THE UNIVERSITY
of EDINBURGH

Permission Impossible - the design and evaluation of a video game that teaches beginners about firewalls

Sibylle Sehl

Master of Science
Computer Science
School of Informatics
University of Edinburgh
2017

Abstract

Firewalls are a complex piece of software that present challenges to novices and experienced users alike. Recent years have seen an increased need for computer security knowledge and awareness to prevent a growing number of network attacks. Educating the general public and aspiring individuals about the topic has proven challenging so far, as the level of understanding required for most technical documentation is beyond what is attainable for most.

Educational games are often considered an engaging and useful tool to teach complex topics. By eliciting requirements from experts and existing games, learning objectives were refined to increase the basic knowledge of beginners and interested parties in the subject of firewalls. A video game was designed and developed to address the identified gaps in knowledge and enable users to apply their learning. Early findings suggest that the general public can be educated about how firewall rules are constructed and how a firewall operates to avoid common misconceptions.

Acknowledgements

I would like to thank my supervisor Dr Kami Vaniea for accepting me for this exciting and interesting project and her continuous help and support throughout the entire duration of the project. I would also like to thank her for being critical, and for providing feedback for ideas whenever possible, igniting my interest in an exciting new field and making the dissertation project such an enjoyable and rewarding experience. I would also like to thank Catherine Crompton for answering all of my questions relating to questionnaires and research methods and her help in designing the research sessions. Moreover, I would like to thank Marcus Lancaster, Ksenja Kusmin and my family for their support throughout the project and beyond.

Declaration

I declare that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified.

(*Sibylle Sehl*)

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Firewalls and Computer Security in Games

While there are more and more students entering the field of computer science, computer security is still underrepresented or offered too late in the degree in many Computer Science curricula, effectively leading to even computer science students having not much or not any exposure to topics in Computer Security (Flushman et al., 2015; Gondree and Peterson, 2013). While Computer Security is a topic that is generally considered important and people know that it should be taken more seriously, many fail to actually address this shortcoming of knowledge in their behaviour (Monk et al., 2010).

Gondree et al. (2013) have outlined the importance of attracting high-school students and interested individuals to such disciplines early in their development as to effectively increase the amount of people choosing to go into Computer Science and Computer Security. In fact, even former President of the United States, Barack Obama, has called for increased efforts in the space of digital safety, ethics and security (Obama, 2009).

Firewalls are one of the topics that are commonly explored in the context of computer security. A firewall can be described as a means to "regulate network traffic, preventing all communication except those between explicitly permitted IP addresses/port numbers" (Kandogan et al., 2012, p.24). By evaluating established rules from a rule set, defined usually by the system administrator, incoming and outgoing traffic is restricted to that explicitly being allowed, and thereby

blocking any other traffic that does not match these rules. Firewalls, however, can prove complex and even many experienced system administrators still make mistakes and can fail to accurately understand its underlying complexity (Kandogan et al., 2012). If even experts struggle to accurately manage a firewall and experience different kinds of errors, a beginner will surely struggle more, especially as there are many more resources for an experienced system administrator to learn from compared to very few for absolute beginners.

In order to bridge this gap of knowledge in pupils and students, educational games can be used to teach difficult topics or educate about a specific subject, ranging from pre-schoolers to students to adults (Druin, 2002; Olano et al., 2014; Cone et al., 2007). There are a wide range of general computer security related games, some focusing on general awareness on a lower level and some of them requiring specialist knowledge and being clearly aimed at experts and professionals, for example "Elevation of Privilege" (Microsoft, 2013). However, very few of them explored firewalls in detail and even fewer have attempted to teach firewall terminology and concepts to a complete beginner.

Following the research provided by experts in the field of computer security, this project aims to extend the delivery of knowledge in the particular area of firewalls to beginners. Increasing awareness of firewalls and introducing more students and interested parties to the topic will generate a greater understanding among all parties and provide beginners with a gentle introduction to firewalls. Previous students have tried to teach firewalls in the fashion of a video game, however, their implementations still proved difficult for beginners or did not contain enough instructions to get started. My suggested solution contains explanations and instructions as well as an application of the learning in a friendly environment which is outlined in the second design phase and available online [1]. An evaluation in terms of knowledge by using a pre-/post test and in terms of usability through the system usability scale suggest that the game is an appropriate solution to teaching beginners about firewalls and piquing their interest to learn more.

[1] `http://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/`

1.2 Research Goals

The principal goal of this project is creating a video game that teaches beginners about managing incoming and outgoing traffic at the firewall, loosely based on the specialist tool of *iptables*. The dissertation will discuss different possible learning goals and addresses different angles that might be taken in the concept of the game in two different design phases but provides reasoning why the particular approach of the second design phase was taken.

In particular, the game addresses the following research questions:

1. Is a video game suitable to teach a target group of beginners and novices about firewalls?
2. Has the target group increased their knowledge and learning according to the learning goals identified?
3. Can the target group identify firewall terminology and concepts?

1.3 Paper Structure

The remaining chapters of the paper are organised as follows.

Chapter 2 provides a literature review of games in a computer security context and a literature overview of firewalls and *iptables*. The literature review informs the requirements gathering stage of the project and provides the context in which the project is placed.

Chapter 3 contains a short summary of the methods contained in this dissertation and whether they occur during the Requirements Gathering Phase, the Implementation Phase or during the Evaluation Phase.

Chapter 4 details the requirements gathering that I carried out prior to the first design phase. It includes two expert interviews and a lab study/research workshop description and analysis and summarises desirable features as well as the chosen learning goals.

Chapter 5 describes the initial thoughts and methods that I used for the creation of the first video game iteration. It furthermore provides an evaluation of this first iteration of the game, summarises shortcomings and discusses considerations taken for the second iteration.

Chapter 6 provides a summary and justification for the second iteration of the game, in which I included feedback from users as well as a Game Design interview and Expert Feedback which informed the final design of the game. This design phase constitutes a full design overhaul after shortcomings in Chapter 5 were identified.

Chapter 7 forms the evaluation of the final game and outlines that the game has successfully met the majority of the learning goals. It furthermore provides an evaluation of the usability which found that the game scores highly in terms of usability for all participating users.

Chapter 8 encompasses the conclusion of the dissertation, and draws the findings of the research questions together. Furthermore, it provides an outlook for the future by mentioning which aspects should be improved upon in the future.

Chapter 2

Literature Review

The literature review will introduce some background and related materials on the context of firewalls, the specialist tool of *iptables* and a brief introduction to educational games. It will also contain a overview of two board games and two video games and provide a brief comparison of the two.

2.1 Firewall

According to Cheswick et al. (2003), a firewall can be described as a device, software, arrangement or equipment that limits network access, be it a software layer or a physical box that you buy. While they all share the goal of regulating network traffic and restricting or preventing the communication except those explicitly permitted (Kandogan et al., 2012), there are different ways of achieving this goal. Cheswick et al. (2003) differentiate between packet filtering, circuit gateways and application gateways, each of which reside within a different layer in the TCP/IP protocol stack.

Incoming and outgoing packets are examined according to a specified ruleset or a sequence of rules which ultimately determines whether to accept or discard the packets (Gouda and Liu, 2007). Writing these rules correctly is easier said than done and many problems can potentially occur. With many relating to the rule ordering, verbose and hard to follow rules, and keeping the number of rules to a minimum (Gouda and Liu, 2007; Cheswick et al., 2003). Wool (2004) has also analysed common errors typically encountered when administering firewalls, once more illustrating the difficulties companies and individuals face when setting

up a firewall. These include errors spanning from allowing "any service" inbound and outbound, insecure access such as un-encrypted access to the firewall and using implicit rules with regard to TCP, UDP and ICMP.

A few years later Wool (2010) concludes that the errors cannot be avoided by upgrading or more advanced pieces of software, since many errors occur due to user-specific rules and also highlights that newer software does not help users to write better filtering rules. Even experienced system administrators, in charge of managing a firewall, still experience difficulties or struggle to grasp certain concepts, leading to even greater misunderstandings in a bigger organisational context (Kandogan et al., 2012). Oppenheimer et al. (2003) even suggest that administrator errors are the largest cause of failure for Internet services and that policy errors are the largest category of those errors.

2.1.1 iptables

iptables, the newer version of *ipchains* and being shipped with the Linux kernel, is a free and powerful tool to start administering a firewall which contains stateful packet-filtering (Barrett et al., 2003). It is sometimes suggested that *iptables* are a good introduction to managing your own firewall due to its simplicity. *Iptables* also express firewall restrictions with rules which are categorised into *chains*. There are three system chains: INPUT, OUTPUT and FORWARD, however the user also has the ability to specify his own chains (Andreasson, 2006). The FORWARD chain is used to route packets that are not destined or originated for and from the local host, whereas the input and output chain are related to incoming and outgoing network traffic respectively. Cheswick et al. (2003) describes chains as a construct of rules or a collection of rules that go together logically. The other important element to take into account are the different tables which can be used in *iptables*, mainly *raw*, *nat*, *mangle* and the most commonly known *filter*. The actual filtering of packets is only taking place in the *filter* table, a distinction important to make. *Iptables* are not necessarily the tool of choice to use on an enterprise level but provide an easy enough introduction to the complex world of firewalls.

As the name *iptables* suggests, *iptables* contain tables, which in turn contain chains, which contain rules. Firewall rules are traversed in order when a packet arrives at the firewall in the *filter* table. The packet is matched against the first rule: if it matches the classification of the rule, a target such as ACCEPT, DROP or REJECT determines what happens next. The ability to specify user-defined chains, also enables the user to replace the target by another chain that the user can define in order to traverse further, as can be seen in Figure 2.1. Ordering these rules in a sensible way is of utmost importance and is an error that is encountered by many system administrators.

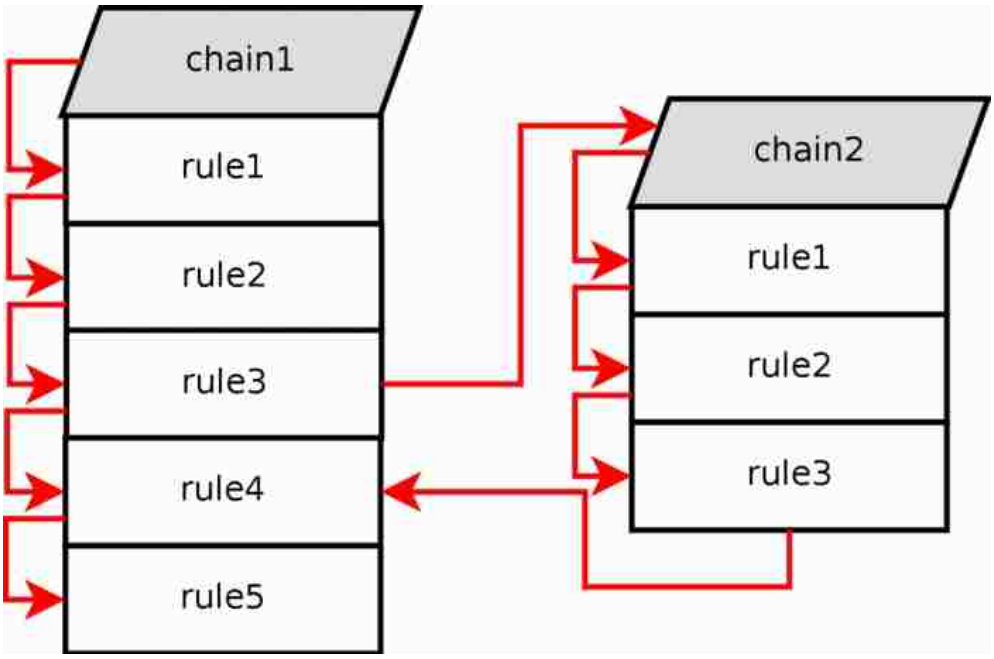


Figure 2.1: Rule traversal with two chains of which at least one is a user-defined chain (taken from Andreasson (2006))

Iptables rule

The below expression is an example of a rule in *iptables*:

```
iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,
ESTABLISHED -j ACCEPT
```

The -A relates to specifying whether the rule is added, inserted or deleted,

where each first letter of the word is specifying the command. Add means that the rule is added at the end of the rule set as opposed to being inserted elsewhere. The capitalised INPUT relates to the chain into which the rule is inserted, whereas -i and -p define the interface and protocol the rule applies to (in this case eth0 and tcp respectively). The –dport 80 describes to the destination port, in this case 80. "State" indicates for which state of a connection the packet should be accepted, which in this case relates to new connections (where the packet is a new packet and not part of a previous connection) and established connections. The target of ACCEPT at the end specifies that packets that match the rule defined above should be accepted. *Iptables* are also case-sensitive, meaning that the words need to be capitalised as indicated. Moreover, forgetting a dash or putting extra space into the command can also lead to complications, which requires special scrutiny from the system administrator.

2.2 Educational Games

The last few years have seen extensive research in the field of educational games, especially since they can teach difficult and hard to grasp topics in an engaging fashion. They have the potential to attract a wide range of audiences and can be used with children, students and adults alike (Druin, 2002; Cone et al., 2007; Olano et al., 2014). Educational games usually offer a certain level of engagement which make it fun to play, but they can also offer the opportunity to capture the players' attention for increased periods of time (Dondlinger, 2007), which offers great potential for difficult topics or topics considered more "boring".

There is some debate to make a distinction between educational games and edutainment games, in which edutainment games present the "skill and drill" repetitive learning of a task whereas educational games are considered to be played by using strategies and testing hypotheses and advanced problem solving (Dondlinger, 2007). However, not all literature agrees on this distinction. Concerning the narrative of an educational game, there have also been different approaches suggested. Fisch (2005) have advocated to place the educational content at the heart of the game play, whereas Monk et al. (2010) suggested "stealth learning" in which the user is not aware that he is learning about a complex topic.

Being able to teach potentially hard to grasp topics, which firewalls can often present (Kandogan et al., 2012), could be a major stepping stone in educating people about the use of firewalls and their inner workings. Few games have attempted to explore firewalls in detail, e.g. games produced by previous master students from the University of Edinburgh, and often centre on users already somewhat proficient with iptables and the command line (Thompson, 2017; Mjartan, 2017).

2.3 Computer Security and Firewall in Games

There are a few games that have attempted to teach computer security terminology and concepts to beginners and experts alike due to their fun and engaging nature. Computer Science and Computer Security can sometimes struggle to attract students and pique interest into the subject at the right point of time. While the curriculum can inform, innovative ways of teaching and retaining knowledge are often preferred by students, and educational games or edutainment games are no exception. For a more extensive list of games that have been created in the wider computing context, refer to Battistella and Wangenheim (2016) who created a systematic review.

The last few years have seen a lot of development of both, board games, such as [d0x3d!] (Gondree and Peterson, 2013), Control-Alt-Hack (Denning et al., 2013), Android: Netrunner, Firewall, Protection Poker (Williams et al., 2010) and Elevation of Privilege (Microsoft, 2013) and video games, such as CyberCIEGE (Cone et al., 2007), SecurityEmpire (Olano et al., 2014) and Anti-Phishing Phil (Sheng et al., 2007) for the wider computer security context. Some of these have been successful in an educational context, with students, teachers and even parents reporting that they enjoy these games. The following provides a closer look at two board games and two video games.

2.3.1 Board games

2.3.1.1 [d0x3d!]

[d0x3d!] is a table-top, open source computer security board game that has been developed by Gondree and Peterson (2013). Players take the role of white hat hackers that need to navigate through the network to reclaim digital assets such

as personal identifiable information or authentication credentials to avoid embarrassment and the data being made public. In order to decrease the competitive notion between male and female players and reduce barrier to entry (Gondree and Peterson, 2013), it is played in a collaborative fashion, meaning that players either succeed together in reclaiming stolen digital assets or lose together by being detected by the adversarial network.

The game is aimed to be played by people having no, or very little experience, with computer security and should be seen as an introduction to the topic of Computer Security or a primer that piques players' interest to find out more. While [d0x3d!] undoubtedly succeeds in introducing new terminology and raising accessibility to the subject, it is not clear that the learning objectives or learning goals beyond this are met. This includes learning concerned with network representation, threat representation and defense representation (Olano et al., 2014), despite Gondree and Peterson (2013) acknowledging that their game cannot describe the digital complexity of a network accurately and exhaustively.

2.3.1.2 Control-Alt-Hack

Similar to [d0x3d!], Control-Alt-Hack constitutes a table-top board game and serves as an introduction to Computer Security as a subject. Created by Denning et al. (2013), it targets people aged 15-30 that have an interest in computer science and engineering but an non-existent or limited background in computer security. Its main learning goal and objective is to raise awareness of computer security as a discipline as well as its challenges and needs by performing a variety of penetration-testing missions (Gondree et al., 2013). The topics concerning computer security in Control-Alt-Hack include: "the creativity of motivated adversaries, the breadth of technologies – particularly embedded and cyberphysical systems – that are impacted by computer security, the different ways successful attacks can impact human assets, and the potential things you can do with computer security skills." (Gondree et al., 2013).

It aims to break down perception errors and stereotypes of the "hacking" profession by showing the white hat hackers, that players pick upon starting the game, as varied as possible and in activities that are not related to computers.

According to the research presented by Denning et al. (2013), these learning objectives are generally met, including engagement between interested parties. Main criticism concerning the game can be summarised as difficult to learn and play, which might hinder players to play it in the first place and Olano et al. (2014) stating that Control-Alt-Hack has a security theme but does not teach security.

2.3.2 Video games

2.3.2.1 CyberCIEGE

CyberCIEGE is a single-player video game in which the players can play through a number of different security scenarios and present people with a resulting simulation of that scenario. It is aimed to increase training and awareness of Information Assurance concepts by engaging players in a "security adventure" (Cone et al., 2007). CyberCIEGE differs to many games in the sense that it is easily extended with new scenarios that can be constructed using their own CyberCIEGE game engine. Some of the topics and concepts covered include: definitions and descriptions, protecting high value information, access control mechanisms, social engineering attack prevention, password management, safeguarding data and physical security mechanisms. The learning goals of the game are not as clearly formulated, apart from raising awareness, but relate to the learning of carrying out practices through a simulation which should resemble a real-life situation, thereby teaching how to effectively combat them if encountered in a real situation. CyberCIEGE is clearly aimed at security professionals, not high school students or people with limited knowledge in computer security, assuming knowledge that cannot be expected of a beginner or a novice (Olano et al., 2014), especially due to its nature of simulating real-life scenarios.

2.3.2.2 SecurityEmpire

As opposed to CyberCIEGE, SecurityEmpire is a multi-player competitive game in which students that use sound security practices gain an advantage in building up a green energy company. The players ultimately compete in building the most successful company and can buy and trade required components. Security practices are not at the centre of the game but are needed as a means to reach the

goal, for example losing money and market share by failing to encrypt auction bids and gaining an advantage by doing so. Failure by not following good security practices is followed by help and advice on how errors could have been prevented.

Olano et al. (2014) describe their main aim as teaching high school students to "stop and think before executing computer commands and to develop awareness of selected fundamental concepts in Information Assurance", while not requiring a high degree of knowledge in the domain space as is the case with CyberCIEGE (Cone et al., 2007). Evaluations and feedback from students and teachers was positive, describing it as "engaging and immersive", however apart from the evaluations that were being ran by the researchers themselves, SecurityEmpire does not seem to be as prevalent as games like [d0x3d!] and Control-Alt-Hack and thus there is not as much of an array of information considering its potential and learning goals.

2.3.3 Comparison of Video Games and Board Games

While board and card games are often said to spark conversation and offer a collaborative way of learning, video games also offer significant benefits to the players as outlined by Dondlinger (2007) and De Aguilera and Mendiz (2003). The latter describe the cognitive importance of video games and relate this success to the development of skills like: attention, spatial concentration, problem-solving, decision-making, collaborative work, creativity and ICT skills. While not every video game will address each of these in equal measure, the benefits of using video games in educational contexts is apparent. Dondlinger (2007) also stresses the importance of video games in the 21st century, which has grown used to technology and use it on a daily basis, therefore stressing the need for those skills mentioned in De Aguilera and Mendiz (2003). Children and young adults today are digital natives and skilled at using a variety of computing technologies Prensky (2003), which strengthens the case for video games.

As firewalls and computer security are closely tied to using technology and computers, it seems a natural choice to be able to explore them in a video game setting. While the collaboration element of card and board games can spark conversation, video games offer the opportunity to delve into a new world on

your own and in your own time. It also reduces the fear of finding oneself in a group of mixed experience individuals in which the expert dominates the game. Especially since computer security and especially firewalls are considered a difficult topic even by experts (Kandogan et al., 2012), a video game for a single player will increase their knowledge and build it up to a level in which they can compete with more experienced individuals in a board game or card game setting.

Chapter 3

Methodology Overview

The project methodology comprises roughly 3 main phases: The Requirements Gathering phase, the Implementation Phase and the Evaluation Phase. The project overall follows an Agile approach, adding documentation and results to the final report as soon as they were ready. During the development process, I followed an iterative development approach (Larman and Basili, 2003), meaning that the video game was continually revised using the feedback and research from design approaches and evaluations. The section below outlines the different methods that are used within the different phases.

3.1 Requirements Gathering Phase

This phase relied on the previously conducted literature on educational games and common firewall errors, which form the basis of the initial ideas that are being discussed in the requirements gathering phase. Literature reviews can form a "critical step in laying the foundations and contextualising the design enquiry" as pointed out by Hanington and Martin (2012) and will also inform the design in the first design phase. Assumptions in the literature such as common firewall errors and interactions, as well as assumptions about the simple game setting, I will not question further.

