to abandon or expand the questions if needed. Lastly, in a group interview, or focus group, the interviewer acts more like a mediator that steers the conversation of the group. What type of interview to use depends on the situation and the goal of the data collection [39].

User Testing is a collective term for techniques that collects empirical data of potential end users performing realistic tasks with the product. Usability testing is often used in the form of an iteration of tests and re-design, used to expose usability problems, gradually

shaping the product [22]. The number of participants needed for a successful usability test can vary, but a often used and accepted number is five participants [39]. Research has shown that when testing with five participants, 85% of the usability problems are discovered [37]. A number of users below five runs the risk of missing crucial usability problem, and a higher number increases the cost of usability testing with little payoff when it comes to found errors in the design [37]. User tests can be divided into four main kinds of tests. The first one is exploratory testing. The main focus of an exploratory test is to investigate the effectiveness of a certain design concept, to see how "successful" the design is at supporting the user's goals for the product. Exploratory testing is done in the early stages of the design process, when the design is still being shaped. Because of this, exploratory testing relate to the high-level, over all design of a solution and not the more detailed, specific designs [22]. The second type is Assessment testing. Assessment testing aims to elaborate on the results from exploratory testing, and evaluate the lower-level aspects of the product and its usability. The goal is to investigate how well a specific implementation of the conceptual design generated from the exploratory testing is working. Assessment testing can be performed early or mid-way through the design process [22]. The third type of test is Validation testing. Validation testing is performed during the final parts of the design process when the design is close to being fully developed. Validation tests seeks to validate a products usability in regards to previously states benchmarks, or to assure that previously found flaws have successfully been removed, and no new usability problems have been introduced. The fourth and final test type is Comparison Testing. Comparison test differs from the previous three, since it's not connected to a specific phase of the design process. Comparison testing can be be done early in the process by comparing different conceptual designs, mid-way through by comparing the preference of a specific design element, and later on by comparing the solution to competitors. The aim is always to decide which implementation that comes with which advantage [22].

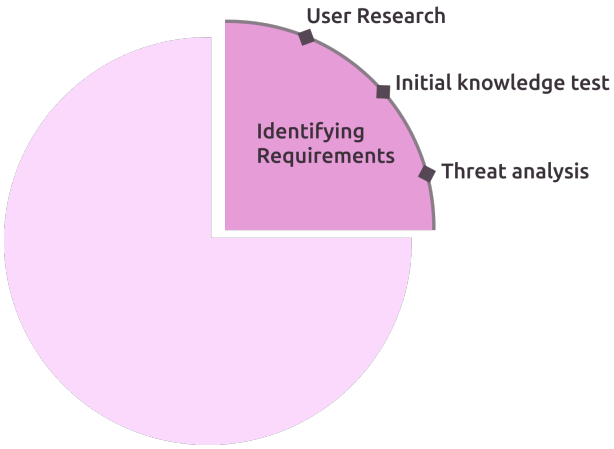
Test Plan A test plan describes how an entire test and test process will proceed, and is therefore an important resource to produce. It answers the questions; *how, when, where, who, why*, and *what* will be tested. A test plan can help describe what resources will be needed to conduct the test, communicates the focus of the test and what goals the test have. What should be included in a test plan can vary depending on the context, but some main points often include [22]:

- Purpose, goals, and objectives of the test
- Research questions
- Participant characteristics
- Method (test design)
- Task list
- Test environment, equipment, and logistics
- Test moderator role
- Data to be collected and evaluation measures
- Report contents and presentation

Personas One crucial part of UCD is to understand the users and the tasks they perform. This information also needs to be accessible and easy to grasp for the designer team. This can be achieved with the use of Personas. Personas are fictitious character descriptions, based on the user research. A persona should capture typical behaviors, wants, and needs of atypical users. The personas are expanded with detailed person descriptions to help the designers see the users as real people [39]. It's beneficial to create one persona for each distinct user group that have emerged during the user research. By doing so, one manages to typify the behavior for many different users into a hand full of fictive persons [22]. The personas can be used during the design process as a reference point, for example during a Cognitive Walkthrough, see paragraph 2.4.3.

Cognitive Walkthrough / Walk-Throughs A cognitive Walkthrough, or Walk-Through, is a method where the designer envision the user's experience of the product. They try to envision the users path, wants and needs, often in response to a conceptual or early design proposal. Hence, it is important that the design team has a clear vision of the users and their tasks [22]. This method is easy to perform, and can reveal significant flaws in the design before time and effort has been spent on acquiring test persons that represent the target group.

Brainstorming is a technique widely used in the field of interaction design to generate and develop ideas. Brainstorming focuses on being an open activity with "no wrong answers", and hence have little guidelines. However, two main factors that contribute to a successful session is that the participants are well understood about the users, and that no ideas should be criticised or debated. The participants are allowed to freely explore ideas, including silly or un-realistic ones, and bounce of each other to gather new ideas for the solution in question [39].



Chapter 3
Identifying Requirements

This chapter will focus on the use of frameworks and methods that helped us get a better understanding of the context of our game. This will include a threat analysis and a user research plan which results in requirements for our game. Our methodology for user research will be based on the theories and techniques discussed in section 2.4 and will be iterated throughout the project to follow the agile way-of-working according to interaction design. The threat analysis will be based on theories presented in section 2.1 and 2.2.

3.1 User Research

To identify and understand the target group of a product constitutes a vital foundation to be able to produce a well-working design. Because of this, it is important to clearly define the user sample. In this study, the users will be employees at Acme (consultants included) with technical competences. Further, we have chosen to not include employees with a high level of knowledge within security topics. This means departments such as HR and Security will not be included. This selection is done based on our research questions, where we want to study learning based on gamificiation and an immersive user experience. Individuals with a high level of previous knowledge within the field will most likely already have knowledge about the topics we will present. Hence, they will not learn from our game. We also want to create a game for technical professionals, and keep the duration of the game within a reasonable timeframe. To accomplish this, we target users that have previous knowledge and experience of software and engineering.

Personas To aid us in our design process we created three personas that represent our user sample. The personas that can be seen in figure 3.1 - 3.3 are based on traits and characteristics of Acmes employees. One persona does not necessarily correspond to a certain employee but it could very well be an actual person working at Acme. We believe that these personas are useful for us to keep in mind when designing.

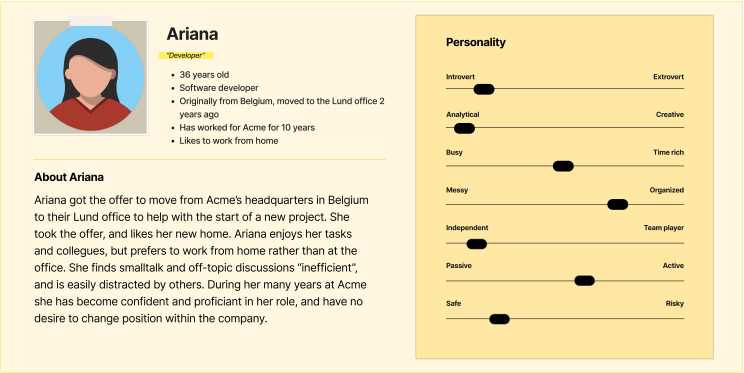


Figure 3.1: Persona 1, Ariana

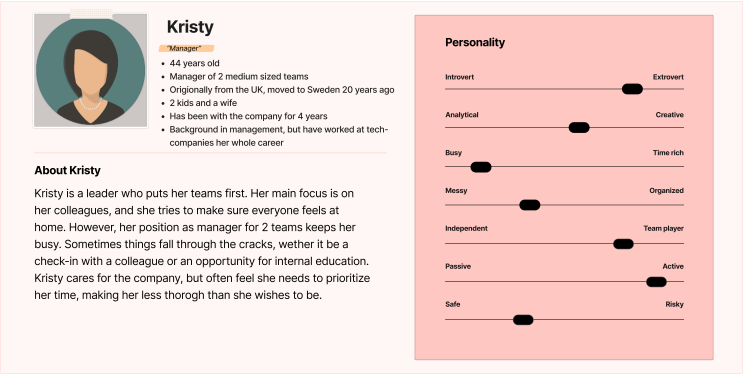


Figure 3.2: Persona 2, Kristy

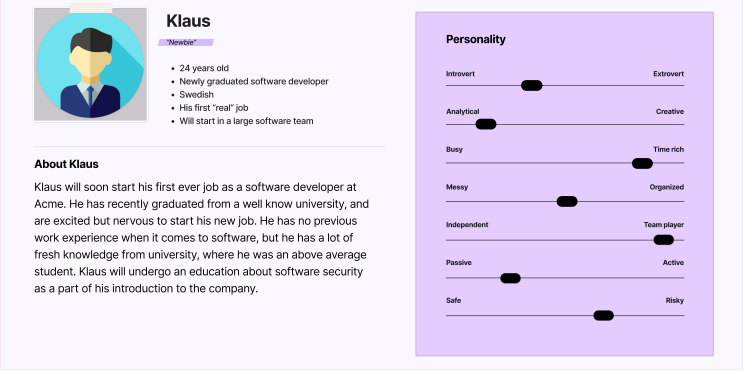


Figure 3.3: Persona 3, Klaus

3.2 Initial Knowledge Test

To be able to see if the employees of Acme learn from either the game we are going to develop, or from a more traditional lecture in security, we had to know their competence from before going trough our education. To get a hold of test persons we promoted our master's thesis in various meetings, consisting of both colleagues in Sweden and Germany. People could then register their interest in participating in our study. We had 20 (n=20) persons who participated. Three identified as female, and 17 as male. The average age was 40.

We then sent out a initial knowledge test, in the form of a survey, which can be found in appendix A. The purpose was to identify what competence the target group possesses in the beginning of the and what competences the lack. As mentioned in section 3.3, the focus areas in the game will be decided based on both the threat analysis and the competence from our target group.

The test consisted of four different parts. The first part was to gather basic info and self-estimation of knowledge of the participants. This was done to investigate if they experienced that they had advanced their competences or not.

The second part was security questions about STRIDE. Since we have used the STRIDE framework to analyse Acme, it is only logical to see what they know of those threats. In this part the participants were given definitions of the treats and had to match the definitions to respective threat.

Following the STRIDE questions were some case questions where the participant were given an explanation of an attack or a situation they could encounter. To each case there were a few alternatives they could chose from to answer the question. The question could be; what kind of attack was described, what they possibly could do to prevent the attack, to what threat in STRIDE the case was connected, what could happen if the attack was successful, etc. The aim for this part of the survey was to see their reasoning skills connected to their security competence.

The last part consisted of general and often considered as common knowledge of cyber security. This part covered the CIA Triad of confidentiality, integrity and availability, which is considered the core underpinning of information security [7].

The results from the initial survey will be considered when deciding what to focus on when designing and developing the game.

3.3 Threat Analysis

This threat analysis will be conducted for each threat in the acronym STRIDE. There will also be a risk-assessment using DREAD grading according to table 2.1. Each component of STRIDE will be scored based on DREAD, where 5-7 is considered low risk, 8-11 is medium risk and scores above 12 is a high risk.

For each component of STRIDE we discussed what potential attacks that could be harmful for Acme. For example, for spoofing we analyzed the treat from the perspectives of damage, reproducibility, exploitability, affected users, and discoverability to detect potential vulnerabilities. Before finalizing the threat analysis our findings were discussed with a software developer in one of Acmes's security teams, to confirm that we were on the right track. When finalizing the analysis we used the DREAD grading table 2.1, to decide what score each com-

ponent of STRIDE would get from the discussions we had both within us but also with the security employee of Acme.

As mentioned in section 1.5 this threat analysis will be mainly limited to the communication system Microsoft Teams and Outlook, and the version control platform Bitbucket.

3.3.1 Spoofing

First and foremost there are several ways of spoofing, e.g. creating a fake website and sending emails containing links, that look legitimate, to such a website (phishing). The attacker could also create an executable or configuration file in the local directory. Moreover, phishing, which is a type of spoofing, is one of the most common cyber crimes [6, 18]. Sending a malicious email with a link is therefore doubtless not difficult and it's hence a possibility that employees at Acme could receive such emails. It is neither difficult to set up a web page resembling, in this case, Bitbucket since the HTML code for the web page can be viewed from the web browser [20]. Here the attacker can lure the victim into thinking they are to access a commonly used website and as per usual enter their credentials. Then a phishing attack alike the one described in figure 2.1 is performed.

Damage - Score: 3 If the attacker gains access to admin credentials by spoofing, the damage potential is high since the attacker then would get full trust authorization.

Reproducibility - Score: 3 There is not a window of when the attack has to succeed. The malicious website can be up and running for a while, and a link to it does not have to be clicked immediately. Moreover, once this attack is up and running, it is easy to reproduce since it does not demand big resources.

Exploitability - Score: 2 One does not have to be very skilled to make a replica website that collects credentials, but on the other hand a novice programmer wouldn't manage it in a short period of time.

Affected users - Score: 3 If the attacker gains access to an account with admin access, to example Bitbucket, it could cause havoc. It could affect many employees work if they lose access to their work and if the attacker destroys work progress etc. This could lead to customers being affected since they wont receive what they paid for in either time nor quality.

Discoverability - Score: 3 As previously mentioned this is one of the most common cyber attacks. Also worth mentioning is that web pages that use Hypertext Transfer Protocol Secure (HTTPS) encrypts close to all data that is sent between a server and client, in contrary to Hypertext Transfer Protocol (HTTP), making it hard to spoof information sent on the channel . If the URL then starts with HTTP one should be cautious. However, one could create an URL similar to the original URL, certainly if the original is long and complicated. The attacker could switch a "l" to a "1", or "I" making it really hard for the user to discover the fake address. For an attacker to discover the possibility of such attack is also

considerably effortless since the only thing the attacker needs is a valid email to which they could send the phishing email.

Total score for spoofing is **14** and is therefore considered a **high risk**.

3.3.2 Tampering

To tamper with shared configuration files, documents or hardware is a potential threat to Acme, for example on Bitbucket. To be able to tamper the attacker need some kind of access to what they want to tamper. This could be done by different kinds of attacks, e.g. by a man-in-the-middle attack where the malicious person intercepts a communication and tampers with the messages sent between two parties at Acme. A malicious person can also tamper with hardware, such as the hard drives of a computer. However, at Acme the hard drives are encrypted when not in use and is therefore hard to tamper with, or gain any information from them. Yet another way to tamper with Acmes data is to tamper with the network by redirecting the data packets or modifying the data that is sent over the network.

Damage - Score: 3 If an attacker would be able to perform some kind of tampering, they would be able to not only leak sensitive information but also upload content by modifying a configuration file or any other file you rely on [41].

Reproducibility - Score 1 For an attacker to succeed with tampering there are several aspects that have to match up. If the attacker were to conduct a man-in-the-middle attack the attacker has to intercept the communication at a time where sensitive information is sent. Further, depending on what protocol is used when the communication is established the attacker must launch their attack when this happens. Moreover, information is often encrypted over a secure channel and the network of Acme encrypts data that is sent. When working from home, Acme workers has to use a VPN to be able to connect to internet. Without the VPN they can't even reach ordinary sites such as google, their private mail or a news site. So, the attacker must be aware of a potential security breach to be able to perform the attack at the right time window and even if this were to happen the attack itself is hard to perform. Moreover, if a configuration file is changed, it would probably get noticed since all changes to such files has to be approved by two other users at Acme.

Exploitability - Score: 1 To perform a man-in-the-middle attack is not effortless. Firstly, authentication to prevent man-in-the-middle attacks are often included in protocols, for example by authenticating one or both parties using a mutually trusted certificate authority[5].

Moreover, with secure connections such as HTTPS and by VPN the information is encrypted [2]. Thus, there are already many preventions in action and the attacker will find it hard to perform such an attack on Acme since they use VPN, secure connections, encrypted hardware etc.

Affected users - Score: 1 If a tampering is performed some users can be affected. The systems used at Acme are configured and adapted to suit each team. Therefore, there are few files that could be tampered with that would affect a large part of the company.

Discoverability - Score: 1 It can be difficult to discover a man-in-the-middle attack, however in many cases such detection is already implemented in the used systems. On the other way around, it is very hard for an attacker to find an exploit in the systems leading to tampering attacks. All systems that Acme use are closely monitored and to find a bug so obscure before it is fixed is highly unlikely.

Total score for tampering is **7** and is therefore considered a **low risk**.

3.3.3 Repudiation

Repudiating can sometimes be an honest mistake by people that have misunderstood how the system works and can instead be a sign of bad user experience [41]. Hence the person sabotaging might not do it purposely and might be a security threat due to the systems being poorly designed. However, errors can often be found by keeping logs and it is therefore of importance for Acme to log what people are pushing to e.g. Bitbucket. This provides a structure ensuring against repudiation threats [31], since it makes it hard for an employee to lie or deny their actions. However, if the logs were to be modified it would be harder to track who's done what.

Damage - Score: 2 There would not be a direct damage to Acmes services since the logs do not affect their services. The logs keep track of who does what and it would be possible to gain usernames or emails that could be used in a phishing attack. The logs at Acme encrypts information that is secret and the attacker would not by an attack on the logs be able to gain access to further services.

Reproducibility - Score: 1 As mentioned, access is needed to the logs. Further, since the logs are automatically generated, an employee wouldn't be able to tamper with them either. Not only does the attacker need access to an employees account, but also to find a security breach in Bitbucket's and Microsoft's services to change the logs and how they work. These big companies have a lot of monitoring of their systems and it would be hard for a attacker to successfully hack their services. Moreover, repudiation is a unusual type of issue [31].

Exploitability - Score: 2 Alike other threats, the attacker needs access to be able to modify or read the logs, which demands a high level of programming skills. On the other hand, there are several well-known ways of tampering with logs, commonly used by ethical hackers to find breaches [3]. Acme has a lot of protection against these attacks, but to perform such attack, not necessarily a successful one, does not demand extreme programming skills.

Affected users - Score: 2 If the log were to be attacked it would first off affect a certain team. However, this could spread to affect more users, since the breach of protecting the logs probably would exist globally in the services Acme uses.

Discoverability - Score: 1 If there are no logs to analyze or that the logs are tampered with, it is hard to discover malicious behaviour [41]. However, at Acme git blame, or plugins enabling it, are used to be able to track who wrote what kind of code snippet, or added which files. However, noticing that something is logged incorrect might not happen at once. For an attacker to find a breach that makes the logs vulnerable is hard. If such breach were to be exploited the services that Acme uses would repair it quickly.

Total score for repudiation is **8** and is therefore considered a **medium risk**.

3.3.4 Information Disclosure

At Acme managers, department heads and scrum masters can grant access to different systems. In some cases employees can also request access that has to be approved by someone with such authorization rights. In general an access control lists (ACL) is used to decide who gets access to read, modify and write files and if these were to be incorrect or something missing an attacker could take advantage of that and get access to things they shouldn't get access to.

