DDoS simulation through the process of game mechanics

Master Thesis

CLAES NIELSEN

Aalborg University Copenhagen

Medialogi

Aalborg University Copenhagen

Semester: Master thesis: Med 10

Title: DDos Simulation through the process of game mechanics

Project Period: 15/6-2018 to 10/9-2018

Semester Theme: Master thesis

Aalborg University Copenhagen
Frederikskaj 12,
DK-2450 Copenhagen SV
Semester Coordinator: Stefania Serafin
Secretary: Lisbeth Nykjær

Supervisor(s):

Lars Reng

Project group no.:

Members:

Claes Nielsen

Abstract:

In this thesis, research is being made into the background of hackers and hacking with the intent to find motivation aspect of fun and research there upon. Following the background area, a final problem statement is made with testable hypotheses. An artifact is built in the form of a simulation game for an autonomous web based split testing. Finally, when the results are analyzed through statically difference the problem statement is rejected through failure to reject the null hypotheses.

Table of Contents

INTRODUCTION

Currently in the world, almost every person walks around with cellphone in their pocket. But do they realize that every second they walk around that cellphone is sending signals out, even when requested not to. Technology is being used every single day, but most people does not see the danger around them. This is left for the hackers to see because just as they are the evil doers which will attack your phone and steal your data, these experts are also the ones providing your phone with the security that prevents this.

Currently in the world of hacking research there exist a typical of two angles. Either you test a system based on the theories made from earlier hack attempt to verify its security or what it can handle. Or it focuses on an individual or group which have a specific malicious intent of damage which they tried or will try again.

This Thesis aims to change this view on hackers, make it viewed that they exist not only as the malicious people news are reporting but also humans having fun and just curious about what technology will allow them to do. If hackers are just humans, is it may be possible that instead of building aggressive technologically heavy processes on our network. It all could diverted by simply making it not interesting anymore.

BACKGROUND

This thesis first aims to research the elements of the world of cyber security, the people and the mechanisms laying the ground of the industry and subject. This will help to form a final problem statement with testable and falsifiable hypotheses with requirements for later testing. This chapters will lay the foundation of knowledge that any person needs to know to follow the possible findings including the clarification of terms and definitions.

This background chapter seek to give an understanding of the foundation of people behind security and attacking, the current defense mechanics, and the motivation aspects for the malicious attackers.

MALICIOUS ATTACKERS

Terms related to the aggressors of IT security, i.e. the people attempting to attack the security for various reasons, are often used with the assumption of bad intentions. This section will define the general terms of hackers, and the action of hacking, ending examples of some of the worst cases found in history of malicious attacks. The purpose is to establish a beginning knowledge and understanding of the situation and terms used currently in the world.

DEFINITION OF HACKER

The term hacker is often defined as a person who can gain unauthorized access to other computer and networks. This is easily found to be the common understanding with a quick Google search. Per Christenson (BSc in Computer Science) [1], for example, has this definition, but also explains that hacker used to be defined as a person or individual who was an expert at programming. Oxford dictionary [2], which is a well-known dictionary for terms in all fields of knowledge, defines that the term hacker is currently referring to a person who uses computers to gain unauthorized access to data, focusing more on getting unauthorized access to the data and not the system itself. However, as this section will explain further, hacker as a term has history that has been buried by general assumptions. The goal is to get a better clarification and understanding of what the term really covers.

Business dictionary is made by the trusted Web Finance INC and have a unique and more personalized view on the term of hacker. It is defined as a skillful computer programmer who can break into computers through either password breaking or gaining remote access to a computer system (and not just a computer), often just for the thrill of it. Unlike most other dictionaries a difference is made between the term hacker and cracker, where a cracker is known to only perform criminal activities, a hacker may or may *not* perform criminal activities such as stealing data, unlike the Oxford dictionary that defined it only as an unauthorized activity.

By this point hacker already have connections to terms like programming, unauthorized access, network, systems and cracker.

In the paper from 2016 named "A genealogy of hacking" [3] Tim Jordan explains just how wide an understanding people can have on hacking. Examining chapter 2 "the golden age of CR/Hacking", Jordan gives a historical view of the time, where cracking and hacking was still distinct. Cracking was breaking into a system using engineering, while hacking was more about the explorative nature of technology, computers and network systems. However, as policies were being made to halt breaking into electronic systems, the lines were blurred. Only made worse by how hacking communities started showing up, talking about how they, purely out of the urge of the thrill, had managed to trick or find a weak spot to enter systems. This meant that while crackers might have an evil intent, a hacker was a person that might break into your system, but then tell you how to improve security and help you fix the issue to prevent it in the future. This did not mean that because hacking was for the intellectual gain that it was innocent, and the different names started to overshadow each other. As the cyberspace evolved and new policies were made to define laws and differences, hacking also evolved into a subject of amazing programming instead of simply curiosity. This evolvement took the last real step to make hacking and hackers take over the term of cracking fully because of cracking generally covers using flaws or social engineering etc. to break into systems. Hacking was now able to make advanced self-running programs like computer worms etc. which crackers would also use since they were better at breaking security.

All this is also referred to by the TechRepublic blogger Chad Perrin [4] who have written an article trying to simplify how the two words technically still have a difference in meaning and community of journalists and cyber security should retain from comparing malicious security crackers and term of hacker.

RESUME

The term hacker has had a while in the history of change. While the cyber world is evolving, so have the terms but not necessarily correctly for the common understanding. Hackers are not some inherently evil people, in fact hackers might never have used their abilities to gain unauthorized access to any data or systems. This paper will therefore consider the term hacker as a person with the capabilities of advanced programming and engineering that might include the ability to build security-breaking threats, but the term will also include the people who have never actually done so.

TECHNICAL EXPLANATION OF HACKING

Knowing what the term hacker means is one aspect, but the definition of hacking also has a meaning. Much like how hackers might be able to perform actions with bad intents, it is not always the case. Therefore, we need a clear explanation what hacking involves.

Cambridge dictionary's [5] attempt to define hacking fits very well with mentions from the definition of hackers, defined as an activity using a computer to gain access illegally to information stored in another computer system, but also very precisely define the act of spreading a virus as a definition of hacking.