During the requirements gathering phase, I conducted two "Expert interviews" with a Firewall Administrator and a Network Engineer, as I deemed their opinions and information crucial to the requirements gathering phase and defining the resulting learning goals on which the game was based. The method of

using "expert interviews" (Littig, 2013) to inform the build and design provided give deep insights and identified tacit misinformed assumptions if present.

The other research method I used during the requirements gathering phase was a research workshop/lab study with people of varying backgrounds in which a common security board game was played. This included Pre-/Post tests to assess whether the learning of the students increased following the game and included their perceptions before and after (Vaniea, 2016). Participants filled out a short questionnaire in which questions were tailored to reflect the pre and post nature of the questions. Following the research workshop, a short focus group was conducted to ask for more detailed opinions. Focus groups are usually conducted at the planning and scoping stage, which made them a good fit for the requirements gathering stage (Hanington and Martin, 2012).

3.2 Implementation Phase

The implementation phase encompassed the design, build and adaption of the video game. Methods used included the Agile methodology for iterative development of the video game (Larman and Basili, 2003). Resources used to build the game included the well-known game engine Unity (Unity Technologies, 2017) to facilitate the development. I also conducted another expert interview between the first and second design phase to understand best practices towards game design.

3.3 Evaluation Phase

The evaluation phase formed the last part of the project and identified whether the learning goals defined in the requirements gathering phase were met successfully. These informed the choice of the dependent variables for the evaluation. The method chosen to test these was a Pre/Post-test that assessed the knowledge of the subjects before completing the educational video game and after (Vaniea, 2016). The project was deemed successful, if most of the learning objectives have been met and increased the participant's knowledge of firewalls and *iptables*. If the knowledge of firewalls decreased, the project will not have met its learning objectives and explicit description and discussion of these reasons will be needed.

Chapter 4

Requirements Gathering

In order to define the learning goals and audience for the game to be created, I planned and conducted exploratory expert interview sessions and a research workshop. These expert interviews and the research workshop with people of varying backgrounds acted as a first source of information to ensure that plenty of data was gathered. The expert interviews were scheduled in the very beginning of the project to discuss initial thoughts and ideas, followed closely by the research workshop. These two key actions took place before the actual project start date as to inform the development as much as possible in advance.

4.1 Interviews with Experts

To gather information on how system administrators operate and manage a firewall, I decided to run two expert interviews. Interviewee A has 20 years of experience in networking, currently completing his PhD and is working on the university teaching space and ISP "hubs" in his free time. Interviewee B has 3 years of experience and is working on "hubs" full-time. Both of them use the same ISP which uses the firewall tool *ipfw* and the automation engine *Ansible*. I conducted these interviews at the very beginning of the project to inform my game design as much as possible by expert opinion.

The interviews were setup to be semi-structured as to allow for the interviewees to explain and talk as much as possible and to allow for personal reflection. The interviews were audio recorded after the interviewees gave their consent.

4.1.1 Aims

The aims of the expert interviews was to gain initial information on the difficulty of the subject of firewall administration and common errors they encounter during the process of firewall administration. I also asked the experts to provide some feedback on initial ideas for the gameplay and what they deem critical to include.

4.1.2 Method

Criteria for Inclusion

Both experts were selected because of their expertise in the field of Firewall Administration and their frequent exposure to it.

Materials

Before the interview, I prepared a semi-structured interview script to aid the interview process and to provide a loose structure for the experts to follow. The script that I used and prepared during the interview can be found in Appendix B.

In order to focus fully on the expert and his explanations and thoughts, I used a recording device because it is a specialist type of equipment that can capture high quality audio, and because it would also cater for the experts that might have strong security concerns and would prefer not to be recorded via mobile phone. Using the recording device allowed me to focus fully on the expert and make him feel comfortable and at ease.

Procedure

After Dr Kami Vaniea had established the first contact, I met the experts in an informal environment to find a suitable time and place to conduct the interviews. Further communication before the interviews took place via email. The experts were told that interviews would take around 30 - 45 minutes and that the interviews would be recorded. On the day of the interview, I handed the experts a consent form that reminded them that their audio will be recorded and that quotes may be used by me in my thesis. Once the experts agreed to the recording,

I asked them to provide some initial information about themselves before I officially started the semi-structured interview, with plenty of room for the experts to elaborate on their thoughts and ideas.

4.1.3 Interview A with Network Engineer

Area of Expertise

Interviewee A described himself as "not a specialist in firewalls" but explained that he has done network engineering for the last 20 years. He has worked for a variety of organisations: universities, international organisations and smaller scale organisations. He is currently completing his PhD at the University of Edinburgh and is working on a university-owned teaching space called "hubs", an ISP, in his free time, which manages a firewall using a commonly known tool ipfw and the automation engine Ansible.

Outcomes

I met Interviewee A in an informal environment in his chosen work space to make him feel comfortable and at ease while being interviewed. He consented to the audio recording and also volunteered to assist at a later stage if needed.

Interviewee A could not describe a typical day for him as the tasks vary too much. He broadly categorised three kind of tasks that he encounters during his line of work

1. Regular care and feeding of the network: maintenance
2. Future Developments for the network: extending
3. Reacting to problems that occur unexpectedly

His day often consists of all three tasks, even though he himself and the other people working on the ISP try to minimise Task 3 as much as possible he explained. He also described maintenance and reactive changes as necessary to effectively deal with the second category of tasks, namely the extension and adding of new parts for the network. He described the second task as the most

creative which he enjoyed the most.

In the following, Interviewee A was asked to remember the last time that he edited a firewall rule. However, he did not give a specific example but provided more of an overview of how a firewall should work and how the ISP "hubs" operates. He explained that firewalls and the decision of where packets should go resembles a decision tree and mentioned that this can grow in complexity rather quickly. This growing complexity provided his rationale for automation of configuration of devices, thereby adding some degree of being repeatable. "Hubs" has chosen to use *Ansible* as a Python tool to achieve the concept of many different hosts having both the same and different rules. Moreover, it can use templates to generate rules. Interviewee A mentions that this automation is a "far better way of doing this" and that he "cannot even reliably remember the syntax", showing how powerful *Ansible* is.

When I prompted him to remember a time where he experienced difficulty editing a firewall rule, he explained the problem system administrators face more generally: working remotely and then locking themselves out, ultimately leading to the situation that someone local has to fix the problem onsite. He highlighted that this happened to him on a few occasions but that unfortunately mistakes happen. After this, he classified three different types of errors that can usually be encountered:

1. Conceptual error: You think you know what your model does, but you really do not
2. Threat model error: Not having the correct threat model
3. Typos and ordering errors

He explained that while the typo and ordering errors do happen and are equally important, that they are not as interesting and largely taken care of by the tool *Ansible* and its automation.

The conceptual and threat model mistakes are harder to detect for yourself and require more thinking. Conceptual errors can arise by not being clear on exactly how your system performs, e.g allowing no inbound traffic but allowing

outward connections by reverse telnet and exploiting this to establish a connection, Interviewee A explains. Threat model errors on the other hand, arise due to not being clear about the threat level a network that you connect to poses, and the danger it poses for your device. Careful thinking whether a network can be trusted should be established in order to avoid these errors. Conceptual and threat model errors are harder to "automate" away as Interviewee A stresses and therefore the level of education on these two errors should increase.

Being asked about the most valuable aspects that need taught, Interviewee A highlighted that concepts rather than tools should be educated. He furthermore explained that the most important thing to understand in his opinion would be the concept of chains and different levels in the firewall, starting with the levels of classification and actions. This classification of where the packet is originating from, makes it possible to classify it as a "friend", thereby performing one action, or classify it as "not a friend", thereby performing another action. Classifying in the first instance allows the firewall rules to be easily repeated instead of having to specify new rules for each and every new origin as Interviewee A explains in great detail.

Interviewee A generally thought that creating a video game sounded like a good idea to engage the the player and teach complex topics. He agreed that a story could be a beneficial concept for the video game as they allow you to relate the concepts in an understandable situation. He furthermore added that knowing how to troubleshoot would be an important skill as well as levelling the errors and tasks by difficulty, starting with reactive tasks before going on to future development.

4.1.4 Interview B with Firewall Administrator

Area of Expertise

Interviewee B has been working at the ISP teaching space "hubs" for the last 10 months, but he explained that he has unofficially contributed to it for the last 2-3 years. He is working on the teaching space "hubs" full-time, with 4 others who are working on it voluntarily. They use the firewall tool *ipfw*, the automation engine *Ansible* and github for collaboration. Interviewee B was chosen to be interviewed

as Interviewee A recommended to talk to him and since he is working specifically on firewalls.

Outcomes

When I asked Interviewee B to illustrate a typical day for a firewall administrator, he was quick to explain that there is not really a typical day. He explained that he is not constantly working, and can freely alternate between free-time and working on the ISP as he sees fit, as long as the hours add up. He called this an "advantage" as he can do the work when he wants to. But he also mentioned that it might mean that he has to be up at 3 am to fix something important, because 3 am is a time where most people are usually asleep, not disrupting service for the user. He jokingly called a firewall a "hell-hole" and laughed, illustrating that it does not always work as expected for him and sometimes presents difficulties. He added that he is of the opinion that a firewall is not really needed for really small networks.

Concerning the tools and workflow, he explained that he uses *Ansible* to edit a rule and edit in a line. A makefile then does checking and does sanity checks with one command. In order to collaborate between the administrators and contributors, they use git to see what other people have done and edited as you can raise issues and comment on your changes. Interviewee B also explained that using git and github for firewalls is not an isolated case related to their ISP, but that even many larger companies use it to manage the collaboration and that their firewall is completely automated. However, "hubs" is not that automated, and Interviewee B and the other administrators commit to the master branch and check and run things to be applied by hand. Commits are done before running them as to not overwrite and accidentally change settings.

Interviewee B stressed that he does not really encounter problems with editing rules, due to the fact that *Ansible* is taking good care of the firewall and translation of rules. He mentioned that the source of problems is usually the actual setup of the ISP, *ipfw* and the workflow. He further explained that all the configs are in yaml files, which *Ansible* is able to reads and then converts them to the right commands before running them on the server.

Moreover, he mentioned that he does not really talk to other people about firewalls in his free time, but highlighted that the teaching space "hubs" itself is a teaching tool. According to him, it was made for 2 reasons. 1) to provide a generic system for everyone to get internet and organise it effectively. 2) being based at university - which means that it can be used for teaching. He added that it is not restricted to the University of Edinburgh though, as sometimes other universities such as Edinburgh Napier come in as well to receive teaching, which happened twice in last 10 months.

When asking Interviewee B about common errors he encounters, he said that the biggest source of error is probably the ordering of the rules. He was of the opinion that the basics of the firewall rules are easily understood but that the ordering is an aspect that requires special scrutiny. He told me "I can tell you that you go home and try out the ordering and you will get it wrong", illustrating that he felt strongly about this source of error and that beginners often make these types of mistakes.

In the following, I asked Interviewee B about potential scenarios that could be included in a game-setting. He painted the following scenario: "[I would be] setting up a webserver, two different ports for that, ssh port only allowed by these users, web for everyone, in the end, deny all", which would allow for day-to-day scenarios and allow to learn about management machines. He deemed interaction with other people or administrators to be out of scope for a video game and explained that interaction between players would appear anyway as they are helping each other to solve tasks. Interviewee B liked the idea of a small story to be included in the game, but would not include anything too complex.

In the end, he gave more reasoning on *ipfw* and the similarity to other tools. He said that *ipfw* was not his tool of choice but that it was just the tool that was available when he joined. As it worked, and did so on 30 machines, he explained that it was faster for him to learn how to use *ipfw* than setting something new up from scratch. However, he also added that once you know one tool, it is just the syntax being different and that he found it easy to transition, knowing just the basics of *iptables*. In his final remarks, he added that it is down to me to decide if a UI or Terminal works best to teach concepts and that it would effectively

depend on the learning goals and objectives of the game.

4.2 The Lab Study/ Research Workshop

4.2.1 Aims

In order to inform the design of the video game I am creating, I ran a research workshop during the requirements gathering phase to gain opinions and understand experiences of the research participants with relation to computer security. The session was centered around the board game [d0x3d!] which is aimed at beginners and looks to teach some basic vocabulary in an informal and fun setting. By extracting the participants' negative and positive experiences and attitudes from the board game session, I could derive findings that in turn inform the creation of the video game.

4.2.2 Method

Participants

The participants of the study all had different backgrounds ranging from no experience with networking and security to very experienced as was indicated by the Pre-Test. Participant A has 20 years of experience with networking, security and managing firewalls, participant B has a year of experience and participant C no experience in networking and security but several years of experience in Human-Computer Interaction. This group of participants thus presents a diverse group of participants with varying degrees of knowledge that all experienced the board game together.

Setting

The research workshop was carried out in the Mini Forum in the Informatics Forum of the University of Edinburgh. This room enabled small groups of people to sit around low tables which facilitated the playing of the board game as each participant could reach for the board easily and everyone could see each other with ease.

Materials

Documents

First, I asked the participants to fill out a consent form and then to fill out a pre-game questionnaire that looked at their current experience and knowledge of networking and security and more specifically firewalls. The participants were also supplied with a 1-page instructions document that summarised the more lengthy instructions that were originally included in the board game that I found too hard to start with. After gameplay, I asked the participants to fill out a post-game questionnaire again. I also brought a document with that outlined the session with me as well as a document that summarised questions for the focus group that followed the gameplay. All of the documents can be found in Appendix B.

Board game

I brought the original board game [d0x3d!] instead of a printed version to the research workshop as it included a game board made up of individual tiles, several pawns, loot and patch cards, asset tokens, role cards, and a token for the security level board and did not require any other preparation.

Procedure

First of all, the participants were handed the the consent form to fill out. After each participant agreed, I turned on the video camera to capture the board game and the players' interaction with the game and each other. The camera also captured audio to include the conversations of the participants, as well as their emotions and attitudes.

The participants were then asked to fill out the pre-game questionnaire that assessed their current knowledge concerning Computer Security, Computer Networking and firewalls. Instructions and explanations concerning the rules and the gameplay were given ahead of the actual play as to reduce confusion and make the participants feel at ease. I also instructed them that they can leave the study at any point of time without giving reasons and reminded them that they could ask questions. While the participants filled out the pre-game questionnaire and read the game instructions, I assembled the tiles in a setup that was not random

but resembled a network topology, to understand whether participants take away learning from a chosen setup as opposed to a random setup.

The three participants including myself played the game for roughly 30 - 35 minutes, before the game ended naturally as no further moves could be made. The participants were then asked to fill out a post-game questionnaire which contained the same questions as the pre-game test and looked to assess whether participants would answer differently after playing the game. After completing this, I asked the participants to share their experiences in an informal focus group setting.

4.2.3 Results

The participants all grasped the gameplay, rules and aims of the game quickly, including participant C that had no experience in networking or security. Despite the new vocabulary that the game introduced such as “compromising”, “zero-day exploit”, “patch” and “loot”, participant C seemed very engaged and asked the other more experienced players for input and collaborated effectively. Participant B was a little more quiet but grasped the rules really well and explained them to the other two players if necessary. He seemed very focused on understanding each element of the game. Participant A on the other hand felt more strongly about the actual learning objective and learning points. On more than one occasion, he said that one is just “chasing around for a picture”, not really teaching the players about the picture and term itself.

Normally, if [d0x3ed!] was played according to instructions, the layout of the “network” tiles/nodes would be entirely random. However, in order to increase the learning goal, it was decided to at least provide a semi-structured network topology that would provide certain teaching goals, of which a slight variation is provided below.

Participant A however, still did not think that the current setup provided enough structure and was particularly not happy about the “soup in the middle” meaning that with his expertise in the field he would have rearranged the network tiles differently. In general, participant A did not fully agree with some of the

Figure 4.1: A very similar topology to the one that was used during the gameplay of [d0x3d!]

learning goals and also mentioned that he does not agree with the concept of intellectual property and that it is a harmful concept to teach that you can "own ideas".

In the following, the research participants all expressed their opinions concerning the game in a Focus Group setting, with the group dynamic enabling a setting in which every member could feel comfortable to contribute. All participants agreed that they did not learn a lot from playing [d0x3d!] apart from new terminology which is in line with the findings of Olano et al. (2014). Participant B expressed that you do not need to think about the context at all in order to play it and participant A added that even his 8-year old son could play the game, despite the game being advertised for ages 12 and upwards. None of the

participants felt that a completely random setup of tiles in the network would be sensible and all agreed that there should be a certain network that resembles reality. They all agreed that the element of randomness would still hold because of the loot and patch cards that are randomly drawn.

4.3 Discussion

Having conducted the requirements gathering phase by conducting expert interviews and a research workshop, I compiled a list of desirable features and goals which resulted from negative as well as positive experiences in gameplay. This list of features does not outline that all these features will be provided or met by my created video game, this list merely presents all features that might be worth exploring further and will also relate to further work that can extend beyond my project. This list includes many of the features that research participants and interviewees mentioned. Planning and choosing between these ideas is necessary to formulate the resulting learning goals which will be pursued in the video game and will be discussed in the next section.

4.3.1 Desirable features

- Explaining the firewall and teaching the vocabulary instead of introducing the terms without explanation
- Educating on concepts rather than focusing on tools: chains, classification, actions
- Teaching the different tasks a system administrator might face (Maintenance, future development and reactive tasks)
- Allowing for some exploration of terms of concepts and problem solving
- Teaching how to create a ruleset
- Developing active exposure to the firewall and security rather than just learning about it in an abstract sense
- Teaching you about the different type of errors (conceptual, threat model, typos/ordering)

- Including Some aspect of a storyline or backstory as to why learning about firewalls is important
- Developing an automation tool that can translate firewall rules for realistic setup
- Constructing a powerful engine that can understand user's written input
- Introducing Some aspect of repeatability or randomness in the game
- Including a mode for collaborative gameplay
- Allowing for an Attacker/Defender dynamic
- Differentiating between ISP and Enterprise networks
- Teaching how to troubleshoot and find the source of an error
- Allowing for a high degree of freedom and different outcomes
- Educating about different stakeholders and roles

This list of desirable features contains too many features that could possibly be explored in a single game. Moreover, some of the features might even run into conflict as the areas you might want to explore as a beginner differ greatly from those of an expert. Keeping in mind the different target audiences I spoke to, the recommendations by the network administrators and my own strengths and knowledge, I compiled a list of learning goals that my game will try and achieve.

4.3.2 Learning goals for the video game

- Providing structure and explanations of terms and the firewall itself instead of only introducing them
- Educating on concepts like chains, classification and actions
- Allowing a beginner to explore and solve problems rather than being scared to make mistakes
- Creating a friendly environment for learning without fear to make mistakes
- Attempting to teach the logic of creating a rule set to a beginner

- Teaching about some of the different types of errors: conceptual, ordering and threats rather than typos

These learning goals and the game tied to it are aimed primarily at people who are new to computer security and firewalls as a subject and should cater as an introduction to the subject of firewalls and security rather than teach best practice in the industry. There is a wealth of resources available for interested parties to engage in more intermediate or advanced tutorials such as from Du (n.d.) which require to setup virtual machines and might not work if the exact setup is chosen. This presents challenges for someone less experienced or less confident, and leads to them abandoning the task before they can be successful and learn. This is especially true if scripts and setups from tutorials no longer work after upgrading systems, leaving the beginner struggling and without a chance to learn. Focusing on the above learning goals will provide more general awareness about the topic of firewalls for beginners and why it is important to be mindful and not ignore security on their own chosen operating system. It might also prompt interested beginners to go further and learn more about firewalls beyond the created games, especially since the first encounter with firewalls was a more positive and less scary experience as opposed to presenting challenges to them beyond their reach.

The justifications for choosing the above learning goals are manyfold. The research workshop enabled players to identify terms with relation to firewalls in the board game [d0x3d!] but uncovered that the game fell short of properly explaining them, which was furthermore underlined by Olano et al. (2014). The concepts themselves and how these work in particular are not offered by [d0x3d!] which provides the reasoning for creating a game that includes explanations and structure of the gradual explanations of the terms rather than simply introducing them. A friendly environment with room to make mistakes, similar to Anti-Phishing Phil (Sheng et al., 2007) which focused on malicious URL identification, should encourage beginners to explore. In a similar fashion, beginners should be able to interact with the objects in my game, in an environment in which mistakes can happen without any grave consequences.

Interviewee B, who works with firewalls on a daily basis, regards ordering to be a topic that requires special scrutiny rather than focusing on typos. Interviewee A

also shared the opinion that typos should not be dealt with in great detail. While they do happen, they are not as important as other errors, as pointed out by both Interviewee A and B. This also strengthens the case for creating a game that lets the user interact with the firewall in a Graphical User Interface (GUI) as no typing is involved. Moreover, since the learning goals relate to beginners learning about firewalls and how to create a ruleset, a GUI might be more intuitive, which was also suggested by Interviewee B who remarked that the choice of Terminal or GUI will relate to my learning goals. Interaction with other people as well as a multi-layered story were deemed too complex by Interviewee B, which provides the reasoning for not including either in the game.

Chapter 5

First Design phase

The first design phase contains an overview of the first build of the created game and presents an evaluation of this iteration of the game. It also features a discussion of learning points for the participants and identifies shortcomings that are addressed in the second design phase.

5.1 First build

Using the defined learning goals, I put together the first version of the game that could be played by participants and to test whether I can successfully teach those learning goals to a complete beginner and a computer science student with a limited background in computer security.

5.1.1 Chosen Platform

I conducted a lot of research which Game Development Engine to use for the build of my game, especially since I had not worked with any of them before. In the end I settled on using Unity (Unity Technologies, 2017) because it offers a lot of documentation and support and allows for complex game dynamics if desired. After working through many materials such as the book by Tristem and Geig (2015) and also given the limited time of the project, I chose to focus on making a 2D game. The extensive possibility to write C# scripts for behaviour of the game components allowed me to customise the elements to my wishes. Moreover, Unity offers the possibility to build the games for Windows, Mac and Ubuntu Linux as well as a WebGL application that can be run through a HTML file, which will allow for a slightly more convenient distribution of the material.