Damage - Score: 3 An attacker could possible leak sensitive information by finding crypto keys on a disk or from error messages from username and password to entire database tables [41]. In addition, information disclosure promotes other attacks since it can disclose security breaches, e.g. by leaking databases, error messages and database connections [41].

Reproducibility - Score: 2 Here, the human factor plays a big role since it in many cases is a person who authorizes access. In combination with inappropriate or non existing ACLs and temporary database permissions such an attack could possibly be successful.

Exploitability - Score: 3 Once the information is disclosed, leaking sensitive information is not difficult if you know where to look. If an attacker gains access, it is considered trivial to find actual ACL files, especially if they are handled inappropriately.

Affected users - Score: 3 Since disclosing information can benefit other attacks this could lead to all user getting affected.

Discoverability - Score: 2 There are several attacks that could lead to information disclosure if successful, such as phishing, man-in-the-middle or buffer overflow. For all of these attacks there are published information on how to perform them, but at Acme there are protection against many of these attacks making it hard for the attacker to actually find a breach.

Total score for information disclosure is **13** and is therefore considered a **high risk**.

3.3.5 Denial of Service

A DoS attack would prevent Acme employees to work for the duration of the attack. If Bitbucket and Microsoft communication services were exposed to a DoS attack the resources would possibly become inaccessible. However, the services that Acme use are DoS protected. Bitbucket runs on Amazon Web Services, which has DoS protection [40] and so does Microsoft cloud services [32].

Damage - Score: 1 The main damage that could be done here is if the attacker possibly slows down the systems, absorbs CPU or memory, or consumes all network resources. However, no particular information would be leaked.

Reproducibility - Score: 3 This attack could be performed anytime and would work during a longer time window. However, it requires large resources to be able to send enough request to overload the servers and block the users.

Exploitability - Score: 1 For a DoS attack to be possible one would have to find an exploit in Microsoft's and Bitbuckets DoS protection. Such an exploit is pretty obscure and even if the concept behind a DoS attack is straight forward and that they could be performed in a smaller scale you would still have to be a skilled programmer to make it work.

Affected users - Score: 3 If Microsoft or Bitbucket were to be exposed to a DoS it would affect close to all employees on Acme since these services are used globally. In turn, this could lead to customers getting annoyed since neither the communication with Acme works, nor the delivery of services and products.

Discoverability - Score: 1 There are published information on how to build and launch a DoS attack, but it won't be successful at Acme. Acme's network has enabled firewalls and VPN protecting against spam requests, and discovers potential DoS attacks. Therefore, for an attacker to find some kind of way in to their systems is hard. As has been touched upon, Microsoft and Bitbucket both enables DoS protection and are considered hard to break.

Total score for denial of service is **9** and is therefore considered a **medium risk**.

3.3.6 Elevation of Privilege

Elevation of privilege is, much alike information disclosure, based on what permissions employees are granted. Here an attacker could get access to run certain bits of code and modify configuration files to make the disk behave improperly. It can also be done by an attacker sending inputs to code that it can't handle via a Buffer Overflow attack. When the amount of data in the memory buffer exceeds its capacity, data flows into other locations in the memory [15]. Hence, the data that previously was on those locations in the memory are overwritten or corrupted with new data. Because of this, the attacker could overflow a memory so that the data in memory now enables access to services. These kind of potential exploit should however be kept in mind for those who implements systems [**?**].

Damage - Score: 3 An attack where a malicious person sends input that software can't handle are common and usually bring a lot of damage [41]. Further, if a person gets access to Bitbucket and can change configuration files, and have access to sensitive information, it can cause damage affecting in many ways, such as leaking information and harming the service that is sent to customers.

Reproducibility - Score: 3 The risk of an elevation of privilege attack is considered a medium risk since file systems can exploit and manage privileges and access [**?**].

Exploitability - Score: 2 Once an attacker receives privileges it is not particularly difficult to send bad input to software or modify bits on disk. However, to perform a successful attack, e.g. Buffer Overflow, is nothing a beginner programmer could do.

Affected users - Score: 2 Some attacks that elevation of privilege can lead to can enable other attacks, which in turn then can affect many users. However, there are few accesses that could be gained by an attacker that would affect all the user of Acme.

Discoverability - Score: 2 There are published information which states how, for example, a Buffer Overflow attack could be conducted. However, many systems are providing checks against this.

Total score for elevation of privilege is **12** and is therefore considered a **medium risk**.

3.4 Final Requirements

From the results of the initial knowledge test and threat analysis we derived three security topics that will be the main focus in the game. These focus areas were not only decided in relation to the employees' knowledge and the actual threat to Acme, but also how common and relevant the threats are to the employees to know about.

3.4.1 Results from Initial Knowledge Test

As mentioned in section 3.2 the participants answered questions about their perceived knowledge, questions about definitions of threats, and case questions whose purpose was to measure deeper knowledge. The results from this can be seen in figure 3.4 below.

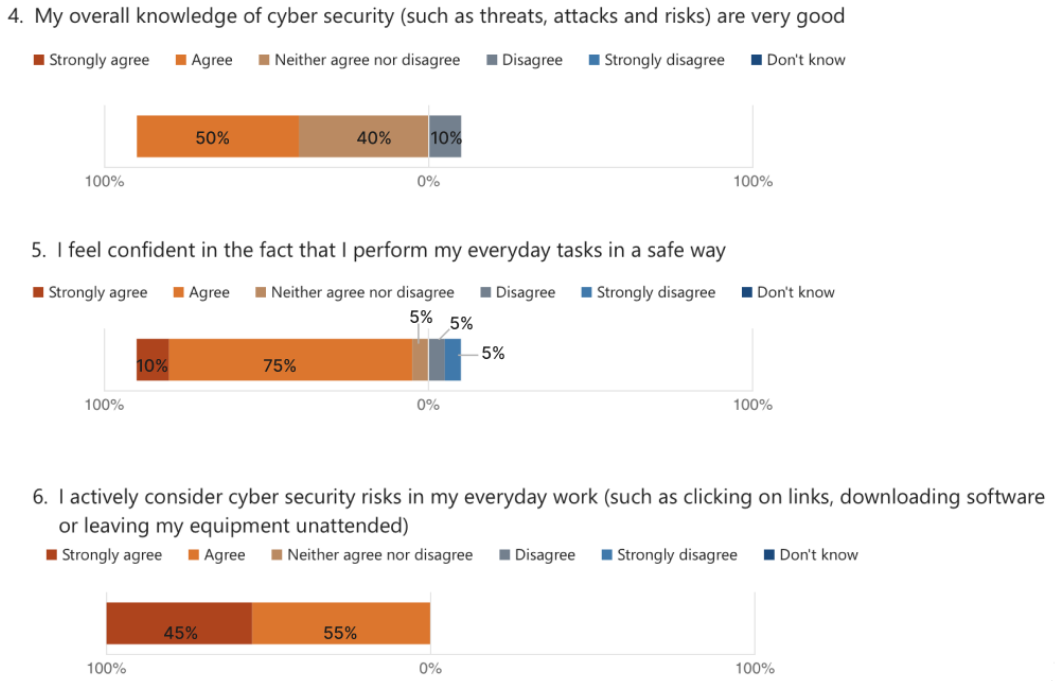


Figure 3.4: Results from initial self estimation

The table 3.1 below gives an overview of the result from questions about definitions and case questions. For each STRIDE component, we have calculated the percentage of people who answered correct, incorrect or chose to answer "I don't know". As can be seen in table 3.1, spoofing, repudiation and information disclosure scored the lowest when it comes to the definition. For the case question, repudiation, information disclosure, and elevation of privilege scored the lowest. From here we derived that we want to build on Acme's employees knowledge when it comes to repudiation and information disclosure.

Table 3.1: Results from initial knowledge test

	Definition			Case		
	Correct	Incorrect	Don't know	Correct	Incorrect	Don't know
Spoofing	65%	20%	15%	85%	15%	0%
Tampering	90%	0%	10%	65%	30%	5%
Repudiation	47.5%	12.5%	40%	20%	55%	25%
Information Disclosure	70%	15%	15%	35%	60%	5%
Denial of Service	75%	15%	10%	55%	20%	25%
Elevation of Privilege	85%	5%	10%	25%	45%	30%

3.4.2 Results from Threat Analysis

Table 3.2: DREAD scores from Threat Analysis

	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Damage	3	3	2	3	1	3
Reproducibility	3	1	1	3	3	3
Exploitability	2	1	2	2	1	2
Affected users	3	1	2	3	3	3
Discoverability	3	1	1	2	1	2
Total score	**14**	**7**	**8**	**13**	**9**	**12**

Above in table 3.2, the final score from the threat analysis is presented. The result show that spoofing is the biggest threat based on the DREAD score while repudiation scored the lowest.

3.4.3 Derived Requirements

Based on the results from the initial knowledge test and threat analysis, see section 3.4.1, we decided to focus on three out of six components of STRIDE.

The first area is spoofing, which according to our threat analysis is the biggest threat for Acme. On the other hand, the knowledge test indicated that spoofing is the treat that the employees of Acme has the most knowledge about according to case questions, but since spoofing is known as one of the most common attacks [6, 18], we chose this as one of our three focus areas.

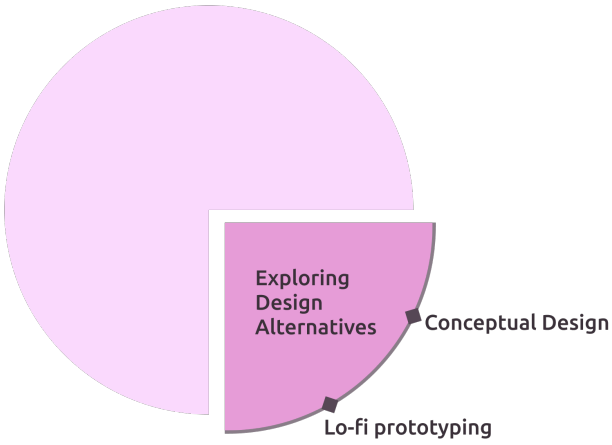
The threat that scored second highest was information disclosure, and a like spoofing is therefore something we want to focus on in game. We could see from the knowledge test that overall people had basic knowledge about the threat, but there were fewer who had knowledge about information disclosure compared to tampering and spoofing.

From the knowledge test we concluded that the repudiation threat is the threat which the employees knew the least about. It it considered a medium risk and scored second to last in the threat analysis. However since the test persons knew little about the threat, we want to raise awareness to its meaning and what could be done to prevent attacks leading to repudiation.

This means that we will not focus on tampering, denial of service and elevation of privilege. Tampering is the smallest threat and scored the lowest in the threat analysis. Generally people had good knowledge about that certain threat. The employees were also aware of denial of service and even though it is considered a medium threat for Acme, it is hard for a team member to prevent a DoS attack. This should instead be the people implementing the systems area of responsibility. Lastly, elevation of privilege scored third highest on the threat analysis and is considered a medium threat. The initial knowledge test shows that the participants knew the definition of the threat, but generally answered the case questions poorly. However, much alike DoS attacks, this is not necessarily a threat that a common employee could prevent. That threat could rather be included in a education for managers or people administering access. In addition, we had to chose what to focus on to fit the scope of this master's thesis, and therefore had to limit the number of threats focusing on.

Worth mentioning is that an employee of Acme do not have the power to prevent all of the threats above, but are rather aspects that the company developing and deploying the

services have to take into consideration. For example, a DoS attack is not something an employee using teams, outlook, or Bitbucket could prevent. This means that even if some threats are a high or a medium risk, it would not necessarily mitigate Acme's security risks if we focused on those in the game.



Chapter 4
Exploring Design Alternatives

To give the reader an insight into the early stages of the game development, this chapter will focus on creating alternatives and conceptual designs for the game. It will firstly go trough how we brainstormed conceptual designs from which we designed a lo-fi prototype of the main idea and flow of the game. Lastly it will touch upon how the prototype was tested and the results from those tests.

4.1 Conceptual Design

The conceptual design was developed based on the result of a thorough brainstorming session. The session commenced with seven minutes of individual brainstorming, where we wrote down our own personal high level, conceptual ideas for the product. We encouraged each other to think as freely as possible. After the seven minutes were up, we presented our ideas to each other and duplicates were removed. After that, another brainstorming session were conducted, where we brainstormed further ideas and high level features based of the previous ideas. We tried to keep thinking as freely as possible, ignoring any potential difficulties and/or restrictions. This resulted in five different conceptual ideas, each with high level features and ideas. We then discussed each and every one of the five ideas, focusing on potential pros and cons, such as how hard it would be to implement, how easy it would be to add gamification elements, and how "fun" we felt the idea was to us personally. We came to the conclusion that one of the ideas would be too difficult for us to implement during the time frame of this thesis, and a second one seemed to require a large amount of animations

to accomplish, an area were we have no previous experience. These two ideas were therefore weeded out, and we were left with three ideas we considered realistic to proceed with.

The next step was to prioritize the three selected concepts and determine which one we should move forward with. With the help of the previously created personas, we conducted a cognitive walkthrough as described in section 2.4.3 to further explore the pros and cons of each conceptual design. We investigated each one of the ideas in regards to likes and dislikes of the personas. We noticed that each solution came with pro's and con's, and each one of the three personas corresponded slightly better to each one of the three conceptual ideas. Since we did not reach a definite conclusion via this technique, we decided to talk to employees of Acme and see what they preferred. We spoke to six employees, five that corresponded to our target group and one within a security team, hence having deep knowledge of the subject. We set up storyboards representing the ideas to easier present them to the employees, as seen in figures 4.1 - 4.3. One of the concepts were liked by all of the respondents, and the preferred choice for five out of the six employees. They showed immediate interest and excitement for the idea. Based on this feedback we came to a conclusion. We decided on a game concept where the user takes the role of a hacker, as seen in figure 4.1, and via that viewpoint learns about the cyber security risks and hazards of the company. We quickly notices that the employees seemed intrigued and excited about this idea, something that is important to enable a fun and educational experience of our solution. Hence, the idea of a game were the player takes the role as a hacker is the one we have decided to go with for this project.

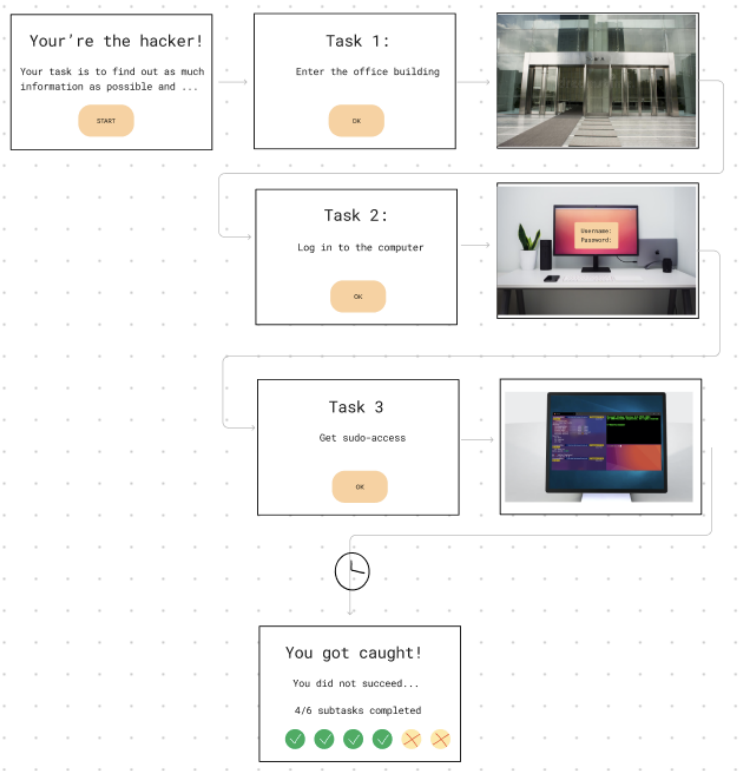


Figure 4.1: A storyboard visualizing a game concept of taking the role of being a hacker

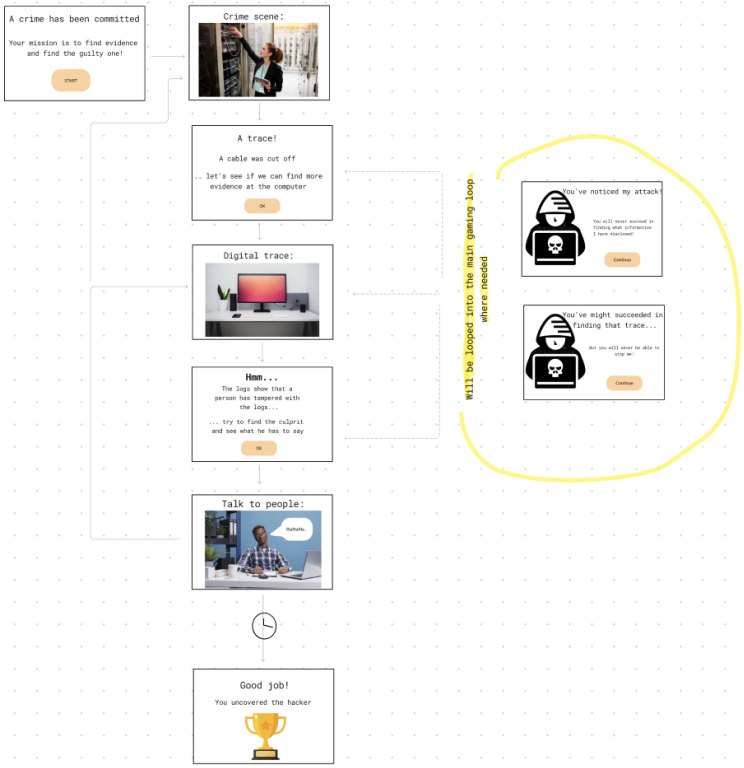


Figure 4.2: A storyboard visualizing a game concept of taking the role of a technical detective looking for digital tracks

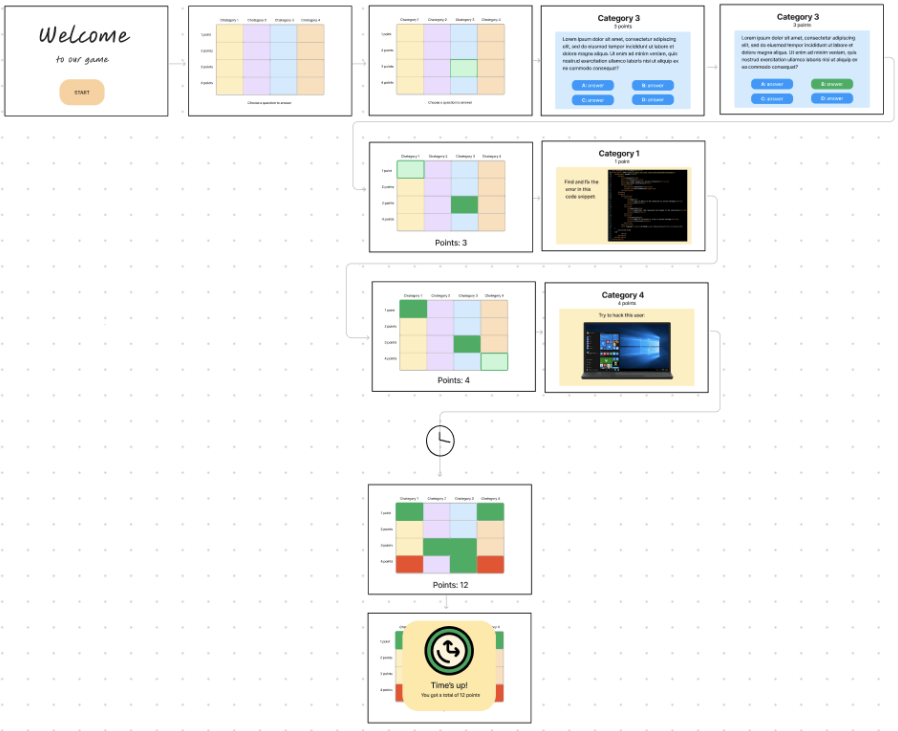


Figure 4.3: A storyboard visualizing a game concept similar to Jeopardy

When we had decided on an idea, we looked into the Octalysis gamification framework, see section 2.3.4, to see which of the motivators we could apply to our game. Based on our target group and the overall context and setting of our game, we decided to mainly focus on two motivators. The first one being Development & Accomplishment. As describes previously, this motivator drives the player to develop their intelligence within the field in question to try to overcome challenges. This is relevant for this study since one area we want to investigate is how a person can learn and develop new skills by using our solution. The second motivator we will focus on is Empowerment of Creativity & Feedback. This motivator drives people by engaging them in a creative process where they have to try different courses of action to be able to find a solution to a given task. This also connects to the experiential learning-theory presented in section 2.3.1, where learning is viewed as a process of testing an approach to solving a problem, acknowledging the outcome of that experiment, and transferring the new information onto a higher level of reasoning, thereby using that experience as a basis for future problem solving. Based on these two motivators and the theory of learning, we will add elements such as distinct feedback, room for exploration and creativity, and clear rewards for progress in our game.