In the paper from 2001 “Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated” [6] we can achieve a greater insight into how hacking functions on a multitude of planes. E.g., the thoughts of how hackers amongst many other things will attempt to use tools like “Nmap” to node a network before an attack - or the more complexed tools, like Netcat which can make a ping request look as if the server asked requested it to the hacker’s own computer and hide a command in the response to the server or system which when returned will be run. Further into the paper it looks at rootkits, which is an attack style targeted to the kernel of a system making it possible to modify core functionalities. Denial of service attacks (DoS) also known today more commonly as Distributed Denial of Service (DDoS) where you use already attacked computers (referred to as zombies in this report) to combine in an attack for a system. The paper continues through several other tools and terms of hacking including hacking web sessions. An example back from 2001 is made that though the connection might be encrypted by the system Secure Socket Layer (SSL), which we still know today, a hacker would still be able to highjack the session from a user by stealing their unencrypted IP address thus making the secure information being transferred to the hacker instead of the user. This paper introduces a multitude of new terms, which we will have go through later in the thesis. It also shows that gaining access to a system will take preexisting work and preparation and is not as easy as seen on the movies, where a person starting a command prompt that gives him or her access to writing a couple of lines which suddenly give them full access. All these tools have been combined in the internet tech magazine Lifewire [7] which have written a short article about some of the aspects that hacking touch to function, split into three main categories; *Brute force* which is fighting the actual defense system, forcing the system to give up or break down. *Social engineering attacks* which is based around getting secure information through people instead of the system like phishing emails and use the details received to walk into the systems, behaving as someone else. A*dministrator backdoors,* which as an example could be to take advantage of a master password used in programs debug files.

Like with the term hacker, hacking also seems to focus around the illegality and history of the terminology. Therefore, there is a history which define hacking as much more than simply fighting cyber security.

In the paper from 2016 “A genealogy of hacking” [3] mentioned earlier in this chapter, chapter 1 – “A History of Hacking: A Partial Presentation“ also helps define an earlier stage technical explanation of hacking. As mentioned earlier hacking evolved from being intellectual to about programming and started out as a method to use new technology in a manner it was not intended to do. This involved running complex railroads that was not designed to do this or finding signal tones for phones allowing you to call without paying. In the early stages of the term hacking it had no real connection to the cyberspace of computers, servers or the internet, but relied simply on hacking technology of any kind exploring the possibilities outside the scope of the technology.

An article from the economist [8] explains how in the early days of hacking it had nothing to do with the cyberspace, but was instead a part of the MIT model trains railroad club, hacking the systems to make them more advanced and later finding methods to cheat phone signals etc. Featured in MIT magazines the term hacking slowly spread and was first later adapted into the cyberworld, as the original idea of the term functioned just as well in cyberspace also. A quote is made which puts the mentality of hacking ***“The default assumption is that everything is vulnerable”*** – Quote: Robert Watson [8].

RESUME

Like the term hacker, hacking also has a history, which is completely different than what the common understanding of the word is. Looking at it though it can easily be seen how the term hacking to day means breaking into something. There are few electronic things not covered by some level of protection or “terms of use” meaning you are not allowed to simply “explore” in the systems and as minimum you will lose the guarantee of the product much like if you physically open a computer beyond a certain point. This thesis’ explanation of the term hacking will be exploring

technology beyond the intended use, including exploring methods of gaining access to systems and using the tools of hacking to break through security protocols.

EXAMPLES OF WORST ATTACKS IN HISTORY

Five of the newest hacking attacks considered the worst in history [9], involving the Ransomware "WannaCry", which locked files and forced users to pay a ransom for unlocking it again. Hacks of personal info through the American bank JPMorgan Chase & Co in 2015 resulted in up to 100 million user's personal information stolen by a trusted network, but worse the information gained from financial sector were used to influence the stock market. There were also the 2015 direct banking hacks done by Russian hackers. More known is the 2014 hack on Sony, which also later was targeted by DDoS afterwards, resulting in crippling results. It was never truly solved who did the hack, other than a research into the authorized attack claimed to have been made from North Korea as a response to the movie "The Interview". Lastly a quick tour on the Yahoo security break from 2013, which resulted in no less than 1 billion Yahoo users' data being stolen. Yahoo has been attacked several times following that event, and today it is very uncommon that anyone old enough to use an e-mail account chooses Yahoo over other services like Gmail etc., due to their information stolen through previous attacks.

TechNadu [10] news supports that the Yahoo breach is one of the worst attacks ever in history with the over one billion user's information stolen. In addition, they also have a point of view on cyberwarfare, suggesting that attacks like Titan Rain, which did not do much damage, was one of the first cases of suspicions of a major superpower (China) using hacking as a virtual battlefield to gain information. Other examples are made on cyberwar, e.g. from Estonia, where hackers joined together with Kremlin to shut down Estonia services in large sections. Ending in two old well known cases here under the CIA making the first "Logic bomb" which was able to trigger based upon events like a user logging in and having results as bad as blowing up gas lines. Also, the worm known as "Stuxnet" which infected a nuclear facility and racking havoc while being in the systems including damaging several nuclear centrifuges.

Wired.com [11] here mentions how the breach of Yahoo was not only concerning 1 billion users, but closer to 3 billion user accounts, which was every single Yahoo account that existed at the time. This including another attack in 2014 where 500.000 million users were comprised in a new separate attack again shows how this breach had a severity in amount, which probably not will be seen for a long time again. Though all these accounts were exposed, more than 3 billion, when there are approximately 7-8 billion people in the world currently, most worrying was the wait before disclosure of the real numbers and the attacks, but also how long the investigation took before people knew just how large the breach was.

RESUME

Looking at just a few of the different attacks, the severity of the issue becomes quite clear, through the paper more examples will come to light but for now this part of the Analysis is clearly showing the issue exist and that there exist malicious hackers of different types perform.

DIFFERENT STYLES OF ATTACKS

We earlier mentioned the terms Hacking and hacker. But now we will focus upon a sub category of hacking referred to as Cybercrime, a more specified term used when talking about hacking for the singular purpose of breaking into computer or networks using cyberspace.

Norton Security [12] have written a short article explaining the term and the attack styles used in cybercrime. Separating it into two simplified categories, Cybercrime to perform harm on a system and Cybercrime to steal or gain information from a system. No matter which category of attack used they both take advantage of social engineering, flaws in a system or backdoor access as mentioned earlier. This chapter is aimed at explaining some of the attack styles and terms used to in cybercrime.

WORM

Worms [13] is a form of malware, defined because of the possibility of later damage after infection. Per definition computer worms is not by themselves harmful since they are designed to run by themselves and replicate across connections as internet or movable hardware. Example could be a USB stick infected with a worm replicating itself to every computer or system it gets in touch with without any human interaction or simply a worm that when infecting a system chainmail an attacked replicate to a mail and sends it to the users address catalog. The reason its classified as malware is that a worm can be loaded with a payload which can cause serious harm. An example is made with the payload named Witty which simply kept writing data to the hard disk in the computer until the system broke down.