5.1.2 Game Mechanic

The first iteration of the game was loosely based on the game "Lemmings" [1] which enjoyed popularity in the early 90's. Packets would symbolize the Lemmings travelling from one computer to the next. The game focused solely on packets travelling from top to bottom and mostly ignored anything travelling left or right in the early levels that were created, see Figure 5.1. Players could place building blocks in the path of the packets to alter the path, with blocks turning green and letting packets through and other building blocks that stayed white and blocked them from passing through.

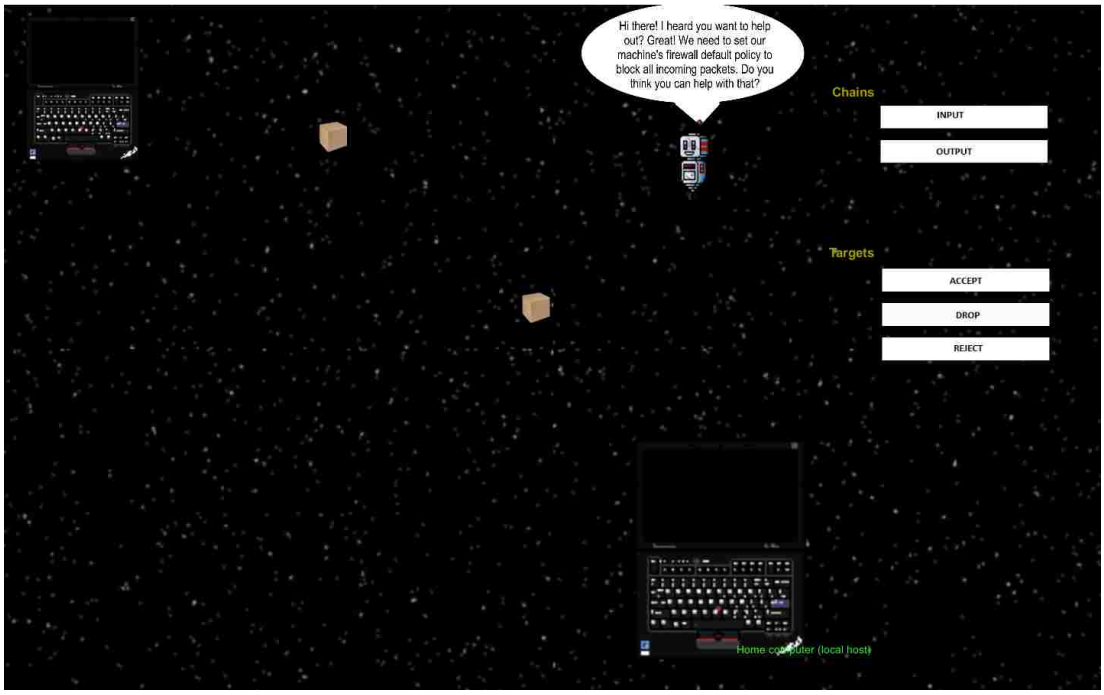


Figure 5.1: Screenshot of the first level illustrating packets travelling from top to bottom and the given instructions

The building blocks resembled the different commands and elements of a firewall rule in *iptables*. The length was shortened for ports and associated numbers, whereas commands as ACCEPT and DROP as well as Chains had a longer building block. I intended for the blocks to be placed in order, with the DROP and ACCEPT command at the end either allowing to pass or blocking the packets or lemmings to enter the computer as can be seen in Figure 5.2.

[1] available at `http://www.elizium.nu/scripts/lemmings/`

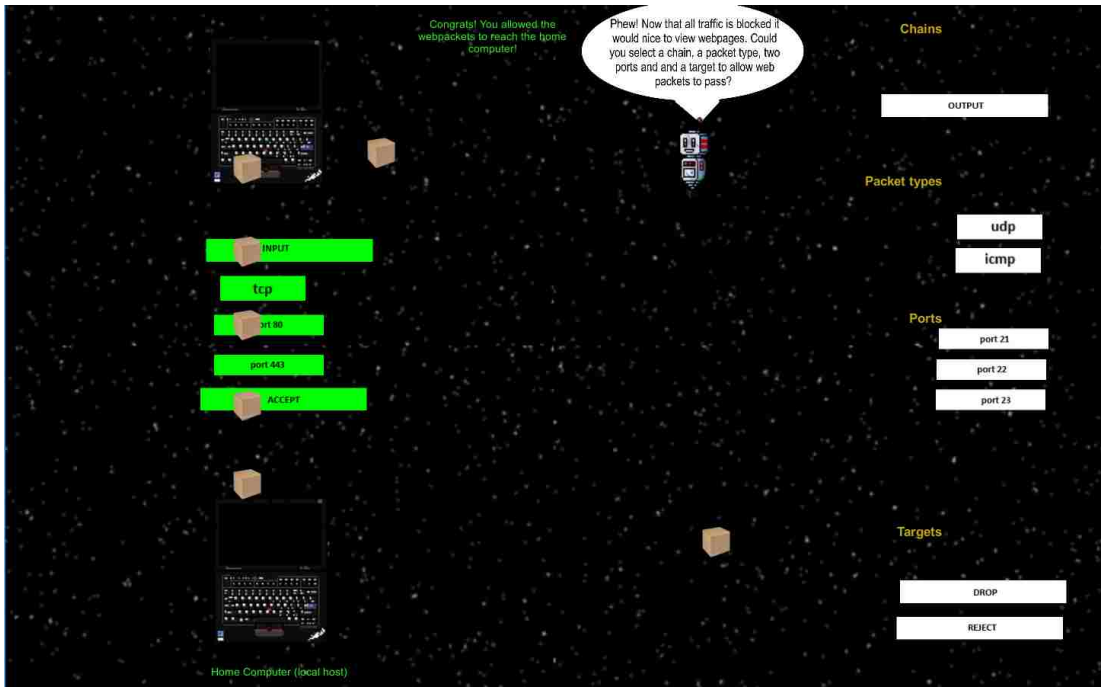


Figure 5.2: Screenshot of the second level showing the green building blocks for correct input, building block length and win message at the top

Four initial levels were created which got slightly harder in difficulty once you progressed through a level. The game could be controlled using the mouse in a "drag and drop" style, supporting the Interaction types of manipulating (Rogers et al., 2011), which allowed the players to drag and drop the elements anywhere on the screen. I had intended them to be placed in the line of path between the computers, however the game was not refined to enable this at this stage. Points for winning and losing points for not achieving the desired outcome were not included. Similarly, a clock or time count was not included. Feedback to the user was given only by messages that were either symbolizing "You won!" or "You lose!" and a short explanation as to why. No tutorial was given ahead of the game, as it was intended to be self-explanatory.

Certain wrong behaviour that the game exhibited, was not corrected before showing it to the participants. This was mostly due to difficulty to attaching different behaviours to all the different game objects, e.g only allowing a user to pick one of each instead of dragging all items around as you see fit. This behaviour, which was not corrected ahead of the evaluation, is shown in Figure 5.3.

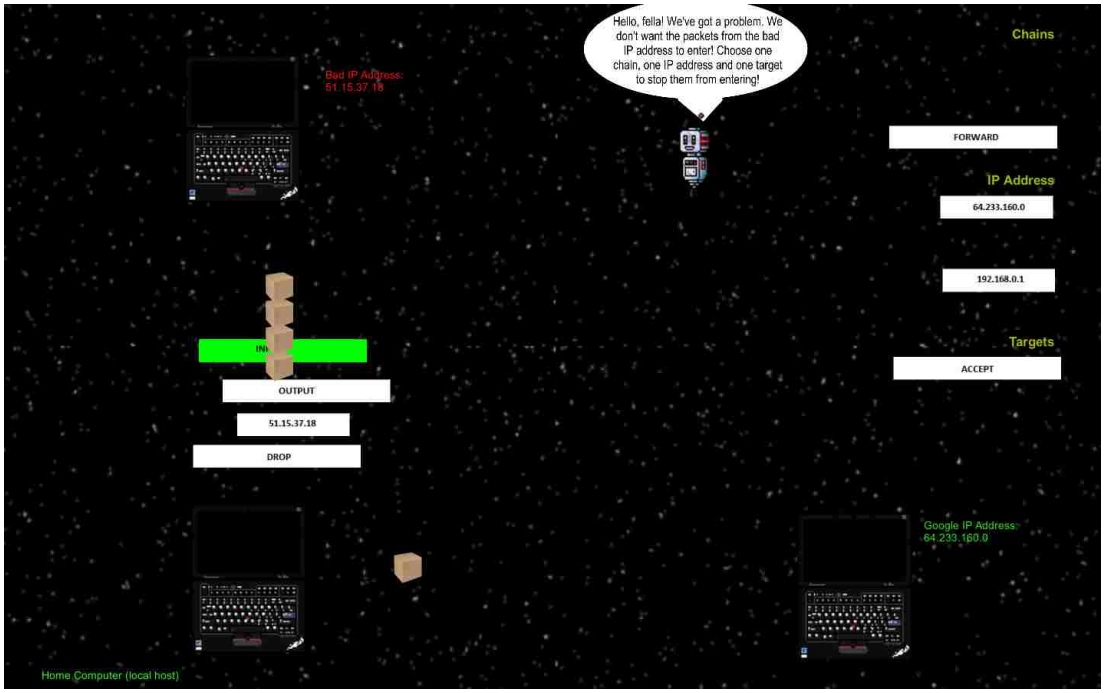


Figure 5.3: Screenshot of the third level showing unintended behaviour which the game permitted (placing Output under Input)

5.2 Evaluation session & Focus Group

5.2.1 Aims

In order to test the initial game that I put together, a workshop session was run to enable two students to play the game and give feedback. A pre-/post test, was once again used to compare the learning and knowledge acquired by the participants without having played the game (pre-test) and after playing the game (post-test). The same method as in the lab study was used as to compare if the knowledge of the participants increased after playing the game. A short discussion was also led to enable the participants to share all of their experiences and opinions.

5.2.2 Method

5.2.2.1 Participants

The participants chosen were a complete beginner, inexperienced with computer networking and security (participant A) and a Computer Science MSc student who has taken classes in Networking and Security but still describes herself as a novice (participant B). They therefore fit well with the intended target group and the associated learning goals. Both of them agree that they are reasonably confident in using the computer and the internet.

5.2.2.2 Setting

I chose to conduct the evaluation in Room 2.33 in the Informatics Forum at the University of Edinburgh as it was big enough to accommodate the participants and since plenty of light enabled the participants to look at the computer screens.

5.2.2.3 Materials

Two kinds of materials were given out

Documents

I handed the participants first of all, a consent form to agree to audio and video recording. Afterwards, I gave them a pre-game questionnaire which I asked them to fill out. After the gameplay, they were handed a post-game questionnaire that was very similar to the pre-game questionnaire, with the wording slightly adapted to fit the post-play nature. Finally, I showed them a wireframe of a game screen during the Focus Group and asked them for further feedback. All of the documents can be found in Appendix C.

Video game

I provided the first basic iteration of the video game to the participants on a flash drive, USB device, so they could drag the corresponding files onto their own computers. They were given 4 independent levels to play through that were not linked at this stage, which were only playable in the Windows Operating system.

5.2.2.4 Procedure

The participants were asked a week in advance whether they would be willing to attend a first session to evaluate the first iteration of the video game and that the session would last roughly an hour. During the session, I presented them with the consent form which asked them whether they agreed to audio and video recordings, which both of them did. The video camera was then turned on and captured the back of their heads, their hands and their computer screen to capture how they interact with the video game. I handed out a pre-game questionnaire to the participants to fill out before the actual gameplay to assess their experience, knowledge of computer security, networking and firewalls and opinions concerning some game elements such as rectangular boxes, packets and a little robot character. After completion, they were asked to interact with the video game as they see fit and explore the elements. Following the gameplay, I again handed out a post-game questionnaire and asked them to complete it. In the last instance of the session, I asked the participants a few questions concerning their opinions and experiences of the gameplay and also presented them with another planned screen for the game and asked whether they would include it or not.

5.3 Results

5.3.1 Pre-game questionnaire

In the Pre-Test, I confronted the participants with a screenshot of an interface of one level of the game to show the different game elements. The questions centered on finding out whether the participants knew what the game elements presented, whether they liked the look and feel of the elements, if any of the terms on the screen were familiar to them and any other general comments. Participant A's responses indicated that none of the words on the screen seemed familiar to him, which he openly admitted. While he was aware that the game should center around firewalls, it did not seem clear to him what a packet is, that these data packets travel to his machine. Instead he mentioned that the robot on the interface controls the firewall, which was not intended.

Participant B grasped that the data packet sprite is indicating packets of

data and shows the transmission of data from one network to another, as she has written in her questionnaire. When being prompted what the rectangles signify, she mentioned layers, not realising that they are related in any way to a firewall rule. She could point out and correctly identify protocols and port numbers but seemed a little unclear on the terminology of chains and targets. She understood that the robot was giving her instructions on what to do and liked its appearance. At this stage, without even having played the game, she mentioned that space is not utilised efficiently ("lots of empty space in the middle") and also found the background to be quite dark, especially with regard to the computer icons which were also quite dark which can be seen in Figure 5.1.

5.3.2 Game Testing

In the following, the participants were invited to playtest the game and try it out. I encouraged them to speak up if they didn't understand anything and to make comments if they wanted to. The participants went closer to the screen, it appeared that they found it hard to read the text or didn't read it at all because it was too small and since the game was already ongoing. Moreover, the instructions of the first level which were the following:

```
Hi there! I heard you want to help out? Great! We need to set
our machine's firewall default policy to block all incoming packets.
Do you think you can help with that?
```

did not tell them enough to understand the objective of the game. The participants wildly selected multiple boxes, changed the path of the packets and used the game elements in undesirable and unexpected ways, especially in the first level.

In the second level, the behaviour of the two participants differed. Participant A did not read the instructions and still dragged many objects around the screen. Participant B however, followed the instructions and dragged them into the intended game area, as can be seen in Figure 5.4.

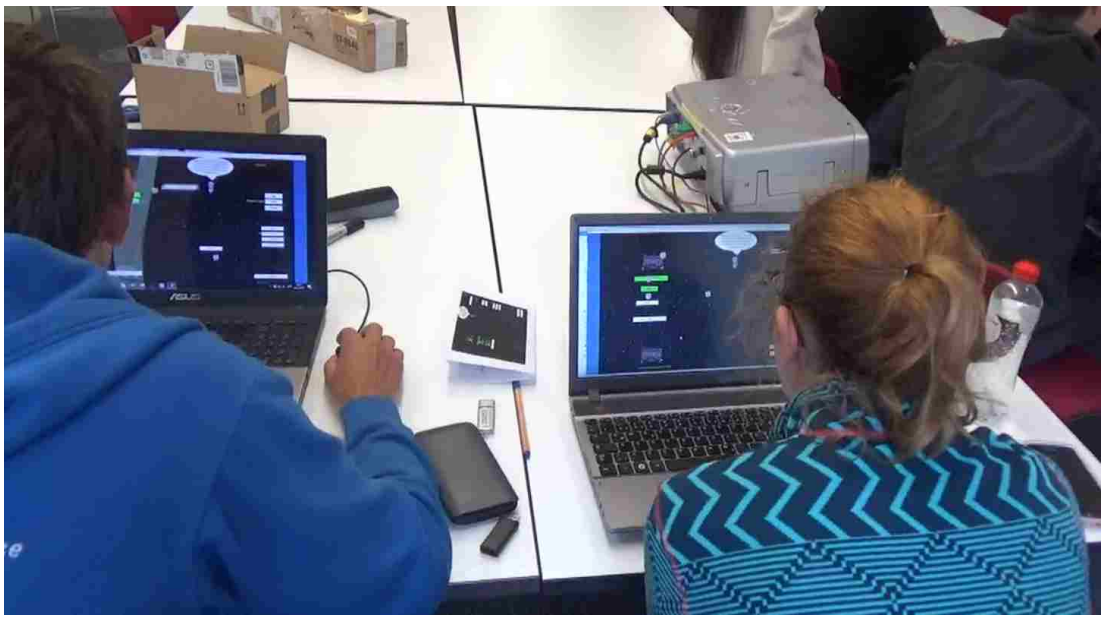


Figure 5.4: Participant A and B using the game in different ways (Level 2)

Participant B explained to participant A that here it helped that "she studied computer science", meaning that she knows what "tcp" and "ports" mean, despite her lack of knowledge when it comes to firewall rules. She seemed to be able to put a firewall rule together according to the structure, without fully realising that she did. Participant A on the other hand, dragged every object on the screen around that he could, putting the elements in random positions and without paying much attention to the rules. Despite the self-described minimal knowledge in networking and security, participant B's interaction with the second level was much better, she seemed to understand what she was supposed to do as opposed to participant A whose lack of knowledge seemed to affect his behaviour. Figure 5.5 illustrates participant A's behaviour and shows clearly how it differs from participant B as he accumulated all game elements in one spot without trying to accomplish the game objective.

In the third level, where the participants had to block a certain IP address, it appeared that both participants did not read the correct IP address but instead found it through trial and error and just saw what worked. Despite the malicious IP address being indicated next to a computer, the visual cue was not enough to make them associate it with one of the game element's white rectangles. Again, participant B managed to select the right chain and target box as can be seen in Figure 5.6. But she admitted that she only chose the correct IP address by

Figure 5.5: Participant A interacting with the game screen

accident, which illustrates a shortcoming in the game design so far. Participant B's statement of "Now I get it" which should express her sudden understanding only appeared much later in the game testing when she talked to participant A. The fourth level was very similar to level 2, where one has to allow access for a certain port, and both participants exhibited similar behaviour in this level as they did in the second level, with the difference that participant A managed to build a correct firewall rule in the end.

5.3.3 Post-game questionnaire

The post-game questionnaire was used as to assess whether the participants learned from playing the video game and if they managed to learn terminology and some of the specifics of the game. The first question of the questionnaire centered around whether the participants actually associated the terminology with

Figure 5.6: Participant B completing the Level 3 as intended

firewall rules and if and how the components of the screen were related to each other. Participant A seemed to understand at this point that a packet is transferring data from one machine to another (which he was unaware of before playing the game) and also that the targets "accept" and "drop" let the packets through to his machine and block them respectively. This illustrates that Participant A has taken away some limited terminology and concepts from the game, despite his initial lack of knowledge.

Participant B seemed to be able to differentiate between the components of chains, packet types, ports and targets and what they do to the packet and could now effectively link them to a firewall rule. She seemed a bit unclear on chains however, which might be due to the fact that the four levels shown to her focused on the INPUT chain. Concerning the instructions, both participants felt that they could have been much clearer and that they were too small, not helping them much to complete the task at hand. They both felt that an introduction to the concepts is necessary in order to then apply the knowledge and reinforce it. Participant B also felt that some details should be explained further in the end, for example what a "tcp" packet is and how it differs from "udp". Participant B also suggested having predefined outlines for the rectangles/rule components, which would act as visual cues based on length on which part of the firewall rule they would need to select, making the decision process easier and less intimidating. Participant A verbally agreed that this is a good idea, whilst participant B was

drawing on her paper. Participant B furthermore explained that implementing this feature would also make it attractive as an app to play on a mobile phone.

5.4 Discussion

The Focus Group and Evaluation Session revealed a lot of areas for improvement. These centered on many areas, ranging from look and feel, building blocks, introduction and tutorials to smaller areas of improvement. The look and feel of the game did not appear polished to the participants or myself and I thus decided to change the design drastically in the next iteration of the game to make it appear more coherent. This also prompted me to start looking for game assets and icons that I could assemble together to ensure that the next iteration would look more aesthetically pleasing and engaging.

The game mechanic of lemmings also did not appear to work as well as anticipated and seemed to lead to confusion on the participants' side. The simultaneous building of the firewall rule and packets/lemmings moving around did not achieve the learning goal and led to more trial and error reactions because of short amount of time available, rather than actually reading and absorbing the instructions and thinking about the next movement. It appeared to me that this had to change to reflect a more problem-solving approach, with a focus on exploring to actually support the learning goals that were defined at the start of the project.

Instructions were also not sufficient to explain to the participants what exactly they were trying to achieve in the game: managing the traffic of packets between the computers. The instructions of the task at hand seemed too small and were not explicit enough to be remembered by the participants throughout the game. I decided to spend some time developing introductory texts in a short and succinct manner that could be presented in the next game iteration ahead of playing the game. I also planned to develop the quests better so it is clear to the participants what they are trying to achieve.

Moreover, the styling of the building blocks needed to be improved as well as where they need to be put in order to accomplish the level. The suggestion of an area for them to be dropped, containing a faint outline, would work as an

affordance for people to know instantly where to put them and that it would not be intended to put them anywhere else, a technique commonly used in HCI (Rogers et al., 2011). As this was suggested by two different people and was already something I had considered, it seemed like a good idea to try and focus on implementing this in the second design phase.

Chapter 6

Second design phase

Since the first iteration of the game highlighted many areas for improvement, I decided to completely redesign the game in order to support these. This meant that additional requirements gathering would need to be conducted to inform myself about certain functionality and the game's design, to ensure that the game is a success and can be played by the participants. Since the expert interview had worked well in the initial requirements gathering phase, I decided to run another expert interview to inform the redesign of the game. I did this ahead of finalising the new game mechanics, design and elements in order for it to allow for additional advice to be considered in the redesign. The final version of the second design phase and the resulting game can be found online [1].

6.1 Interview with Expert

In order to learn more about game design, good practices and common pitfalls, I decided to conduct an Expert Interview ahead of the second iteration of the game to inform more requirements gathering.