4.2 Proof of Concept - Lo-fi Prototype

A lo-fi prototype was created to concretize and further develop the conceptual design that was created earlier in the process. The lo-fi prototype consisted of a simple paper prototype, consisting of a brief intro to the game, followed by two initial tasks to materialize the main flow and thought of the game structure. Four figures of the lo-fi prototype can be found in figures 4.4 - 4.7. The goal was of course to add more tasks in the final version of our game, however we believe that two tasks was enough to demonstrate the overall game flow and present the concept to the user. To evaluate our concept via the prototype, a test plan was created and followed during five user tests, the number of participants suggested in section 2.4.3.

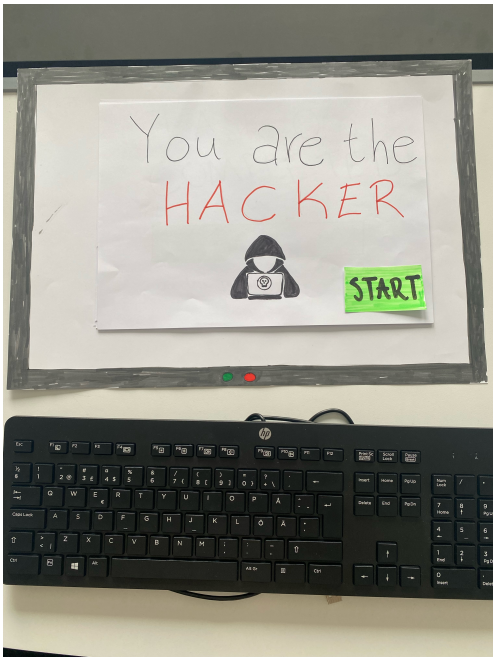


Figure 4.4: First page of lo-fi

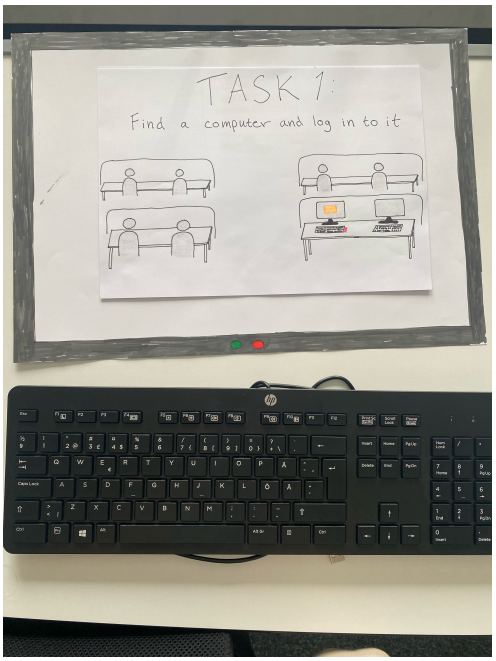


Figure 4.5: Task 1 of lo-fi

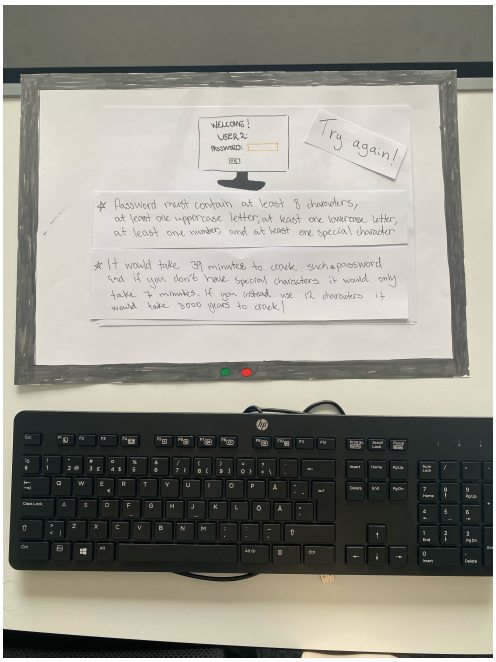


Figure 4.6: Part of task 1

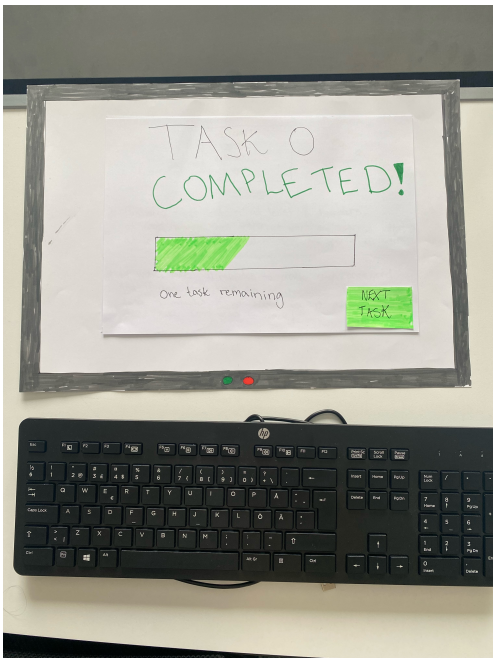


Figure 4.7: Task completed

4.2.1 Pilot Testing

To get a first impression of our game and ensure that the game follows a structure that enables learning opportunities, a pilot test was conducted. The test followed an open test structure

where the tester was invited to freely express their thoughts on the game experience, the game flow and any other aspect of the lo-fi prototype. To facilitate this, the pilot tester was an Acme employee with a technical background as well as deep knowledge of security topics. The pilot tests for both the lo-fi and the hi-fi prototype was conducted by one and the same participant who did not participate in the usability testing nor the final knowledge study.

The pilot tester appreciated the idea of the game and could clearly see the learning opportunities that the game created. However, they stated that it was important for us to balance fun with knowledge, and to make sure that the game scenarios remained true to the real world. This is an aspect that we valued highly, and we have kept it in our minds as an important aspect throughout the development of the game.

4.2.2 Test Plan

The purpose of the lo-fi testing was to explore the design of our solution on a high level. We aimed to investigate how the flow of the product could look, and if it had the potential to reach our overall goals and answer our research questions. We also wanted to investigate the usability aspect of our solution by asking the user about what emotions the game gave rise to, and comparing them to the User Experience Goals presented in figure 2.2. The questions we wished to answer was:

- What emotions does the game give rise to?
- What parts of the game support learning opportunities?
- What parts of the overall game flow feels natural and logical to the user?
- What common questions/confusions keeps coming up and needs to be addressed?

The testers were five people who corresponded to our main target group. The average age range was 25-30 and all participants identified as male. The tests followed an open structure, where we together with the tester explored and discussed aspects of the product freely. Because of this, the only task the user was given was to play the game. The test was performed in a separate room at the Lund office to limit distractions for the testers. The people in the room were the participant (user), the test leader (Anna/Felicia) and an observer/ discussion partner(Anna/Felicia). The data that was collected was the overall impressions, thoughts and opinions of the tester, and this was done via video recording of the test as well as notes from the observer and the test leader. The material needed to conduct this test was the lo-fi prototype, a computer and recording equipment. The results were compiled and analyzed and used as a base for further prototypes.

4.2.3 Results

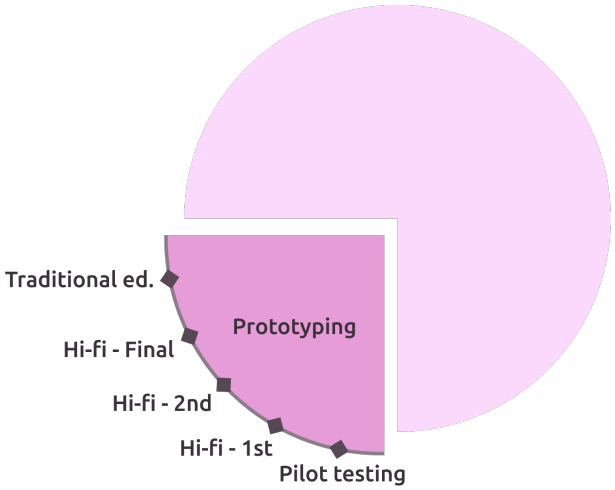
During the five lo-fi usability tests the research questions stated in section 4.2.2 were answered. All five participants found the solution fun, enjoyable and joyful. All participants also saw the potential for learning opportunities within our solution. Three out of five participants had no problem with the overall flow of the game, they found it intuitive and fun. However, two of the users found a specific part of our solution slightly confusing. The confusion appeared mainly in task 1, where the user were supposed to brute force a password to log

in to a computer. The two users did not find it clear that you were to keep trying different passwords, but instead hesitated and asked us questions about the task. This is something we will keep and mind when further developing our solution.

4.2.4 Conclusions

The main takeaways from the usability tests of the lo-fi prototype were:

- The progress bar was overall appreciated, but it needs to be clarified what it relates to (a specific task or the overall number of tasks)
- The game had a fun perspective with the player being the hacker
- It is nice with security information in between tasks, but some of the information might need to be rephrased
- The overall flow of the game worked nice, however some subtasks were not clear for all.
- For some users the clickable items (marked in orange, see figure 4.5) clearly signalised that they were clickable. For others, this rather implied that something was wrong with that item
- The player's role was a little unclear to some. A further introduction explaining the purpose and what kind of support/help the user have in the game was given as an example by a test participant that might help to make this clearer



Chapter 5
Prototyping

This chapter presents the progress of the game design, based on the open source gaming framework Root the Box, presented in section 2.3.3. Some modifications to both the interface and the logic of the framework were done to enable a user-friendly gaming experience aimed towards our target group, and those improvements will be presented in this chapter. However, the main game flow, appearance and structure of the game remain the same as the original framework, presented in section 2.3.3. The overall course of action for the development of the game is based on the theory of User Centered Design and User Testing, described in section 2.4.2 and paragraph 2.4.3. We have followed an iterative approach to continuously improve the game until we reached our final version, that is presented in section 5.5. The iterations consisted of one initial pilot test, followed by two iterations of usability testing of the game, to finally create the final version of the game.

5.1 Baseline version of the hi-fi prototype

Before usability tests of the game could be conducted, an initial version of hi-fi prototype of the game had to be created. This very first version was heavily based on the pre-existing functionally of the Root the Box game framework, described in section 2.3.3, and utilized features such as basic text questions as seen in figure 5.1. All of the visual design elements, such as buttons and general layout, was also the default for the framework. Figures 5.1 - 5.3 shows some main elements of this baseline version of the hi-fi prototype of the game.

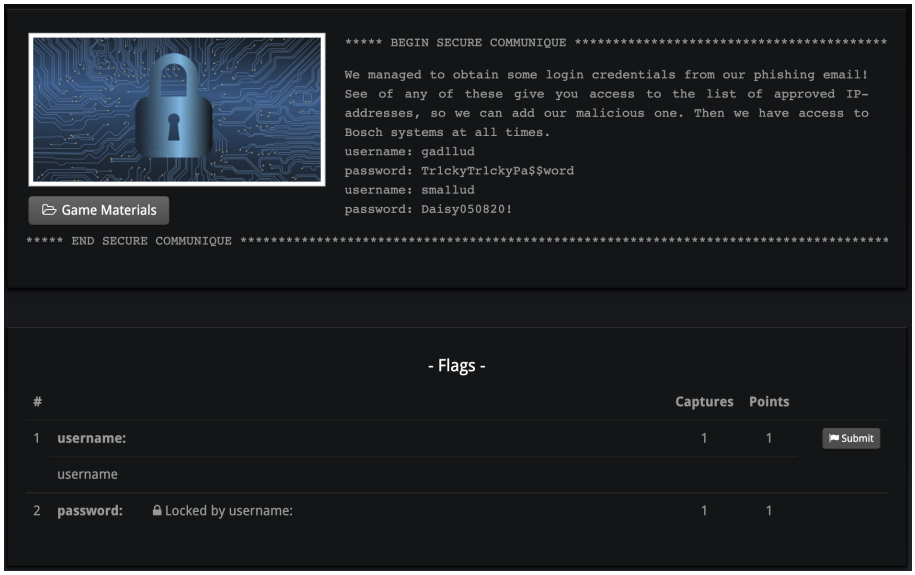


Figure 5.1: Example of basic text-based questions used in the baseline version of the prototype. This example shows the initial version of the login task

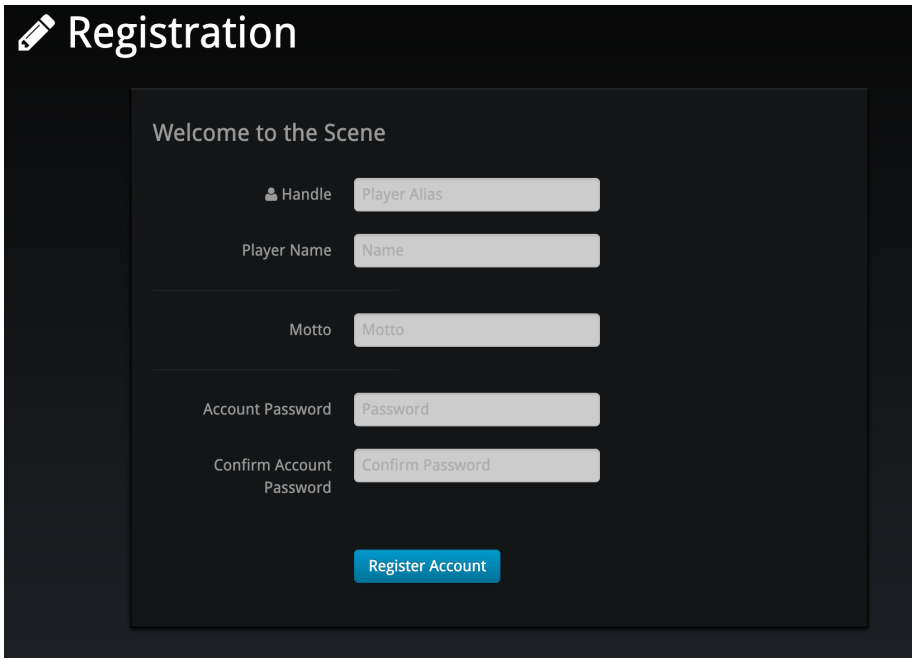


Figure 5.2: Default login page of the game

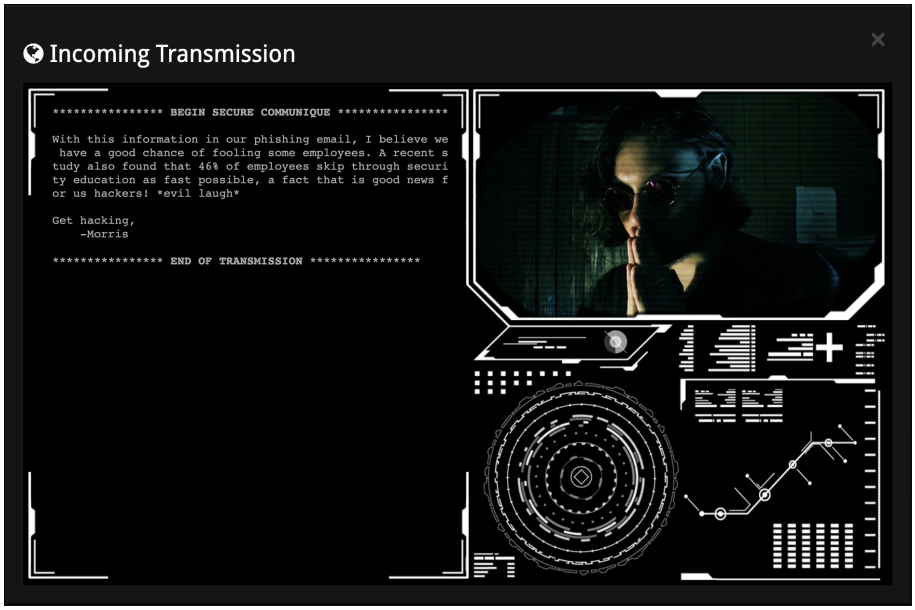


Figure 5.3: Default dialogue view of the game

5.2 Pilot Testing

To ensure an overall positive user experience and identify any major improvements, a pilot test was conducted for all three levels of the game. The test followed an open test structure where the tester was invited to think-aloud and share their thoughts on both the game experience and the facts and questions within the game. To enable this, the pilot tester had a technical background as well as deep knowledge of security topics. The pilot tests for both the lo-fi and the hi-fi prototype was conducted by one and the same participant who did not participate in the usability testing nor the final knowledge study.
The tester got an overall positive impression of the game, and stated that it was more engaging than traditional security educations. The general game flow and concept was understood and appreciated by the tester. However, some remarks were:

- The text layout could be improved
- Questions and statements could be clarified
- The submission of an answer was unclear to the user, see figure 5.1
- The "X"-button could be more prominent, see figure 5.3
- The game flow for level 3 could be more similar to real life scenarios

These points were taken into consideration and the game was improved according to said points before the next step, the first test of the hi-fi prototype, was conducted.