MALWARE

The term malware [14] describes when a user places malicious software onto their system without knowing or giving permission and is used for people that have fun just as well as high end cyber criminals. Malware can be achieved through several methods of either unsuspecting users that download software or give information without knowing its used to give them malware or vulnerable weak points in preinstalled software or applications that example allow malicious users to sneak malware in through an insecure network transmission, or a security flaw in a driver update. Malware can have several types of attacks which in this article is separated into four different types. Infectious which include viruses that do harm or worms designed to spread upon networks. Web threats like keyloggers noting down every keypress including password and usernames and transmitting it back to the malicious user. Spyware which reads through files and send information back or adware which modify advertisement to what the malware which you see lastly making the system a bot which gives the attacker the ability to control the system remotely, multiple computers made into bots or zombies are often referred to as a botnet and can be used for illegal activities. Concealment malware like fake antivirus programs or trojan horses, these typically exist to keep other malware secret or provide backdoors for an attacker to later have easier time when attacking the system. Lastly Ransomware exist which is designed to encrypt files on a person's system with the later intent of ransoming the owner for money or services in return for unlocking the files again.

VIRUS

Hard to distinguish from malware, not all viruses are malware. [15] Unlike Malware like spyware which is intended to monitor the user and send data back, Viruses is designed to attack the computer in the form of actual harmful processes that can be silly like opening things to deleting content. But like malware is designed to replicate itself to prevent removal and get users to spread it without knowing. Viruses is designed to often not be a question of quantity of infections but quality of the virus results.

Virus [16] is a type of malware designed to annoy the user more than spying on them, but if it's not designed for spying then why are they being made still, considering a computer virus unlike in nature does not just evolve by itself but have to be manufactured there need to exist reasons for it to exist. These causes include; for the fun of it like the ika-tako virus which had no purpose other than replace files and programs with simple images of squids. Evil is also a reason to make a virus, designing them to delete data or ruin systems these evil acts of viruses have amongst other things received credit for via the Mydoom virus slowing the internet down with 10% since its release via cyber bloat. Viruses can be spread via all kind of methods today like Email, filesharing, software download etc. If you end up receiving a virus it have a multitude of different variations you can be infected with like boot Sector aimed at the operating system, Direct action which go through files and do a single targeted action like deleting themselves when finished, resident viruses which is cable of actually saving itself in the hardware like in your RAM making them extremely hard to remove or maybe just a polymorphic version designed to mutate at every replication making them never look the same for every system they infect.

PHISHING

Defined by Norton security online [17] Phishing is a version of social engineering. Methods designed for the singular purpose of stealing personal information which unlike malware is only designed to produce identity theft of users. Examples made is the widely known Nigerien prince scam emails which is send as spam to people and preying on getting people to either transfer money or write their bank details for later theft.

AVG antivirus [18] have made a guide for people online to understand things easier and here Phishing is explained much in the same patterns as prior. But defines phishing as more than just identity theft but also includes the idea of just outright theft or even malware distribution methods. A major keynote from this article is that phishing does not have to be spam but can just as well be made targeted for you known as spear phishing. These attacks are targeted for a user or organization precisely and uses tactics as waterhole attack where the person performing the phishing will attempt to gain access to an organizations or companies internal communication or other trusted work source of information and then use this trust to send out phishing attacks. There also exist phone phishing which will attempt to use phone calls as their attack source, making it also referred to as vishing, this type of attack is often actual people pretending to be technical help, supervisors etc. and will use this personal layer of trust to gain the information much like with email phishing. One of the worst types of phishing is the Evil twins attack, where an attacker makes an evil copy of a person, application, game etc. and then use the users trust in what they see to trick information out of them.

DoS

Denial of Service (DoS) is the action scenario where a computer or network connects to a service using its own communication packets against a service by flooding it with information, example of this could be the case of a computer sending constant requests saying to a server that it would like to connect. Earlier in Malware botnet was mentioned and these can be used in a Denial of Service attack to make it into a Distributed Denial of Service (DDoS) where a service or server is being attacked from multiple users simultaneously with the intend of flooding the service with requests. [19]

Denial of Service (DoS) attacks have multiple different types of attack. Here under the most commonly referred to is Distributed Denial of Service (DDoS) which is depended upon using a multitude of systems like a prier prepared or bought comprised botnet allowing a hacker to redirect traffic from a zombie computer/network to send packets to the attacked service. But this type of attack is not the only version classified as a DoS attack. Though the Internet of Things (IoT) have changed over time and made it easier as the internet have evolved to redirect traffic and get access to remote networks and computers. A well-planned DoS attack from a single computer can still do massive amount of damage. These attacks can be the Shrew attack style, this rely on the Transmission Commission Protocol (TCP) which have built in features to handle bursts of communication with a timeout of slowdown protocol which then influence everyone else trying to use the service. A more common version used on smaller networks is Smurf attacks which rely on a failed setup in limited message protocols in a service. So, example of performing would be Spoofing (acting as you are the owner of the services IP address) a massive server network with connection requests making this large Network respond back to the service with massive large packets of responds to the original service flooding its traffic. [20]

Motivation of hacking

As the hackers are not only cruel people, this must mean they have reason to break security, this is often referred to as a motivational reason and this chapter aims to look at some of these motivational aspects of hackers.

Different styles of hackers (white, Grey and black hats)

Individuals

There exists a common reference to hackers wearing different styles of hats, this reference originates from black and white Western movies where a bad guy would wear a black hat and the good guys white hats for clear indications for the viewers, this have followed over into defining hackers as this web article illustrate by defining everyone by different hat colors. Most notable is that there exist script kiddies also which is not defined by hackers by this author but instead people playing around with other people's software like making a DDoS attack by downloading a software and simply clicking a button. Secondly, we have the White hats, the "good guys". These hackers are the ones you will often find helping people getting rid of viruses and reporting security flaws in services. Black hats on other hand aim for finding weak security or worth valued challenges and does not care about the law. Gray hats are the people in between which you will see hacking a

website just as a trolling task to make a politician look racist etc. But rarely is seen doing the good deeds of a white hat. Green hats are the rookies which intent to become a pro. These people often do not have a side yet but instead learn from anything they can find. Red hats is vigilante of the internet, instead of reporting black hats etc. they take matter into their own hand and make personal attacks aimed at the "bad guy" and last the author define the Blue hat as a script kiddie which want to do something bad, so they use a DDoS attack as a revenge on a website though they do not have the knowledge to perform a prober attack. [21]

Norton Antivirus have also made a definition of hackers based upon these hats [22], but they limit themselves to the three main ones White, Black and Gray. Black being the bad guys wanting to hack a bank and steal companies or personal information. White is the good guys that will work for protecting people. They are defined by asking permission or having special connections meaning they legally hack into systems with the intent of fixing security issues. Lastly, there exist the gray hat which is a middle ground. They do not aim to be doing harm but is often much like a white hat just without the permissions. They also sometimes instead of reporting their findings to companies will display them on the internet for the world to see.