6.1.1 Aims

The aims of the expert interview were numerous. First of all, aspects considered crucial in game design were supposed to be identified. Moreover, I looked to elicit opinions concerning certain principles in design and whether they would fit in the computer security scenario. I also asked the expert which elements should

[1] `http://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/`

be decided upon first and also to identify current pitfalls and how best to avoid them.

6.1.2 Method

6.1.2.1 Criteria for Inclusion

The expert participant was chosen for the interview due to her expertise in the field of game design and educational technology. She is a researcher within the School of Informatics and also teaches undergraduate students.

6.1.2.2 Materials

To aid the interview process and provide prompts if necessary, I used a semi-structured interview script which had been prepared in advance, which can be found in Appendix D. The expert participant also filled out a consent form to acknowledge her participation and use of audio recording. The interview was digitally recorded on a mobile phone so as I could fully focus on the participant and take occasional notes.

6.1.3 Procedure

After initiating contact via email, I met the expert in her office in the Informatics forum during a time suitable for both of us. The expert was informed in advance that the audio would be recorded. During the day of the interview, I first handed out the consent form which then enabled the recording device to be switched on. I then asked her a little bit about herself, before starting the actual interview. The format of the interview, which was semi-structured, allowed the expert to elaborate on her thoughts and explain crucial information in more detail.

6.1.4 Interview C with Game Design Researcher

6.1.4.1 Area of Expertise

Interviewee C has 30 years of experience in developing educational technology, initially more AI based. More recently, she focused specifically on designing games for people with autism to improve communication skills. She has looked more at game based approaches for the past 7 years. Participatory design approaches at

various stages in her career were also involved, more specifically for the last 10 years.

6.1.4.2 Outcomes

Interviewee C first explained what she considered to be the most crucial aspects of game design. She mentioned the main critical feature in game design is engagement and making it fun for the players. If people are not engaged in the game, other issues will not matter, she explained. Gameplay was also mentioned as very important, as well as the narrative and reward system that would need to be in place in order for the game to be successful. She suggested using a participatory design approach or the role of participant and experts as design informants, contributing to the design but not making the final decision. She also talked about design by proxy - in this case experts in Human-Computer Interaction, Computer Security or Game Design, and students that don't necessarily fit the target group. The game design needs to be informed by participants, theory and empirically informed (by design workshops and formative evaluations) in order to be justified.

The nature of problems being dealt with in security, technical but containing consequences and actions, as well as understanding causal relationships, prediction and modelling skills, lend themselves to include a reflective learning element, Interviewee C explained. She elaborated that testing consequences of certain actions and getting people to think deeply would enable them to learn about security.

When I prompted her on characters and whether it would be useful to include them, she asked what the goals of the game are and what the intended target group is, as this will ultimately influence the decision of including characters. The learning goals need to be defined at the start she said and also mentioned there's more scope at the beginner level to do this. She illustrated that there is a distinct difference between exploratory learning or problem solving learning, meaning there's a correct answer or specific goal to achieve. She highlighted that I would need to decide whether to mix them or include them in a laddering approach of levels, with first offering exploratory learning then increasingly show more problem solving.

She also talked about the importance of deciding on how the system should be used and how the user is interacting with it, meaning whether the user is suggesting to the system what to do or whether the system coaches the user, the former offering a bit more "fun" she explained. She added that different profiles of the character: cynical, trusting, etc - could represent different types of characters who have different attitudes to security which in turn enables the user to step back and think about what the characters in the game and that those characters represent different strategies and attitudes to security.

Concerning the content of the game, she suggested coming up with a single concrete idea for a quest first and then come up with framework for that type of game. This would in turn allow for making variations of characters for that quest. While doing this, it would be important to decide on what exactly the players should know about and to make explicit what their background is and what they know or do not know. Some interviews and surveys to find out which environments and background motivate them might help, she added, which is closely tied to the learning goals and inform the gameplay. She also mentioned that variation in terms of levels is important since people will want to see some sort of progress, even if just a change in looks or environment.

Common pitfalls she identified were students starting to think about visual resources in the first instance instead of deciding on gameplay which according to her is much more important, especially if it is an educational game. She reiterated that the game at this stage is more of a proof of concept, it will have a few example scenarios, however since it is being critically evaluated, it would provide more value than a "flashy but useless" game.

6.2 Second build

The second design phase saw a complete redesign of the game, to alleviate the shortcomings identified in the first design phase. I chose an agile methodology for iterative development for the development of my game, to continually get feedback from potential users and rework parts if necessary (Larman and Basili, 2003). The potential users fit roughly with the target group with members having

no experience at all with Computer Science and Computer Security, and some members having Computer Science experience but not necessarily knowledge in Computer Security. The users provided me with their opinions continually, offering support concerning the look and feel of the game, instructions provided, feedback given by the game and its usefulness, as well as the general game dynamic. This enabled me to build a game according to users' needs as opposed as letting my own decisions take precedence.

6.2.1 Sketches

In order to get some feedback from the potential users early on, I presented sketches of initial ideas to them and asked them to share their thoughts with me. These sketches included a rough sketch of the game screen itself that you could interact with (see Figure 6.1), as well as some thoughts which services could be included and how they would be presented to them.

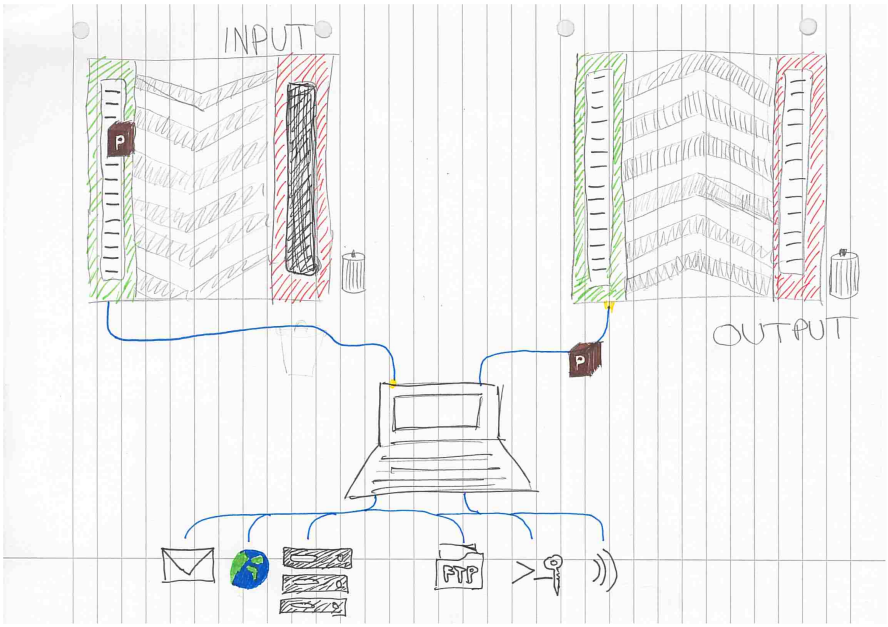


Figure 6.1: Sketch of a game screen showing INPUT and OUTPUT areas as well as packets and services but not including the shaded slots and building blocks

Showing the game screen sketch (Figure 6.1) to the potential users, it became apparent that they liked the INPUT and OUTPUT boxes and that their background was indicating direction of travel. One shortcoming identified in the first

design phase was the absence of a path as packets only travelled over the screen without indicating where they were going, see 5.1. Hence, I decided to include "cables" that connected the boxes with the computer and the services, despite the fact that this is not technically accurate. The potential users mentioned that this helped them to visualise where packets would be headed roughly and which path they would go down. The bin also seemed to suggest to them that certain packets do not go to the PC but get put in the bin.

6.2.2 Mockups

After a few very rough sketches, I chose to mock up some of the tutorial screens using the tool proto.io [2] as it provided more functionality than the previously used balsamiq [3]. Proto.io offered more functionality and prototyping elements as well as the use of colours and how appealing the elements looked to participants and how they would go from screen to screen. Examples of some of the screens can be seen in Figure 6.2, Figure 6.3 and Figure 6.4.

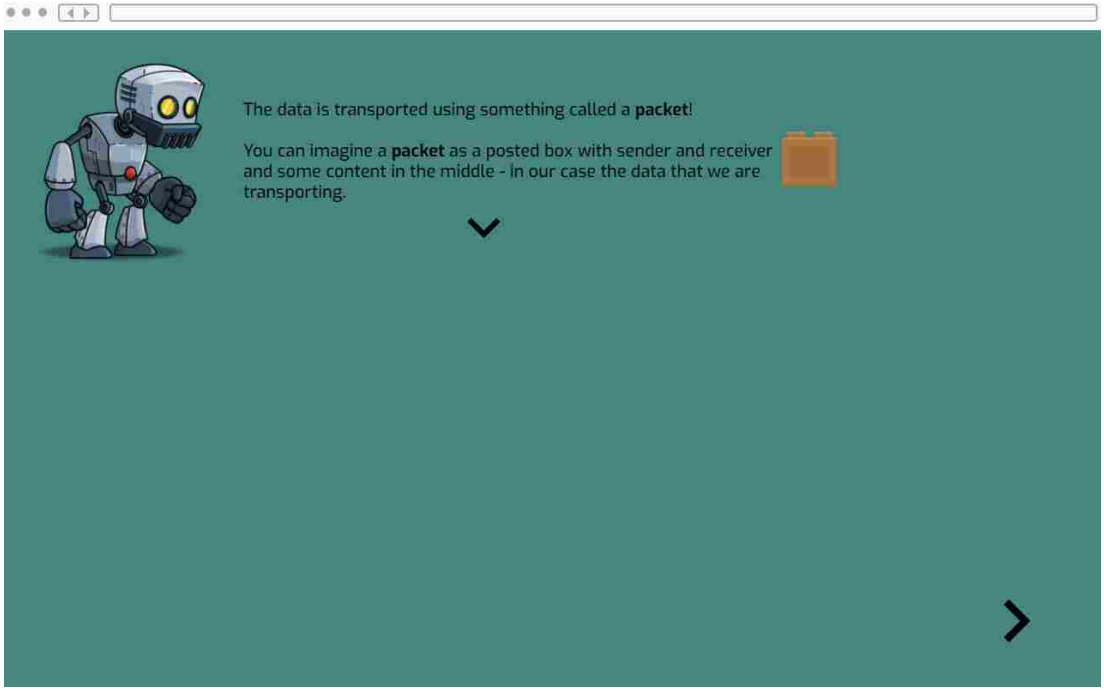


Figure 6.2: Example of not showing the user all text at once but let him select chunks at a time

[2] https://proto.io
[3] https://balsamiq.com/

Showing the screen from Figure 6.2 to potential users, I got positive feedback for choosing not to display all text at once. However, they remarked that it did not make complete sense to them to display an arrow for more text but also display an arrow pointing at the right for indicating to go to a next screen. This distinction was noted and to be included in the actual game tutorial screens.

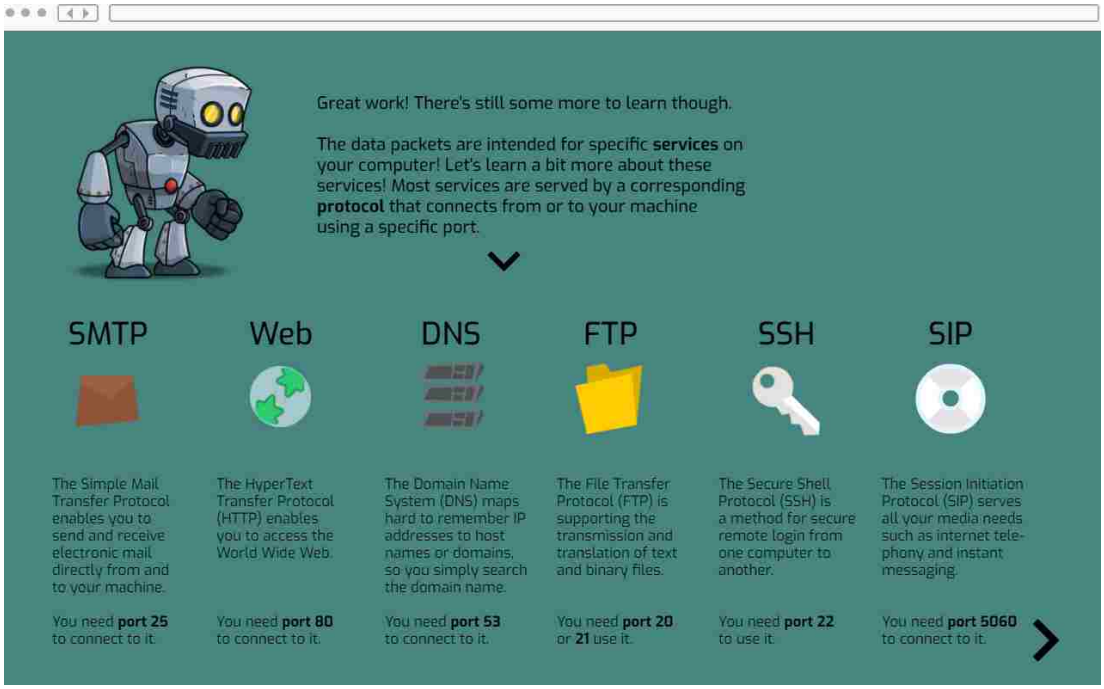


Figure 6.3: Example of a prototype screen that shows information regarding the services included in the game

Figure 6.3 displayed the services which I deemed to crucial to include after following the literature in Cheswick et al. (2003); Zwicky et al. (2000) and reading several tutorials on setting up basic rules on your home computer. While the brevity of describing the services was liked by the potential users, they all agreed that there was too much information on one screen and that the information should be displayed in different levels, rather than introducing all the information on ports, services and protocols at once. Same applies to Figure 6.4 which shows how a firewall rule might be constructed. The potential users agreed that this was far too complex for a beginner at this stage, despite the explanations. It was also decided to scrap certain expressions such as **-j,** –**state, -p** and specifying the interface as to not overload the learner and to focus on teaching the important material rather than checking specifics. The potential users also

mentioned that too much information was present on the screen and that the game should support gradual learning, sometimes called scaffolded learning, such as in Baylor and Ritchie (2002) and Cho and Jonassen (2002). I thus decided to focus on teaching one service at the time instead of trying to convey information on all of them at once.

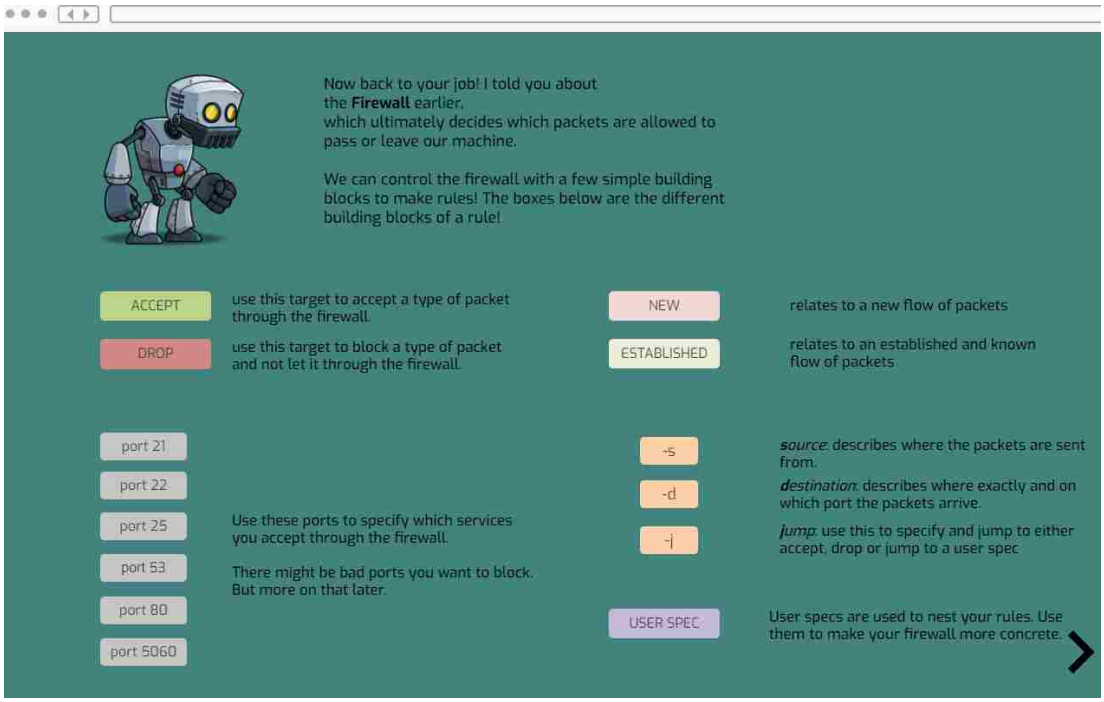


Figure 6.4: Screen showing how to construct a firewall (later discarded)

It is worth noting that the icons below the service name looked different initially and were updated at a later point before building in the chosen platform to reflect a mockup which is more similar to the game screen assets before building the tutorial screens. Showing these icons again to the potential users, I received mostly positive feedback for their look and feel. The robot sprite also felt more polished for the potential users.

The mockup screens can be viewed at at proto.io [4] without the need to create an account.

[4] `https://pr.to/C1OH8L/`

6.2.3 Chosen Platform

Given that I already learned a lot using Unity in my first game iteration, I decided to keep developing with the Unity Game Development Engine (Unity Technologies, 2017). The possibility of building the game cross platform was appealing and also meant that software such as Flash could be avoided. Unity appeared to be a viable choice since newer versions offer powerful UI components and building GUIs.

6.2.4 Game Mechanic

Game Assets and Sprites

Since the look and feel was a big consideration during the second design phase and as the Game Design Expert suggested I should not spend my time on developing "flashy images", I decided to look for free to use Game assets and sprites which I could use in my game. Kenny's Game assets [5], which are free to use and available under the CC0 1.0 Universal Licence, was selected as a source for many of the game assets. Since Kenney offers many free collections of Sprites, I could pick freely from all of them and use them as I saw fit. These game assets also included some UI buttons, of which I kept some and modified others to fit the style of my game. The music included in the game is also royalty free [6].

The robot sprite which could already be seen in the proto.io mockup screens, was not a free game asset and was purchased for a price of roughly £6 at Game Art Partners [7]. I searched for free game assets of a robot sprite but could not find anything that was suited to my needs, which is why I decided to purchase this sprite for use in one application, my game. Since I am not redistributing my code or assets in isolation, I can use this robot sprite and its associated animations. I do not own this image and the copyright stays with the owner and creator but I am allowed to use it in my application [8].

[5] `https://kenney.nl/assets`
[6] `https://www.dl-sounds.com/royalty-free/category/game-film/video-game/`
[7] `https://gameartpartners.com/downloads/big-hands-robot-character/`
[8] Please see Licensing for Paid Game Art `https://gameartpartners.com/licenses/`

Game Screens, Tutorial Screens and Elements

The elements of the game can be roughly divided into Game Screen Elements and Tutorial Screen Elements. While the game screen is the interactive element, the tutorial screens are a presentation of concepts and knowledge.

Game Screens

This section provides an overview of how the user can interact with the game screen and build a firewall rule that is based very loosely on *iptables*. Figure 6.5 shows how the user can drag and drop the building blocks onto the INPUT chain area and the OUTPUT chain area slots to signify incoming and outgoing traffic, using the interaction type of manipulation (Rogers et al., 2011). The building blocks that can be dragged, each also have a different colour to differentiate their different functions in a firewall rule. The corresponding colours of the slots in the INPUT and OUTPUT chain area make it easier for the player to see where the components might go and reduce the fear of making too many mistakes. The predefined outlines of the slots were chosen as to provide the user with an affordance to make clear that the blocks did not need placed elsewhere on the screen (Rogers et al., 2011).

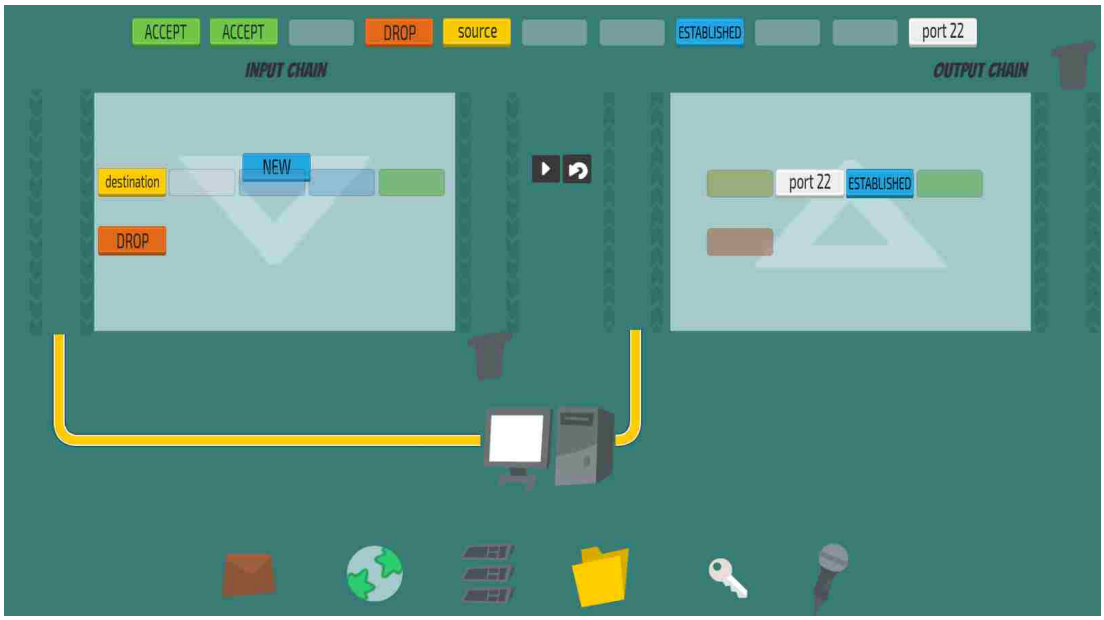


Figure 6.5: Level 2: Allowing SSH traffic inbound and outbound with a default policy of DROP - illustrating the interaction type of manipulation in a drag and drop fashion

The INPUT chain and OUTPUT chain area contain an arrow that signifies the direction of travel for the packets the user is controlling. The chevrons at the sides of each area box are also containing little arrows to show direction of travel. The bins that are appearing at either end signify the dropped packets which are not let through the firewall. Once the user has dropped all the building blocks onto the respective slots, he can then press the play button to see what happens. If the rule has been constructed according to the instructions, packet movement is enabled as can be seen in Figure 6.6. The scripts that have been used to enable the paths and the movement have been taken and adapted slightly from Palacios (2016). The packets have an icon on them based on the service they are headed for, in this case SSH. The generic packet sprite relates to all other packets in this instance.