5.3 Hi-fi - First Iteration

The first round of usability testing of the hi-fi prototype was carried out when the main points found during pilot testing had been taken into consideration and improvements had been implemented. The first iteration focused on level one and two, since the functionality for level three had some technical issues in regards to the game framework that would take time to solve. However, we wanted to collect usability feedback in regards to the first two levels, as well as the overall impressions from the users of the concept, game flow and visual design. Hence, we decided to proceed with usability tests for the first two levels, while simultaneously working on the implementation of level three.

5.3.1 Test Plan

The test participants were five people who correspond to our main target group, as described in section 2.4.3. The average age range for the participants were 25-30 and all participants identified as male. Two out of the five participants had previously participated in the usability testing of the lo-fi prototype, while the remaining three had conducted no previous usability tests of the product. The tests followed an open structure, where we together with the participant explored and discussed aspects of the game and the user experience freely. Because of this, the only task the user was given was to play the game. The test was performed in a separate room at the Lund office to limit distractions for the testers. The people in the room were the participant (user), the test leader (Anna/Felicia) and an observer/ discussion partner (Anna/Felicia). The data we collected were the overall impressions, thoughts and opinions of the tester, as well as observations by the observer, and this was done via video recording and notes from the observer. The material needed to conduct this test was the hi-fi prototype, a computer and recording equipment. The results were compiled and analyzed and used as a base for improvements of the prototype.

5.3.2 Results

The results from the first round of usability tests were overall positive. Four out of five of the users expressed excitement and said that they felt more motivated and engaged compare to educations they had previously conducted. All participants enjoyed the viewpoint of taking the role as the hacker in the game.

5.3.3 Conclusions

Some points of improvements that was expressed by the users and observed during the test session was as follows:

- Ease the initiation process of the game, as seen in figure 5.2
- Create a separate, realistic login page to reach the file system needed for level 3, as seen in figure 5.1. This improvement can be seen in figure 5.13
- Introduce constraints to the game design to aid the user

- Decrease wait periods between the display of text
- Clarify questions, statements and concepts
- Mark the correct chosen answer in a task, enabling users to go back and review the correct answer
- Enable users to choose an answer directly from the main interface
- Put the question as the headline of the pop-up window when submitting a task
- Evaluate the need of users' motto
- Make "continue"-buttons more prominent and change from [X]-button to "continue"-button, see figure 5.3. The final improvement of this can be seen in figure 5.8
- Change the design of "submit"-button to increase the usability, as seen in figure 5.1. The final improvement of this can be seen in figure 5.10.
- Make the login site for level 3 task 1 more authentic to increase the usability, as seen in figure 5.1. The final improvement of this can be seen in figure 5.13
- Change the flow of task 1 in level 2 to increase the usability

These points were used as the base for improvements done to the prototype. However, some of the feedback given by the users was difficult to accommodate due to the limits of the gaming framework used. This will be discussed further in section 7, Discussion.

5.4 Hi-fi - Second Iteration

The second round of user tests was conducted on a version of the game that included all of the levels, one, two and three. Based on the feedback from the first round of testing, presented above in section 5.3.2, we aimed to fix all of the points that needed improvement to create a seamless user experience. Unlike the open structure of the first round of testing, the second round incorporated both a set of post-test interview questions, as well as a concluding NASA TXL survey to enable us to have both qualitative and quantitative usability data to evaluate the game.

5.4.1 Test Plan

The purpose of the second round of hi-fi testing was to validate that the solution facilitates a seamless and fun user experience where the user feels they are given the opportunity to learn about security, and feel motivated to do so. The goal was to make sure we had created an interaction that enables the user to focus solely on the materials within our game, and not be distracted by any part of the interaction. The tests followed a semi-closed structure, divided into three parts. Part 1 consisted of the user being asked to do one task; play the game. No further instructions were given during the game, unless the tester clearly signaled they were uncomfortable and in need of some guidance. If so, instructions were kept to a

minimum. During the first part of the test the user was asked to think-aloud, and the test leader observed their behavior. During part 2 of the test, the participants were asked a couple of questions. The first few questions were based on feedback from previous tests, and aimed to ensure we had tackled previous difficulties. Lastly, the participant were asked to raise any questions, thoughts or confusions that may have occurred during the test. If needed, follow up questions were asked to ensure we got a full understanding of the opinion of the user. The set questions that was asked were:

- Did you find the game to be fun and motivating?
- What did you think about the game design of looking for answers at sites separate from the actual game platform?
- Do you enjoy the option to choose a motto or did you find it superfluous?
- What did you think about the design choice of the text appearing in parts instead of all at once?
- Any thoughts or confusions that you want to share with us?

The third and final part of the user test was for the user to conduct the first part of a NASA TXL survey, as described in section 2.4 and appendix 2.5. We chose to only conduct the first part of the survey to not compromise the reliability of the test, as described in section 2.4. The participants consisted of five people who corresponded to our main target group. The average age range for the participants were 25-30 and three out of the five identified as female, and the rest as male. One out of the five participants had previously participated in the usability testing of the lo-fi prototype and the first iteration of the hi-fi prototype, while the remaining four had conducted no previous usability tests of the product. The test was performed in a separate room at the Lund office to limit distractions for the participants. The people in the room were the participant (user), the test leader (Anna/Felicia) and an observer/discussion partner (Anna/Felicia). The data we collected was the overall impressions, thoughts and opinions of the tester, as well as their answers to the questions mentioned above. This was done via notes and video recordings. The material needed to conduct this test were the hi-fi prototype, a computer and recording equipment. The results were compiled and analyzed and used to make any final adjustments to the game before conducting the final test.

5.4.2 Results

Once again the overall impressions of the game were positive. In regards to the first question, if the game was fun and motivating, four out of the five tester agreed that the game was fun. The fifth tester would describe the experience as interesting, rather than fun. In regards to the second question, thoughts about the game design of looking for answers at sites separate from the actual game platform, the opinions were mixed. Four out of five also found the option to choose a motto to be unnecessary.

The results from the NASA TXL survey is displayed in figure 5.4 - 5.5.

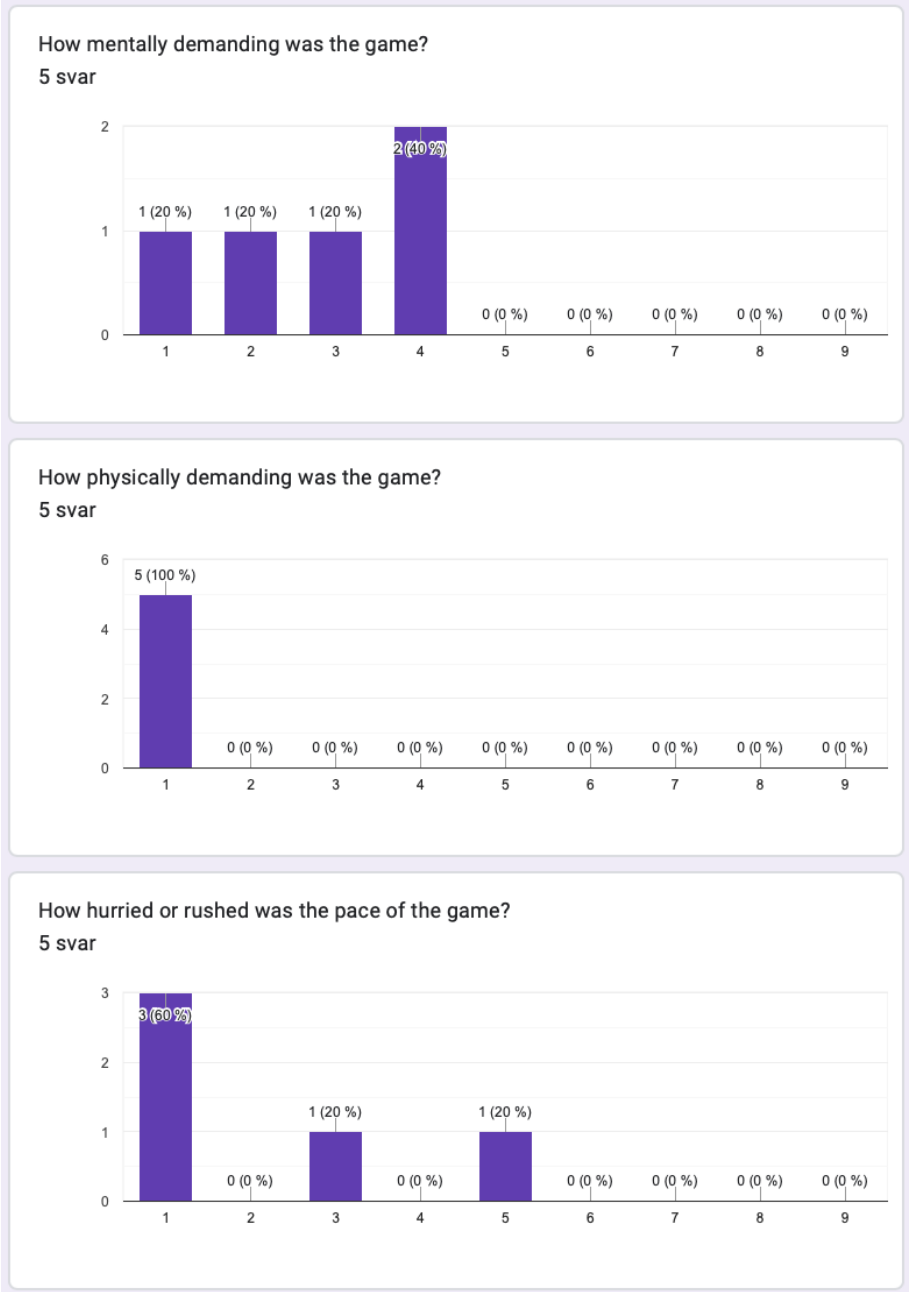


Figure 5.4: Results from the NASA TXL survey, question 1,2,3

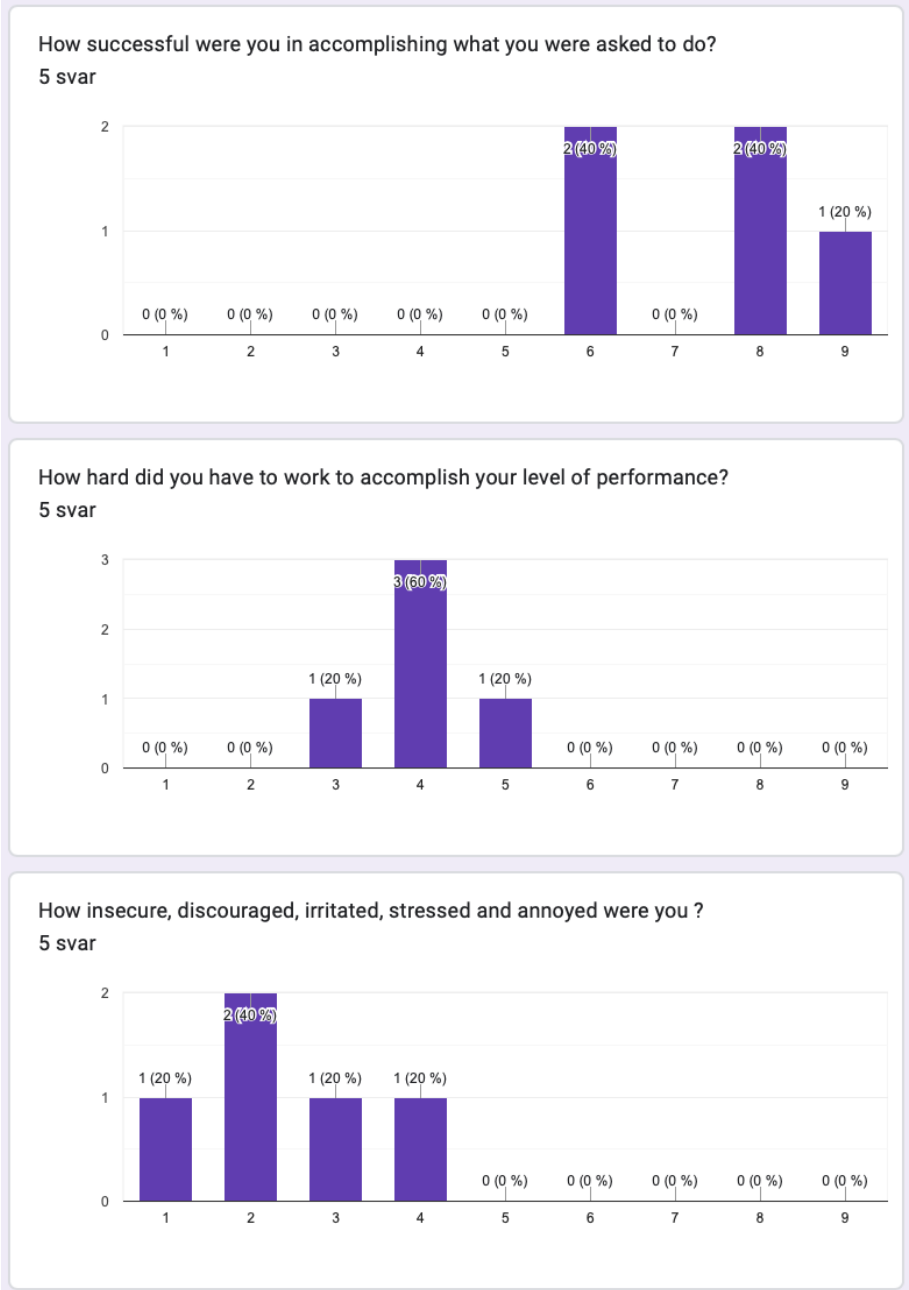


Figure 5.5: Results from the NASA TXL survey, question 4,5,6

5.4.3 Conclusions

It was further noted that the following points should be taken into consideration:

- Ease the initiation process of the game further by creating accounts for each user. This improvement can be seen in figure 5.9
- Introduce further constraints to the game design to aid the user
- Clarify questions, statements and concepts

- Modify the messages from the hacker companion to be more organic
- Make the error messages more prominent
- Make the continue button more prominent. This improvement can be seen in figure 5.8
- Make instruction in task 1 level 2 larger and more prominent
- Decrease wait periods between the display of text
- Display the logo images in level 1 task 1 directly in the main interface
- Remove the option to choose a motto. This improvement can be seen in figure 5.9
- Change "answer"-button to "click here to select answer"-button. This improvement can be seen in figure 5.10
- Merge task 2 & 3 in level 3 into one task
- Modify the order of task 1, 2 & 3 of level 1 to create a smoother story line
- Block Google pop-ups

5.5 Final version of the Game

After two iterations of usability testing and feedback of the hi-fi prototype of the game we implemented a final product. The game consisted of three levels covering our three focus areas, information disclosure, spoofing, and repudiation.

As mentioned in section 2.3.3, the game builds upon a Capture the Flag (CTF) framework. Our game is built upon the usual CTF structure, where you play the game outside of the CTF framework, e.g. on other webpages, applications or in the computer's file system and the findings is then entered into the CTF web page.

The main story line revolves around the player being a hacker, and the hacker's companion Morris. They will, by finding information about Acme, create a phishing mail to collect employees credentials. When someone falls for their spoofing mail they will obtain credentials used to login to an employees file system. From there they will whitelist a certain IP address and then hide their tracks by deleting relevant logs.

Each level consisted of a few tasks of game elements where the player for each task came closer to the goal of hacking Acme. In order to progress and finish each level the player had to finish the tasks and also answer a few questions regarding that level's topic.

