TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Science

ITV70LT

Tiia Sõmer 1222414 IVCM

EDUCATIONAL COMPUTER GAME FOR CYBER SECURITY: GAME CONCEPT

Master thesis

Rain Ottis, PhD

Associate Professor, Tallinn University of Technology

Tallinn 2014

Author’s declaration

I declare that this thesis is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Tiia Sõmer

…….. …….

(date) (signature)

Annotatsioon

Käesolev magistritöö käsitleb küberturbealase haridusliku mängu kontseptsiooni loomist, mis oleks kasutatav Riigikaitse valikaine raames küberturbe õpetamisel. Iga mängu loomise aluseks on eelnev kontseptsioon, ning haridusliku mängu kontseptsiooni välja töötamine on käesoleva töö põhieesmärk. Paralleelselt käesoleva magistritööga – ning lähtudes tema tulemustest – on alustatud vastavasisulise haridusliku mängu välja töötamisega.

Töö teostamisel uuriti mängustamise teooriat ja tõsimänge. Samuti vaadati põhikooli ja gümnaasiumi riiklikku õppekava ning analüüsiti seal esitatud pädevusi küberturbe vaatevinklist. Eraldi analüüsiti Riigikaitse valikaine raames õpetatavat, ning välja töötatud mängu kontseptsioon põhineb eelnimetatu raames kasutataval programmil.

Tõsimänge ei kasutata Eesti haridussüsteemis palju, mistõttu analüüsiti ka praegu Majandus- ja Ettevõtlusõppe valikaine raames kasutusel olevaid tõsimänge. Analüüsiti ka maailmas välja töötatud ja kasutusel olevaid arvutimänge küberturbe teadlikkuse tõstmiseks.

Töö tulemusena valmis mängu kontseptsioon, mille alusel saab edasi arendada välja töötatavat prototüüpi.

Annotation

This thesis discusses developing a game concept for an educational game on cyber security, that could be usable for teaching of cyber security within the national defense elective course in Estonian schools. The basis for any game development is a game concept, and the main outcome of this thesis is the provision of a concept for an educational game. In parallel with this thesis – and based on its findings – work on a game prototype has started.

In writing this thesis, the theories of gamification and serious games were analysed. Estonian national school curriculum at all levels was also analysed from the aspect of cyber security competencies. The teaching of cyber security within the national defense elective course was looked at in more detail, and the game concept developed is based on the program as used in the latter.

Serious games are not used very widely in Estonian school system, and therefore those used within Economics and Entrepreneurship elective course were also studied. Cyber security games available and used around the world were also analyzed.

The result of this thesis is a game concept, based on which the game prototype can be further developed.

Contents

1. Introduction

> "I urge you to consider, how you can help by practicing good network hygiene with strong passwords and security protection, and by ensuring that our Internet-savvy children and grandchildren are as familiar with the principles of cyber security as they are with the latest games and apps."
>
> General Keith B.Alexander, Commander, U.S. Cyber Command

1.1. Background and problem statement

The idea for this thesis started from participating in a business model competition held at the Tallinn University of Technology's Innovation and Entrepreneurship Center Mektory in December 2013. The business idea was to develop an educational computer game for cyber security. This idea won the competition and was thereafter presented to persons of different specialties at an award trip to Silicon Valley. The idea of using serious computer games to teach people about cyber security was deemed interesting, and the author believes it is an avenue to be taken forward.

Security can be a difficult thing to teach. Human beings do not like getting into embarrassing situations, and this brings the temptation to leave security incidents unreported in the hopes they will just go away (Kikkas 2014). A lot of useful information has been published about cyber security, but people seem to have to experience a problem in order to understand it. Cyber security training and education can benefit from interesting teaching methods which have the potential to influence behavior of a wide audience, including average end-users.

The internet started off by linking a small number of computers in previously stand-alone closed systems. It then developed to connect a small number of computers, to connecting billions of devices today. Today not only computers, but also phones, other smart devices and even some cars are connected to the internet. The internet has evolved from something just useful to being an essential infrastructure for the functioning of the society (OECD 2012).

Internet is reshaping the way people live, bringing a larger variety of digital goods and services, lower prices, improved information gathering, more distribution channels and so on (ibid). The developments in technology have implications in that we are all more and more dependent on these technologies in our everyday lives, social interactions, economical activities and our interactions with the government (ibid). The well-being of the society as a whole and each individual person depends on ICT. In addition to increased opportunities, this brings also a number of threats that can limit our rights and freedoms. Cyberspace is also a world for cyber criminals. They are often times more skilled, more motivated and have better equipment than their victims. Intrusions are becoming more and more common – increasing bandwidth, social networking and ever bigger number of mobile devices connected to internet are part of the reason for the growing cyber attack problem (Nagarajan, Larssen 2012).

Cyber threat is real and every person is an important actor in ensuring security – being responsible and in control of his own information and devices. Everyone should be aware of the relevant security risks and preventive measures, they should know how to recognize incidents and what to do once an incident has happened. They should know how to manage their personal cyber security in their everyday personal and professional lives. Education is a key element in combating cyber threats and in increasing awareness: it's hard to fight against cyber threats when you are not aware of them, and it's hard to be aware of security problems when you don't know what these could be. That's why well thought-through security awareness training is so important. Games and simulations have become increasingly accepted as having enormous potential as powerful teaching tools that may result in an "instructional revolution" (Cone, Irvine, Thompson, Nguyen 2007). Games can provide an engaging environment that is interesting and stimulating for more people (Nagarajan, Larssen 2012).

Studies show that people are concerned about their personal cyber security: around half of the internet users in the EU are concerned about experiencing identity theft or being victim to online fraud; just under half are concerned about having their social media or e-mail accounts hacked, accidentally discovering child pornography online, scam e-mails or online fraud. In addition 37% are concerned about not being able to access online services because of cyber attacks. (EU Commission 2013)

The availability, reliability and security of networks and information systems are increasingly central to our economies and societies (EU Commission, 2006). People underestimate threats coming from cyberspace for various reasons, but the EU

Commission concludes the reasons to be “in the case of enterprises, the poor visibility of the return on investment in security and, in the case of citizens, the fact that they are not aware of their responsibility in the global security chain“ (ibid). This thesis has its focus on end-users: they need to understand that their home systems are critical to the overall security – and they shouldn’t be the “weakest link“ in this security chain. Therefore education about cyber security should start already at schools, and an effective teaching method could be through the use of games. Gamification and serious games are used in both education and business sector to train people in different areas and this thesis looks at how using serious games in schools can contribute to raising cyber security awareness.

To understand the issue thoroughly, this thesis looks at the theories of gamification and serious games. It then goes on to study the use of serious games in education in Estonia, followed by the use of computer games on cyber security from around the world. The thesis also studies polls conducted with regard to cyber security and awareness. To gain additional insight, the author conducted a survey among teachers in Estonia and conducted interviews with teachers, governmental authorities and university teaching staff. Teaching of cyber security topics in schools was also looked at during the research for this thesis.

It is the hope of the author that the results of this thesis could be used as a teaching aid for increasing cyber security awareness for students.

1.2. Aim of the thesis

The gamification approach has the potential to provoke interest in everyone: we all use computers, hardware, and software programs, which have vulnerabilities and problems. Computer games can provide a means to train people in an entertaining way, providing also different levels for different backgrounds. In parallel with this thesis and based on its findings, a computer game for cyber security will be built. This work will exploit a growing acceptance of computer games in education (Nagarajan, Janssen 2012).

The aim of this thesis is to analyze the potential of using serious games in cyber security and to come up with a game concept for an educational cyber security computer game usable in Estonia. It will focus on teaching of cyber security topics within the national defense elective course. In order to achieve this, the author needs to answer the following research questions:

1. What are games, gamification and serious games?

2. How are serious games used in Estonian schools?

3. How is cyber security taught in Estonian schools?

4. Could a serious educational computer game on cyber security be introduced in Estonia?

5. What should be included in the game concept in computer game for cyber security?

The first research question is answered through literature review, where well-known experts on gamification suggest definitions for the terms and give theoretical background to the issue. The second research question is answered by interviews with educators who are using serious games in their teaching. The third research question is answered by a survey conducted for the purposes of this thesis among teachers in Estonia, followed by semi-structured interviews with teachers and other educators. School curriculum and other documents regulating the area are also analyzed. The fourth research question examines the potential of using a serious educational computer game on cyber security in support of cyber security teaching in schools. The fifth research question looks at what should be included in a game concept and proposes a concept for an educational computer game on cyber security.

The current thesis is divided to five chapters. Chapter 1 introduces the topic and the methodology used.

Chapter 2 discusses the current situation and analyses the problem in more detail. The chapter defines cyber security, gives an overview of current practices of teaching cyber security and assesses its positives and negatives. It also gives a proposal for solution: a computer game, and narrows the aim for this thesis.

Chapter 3 looks at games, gamification and serious games and defines these terms. It also gives an overview of game characteristics: genre, machines, mechanics and concept. Further on we will look at the use of serious games in Estonian educational establishments. We then look at the use of educational cyber security games around the world. The chapter concludes with an assessment to the use of computer games in education, specifically for cyber security, in Estonia.

Chapter 4 concentrates on the solution as derived from the previous chapter: a computer game, and provides a game concept. The game concept will provide objectives of the game and give a proposal as to how to integrate the game to cyber security teaching within

national defense elective subject. The chapter will conclude with outlining potential additional uses of the game.

Chapter 5 concludes the thesis, providing topics for future research.

1.3. Methodology

Since this thesis discusses the potential of educating people and increasing cyber security awareness through the use of an educational computer game, there is a need to define "games", "gamification", "serious games" and "educational games". In order to do that, the author conducted a literature review of well-respected academic literature on the subject and looked at how serious games are both taught and used, in Estonia. The cyber security computer games used around the world were also analyzed.

To gain understanding of people's perception of cyber security, surveys conducted by the EU Commission, EU Kids Online, and the The Organisation for Economic Co-operation and Development (OECD) were studied. To get insight into how cyber security is addressed at high schools, Estonian high school curriculum was looked at in more detail. As cyber security is additionally taught within the framework of national defense teaching, we also looked at this specific curriculum. Further, to see how serious games in general are used in schools in Estonia, we conducted interviews with teachers and educators.

Literature review

In order to find relevant literature, the author approached a Tallinn University professor, different experts on gamification, used search on the internet and research on databases. The academic literature (with their extensive reference lists) as suggested by experts also provided a good source of information.

Survey of teachers

The software tool which was used for creating the survey and collecting data was Google Docs. Google Docs is a web based application that allows the creation of various document types. Among the documents that can be created, there are questionnaires. This allowed for

time savings as compared to distributing the survey in printed form, and was thus the preferred method for data collection. A disadvantage of Google Docs is that it is not possible to prevent people from submitting multiple replies; something which could result in duplicate entries.

For informing the survey participants of the followed ethical practices, a statement of informed consent was added in the beginning of the survey. This statement included:

- The purpose of the research
- The name and contact details of the author
- The identification of the university
- An assurance of confidentiality
- An assurance of privacy

Conforming to the basic principles of ethical research, the only collected data is the participants' answers and the timestamp of submission. The timestamp value was only used to remove accidentally submitted duplicate records. The survey took place between 15 February 2014 and 15 May 2014, after which it was not available for filling online. The full details of the questionnaire can be found in Annex 1.

The survey was distributed through an Informatics and IT teachers' mailing list and had a total of 20 respondents, which accounts for 10% of all high schools in Estonia. Due to time constraints and availability of information the author did not manage to look in detail into how different schools teach cyber security issues. One school's Informatics program and one national defense teacher's cyber security teaching program were looked into in more detail.

Interviews

Semi-structured interviews were selected as the means of data collection because of one main consideration. In the case of structured interviews the wording and order of questions is exactly the same for each respondent so that we can be sure that any differences in the answers are due to differences among the respondents rather than in the questions asked. In

contrast, the semi-structured interview method follows a framework but is open, allowing new ideas to be brought up during the interview as a result of what the interviewee has responded (CERIS 2007). An interview guide was prepared (Annex 2), which provided an informal grouping of topics to be covered during the interview. The semi-structured interview method allowed for the tailoring of questions to each specific interview situation and to each person individually.

The interviews with teachers and the survey conducted resulted in a more thorough data and interesting nuances, that were at times unexpected even to the author, and made it possible to plan for next interviews from sometimes different angles, and also to plan for further steps in the thesis.

The author prioritized the survey of teachers to any other, since the main outcome of this thesis could be usable as a serious computer game to teach cyber security awareness at schools. Also, the teachers have a unique view on both the real skills, requirements, wishes and worries of students. The survey of teachers also provided important information for conducting interviews with the other parties (academia, government institutions) as teachers, being in everyday contact with students, are the connecting point between the students and the society.

Focus Groups

The focus groups of interviews for this thesis consisted of 23 high school teachers, 4 university teaching staff members, and 7 government officials. The interviews of different parties were not combined, as the aim was to reach a bigger focus group and thereby see wider tendencies. The aim was to reach a common conclusion, and not to research single activities at the micro levels. Different focus groups each had a specific expertise and points of view to the topic of the research – cyber security – which with the method chosen allowed for analysis of the experiences and requirements of a wider audience.

Qualitative analysis

The different target group interviews were conducted in the form of semi-structured questionnaire and interviews. Those with teachers – including the results thereof – formed the basis for all others (university teaching staff, government institutions).

The research questions and research instruments that form the basis of this thesis were intertwined: the first – survey of teachers – and the results thereof, led to next steps (as depicted in Table 1). This came from the requirements to look deeper into the views and understandings of teachers concerning the terminology and the potential of teaching cyber security in high schools; but also the views from other related parties (academia, cyber security professionals, government institutions).