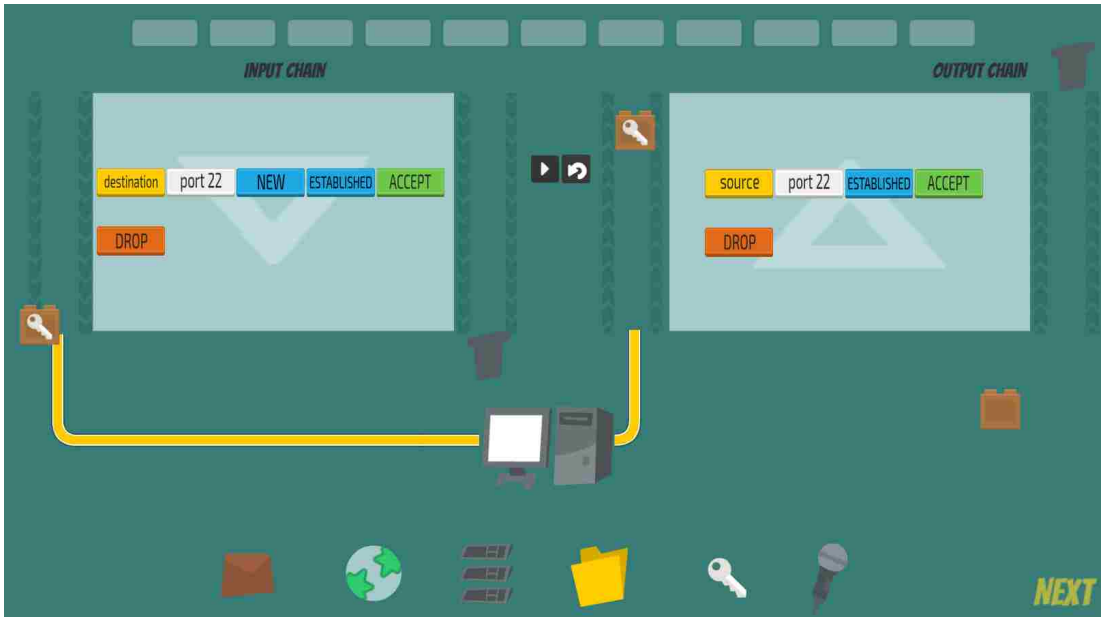


Figure 6.6: Level 2: Allowing SSH traffic inbound and outbound with a default policy of DROP - showing the movement of packets

If the rule is wrong no packet movement is enabled, and the robot sprite is appearing in the corner to tell the user to try again as can be seen in Figure 6.7. I initially felt strongly about showing the user how wrong inputs to the slots would alter the packet movement. I showed this feature which I built to potential users but they suggested that they rather not see the packets move and want instant feedback that they made a wrong decision so they can recover from it quickly.

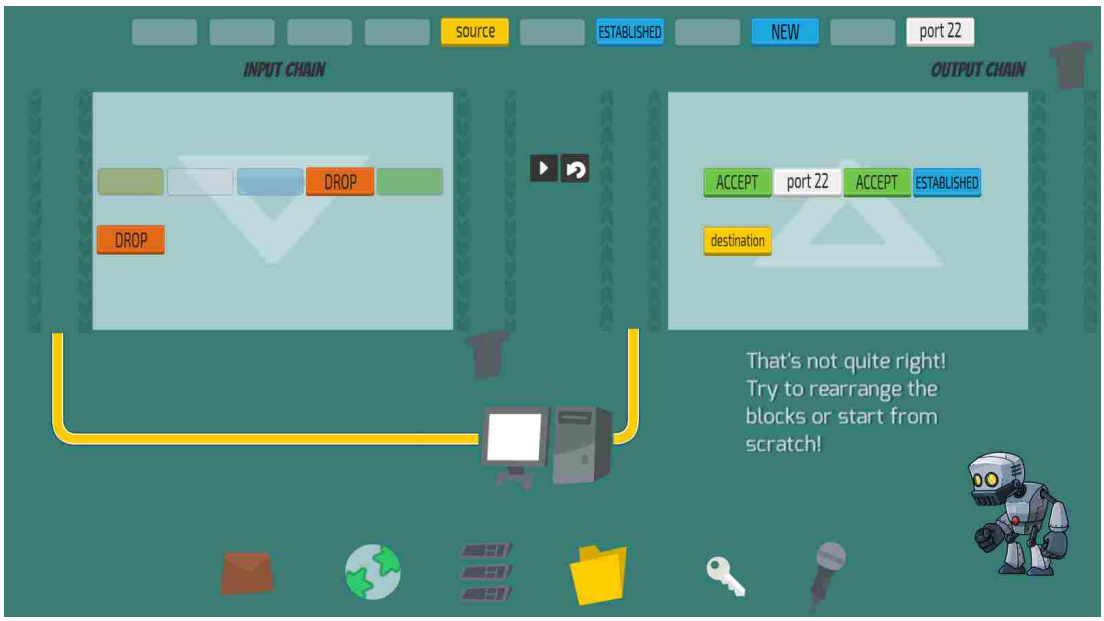


Figure 6.7: Level 2: Allowing SSH traffic inbound and outbound with a default policy of DROP - feedback for selecting a wrong rule

This was a slightly surprising finding, but since the potential users felt strongly about this, I incorporated such feedback in the game as shown in Figure 6.7.

The reset button which appears next to the play button resets the current screen and lets the user start from scratch instead of dragging and dropping all the items back around again. This was implemented as a means to speed up the process of completing a level instead of dragging and dropping until the user becomes frustrated.

This is only one example of a particular game level to explain the game screen. I have built several other levels that are playable by the user[9].

Tutorial Screens

There are many different tutorial screens and they could not possibly all be included in this section. I will try and provide a few examples to illustrate the components of a tutorial screen and the thinking process that was involved in

[9]Available to play at the following `http://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/` or `http://sibyllesehl.me/Game_Final_SibylleSehl/index.html`

constructing these.

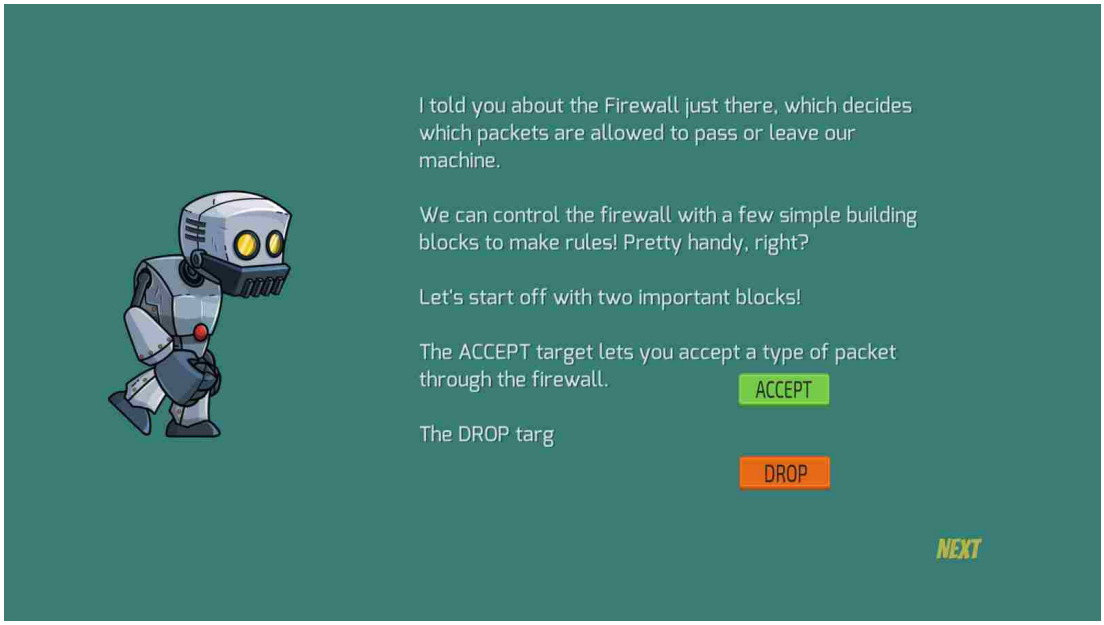


Figure 6.8: A tutorial Screen for Level 1 that presents very basic knowledge to the user

Figure 6.8 is one of the screens that is displayed to the user before the first level. The information is set to a minimum on the first few tutorial screens as to not overload the user's attention span and learning at the start. The writing illustrates the robot speaking to the user and the typewriter effect is used to provide a more interesting game dynamic. The potential users preferred the typewriter screens to seeing just a full screen of text, which one user mentioned would just resemble a power point presentation. The robot is animated and walking on the spot while telling the user about the help he needs in setting up a policy or rules.

Later levels are introduced by one longer tutorial screen as the user gradually becomes more confident. This is slightly similar to scaffolded learning in which the help and aid is gradually reduced. Figure 6.9 shows how a new service is introduced at the same time as the user is informed about the upcoming quest. Employing scaffolded learning here, I also reduced the need to click through multiple screens which might bore a user when he gets more confident.

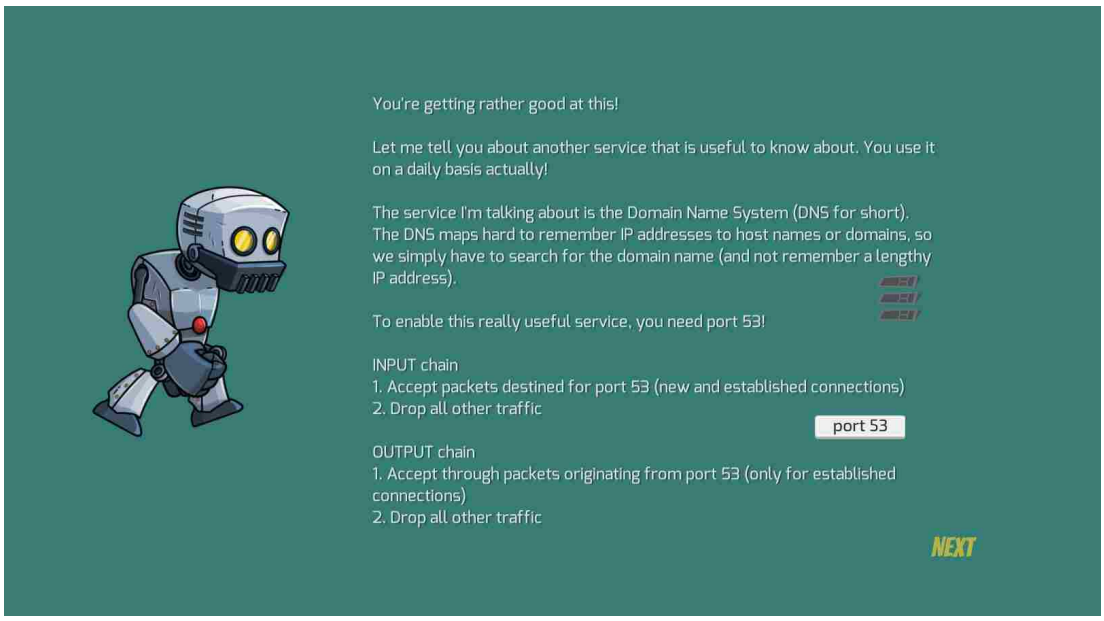


Figure 6.9: Tutorial Screen that is used later in the game to introduce the Domain Name System and provide a quest assignment to the user

Level Structure

The game contains 10 levels which increasingly present fewer instructions and introduce new concepts the further the player advances in the game. The last level (Level 10) contains increased difficulty as opposed to the previous levels by reducing help such as shaded slot backgrounds and giving the user more building blocks to than necessary for constructing the firewall rules. The services the user learns about during the course of levels 2-7 are considered crucial by Cheswick et al. (2003) and Barrett et al. (2003) and many online blogs. The music changes for Level 8 and 9 and then again in Level 10 to reward the user for the increased difficulty of quests he is now completing.

Level 1: Apply a policy

Level 1 and the associated Tutorial Screens teach a lot of new material to the user. Terminology such as targets, rules, ACCEPT and DROP are introduced in the tutorials. The interactive game screen in which the user completes their quest, contains only two building blocks ACCEPT and DROP as to ease them into manipulating the building blocks and learning where they can place them. Users should understand at this stage that DROP means that packets will not go to the machine (if implemented at the INPUT chain) and get “binned” and

that ACCEPT means that the firewall will let them through.

Level 2: Allow Web traffic

Level 2 presented the student with new knowledge concerning rules, policies, chains and how rules are read to construct them in the associated tutorial screens. The terms were explained in an easy-to-understand fashion as much as possible. The interactive game screen now contained a rule and a policy at both INPUT and OUTPUT chain. The user was provided with all of the necessary building blocks to build both the rules and the policy. The slots on the INPUT and OUTPUT chain were coloured to ease the participants matching of the building blocks to the corresponding order of the slots. Web traffic packets were chosen in this level, as it was anticipated that most users knew about the World Wide Web.

Level 3: Allow Incoming and Outgoing SSH

Level 3 introduced the service of the Secure Shell Login. It was anticipated that Computer Science students that might not have worked with Computer Security would have used SSH during the time at their time at university or at work. It was thus included straight after the well known web traffic to not confront the user with too much new knowledge.

Level 4: Allow FTP connections

FTP was included as some organisations use FTP connections and because I anticipated that selected users might have used it in the past, thereby still recalling at least its name or function. In similar fashion to level 2 and 3, the service was introduced and required the user to input the same rule and poliy as before, however recognising that the port they had to select changed.

Level 5: Allow DNS packet traffic

Level 5 briefly introduced the term of the Domain Name System (DNS) and mentioned that users might not even realise that they are using the DNS on a daily basis. Apart from introducing this new service and a new associated port and showing new packet flow, the level was very similar to previous levels.

Level 6: Allow SMTP traffic

SMTP and its associated port was shown to the user in the 6th level. The rule constructed by the user remained the same as those for services introduced in earlier levels.

Level 7: Allow Media services by enabling SIP traffic

This media port was included since it was a port that is generally considered safe for media use, especially since many game and media related ports are considered potentially dangerous. I also considered a port for media a useful addition to the previously mentioned services that were all contained within Cheswick et al. (2003) "Services we like".

Level 8: Allow two services at the same time

Levels 2-7 served as a gentle repetition of constructing a rule to let particular types of packets pass through the firewall while blocking all other traffic. Level 8 was implemented so as the user could understand that he could chain different rules after each other and educating them on the default policy which would grasp all else that would not match the classification of those rules. This level provided more difficulty in the sense that the principle of checking each rule in turn should be understood by the player. Three different kind of packets: web, ssh and generic packets were turned on by the player once the "Play" button was pressed.

Level 9: Block a malicious IP address

As opposed to the previous levels which all required the user to implement a default policy of DROP, this level pictured a situation in which the default policy was ACCEPT. A specific IP address is supposed to be blocked by the player, thereby dropping red coloured bad packets in the Game screen and letting through the generic packet. This level intentionally did not present the ACCEPT default policy as the best option, but merely described the situation. This was done as to let the player think about the different consequences of having different default policies.

Level 10: Construct sensible rules yourself

Level 10 saw the removal of the colour shaded slots, no concise instructions and the provision of more building blocks that the participant could choose from. These were all implemented to paint a scenario in which the user needs to make more complex decisions himself. Moreover, the malicious IP address was included to see whether users would understand that the default policy of DROP would drop its packets as long as the packets were not destined for port 80 or port 5060.

6.3 Evaluation with Expert

6.3.1 Aims

The aim of this brief unstructured interview and demonstration of the game was to get some feedback on the design, mechanic, engagement and perceptions of the expert ahead of the user evaluation to make changes if necessary.

6.3.2 Method

I conducted this evaluation in the fashion of an unstructured interview that gave me the opportunity to ask many questions at the time at which they occurred. As opposed to a more structured interview, it also allowed me to ask questions more freely and let the expert explain in plenty of detail.

Participants

The session included myself, the other two students that work on creating a game in a computer security context and of course the expert himself.

Setting

The expert was met in an informal environment in the Informatics Forum, in Mini Forum 2 which offered couches and low tables for close interaction.

Materials

Apart from the consent form, that informed the expert that his quotes might be used for research purposes, he only interacted with the game on my personal computer. An interview script was not included.

Procedure

After having handed over the consent form, he signed the consent form and was invited to briefly talk about himself. The unstructured interview and demonstration of the game lasted roughly 30 minutes, which the expert had allocated to each of the students including myself. After he learned a bit about each of our games, he proceeded to look at each of our games in turn. My game was looked at in the middle of this evaluation, while the card games' evaluation took place first and last.

6.3.3 Unstructured Interview with Expert D

Area of Expertise

Expert D has finished his Masters at the University of Edinburgh in 2016 and now works as a Firewall Administrator in Edinburgh. He is familiar with several firewall tools, very experienced in rule construction and also deals with clients' problems on a regular basis. As opposed to Expert A and B, he is not working at an ISP but at Enterprise level which differs greatly from the work an ISP might experience.

Outcomes

After handing the expert the consent form which he signed ahead of playing through everyone's game, he first played through a card game which relates to firewalls created by one of the other students. He seemed very apprehensive about teaching firewalls in a card game and seemed to prefer the idea of a video game to a board or card game.

Expert D had very strong opinions on a range of different aspects related to firewalls. He seemed very apprehensive about the tool of *iptables* and explained that in his opinion, noone uses them at Enterprise level. He mentioned that he cannot remember all the terms and concepts relating to *iptables* and last used it a few years ago.

When playing my game and clicking through the tutorial screens, he seemed to like the general aesthetic of the game and called it pretty. He liked the tu-

torial screens ahead of the game screen as said that they provided a reasonable portion of information. He also commented that he liked that the game provided a little story as to why the firewall needs managed and maintained. However, he was of the opinion that more context could be provided to make the game more engaging and provide reasoning as to why the firewall is important and needs maintained. When I asked him whether he found the game engaging, he was neither particularly positive or negative.

Concerning the game elements, Expert A provided some design improvements that would make the game more polished and make certain elements clearer. He mentioned that he missed a button to go back to the instructions as to check again what exactly he was supposed to do. He also highlighted that a cloud between the INPUT and OUTPUT area that contains the name of the service he is learning about or which he is allowing through the firewall, could be written on this cloud as to avoid the situation of people stopping and resuming without knowing where they have left off.

He indicated dissatisfaction concerning the cables that are shown between the areas as they were not technically accurate but did not bring this up again at any other point of the session. In general, Expert D seemed to grasp very quickly what he was supposed to do and accomplish in the game and could get started quickly. This provided an advantage compared to the card games whose instruction process he found quite lengthy.

6.4 Discussion

Expert D could provide me with a range of features that I could potentially implement at this stage, but due to the advanced nature of the project at this stage, he suggested that making changes to the interface, such as the cloud as well as a back button, should be my primary focus. These changes were feasible before the user evaluations which is why I decided to implement them.

The general dislike of *iptables* by the expert is a criticism that was noted by myself and another student, but since literature suggested otherwise and usually

recommends it as a free to use solution and easy to understand by beginners (Cheswick et al., 2003; Barrett et al., 2003), it was decided to not explore this in further detail. This is especially true, since my game is loosely based on *iptables* and not teaching the user the correct commands he might need to enter in the command line when setting up *iptables*. Some of his other criticism related to the building blocks my game contains but since they were loosely based on *iptables*, this commentary was not regarded as important as others.

It is also worth remembering that Expert D is very experienced with Firewall Administration and that his learning goals would differ greatly to those of a beginner. Being an expert does not automatically qualify one to teach concepts and terms in easy fashion (Scalfani, 2016). Since the learning goals were to introduce terms and explain them, and offer an opportunity to make mistakes and recover from them, the technical accuracy of the pictures such as cables was not as important for me to improve, especially given that the project was near completion.

6.5 Implemented changes

Given the expert's feedback, I implemented the suggested improvements in the interface. A few images such as a cloud at the top of the Input and Output chain area boxes as well as a red brick wall, symbolising the firewall, were added to the screen as seen in Figure 6.10. I decided against writing the name of the service of the tutorial on the cloud, since later levels contain multiple services or do not focus on them at all (Level 9: Blocking a specific IP address). Instead, back buttons and menu buttons were implemented into the game screens as to improve the navigation experience for the user, see Figure 6.10.

If a tutorial sequence lasted longer than a single screen, I also implemented back buttons so that the potential user could review the tutorial for the current level. Moreover, the user is also able to see the level he is aiming to complete when undergoing the tutorial corresponding to that level. I implemented this as my supervisor suggested that it would be good to show the user their current progress in the game. Both of these features can be seen in Figure 6.11.