In figure 5.6 Morris first introduces himself to give the player information about their mission. Then the main home page, containing all available tasks, is presented in figure 5.7

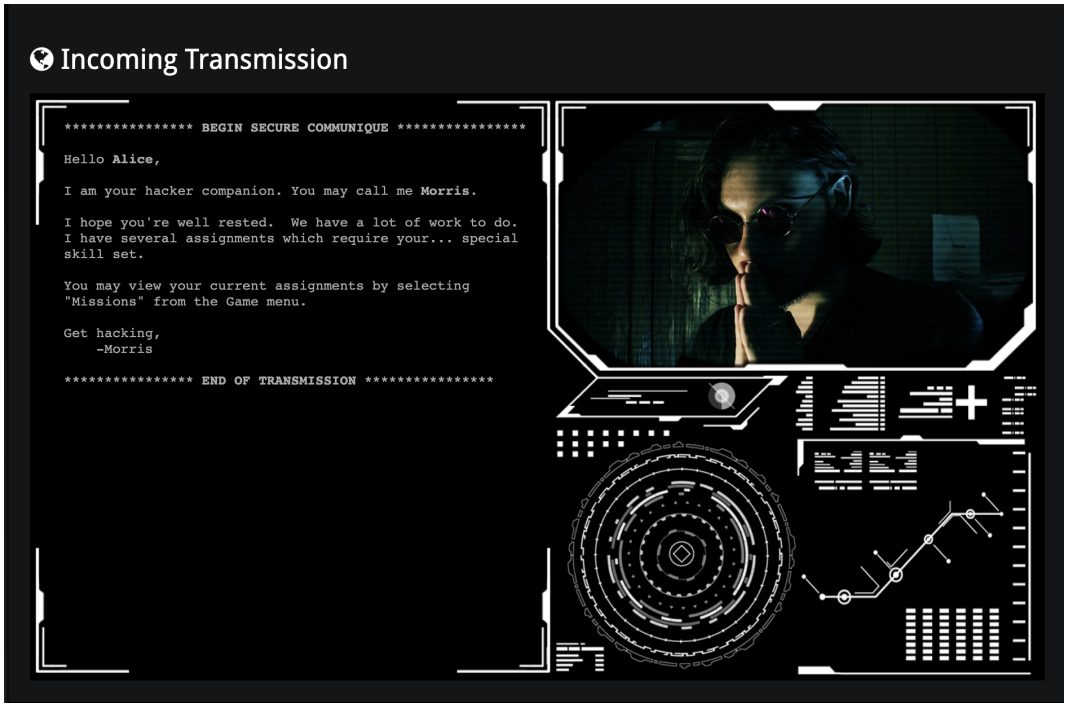


Figure 5.6: Game introduction of Morris

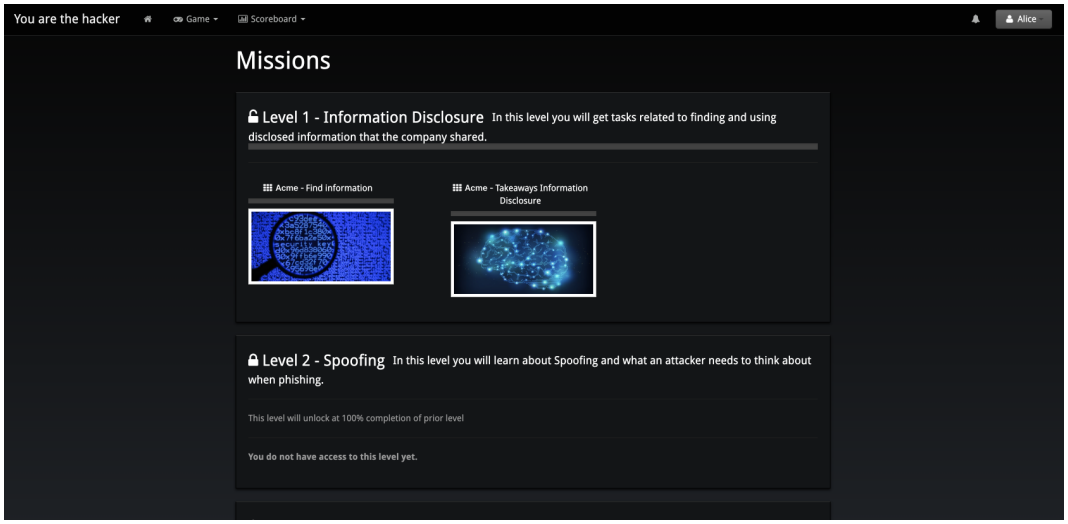


Figure 5.7: Overview of home page

In between succeeding with tasks Morris also pops up giving feedback and interesting information about security, for example as in figure 5.8

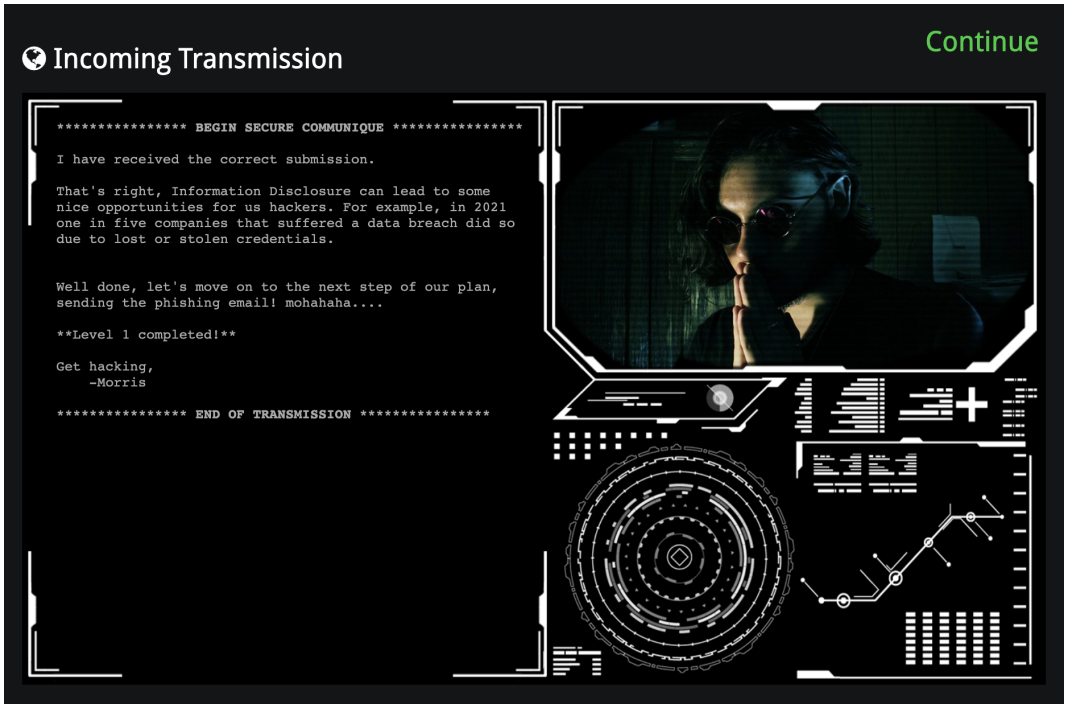


Figure 5.8: Example of feedback and information about security given by Morris

Figure 5.9: The final login page of the game

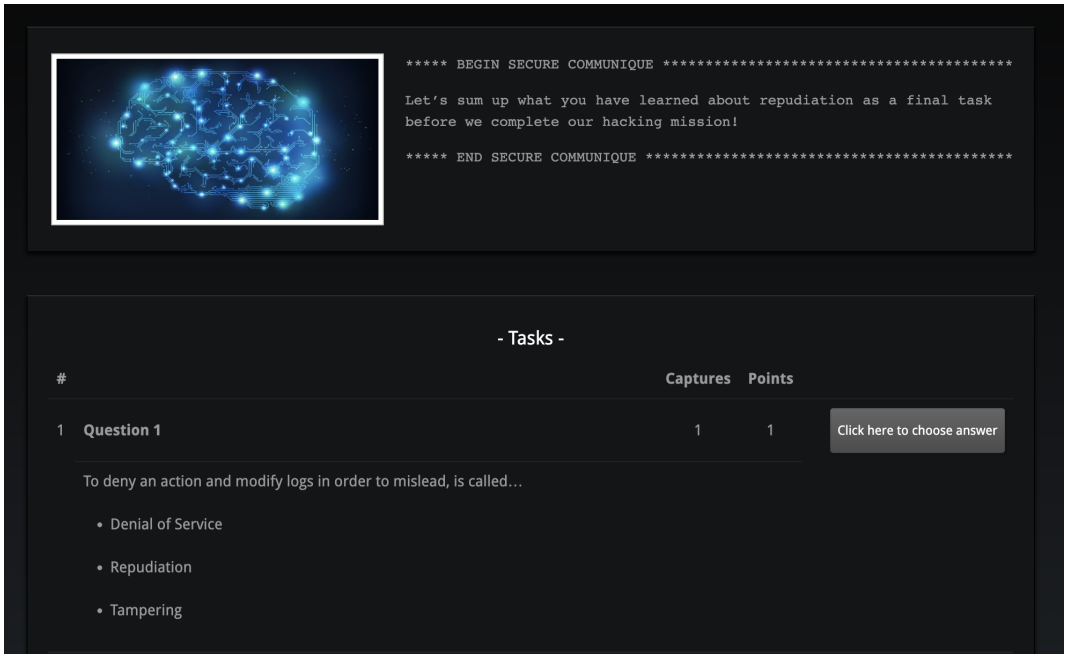


Figure 5.10: Example of a final task of the game

After each level is completed the player has to answer a few questions about takeaways to be able to advance in the game. The idea behind the game flow is to follow Kolb's cycle of experiential learning, presented in section 2.2, where the user learns based on experiencing something and then reflects, learns and tries it out. Thus, the user experiences the life of a hacker, reflects over the information found, and then learns from that experience. The first phase in Kolb's cycle is covered by the player experiencing the role of a hacker. From the information and actions performed when being the hacker, the player reflects on their finding and what they can be used for and how, referring to phase 2 & 3 in Kolb's cycle. The last phase of Kolb's cycle is tested after the player has finished the game and is tested on different security questions and possible real life scenarios.

When implementing the game we have also focused on the chosen two motivators; Development & Accomplishment and Empowerment of Creativity & Feedback. Throughout the game the player clerarly sees their progress and accomplishments in the game by a progress bar, and they see their development when they are compelting tasks and answering correct to the quetions. We have also put a few tasks where the user has to be creative, for example when they are asked to create a spoofing mail. They also have to try out different solutions to advance in the game and the answer is not always what they guess firstly. The user also gets feedback from Morris each time they submit an answer, to aid them advancing through the game.

5.5.1 Level 1 - Information Disclosure

The first level focuses on information disclosure. Here the player is asked to visit a website to find information that could be used to construct a spoofing email.

From the website below, in figure 5.11, the player can see the logo of the company and some email addresses. From that information the player can derive the pattern of the email

addresses used in the company. The task is then to choose from a list of logos, email addresses, and subject lines to create an email which would trick the receiver of such an email.

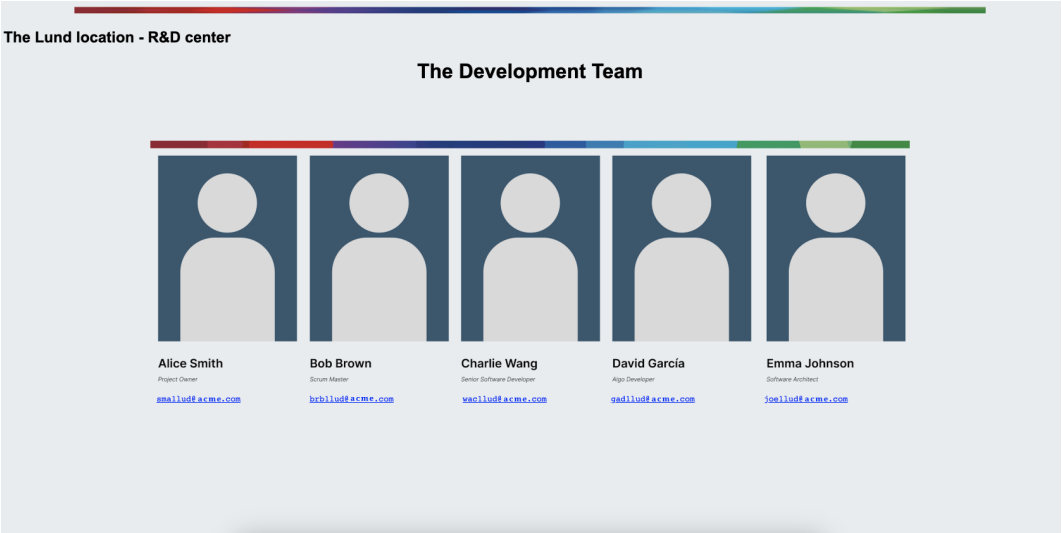


Figure 5.11: Acmes website with disclosed information

After succeeding in finding information disclosed by Acme, the player has to answer some take away questions, as described in section 5.5.

5.5.2 Level 2 - Spoofing

In this level the player creates a spoofing email by a drag and drop element in the game, as can been seen in figure 5.12

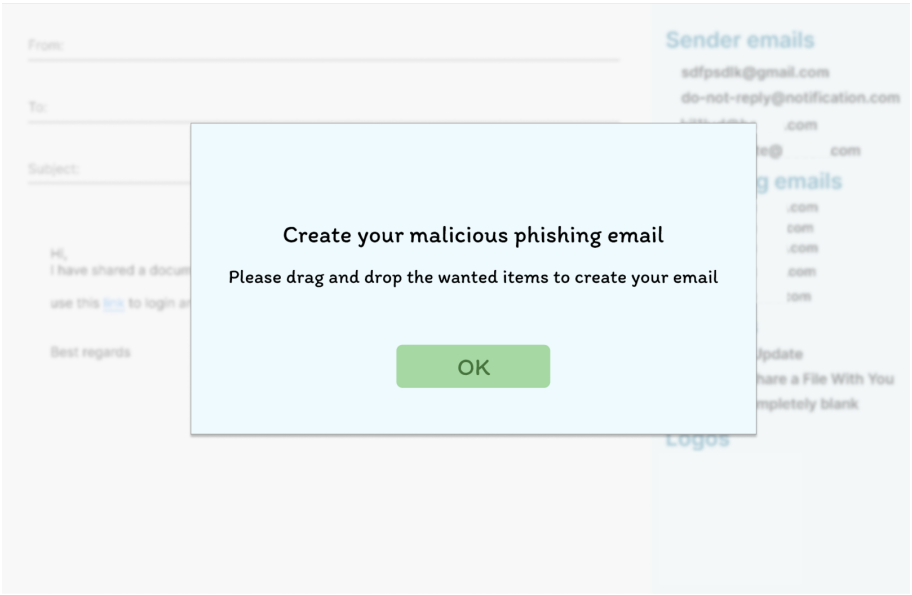


Figure 5.12: Drag and drop element to create a spoofing email

The phishing email should contain a sender email address that mimics Acme's, a tricky subject line and the correct company logo. It should also be sent out to as many known email addresses as possible, hence the ones that were found on the website in the previous level. When the email fulfills the requirements a secret key will be displayed, which is to be entered in the CTF web page to proceed. The email is then sent out by Morris who collects credentials of the ones who gets tricked by the mail. After creating the actual email, the player is asked to answer a few take away question.

5.5.3 Level 3 - Repudiation

The last level teaches the player about repudiation. Morris gives the player login credentials obtained from the phishing mail, which the player should enter into a login page, seen in figure 5.13, to then get access to a user's file system, seen in figure 5.14.

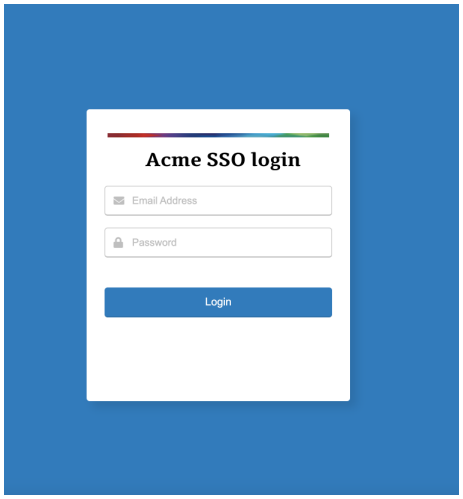


Figure 5.13:
Login page

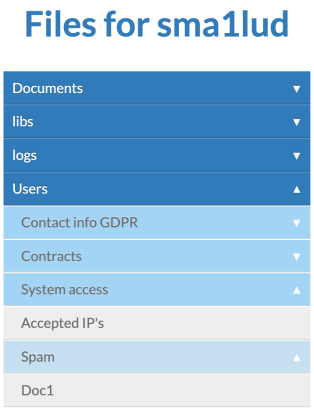


Figure 5.14:
File system

From the file system they should look for a file with whitelisted IP addresses, pictured in figure 5.15, and add their own address to that file. The last step is then to delete their tracks by deleting revealing logs, as can be seen in figure 5.16

Figure 5.15: Whitelist of IP addresses the player is asked to modify

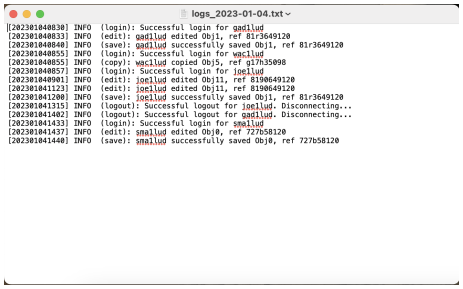


Figure 5.16: Log file the player is asked to modify to hide their tracks

The edited files, e.g. the white list and logs, is then uploaded to the CTF web page. Similarly to level 1 and 2 there are also a few take away questions before the player has completed all levels.

5.6 Traditional Security Education

To be able to compare the learning outcome from our game to Acme's usual security educations we created a corresponding *traditional security education*. This was created based on Acme's other security educations to imitate their structure as much as possible to make a as similar education as possible. For this master's thesis it resulted in a PowerPoint with animations, covering the same security topics and information as the game. As can be seen in figure 5.17 - 5.20, the PowerPoint was divided into three parts, one for each focus area. Each area had three sections; what the threat is, what threats it presents, and what one could do to protect against it.

Figure 5.17: First page of Traditional Security Education

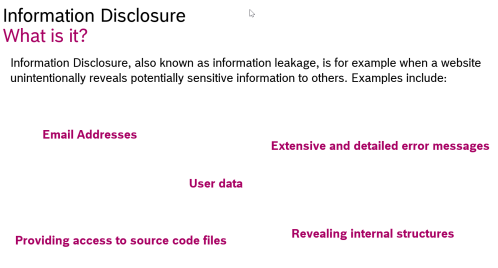


Figure 5.18: What is Information Disclosure?

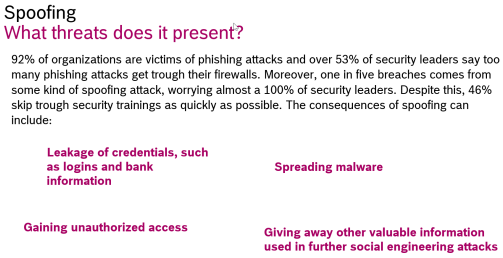
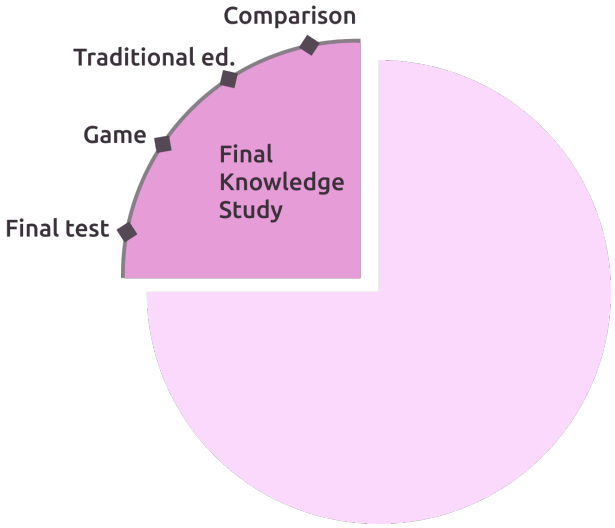


Figure 5.19: What threats does Spoofing present?

Figure 5.20: What can be done to protect against Repudiation?



Chapter 6
Final Knowledge Study

This chapter presents how the final knowledge study was conducted. To be able to discuss how one could teach about security topics we divided the test group into two, one group which got to play the game and one group which completed a traditional security education in the form of a PowerPoint presentation. For each test we set up a test plan where the participants conducted the education and then answered a quiz containing questions about security. This quiz was both answered directly after completing each respective education, and also two weeks later.

6.1 Final knowledge test

Alike the initial knowledge test used to derive our three focus areas, we also created a quiz that the participants answered after conducting their education. Two weeks later the participants answered the same quiz again. This is to fulfill Kolb's cycle of experiential learning, see figure 2.2. The last step of Kolb's cycle of experiential learning is to be able to utilize the learnt theories for decision-making and problem-solving. This is therefore tested by investigating if the participants could use their problem-solving abilities to reason and understand concepts when answering the quiz questions.