Table 1: overview of semi-structured interview methodology and findings

Method	Target group	Timeline	Main findings
Semi-structured survey (informatics teachers, national defense teachers)	20 teachers	15 Feb – 15 May 2014	Terminology Lack of unified teaching material Different approaches (depends on teachers)
Semi-structured interviews	3 teachers	15 Mar, 26 Mar, 23 Apr 2014	Detailed overview of teaching in Tallinna Reaalkool and by two national defense educators.
Semi-structured interviews (academia)	2 Tallinn University professors 2 Baltic Defense College professors	March-April 2014	Guidelines for approach on serious games. How serious games are used in Estonian educational system Terminology and problematic thereof.
Semi-structured interviews	National defense teachers	15 Mar-15 Apr 2014	No "set" teaching program, this is a pilot project conducted in 10 volunteer schools; educational content decided by Estonian Defense Forces, in coordination with other governmental authorities.
Semi-structured interviews with government institutions (Ministry of Education, Ministry of Defense, Ministry of Economy, State Chancellery, Estonian Information Systems Authority)		April-May 2014	New national cyber security strategy and its ambition for teaching cyber awareness. New upcoming national defense curriculum for cyber defense. Need for teaching cyber security.

1.4. Acknowledgements

The author would like to thank Dr. Rain Ottis for reviewing and ideas, Martin Sillaots for providing insight to researching gamification and serious games, Tallinna Reaalkool for assisting in understanding the teaching as currently done within the national school curriculum and for providing access to their e-learning environment, and Andres Kuusk for providing valuable insight to teaching of cyber security within the national defense elective. This thesis might not have started without a business model competition held at the Tallinn University of Technology Innovation and Entrepreneurship Center Mektory, who awarded the game project with an award trip to Silicon Valley, something that proved valuable for this thesis as well. Thank you also to Erik, Triin and Erkko for being a great team in working on the game prototype. Special thanks go to Andres Hairk, who allowed to take time off from work duties in order to attend lectures and finalize this thesis. And last, but not least, special thanks to my family for standing by me for the duration of this undertaking.

2. Analysis of the current situation

This chapter defines cyber security, gives an overview of current practices of teaching cyber security and assesses its positives and negatives. It also proposes a solution – a computer game – and narrows the aim for this thesis.

2.1. Cyber security

Any discussion on cyber security should start with clearly explaining the scope: is the discussion about devices connected to the internet, the internet infrastructure, applications, communications, data, identity, or services? Or is it about the "problem" between the keyboard and the chair? Cyber security as a term means different things all referred to by one name, from one end of the spectrum (e-safety) to the other (cyber war). Conducting an analysis of national cyber security strategies, the OECD noted: "… where cyber security policies exhibit a troubling lack of specificity is … in the definition of them. "Cyber security" has come to mean a huge spectrum of things." (OECD 2012)

It is difficult to understand the term (prefix) "cyber" [1]. There is no universal definition to the term "cyber security", and there are different views as to what is "national" and what is "private" cyber security. Cyber security refers to tangible concepts (computers, networks and information assurance), but the term "cyber" also refers to anything based on IP traffic, with users being part of that. Terminological and conceptual confusion is aggravated by the lack of taxonomy on the subject, and today it is common that the level of awareness of cyber as an environment or as a tool is very low, making it difficult to introduce more sophisticated and complex issues, but also in the design of education and training strategies. (Kerttunen, Tikk-Ringas 2014).

The survey among Informatics teachers in Estonia conducted for this thesis showed a mixed understanding of the terms used: some respondents referred to e-safety (and in general safe computer literacy habits), some referred to IT security, while others made a note that "cyber security" only means areas in warfare and national security. Arguably both sides are correct in their statements. However, it is clear that cyber security is not only an e-safety or IT security, and not only a national security issue. It encompasses both.

[1] The use of the prefiks "cyber" derives originally from the US diplomatic culture and has been adopted world-wide (Kerttunen, Tikk-Ringas 2014)

2.1.1. Cyber Security definition

This thesis addresses the "personal cyber security" issues and the following definitions are used:

Personal for the purposes of this thesis means the single end-user using their computer for personal purposes.

Cyber security for the purposes of this thesis means the combination of human and technical factors contributing to the well-being of a person and his or her computer in cyberspace.

Awareness for the purposes of this thesis means for the end-user being knowledgeable of the risks they are likely to face in cyberspace and ways to potentially mitigate those risks.

2.1.2. Constraints

There are four main constraints to the effective application and use of serious gaming framework for teaching cyber security:

1. people's general non-interest in cyber security issues (Nikolakopoulos 2009);
2. misunderstanding of cyber security and the value any single person can be to cyber criminals (EU Commission 2006);
3. use of traditional teaching methods and reluctance of using games for teaching (Adams 2010);
4. provision of a good content for uninteresting subjects like passwords, network settings, configuration, or access control through an exciting storyline (Nagarajan, Janssen 2012).

In general, the constraints are that people want to use their ICT and expect it to work, but they do not want to worry about or deal with security issues (Nikolakopoulos 2009). Cyber security is a topic, that seems to be over-mystified and something the average home-user can not understand. In addition, people – and even enterprises – do not think they have anything valuable in their computers, or that they could be valuable targets to cyber criminals (EU Commission 2006). People do not see their role in an overall security chain (ibid). Furthermore, school systems are set up in a way that values traditional teaching methods, and even though some innovative solutions are used, there is still reluctance to using games for teaching (Adams 2010). Games are seen as play, as entertainment, and not as serious instruments that could be used for teaching. Finally, cyber security professionals have difficulties in finding an engaging way of presenting uninteresting subjects in an interesting way (Nagarajan, Janssen 2012). When those who teach have difficulties in

explaining the subject in an engaging way, it limits the introduction of innovative teaching aids.

2.1.3. Cyber security awareness

OECD Guidelines for the Security of Information Systems and Networks (OECD 2002) discusses awareness:

> "Awareness of risks and available preventive measures are the first line of defense for cyber security. Information systems and networks can be affected by both internal and external risks. People should understand that security failures may cause problems to systems and networks they use. They should also be aware of the potential harm their actions can cause to others due to the interconnectivities and dependencies. People should be aware of the configuration, available updates, their system, its place in the networks, good practices they can implement to enhance security and needs of other people." (ibid)

Cyber security is not a separate, stand-alone entity, not just one single issue. It's a combination of technical and human factors that form a system, where no part of that system can be disregarded. While technology is important, people are part of the system: they are the ones who access and transfer information, and should ensure their part of the security of system. Awareness of the risks and available safeguards is the first line for defense of security of information systems and networks (ENISA 2006).

Cyber security training is getting more important. Over the past years we have seen a growing trend in the number of cyber attacks (Kaspersky 2013). Media reports on incidents compromising the confidentiality, integrity and availability of information systems and networks are also increasing (OECD 2012). The security will depend on whether home users, businesses and governments feel safe using the internet and trust it enough to operate there.

The OECD conducted an analysis of cyber security strategies of 10 volunteer member states[2] (OECD 2012). Among other things, the analysis discussed raising awareness and educating people. Compared with previous versions of cyber security strategies, awareness raising and education remained very important for the countries analyzed.

[2] The 10 volunteer member states analysed were: Australia, Canada, Finland, France, Germany, Japan, Netherlands, Spain, the United Kingdom and the United States. (OECD 2012)

> "Awareness raising initiatives generally focus on the general population, including specific targets such as children, and on businesses and government bodies, including specific targets such as decision makers, and critical infrastructures. Education efforts towards the general population include, for example, cyber hygiene education in schools at all levels, using social media, through partnerships with ISPs, via the possible establishment of an "information security support service"." (OECD 2012).

The analysis also concluded that one country had created a cyber security education and training center and another had introduced a concept of "responsible digital citizenship", based on digital literacy and awareness to exploit online opportunities and mitigate cyber threats (ibid).

2.2. Current practices of cyber security teaching in Estonian schools

The current national school programs for all levels of school do not cover cyber security as a separate subject, but some elements of it have been included. The national curriculum states the main competencies the students should be able to possess upon finishing the school (PRÕK 2011, GRÕK 2011).

Põhikooli riiklik õppekava (PRÕK, covering grades 1-9) states that after the first level of school (grades 1-3) the students should be able to use simple computer programs and technological devices used at school and at home. The second level of school (grades 4-6) students should be able to use computers and internet as a communications device. The third level of school (grades 7-9) students should be able to manage in the world of technology, use ICT purposefully, and without risks. For the purposes of this thesis, there is one cross-cutting theme of relevance in the curriculum: Technology & Innovation. The aim of the Technology & Innovation theme is to grow the student to be a person who can use current technologies responsibly and purposefully. PRÕK Annex 7 discusses the subject of Technology and states that by the end of lower secondary school, the student should be able to understand and use contemporary technology, but also analyze threats and opportunities arising with the use of technology. The PRÕK also states that theory should be amended with practical activities wherever possible. (PRÕK 2011)

PRÕK also states that Informatics is an elective course that can be taught and gives guidance as to what should be taught within this course. The teaching of informatics is concentric – what has been learned at lower levels of school, will be reintroduced more

thoroughly in higher levels. The main aim is on practical computer usage while learning different subjects. In the first level of school, the ICT related topics are integrated to other subjects and special Informatics course is not considered necessary. By the end of second level of school it is recommended to teach use of computer skills and students should be able to protect their virtual identities, set strong passwords and change them frequently, not publish sensitive information online, and be able to securely attach external devices to their computers. Within the third level of school it is recommended to teach the course on information society's technologies. By the end of third level of school the students should be able to use virtual environments safely, differentiate between different levels of security of websites (i.e. http vs https) and have basic knowledge about security certificates, as well as use their virtual identities securely and ethically. The objective for teaching Informatics, among others, is that the student recognize and avoid threats coming with the use of ICT to their security and personal information. The PRÕK suggests that Informatics should concentrate on everyday use of ICT, but also suggests that schools with emphasis on hard sciences offer an additional course "Introduction to Computer Science" to their students. The PRÕK states the main principles for teaching informatics to be relevance to real life, active learning and creativity, use of innovative technologies and solutions in teaching the subject, but also security. (PRÕK 2011)

The *Gümnaasiumi riiklik õppekava* (GRÕK, covering grades 10-12) states that students should be able to use contemporary technology with responsibility and have an informed opinion as to the developments of technology and questions related to its use. One elective subject stated in the curriculum is the "Use of Computers for Research", with a specific program for that subject specified. The curriculum also states compulsory cross-cutting themes that each school should take into account. The aim for these cross-cutting themes is that they are not any one subject-specific but rather support all subjects, they enable the student to understand the developments in the society, and enable them to apply their knowledge in various circumstances. For the purposes of this thesis, there is one cross-cutting theme of relevance: Technology & Innovation. The aim of the Technology & Innovation theme is to grow the student to be a person who can use current technologies responsibly. In gymnasium (high school) level the teaching is primarily conducted through team-based research tasks. By the time of graduating, the gymnasium students should be prepared to use the ICT in their everyday lives, studies and for work. (GRÕK 2011)

2.2.1. Survey of teachers

Based on the survey conducted for this thesis, cyber security is taught within different formats in schools in Estonia (Figure 1). Mostly, it is discussed within the Informatics/ Computer Science and National Defense classes. But not only, the cyber security problematic is also covered in class teacher sessions, and – interestingly – within the teaching of mathematics. 95% of the teachers surveyed were teaching cyber security topics (Figure 3), and majority of teachers consider it either important or very important that cyber security be taught in schools (Figure 2). Mostly the focus is on e-safety[3] and cyber hygiene[4] (regular school program: informatics and class teacher sessions). For this, a number of games are used – some developed by and for specific schools, some nationally. The games developed and used concentrate on e-safety and cyber hygiene. To some extent within the teaching of national defense, the questions of critical information infrastructure, cyber terrorism and cyber warfare are discussed. The national defense teaching is coordinated by the Ministry of Defense and the teaching is conducted by specialized teachers or active duty military personnel; all other subjects are coordinated by the Ministry of Education and Science and taught by subject teachers.

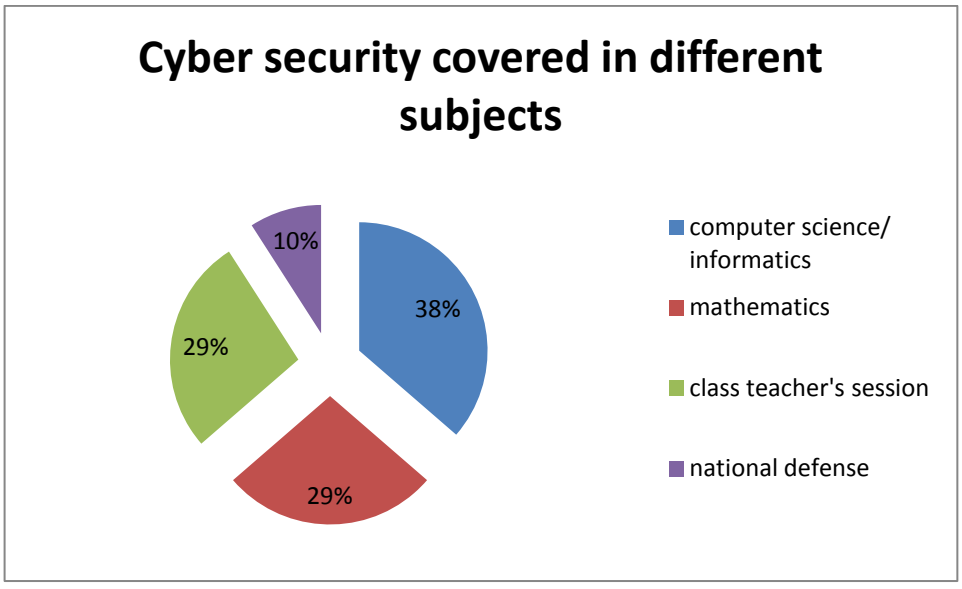


Figure 1: Teaching of cyber security issues in different subjects (Source: survey for this thesis).

[3] E-safety is about utilizing information and communication technologies in a safe and responsible way.
[4] Cyber hygiene refers to steps that computer users can take to improve their cybersecurity and better protect themselves online.

While covering cyber security issues in informatics, computer science and class teacher's sessions is logical, the two other (mathematics and national defense) require some explanation.

Cyber security is not discussed thoroughly in mathematics, but it comes in as a related issue when students start learning geometry. For teaching geometry teachers use GeoGebra[5] software tool, or for calculation they use Pranglimine program[6]. An example brought forward by one respondent to the questionnaire was explaining to students the difference of just closing a window vs. logging out and closing a window.