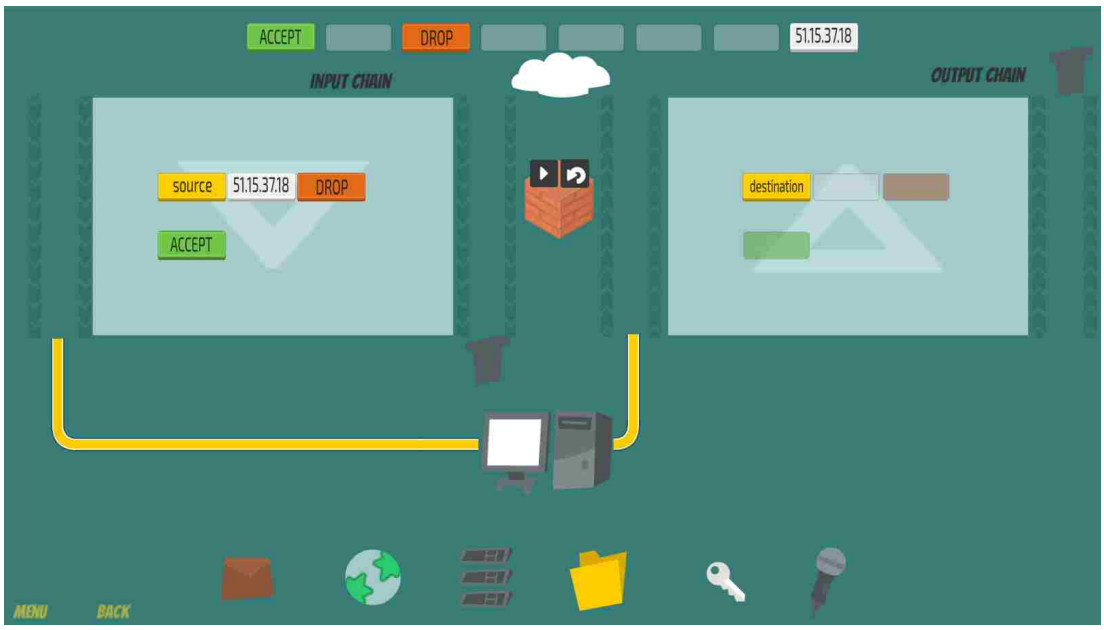


Figure 6.10: Game screen of Level 9 showing a brick wall, a cloud and menu and back buttons

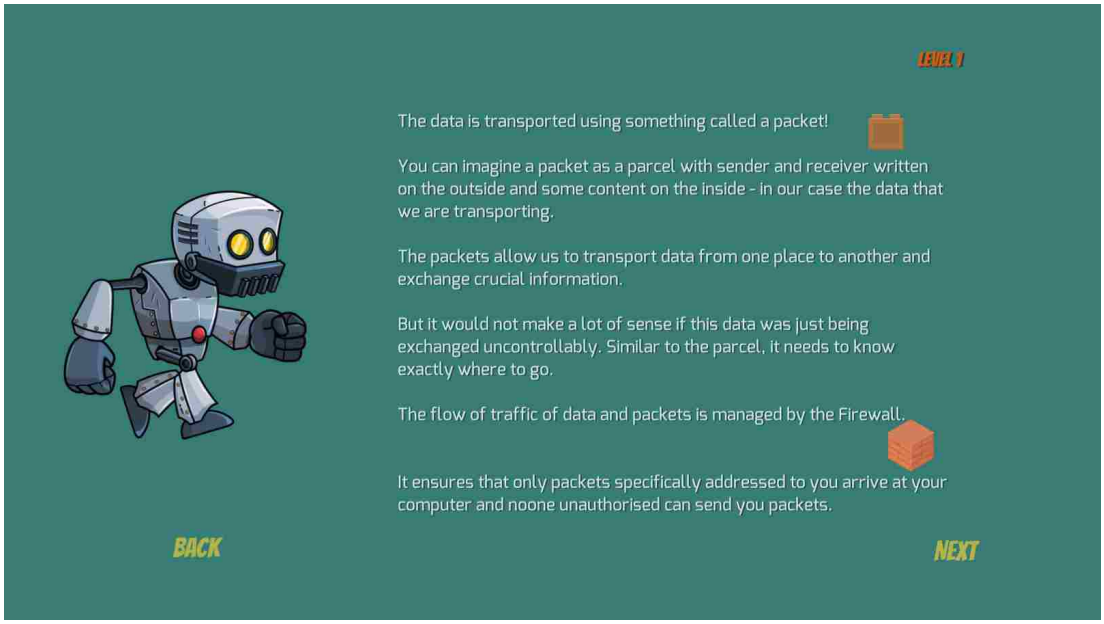


Figure 6.11: Tutorial screen showing the current level in the top right hand corner and a back button in the bottom left hand corner

To aid the navigation further, I also implemented a level selector. The respective buttons for each level take the user to the first tutorial screen associated with the level. Levels are read first from left to right in rows as can be seen in Figure 6.12. I initially implemented the level selector buttons from top to bottom

in columns, but potential users were confused by this arrangement.

Figure 6.12: Level Selector that lets the user navigate to each level and its first respective tutorial screen

Chapter 7

Pre-/Post and Usability Evaluation with Target Group

This chapter comprises the evaluation of the game that was created during the second design phase to understand whether the learning goals set for the game were achieved and to assess whether the created game adheres to usability standards. The evaluation of the learning goals was designed around a pre-/post test, to compare knowledge before and after playing the game. Concerning the usability of the game, I used the System Usability scale by Brooke et al. (1996) and asked ten participants to score my game.

7.1 Aims

In order to test whether the second build is successfully conveying the learning objectives I defined in the requirements gathering phase, I ran an evaluation session with a range of different participants. Participating users filled out the same evaluation questionnaire before and after playing the game to assess their knowledge before and after and to identify areas that could potentially be improved in the future. In addition, to understand whether the game I created is usable and user-friendly, I used the system usability scale to see if the participants found my game easy to use and could complete the tasks without external help.

7.2 Method

The evaluation consisted of two questionnaires, a pre-/post test type evaluation questionnaire and a user feedback questionnaire that contained the System Usability Scale (SUS).

The System Usability Scale (SUS) is a "simple, ten-item scale giving a global view of subjective assessments of usability" (Brooke et al., 1996). It is a subjective Likert scale and covers areas such as the need for support, training, and complexity of a system. By using the System Usability scale, I could calculate the SUS score which can range from 0 to 100, where 0 indicates that the system is not usable at all and 100 indicates that the system is perfectly usable.

I chose the method of a pre-/post test for assessing participants knowledge, as I had already used it during the lab study in the requirements gathering phase as well as during the evaluation in the first design phase and as it proved a useful method in both of these situations.

7.2.1 Evaluation Questionnaire Design

The evaluation questionnaire which I provided the participants with before and after the game play, contained a number of different sections. The resulting questionnaire can be found in Appendix E.

Demographics

These questions were included to learn about the participants age, gender and academic background and ease the respondent into the questionnaire (McFarland, 1981).

Knowledge of firewalls

Questions 4 to 9 were based on the participants' knowledge of firewalls. The questions included whether participants had heard of the term firewall before, whether they knew why their computer needs a firewalls and if they knew how a firewall operated. As the game is targeted specifically at beginners and people

with a limited amount of knowledge prior to completing the game, I felt that asking participants those questions would provide me with some detail concerning their current knowledge before the game and more refined answers after having played the game. The very first question "I have heard the term Firewall before" was included as was anticipated that most participants would have heard it and to give all users to opportunity to answer a question with "Yes" in the very beginning.

Knowledge of firewall related terminology

Questions 10 to 13, 15 and 16 as well as Questions 18 and 19 were all used to assess the participants' familiarity and knowledge in relation to firewall terminology. I used different ways of asking the participants for their current knowledge as to not frustrate less experienced users, for example by asking for the familiarity of terms in Question 16 and by asking "Firewalls..." in Question 12 to give users the ability to simply identify terminolgy that seemed familiar. The more elaborate questions looked to identify their current knowledge in the pre-test and by comparing their answers to desirable answers in the post-test.

Ability to read an iptables command

Question 14 tested each participant's ability to understand an iptables command prior to playing the game and after playing the game. Since the game I created was loosely based on *iptables*, it was anticipated that at least a small percentage of people would succeed in successfully understanding the iptables command after playing the game.

Ability to differentiate between Input and Output rules

Question 17 was included in the questionnaire for two reasons. In the pre-test, the question aimed to identify whether participants would at all think about INPUT and OUTPUT in terms of the firewall. In the post-test, the question looked to understand whether participants could correctly link those terms to the chains and the rules that underlie these.

ID	Age	Gender	CS knowledge	Security knowledge
P1	22	Male	Yes	Yes
P2	23	Female	No	No
P3	28	Male	Yes	No
P4	22	Male	Yes	Yes
P5	26	Female	Yes	Yes
P6	26	Male	No	No

Table 7.1: Participant Mappings where CS means Computer Science and Security refers to Computer Security

Ability to understand the game interface

Questions 20 to 27 were included to understand whether the participants understand the interface prior to playing the game and also which assumptions they would make if they had to associate firewall terminology with the interface. In the post-test, these question served the purpose of not only showing how understandable the interface is but also whether their learning moved beyond learning new terminology and whether they could correctly identify concepts presented to them on the screen in an abstract fashion.

Participants

Most of the participants had initially expressed their interest in testing the game which led me to contacting them prior to the evaluation. The six participants that took part in this evaluation were from Informatics and Non-Informatics background as well as containing participants that had knowledge of computer security. All of the participants are currently studying for a degree or recently completed one. All of the participants are aged 22 to 28, see table 7.1. All the participants which filled out the Pre-/Post Evaluation also filled out the Usability Evaluation. In addition, four more people filled out only the System Usability Scale survey, which leads to a total of 10 participants. Three participants were female, and seven participants were male. Moreover, six of the 10 participants did not have an Informatics or Computer Science background, whereas four participants did.

Setting

Four of the participants filled out the consent form, questionnaires and SUS forms at my own flat as the evaluation took place on a Saturday. The participants were thus able to play the game on a large screen while I could control the environment. Two participants could not join the evaluation in person but had agreed to take part from their own homes.

Materials

The following materials were used during the session:

- The Game, shown as a WebGL application in a Firefox Browser Window
- Computer, screen and mouse, as to enable viewing the game and interacting with it
- Consent Form
- Pre-/Post Test (called "evaluation questionnaire" for the participants)
- System Usability Scale (called "User Feedback Sheet" for the participants)
- ShadowPlay video recording software
- VLC video recording software

The participants that agreed to come to my apartment were shown the game on a big computer screen and were provided with a mouse to interact with the game. The game was run locally on the machine and viewed in a html file produced by the WebGL Unity Application. The consent form as well as the evaluation questionnaire can be found in Appendix A and E.

Procedure

After agreeing to take part in this evaluation, I gave a consent form to the participants and asked them to fill it out. I then provided all the participants with an evaluation questionnaire to fill out. This questionnaire was four pages long and can be found in Appendix E. It also contained a screen from the game which was also shown to the participants on a laptop screen to make sure that they could accurately see each of the components they were asked about. This screen can

be seen in Figure 7.1.

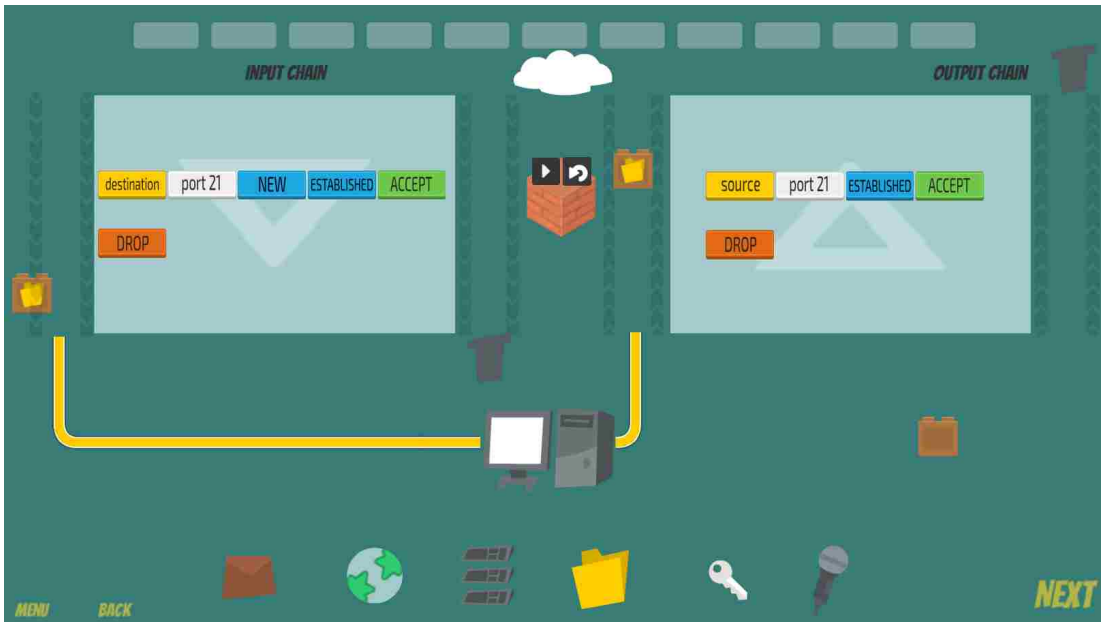


Figure 7.1: Game Screen that was included in the Evaluation Questionnaire

After completing the evaluation questionnaire for the first time, the participants were invited to play the game on my personal computer and a big screen. I advised them that I would turn on the video capturing software ShadowPlay[1] which would record their interaction. Participants completing the evaluation in the comfort of their own home were only sent a link to the game once they had sent me the completed consent form and first evaluation questionnaire. They could access the game via my personal website [2]. After playing the game, they were first asked to fill out the System Usability Scale in a quick and intuitive fashion. I also instructed the participants not to think about their answers too deeply. After completing the System Usability Scale, the participants were asked to fill out the evaluation questionnaire again. Finally, I asked them whether they had any further questions and thanked them all for their participation.

[1] https://www.nvidia.com/en-us/geforce/geforce-experience/shadowplay/
[2] http://sibyllesehl.me/Game_Final_SibylleSehl/index.html

7.3 Results

7.3.1 Pre-game questionnaire

Prior knowledge of firewalls according to participants

Each participant indicated that they had heard the term "firewall" before and could roughly describe that it prevents unwanted access (P3) and protect the computer from hackers (P2). Not all participants were aware of how a firewall operates. P1, P2, P3 all indicated that they did not know how firewalls operate whereas P4 and P5 did. P6 had to be excluded from the knowlege acquisition results as he only returned one questionnaire and did not indicate whether the document was filled out before or after the game.

Prior knowledge of firewall related terminology

Concerning their familiarity of firewall terminology, the answers varied. P2 who had no knowledge of Computer Science indicated that she did not know what a packet is. She also indicated limited familiarity with protocols and services and did not know what policy, rules or protocols signify. P1, P4 and P5 all indicated that they had knowledge of computer security but did not successfully indicate all the terms related to firewalls prior to playing the game. They did however recognise a higher number of protocol names and services. None of the participants could explain what "chain" meant in terms of firewalls.

Prior ability of reading an iptables command

Apart from P4, every participant struggled to read an *iptables* command and could not identify what the words and numbers meant to them.

Prior ability of differentiating between Input and Output rules

It was not expected at this stage that participants would understand the difference between INPUT and OUTPUT but I included this question in the pre-test to check whether they would relate the terms to incoming and outgoing traffic. P1 and P4 (both having Computer Security knowledge) correctly identified the terms relating to connections, however P5 despite having Computer Security knowledge

did not. P3 tried to relate it to something being inputted and outputted from the computer but did not relate the knowledge to firewalls.

Prior understanding of the interface without having played the game

Figure 7.1 was shown to each participant to see whether they could understand the interface of the game. I asked them to associate terms with certain game elements on the screen to see whether they could make connections between terms and the design elements. Results from this question varied greatly. Every participant apart from P1 could correctly identify the packets on the game screen and label them accordingly. Each participant, apart from P4, only circled the brick block to show the firewall and they did not identify the Input chain and Output chain to be part of it at this stage. Three participants did not correctly identify a firewall rule at this stage or identify the policy, with the exception of P4 and P5 who both have computer security knowledge (see Figure 7.2 for a correct understanding of the interface prior to the game). Three participants could not point out that the 6 symbols below the computer indicate the different services at this stage. The purpose of the bin was clear to three participants. The identification of the cloud to signify the internet was not clear to two participants and they related it to data storage instead.

7.3.2 Game testing

I asked each participant to play through the game and take as much time as they need to complete the tasks. Especially since the game requires the participant to read a lot before completing the associated levels, I anticipated that the completion times would vary across participants according to their reading speed.

Every participant carefully read through the first set of instructions for the first level and tried to understand the tasks given to them. P1 and P3 needed prompted that the blocks at the top could be dragged around the screen, whereas P2, P4 and P5 seemed more familiar with the drag and drop style of the game. Once, P1 and P3 figured out that these elements could be dragged, none of the participants had visible problems with the first level and each participant could successfully advance to the next level. P1 also clicked on the packets to

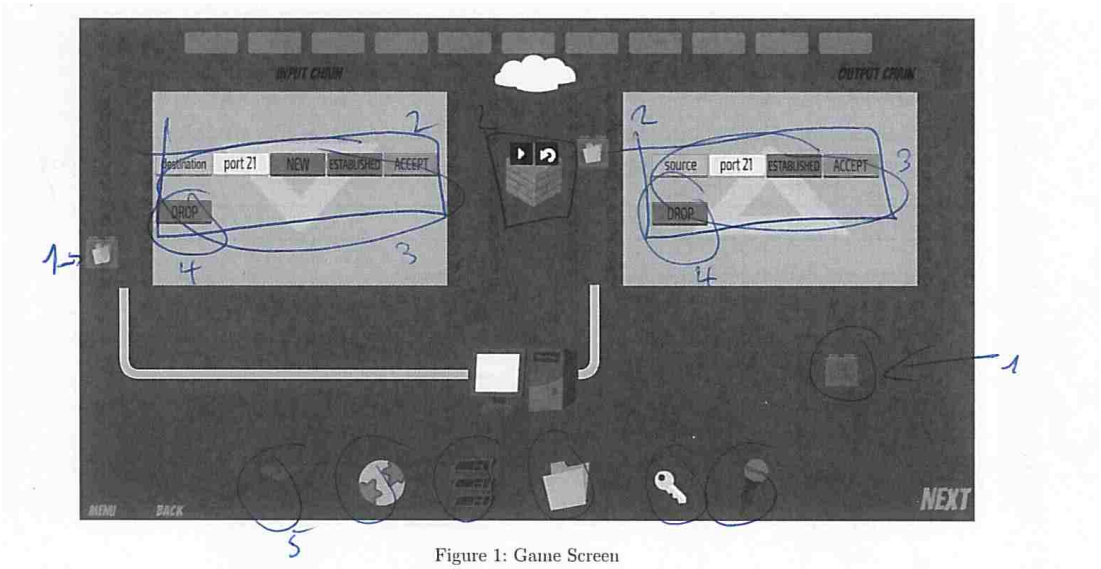


Figure 7.2: P4's correct labels of the game screen where (1) identifies packets, (2) describes everything part of the Firewall, (3) describes a rule, (4) describes a default policy and (5) illustrates the services

see whether he could interact with the packets until realising that the dropped packet went to the bin to be destroyed.

The second level presented an increased challenge to the player because the user was required to build up a rule at both the INPUT and the OUPUT chain and set a default policy. The tutorial screens preceding the level gave the user information on chains, rules and how the rules are read. It also gave the user concise instructions on what exactly he had to implement in the game as to not overwhelm the user. Despite the slots in the INPUT and OUTPUT chain area being colour shaded in the same colour as the building blocks at the top, P1 and P3 did not initially make the connection between the colours. Since both of the participants had experience in Computer Science, it is unlikely that they did not make the connection due to less experience with the computer. P2, P4, and P5 all matched the colours of the building blocks with the rule which helped them to accomplish the level faster than P1 and P3.

Each participant, regardless of their background, had problems to correctly place destination within the INPUT chain and source at the INPUT chain in Level 2. This problem occured despite the tutorial screen specifically stating

"destined for port 80" and "originating for port 80" in the different quests. This problem still occured in later levels for each of the participants, although they recovered quicker from the error. By the time they reached level 6, all participants successfully managed to make the distinction.

P2, P3 and later P4 also had initial trouble in recovering from their error when placing first ESTABLISHED and then NEW (intended was the other way around) in the INPUT chain. They could not recall reading from the instruction on the previous screen that the blocks should go in the opposite order. Unfortunately, the robot's feedback did not check for this specific error which made it harder to figure out for them where their mistake occured exactly given that all the other blocks were placed in the correct fashion and colours matched accordingly. P4 was the only participant that made use of the Back button to review the assignment given to him and noticed that New has to go before Established and recovering from his error.

Level 9 which presented the players with an ACCEPT default policy and the task of blocking a malicious IP address again highlighted that identifying source and destination presented problems for the players. It appeared that players were used by now to placing destination and source at INPUT and OUTPUT chain respectively, whereas Level 9 required them to put them the other way around. This time I had implemented feedback for these two wrongly assigned building blocks as I had anticipated this problem, so the participating players could easily recover from this error. P4 seemed to have thought that he was smarter than the game and had forgotten that the IP address belonged to a malicious sender. P2 seemed interested in how once can spot a malicious or suspicious IP address and I explained to her that certain numbers indicate suspicion and that there are directories on the internet summarising which IP addresses should warrant special caution. Given that P2 had no previous knowledge, this interest was seen as a positive learning experience that extended beyond the game itself.