The quiz questions have been divided into four categories; basic information about the participant, self assessment of one's knowledge levels, definitions, and cases. The first cate-

gory was used to enable screening of the participants. The second category of questions was used to get an insight into the perceived level of knowledge among the participants. The third and forth categories tested different aspects of the participants' knowledge in regards to the relevant security topics. The third category tested how well they knew and understood the terms, and the forth category their understanding of the concepts and reasoning within the security areas. Category three will be referred to as "Definition", and category four as "Case". The quiz can be viewed in its entirety in appendix B.

6.1.1 Calculation of results

The results from category three, *definitions*, and four, *cases*, have been analyzed and reviewed according to the following guidelines. The percentage for the definitions are directly derived from the survey, since the survey contained one definition question per subject area. The percentage for the cases are calculated as the average value for all the case questions within that subject area, since multiple case questions were asked in regards to one subject area. Six out of the ten case questions only had one correct answer, while four were multiple choice questions.

The answers from both definitions and cases have been sorted into either *Correct*, *Incorrect* or *Don't know*. If one has answered Don't know, the answer is sorted into the Don't know category, no matter if the participant also chose different answers as well as Don't know. If an answer contained an incorrect answer, no matter if it also contained correct ones, the answer was sorted as Incorrect. To fulfill the qualifications for a Correct answer for a multiple choice question, the participant needed to have chosen a majority of the correct answers. For example, if three out of four alternatives were correct, the participant needed to select two out of the three correct answers for it to be sorted as a Correct answer. If less than the majority was chosen, the answer was regarded as incorrect. If the question only had one correct answer, and the participant chose that answer, it counted as a correct answer.

6.2 Game

The following two subsections will in further detail describe the test plan for when the participants played the game and give an overview of the results from the security quiz. The result tables show results from both the quiz answered directly after playing the game. and the one answered after two weeks.

6.2.1 Test Plan

Ten (n=10) users conducted their learning opportunity by playing the final version of the game, presented in section 5.5. The average age range for the participants was 30-39 and one out of ten identified as female, and the rest as male. All of the respondents represented the target group. The players were simply asked to play the game on the computer that was given to them, and that ran the game. Immediately after the player had finished all levels of the game, they were asked to conduct the knowledge survey described in section 6.1. They were not allowed to look for information of any sort during this time. The tests was conducted in separate room at the office to limit distractions for the participants. The people in the

room were the participant (user), and two observers to ensure the game ran as planned and answer any questions directly relating to the test setup (Anna/Felicia). No help was given to the players by the observers in regards to progressing in the game, and no questions about the content of the game and/or its questions were answered. When two weeks had passed since they took part in the education, a second round of the knowledge survey was sent out to the participants.

6.2.2 Results

Below, the results of the knowledge test, both from filling out the test immediately after completing the game, and after two weeks, are presented. Firstly, an overview of the self estimation is shown, and then tables containing results from the two knowledge tests are shown.

Self estimation results

In the initial part of the knowledge survey, the participants were asked to self-estimate their perceived knowledge in regards to three statements. The aim of this was to get an insight into the confidence and perceived knowledge levels of the participants. The results from both round one and round two can be seen below in figure 6.1 and 6.2

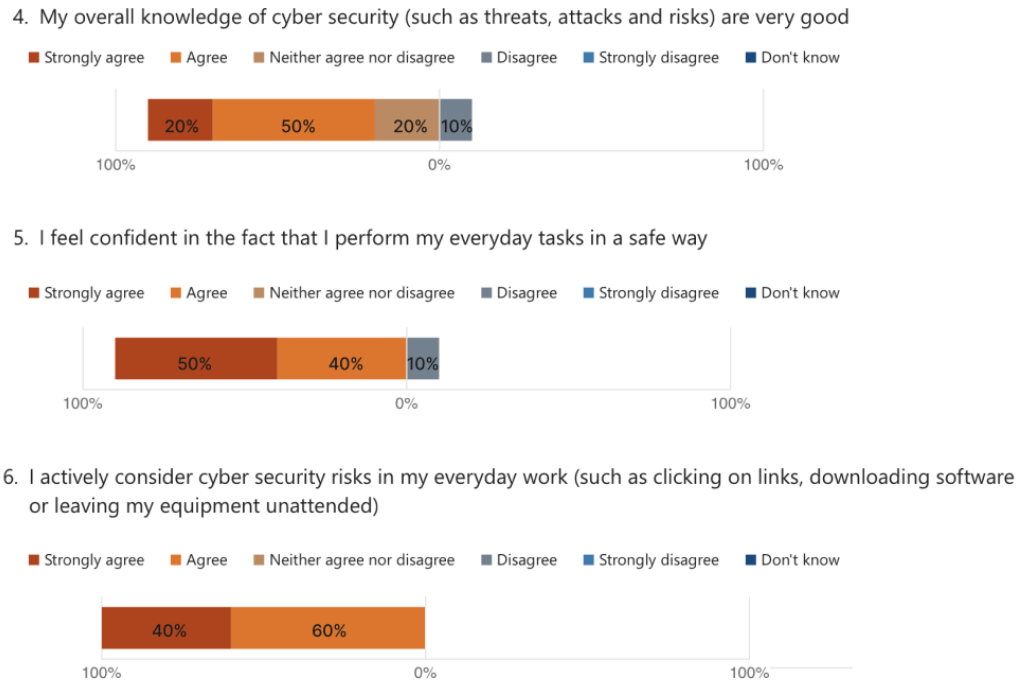


Figure 6.1: The self-estimations of the game participants for round one of the knowledge test

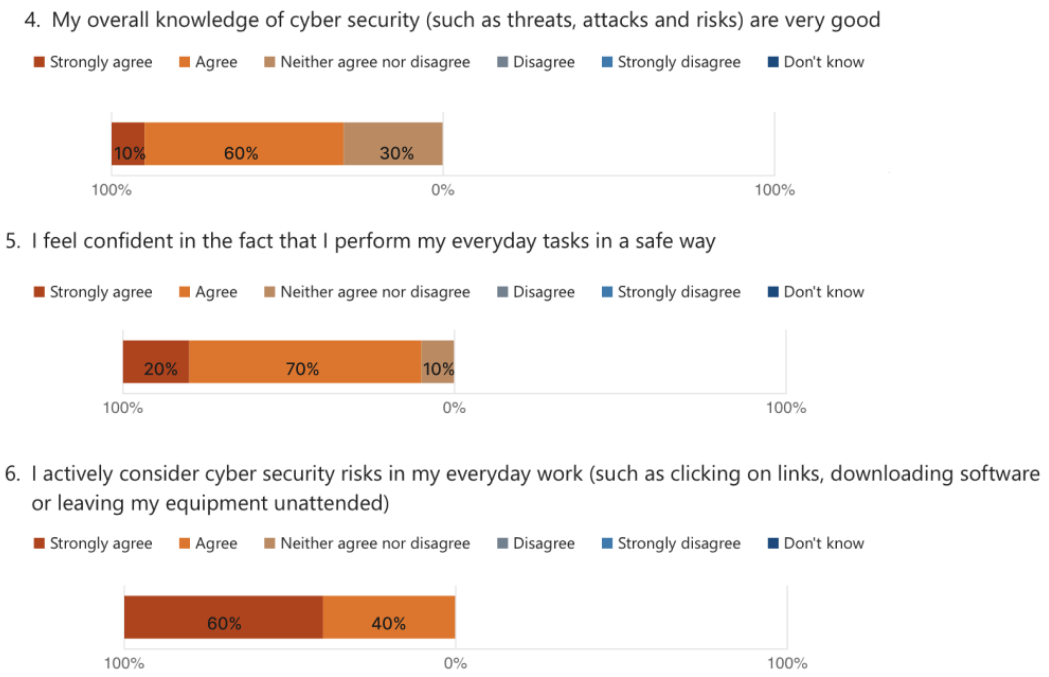


Figure 6.2: The self-estimations of the game participants for round two of the knowledge test

Knowledge test results

Below, in table 6.1 and 6.2, the results from the quiz can be viewed. Table 6.1 shows the percentage of participants who are *Correct*, *Incorrect* or *Don't know* within the three security topics, calculated according to the guidelines described in section 6.1.1. Table 6.2 shows the participants results when taking the quiz two weeks later.

Table 6.1: Results from knowledge test right after playing the game

GAME ROUND 1	Definition			Case		
	Correct	Incorrect	Don't know	Correct	Incorrect	Don't know
Spoofing	80%	10%	10%	82%	14%	4%
Repudiation	90%	10%	0%	50%	50%	0%
Information Disclosure	80%	20%	0%	65%	35%	0%

Table 6.2:
Results from knowledge test two weeks after playing the game

GAME ROUND 2	Definition			Case		
	Correct	Incorrect	Don't know	Correct	Incorrect	Don't know
Spoofing	90%	10%	0%	78%	20%	2%
Repudiation	80%	10%	10%	45%	50%	5%
Information Disclosure	100%	0%	0%	85%	15%	0%

The results will be discussed in further detail in chapter 7, however a few main takeaways from the above tables, will be presented in short.

Generally, after playing the game the knowledge of spoofing has remained on the same level as when the initial knowledge study was conducted. The knowledge concerning the definition of spoofing has increased slightly, while the deeper knowledge, measured with case questions, remained nearly the exact same. However, there were a big knowledge improvement concerning repudiation and information disclosure, both regarding definitions and case questions. Nontheless, repudiation scores the lowest and might depend on language barrier, which will be discussed in chapter 7.

From the results from both rounds of the game, it shows that the knowledge improved from the first round to the second round regarding the definitions of spoofing and information disclosure, while the knowledge dropped concerning repudiation. The results from the case questions showed that the scores of information disclosure increased to the second round, while spoofing and repudiation decreased.

6.3 Traditional

The traditional security education consisted of a PowerPoint based education, described in section 5.6, and the same knowledge quiz as the participants playing the game, shown in appendix B. The participants completed the PowerPoint education, then answered the quiz about the security topics. Two weeks later they took the same test again.

6.3.1 Test Plan

The PowerPoint presentation was sent out via Microsoft Teams to ten persons who volunteered to participate in this study, none of which conducted usability tests of the game. However, we only received nine (n=9) answers due to the fact that one employee left the company. The average age range for the participants was 40-49 and two out of nine identified as female, and the rest as male. All of the respondents represented the target group. To enable a comparison of knowledge between the two groups, none of the participants that received the traditional security education also played the game. The participants were asked to go through the education on their own without our supervision by reading the slides. When the presentation was completed, they were requested to conduct the knowledge survey immediately. The participants were told not to look for information at any source while filling out the survey, and they were not allowed to return to the PowerPoint education during this time either. When two weeks had passed since they took part in the education, a second round of the knowledge survey was sent out.

6.3.2 Results

Below, the results of the knowledge test, both from filling out the test immediately after completing the traditional education, and after two weeks, are presented. Firstly, an overview of the self estimation is shown, and then tables containing results from the two knowledge tests are shown.

Self estimation results

In the initial part of the knowledge survey, the participants were asked to self-estimate their perceived knowledge in regard to three statements. The aim of this was to get an insight into the confidence and perceived knowledge levels of the participants. The results from both round one and round two can be seen below in figure 6.1 and 6.2

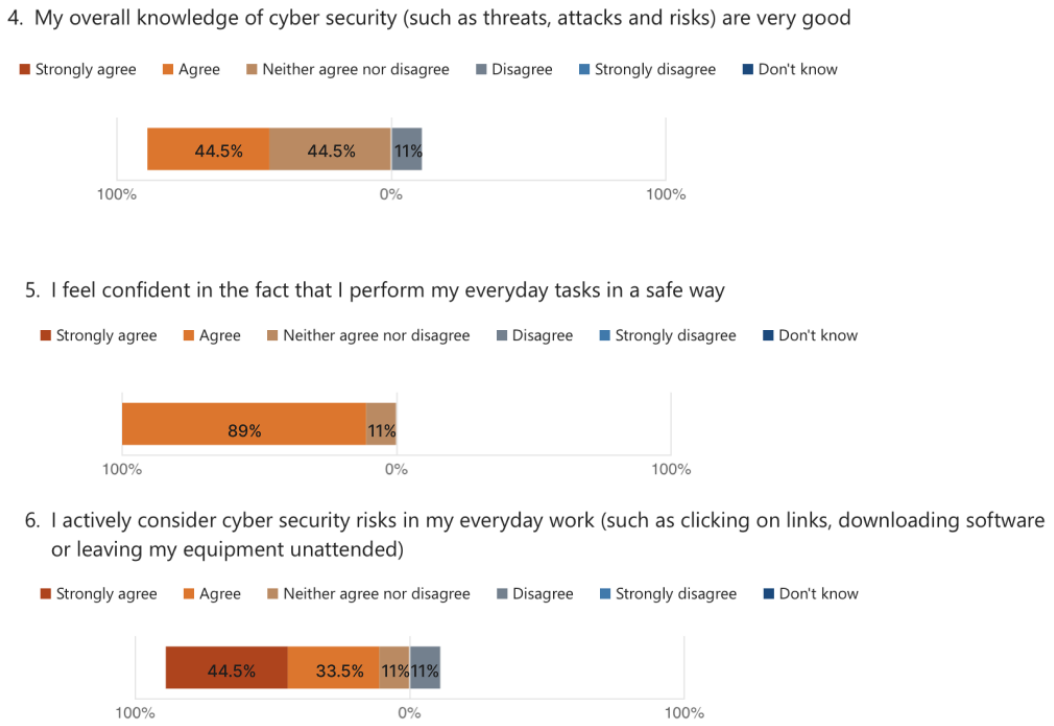


Figure 6.3: The self-estimations of the traditional education participants for round one of the knowledge test

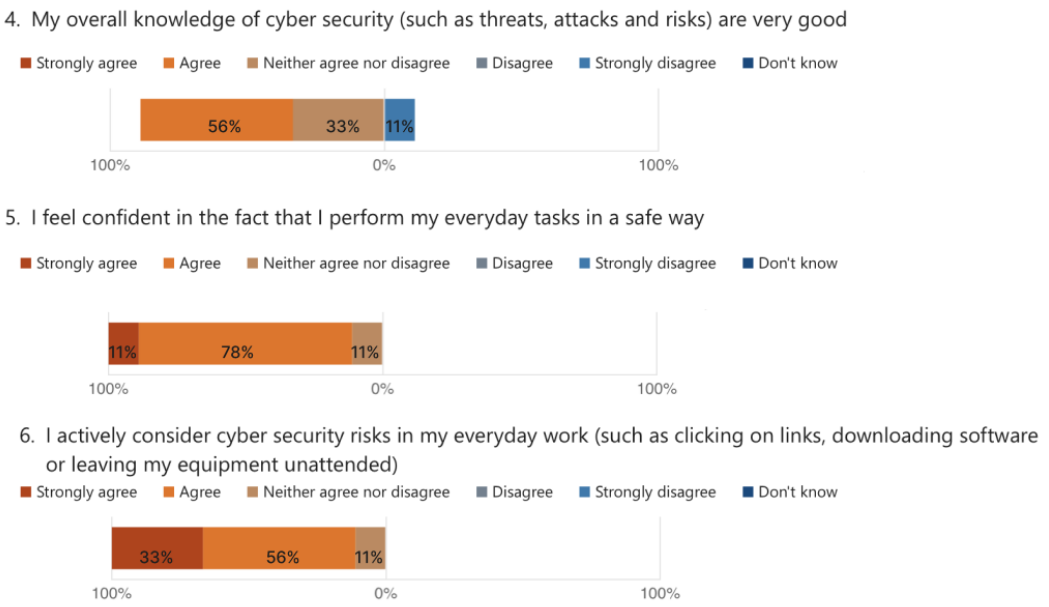


Figure 6.4: The self-estimations of the traditional education participants for round two of the knowledge test

Knowledge test results

Below in table, 6.3, the results from the quiz can be viewed. Table 6.1 shows the percentage of participants who are *Correct, Incorrect* or *Don't know* within the three security topics, calculated according to the guidelines described in section 6.1.1.

Table 6.3: Results from knowledge test right after completing traditional security education

TRADITIONAL ROUND 1	Definition			Case		
	Correct	Incorrect	Don't know	Correct	Incorrect	Don't know
Spoofing	89%	0%	11%	78%	20%	2%
Repudiation	89%	0%	11%	67%	16.5%	16.5%
Information Disclosure	78%	0%	22%	78%	16.5%	5.5%

Table 6.4: Results from knowledge test two weeks after completing traditional security education

TRADITIONAL ROUND 2	Definition			Case		
	Correct	Incorrect	Don't know	Correct	Incorrect	Don't know
Spoofing	56%	22%	22%	69%	20%	11%
Repudiation	67%	0%	33%	50.5%	22%	27.5%
Information Disclosure	78%	0%	22%	56%	22%	22%

From the above results, a few general conclusions can be drawn.

Compared to the results from the initial knowledge test, which can be found in table 3.1, the employee's general knowledge about repudiation and information disclosure has advanced, meanwhile the spoofing knowledge has suffered a drawback.

When comparing the results from the knowledge test directly after completing the PowerPoint education and two weeks after, there has been a significant drop in knowledge regarding the definitions of spoofing and repudiation. However, knowledge about the definition of information disclosure has remained the same.

6.4 Comparison

Table 6.5: Overview of the results from all tests

	Initial		Game 1		Game 2		Traditional 1		Traditional 2	
	Definition	Case	Definition	Case	Definition	Case	Definition	Case	Definition	Case
Spoofing	65%	85%	80%	82%	90%	78%	89%	78%	56%	69%
Repudiation	47.5%	20%	90%	50%	80%	45%	89%	67%	67%	50.5%
Information Disclosure	70%	35%	80%	65%	100%	85%	78%	78%	78%	56%

Some general conclusions can be drawn when analyzing the results shown in table 6.5. When one compares the results from round one of the game and round one of the traditional education, it is clear that traditional performs better on the case questions for repudiation and information disclosure, while the result for spoofing is quite similar with a slightly higher score for the game. This is interesting since traditional performed better in regards to the definition of spoofing.

When analyzing round two of the game and the traditional education, the game participants performs significantly better than the participants that completed the traditional education on all areas, with the exception of the case questions for repudiation. It is also clear that the participants that played the game in greater occurrence answers incorrectly rather than Don't know while the opposite is true for the one's that participated in the traditional education, as seen in table 6.1 - 6.4. These points will be discussed further in chapter 7. One can also see that the case knowledge of spoofing has decreased for both the game and the traditional education compared to the initial knowledge levels, while the opposite is true for repudiation and information disclosure. The knowledge level of definitions have generally increased for both groups, with the only exception being the definition of spoofing for round two of the traditional education.

The self-estimations of the knowledge and confidence levels of the participants show that the game participants in general are more confident in their knowledge levels compared to the participants that completed the traditional education. This will be discussed further in chapter 7.

Chapter 7
Discussion

This chapter will explore findings and discussion points from all phases of the thesis, including the methods used, patterns and possible reasons for the knowledge results, as well as answering the research questions of the thesis and possible future work.