Teaching of national defense is the responsibility of Ministry of Defense. Within the national defense program, there has for the last two years been an experimentation to teach cyber security in 10 voluntary schools all over Estonia. National defense is an elective course at gymnasium level. Since 2013, the Estonian Defense Forces have proposed to teach cyber security under the framework of national defense, and the decision to do so has been taken at school level. This teaching covers a wide spectrum of areas: from terminology, data protection, value of information, social networks, cyber warfare, attacker motives and means, to critical infrastructure.

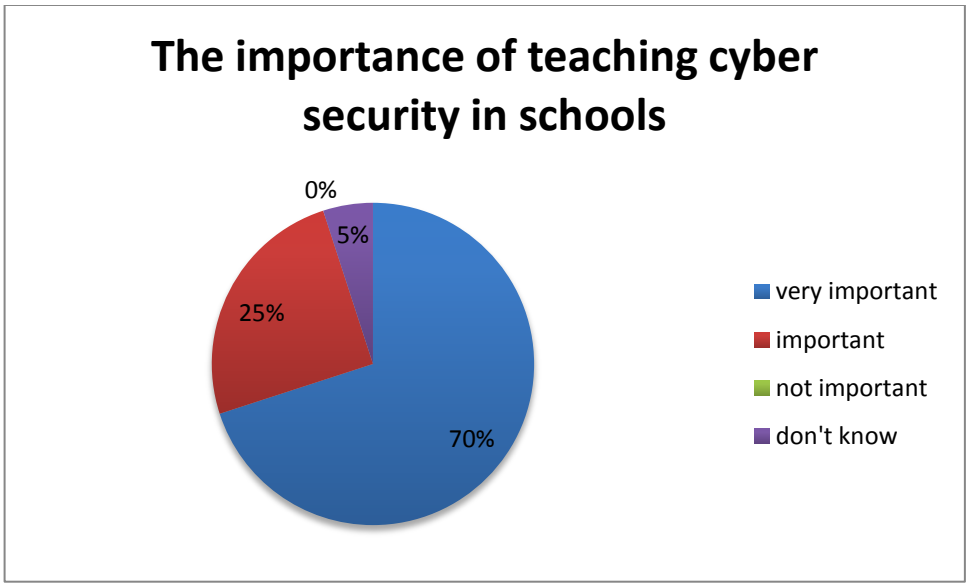


Figure 2: The importance of teaching cyber security in schools (Source: survey for this thesis)

[5] GeoGebra is a free and multi-platform dynamic mathematics software for all levels of education that joins geometry, algebra, tables, graphing, statistics and calculus in one package. In Estonia it is used from 7th grade onwards, as a recommended educational software.
[6] Pranglimine is mental calculation competition used in Estonia

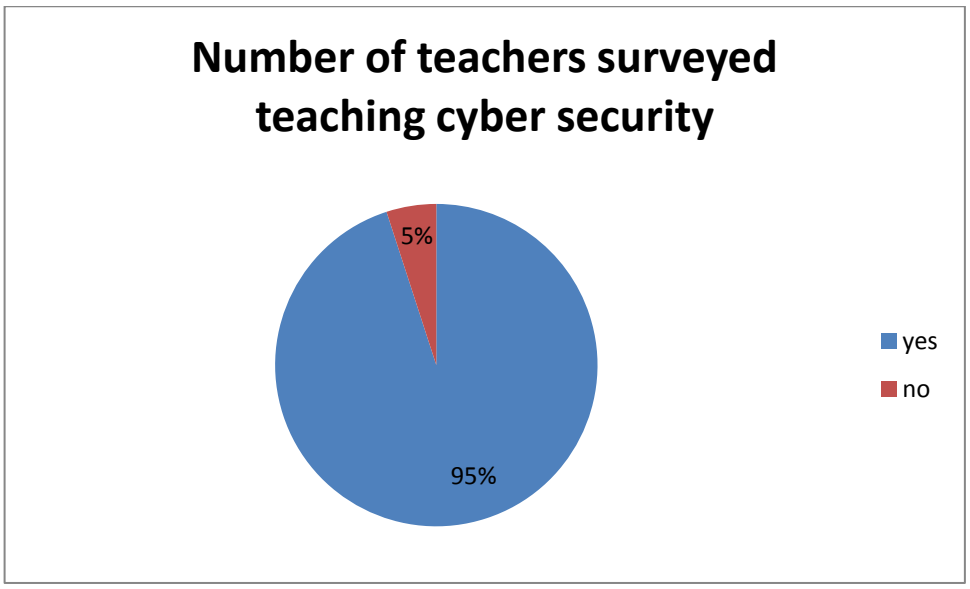


Figure 3: Number of teachers surveyed teaching cyber security (Source: survey for this thesis)

The perception of teachers

The survey conducted also asked teachers, what they thought about using a computer game in teaching cyber security issues. The majority of respondents were positive to the idea, and some use existing games to teach e-safety issues. They thought that cyber security is a right issue to be taught through a game, that children learn better through games, that a well-designed game can be a useful additional tool for teaching, and that using games may make it more understandable for students. They also thought it is an interesting idea and using games can make a subject more attractive. One respondent did not see a difference on how something is taught, considering that computer game is just one method. All respondents were ready to use a computer game in their teaching, or were already using some games in teaching.

Some respondents considered that games would be useful for I and II level school (i.e. grades 1-3 and 4-6), while older students should learn more about theory and read different materials. This probably proves that games are considered something playful, and not as serious games. As we will show in Chapter 3, serious educational games are a category on their own and are not considered entertainment.

The teachers surveyed noted that the security awareness of students is indeed quite low – the subject has to be dealt with and it has to be done fast. Cyber security can be effectively integrated to other subjects: societal studies (*ühiskonnaõpetus*) and family studies

(*perekonnaõpetus*). Based on the survey conducted for this thesis, in addition to teaching cyber security within the Informatics subject, it is currently integrated also to the teaching of mathematics and national defense. Integrating it to any other subjects could prove useful due to the interdisciplinary nature of the subject. Two respondents also considered it important to add a cyber security chapter to national defense textbook. The same respondents considered it necessary to task the Defense League's Cyber Defense Unit with drafting a study program for schools, as well as teaching the subject in schools.

When asked in which grades cyber security should be covered in schools, 37% of teachers surveyed thought that it should be covered in lower and upper secondary school, and 26% considered it should be also taught in elementary school. One comment in the survey stated that cyber security in some form should be taught in every school level, as children start using computers or other computerized devices at an early age.

The teachers also considered it necessary to have some kind of teaching material prepared by some authority centrally, so that teachers can then use it in their respective lessons. The schools themselves have difficulties in preparing materials.

One respondent drew the attention to the need for defining what is cyber security and what is cyber defense, another respondent also commented on the need to have clear understanding about what is meant by different terms.

2.2.2. Tallinna Reaalkool's teaching of subjects related to cyber security

Tallinna Reaalkool is teaching Informatics at the lower and upper secondary schools, i.e. grades 7-9 and 10-12, but the first lessons on e-safety are introduced from the 5th grade. In the 5th grade the students are given an introduction to the safe use of Facebook. The teaching for lower secondary school (grades 7-9) and upper secondary school (grades 10-12) is conducted using the Moodle[7] environment, and students can only use their official school e-mail address (name.surname@real.edu.ee) for communication with the school (Niggulis 2014).

For the 7th grade the topics taught are virtual identity, copyright issues, safe and ethical use of internet, and information search from internet. For teaching these, the subjects of e-safety and netiquette, cyber-bullying, piracy and viruses are included in the teaching. In the

[7] Moodle (*Modular Object-Oriented Dynamic Learning Environment*) is a free open source e-learning environment, known for managing learning environments.

9th grade M-learning programs are covered in addition to e-safety. Within the teaching of M-learning, the students get acquainted with educative M-learning programs, but also learn about using their smartphones safely and protecting these from malware. Creation of QR codes is also covered. For e-safety the students get a teamwork task of creating an e-poster about rules and recommendations to survive in social networks and will present it in the class to others. In the 7th and 9th grades Informatics is taught during one semester. (ibid)

In the 10th grade Informatics is a compulsory elective course in Tallinna Reaalkool, with duration of 35 hrs. The subject is "Use of Computer for Research" and focus is on online research and referencing of information, as well as using critical thinking for found information sources. In addition to referencing, copyright issues are also covered. The 10th grade students also have to present a research paper. In the 11th grade the subjects of intellectual property, copyright and plagiarism are covered. Overall, Informatics is integrated to different subjects in Tallinna Reaalkool. (ibid)

Up to lower secondary school level, the main worries of students are related to (secure) use of smart devices and social networks. Students are in general interested in their personal security online. (ibid)

2.2.3. Cyber security teaching within national defense elective

The aim of national defense teaching is not only military-specific teaching, but "good citizen" development in general (MOD official interview 2014). National defense is an elective course for upper secondary school level students (GRÕK 2011), with the duration of 70 hrs. The goal of the Ministry of Defense is to introduce national defense as an elective course to all gymnasium-level schools in Estonia by 2018 (MOD official interview 2014).

The primary aims for the subject are stated in GRÕK 2011, and most of these are relevant to cyber security as well. Upon graduating, the person:

- is a loyal citizen with positive attitude and acts with rule of law principles in mind (does not engage in cyber crime activities);
- understands how national defense is related to the rest of the society (military cyber defense and civilian society's activities for cyber security);

- understands how defense is built up, responsibilities of different actors, and relevant legal documents (national cyber security strategy and the role of different parties);
- understands the principles of NATO's collective defense (collective defense at times of cyber or other crises). (GRÕK 2011, Kuusk 2014)

The subject description for national defense elective covers traditional military areas from military history to field training exercises. Cyber security as such is only mentioned as part of "Contemporary Crises, Wars and Armed Conflicts" topic (GRÕK 2011). Since 2013 the Estonian Defense Forces have proposed to include cyber security within the national defense curriculum (Kuusk 2014). Whether this is done, is decided by schools. As of April 2014, this opportunity has been used by ten schools.

Teaching of cyber security within national defense studies covers terminology from data protection to cyber warfare; the value of information or what do we defend; cyber warfare and cyber in warfare; cyber weapons; different attacker motives and targets; the world of malware; botnets; critical infrastructure threats; social engineering; defacement; phishing; attack scenarios using social media or other everyday life events. The teaching goes on to explain who is defending the nation on the civilian and on the military side together with their respective responsibilities. It then covers the threats that the students can face – that the criminals are interested in their data, money, devices and identity; and how problems can be let in – malware, external devices, phishing, etc. It is also explained what the criminals can achieve if they are successful, how to recognize an infected device and what being attacked or infected can mean to the students themselves (Kuusk 2014).

Five main areas are covered: computer, web, wifi, smart devices, and social networks. It is explained how to defend one's computer (regular updates, firewalls, judicious use of administrator rights, anti-virus programs, regular backups, encryption). It is also explained how to select safe passwords or passphrases and secure one's accounts and how to use internet safely. Setting up and securing wifi connections is also covered (setting up encrypted connections, allowing usage from specific devices only, using VPN). Since students use a lot of smart devices, the security of these is covered as well – securing updates, installing virus protection, installing apps from trustworthy sources only, locking one's device and performing backups (Kuusk 2014).

2.3. Assessment of current practices

E-safety issues, but also cyber security, are taught in Estonian schools today within elective courses of Informatics and National Defense. However, different aspects of cyber security are integrated also to other subjects: mathematics, societal studies, class teacher sessions. Mostly the focus is on e-safety and cyber hygiene, where computer games are also used. To some extent, within the teaching of national defense, the questions of critical information infrastructure and cyber terrorism/ cyber warfare are discussed. The national defense teaching is coordinated by the Ministry of Defense; other subjects by the Ministry of Education and Science.

The current national school curriculumc for all levels of schools do not cover cyber security as a separate subject, but give the main competencies the students should be able to possess upon finishing the school, among those also cyber security related competencies (PRÕK 2011, GRÕK 2011). The first, second, and third level of school students (grades 1-9) should be able to – with successive deepening of teaching – use computer programs for study and leisure and manage in the world of technology without risks. By the end of 9th grade, the student should be able to also understand and analyze threats and opportunities arising with the use of technology. The PRÕK 2011 also states that theory should be amended with practical activities wherever possible. The main aim is on practical computer usage while learning different subjects. The objective for teaching Informatics, among others, is that the student recognize and avoid threats coming with the use of ICT to their security and personal information. (PRÕK 2011)

The Gymnasium level students should be able to use contemporary technology with responsibility and have an informed opinion as to the developments of technology and questions related to its use. One elective subject stated in the plan is the "Use of Computers for Research", with a specific plan for that subject specified (GRÕK 2011). The plan also states compulsory cross-cutting themes, with one of them being Technology & Innovation. By the time of graduating, the gymnasium students should be prepared to use the ICT in their everyday lives, studies and for work. (ibid).

Within the elective course of Informatics the teachers mainly teach what is stated in the national school programs, and related to e-safety. The elective course of national defense also covers more specific areas, such as updates, firewalls, backups, encryption, VPN, and smart device security. Five main areas are covered: computer, web, wifi, smart devices, and social networks.

The survey conducted among teachers for this thesis showed that teachers do teach and want to teach cyber security issues. However, there is a lack of teaching material, lack of qualified teachers on the subject and confusion to the terminology itself. The survey also showed that despite of all difficulties, teachers are open to new material and information, and are willing to try different approaches in their teachings. This has been an auditable process which provides a good basis for designing a game concept for a cyber security computer game.

With the introduction of the new National Cyber Security Strategy later in 2014, there will be renewed emphasis on cyber security awareness development in schools. For the moment, no exact plans have been formulated yet. Once the strategy will be approved, teaching curriculum will be looked at in more detail (Ministry of Economy and Communications official 2014).

2.4. Proposed addition – computer game

Research has shown that students learning theory and facts with traditional methods may be able to pass tests, but may not be able to apply what they have learned to solve real-life problems (Mead 2013). In contrast, computer games give "situated meanings", where things are learned within concrete contexts (ibid). It is therefore concluded that games allow people to get knowledge that they retain for longer and will be able to apply in practice – they will not only learn facts, but also different ways of thinking and understanding the topics (ibid).

The PRÕK 2011 suggests that Informatics should concentrate on everyday use of ICT, but also suggests that schools with emphasis on hard sciences offer an additional course "Introduction to Computer Science" to their students. The PRÕK 2011 states the main principles for teaching Informatics to be relevance to real life, active learning and creativity, and innovative technologies or solutions. (PRÕK 2011).