P4 also explained during game play that he could just colour match and "win the game anyway". This was echoed by P1. Both participants had computer security and computer science knowledge, so it is not surprising that they found the repeating levels teaching about services easier than P2 and P3. However, the

last level also presented great difficulty to them with both, P1 and P4, verbally regretting, cursing and then laughing that they did not pay attention enough and thought that they outsmarted the system. P5 was the only player to successfully complete this level without making any mistakes and also completed it the fastest.

Players all verbally regretted that the Robot did not congratulate them after finishing the level, which could not be implemented by myself due to time limitations. The completion time of the game also varied greatly with P1 taking around 23 minutes, P2 taking 33 minutes, P3 taking 38 minutes, P4 taking 26 minutes and P5 only taking 13 minutes. These different completion times correspond roughly with the users' experiences.

7.3.3 Post-game questionnaire

Knowledge of firewalls according to participants after playing the game

Knowledge of the term firewall itself and why it is needed did not change for any participants. However, participants that previously indicated that they did not know how a firewall operates now provided an answer. Participants included answers such as "A firewall has rules and checks whether packets match these" by P2 who previously indicated that she did not know anything about Computer Science or Computer Security. P2 also learned about the term "packet" from playing the game and afterwards could accurately describe them.

Knowledge of firewall related terminology after playing the game

All participants checked more correct answers in the firewall related terminology questions and also indicated that more terms on average sounded familiar to them (Question 16). All participants could correctly identify that firewalls use rules, policies, ports and read IP addresses. P2 could not explain what a chain is exactly and did not indicate that this word sounded familiar to her. P3, P4 and P5 could illustrate that a chain is a "a set of rules" (P3) that are being made related to incoming and outgoing traffic.

Ability of reading an iptables command after playing the game

The ability to understand parts of the iptables command increased after playing the game for all of the participants. Even P2 who has no Computer Science or Security background could accurately describe what the commands meant.

Ability of differentiating between Input and Output rules after playing the game

Through interacting with the game and identifying source and destination ports within the game and completing the assignments, participants could explain the difference in the post-test. P5, who left the explanation blank in the pre-test, explained that the "Input rule specifies which packets are allowed to enter the system. Output rule specifies what is allowed to leave the system".

Understanding of the interface after having played the game

P1 did still not identify packets correctly, despite his knowledge of computer science and security. Every other participant correctly identified the packets again. P1, P2, P3 and P4 could now identify that the INPUT chain and OUTPUT chain areas were part of the firewall whereas P5 could not. Four participants could correctly identify a rule after playing the game, with the exception of P1 who circled "Established". The default policy was correctly identified by P2, P3 and P4. The identification of services was mixed and only P2, P3 and P4 correctly identified these. Figure 7.3 shows P2 (who was inexperienced in Computer Science and Computer Security) understanding of the interface after playing the game.

Results relating to the usability of the system

The average score for the SUS for the ten participants was 88.25, which is generally considered a high degree of usability. Non-Informatics participants found the system slightly less usable at 86.25, whereas Informatics participants considered the system usable at 91.25. Moreover, female participants also considered the system more usable at 89.167 whereas male participants gave the system an average score of 87.857. All of the individual results can be found in table 7.2.

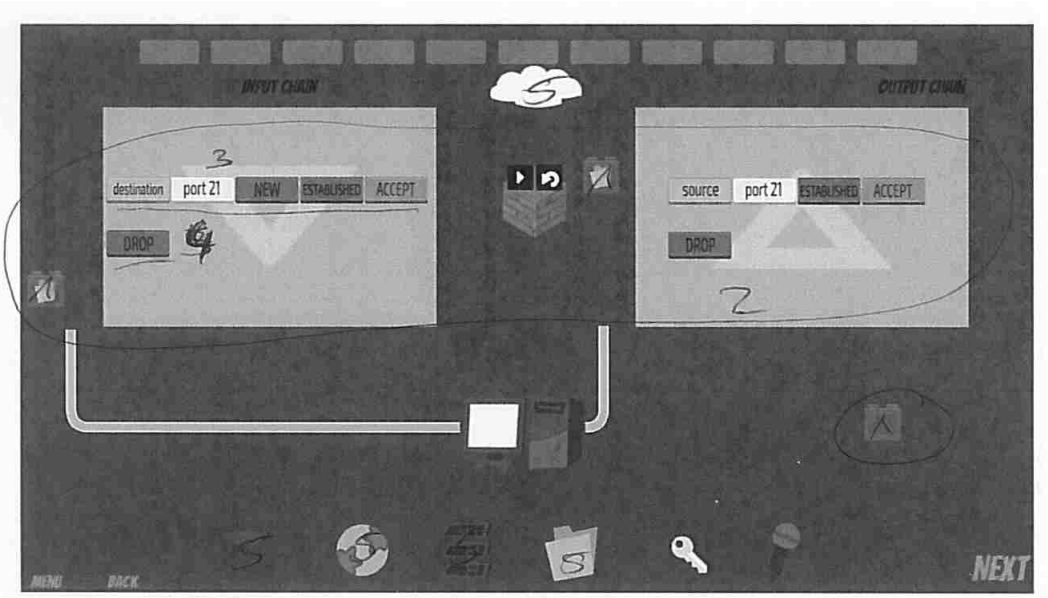


Figure 1: Game Screen

Figure 7.3: P2's almost correct labels of the game screen after playing the game where (1) identifies packets, (2) describes everything part of the Firewall, (3) describes a firewall rule, (4) indicates a default policy and (5) illustrates the services - the cloud is mistakenly seen as a service too despite it indicating the Internet

Other comments

P1 did not seem to understand that the block in the middle was used to represent a visual firewall and asked for further clarification on it. P2 wished for further clarification on the bins. P3 indicated that he learned a lot and enjoyed playing the game. P4 described the game as "beautiful". P5 described the game as "cute".

7.4 Discussion

The results have shown that certain learning objectives as defined in section 4.3.2 have been achieved after playing the game for the five participating users.

New terminology was acquired and certain terminology like: rules, default policy, ACCEPT, DROP, packets were not only introduced to the participants and recalled but participants could explain these in the post-test and correctly identify them in the interface. This is visible from a statement by P2: `A packet is`

ID	SUS	Age	Gender	CS knowledge	Security knowledge
P1	90	22	Male	Yes	Yes
P2	87.5	23	Female	No	No
P3	87.5	28	Male	Yes	No
P4	92.5	22	Male	Yes	Yes
P5	95	26	Female	Yes	Yes
P6	82.5	26	Male	No	No
P7	85	24	Male	No	No
P8	90	23	Male	No	No
P9	85	56	Female	No	No
P10	87.5	56	Male	No	No

Table 7.2: Participant mappings of ten respondents, their SUS score and their background information

`data which is put through the firewall under rules which are set`.

This statement does not only show that this participant, who had no computer science knowledge or computer security knowledge, now understands what a packet is, a term previously unknown to her, but also understood that the packets are filtered at the firewall according to the rules she had set in the game. P2 could also correctly identify that default policy was: `A set rule to go through at the end` which indicates a certain understanding that each packet is evaluated against "this special rule" if not matching any previous rules. P3 also noted that DROP constitutes a default policy which is interesting because it indicates that he thinks that DROP is the more sensible choice after playing the game.

P2 is of special importance in this evaluation since she has no computer science or computer security knowledge and thus aligns perfectly with the target demographic as defined in the learning goals and requirements gathering phase. P3 is also a potential user who would be more likely to come into contact with the game, as opposed to P1, P4 and P5. I had not anticipated that P2 would understand the *iptables* command in full after playing the game, which I expected the experienced users to learn. However, both P2 and P3 could correctly provide some information on the *iptables* command. While the terminology of rules and

default policy have been understood and correctly applied by both P2 and P3, shortcomings in terms of learning have been identified for term protocol and in parts ports.

In general, the participants seemed a bit unclear how ports, services and protocols were related. While they did understand that the port was indicating letting through specific packets for a particular destination, it did not appear clear to them how they were related to a protocol. It might be that the terms protocol and services confused people at this stage and that they should either be left out, or that more efforts should be taken to explain them better. Watching the videos of the gameplay also revealed that people had trouble initially to specify destination at the INPUT chain and source at the OUTPUT chain but this improved throughout playing the game.

The last level (Level 10) that the participants had to solve during the gameplay, proved more challenging for new learners and easier for people with a computer science background. The increased difficulty of providing the user with more building blocks to select and choose from and removing the color shaded slots in the INPUT and OUTPUT chain areas, proved too difficult for new learners. Even more experienced participants such as P4 initially faced problems after relying on the colour shaded slots. This might identify that more scrutiny should be placed on when the blocks should be coloured in and removing them earlier to encourage learning where the blocks should be placed.

Watching the gameplay as well as looking at the participants' answers in the post-test also revealed that most of them understood that you are writing rules for the packets and that the packets are matched against the rules in order, before the default policy at the end decides what happens to the packets when no further rules are specified. Learning to classify packets, and that based on this classification certain actions happen, was part of the learning objectives and it is useful to see that this learning objective could be achieved.

On the other hand, the game did not provide the participants with ample room to think about conceptual, ordering and threat errors as was first anticipated when defining the learning goals in Section 4.3.2. I could not include all of

these in the time I had been given and had thus not included them in the game which was shown to the participants.

As can be seen from some of the participants feedback, they thought that the game provided a friendly learning environment. Written comments such as "I learned a lot" as well as "beautiful" and "cute" alongside oral feedback that they enjoyed the game and interacting with it, show that the participants felt that the environment provided to them was a friendly one. As the learning goal was to create a friendly environment rather than an environment that would pose them to abandon a task or scare them to make mistakes, this learning goal could be seen as being achieved successfully.

In terms of usability, the game seems to be generally considered usable and easy-to-use by all participants. The indicated overall average of 88.25, as well as the averages for male vs female and non-Informatics vs Informatics participants, were all reasonably high and indicate general satisfaction of the participants. A score of over 70 is generally considered normal (Bangor et al., 2009), which illustrates that the created game is scoring above average. It is worth noting, that ten participants do not constitute a large sample size for making general statements but they can give an indication of the overall consensus.

Participants that did not have a background in Informatics found the game slightly less usable (86.25) than those who did (91.25). A potential reason might be the added complexity of learning about the content of firewalls in the game. This added complexity might lead them to believe that they require more knowledge beforehand or do not feel as confident about their abilities.

Chapter 8

Conclusion

This dissertation provides an investigation into the use of video games in the educational context of firewalls and into the development of a game to teach concepts and learning related to firewalls. In the beginning, the existing literature was analysed which laid the foundation work for the requirements gathering phase. The requirements gathering phase explored many potential teaching areas for firewalls, but concluded that exploring how firewall terminology and concepts could be taught to beginners in a game context would be most useful. A first and second design phase followed the requirements gathering phase and were improved iteratively to ensure best practices were being followed. Continuous feedback from users and experts was sought to ensure that the result of the second design phase was an enjoyable and useful game. Finally, the created game was evaluated with different users to identify whether new knowledge has been acquired and whether the game adheres to usability principles.

This chapter concludes the dissertation and will provide answers to the research questions outlined in the first chapter as well as provide any future work that might be conducted in the future, in relation to work that could not be completed in the time frame available or future work that could be improved upon based on the evaluation with users.

8.1 Research Questions

The research questions that were laid out in the introduction of this dissertation provided the rationale for the research in this dissertation.

1. Is a video game suitable to teach a target group of beginners and novices about firewalls?
2. Has the target group increased their knowledge and learning according to the learning goals identified?
3. Can the target group identify firewall terminology and concepts?

The literature review has proven that educational games in the form of board games or video games can be a powerful tool in education, especially to teach complex and material considered "difficult" or "boring" in a computer security context. As video games have proven useful and enjoyable, and offer the chance for a novice to learn without the fear of playing against more advanced players and immerse themselves in the learning environment, video games are deemed a suitable tool to teach beginners and novices. This was also reinforced by experts in the security context that were of the opinion that a video game could be a powerful tool if specifically tailored to the learning objectives of the target group. The evaluation I conducted in Chapter 7 also suggests that less experienced participants or beginners feel comfortable in playing a video game and find a video game an enjoyable experience.

While the first design phase fell short of its learning objectives and captivating a beginner's attention, I placed special emphasis on taking feedback from the first design phase as well as expert feedback into account for the second design phase. Most of the decisions made in the second design phase were based on the literature, expert feedback, user feedback or common practice in HCI to ensure that a well rounded product was being developed.

To measure whether this game is suitable for teaching novices in terms of usability, the game was evaluated using the System Usability Scale. Findings suggest that users find the game very usable and easy to use, scoring above average for all of the participants.

The user evaluation contains promising results in terms of knowledge and learning, which indicated that absolute beginners and those with a limited background could correctly learn terms and their explanation within the game context. The evaluation revealed that these participants not only learned new words but

also learned on a conceptual level how firewall rules are constructed and how incoming and outgoing traffic of packets is evaluated using rules and a default policy.

The target group did not learn at this stage to identify errors and classify between: conceptual, threat and ordering errors, as this particular learning objective was not fully implemented into the game.

8.1.1 Discussion

The research I provided in this dissertation constitutes a step towards the exploration of using video games to teach the topic of firewalls to beginners. It aims to build upon the existing literature that focused on computer security and provide a rationale on how video games can be used to teach difficult and complex topics to a novice. While certain learning goals were achieved, the game cannot be considered complete and many adjustments can be made to improve it.

8.2 Limitations

The evaluation of the video game I have built during the second design phase was conducted with a small sample of users (n=5). One cannot extrapolate from this small sample of users to the general public and assume that they behave in a similar fashion as users from a similar background in the evaluation. Given that there is a very limited amount of work in the area of games and in particular video games about firewalls, this research can mainly serve as a first investigation into the topic and will require further work in the future.

8.3 Future Work

In terms of future work there are roughly two aspects to consider: work that could not be completed due to time limitations and areas of improvement identified in the evaluation. The game in its current form only teaches beginners a limited amount of knowledge and more levels could be developed by myself or others to reflect more complex problems. While the last level in the game (Level 10) aims to assess more complex problem solving, more levels of this sort should be created to keep the user engaged and apply the knowledge he has learned.

More levels that apply to the learning goal of educating the user about conceptual, ordering and threat errors should also be created in the future, since the created game did not explore this in the necessary fashion due to time limitations. More work on how these might be presented to a beginner might be necessary, as adding these errors will certainly increase the level of complexity.

Several design improvements could also be made to emphasize certain aspects of the game. The services could be visually connected by cables to the computer as to make obvious that they lie on the path of the packets. One could also think about placing another visual border around both the input and the output chain to make clear that they part of the firewall as not all participants in the evaluation connected these immediately.

A screen that congratulates the user at the very end of the game as well as a stronger reward system or point system should also be integrated into the game, both of which were not included due to time limitations of the project. Especially if the game grew in size, a reward system would be essential to keep up the player's motivation.

The evaluation also showed that some of the explanations of difficult and new terms could be improved further, to explain certain terms such as ports and protocols better and distinguish them from others. Further testing on the actual content of the tutorial screens could also be conducted to ensure that a maximum amount of learning is taken away from them.

Appendix A

Example consent form

RT Number: 1961

Evaluation Consent Form

As part of my MSc thesis work I am creating a video game for beginners in Computer Security, in particular Firewalls. The outcome of this evaluation will help me to improve this game effectively.

Today I will be asking you to play a version of this game. I will also ask you to give some feedback on some of the game elements and the game play and to share any other opinions you may have.

Ideally, I will be audio and video recording the game playing session, although this might not be the case. The video recording will focus on the video game itself and how you are interacting with it, but may also capture some video of you as well. If you want to say something and not have it recorded, then you may either ask me to stop the recording or tell me that the next bit should not be quoted.

Recordings and the output of the evaluation will be used by my research group to learn about security game play so that we can design a game that is likely to be helpful to students. The audio and video will be kept for a maximum of one year and then destroyed. Anonymized quotes from the audio or short non-identifiable video clips may be retained longer for use by future students on this project and presentations.

The project is supervised by Dr Kami Vaniea (kvaniea@inf.ed.ac.uk) and conducted by myself, Sibylle Sehl (s1133167@sms.ed.ac.uk).

[ ] I understand that I am participating in a study as part of the “Firewall Administration – the game” project.

[ ] I am willing for the video and audio to be digitally recorded and transcribed for the use as part of the research project.

[ ] The researcher may use **audio quotes** from this session in publications provided that the quote is anonymised and cannot be connected back to me.

[ ] The researcher may use **video clips** from this session in publications provided that the video segment is not associated with my name or identity.

Interviewee: _____ Date: _____

Interviewer: Sibylle Sehl Date: _____

Contact details:
Sibylle Sehl, email address: s1133167@sms.ed.ac.uk

Appendix B

Requirements gathering documents

Semi-Structured Interview Script

Firewall Administration Interview Questions

Hi, my name is Sibylle and I am writing my dissertation on Firewall Administration and trying to understand which problems could arise when configuring Firewalls and the vulnerabilities you might face. I am also interested to know what aspects of Firewalls you think should be taught better or are not well understood. Your contribution to this study for my dissertation is extremely valuable for me, and thus I would like to ask for your consent for taking audio and video recordings and photographs. Please be rest assured, that this purely for data gathering purposes and that your data will be treated confidentially. But enough of the technicalities. Now I would like to know a bit about yourself.

Easy introduction questions

1. Details (Name (don't disclose), Gender, Field of work and job title, Years of Experience/ time in current job.), size of organisation (<10, >100, > 500).
    a. Ask the participant how they are feeling today: Indicates how they feel in the interview situation
    b. What are your interests/ goals?
    c. What do you do in your free time?
2. What does your typical day at work look like?
3. How would you describe the concept of a Firewall to non-experts?

Main body questions:

1. Tell me about the last time you had to edit a Firewall rule.
    a. How did you know you have to change it?
    b. Is there an email as an example?
    c. Can I see it?
    d. How were you certain that your modification is correct?
    e. Who did you communicate with?
2. Tell me about a time when you had a lot of difficulty editing a firewall rule.
3. Tell about the last time when you had to teach someone.
    a. What would be the most valuable things to learn?
    b. What would be the first?

I'm trying to put together a video game to teach students about firewalls and would like to include a story to support the learning and reinforce the learning experience. I want to focus on iptables.

4. Do you think a story is a good idea to teach Firewalls with?
5. Which elements do you think are crucial to include?

6. How important do you think it is to include the relationship of the System Administrator with the rest of the team?
7. What modes of interaction do you think should be supported? Manipulation (button pressing, zooming etc)/ Instructing (writing commands), Exploring or Conversing? Gui/ Command line etc
8. Which aspects of a storyline do you think are most important to include?

Easy questions to diffuse tension

Closure:
I think this brings us to the end of the interview. Do you have any remaining questions or remarks?
(Two alternative scenarios)

1. Alternative questions
    a. Discuss questions and provide reasonable answers
2. No remaining questions

→ Well then, thank you very much for your contribution in our research and taking the time out of your busy day to talk to me and share your insights with me.
(switches recorder off)

[d0x3d!] Workshop - Simplified Rules

Aim of the game: Your digital assets such as personal identifiable information, financial data, intellectual property and authentication credentials have been stolen and now you want to get them back. However, your opponent is clever, and you have to move through the network undetected and recover your assets and then escape.

[d0x3d!] is **played collaboratively**: meaning we either all lose or all win together.

First each player, picks a hacker role.
Each role has special abilities - can be move or exchange rules. The roles on offer are:
cryptanalyst, war driver, social engineer, insider, malware writer and botmaster.

When it is their turn, each player has to follow the following 4:

1) Take 3 actions
2) Draw 2 loot cards
3) Draw patch cards (2 - 5 depending on INFOCON Level)
4) Check and discard

Actions available:

- Compromise
- Move
- Drop - can drop a loot card on the current tile
- Pickup - can pickup a loot card on the current tile
- Give when on same tile
- Exchange when on same tile
- Recover (meaning you “pay” with 4 equal cards to get back the digital asset)

You can take 3 actions in your turn

Loot cards:

- Zero day exploit: can be used to comprise any card, stop a decommissioning attempt or block a patch. Must also be played by 1 person when finishing the game
- Honeypot audit: draw patch card - if node is compromised, you’ve been spotted → raise the infocon level
- Intrusion detected: raise the infocon level

Patch cards:

- If no pawn on tile, just flip it over to uncompromised again
- If pawn on tile, hacker must move to compromised tile immediately, then tile gets decommissioned = meaning tile and patch card removed from game; if no move possible → game ends.

Game ends:

- If infocon level 1 is reached
- Or if it becomes impossible to win:
    - Internet gateway tile is decommissioned
    - Hacker is ejected from network (i.e. can’t move after patching)
    - Both capture points for one asset are decommissioned

To win:

- All digital assets must be recovered
- All players must occupy the internet gateway node
- And someone needs to play a zero day exploit.

Occupation: If Student, which year:
Age band: Gender:
Years of Experience:

1. What is your experience with computer security and computer networking?

2. PRE: If those are 5 tiles of the game, how would you arrange them?

3. What is your experience with firewalls?

4. Which role does the firewall play in the network?

5. Which part of the network does the firewall protect?

6. How does the Firewall achieve this?

POST ONLY (and if has been played in random mode):

7. What would a harder board look like in your opinion?

MiniForum 2 Lvl 4 - 10 am, 7/6/17

Timeline and Introduction to Session

1) **Introduction (2-3 min)**

Hi everyone, my name is Sibylle. I am a MSc student in Computer Science and I am writing my dissertation on Firewall Administration and trying to understand which problems could arise when configuring Firewalls and which aspects of it are not well understood.

Today, I will play a network security board game with you all, called [d0x3d!], and later gather some opinions on your experience.