7.1 Method discussion

For the following sections the used methods will be discussed to give the reader perspective on the chosen methods, and also to present potential pros and cons of using certain methods. Moreover, it is of interest to discuss certain events troughout the method.

7.1.1 Collection of data

The method of data collection for the knowledge study was the test presented in section 6.1, and can be seen in its entirety in appendix B. The participants completed the knowledge test without assistance or monitoring by us, and completed it anonymously. We believe this method enables the participants to answer the test honestly, without the feeling of being judged or shamed by their knowledge level. However, this method also resulted in some difficulties. One main issue is that we cannot be completely certain that participants did not violate our guidelines of answering the test. The guidelines clearly stated that the participant were **not** allowed to search for any information while filling out the test. However, due to the lack of monitoring, we can not guarantee that this was respected by the participants. Likewise, the anonymity posed a problem for us. This study consisted of multiple occasions where the user were asked to partake in filling out the test to measure their knowledge. Due to the anonymity, we could not see which participants had completed the test, and whom had not. Because of this, we had to contact all participants multiple times to remind them all to please complete the test. This resulted in additional workload for both us and the participants that could have been avoided if the test was not anonymous. However, we believe that the value of having the test being anonymous out-weights this additional workload.

7.1.2 Test participants

In the following sections we will be discussing the age range, gender distribution and the participants nationalities, of our participants. Both the participants from the usability testing done on our different prototypes, as well as the participants from the final and knowledge test will be discussed.

Usability testing

The participants of the usability tests throughout the study volunteered to participate freely. This means that the representation of age and gender identity does not completely match the overall representation within the company. We chose to enable users to participate freely because we wanted to get thorough data from employees who were interested in the project and were willing to share their honest opinion. Additionally, user testing can be quite time extensive, another reason why we chose to use volunteering participants. We also chose to only perform usability testing at the Lund office. This was due to that fact that we wanted to perform all usability tests on site to enable observation of behavior, and we had a strict time limit for our visit to Germany that did not allow time for both usability testing and the final knowledge test. Hence, we only performed usability tests at the Lund site.
Another important aspect to discuss is why we decided to mix both participants who had conducted usability tests on previous versions of the game, as well as participants who had not previously usability tested our product. This was a conscious decision we made due to the fact that we wanted to collect the viewpoints both from participants who had experienced previous versions of the game and hence could comment on the development and improvements of the game, as well as participants that played the game for the very first time. The viewpoint of participants who plays the game for the first time is also very important, since it reflects how the game could be used in the future by Acme, as well as by the participants of our final knowledge study.

Final knowledge study

For the initial knowledge test we had twenty (n=20) participants, ranging in age from 19-55 and three of them were women. Even tough one might want 50% men and 50% women participating, we did not strive for that since it would not reflect Acme's gender distribution.

Five of the test persons were German employees and were based in a German office, all of which took part in the group playing the game. There is a reason behind not splitting the Germans in to the two different groups, letting half of them play the game and half of them go through the traditional one. Firstly, the reason behind one group doing a traditional security education is to have a control group, that is educated the way Acme does today, so we can compare the outcome. The Germans have all their current security education in German and we are not fluent in German and could hence not make a German version of the traditional security education. This means that we could not offer a way for the Germans to complete a traditional security education the way they are used to. The aim for this study is to investigate how to teach about security topics in a global company, meaning that there are language barriers that has to be taken into consideration. The aspiration is that all employee's will be able to play the game in English and not translated into their native language. This since a global tech company needs a common language, and moreover the language of internet,

tech and security is considered to be English. Therefore, to keep the control group as close as possible to Acme's current security educations and to investigate how to educate a global tech company we put all Germans in the game group.

An important aspect to mention is that three out of the total amount of eleven people who participated in the different iterations of usability testing of the game also participated in the game group of the main knowledge study. This is not ideal, since the participants had previous experience of the game and it's topics before the educational opportunity, and hence could affect the knowledge levels in a biased way. The reason for this was mainly the lack of available test participants from our main target group. However, if the study was to be re-conducted and/or expanded further, this is something that should be avoided to reduce the risk of biased results.

As mentioned in sections 6.2.1 and 6.3.1, the average age of the game group were 30-39, and 40-49 for the group that underwent the traditional education. It could have reflected our target group better to have the same average age and age span for both the groups. However, since the study is based on participants that voluntarily played the game or did the traditional education, it was hard to pick exactly which participant we wanted for which group within the study. Playing the game also required a bit more time than doing the PowerPoint based education, which older employees with more responsibilities sometimes have harder to find. Instead they preferred the traditional education which both was faster to complete and could be done whenever it fit their schedule.

In the beginning of this study we derived requirements, the three threats that the game focuses on, partly by letting all twenty participants take the same initial knowledge test. We chose to base the requirements on all twenty participants, instead of splitting the group in to two smaller groups, which is done later in the study. If we would have derived the requirements on two different groups, with ten participants in each, the results for each group could have differed from each other, resulting in different needs for the two groups. We would in that case have to make educations and knowledge tests focusing on different threats, making it hard to compare the knowledge and ways of learning. However, that would have made the educations more adapted to each group. If we had a larger sample size, where we could be sure that the derived requirements reflected a much larger part of the company, it would have been interesting to keep the groups separated trough out the entire study. Therefor, since the sample size is small and we wanted to compare their knowledge, we chose to base the requirements on all twenty participants and then split them in to two groups later in the study.

7.1.3 Usage of STRIDE & DREAD

As mentioned in section 2.1 STRIDE has been criticised [28] for being cross-correlated, meaning that some of the threats STRIDE process imply each other. However, diverse threat modeling are not necessary contradictory and thus multiple models can be applied to the same organisation [11]. To get a wider knowledge and more perspectives of the potential threats Acme could be a victim of, we chose to use two different frameworks. Even though they sometimes overlap each other, it is rather beneficial while it proves conclusions, rather than sprawls the analysis. By using first using STRIDE to identify threats and then evaluating them using DREAD we have gotten a good overview of Acmes relation to that threat. Worth mentioning is that the analysis is done on a high level, and nor do these used frameworks

promote detailed analysis. For the sake of Acme, it is the high level threats that needs awareness to get general knowledge about different threats, instead of very detailed information about a certain threat.

7.2 Result discussion

The following section brings up discussion points in regards to the results presented in chapter 6. Both findings from the knowledge study as well as the self-estimation of the participants will be discussed.

7.2.1 Knowledge results

Some interesting points can be discussed in relation to the knowledge results found in this study, presented in chapter 6. A first important point to discuss is the assessment of *Correct*, *Incorrect* and *Don't Know*. We decided to do the assessment according to the method described in paragraph 6.1.1, a rather harsh way of measuring the results from the knowledge tests. However, one of the main aspects of both the game and the traditional education is to highlight the depth of the three chosen threats, and the multiple consequences they can give rise to. Because of this, we chose to rate the answers according to a "majority" principle, where the participants had to choose the majority of the correct answers for it to count as correct, not just one of them. However, this method gave rise to an interesting phenomenon in the results. It became clear that the game participants often answered incorrect rather than Don't know. This might give the appearance that the game participants did not have as deep knowledge as the traditional education participants. However, due to the method of deciding what is correct and what is not, this must not necessarily be the case. When closely examining the individual answers, we noticed a trend that rather showed that the game participants that answered incorrectly often combined incorrect and correct answers, resulting in an overall incorrect answer according to our method of grading. Thus, the game participants in greater occurrence chose both correct and incorrect answers for the multiple choice questions, while the traditional education participants rather choose the answer Don't know.

When analyzing the results from each separate threat, we also found some interesting areas of discussion. The initial knowledge level for spoofing was high, and remained relatively high for both the game and the traditional education, making it difficult to draw any clear conclusions. However, the result for spoofing from round two of the traditional education shows a decline in knowledge from both the initial level and the level from round one. This is interesting, since this means that the participants decreased their knowledge over time, although they partook in a learning opportunity during that time. This can have many different causes, such as confusion, uncertainty or stress for the participants.

Information disclosure was the area were one can see the sturdiest increment of knowledge from both groups. This might be due to the linguistic phrasing of the threat. The term information disclosure quite clearly reflects the threat and it's consequences, resulting in that once the participant learnt the meaning of the threat, they could connect and remember the meaning of the threat to the name of the threat, aiding in learning.

A similar reasoning might explain the results found for repudiation. The increase from the initial knowledge levels to the knowledge levels of round one were large for both groups,

and for the game participants remained on a high level even for the second round of the knowledge test, although with a slight decrease. For round two of the traditional education however, the knowledge levels dropped quite a lot in regards to repudiation. This might also be due to the linguistic phrasing of the threat, that might rather present a difficulty in the case of repudiation. Repudiation is not as common as the words information disclosure, and at least four of the participants expressed that they were unfamiliar with the word during the knowledge test. In regards to the difference in knowledge between round two of the game and round two of the traditional education, this might be due to the reason that the game participants actively explored the meaning behind the threat, and not only read about it, enabling a deeper level of knowledge. This theory also have support in the experiential learning theory, where one can achieve a deeper level of knowledge by experiencing the concept, as described in section 2.3.1. Another interesting trend that supports this suggestion is that the game participants increased their knowledge levels from round one to round two of knowledge tests, even though no further education opportunity was conducted. This supports the statement that the game enabled the players to have a more profound learning experience, that grew and substantiated over time, resulting in higher knowledge levels for round two.

7.2.2 Self estimation vs Result

As presented in section 6.4, the results from the self-estimation questions of the surveys show that the game participants rate their knowledge and confidence higher than the traditional education participants. This is interesting, since it on an overall level corresponds to their actual knowledge levels. In other words, the game participants perceive themselves as more knowledgeable than the traditional education group, and they are, according to the results presented in section 6.4. If one looks at round one versus round two of both the game and the traditional education, one can see a slight increase in the self-estimation of knowledge. However, this increase is too slight to serve as a base to any generalizations about the results.

7.3 Research Questions

Which are the biggest software security risks at a global tech company? From the initial knowledge test and the threat analysis, found in chapter 3, we concluded that spoofing, repudiation and information disclosure are the biggest threat to Acme. The employees of Acme had the least knowledge about, according to the results from initial knowledge test in section 3.1, repudiation which is denying having performed an action or changing logs logging such actions. This was closely followed by information disclosure which concerns allowing people to access information to which they are not authorized to access. Compared with spoofing, tampering, denial of service and elevation of privilege, Acme employees had less awareness of repudiation and information disclosure. This can be due to spoofing and denial of service being commonly known threats, and tampering and elevation of privilege are threats which meaning can be derived from the actual words. From the threat analysis, which results can be found in table 3.2, Spoofing is the biggest threat, followed by information disclosure. These are hence the biggest technical threats to which Acme is vulnerable to. From these we concluded that spoofing, repudiation and information disclosure are the biggest threats for a tech company, both when existing knowledge and

potential ways of performing threats, are taken into consideration.

How can a user experience based on usability and gamification aid in learning? This study explored a user centered solution, focusing on usability, gamification and psychological theories in regards to learning. The result showed an overall clear increase in the users knowledge levels, both in regards to concrete knowledge such as the definitions of terms and key words, as well as on a more high level, abstract conceptual level in the form of scenarios. The study also showed that a user centered solution cause a deeper level of learning, since the users remained on a high level of knowledge during the follow up test two weeks after the learning opportunity, and in some cases even increased their knowledge levels compared to the test taken directly after the learning opportunity. Hence, one can conclude that a user experience based on usability and gamification, with a focus on engagement and experiential learning, aid in both concrete and abstract knowledge.

How can you achieve a higher level of learning with the use of a digital, interactive tool compared to traditional learning in regards to software security? An interesting pattern emerged in the results of the study when comparing the digital, interactive solution to the traditional learning method at Acme. The results from the knowledge tests conducted directly after a learning opportunity show that the ursers who partook in the traditional education performed slightly better compared to the users who used the interactive tool. However, the results witness about the fact that the digital, interactive solution enables a deeper level of knowledge. When looking at the knowledge levels two weeks after the users partook in a learning opportunity, an interesting fact was found. Not only did the users who conducted the education via the interactive solution perform better than the group who partook in the traditional education, they even performed better than themselves two weeks prior. This suggests that the digital, interactive tool gives rise to a deeper, more profound learning experience that grows the users knowledge over time in regards to software security.

7.4 Future Work

To continue and improve this study regarding whether gamification can aid in learning there are a further developments that could be done.

To start with, the implemented game was significantly limited to the used framework and the time scope of this master's thesis. The game was therefore in many cases not too advanced when it comes to graphical game element, which could be further explored. Perhaps the player would get more involved in the game, but maybe at the expense of missing the learning opportunity by being too caught up in the game.

For this game we have focused on two motivators, Development & Accomplishment and Empowerment of Creativity & Feedback from the Octalysis Framework, described in section 2.3.4. For future work it would interesting if focus were put on two different areas to see if the game motivated the players more and aided even more in learning about security topics. One idea would be to focus on the motivator Ownership & Possession where user could make their own character to which they perhaps would care more about and connect to. Here one could include the motivator Epic Meaning & Calling which means that the player feels that

it is doing something for the greater good. By changing the conceptual design from being a hacker to being a hero saving Acme from security threats, that motivator would be included in the game, and perhaps motivate the players even more. However, every person is motivated by different things and it is therefore hard to decide which motivators to focus on since the framework says to focus on a few rather than implement all.

Additionally, it would be of value visiting, discovering and including more offices around the world to further investigate how to educate Acme in security topics. As previously mentioned in section 7.1.2, Main Study, we wanted people based in other countries with native languages other than English or Swedish, to play the game to examine how to educate a large organization.

Further, a follow up even later than two weeks could be interesting. This is to see if the participants have reached the final phase of Kolb's Circle of Learning and hence absorbed the knowledge and are able to use it for decision-making and problem-solving. A new knowledge test, containing new questions, could be introduced to test deeper knowledge and to examine if the participants have reached the last phase in Kolb's Circle of Learning.

One of the ambitions for this master's thesis was to improve the security education throughout employees work life, which corresponds well to UN's global goal no 4 *Quality Education*. Since it seems like this study shows that gamification aid in learning, this is an area in which it would be of interest to investigate further development. That could lead to more innovations within the area, promoting inclusive and sustainable industrialization and fostering innovation which is UN's global no 9.

Chapter 8
Conclusion

This master's thesis has investigated how user experience based on usability and gamification can aid in learning in regards to software security. This was explored by creating a computer game which Acme's employees tried out as a new way of learning about software security.

To identify which security topics to aim attention to in the game we concluded a user research on Acme's employees and a threat analysis on the services used by Acme's employees. Using the threat analysis frameworks STRIDE and DREAD, analyzing Acme on a high level, combined with a user research consisting of a initial knowledge test, resulted in three security topics to focus on. These three security threats, spoofing, repudiation, and information disclosure, were then considered as the biggest software security threats to Acme.

From the derived security topics we created a game, where each level focused on a security threat, keeping user experience and usability in mind when creating tasks. Even though our hands were tied a bit by the framework, Root the Box, we designed the game to be as user friendly and motivating as possible, by usability testing, re-implementing and utilizing the frameworks already built-in features to suit the chosen motivators from the Octalysis framework.

The final conclusion was not only that experience based on usability and gamification do aid in learning, but also that deeper learning concerning security also benefits from learning with the use of a digital, interactive tool compared to traditional learning. This was shown by letting one group of Acme's employees undergo a traditional security education, while another group played the game. The two groups results from taking a knowledge test immediately after and two weeks after the education were then compared, showing that the ones who played the game performed better. Not only did the group playing the game perform better, but also estimated their knowledge as higher, which corresponded to their actual knowledge level.

However, the results could be a coincidence, and supplementary studies with more participants and more thorough investigations could contribute to and support this master's thesis further.

References

[1] Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel. New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers, 2022. Accessible: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers.

[2] The Ascent. 5 Ways to Prevent a Man-in-the-Middle Cyberattack, 2022. Accessible: https://www.fool.com/the-ascent/small-business/endpoint-security/articles/mitm/.

[3] Greg Belding. Ethical hacking: Log tampering 101, 2019. Accessible: https://resources.infosecinstitute.com/topic/ethical-hacking-log-tampering-101/.

[4] Ernesto A. Bustamante and Randall D. Spain. Measurement invariance of the nasa tlx. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 52(19):1522 – 1526, 2008.

[5] Franco Callegati, Walter Cerroni, and Marco Ramilli. Man-in-the-middle attack to the https protocol. *IEEE Security Privacy*, 7(1):78–81, 2009.

[6] Conor Cawley. Phishing Scams are the Most Common Cyber Attack, Says FBI, 2022. Accessible: https://tech.co/news/phishing-scams-most-common-fbi.

[7] Wesley Chai. What is the CIA triad (confidentiality, integrity and availability)?, 2023. Accessible: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA.

[8] Krittika Das, Rajdeep Basu, and Raja Karmakar. Man-in-the-middle attack detection using ensemble learning. In *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–6, 2022.

[9] Sowmya Dhandapani. Integration of user centered design and software development process. In *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 1–5. IEEE, 2016.

[10] Victoria Drake. Threat Modeling, 2021. Accessible: https://owasp.org/www-community/Threat$_{M}$*odeling*.

[11] Chuck Easttom. *Threat Analysis*. Springer International Publishing, 2020.

[12] Braiterman et. al. Threat Modeling Manifesto, 2020. Accessible: https://www.threatmodelingmanifesto.org/principles.

[13] Moloch et al. Root the Box, 2023. Accessible: https://github.com/moloch–/RootTheBox.

[14] EC-Council: Cybersecuirty Exchange. DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis, 2022. Accessible: hhttps://eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/.

[15] Fortinet. Buffer Overflow. Accessible: https://www.fortinet.com/resources/cyberglossary/buffer-overflow.

[16] Robert W. Gehl and Sean T. Lawson. *Social engineering. how crowdmasters, phreaks, hackers, and trolls created a new form of manipulative communication.* The MIT Press, 2022.

[17] John D. Gould and Clayton Lewis. Designing for usability: Key principles and what designers think. *Commun. ACM*, 28(3):300–311, mar 1985.

[18] Charles Griffiths. The Latest 2023 Phishing Statistics (updated January 2023), 2023. Accessible: https://aag-it.com/the-latest-phishing-statistics/.

[19] Shawn Hernan, Scott Lambert, Tomasz Ostwald, and Adam Shostack. Threat Modeling Uncover Security Design Flaws Using The STRIDE Approach, 2019. Accessible: https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach.

[20] Computer Hope. How to view the HTML source code of a web page, 2021. Accessible: https://www.computerhope.com/issues/ch000746.htm.

[21] Ruben Hubert, Anna Bánáti, László Erdődi, and Rita Fleiner. Strengthening database security with capture the flag exercises. In *2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES)*, pages 000137–000142, 2022.