While the teaching of national defense covers a number of areas of relevance in cyber security not covered elsewhere, it is currently only theoretical, with some audio-visual additions and lacks a practical aspect to it.

For people who have grown up using internet and playing games for most of their lives, traditional learning methods are not interesting and their attention span is limited (Kapp

2012). It is therefore concluded that computer game could be a useful teaching aid for teaching cyber security and would make the subject more attractive.

2.5. Specifying the aim of the thesis

This thesis will focus on teaching of cyber security topics within the national defense elective course. The five main areas are covered (computer, web, wifi, smart devices, and social networks) will be taken as a guide to introduce a concept for an educational computer game as teaching aid.

The defense forces and teaching of national defense would certainly become more attractive with the introduction of innovative non-traditional means of teaching, i.e. using a computer game.

3. Games, Gamification and serious games

Chapter 3 looks at games, gamification and serious games and defines these terms. It also gives an overview of game characteristics: genre, machines, mechanics and concept. Further on it will look at the use of serious games in Estonian educational system. This will be followed by a look at the use of educational cyber security games around the world. The chapter concludes with an assessment to the use of games in education, specifically for cyber security, in Estonia.

Many organizations in public and private sector use gamification to train their staff. It is possible to find an example of gamification for learning, innovation, or problem solving in most areas of work. (Kapp 2012).

Cisco developed a game called „The Binary Game“, an arcade game that looks like Tetris – the idea is to teach people binary numbers, without previous knowledge. The game exposes players to forty or fifty binary problems. The players will recognize patterns and develop strategies, trying to beat the game – but in fact these patterns and strategies give them abilities to think in binary. IBM created an interactive first-person thinker game called INNOV8, teaching business process management, with players responsible for making decisions in a company. The game is designed to bridge the gap in understanding between IT teams and business leaders in organizations; and it is used in business and IT programs in hundreds of schools around the world. Skills learned in this game include business problem solving, prioritization and consensus building – a gamified approach to teaching decision making (ibid).

The military has always been an advocate for games, and has gamified military strategy, war preparedness and tactical training since ancient Greece. Military organizations worldwide have found that, when dealing with life and death, game-based training scenarios make an impact on the learners. (Mead 2013)

Until not so long ago, work as a pilot meant taking big risks even during training flights. Then came simulations and learning to fly became easier. And now the new generation of pilots is being trained to operate unmanned aerial vehicles (UAV-s) directly from their computers, like using computer games. Recruiting young people with considerable Xbox,

Playstation, or any computer game experience is useful for the future work of these new UAV pilots. (ibid).

Militaries have used gamification in a wide range of subjects: recruiting, individual combat training, unit training, flight simulators, ship simulators, weapons and weapon systems simulators, table-top exercises, and more recently also for non-traditional areas: cultural training for missions in distant areas, and even Post-Traumatic Stress Disorder treatment. An innovation in military gamification is the use of games to solve military problems: the U.S. military was trying to generate new ideas on how to battle Somali pirates through the use of a massive online multi-player game, in a way crowd-sourcing this military problem to civilians. The goal was to find innovative solutions by observing what (non-military) players do within the game environment. (ibid)

3.1. Defining games

For people who have grown up using internet and playing games for most of their lives, traditional learning methods of lectures, remembering by heart, and tests are not interesting, and their attention span is limited (Kapp 2012). Therefore learning should turn to being engaging and goal-oriented – a focus on gamification can increase engagement, relevance, and immersion, and can combine learning with real-life situations (ibid). And as noted below, this is what children like to do.

The young generation of today does not know and has never experienced a world without mobile phones, internet and computer games. According to EU Kids Online study, it is surprising that 85% of children use internet for studying, 83% play games, 76% watch videos and 62% chat online. In other words: children study, play games, watch videos and chat online. (EU Kids Online 2011).

The high placement of "games" in children's online activities reflects the role of games and their unused potential in teaching, interest in video shows the potential of emergence of a new audio-visual style for studying, and online chat refers to the importance of communication. People do not play games just for „points", but for engagement, immediate feedback, feeling of accomplishment, achieving success against a challenge and overcoming it (ibid).

Game-like reward systems are gaining popularity even in our everyday lives – there are different loyalty cards, scoring systems, rewards for achievements. Different organizations

have realized the usefulness of integrating game mechanics to anything from software design or keeping customer loyalty, to regular meetings. Gamification is also used in position-based mobile applications such as Foursquare, which uses game mechanics to let one's friends know where one is. The user logs in to a location, and this gives him points and rewards, and, most importantly, gives him special offers and rewards in real world. (Dignan 2011)

What are games?

Games are based on real world, they are a kind of abstracted reality. Games offer people what they long for: challenges, feedback, and victory. A game may be regarded as a dynamic model of reality in which the model provides a representation of reality at a particular period of time. In academic literature this is known as an *operating model,* as distinct from verbal, graphical, mathematical, or physical models (Kapp 2012).

Abstracted reality in games helps the players to understand what is going on in the game, minimizing complexity – Monopoly and Chess are such abstractions, where financial monopolies and military strategy are literally reduced to the space of a game board (ibid). This makes it possible for those playing the game to work with questions of strategy and finance without having to go to war or be in a monopolistic position. In games, cause and effect can be more clearly identified – in cities (or countries), for example, raising taxes may have long-term effects of people moving away; issues like quality of life, availability of employers, schools, kindergartens or a number of other factors may influence people's decision to stay (or not) within a certain location (ibid). Games can highlight these factors, their relationships, and simulate consequences. Abstracted reality in games also reduces time required to grasp concepts, which for complex systems can be overwhelming (ibid).

A game should be seen as an activity, rather than a system of rules (Adams 2010). Even if all (or most) games need rules, these alone do not make a game. What makes a game, is that it is played – otherwise it is just a theoretical thought exercise (ibid). Thinking of a game as an activity focuses the attention at players.

"A game is a type of play activity, conducted in the context of pretended reality, in which the participant(s) try to achieve at least one arbitrary, nontrivial goal by acting in accordance with rules." (ibid)

The essential elements of a game are play, pretending, a goal and rules (ibid). Unlike books, films and theatre – which are presentational forms of entertainment, play is a participatory form (ibid) - when one reads a book, it entertains, when one plays, one entertains oneself. All the while we read, no matter how many times, the book doesn't change. While playing, we make choices that have influence in the outcome of the game – different choices lead to different outcomes. In a game, one has the freedom to act and the freedom to choose how to act (ibid). This freedom has limits – bound by the rules of the game requiring to use wit, skills and imagination (ibid). Games can be played for serious purposes, such as learning or research (ibid).

According to Kapp, "Gamification encompasses the idea of adding game elements, game thinking, and game mechanics to learning content. The goal of gamification is to take content that is typically presented as a lecture or an e-learning course, add game-based elements (story, challenge, feedback, rewards, etc) and create a gamified learning opportunity either in the form of full-fledged educational game, in the form of game-elements on top of normal tasks like running for exercise, or in the form of an engaging classroom experience wherein learners participate in a story-based challenge to master the content presented." (Kapp 2012).

In other words, gamification is using game-based thinking and mechanics to deliver content other than pure entertainment; and creation of a serious game falls under the process of gamification and serious games are a form of gamification.

The idea of using games in education, health, and other sectors have already yielded positive results and research is advancing in modeling and simulation that could be applicable to cyber security and defense gaming (Nagarajan, Larssen 2012).

3.2. Game characteristics

In this part we look at the characteristics of a game: genre, machines, mechanics and concept.

3.2.1. Game genres

Games fall into eight main genres: action games, strategy games, role-playing games, sports games, vehicle simulation games, construction and management simulations,

adventure games, and artificial life and puzzle games (Adams 2010). Below is an overview of each.

When people hear about computer games or video games, they immediately think of **action games**. The reason is historical – almost all early games were action games: Asteroids, PacMan, Space Invaders. "An action game is one in which the majority of challenges presented are tests of the player's physical skills and coordination. Puzzle-solving, tactical conflict, and exploration challenges are often present as well". Action games require good hand-eye coordination and usually quick reaction. The player doesn't have time for strategy or planning, the skill required for challenges is not very high. **Strategy games** are probably among the oldest in the world – it is believed that the game Go was first used around 2200 B.C. Strategy games challenge the player to win the game through planning a number of actions to achieve a result, and most strategy games today are war games. "A strategy game is one in which the majority of challenges presented are strategic conflict challenges and the player may choose from a large variety of potential actions and moves at most points in the game. Victory is attained by superior planning and taking the optimum actions; the element of chance must not play a large role. Other challenges, such as tactical, logistical, economic, and exploration challenges may also be present. Physical coordination challenges play little or no part." **Role-playing games** let the player get involved in complex worlds, where their characters are avatars. Gameplay can be in different areas: exploration, inventory or communications, but both the game design and content design is very intense and a big undertaking. "Role-playing game is one in which the player controls one or more characters, typically designed by the player and guides them through a series of quests managed by the computer. Victory consists of completing these quests. Character growth in power and abilities is a key feature of the genre. Typical challenges include tactical combat, logistics, economic growth, exploration and puzzle solving." If most other games take place in an imaginary world the player doesn't know, **sports games** simulate the actual world the players know. Sports games simulate real or imaginary sports, playing it or managing it. **Vehicle simulations** intend to create a feeling of flying or driving a vehicle, whether on land, air or sea. **Construction and management simulations** give players a chance to build things (like cities), while operating under economic constraint. The game is all about processes, the majority of challenges are economic and concern growth, and construction activity is an essential element in these games. **Adventure games** are different from any other game genre, this

kind of game is not competition or simulation, there's no process to manage or no opponent to defeat. The game is an interactive story, story-telling and exploration are essential elements of the game. **Artificial life games** are simulations about people or animals; it can be about individuals or relationships, or it can be a simulation of an ecosystem. **Puzzle games** offer the player with hours of strategy and problem-solving. (ibid).

Application of game genres to cyber security

The best genre option for cyber security is deemed to be the strategy game, as cyber security is intrinsically about management of risk, planning of resources, strategically planning different actions to achieve an ultimate goal. In strategy games there is often times not just one correct answer, but it is the end result which counts: through the steps taken the player either achieves the objective or not.

3.2.2. Game machines

There are different types of machines used for games, and in order to define a concept for a computer game one should also discuss which machine (or machines) the game runs on – some genres of game are better suited for one kind of machine than any other and it is important to know the strengths and weaknesses of each, and how they are used (Adams 2010). The different types of game machines are described below:

Game consoles

Home game consoles are usually set up in living rooms, 1-2 meters from the television screen, several players can see the television screen at the same time and as one console accommodates up to a certain number of people, they are excellent for multiplayer games. Nintendo Wii has changed the home console landscape dramatically, making games intuitive and easy to learn, and they are used in even unexpected ways: therapy or exercise, for example. For development, however, you need licence from the console manufacturer. (Adams 2010)

Personal Computers

Personal Computers are intended for use by one person at a time, and PC games are very rarely designed for more than one person to play. However, as PC-s are connected to the internet, it is the machine of choice for multi-player networked games. PC games are divided to stand-alone games (installed on the PC) and browser-based games (running inside web browsers). (ibid)

Stand-alone games can use all resources available of a PC (assuming no other programs are running), and they are usually most visually appealing. Browser-based games are rapidly gaining popularity. Their advantage over stand-alone games is that they are isolated from the machine's hardware. This comes at a price, however – when stand-alone games can use the full advantage of 3D technology, then browser-based games are 2D games. Beginning with browser-based games is an excellent way to start in gaming, as you don't have to worry about machine's hardware. (ibid)

Other devices

Handheld game machines are very popular and inexpensive, they offer a set of built-in games. There are limits to the audio, video, graphics and animation that can be included. For development, as with home console machines, you need license from the manufacturer. (ibid)

Mobile phones and wireless devices have a big advantage over traditional handheld games – their wireless connection allows for networked play. (ibid)

Application of game machines to cyber security

Developing console games or separate handheld machine games for educational purposes is complicated: one needs to work with specific manufacturers and build a game for one specific machine. This will limit the distribution of the game, and therefore will also limit its educational usage. It is therefore concluded, that the best game machine for cyber security game would be a PC based game. It is also concluded that browser-based games would be more usable and useful, since they do not require installation of specific software on the PCs. Also, the constant updates required due to the dynamic nature of cyber security

can be more effectively managed from a central game server, rather than the regular provision of updates to standalone games.

3.3. Use of serious games in Estonian school system

Serious games are used mostly for teaching economy within the school program in Estonia (Sillaots 2014). Two games are used: JA Titan (for high school students) and Simulaator 7 (for middle school students). The games have been introduced within the elective subject Economy and Entrepreneurship, and are managed by Junior Achievement Estonia.

JA Titan

Junior Achievement (JA) launched JA Titan as a Web-based product in 2000. The game is set in year 2035, and creates a world in which players are CEOs of their own companies. JA Titan was originally developed in 1980s as a Management and Economic Simulation Exercise (MESE), and is used as a business simulation game for secondary school students today around the world. During game play, the students run a manufacturing company and make six business decisions: price of product, production levels, marketing expenses, research and development costs, capital investment level, and charity. (Saar 2014)

Success in JA Titan is measured by a "Performance Index," an evaluation of each fictional company's performance based on: Earnings, Supply and Demand Potential, Productivity, Market Share and Growth. During the game, players have to try to achieve the highest Performance Index possible. At the end of game, the player with the highest index wins. (ibid)

JA Titan is used in teaching economy in Estonia and for national competitions between participating schools. Since 2009, JA Titan has also been one part of "Economy Olympics" in Estonia. (ibid).

Simulaator 7

Simulaator 7 offers lower secondary school students an opportunity to manage a virtual company with limited resources. The game engine has five different scenarios (provision of services and buying or selling goods), which even with repeated use makes the content exciting and new. The players can sell ice-cream, post cards, flowers, printer cassettes, or wash cars. (ibid)

The game is divided to periods corresponding to one week. At the beginning of each period, the simulator gives players a simplified account of the company, together with a virtual economic space. After reading the accounts, the players have to make three decisions: goods to be bought for the period of one week, wholesale price for goods or services, and expenditure for advertising. Teacher controls the functioning of the market, and can change parameters as required: importance of advertising, wholesale prices, running expenditures, salary costs, and general market environment (demand for goods) – this gives possibility for the creation of different unique scenarios. The goal of the game is to make enough profit in a situation, where there is competition and changes in economic environment. (ibid)

The game can be played within one classroom, or as a competition between different schools.