An example of a gray hat moves, a look toward the 2018 act of google play store is an example of a large company doing it [23]. When Fortnite decided to not use the play store as their publishing service and instead rely on their own launcher, google performed a security check on the launcher. Instead of waiting for the fix to be launched and in collaboration work with the Fortnite to make sure the flaw was fully fixed, they waited the minimum amount of time and then publicly reported the security flaw. Which hackers could see as a chance for an open invitation to hack peoples accounts.

The white hats or good guys is also often referred to as bounty hunters as companies is more commonly today setting out prices and bounties for hackers to under controlled scenarios hack into services and find flaws. This is even considered part of the common defense many people are covered by which they do not realize. That someone reporting the bug that allows hackers to enter your service is what protect your service and in turn you the user [24] [25].

GROUPS

When looking at groups of hackers, its normal describe them as cybercriminals which help each other or make a network able to stay away from being caught. Though there exist multiple networks of malicious hackers being shutdown at a constant rate, AVG Antivirus have compiled a list of some of the worst hackers through history. These are the hackers and groups that are still managing to live though being well known.
First of starting out with one of the most well-known hacker organizations in the world "Anonymous" which was born in the 2003 as a troll group of sub hackers the community evolved and by the 2008 became a group that together launched their first collaborative attack named "Project Chanology" which was their war against the religion of Scientology. Since then the hacker group is known for both attacking Sony networks, PayPal and many more companies and individuals. Their true strength lay in the massive decentralized network allowing everyone to

communicate but no one to be leaders over more than a project at a time *"We have members throughout society, at all stratas of it, worldwide. Yet we have no leadership."* [26].

The next person on their list, though an individual and not a group, have a so big following because of the abilities demonstrated and that he walks free and converse with people today. That it will be included here also, the person Evgeniy Mikhailovich Bogachev is known for the massive botnet he controlled and had infected with malware etc. which is considered one of the most damaging networks a cybercriminal has made. Though currently known to be in Russia the government have no intention of prosecuting him and the American government still have the highest bounty ever made for a singular cybercriminal on him.
Evgeniy Mikhailovich Bogachev is rumored to be on the Russian payroll, but the group Bureau 121 is on a governmental payroll, more precisely the North Korean. This group was behind the Sony Pictures hack in 2014 which from the second it happened was rumored to be North Korea retaliation for the movie "The interview" but is judged to have had several major impacts on severe hacking scenarios in the world through time while being paid by North Korea for their services.
Something interesting to see on this list is that most of these groups and persons is either rumored or directly confirmed to be paid by the government and are the source of some of the worst attacks existing. Like Marcus Hutchins paid to help against the WannaCry ransomware that was unleashed upon the world and then later arrested for his bad deeds along the way as a hacker in the current world. Chinese hacker army known by the name of PLA Unit 61398 which China openly have told existed as a cyber defense team but is judged to be existing mainly to stealing governmental intelligence. Lastly Israel Unit 8200 known for their advances in the cybercriminal world for some of the strongest malware productions in existence and known for both spying on people but using their intelligence to also foil terrorist attacks [27].

The article "SOCIAL NETWORK ANALYSIS OF A CRIMINAL HACKER COMMUNITY" from 2010 [28] is one of the few papers that exist looking at the structure of hacking communities. The norm for researching the field of hacking is normally either focusing toward the individual hacker's process or from the technical perspective of simulations and attacks styles of the defending service. The article aims to focus on the four research questions
1. What is the network centralization of a computer hacker network?
2. Are there members of a hacker network who stand out as critical leaders!

3. How strongly do leaders influence a hacker network?

4. What subgroups exist and interact in a hacker network?

The article used the hacker network known as Shadowcrew which is a shutdown community that is known for Identity thefts and credit card fraud. By using their logged texts, a mapping of communication was produced, and the results of the article answers all their questions by generating empirical data of the members in the Shadowcrew community. Most notable the article states that Shadowcrew was a decentralized group with multiple leaders that had influence on their work and these leaders had power which could be seen through sub groups and cliques of the Shadowcrew network.

MOTIVES FOR HACKING

In the Netflix show Bill Nye saves the world a debate is made with three people shortly, where the introduction of curiosity and wanting to understand how something works is a driving force for hackers to keep engaged in a task [25].

Much like the debate from previous the documentary of Anonymous have several points where the members reference the idea that they were doing an action because of sense of doing what is right but also the feeling that they wanted to troll (Annoying a person with unsolicited or controversial provoking actions to people [29]) people in the form of attacking them [26].

In 2002 the Boston Consulting group managed to make a survey on the motivation of hackers [30], filling several potential motivation aspects as intellectual stimulating, work functionality, professional status or code should be open as motivation etc. based upon 684 responses where 30 % was paid and rest was volunteer they manage to separate the results and compare the motivation answers of the survey group. Here they segment the Hackers into four groups based open the answers.

1- Community believers (group): 19%
2- Professionals (work): 25%
3- Hobbyists (non work): 27%
4- Learning and stimulations (improvement and fun): 29%

Forward the presentation looks at how the hackers work and would be usable in the form of open source project development with certain key points as example their respondents had a very high tendency to do volunteer work on projects.

The paper from 2017 “A Q-Analysis on the Motivation of computer hackers” [31] is one of the few papers launched with well documented findings that does not take the focus from the defense perspective or an individual hacker. Instead it aims to use the Q-Methodology to classify motivation aspect of hacker clusters. For the questionnaires they managed to gather two rounds, first with 20 hackers and second round had 23 hackers. The hackers were self-proclaimed hackers which had a tie to an organization not named which is common in these areas considering being hackers is monitored with the claim of state protection any volunteer would not normally openly tell their identity in a paper. By using PQ-method software they ended up with Q-Samples translated into their classifications of clusters. Seven groups were classified

1- Social Positive
2- Social Negative
3- Intellectual gain
4- Social satisfaction
5- Economic reward
6- Technological positive
7- Technological gain

The respondents ended with indicating results in the form that they hacked with the motivation of external inputs like greed or social acceptance but also had indications of situations of displeasure or stress.

The paper also presents three factors of reason why a hacker accepts doing something in the form of illegal activity.

1- Superiority (white hats)
2- Explorative
3- Opportunistic (black hats)

Ending with the conclusion that people hack motivated by self-expectations of not being caught while gaining their individual values to themselves.

DEFENSE SYSTEMS

Monitoring the method hacking is used across the world is sometimes one of the best versions of defense. The reason for this is to know what to predict and keep up with the newest methods that companies must defend themselves. Symantec have been one of the leaders in doing this for last many years producing detailed reports of breaches and methods used. Interestingly tracking the origins of the attacks where in 2018 China was leader. Showing the trend that people need to be more aware of new technologies also being sources of breaches like cellphones [32].

This chapter will look at some of the suggestions, rules and software used to help protect people and companies against the constant real threat of cybercrime.