[22] Dana Chisnell Jeffrey Rubin. *Handbook of Usability Testing, Second Edition.* Wiley Publishing, Inc., 2 edition, 2008.

[23] Yu kai Chou. The Octalysis Framework for Gamification & Behavioral Design, 2013. Accessible: https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/.

[24] Sangkyun Kim, Kibong Song, Barbara Lockee, and John Burton. *Gamification in Learning and Education. Enjoy Learning Like Gaming.* Advances in Game-Based Learning. Springer International Publishing, 2018.

[25] Loren Kohnfelder and Praerit Garg. hat is STRIDE and How Does It Anticipate Cyberattacks?, 2021. Accessible: https://securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks/.

[26] David A Kolb. *Experiential learning : experience as the source of learning and development.* Prentice-Hall, 1984.

[27] John Leach. Improving user security behaviour. *Computers & Security*, 22(8):685–692, 2003.

[28] David LeBlanc. DREADful, 2014. Accessible: https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff699289(v=pandp.10).

[29] Yatao Li and Danqing Zhao. Design and development of problem-based educational game. In *2022 4th International Conference on Computer Science and Technologies in Education (CSTE)*, pages 309–313, 2022.

[30] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla, and Anandha Murukan. *Improving Web Application Security: Threats and Countermeasures*. Microsoft, 2003.

[31] Microsoft. Repudiation, 2021. Accessible: https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/repudiation.

[32] Microsoft. Microsoft denial-of-service defense strategy, 2023. Accessible: https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-dos-defense-strategy.

[33] Rajalakshmi Shenbaga Moorthy and P. Pabitha. Optimal detection of phising attack using sca based k-nn. *Procedia Computer Science*, 171:1716 – 1725, 2020.

[34] United Nations. Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation. Accessible: https://sdgs.un.org/goals/goal9.

[35] United Nations. Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all. Accessible: https://sdgs.un.org/goals/goal4.

[36] United Nations. THE 17 GOALS. Accessible: https://sdgs.un.org/goals.

[37] Jakob Nielsen. Why You Only Need to Test with 5 Users, 2000. Accessible: https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/.

[38] Brian Gore Phil So. NASA TLX, Task Load Index, 2020. Accessible: https://humansystems.arc.nasa.gov/groups/tlx/index.php.

[39] Jennifer Preece, Yvonne Rogers, and Helen Sharp. *Interaction Design - Beyond Human-Computer Interaction*. Addison-Wesley Professional, 2 edition, 2016.

[40] Amazon Web Services. AWS Shield, 2023. Accessible: https://aws.amazon.com/shield/.

[41] A. Shostack. *Threat Modeling: Designing for Security*. John Wiley & Sons„ 2014.

[42] Stefan Stieglitz, Christoph Lattemann, Susanne Robra-Bissantz, Rüdiger Zarnekow, and Tobias Brockmann. *Gamification. Using Game Elements in Serious Contexts.* Progress in IS. Springer International Publishing, 2017.

[43] Verizon-Business. 2022 Data Breach Investigations Report, 2023. Accessible: https://www.verizon.com/business/resources/reports/dbir/?CMP=OOH$_S$$MB_OTH$ $_2$2222$_M$$C_2$0200501$_N$$A_N$$M20200079_0$0001.

[44] Le Wang and Alexander M. Wyglinski. Detection of man-in-the-middle attacks using physical layer wireless security techniques. *Wireless Communications and Mobile Computing*, 16(4):408–426, 2016.

[45] K. Yonemura, K. Yajima, R. Komura, J. Sato, and Y. Takeichi. Practical security education on operational technology using gamification method. National Institute of Technology, Dept. of Information and Computer Engineering, Chiba, Japan, 2017.

Appendices

Appendix A
Inital Knowledge Test

Initial knowledge test - How to educate an organisation within security topics

Hello, and thank you for taking the time to answer our survey and help us with our master's thesis. Before you start, we would like to point out a few things:

- This is not a test meant to rate your personal knowledge. We will focus on how people learn, not the specific knowledge of certain employees.
- Take your time to answer this survey, but do not over-think your answers. If you do not know the answer to a question, that's ok. Like previously mentioned, we want to investigate learning, not individuals specific knowledge per se.
- You are not allowed to google or look for answers in any other way during this test.

If you have any questions, don't hesitate to contact Anna Dahlström or Felicia Gabrielii Augustsson.

Questions marked with * are mandatory. Questions with circles only allow for one chiose while quetions with boxes/squares allow for multiple choice.

Basic info and self-estimation of knowledge

1. **Profession / role at Acme: *:** _____
2. **Gender identity: ***
   - ○ Woman.
   - ○ Man.
   - ○ Non-binary.
   - ○ Prefer not to say.
3. **Age: ***
   - ○ 20-29
   - ○ 30-39
   - ○ 40-49
   - ○ 50-59
   - ○ 60-69
   - ○ Other: _____
4. **My overall knowledge of cyber security (such as threats, attacks and risks) are very good: ***
   Strongly agree ○—○—○—○—○—○ Strongly disagree
5. **I feel confident in the fact that I perform my everyday tasks in a safe way: ***
   Strongly agree ○—○—○—○—○—○ Strongly disagree
6. **I actively consider cyber security risks in my everyday work (such as clicking on links, downloading software or leaving my equipment unattended) : ***
   Strongly agree ○—○—○—○—○—○ Strongly disagree

Security questions about STRIDE

STRIDE is a threat modeling framework developed by two security engineers on Microsoft. STRIDE is an acronym and each letter represents a security threat, Spoofing, Tampering, Repudiation, Information Disclosure, denial of service, and elevation of privilege. In the following questions, please fill in the blanks.

7. **… is pretending to be something or someone other than yourself. ***
   - ○ Tampering
   - ○ Information Disclosure
   - ○ Repudiation
   - ○ Spoofing
   - ○ None of the above
   - ○ I don't know
8. **… is when a malicious person attacks the logs, by changing them, making it hard to see who did what. ***

- ○ Spoofing
- ○ Information Disclosure
- ○ Denial of Service
- ○ Elevation of Privilege
- ○ None of the above
- ○ I don't know

9. **… is when an application gains rights or access that should not be available to them. ***
   - ○ Spoofing
   - ○ Tampering
   - ○ Elevation of Privilege
   - ○ Information Disclosure
   - ○ None of the above
   - ○ I don't know
10. **… is to deny that you have performed a particular operation or were not responsible for the operation. ***
   - ○ Denial of Service
   - ○ Spoofing
   - ○ Repudiation
   - ○ Elevation of Privilege
   - ○ None of the above
   - ○ I don't know
11. **… is when access to a particular service should have been granted, but in fact was improperly rejected due to the resource being absorbed. ***
   - ○ Repudiation
   - ○ Denial of Service
   - ○ Elevation of Privilege
   - ○ Tampering
   - ○ None of the above
   - ○ I don't know
12. **… is to modify something, e.g. on a disk, on the network or in memory. ***
   - ○ Elevation of Privilege
   - ○ Repudiation
   - ○ Tampering
   - ○ Denial of Service
   - ○ None of the above
   - ○ I don't know

13. **… is allowing people to see information which they were not authorized/privileged/allowed to see. ***
    - ○ Spoofing
    - ○ Elevation of Privilege
    - ○ Tampering
    - ○ Information Disclosure
    - ○ None of the above
    - ○ I don't know

Case:

In the following section of questions there will be some examples of possible cyber security attacks. Choose the option you find most fitting to the described attack, or "none of the above" if you don't think any option is suitable.

14. **Fake email messages appearing to be from a trusted business asking for personal information such as passwords can be considered as a phishing attack. What should you do if you think you've been exposed to a phishing attack, i.e. you have entered your credentials on a malicious website? ***
    - ○ Go back to the same malicious website and enter a fake password to your username to trick the attacker
    - ○ Avoid changing passwords since the attacker will be able to see those as well
    - ○ Change password as soon as possible before the attacker has the chance to
    - ○ Get the unit offline so the attacker can't gain access to anything else
    - ○ I don't know
15. **A Man-in-the-middle attack is a cyber attack where a malicious person listens in on, and potentially alters, the communication of two parties who think they are communicating directly with each other. The man in the middle can for example make individual connections with the two parties and pretend to be the person they intend to communicate with, while the man in the middle actually controls the entire communication between them all. Is there any way to effectively protect yourself from a man-in-the-middle attack? Choose the answers you find most fitting, or "none of the above" if you don't think any option is suitable. ***
    - ☐ A VPN is an effective way to protect yourself
    - ☐ Never visit sites that does not use the https protocol
    - ☐ Don't download software from sources you are unsure of
    - ☐ Only use wifi's that are password protected
    - ☐ Non of the above
    - ☐ I don't know

16. **A so-called Yo-yo attack, a type of DoS attack, is aimed at cloud-hosted applications which use autoscaling. The attacker generates a flood of traffic so the cloud-hosted service scales outwards to handle the increase of traffic, then halts the attack, leaving the victim with over-provisioned resources. When the victim scales back down, the attack resumes, causing resources to scale back up again. This can result in a reduced quality of service during the periods of scaling up and down and a financial drain on resources during periods of over-provisioning while operating with a lower cost for an attacker compared to a similar attack, as it only needs to be generating traffic for a portion of the attack period. Can you as an employee of Acme do something to protect yourself from being exposed to a Yo-yo attack? ***
    - ○ Yes, I can make sure not to visit services I'm not currently using
    - ○ No, I'm not in charge of the servers
    - ○ No, not directly but I can let the IT department know that I'm having trouble using the resource I want
    - ○ Yes, by using as many services as possible so the cloud-hosted service don't scale down
    - ○ I don't know
17. **You notice that some of the configuration files have been changed and behave incorrectly. You check the logs and who have changed them. You go and ask the colleague about it but they deny having changed the configuration files. To what threat is this connected? Choose the answer you find most fitting, or "none of the above" if you don't think any option is suitable. ***
    - ○ Repudiation
    - ○ Spoofing
    - ○ Denial of Service
    - ○ Elevation of Privilege
    - ○ None of the above
    - ○ I don't know
18. **Process Injection is a tool that has the capabilities to enumerate all running processes on a system as well as the account running the process. A process can then be identified, and injected by the attacker by a simple command. What does a attacker need in order to perform this attack? Choose the answer you find most fitting, or "none of the above" if you don't think any option is suitable. ***
    - ○ Be on the same network as the victim
    - ○ Access to an account with higher permission levels
    - ○ A physical access card
    - ○ Information on how to request access to the wanted process
    - ○ None of the above
    - ○ I don't know

19. **The Access control list (ACL) is a list of permissions that specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. An attacker could take advantage of inappropriate or missing ACLs. What could happen if a attacker gains access to the ACLs? Choose the answers you find most fitting, or "none of the above" if you don't think any option is suitable. ***
    - ☐ Get access to more data than they are supposed to
    - ☐ The attacker can see who has access to what
    - ☐ The attacker could focus future attacks on specific individuals based on their access
    - ☐ The attacker gets access to all users on the ACLs passwords
    - ☐ None of the above
    - ☐ I don't know

Last few sequrity questions

This section will cover some general security questions.

20. **The CIA Triad of confidentiality, integrity and availability is considered the core underpinning of information security. What does confidentiality mean? ***
    - ○ It means that only authorized persons have access to information, and while unauthorized persons are denied access to them
    - ○ It means that the only person who knows what data you can access is yourself
    - ○ It means protection against improper modification and destruction of information, ensuring that information cannot be changed undetected
    - ○ It means that it should not be possible to see who is has access to what kind of information to prevent social engineering attacks
    - ○ I don't know
21. **The CIA Triad of confidentiality, integrity and availability is considered the core underpinning of information security. What does integrity mean? ***
    - ○ It means protection against improper modification and destruction of information, ensuring that information cannot be changed undetected
    - ○ It means that all data you are authorized to read should also be authorized to modify undetected
    - ○ It means that no one should be able to see who changed what pieces of data, since this intrudes on one's privacy
    - ○ It means that you should have a choice of what information you would like to share
    - ○ I don't know
22. **The CIA Triad of confidentiality, integrity and availability is considered the core underpinning of information security. What does availability mean? ***
    - ○ It means that people get access to the information they are supposed to have.

- ○ It means that you are responsible for what kind of information you have access to.
- ○ It means services should be up and running at all times
- ○ It means that the default rule is that everyone should have access to everything, to achieve transparency
- ○ I don't know

23. A computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems is called. *

- ○ An ethical hacker
- ○ Programmer
- ○ Malicious person
- ○ Social engineer
- ○ I don't know

24. What is the purpose of a Virtual Private Network (VPN)? *

- ○ VPN tunnels slow down internet traffic, making it harder for hackers to sniff valuable information during such long times.
- ○ The user of a VPN becomes anonymous since it redirects the IP address, making it hard for an attacker to know where to aim their attack.
- ○ VPN redirects your IP address and sets up a secure connection and encrypts your data, making it secure to use even on a open network.
- ○ It protects you against installing malware since the VPN tunnel protects you from viruses.
- ○ I don't know

25. How can you decide if a link in an email is a phishing link or not?? *

- ○ They ask for your login credentials to authorize yourself
- ○ By looking at the sender to verify it's from a trusted source
- ○ By closely inspecting the URL and see if it looks ok
- ○ Click the link, enter your username with the incorrect password and if the incorrect password is accepted you know it is a malicious website
- ○ I don't know

Appendix B

Final knowledge Test

Final knowledge test - How to educate an organisation within security topics

Hello, and thank you for taking the time to answer our survey and help us with our master's thesis. Before you start, we would like to point out a few things:

- This is not a test meant to rate your personal knowledge. We will focus on how people learn, not the specific knowledge of certain employees.
- Take your time to answer this survey, but do not over-think your answers. If you do not know the answer to a question, that's ok. Like previously mentioned, we want to investigate learning, not individuals specific knowledge per se.
- You are not allowed to google or look for answers in any other way during this test.

If you have any questions, don't hesitate to contact Anna Dahlström or Felicia Gabrielii Augustsson.

Questions marked with * are mandatory. Questions with circles only allow for one chiose while quetions with boxes/squares allow for multiple choice.

Basic info and self-estimation of knowledge

1. **Profession / role at Acme: *:** _____
2. **Gender identity: ***
   - ○ Woman.
   - ○ Man.
   - ○ Non-binary.
   - ○ Prefer not to say.
3. **Age: ***
   - ○ 20-29
   - ○ 30-39
   - ○ 40-49
   - ○ 50-59
   - ○ 60-69
   - ○ Other: _____
4. **My overall knowledge of cyber security (such as threats, attacks and risks) are very good: ***
   Strongly agree ○—○—○—○—○—○ Strongly disagree
5. **I feel confident in the fact that I perform my everyday tasks in a safe way: ***
   Strongly agree ○—○—○—○—○—○ Strongly disagree
6. **I actively consider cyber security risks in my everyday work (such as clicking on links, downloading software or leaving my equipment unattended) : ***
   Strongly agree ○—○—○—○—○—○ Strongly disagree

Section 1/7

7. **What is Information Disclosure? ***
   - ○ To pretend to be someone you are not
   - ○ When an application is given access to something that should not be accessible
   - ○ To deny the fact that you have performed a particular action
   - ○ Accidentally sharing information, potentiality exposing vulnerabilities
   - ○ I don't know
8. **Which of these examples can be considered Information Disclosure? ***
   - ☐ Using someone else's user login to perform an action
   - ☐ Sharing contact information
   - ☐ Showing extensive error messages
   - ☐ Giving all users access to everything per default
   - ☐ I don't know

Section 2/7

9. **What is spoofing? ***
   - ○ Searching for sensitive information in error messages
   - ○ Denying your actions upon confrontation
   - ○ Pretending to be someone you are not
   - ○ To modify the network so that phising emails can pass trough easier
   - ○ I don't know
10. **How can you identify a phishing mail? ***
   - ☐ They ask for your login credentials to authorize yourself
   - ☐ By looking at the sender to verify it's from a trusted source
   - ☐ By closely inspecting the link/URL and see if it looks ok
   - ☐ Click the link, enter your username with the incorrect password and if the incorrect password is accepted you knoe it is a malicious website
   - ☐ I don't know
11. **How can I protect myself against spoofing? ***
   - ○ Change the logs before an attacker can track my activity
   - ○ Stop sharing my email with persons outside the company
   - ○ Closely inspecting links/URLs before clicking on them
   - ○ Use a complex password
   - ○ I don't know
12. **What threats does spoofing present? ***
   - ☐ Spreading malware
   - ☐ Automatically gaining access to all user credentials
   - ☐ Loss of credentials
   - ☐ Legal consequences such as lawsuits
   - ☐ I don't know

Section 3/7

13. **What is repudiation? ***
   - ○ To pretending to be someone you are not
   - ○ Hide your tracks by modifying logs
   - ○ Sharing contact information publicly
   - ○ Accidentally sharing your login credentials on a malicious website
   - ○ I don't know
14. **How can a company protect themselves from repudiation attacks? ***

- ☐ Implement autogenerated and non-changleble logs for user activity
- ☐ Keep their firewalls and spam filters updated
- ☐ Be aware of social engineering
- ☐ Avoid using one general account for multiple employees to use
- ☐ I don't know

Section 4/7 - Case Question 1

15. **A user logs into a company's network and performs an unauthorized action, such as deleting important files. The user later denies having performed the action, making it difficult for the company to hold them accountable for their actions. This is an example of... ***
    - ○ Tampering
    - ○ Spoofing
    - ○ Information Disclosure
    - ○ Repudiation
    - ○ I don't know

Section 5/7 - Case Question 2

16. **A hacker sets up a fake Wi-Fi hotsport with a name that resambles a legitiamte Wi-Fi, such as AcmeGuestWiFi. When users connect to the fake hotspot the hacker can monitor their internet traffic and potentially steal sensitive information such as bank information. This is an example of... ***
    - ○ Information Disclosure
    - ○ Denial of Service
    - ○ Spoofing
    - ○ Repudiation
    - ○ I don't know

Section 6/7 - Case Question 3

17. **A hacker sends and email that appears to be from a legitimate company, but with a forged "From" address. The email asks the recipient to click on a link that leads to a fake login page, where the user is prompted to enter their credentials. This is an example of... ***
    - ○ Spoofing
    - ○ Information Disclosure
    - ○ Repudiation

- ○ Elevation of Privilege
- ○ I don't know

Section 7/7 - Case Question 4

18. **A software developer accidentally publishes a source code repository containing sensitive data, such as private encryption keys, on a public code sharing platform like GitHub. The repository is discovered by a security researcher who contacts the developer but by then the sensitive data my have already accessed by unauthorized parties. This is an example of... ***
    - ○ Elevation of Privilege
    - ○ Information Disclosure
    - ○ Spoofing
    - ○ Repudiation
    - ○ I don't know