Simulaator 7 was developed by two Estonians in 2005. They got the idea for the game after graduating from JA Estonia programs by themselves, having played JA Titan. (ibid)

3.4. Use of educational cyber security games in the world

There are a number of cyber security games available and used around the world. There are games focused more on the technical side of cyber security, and there are those focused more on the human aspects. This chapter starts by discussing if a computer game on cyber security can be entertaining and educational, and then continues analyzing a number of games available. The games analyzed below are those that the author deemed relevant for the purposes of this research: serious games with an educational purpose, rather than purely entertainment games.

3.4.1. Cyber CIEGE

Cyber CIEGE is a video- computer game developed at the U.S. Naval Postgraduate School (Monterey, CA) together with Rivermind, Inc. The development of the game was sponsored by the U.S. Navy and other U.S. Department of Defense/ Department of Navy entities. (Irvine, Thompson, Allen 2005)

Cyber CIEGE covers a broad range of cybersecurity topics, focusing mainly on Information assurance. During the game, players buy and configure computers and

network devices, and keep users satisfied while at the same time protecting assets from different incoming attacks. The game has numerous scenarios, some focused on basic awareness training, others on more complex network security issues. The objectives of the game derive from U.S. Navy and Department of Defense guiding documents on Information Assurance. The main challenge for the game according to developers is the dynamic nature of cyber security. (Irvine, Thompson, Allen 2005).

The purpose of the game is to create an extensible Information Assurance (IA) teaching and learning laboratory, where IA concepts can be taught through the use of a scenario definition language (ibid). Cyber CIEGE is essentially a resource management PC-based computer game. Within the game's virtual world the players spend virtual money to operate and defend their networks, and they can also watch the consequences of their actions while attacked (Figure 4). Cyber CIEGE consists of several elements: a simulation engine, a scenario definition language, a scenario development tool, and a video-enhanced encyclopedia (ibid). The game engine was developed using C++. (Cone, Irvine, Thompson, Nguyen 2007)

Cyber CIEGE covers a broad range of cyber security topics. Players buy and configure computers and devices to keep users happy (e.g., by providing Internet access) at the same time protecting assets from different potential attacks. The players can configure workstations, servers, access control lists together with operating systems and access control policies, they can use Public Key Infrastructure (PKI) based cryptography to protect e-mail, VPN or internet traffic. The network security assets addressed (and configured during the game) are firewalls, VPN gateways, VPN clients, link encryptors and authentication servers. (Irvine, Thompson 2005)

The game has hundreds of different scenarios, initially developed at the U.S. Naval Postgraduate School and currently also using open source paradigm by the game website (http://cisr.nps.navy.mil/cyberciege.html), where educators can both submit new scenarios, download existing ones, or share their work with others. Some scenarios focus on basic training and awareness, and others on more complex network security issues. (Irvine, Thompson, Allen 2005)

Cyber CIEGE is used at the U.S. Naval Postgraduate School, various agencies of the U.S. Government, and a small number of schools in the U.S.

The content of the game (teaching objectives) derive from the U.S. Navy and Department of Defense guiding documents on Information Assurance: value of information (personnel

files, legal records, classified information), communications and computer vulnerabilities (malicious software, internet risks, human errors, internet security), basic safe computing practices, password management (generation, protection, change frequency), local physical security procedures (Core, Thompson, Irvine, Nguyen 2007). The developers of the game consider the dynamic nature of IA topics the main challenge (ibid).

Figure 4: Cyber CIEGE screenshot

3.4.2. Cyber PROTECT

Cyber PROTECT (WWW 2014) is an Information Assurance game, created with sponsorship from U.S. Assistant Secretary of Defense for C3I and the IA Program Management Office of the Defense Information Systems Agency. Within the game, one has to buy and apply information security countermeasures in a local area network. (Irvine, Thompson, Allen 2005)

The game is a resource management simulation of a small and simple local area network, which has many internal and external connections, connecting to different parts of the organization and the internet (ibid) (see Figure 6). The game is principally focused on Information Assurance security terminology, concepts, and policy. (ibid)

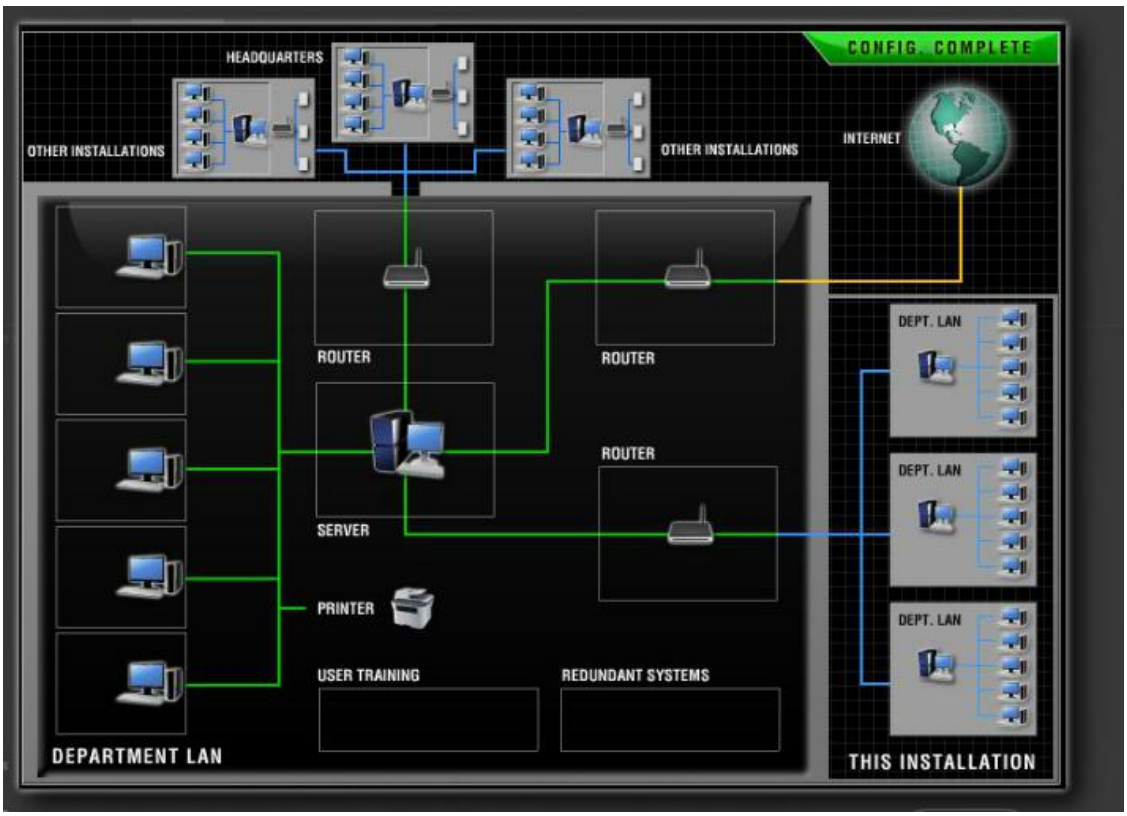


Figure 6: Main page screenshot, Cyber PROTECT

According to the game tutorial, the game takes place over one year, in periods of four quarters. At the start of the game the players have a connected network, and they have a budget to make choices to select tools as available in the game. The tools available to the player are user training, redundant systems, access control, anti-virus program, backups, disconnection, encryption, firewall, and intrusion detection software (Figure 5). The tools are chosen using drag-and-drop method. Attacks take place randomly, and an element of luck is built into the game. The decisions made will be recorded and then a number of attacks take place. (Cyber PROTECT tutorial 2014).

Figure 5: Tool selection in Cyber PROTECT

The numbers of attacks are random, coming from both outside and inside of the organization. Different types of attack include data modification, data theft, flooding, imitation or spoofing, jamming, mole, packet sniffers, social engineering and viruses. Up to six attacks may take place within one period of the game, i.e. one quarter. After each period the players get feedback from the game about the nature and effects of the attack and whether the defense of network was successful or not. In the end the player receives feedback (score sheet), detailing the success in buying and applying network security to defend against attacks. Just like in real world, the element of luck associated with the attacks plays an important role. Therefore, the player may make bad choices and still be successful, or they may make good choices and still be unsuccessful. (ibid).

The game is used for training in the U.S. Department of Defense, and is also accessible online for anyone to play.

3.4.3. Other games

There are many other games available, and for the purposes of this thesis we analyzed games of different focus. The Information Security Wargaming Simulation is principally a decision-making game, the Anti-Phishing Phil a game teaching techniques to spot phishing attacks, 2025 ExMachina a game on social networks. The short analysis is provided below.

Information Security Wargaming System

ISWS was created for the U.S. National Defense University by the Defense Information Systems Agency. It is a simulation that gives insight to attacks and defense. It is a simulation that gives insight to attacks and defense. In the game, the player has to buy and apply information security countermeasures in a Local Area Network. (Irvine, Thompson, Allen 2005)

The player has to make decisions that enable enforcing an organizational policy, selecting defense tools. Within a (game) year, the player decides what kind of resources to buy and install, and after these decisions the simulation starts and the player faces different security attacks (ibid).

This simulation focuses on network-based attacks. For the game the developers worked out a taxonomy of attacks, and exercises focus on one particular attack in isolation.

Anti-phishing Phil

Anti-Phishing Phil is a game developed by Wombat Security Technologies Inc., it is a security training game that teaches people to notice fraudulent and correct URL-s. (WWW 2014). It is an educational game designed to train users about phishing attacks (Kumaraguru, Sheng, Acquisti, Cranor, Hong 2009). The main character in the game is a fish called Phil, who wants to eat worms in the sea, but has to be careful not to eat fake worms, which represent phishing attacks (ibid). Figure 7 shows screenshots of the game. The game is split into four rounds, each lasting 2 minutes. (ibid).

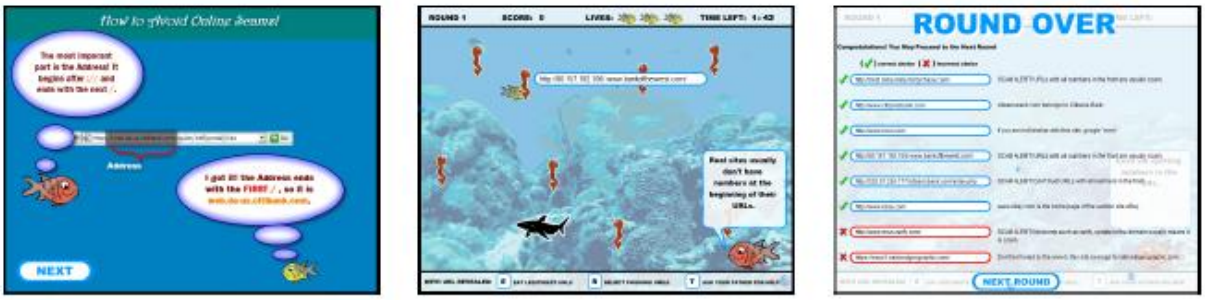


Figure 7: Anti-Phishing Phil

Ex Machina

Ex Machina is a game about using social networks in a smart and secure way. In the game the player is a net-detective and will have to go back in time 20 years to change the social network profile and postings of a person (Figure 8). In the past, this person has posted a lot of information on his social network profile, which provides problems in his life today. The aim for the game is to teach that one shouldn't accept anybody as a friend, and not post anything online. (WWW 2014)

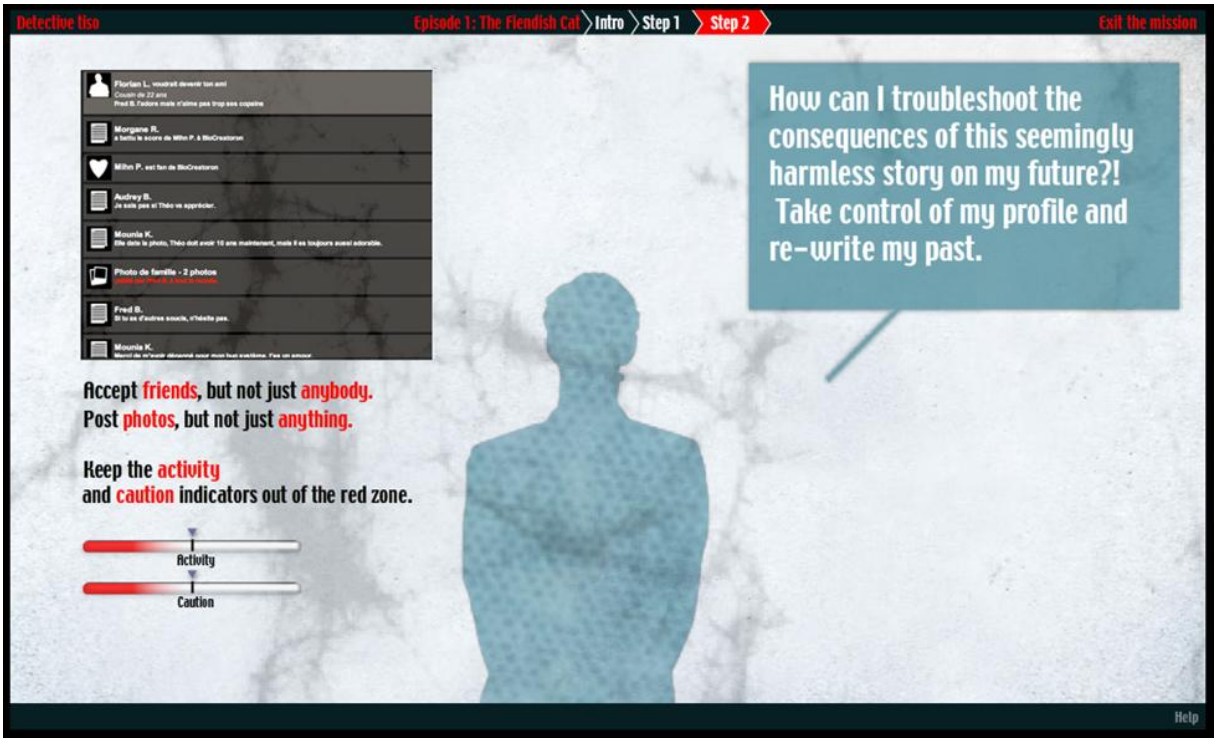


Figure 8: Ex Machina game screenshot

3.5. Conclusion

It is concluded that an entertaining game for effectively teaching cyber security can be built and there is a number of games available, mostly developed for and used by the U.S. military. Even though the Internet can be said to be such a game itself, it is not a good place to learn about security issues due to potential attacker motives. Three of the games analyzed above (Cyber CIEGE, Cyber PROTECT and ISWS) are serious games, and principally resource management games. The Anti-Phishing Phil, though used quite widely, is focusing on one specific aspect of cyber security: phishing attacks. The Ex Machina is a game on posting information on social networks. The common denominator of all these games is that players have to make choices with regard to security, avoiding unwanted outcomes.