CURRENT SUGGESTIONS IN PLACE FOR PREVENTING ATTACKS

Currently when discussing defense in the cyber world the common reaction is looking toward the personal computers defense systems. It was mentioned earlier how these computers can easily become part of a botnet and being a zombie in this system and therefor the correct protection is needed. This is the reason so many companies exist not only for protecting people directly but making a herd immunity protecting the people who might not have defense systems in place. Microsoft who develops and publish Windows, the most used operating system for the private market, have even in windows 10 evolved a constantly background system referred to as “Windows defender” [33] which is designed for performing simple virus and malware scans but also protect the computer at runtime if a program or user tries to do anything that might not be correct.

When a private person uses mail services like google mail (Gmail) [34] they will notice that there exists a folder called spam, this folder is where your unwanted emails end up, but more importantly where chainmail etc. known to be phishing or dangerous automatically is placed. Reason for this is that people opening emails with malware and phishing might spread it to more people and companies like Google have decided to help the private citizen and handle defense for you. This does not mean you should open and download without considering what you received but drastically help protect private users.

The other side is from a company standpoint where a typical employee can be the threat of an entire organization. While companies of every kind must handle situations like North Korea attacking Sony pictures it’s important for them to take time and invest in security protocols. Therefore, major companies like Microsoft who wish to protect

their users and clients, both companies and people, develop guides like “Anatomy of a breach” That define the three steps to look for in a singular attack, first they want to break in, this can be done with phishing, malware or flaws in security updates etc. When an attacker is in the system step two being, looking for access to accounts or systems with a higher clearance or methods to gain access to the system. Starting at step three the attacker will now be in a position so solidify their hold on a company. By example making more accounts or building security flaws in the system for regaining control. All these guides are designed for making companies aware that opening a chainmail from your family member, though being a low positioned employee can be used by the attackers to develop a major security breach.

DEFENSE EXAMPLES

It might be easy to theorize on how combatting cyber-crime functions, like people storming in a room where a dark hooded teenager is covered in bottles of cola like in the movies. In real life though many of the cases is security companies trying to gain access to the origins of attacks and trying to shut down the operation for later prosecution, this was the case with Evgeniy Mikhailovich Bogachev which allowed him to escape for Russia in safety before the actual arrest was made. Symantec [35] managed to gain access to ZeroAccess botnet and shutdown a total of 500000 compromised computers, earlier also referred to as zombies, but this victory though celebrated might seem to the normal person as an indication of how large the issue is considering the ZeroAccess botnet at the time of this was a total of 1.9 million compromised systems. So not even a third of this cybercrime botnet was shutdown.

So, when looking at examples like ZeroAccess its clear why people need to protect themselves. Methods to do this is making sure things is updated and use a trusted antivirus/Antimalware software. Mentioned already is the windows defender system but the threat is so large that companies exist doing nothing than trying to protect users like Symantec. These include several different types and qualities with all their different methods of defense and focus areas. Bullgaurd [36] is an example of a software doing their best to always make sure when shopping online or saving password that your data is secure from ransomware or identity theft. Symantec as mentioned earlier is an advanced system aimed to find and combat cybercrime but interestingly make contracts with subcompanies producing antivirus software instead of producing it themselves. These include Norton security, Avast, Kaspersky and McAfee is in the list over software’s using the Symantec database [37] to always have one of the leading knowledge cores for the newest threats and attacks [38]. These software’s often also consist of enterprise versions allowing scanning and protection of companies with large quantities of computers or downloads with processing. There exist attacks though like with DDoS attacks which is external traffic being sent toward a service. For attacks like these the producers of software and hardware used by companies need to implement security protocols like with the case of Microsoft Azure database which have an always monitoring protection feature. Looking for example DDoS attacks all the traffic going through the software is monitored and if detected the incoming traffic is mitigated and in example the case of flood IP attacks the IP addresses sending all this false traffic is being identified and scrubbed from the actual traffic. Of course, the service also is built in a fashion that constantly updates against layer attacks trying to use Structured Query Language (SQL) injections which is the typical method to communicate with a database. Paying for these complete packages with protection build into them is a major security value [39]. Unfortunately, compiling defense systems across a multitude of points also mean that when a flaw is detected it is not a singular event, but a multitude of users is now at risk, even if the flaw is quickly fixed, much like the case of Fortnite launcher anyone that have not updated in time is now in the risk of being a target. One example of an area often having issues with this are the open sourced content management system (CMS) WordPress which more than once have been targeted because even with updates to security majority of the users does not know to update [40] [41]. Leaving a major security flaw in the systems.

THEORETICAL SYSTEMS BEING EXPERIMENTED WITH TO IMPROVE SECURITY.

The internet might be an amazing place of knowledge and communication but have also opened for more attacks of every kind. In the Symantec reports this is often referred to as the Internet of Things (IoT) [32] This means that communities not only constantly have to combat the current methods of attack but look for new methods to defend themselves.

These advances often come at high cost but regularly something is detected which have a low cost high yield but at the cost of something else. This was case with the advancement of "backbone" to the Internet Service Providers (ISP). Simply applying a scan at these ISP could have a low cost on the delay of the internet but scan for malware and viruses at a constant rate. Though at the proposition was quickly fought because this also means that all traffic being sent through the ISP will be essentially monitored and this argument was a fear that it was simply more freedom sacrificing for the claim of more security [42].

Of course, not every case is like this and a question of freedom sacrifice and every year conferences like GameSec (Conference on Decision and Game theory for security) exist and here proposals are being made every year [43] where in this case using Game Theory to attempt advancing security. Examples from these type of conferences could be "Game Theory Meets Network Security and Privacy" from 2011 which goes through security scenarios like eavesdropping and analyzing them from a game theory perspective looking at the act of security as example a Zero Sum game [44]. Another example could be "A Game Theoretical Approach to Communication Security" using game theory to consider the defense as a game of attacker versus defender meaning instead of working simply with a winner or loser you work in the scenario of best outcome also referred to as Nash equilibrium. But also see the issue that using Game theory on an Intrusion Detection System (IDS) the Players must have a set trust score which is difficult to constantly handle and modify. worse the players of the game, meaning attacker and defender, is not unsoundly rational which means that though simulations and theories might be able to predict Nash Equilibriums to improve security reality most likely will be that behavioral economics would introduce a whole new scenario of complex algorithms that have to work in an already extremely complex defense scenario [45].

No matter which study of field is used there is most likely a use for it in Cyber security to advance the defense of systems all over the world.

ANALYSIS

During the beginning of this thesis as potential early problem statements was being formulated in the form of socializing techniques. Meaning simply presenting thoughts of the problem and getting refreshed new perspectives from other people, this conversation happened.

Me: “What is your favorite game?”

Person: “Guess Tetris cause of the influence in my childhood”

Me: “Would you qualify this as you are having fun while playing it?”

person: “yes”

Me: “Now Imagine I changed Tetris and removed the ability to rotate blocks”

The idea of comparing hacking to games, was first confusing for the conversation but when explaining it with a specific mechanic in a game it began making sense, because of the clear change in the core gameplay by changing this, the idea of changing a mechanic in hacking might have the same influence on hackers.