Your contribution to this study for my dissertation is extremely valuable for me, and thus I would like to ask for your consent for taking audio and video recordings and audio recordings.

Please be rest assured, that this purely for data gathering purposes and that your data will be treated confidentially. The resulting data will be anonymised and every effort will be taken that no video footage can be attributed to yourself. If you do not feel comfortable at any point, just let know and you can stop your participation at any point.

Equally if you have any questions, just let me know and I will do my best to answer them.

2) Pre- Post Test Questions (5-7 minutes of filling out)

3) Game Play (30 minutes)

4) Pre-/Post Test Questions (5-7 minutes of filling out)

5) Focus Group (15 min)

- What did you like about the game?
- What could be improved?
- What did you think of the level the game is pitched at?
- Did you think the game lacked anything that you consider crucial?

I want to develop a video game that helps you to understand crucial concepts in firewall administration that you would encounter in a sysadmin position. I aim to have a certain narrative and scenario/ story to it, to make it engaging so you likely pick the game up again. Some of the ideas I have so far:

- “Leveling up”: slightly increased difficulty
- Reactive changes, new developments etc
- Choosing actions from set of options (hidden vs explicit)
- Change btw third person and first person view (when first person: email)

Appendix C

First design phase documents

Pre - game questionnaire

1. What is your gender?
   - ☐ Female
   - ☐ Male
   - ☐ Prefer not to say

2. What is your age in years? _____

3. What is your current degree level (highest obtained to date) ?
   - ☐ High School diploma
   - ☐ HND
   - ☐ Bachelors degree
   - ☐ Masters degree
   - ☐ PhD
   - ☐ Prefer not to say

4. I feel confident in using the internet safely.
   - ☐ Mostly Agree
   - ☐ Agree
   - ☐ Disagree
   - ☐ Mostly Disagree

5. Others ask me for help when they face problems with the computer.
   - ☐ Mostly Agree
   - ☐ Agree
   - ☐ Disagree
   - ☐ Mostly Disagree

6. When I encounter problems, I know how to fix them on my computer
   - ☐ Mostly Agree
   - ☐ Agree
   - ☐ Disagree
   - ☐ Mostly Disagree

7. I play video games
   - ☐ Daily
   - ☐ Weekly
   - ☐ Monthly
   - ☐ I do not normally play video games

8. What would you say is your current level of knowledge of Computer Security?

9. What would you say is your current level of knowledge of Computer Networking?

10. Describe in a few brief sentences what a firewall does.

This is a screenshot from a particular level of the game.

1.Can you identify the beige packet and which direction it is heading?

2. What do you think about the look and feel of the packet?

3. What do you think the rectangle signifies and why does it turn green?

4. Does the order and syntax of the rectangles/ boxes remind you of something?

5. What do you think about the appearance of the rectangles? Would you change anything, and if so, how?

6. Do any of the words on the screen seem familiar to you? If so, what do they generally mean?

7. What do you think the purpose of the little robot on the screen is?

8. What do you think about the little robot and its appearance?

9. If you have any other comments or ideas that should be included in the game, draw them in here and provide a bit of information on why you think they should be included.

Post - game questionnaire

1. Describe a few components of a firewall rule and how they are related to each other.

2. Outline briefly what the packets are doing and what they are used for. If you can, outline two different types of packets.

3. Can you mention the terminology that allow a packet to pass and that blocks it from entering?

4. Does the robot's task/ instructions seem clear to you? What are you supposed to do?

5. Can you mention why the boxes appear green after a while?

6. Do you have any comments on the general appearance of the game elements?

7. Is there anything that seems unclear to you? If so, please explain and draw what you think is missing.

Focus group questions

1. Which aspects did you enjoy about the game you played?
2. Which aspects did you not enjoy about the game you played?
3. Is there something that confused you when playing the game?
4. Would you play a game about computer security in your free time?
5. Is there anything else that you think should be included in the game?

This is a career map that is going to be shown to you, in between the levels.

What do you think this is showing you?

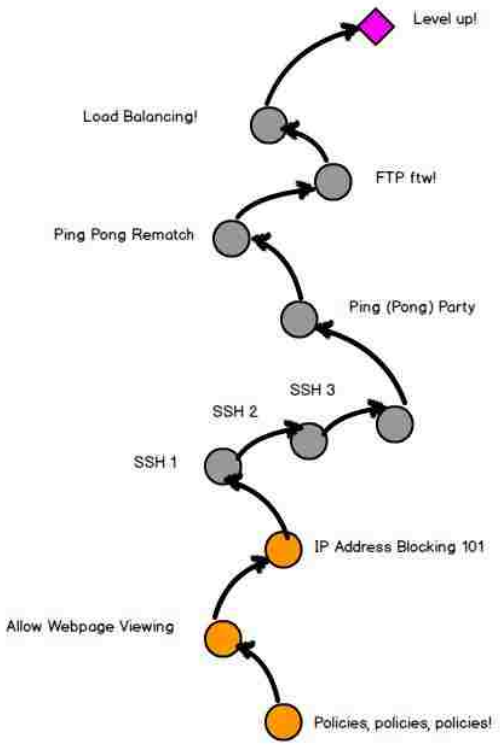
Does it encourage you to keep going and reach a milestone?

Can you tell which current grade you possess and how many levels you have completed?

Welcome back, Novice!

Player 1

Complete the remaining assignments of the Novice track to become Apprentice and unlock more skills!



Back to Main Menu

Appendix D

Second design phase documents

Semi-Structured Interview Script

Game Design Interview Questions

Hi, my name is Sibylle and I am writing my dissertation on Firewall Administration and I am looking to understand which problems could arise for beginners when trying to understand the basics of Firewalls. I am creating a video game for teaching language and concepts and I am interested to know what aspects of Game Design you think should be included in the development process in order to guarantee a successful game creation. Your contribution to this study for my dissertation is extremely valuable for me, and thus I would like to ask for your consent for taking audio recording. Please be rest assured, that this purely for data gathering purposes and that your data will be treated confidentially. First, I would like to know a bit about yourself.

Introduction questions:

1. Details Gender, Field of work and job title, Years of Experience/ time in current job.), size of organisation (<10, >100, > 500).
    a. What are your interests/ goals?
    b. What do you do in your free time?
2. What does your typical day at work look like?

Interview Questions:

1. Tell me about the most important concepts of game design you find crucial to know about.
2. Do you think certain game design principles work particularly well, e.g. reflection learning (time to reflect), story based agent environment (have a character)
3. Could you comment on the importance of feedback (for correct/ incorrect answers)
4. What would be the first aspects to decide on when making a game?
    a. Rules, world, aesthetics, content production, levels, UI?
    b. Rule and Content?
5. Tell me about the last time you had to teach someone about Game Design.
    a. What was the most difficult thing for them to understand?
    b. What would be the most valuable thing to learn?
    c. What would be the first thing to learn?
6. Can you tell me about some commonly made mistakes and how to avoid them?
7. Are there any great resources you would recommend?

Closure:
I think this brings us to the end of the interview. Do you have any remaining questions or remarks?

Thank you very much for your participation!

Appendix E

Evaluation documents

Evaluation questionnaire

Thank you for agreeing to fill out this questionnaire and taking part in the evaluation of my project.

Please be rest assured that all the data is anonymous and cannot be traced back to you. The data is collected for research purposes only and helps me to understand your knowledge and background.

About you

1. **How old are you?** I am _____ years old.
2. **What is your gender?**
   - □ Female
   - □ Male
   - □ Other
   - □ Prefer not to say
3. **Which of these describe you best:**
   - □ Informatics MSc Degree with Computer Security knowledge
   - □ Informatics BSc Degree with Computer Security knowledge
   - □ Informatics MSc Degree without Computer Security knowledge
   - □ Informatics BSc Degree without Computer Security knowledge
   - □ PhD student
   - □ Other MSc or MA degree
   - □ Other BSc or BA degree
   - □ Other: _____

Please answer the following questions

4. **I have heard the term Firewall before** □ Yes □ No
5. **If you selected Yes, please give details**

   _____

   _____
6. **I know roughly why my computer needs a firewall** □ Yes □ No
7. **If you selected Yes, please give details**

   _____

   _____
8. **I know how a Firewall operates** □ Yes □ No
9. **If you selected Yes, please give details**

   _____

   _____
10. **I have heard the term packet before** □ Yes □ No

11. If you selected Yes, please give details

---

12. Please select tick all the statements that you think are correct.

Firewalls ...

- ☐ use chunks
- ☐ use rules
- ☐ depend on order
- ☐ can identify any malicious packet in any given situation
- ☐ have laws
- ☐ combine the same packets
- ☐ have a policy
- ☐ use stations
- ☐ use ports
- ☐ can read an IP address
- ☐ can identify new packets
- ☐ can select products
- ☐ can select services

13a. What do you think a default policy is?

14a. Can you try and tell me what this expression means and what the different words mean to you?

iptables -A INPUT -i eth0 -p tcp –port 443 -m state –state NEW,ESTABLISHED -j ACCEPT

15a. Please explain what a protocol is. If you do not know, please leave it blank

---

---

16. Please indicate which of these words sound familiar to you:

- ☐ Mail
- ☐ DNS
- ☐ IP Address
- ☐ Hyper Text Transfer Protocol (HTTP)
- ☐ Web
- ☐ Simple Mail Transfer Protocol (SMTP)
- ☐ Secure Shell Protocol (SSH)

- □ Ports
- □ File Transfer Protocol (FTP)
- □ Chains

17a. If you can, please explain the difference between an INPUT rule and an OUTPUT rule.

18a. Do you put default policies at the top or at the bottom?

19a. If you can, briefly explain what a chain is.

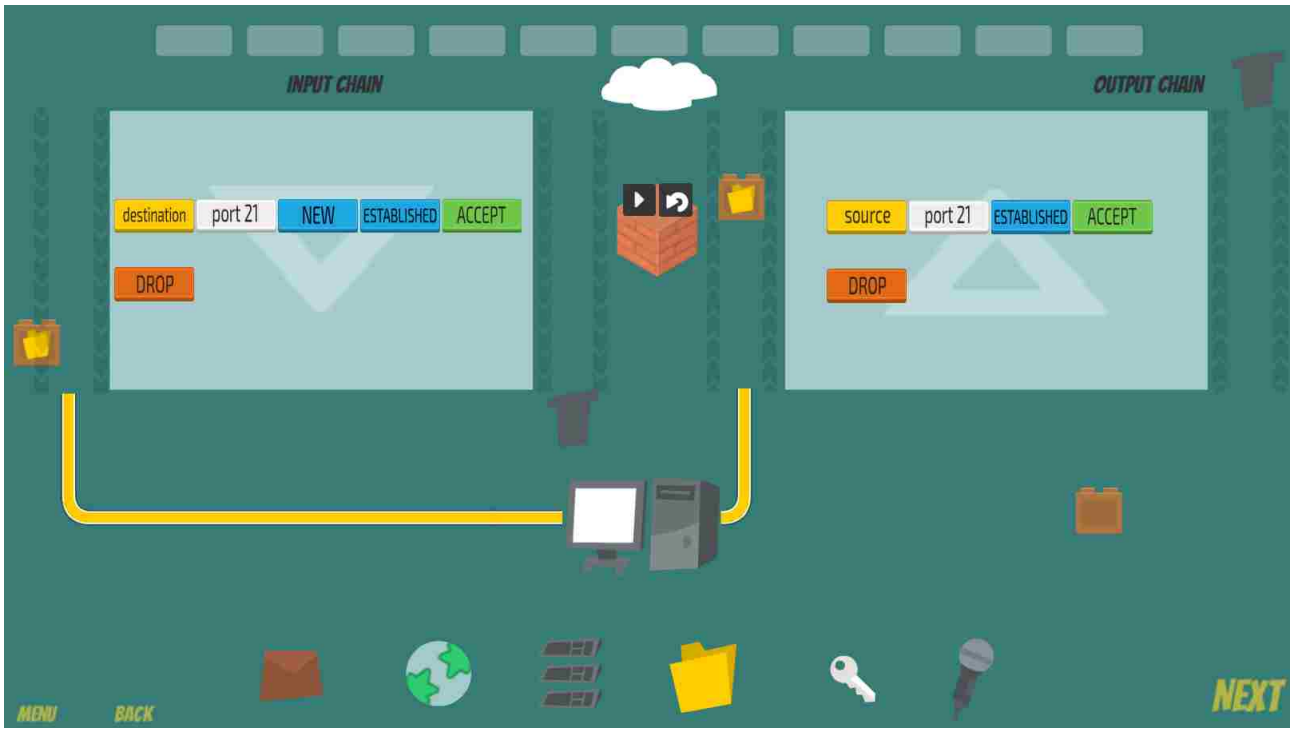


Figure 1: Game Screen

Figure shows a screen from the game I created as part of my MSc thesis. Please try and answer the below.

20. Please indicate what a packet is or what the packets are on the screen by labelling them with (1)

21. Please draw a circle or rectangle around everything that is part of the firewall and label it with (2)

22. Please draw around a rule and label it with (3)

23. Please draw around a policy and label it with (4)

24. Indicate the service(s) that you can see on the screen and label them with (5)

25. What do you think the cloud is representing?

26. What do you think the bin is doing on the screen?

27. If you have any other comments, please leave them below

User Feedback Sheet

Thank you for agreeing to fill out this feedback sheet and taking part in the evaluation of my project. Please be rest assured that your data will remain anonymous and cannot be traced back to you.

Please answer the following questions

1. **I think that I would like to use this system frequently**
   Strongly disagree □—□—□—□—□ Strongly agree

2. **I found the system unnecessarily complex**
   Strongly disagree □—□—□—□—□ Strongly agree

3. **I thought the system was easy to use**
   Strongly disagree □—□—□—□—□ Strongly agree

4. **I think that I would need the support of a technical person to be able to use this system**
   Strongly disagree □—□—□—□—□ Strongly agree

5. **I found the various functions in this system were well integrated**
   Strongly disagree □—□—□—□—□ Strongly agree

6. **I thought there was too much inconsistency in this system**
   Strongly disagree □—□—□—□—□ Strongly agree

7. **I would imagine that most people would learn to use this system very quickly**
   Strongly disagree □—□—□—□—□ Strongly agree

8. **I found the system very cumbersome to use**
   Strongly disagree □—□—□—□—□ Strongly agree

9. **I felt very confident using the system**
   Strongly disagree □—□—□—□—□ Strongly agree

10. **I needed to learn a lot of things before I could get going with this system**
    Strongly disagree □—□—□—□—□ Strongly agree

About you

11. **How old are you?** I am _____ years old.

12. **What's your gender?**
    - □ Female
    - □ Male
    - □ Other
    - □ Prefer not to say

13. **Which of these describe you best:**
    - □ Informatics MSc Degree with Computer Security knowledge

- ☐ Informatics BSc Degree with Computer Security knowledge
- ☐ Informatics MSc Degree without Computer Security knowledge
- ☐ Informatics BSc Degree without Computer Security knowledge
- ☐ PhD student
- ☐ Other MSc or MA degree
- ☐ Other BSc or BA degree
- ☐ Other: _____

14. If you have any other comments, please write them down below:

_____

_____

_____

_____

Bibliography

Andreasson, G. (2006), 'Iptables tutorial 1.2.2'. Available at `https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html` (Accessed 05/06/2017).

Bangor, A., Kortum, P. and Miller, J. (2009), 'Determining what individual sus scores mean: Adding an adjective rating scale', *Journal of usability studies* **4**(3), 114–123.

Barrett, D. J., Silverman, R. E. and Byrnes, R. G. (2003), *Linux Security Cookbook*, O'Reilly.

Battistella, P. and Wangenheim, C. v. (2016), 'Games for teaching computing in higher education–a systematic review', *IEEE Technology and Engineering Education* **9**(1), 8–30.

Baylor, A. L. and Ritchie, D. (2002), 'What factors facilitate teacher skill, teacher morale, and perceived student learning in technology-using classrooms?', *Computers & education* **39**(4), 395–414.

Brooke, J. et al. (1996), 'Sus-a quick and dirty usability scale', *Usability evaluation in industry* **189**(194), 4–7.

Cheswick, W. R., Bellovin, S. M. and Rubin, A. D. (2003), *Firewalls and Internet security: repelling the wily hacker*, Addison-Wesley Longman Publishing Co., Inc.

Cho, K.-L. and Jonassen, D. H. (2002), 'The effects of argumentation scaffolds on argumentation and problem solving', *Educational Technology Research and Development* **50**(3), 5–22.

Cone, B. D., Irvine, C. E., Thompson, M. F. and Nguyen, T. D. (2007), 'A video game for cyber security training and awareness', *computers & security* **26**(1), 63–72.

De Aguilera, M. and Mendiz, A. (2003), 'Video games and education:(education in the face of a "parallel school")', *Computers in Entertainment (CIE)* **1**(1), 1.

Denning, T., Lerner, A., Shostack, A. and Kohno, T. (2013), Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education, *in* 'Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security', ACM, pp. 915–928.

Dondlinger, M. J. (2007), 'Educational video game design: A review of the literature', *Journal of applied educational technology* **4**(1), 21–31.

Druin, A. (2002), 'The role of children in the design of new technology', *Behaviour and information technology* **21**(1), 1–25.

Du, W. (n.d.), 'SEED labs'. Available at `http://www.cis.syr.edu/~wedu/seed/labs.html` (Accessed 16/06/2017).

Fisch, S. M. (2005), Making educational computer games educational, *in* 'Proceedings of the 2005 conference on Interaction design and children', ACM, pp. 56–61.

Flushman, T. R., Gondree, M. and Peterson, Z. N. (2015), This is not a game: early observations on using alternate reality games for teaching security concepts to first-year undergraduates, *in* '8th Workshop on Cyber Security Experimentation and Test (CSET 15)', USENIX Association.

Gondree, M. and Peterson, Z. N. (2013), Valuing security by getting [d0x3d!], *in* 'Workshop on Cyber Security Experimentation and Test, Washington, DC'.

Gondree, M., Peterson, Z. N. and Denning, T. (2013), 'Security through play', *IEEE Security & Privacy* **11**(3), 64–67.

Gouda, M. G. and Liu, A. X. (2007), 'Structured firewall design', *Computer networks* **51**(4), 1106–1120.

Hanington, B. and Martin, B. (2012), *Universal methods of design: 100 ways to research complex problems, develop innovative ideas, and design effective solutions*, Rockport Publishers.

Kandogan, E., Maglio, Paul P amd Haber, E. M. and Bailey, J. (2012), *Taming information technology: Lessons from studies of system administrators*, Oxford University Press.

Larman, C. and Basili, V. R. (2003), 'Iterative and incremental developments. A brief history', *Computer* **36**(6), 47–56.

Littig, B. (2013), *Expert Interviews: Methodology and Practice*, University of Tampere.

McFarland, S. G. (1981), 'Effects of question order on survey responses', *Public Opinion Quarterly* **45**(2), 208–215.

Microsoft (2013), 'Elevation of Privilege card game'. Available at `https://www.microsoft.com/en-us/SDL/adopt/eop.aspx`.

Mjartan, P. (2017), 'Firewall simulator as a webapp'. Available at `http://groups.inf.ed.ac.uk/tulips/projects/1617/FirewallWebApp/` (Accessed 16/08/2017).

Monk, T., Van Niekerk, J. and von Solms, R. (2010), Sweetening the medicine: educating users about information security by means of game play, *in* 'Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists', ACM, pp. 193–200.

Obama, B. (2009), 'Obama's remarks on cyber-security'. Available at `http://www.nytimes.com/2009/05/29/us/politics/29obama.text.html` (Accessed 16/08/2017).

Olano, M., Sherman, A. T., Oliva, L., Cox, R., Firestone, D., Kubik, O., Patil, M., Seymour, J., Kohane, I. S. and Thomas, D. (2014), SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education., *in* '3GSE'.

Oppenheimer, D., Ganapathi, A. and Patterson, D. A. (2003), Why do internet services fail, and what can be done about it?, *in* 'USENIX symposium on internet technologies and systems', Vol. 67, Seattle, WA.

Palacios, J. (2016), *Unity 5. x Game AI Programming Cookbook*, Packt Publishing Ltd.

Prensky, M. (2003), 'Digital game-based learning', *Computers in Entertainment (CIE)* **1**(1), 21–21.

Rogers, Y., Sharp, H. and Preece, J. (2011), *Interaction design: beyond human-computer interaction*, John Wiley & Sons.

Scalfani, C. (2016), 'Why experts make bad teachers'. Available at `https://medium.com/@cscalfani/why-experts-make-bad-teachers-ccaed2df029b` (Accessed 16/08/2017).

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J. and Nunge, E. (2007), Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish, *in* 'Proceedings of the 3rd symposium on Usable privacy and security', ACM, pp. 88–99.

Thompson, S. (2017), 'Firewall administration the game'. Available at `https://github.com/scottwthompson/Firewall-Administration-The-Game` (Accessed 16/08/2017).

Tristem, B. and Geig, M. (2015), *Unity Game Development in 24 Hours*, 2nd edition edn, Sams.

Unity Technologies (2017), 'Unity game engine'. Available at `https://unity3d.com/`.

Vaniea, K. (2016), *HCI: Study Design*, The University of Edinburgh.

Williams, L., Meneely, A. and Shipley, G. (2010), 'Protection Poker: The new software security" game"', *IEEE Security & Privacy* **8**(3), 14–20.

Wool, A. (2004), 'A quantitative study of firewall configuration errors', *Computer* **37**(6), 62–67.

Wool, A. (2010), 'Trends in firewall configuration errors: Measuring the holes in swiss cheese', *IEEE Internet Computing* **14**(4), 58–65.

Zwicky, E. D., Cooper, S. and Chapman, D. B. (2000), *Building Internet Firewalls: Internet and Web Security*, O'Reilly.