Serious games on cyber security are currently used to a big extent by the U.S. military (all services), but also in private enterprises. Most games are based on the IT security policies of either government entities or private enterprises.

Few serious games are used in the education system in Estonia today. The analysis above has given a good overview of serious games used in the educational system in Estonia from one side, and the different cyber security games available in the world from the other side.

This chapter has looked at what are games and what is gamification. The chapter defined these terms, then looked at how games are used and what are their main characteristics. We also looked at how serious games are used in Estonian educational system, and which cyber security games are available around the world. In the next chapter we will define a game concept for an educational game on cyber security.

4. Educational computer game for cyber security

Chapter 4 concentrates on the solution: a computer game, and provides a game concept. A game concept is a description of the game, that allows for developing a product, it is a general idea of the game (Adams 2010). Prior to any game design, a concept is the most important document to be developed (ibid). The game concept will state objectives and give a proposal as to how to integrate the game to cyber security teaching within a framework. We will develop a game concept for teaching cyber security topics in accordance with the program used for teaching in national defense, as shown in Chapter 2. As provided in Chapter 2, five main areas for teaching will be covered in this game concept: computer, web, wifi, smart devices, social networks. The chapter will conclude with potential additional uses of the game.

As it was concluded in the previous chapter, serious computer games for cyber security are used for teaching cyber security related issues in different settings. A serious game can be any game, from which one can learn something, in which the activities of players can be measured, and where the player can be awarded (Kapp 2012). The success of any serious game depends on how it will be implemented. This is particularly so for educational games, as they should be both educational and entertaining. The goal of educational games is that the player can apply the theoretical knowledge received into practice (Adams 2010). The result is influenced by what the player does and how the skills get a practical value: the skills acquired are used to play and in order to win, the player has to improve skills (ibid).

Game-based cyber security awareness training can be more effective and less expensive than traditional lecture- and laboratory-based teaching (Adams 2010). The design objectives for awareness training are defined as: understanding the threats, awareness of weaknesses and attack techniques, and pedagogical objectives.

As we concluded in Chapter 3, games are a kind of play activity, where the players have to achieve at least one goal by acting in accordance with rules (Kapp 2012).

4.1. Game objectives

4.1.1. Educational content

As stated in Chapter 3, gamification uses game-based thinking and mechanics to deliver educational content (Kapp 2012). We should therefore take the content of a cyber security teaching program, add game-based elements and create a gamified learning content. For our purposes, it is considered to use the game in addition to traditional teaching methods.

The educational content of the game needs thorough consideration. The content should let the player to strive to safeguard the confidentiality, integrity and availability of data and systems, all the while acting in conformity with the rules of the game. The game should not only include information about cyber security topics, but also be relevant in a dynamically changing world of cyber security.

Understanding the threats

The first and very important step is to understand what the threats are: they can be anything from beginner hackers with malicious intents to advanced hackers trying out criminal intents. The objective in an educational game should be for the student to understand the different threats that they can face and understand why every person is a target. The game should show who are the attackers, what are their motives and objectives, how they can potentially reach their objectives and what can be done to defend against attacker actions.

Awareness of weaknesses and attack techniques

The objective should be to learn about weaknesses in computers and networks, and to understand how they are used by cyber criminals to their advantage. The objective should also be to gain an understanding as to which vulnerabilities can be eliminated and which not.

4.1.2. Pedagogical objectives

The main objective of awareness training is to train. In order to effectively do this, the game should provide an option to turn concepts into practice, provide a „restart“ possibility to re-start the game at any time, it should move from beginner to specialist scenarios in different levels, provide options to examine different avenues by reconfiguration options, as well as teach problem-solving and resource management decision making skills. One additional objective should be for the player to learn to understand the differences between usual, unusual, and abnormal system performance indicators.

Additionally from the pedagogical side, the game should provide possibility to understand the cause and effect relationships between the different actions.

4.2. Game concept

As we saw in Chapter 3, a game concept is a general idea of the gameplay which includes a high concept, player roles, primary gameplay mode and challenges for the player, game genre, target audience, game machine, competition modes, summary of game progress from start to finish, and short description of the game world. A game concept is a description of the game, that allows for beginning to developing a product, a general idea of how it is intended to entertain through gameplay (Adams 2010). Prior to any game design, a concept is the most important document to be developed (ibid). This chapter proposes the game concept for computer game on cyber security.

In parallel with this thesis a prototype computer game is being developed. The design of game prototype is done together with four other TUT students as a separate project. This thesis provides a conceptual base for prototype development. The game prototype was presented as participatory form of design (Sillaots 2014) to four high school students and two teachers. Their ideas concerning attractiveness and usability of the game were taken into account and relevant elements will be added. The prototype was presented at the independent game developers festival “Mängutis” in Tartu, Estonia, on May 23, 2014. The game developers present at the festival gave positive feedback to the idea, adding that commercializing the product beyond educational use would require additional work on design and user interface, in addition to introducing more complex scenarios.

High concept for the game

The game to be developed should have the potential to become an effective teaching aid for teaching of cyber security within the national defense elective course. It will provide a virtual world, combining human and technical factors, which allows students to learn about cyber security with the help of a game. The main aim of the game is to introduce cyber security topics in a way that the students get a personal experimenting environment, where they can make security choices and see the results of these choices. The game will also explain terminology – for example "wifi router settings" may not sound meaningful, but understanding how the attacker may abuse poor settings and what consequences this brings, will make the abstract concept understandable. The game can be used for illustration of traditional lessons in the school or for homework. At the start of the game, the player has a set of resources: money, and confidentiality, availability and integrity of data and systems. The duration of different parts of the game is not set, but will depend on player decisions. However, it is recommended that game should be used together with classroom discussion limiting duration of game parts to duration of one lesson, i.e. maximum of 45 minutes (Sillaots 2014). In case of giving gameplay as homework, students can play it longer (ibid).

The player roles in the game

The player in this game will play a computer user with different tasks as set in the scenarios. The game starts with buying a computer and then setting up of a small network. The player has to buy different settings, change default settings and manage everything strategically, so that it would be secure and his confidentiality, integrity and availability levels would be retained. In doing so, the player has to think strategically and use his available resources smartly.

Primary gameplay mode and general types of challenges the players will face

The game will start with the player having a set amount of money, as well as integrity, confidentiality and availability of data and the system. These amounts will change during the game, reflecting player decisions. All events taking place within the different scenarios

and the game world will influence any of the four assets, and these will change according to player decisions. There are no correct or incorrect choices, the aim is for the players to understand that all choices made or not made will have a meaning and consequence.

Every move a player makes will have consequences in the game: the player does not see the game mechanics, but has to think and make logical steps. Some settings have more weighted importance than others, and failing to set these will have consequences i.e. in that the network integrity will fall. However, the game then replies with what has happened to network integrity and the player can subsequently take steps to rectify the integrity of his network.

During the game there will be "pop-up news flashes" that introduce events happening in the game world, i.e. discovery of new malware or hackers finding new exploits to use. The player will subsequently have to make choices within the game world to manage the situation and prevent attackers from exploiting the vulnerabilities.

The genre of the game

In Chapter 3 we looked at the different game genres and concluded that the best game genre for cyber security would be a strategy game. Strategy games include strategic and tactical challenges; they challenge the player to achieve victory through planning (Adams 2010). Strategy games fall into two main sub-genres: classical turn-based games and real-time games (ibid). For an educational game on cyber security, a turn-based game is considered more suitable: the players may think about their moves and weigh the benefits of different choices. Even though this can be a time-consuming exercise, the time factor is not important for the purposes of an educational game – the intent is exactly that players make informed and weighted choices. (ibid)

It is suggested that the educational cyber security game give players a fixed amount of resources at start of game, and the players will play until these are exhausted. The players have to defend the confidentiality, integrity and availability of their systems using a set amount of monetary resources given at start of game.

Defining the target audience

Since we are developing an educational game, the target audience is students. This game will not be meant for primary or lower secondary school levels, but rather for upper secondary school (high school) level students, at the ages 15-19. Designing the game we assume that the students have already learned some basic issues of cyber security, and this will be the next level from basic cyber hygiene or e-safety training. The game will be developed based on the cyber security teaching program within the national defense elective.

It is assumed that by the time students join this course, they have received basic Informatics teaching as stated in PRÕK 2011 and explained in detail in Chapter 2 of the current thesis. Background knowledge of basic computer skills is a prerequisite.

However, designing a game for a target audience of upper secondary school level does not mean that all others will be excluded. It is true that children start working with computers earlier, and therefore it will be up to the teachers to decide when and how to use the game in their teachings. Also, the game can be easily tailored to specific needs of specific private enterprises based on their respective security policies. As said before, the game does assume certain background knowledge, or at least a willingness to learn this background information while playing.

The game machine to be used for the game

As we concluded in Chapter 3, the most suitable medium for cyber security would be a PC-game, more specifically web-based computer game. This is so due to the fact that cyber security is such a dynamic topic and changes need to be made to the game constantly. The dynamic nature of the game can be reflected by provision of a web-based computer game.

Competition modes to be used (single- or multiplayer, competitive or cooperative)

The game will initially be developed as a single-player game. The player plays against the game's rule set. The game can be configured and managed in real time by the teacher according to teaching objectives.

In the beginning of the game, the player's integrity, confidentiality and availability levels are all set to 100, and he has a set amount of resources available. During the play, the player uses these resources to buy various assets and his integrity, confidentiality and availability levels, together with resource levels will change according to the strategic decisions made during gameplay. Making decisions on resource use may decrease the integrity level, but smart use of resources could also increase the confidentiality or availability levels.

In later stages of development, it is suggested to also consider including multi-player and cooperative versions of the game.

Game progress

The game starts with an introductory scenario, where the player has to buy a computer and make initial settings so that the computer would be secure. The player is a sales representative working from home, who has some sensitive information stored on his/ her computer. The game continues with a view on wifi settings, where the player will have to secure his connection, set wifi router to encrypted connection, and perhaps even introduce and use VPN. Later in the game, the player has to buy items from the internet and before doing so should learn about using internet securely, especially when conducting financial transactions. In the game the player will travel to Paris, and will only use his smartphone and tablet there. Before going, he also wants to download some city guides and maps as apps for smart devices. For doing that, he has to learn about being sure everything is updated and how to secure his devices with a code or password, and also how to be sure that apps are downloaded from authentic sources. During his travel to Paris, the player wants to share all the excitement and experiences with friends and family on social networks. But in doing so, he should be careful as threats are never far away.

During the whole game, different pop-up news flashes will appear, letting the player know of different security threats happening in the game world. The player has to make decisions as to which actions to take, so that the integrity, confidentiality and availability levels would not fall. The game can be used in class or given to students as homework, to be discussed in later class sessions.

The game is divided to five sessions. In the first session, the player will have to choose his Wifi settings at home. He is a sales representative working from home, who also has some

sensitive data stored on his computer. He has to set up his wifi settings so that his system and data would be secure. He also has to safeguard the confidentiality, availability and integrity of his data and system. At the same time the player must remember that he has a limited number of monetary resources that he can use, and therefore has to make choices that will not exhaust his resources in the initial stages of the game. Upon game start the player is given a scenario and random news events happening in the world. In the example shown at Figure 9 below, a newsflash is given that warns against recently found new vulnerabilities in most popular wifi routers that the hackers use. Our player uses the same router at home and has to therefore make choices about necessary security settings. His options in this example are: not setting anything at no cost, checking basic settings at the cost of 20 units, setting encrypted WPA settings at the cost of 25 units, or setting VPN connection to his work server at the cost of 50 units. The player will make choices, and an attack takes place. He will then see the result and impact of his decisions. As shown in Figure 9, no settings leads to loosing 25 points of confidentiality, 25 points of availability and 25 points of integrity levels, as well as 30 monetary units. Basic security settings lead to no change in monetary assets, but due to potential abuse of vulnerabilities, confidentiality, availability and integrity levels fall by 10. In every step of the game there will be one choice that will not make sense in the game, like VPN in our example. The player will have to learn what is VPN, and the fact that it costs more than anything does not mean it would be the best option in the game. Similar logic will be used throughout the different scenarios. The game mechanism explains the different actions for current 5 scenarios (see Annex 3).