Through the background chapter there was presented sources of several kind talk about how hackers are doing it for the thrill of it, for the fun, for the curiosity and for the intellectual game. This knowledge combined with knowing how fun is defined in the world of game production produce a unique problem statement unlike the common focus upon how the defense improvements and the individual hackers. This thesis aims to look at the motivation of fun in hackers.

This paper though have not looked upon how gaming relates to hacking, though it’s possible to theorize. More information on some of the game theories which relate to hacking scenarios for building a final problem statement and methods to build our testable artifact.

COMPARING GAMES WITH HACKING

Earlier in this thesis it looked at motivation of hacking and the history of both the term hacker and hacking. Though there were results looking at only the monitoring gain and extern motivational inputs. An area and definition existed that was more concerned with the explorative, curiosity and fun aspect of playing with the technology than the outcome or reward of actions. This chapter looks upon the idea of having fun but instead of using the term fun will use game theory and game development theories focused upon the action of having fun while playing also often referred to as the wish to continue.

DIFFERENT METHODS TO ESTIMATE FUN/ABSORPTION ETC.

From the second a game idea is born, not always knowingly the game consists of elements which have been researched for knowledge and often also more monitory gain for developers. Though there exist a multitude of terminologies to go through in this field and will focus upon some of the more well-known during a game designers’ studies. Examples of this can be seen in papers as “A formal approach to game design and game research”, building

a framework based upon the three design parts “mechanics”, “Dynamics”,” Aesthetics” (MDA) which based upon their individual components “Rules”, “System”, “fun”. MDA is a framework designed to go through game designs with an iterative process for every pass finding improvements to design and tuning the gameplay to function better [46].

CAN HACKING BE CONSIDERED A GAME

Games is a part of the entertainment industry, so attempting to compare the dynamics of hacking with the fun of video games can seem impossible. In movies there exist several genres, but only one of them is named comedy though the entire franchise is part of the entertainment industry too. This is because not only does these media which exist of having fun and excitement for the users, but also can be serious, scary, educational and much more. In “Purposeful by Design? A Serious Game Design Assessment Framework” chapter 2 “Beyond entertainment” they state that not all games are intended for being primarily amusing, but this should not be considered the same as a serious game is not boring or without fun. They present the idea that a serious game Is not necessarily designed in the same manner as a regular game but instead focuses upon the impact going beyond the game itself [47]. This is the thought pattern when considering hacking as a game. It’s not designed to be fun but might be built by the same components making the same entertainment impact as a serious game. In the book “Serious games: Mechanisms and effects” chapter 4 – “Serious Games and Seriously Fun Games” [48] discuss the principle of how different serious games receive scores of different enjoyability and though taking only a small subset of 7 games finding that seemingly budget of serious games does not have any direct correlation to the enjoyment level. That it is more about the presentation of the game design via Audio, visual and technical capacity. Asking yourself what is the areas that a player finds enjoyable and invest more time in these areas would most likely increase their overall score though dealing with a serious game.

So, though hacking might not be considered part of the entertainment industry itself. If the ability exists to use the dynamics of it in the production of a game, though it might be considered humorless a focus on the aspects that produce enjoyment in the game mechanics just like in actual hacking can be theorized to increase the enjoyment of “gaming hacking”.

ENGAGEMENT

In the world of video games, like many other areas in the world, the story of player engagement is as important as ever. In the paper “What is User engagement? A conceptual framework for defining user engagement with technology” O’Brien and Toms go through the process of interviewing n = 17 participants while trying to go through steps of their engagement process [49].

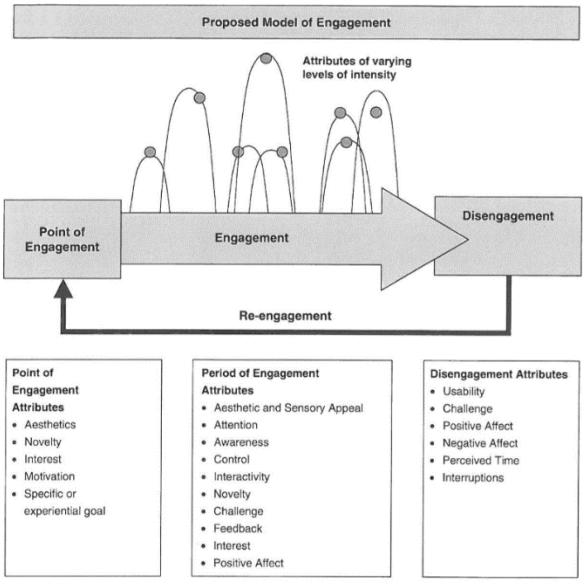


FIGURE 1 [49]

The results of using their framework allowed for the definitions of the different stages with induvial influences on each area as seen on the image over here.

But engagement can exist in several other areas in the daily life including in improving work scenarios. This paper by Osborne and Hammoud named “Effective Employee Engagement in the workplace” [50] aims to mediate the current large loss of costing U.S corporations toward 350 million dollars annually by disengaged employees. By first correlating the work engagement to the intrinsic and extrinsic motivators like physical needs and health but also the satisfaction of the workplace around them. Ending out in three suggestions based upon their research looking at how workers are affected by the global economic crisis and the change in workplace structures. Reward and recognition improve an employee’s motivation and engagement, making meaningful work and seeing the rewards from this improves the workplace engagement. Secondly an employee with more responsibility is motivation to do their best by also seeing their areas of focus thriving cause of their own commitment and receiving indications of their importance. Lastly the bond between leaders and employee can influence the engagement of an employee as they will receive a higher connection to the workplace and coworkers.

Though engagement is important all around in our lives. When developing something for the case of entertainment or serious games, engagement relies on the situational, implicit and explicit, influences of the participant culminating in a wish to keep continuing with the exercise or assignment at hand.

CONTINUATION DESIRE

Engagement can be measured as reason to start something, interact with the process and the reason for leaving. Just as well as the reason for workplace engagement and other aspects in our lives. One of the more unique methods to use the measurements of engagement is in the field of continuation desire or the “wish to continue”.

The authors Schønau-Fog and Bjørner, published a paper in 2012 focused upon the using engagements variety of understandings and influences on a specified term referred to as the wish to continue [51]. Defining a variety of individual engagement causes of different origins. These include

Intellectual engagement cause – result of strategic thinking, puzzles etc. leading to rewards, knowledge or in game content.

Physical engagement cause – the physical exercise to perform during gameplay like mouse movement, touch controls or embodied interactions like with the Wii controls.