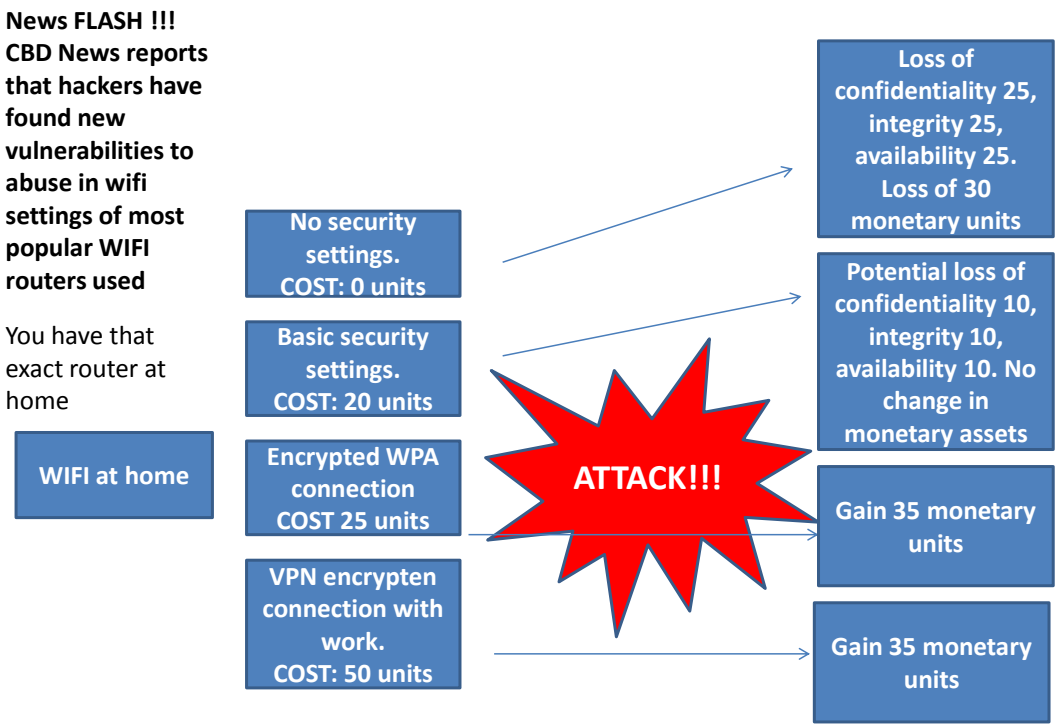


Figure 9: Game progress at single game level explained

Figure 10: Screenshot of prototype, first session (wifi)

The prototype's screenshot is depicted in Figure 10. The player experiences the world as end-user, through a first-person game.

Game flow is explained in Figure 10. The game is organized in levels that correspond to the different scenarios as per teaching program. The player progresses in the game one level at a time by accumulating points in return for accomplishing tasks. In the beginning of each level, there will be an event taking place in the game world. These events will be displayed as pop-up messages and are managed by teacher in accordance with teaching objectives or at random, as decided. In order to progress in the game, the player must make security choices to survive in the cyber world. Survival is measured in confidentiality, availability and integrity of his data and systems. Making good choices will increase resource levels, making bad choices will decrease them. Figure 9 above illustrated the game progress at single level.

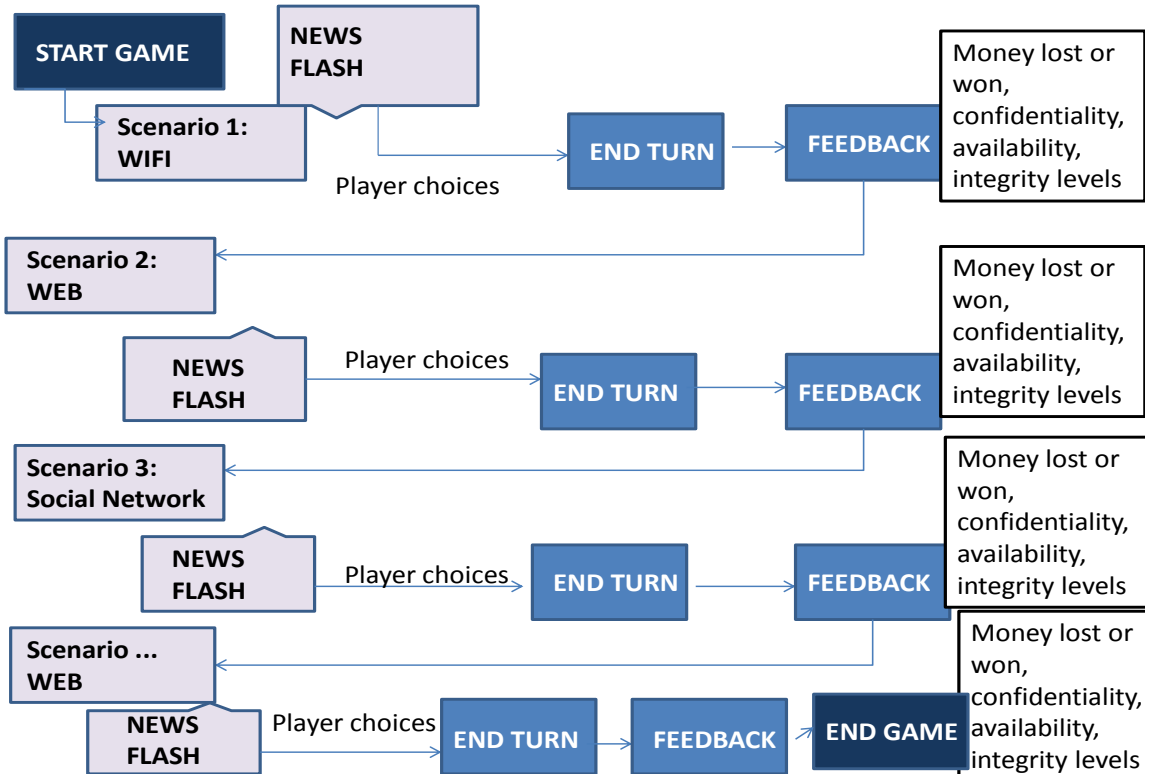


Figure 10: Game flow explained

Short description of the game world.

As the game is based on teaching of cyber security within national defense elective, we will take the five sub-areas covered as basis for game world and scenarios. The scenarios will grow in complexity, starting from an introductory small (home) network and in later

stages growing into networks with subnets and different internal intranet and external internet connections.

The five areas covered initially are those used in the national defense elective cyber security teaching: computer, web, wifi, smart devices, and social networks

A short preliminary description of the scenarios and learning objectives are provided below in figure 12. A common denominator for all games is a pop-up window with random events in the game world of new vulnerabilities, viruses or attack methods found. This will be inspired on real-world events and will be included in the game dynamically as they appear.

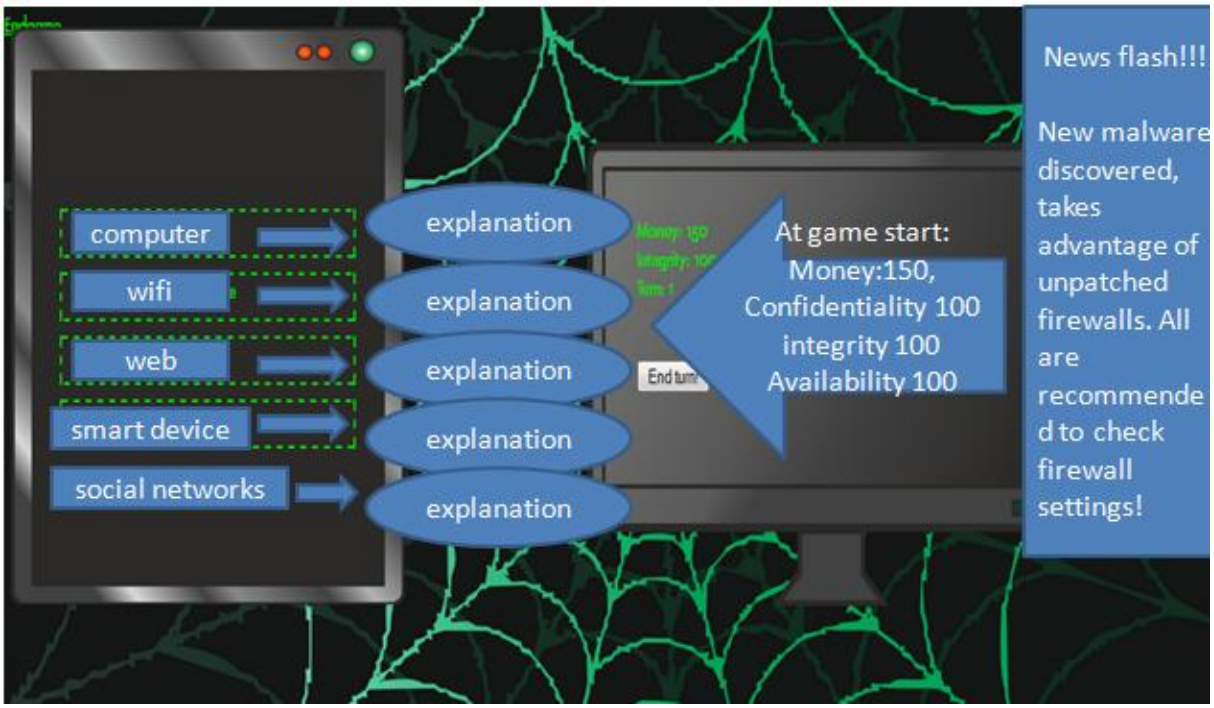


Figure 12: Cyber security game prototype screenshot. First page.

Game scenarios

1) Computer

Introductory scenario. The play starts with buying a computer and conducting basic security settings, then basic network settings. The player will have to learn to:

- set updates to running automatically,

- changing user accounts for different purposes, including administrator account for administrator purposes only,
- set virus protection,
- set a firewall,
- not allow autorun from external devices,
- creating backups,
- encrypting his/ her data.

2) Wifi

In the second scenario, the player is a sales representative working from home. This is a simple network connection with one host; a home computer connected to the Internet. The player stores sensitive data and program files on his computer. The objective is to secure wifi settings so that potential attackers will not get access to his computer. When the game starts, a dialog box is displayed and describes the game objectives along with the game characteristics. The player will have to learn to:

- secure his wifi connection,
- set his wifi router/ hotspot to encrypted connection (WPA2),
- set in his wifi router the MAC and IP addresses of those authorized to use it,
- possibly introduce and use VPN (*Virtual Private Networking*).

3) Web

In this scenario, a follow-on from the previous scenario, the sales representative working from home has to buy items for work from the internet. In order to do so securely, the player will have to learn to:

- use the most updated version of his web browser,
- set the web browser for secure use, including security settings, prohibiting JAVA scripts,
- not to use internet while using computer on administrator account,
- make sure the website is authentic, especially while dealing with sensitive information (financial transactions),
- not to open e-mail attachments from the suppliers, which contain file extensions such as .exe, .bat, .com, .pif, .scr,
- avoid opening files with the above extensions while using the internet.

4) Smart device

As per previous scenarios, the player is a sales representative working from home. Now he will have to travel to Paris, and decides not to take his computer with him. He has a smartphone and a tablet, and can use these for both work and fun while on this trip. He also wants to download an app with tourist information on Paris and a city map. The player will have to learn to:

- make sure the smart device's operating system is updated,
- make sure the apps used are updated,
- download new apps from trustworthy sources only,
- install an anti-virus,
- lock the screen with a code or password,
- make a backup copy of his devices.

5) Social networks

While on the trip to Paris, our sales representative wants to share his new experiences, the beautiful pictures, good food and interesting thing he learned in Paris with friends on social networks. The player will have to learn to:

- understand and change security settings on social networks,
- think of consequences before posting things on social networks,
- not to share too much information on his activities, habits, family and friends,
- not to post anything that could be harmful,
- be careful about other people's postings, as they may not be authentic,
- not to click on links or postings when can not be sure of its authenticity.

4.3. Integrating a computer game to traditional teaching

While teaching cyber security in traditional way, by using lectures, these could be amended by an illustrative computer game. The five scenarios/ case studies above can be a first step in developing this game.

The game concept as above reflects teaching program on cyber security, as done today within the national defense elective program. Using the game concept above and developing a computer game based on that can provide for an effective teaching aid to regular teaching.

4.4. Additional uses for the game

The game can be used for teaching of cyber security in a setting wished, and can be amended with additional scenarios for deeper knowledge for those interested. It will also be possible, with some amendments, to use the game for nation-wide Informatics or Cyber Security competitions between individual students or teams of students.

5. Conclusion

This thesis focused on developing a game concept for an educational computer game, which can be used in cyber security teaching under the auspices of national defense elective. In parallel with this thesis and based on its findings, a computer game for cyber security will be built. The first prototype is already available.

The aim of this thesis was to analyze the potential of using serious games in cyber security and to come up with game concept for an educational cyber security computer game usable in Estonia. Prior to any game design, a game concept must be developed and this thesis provides for that. To do this, the thesis researched theories of gamification and serious games. We concluded that an entertaining game for effectively teaching cyber security can be built and there is a number of games available. We concluded that people don't play games just for rewards, but also for learning, for feeling of accomplishment and achieving success. We also looked at serious games used in Estonian educational system and found that some games are used successfully in the elective course of Economy and Entrepreneurship.

The thesis studied how cyber security is taught in Estonian schools. For that purpose, we looked at the national school curriculum and found that even though cyber security is not mentioned as such, elements of it are. We also concluded a survey of teachers, the results of which showed that teachers consider cyber security to be an important subject. The survey of teachers was followed up by semi-structured interviews with other teachers, university teaching staff and government officials. Having studied the theory of gamification and serious games, and the current situation in Estonia, the thesis continued with provision of a game concept. The game concept developed will be usable for cyber security teaching within the national defense elective.

The game concept provided objectives for the game, scenarios and general game mechanics. Game mechanics are at the heart of any game, because they define the challenges in the game, the actions that the player can take to meet these challenges, and the consequences of player's actions in the game world. The mechanics set conditions for achieving game goals and consequences in doing – or not doing – this.

The target audience for the game is upper secondary school, age group 15-19. The game is intended to be a teaching aid, used in parallel with other means of teaching. It can be used

for illustration of traditional lessons in the school or for homework. The game will provide a virtual world, combining human and technical factors, which allows students to learn about cyber security. The main aim of the game is to introduce cyber security topics in a way that the students get a personal experimenting environment, where they can make security choices and see the results of these choices. The students will learn terminology and the importance of making informed decision with regard to their personal cyber security.

The game will be a web-based computer game, that can be played on any modern PC with an internet connection. It is assumed the students have basic background knowledge about IT and security. It is suggested the game to be a single-player game at initial stages, with potential to develop multi-player versions at later stages. The game will be developed based on the cyber security teaching program within the national defense elective.

In parallel with this thesis a prototype computer game is being developed. The work on prototype is done together with four other TUT students as a separate project.

Proposals for future work

It is recommended to finalize programming and design of the game, based on the game concept as provided in this thesis. For future work it is recommended to develop a user-friendly scenario definition mechanism that would enable to define any additional scenarios as teachers see necessary in an easy manner. It is important to develop it in such a way that the game can be configured and managed in real time. The study content will also need constant development, as cyberspace is a very dynamic environment, and it is therefore recommended to renew this periodically. It will also be possible, with some amendments, to use the game for nation-wide Informatics or Cyber Security competitions.