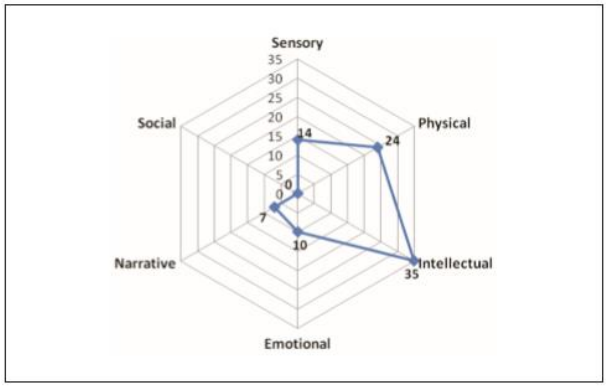
Sensory engagement cause – the understanding of spatial knowledge in the virtual environment example trigged by audio visual feedback in a detailed landscape. Allowing understanding of distances and materials around the player.

Social engagement cause – The social interaction between players in different situations which could be team gameplay, raids or quests only possible with multiple players.

Narrative engagement cause – the presentation of a story narration that intrigue the player to engage longer to finding more conflicts or events in the gameplay.

Emotional engagement cause – is an engagement type that is cable of being influenced by the other types, like a good narration can have an emotional response of a character experiencing something. It's also possible to be the humor or horror in a gameplay which is made by an emotional setting in the game.

Their paper aims to look at the effect of the six causes of engagement in settings of two individual games, angry birds and Wii sports. The findings show that depending on the game and players the importance of different engagement causes vary.



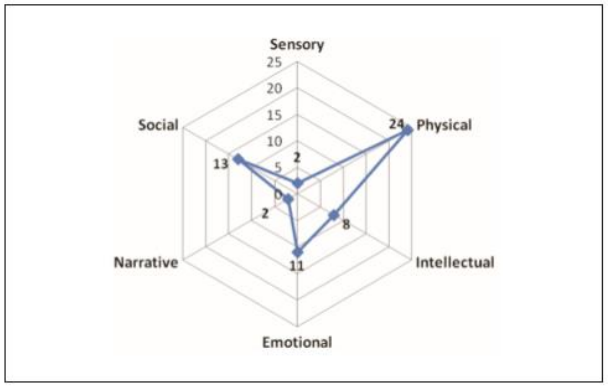


FIGURE 2 LEFT ANGRYBIRDS. RIGHT – WIISPORT [51]

The games might have a special focus of gameplay which allow different causes to have higher influence, like how an open sandbox rarely will have a narrative. Or how gameplay might vary over time through a game. But the players expectations and handling of the individual tasks might change the engagement cause focused upon depending on the player also. The combined causes of engagement are estimated to have a major correlation between peoples wish to continue and the level of engagement introduced to the players.

Another paper named "A Factor-Based Exploration of Player´s Continuation Desire in Free-to-Play Mobile Games" [52]again tries to use Continuation desire but unlike before focusing on

engagement this paper tries to measure user experience based upon the continuation and for this they have to first model their clarification of the influences in the wish to continue playing.

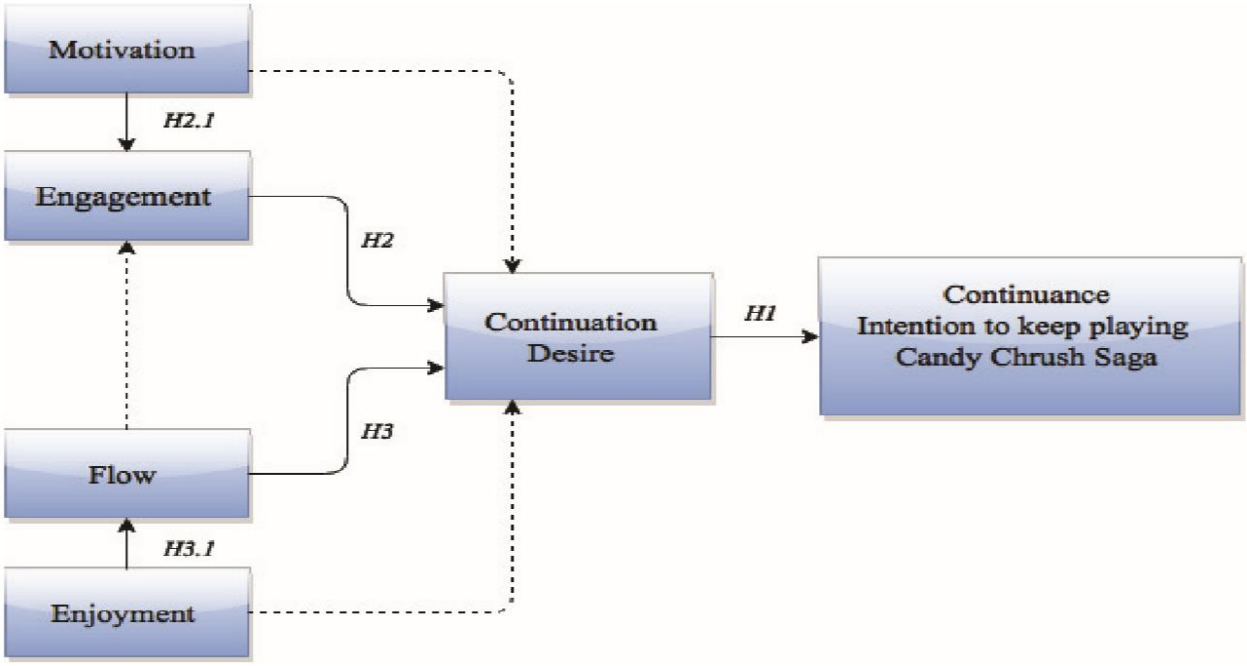


FIGURE 3 THE FOUR CONCEPTS INFLUENCING CONTINUATION DESIRE [52]

Again, looking toward engagement as a main aspect as an influence on continuation desire seen as being influenced by all other areas.

Motivation meaning the background to want to start playing and restarting the game when wished.

Flow being the abilities of player fitting with the games difficulty so a break here could be a jump in difficulty that the player is not ready for.

Enjoyment being the influence of both positive and negative experiences in the game, it's important to realize that a negative experience might still have a positive effect on the wish to continue as a focus to try and get over a frustration aspect.

Engagement being the investment of time and energy into the game combined into the engagement of the game from different inputs of the gameplay.

The paper does show user experience is correlated continuation desire, more interestingly like mentioned before there exist a clear indication of engagement having the highest influence of a players wish to continue and surprisingly flow through a wide researched area have much smaller influence than one would expect.