Once the game will be finalized, it is suggested to make a comparative analysis with two test groups: one receiving traditional lecture-based teaching on cyber security, the other game-assisted teaching. It is suggested to assess the effectiveness in teaching and results of these two test groups in parallel.

In later stages of development, it is suggested to study the potential of using multi-player and cooperative versions of the game, as well as conduct research for that purpose.

Bibliography

A.Dignan. “Game Frame: using games as a strategy for success”, New York 2011

A.Nagarajan, T.L.Janssen. Exploring Game Design for Cybersecurity Training. In *Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, 27-31 May 2012, Thailand*

A.Kuusk. Interview 15 april 2014

A Users’ Guide: How to Raise Information Security Awareness, ENISA 2006

B.D.Cone, M.F.Thompson, C.E.Irvine, T.D.Nguyen. Cyber Security Training and Awareness Through Game Play. U.S. Naval Postgraduate School, Monterey CA.

B.D.Cone, C.E.Irvine, M.F.Thompson, T.D.Nguyen. A Video Game for Cyber Security Training and Awareness. In *ScienceDirect Computers & Security 26 (2007), 63-72:*

CERIS 2007 "Centre Européen de Recherches Internationales et Stratégiques” research guide

C.E.Irvine, M.Thompson. Teaching objectives of a simulation game for Computer Security. In *Proceedings of Informing Science and Information Technology Joint Conference,* Pori, Finland, June 2003

C.E. Irvine, M.Thompson, K.Allen. Cyber CIEGE: An Extensible Tool for Information Assurance Education. In *Proceedings of ninth colloquim for information systems security education,* Atlanta, GA, June 2005

C.E.Irvine, M.F.Thompson, K.Allen. An information Assurance Teaching Tool for Training and Awareness. In *Federal Information Systems Security Educators’ Association Conference* North Bethesda, MD, March 2005.

C.Mead. War Play, Boston, New York, 2013

Cyber PROTECT game. http://iase.disa.mil/eta/cyber-protect/launchcontent.html [WWW] 20 April 2014

E.Adams. Fundamentals of Game Design, 2nd edition, Berkeley 2010

EU Commission. Special Eurobarometer 404 Cyber Security, November 2013, http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf [WWW] (2014-03-22)

EU Commission. A strategy for a Secure Information Society – "Dialogue, partnership and empowerment". Brussels 2006

EU Commission. Special Eurobarometer 404: Cyber Security. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf [WWW] 15 December 2013

Google questionnaire "Survey of teaching cyber security in Estonian schools", 2014

Kaspersky security bulletin 2013 http://media.kaspersky.com/pdf/KSB_2013_EN.pdf [WWW] 15 May 2014

K.M.Kapp. The Gamification of learning and instruction, San Francisco 2012

M.Kerttunen, E.Tikk-Ringas. Interview 15 april 2014

K.Kikkas. Wikiversity. https://beta.wikiversity.org/wiki/Security_and_Privacy_in_a_Networked_World [WWW] april 2014

Ministry of Economy and Communications official. Interview 14 april 2014

Ministry of Defense official. Interview 03 March 2014

OECD. Cybersecurity Policy at a Turning point: Analyzing a new generation of national cybersecurity strategies for the Internet Economy, OECD 2012

OECD. OECD Guidelines for the Security of Information Systems and Networks, OECD 2002

OECD. OECD Internet Economy Outlook 2012, OECD 2012

Riigi Teataja 2011. Põhikooli Riiklik õppekava.
https://www.riigiteataja.ee/akt/13273133?leiaKehtiv
[WWW] may 2014

Riigi Teataja 2011. Gümnaasiumi Riiklik õppekava.
https://www.riigiteataja.ee/akt/13272925?leiaKehtiv
[WWW] may 2014

R.Saar. Interview 28 March 2014

Survey EU Kids Online 2011, http://eukidsonline.ut.ee
[WWW] april 2014

T.Niggulis. Interview 25 march 2014

T.Nikolakopoulos. Evaluating the Human Factor in Information Security, Masters Thesis, Oslo University College 2009

2025 ExMachina http://www.2025exmachina.net/en
[WWW] 19 april 2014

Annexes

Annex 1

Küberturvalisuse teemade õpetamine Eesti üldhariduskoolides

Käesolev küsimustik on koostatud informeerimaks Tiia Sõmer'i koostatavat magistritööd Tallinna Tehnikaülikooli Küberkaitse õppesuunal, teemal "Küberturbe õpetamise võimalused arvutimängude kaudu". Osana tööst kajastatakse hetkeseisu küberturbe õpetamisel Eesti üldhariduskoolides, millisel otstarbel on ka praegune küsimustik koostatud. Küsitud andmeid kasutatakse ainult nimetatud magistritöö koostamisel ning küberturvalisust õpetava arvutimängu välja töötamisel. Vajadusel saate töö autoriga kontakteeruda e-kirja teel aadressil tiia.somer@eesti.ee

* Required

Kui oluline on teie hinnangul küberturbe teadlikkuse tõstmine üldhariduskoolides? *

Valige üks.

- Väga oluline
- Oluline
- Ei ole oluline
- Ei oska öelda

Kas riiklik õppekava sätestab küberturbe õpetamise? *

Valige üks.

- Jah
- Ei
- Ei oska öelda

Kui vastasite eelmisele küsimusele "Jah", siis kuidas ja millisel kooliastmel (alg-, põhikool, gümnaasium)?

Kui vastasite eelmisele küsimusele "Ei", siis kas teie hinnangul peaks?

Sõltumatult riiklikust õppekavast, kas õpetate küberturbe põhimõtteid?

Küberturbe all on silmas peetud teadlikkust küberruumis valitsevatest ohtudest, nende ennetamisest ning vajadusel lahendamisest. Kui te ise ei õpeta, siis palun vastake oma õppeasutuse kohta.

- Jah
- Ei

Kui õpetate küberturvalisust, siis millise õppeaine raames seda teete?

Palun vastake oma sõnadega. Kui te ise ei õpeta, palun vastake oma õppeasutuse kohta.

Kui teie/ teie õppeasutus ei õpeta küberturvalisust, siis kas olete mõelnud selle vajadusele?
Kui peate küberturvalisuse kajastamist koolis vajalikuks, mis on takistanud teil selle tegemist? Palun vastake oma sõnadega.

Kas kasutate/ oleksite valmis kasutama infotehnoloogilisi lahendusi küberturvalisuse õpetamisel *
Valige üks.

- Jah
- Ei

Millisel kooliastmel teie hinnangul peaks küberturvalisust õpetama? *
Valige üks või mitu (vastavalt enda hinnangule)

- algkool
- põhikool
- gümnaasium

Milliseid küberturvalisuse teemasid kajastate oma programmides? *
Palun valige kõik sobivad. Vajadusel kasutage täiendavat tekstirida kommenteerimiseks

- internet turvalisus
- privaatsus
- identiteedivargus
- pahavara (malware)
- laste internetiturvalisus
- küberkiusamine
- spämm
- tehnilised lahendused
- salasõnad
- Other:

Kellega teete koostööd või sooviksite teha koostööd küberturbe ja küberkaitse õpetamisel? *
(avalik- era või kolmas sektor, konkreetsed ettevõtted/ inimesed, Kaitseliidu Küberkaitseüksus, ülikoolid, rahvusvaheline koostöö, vmt.) Palun vastake oma sõnadega, võimalusel nimetades konkreetsed asutused/ isikud.

Mida arvate arvutimängu kasutamisest küberturvalisuse õpetamisel? *
Palun vastake oma sõnadega põhjendades oma vastust.

Kas sooviksite katsetada arvutimängu oma tundides? *

Palun vastake Jah/ Ei vormis ning põhjendage oma vastust.

Kas soovite midagi lisada lisaks ülalküsitule?
Palun kirjutage oma täiendavad mõtted vabas vormis

Juhul kui soovite saada kokkuvõtet antud küsimustikust, magistritööst või väljatöötamisel olevast arvutimängust, palun lisage oma kontaktandmed (teie nimi, kooli nimi ning e-maili aadress).
Vastus ei ole kohustuslik. Palun märkige vabas vormis, millisest jätkuinformatsioonist olete huvitatud.

Annex 2

Interview guide

1. What are the minimum requirements that a student needs to know regarding IT/ cyber security?

2. Is anything regulated in the national high school curriculum?

3. How important do you consider cyber security?

4. Whether and how does your school teach internet security/ e-safety?

5. Do you get outside assistance in teaching cyber security? Where from (i.e. governmental authorities, private enterprises, third sector)?

6. Do you teach protecting computer from viruses/ malware and attacks? How?

7. Do you teach legal aspects of cyber security, i.e. piracy and threats coming with it, legislation? How?

8. Do you teach netiquette and how?

9. What do you think of the idea that while teaching, you should not always grade students, that the process of learning may be more important?

10. Do you have wifi/ broadband connection at school?

11. Can students use their own devices at school (laptops, tablets, any other)?

12. Do you have a web-based forum for learning?

13. Do you think students would be receptive to web-based courses? To game-based courses?

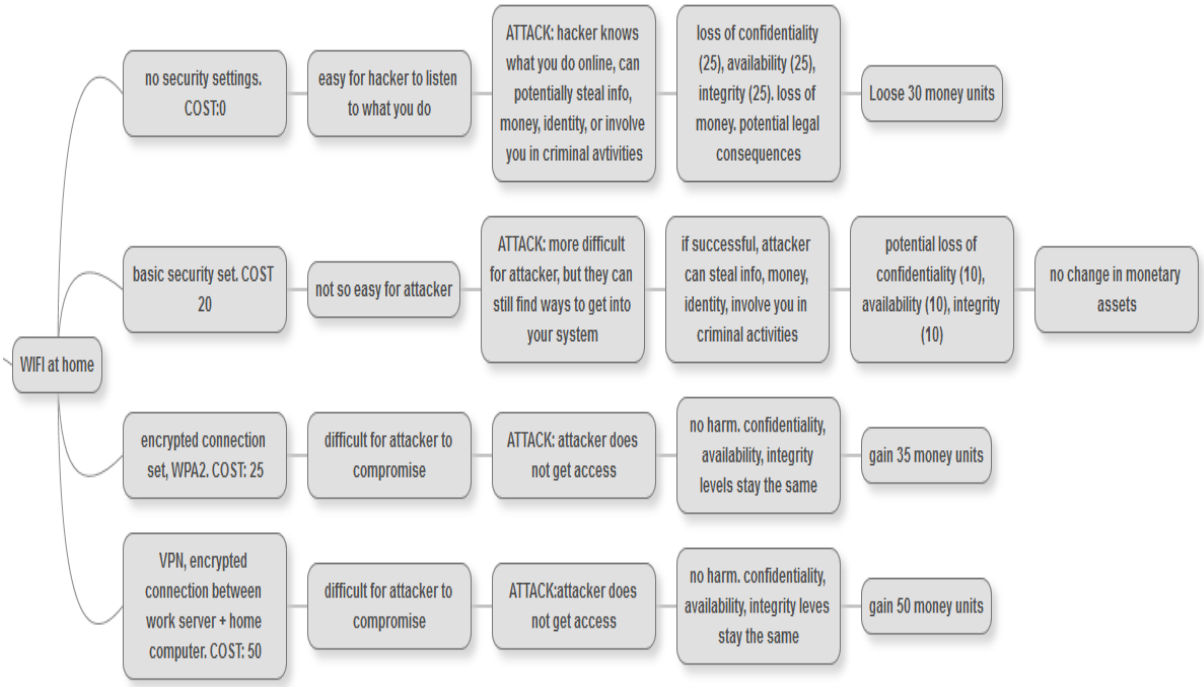
14. Do you think schools would be receptive to web-based courses? To game-based courses?

15. Would you be willing to use game-based teaching aids?

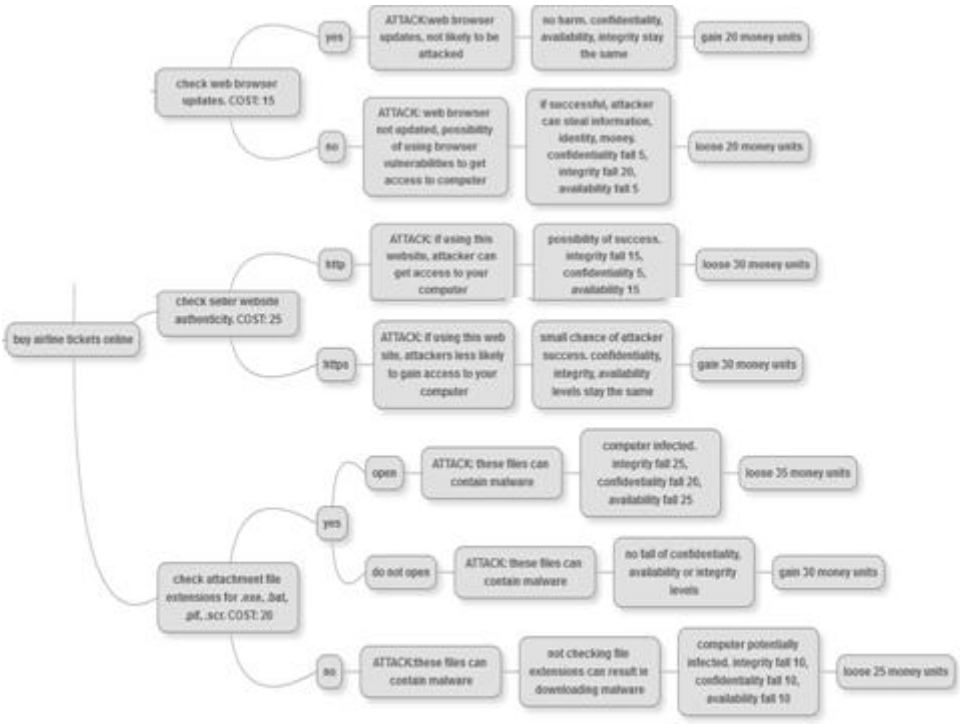
Annex 3

This annex lists the game mechanics as prepared for the three simple scenarios.

1. Wifi



2. Web – online shopping



3. Security before and during travel