Schønau-Fog have also written a paper alone named "The Player Engagement Process – An Exploration of Continuation Desire in Digital Games" [53] aimed at engagement in the aspect of continuation desire but with intention of identifying the processes which a player goes through to achieve a higher wish to continue. Important distinguish is made from motivation and player engagement referring that motivation is what make a person begin playing while engagement is the reason people keep playing and is focused at the gameplay. Meaning in this paper engagement

is the singular area that explains a user's continuation desire. By qualitative methodology using 41 test participants resulting in 205 answers the paper can extract to a Player Engagement Process (PEP) that illustrate a process of engagement a player goes through relating to their wish to continue. This can be illustrated by the Objective, Activity, Accomplishment, Affect (OA3) framework

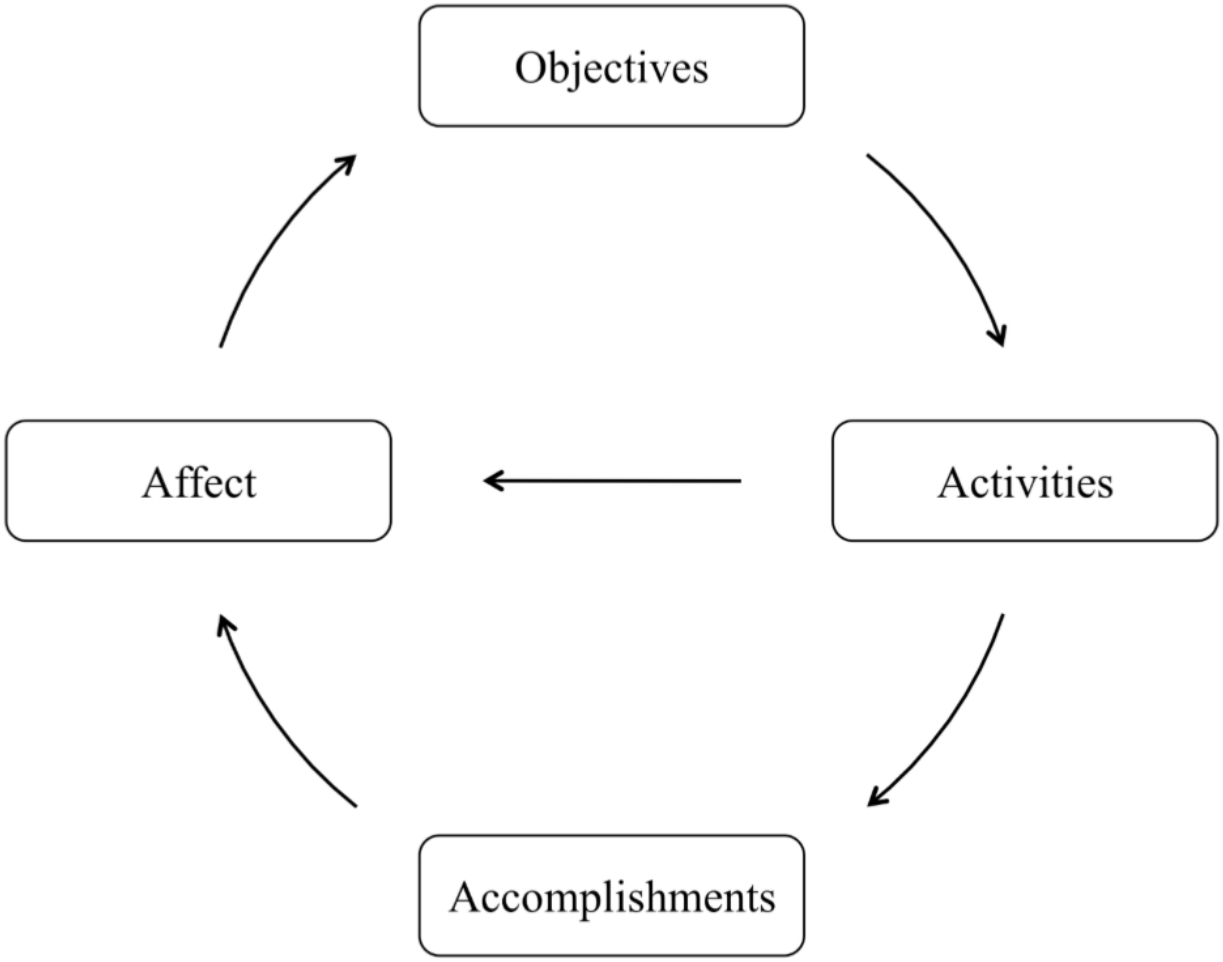


FIGURE 4 OA3 FRAMEWORK CYCLE [53]

The OA3 framework consist of four stages that a player moves through when they have first started playing.

Objective – made either by the player themselves or the game for them this is a goal to finish making them the foundation of the players engagement

Activities – is the actions that a player must perform to complete their objective including creation of new things like in the game Minecraft, destruction of things like in the game Rust, socializing like how in the game of World of Warcraft (WoW) you might need to create or join groups and discuss how to perform a raid. There exist many more activities to do for the goal of an objective which can also be a break in the wish to continue since some players might refuse to play unless there exist certain activities in the game.

From the point of activities, you can move directly to Affect or Accomplishments. Since accomplishment is only relevant when the objective or activities etc. is successful or completed meaning the paper define accomplishment also as progression in the activities needed to be finished before reaching another accomplishment of completion, much like how you are finding the correct spots for the puzzle pieces is all progression towards the completion of the full puzzle game.

Next step in the cycle is Affect referring to the emotional reaction of the earlier stage. Meaning you can have accomplishment stages that result in positive Affect making a player experience emotion like fulfillment or relief. On the other hand, sometimes, a player can experience frustration or feeling they are in an impossible situation and achieving relief from this result in a positive affect also.

A player can though also experience negative Affect that is disengaging like when a narrative activity is dissatisfactory for the player, but a negative Affect does not have to be disengaging. A puzzle might be frustrating you because its does not make sense, but the negative Affect of frustration make you more engaged and wanting to continue because of the want to complete the task.

Lastly as part of Affect is the point of absorption which is the combined effects of the terms Immersion, Presence and Flow. These terms each have a variant of importance when trying to measure fun in game but is typically defined specially for each finding, combining them into singular term called absorption allows for the terms to still have an influence in the overall Affect of the player without trying to make extreme clarifications.

- Immersion – the idea that being pulled into a game that the games actions is your actions.
- Presence - is connected to immersion that it's the pull into the world that a player feels that they are in another place.
- Flow – is the movement of the game, that gameplay meets the expectations of the player so a sudden drastic change or break in the worlds gameplay is a break in Flow.

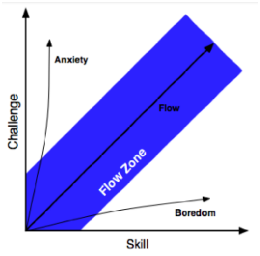


FIGURE 5 PLAYERS FLOW ZONE [54]

So, example suddenly changing characters and place is a break in immersion presence and flow.

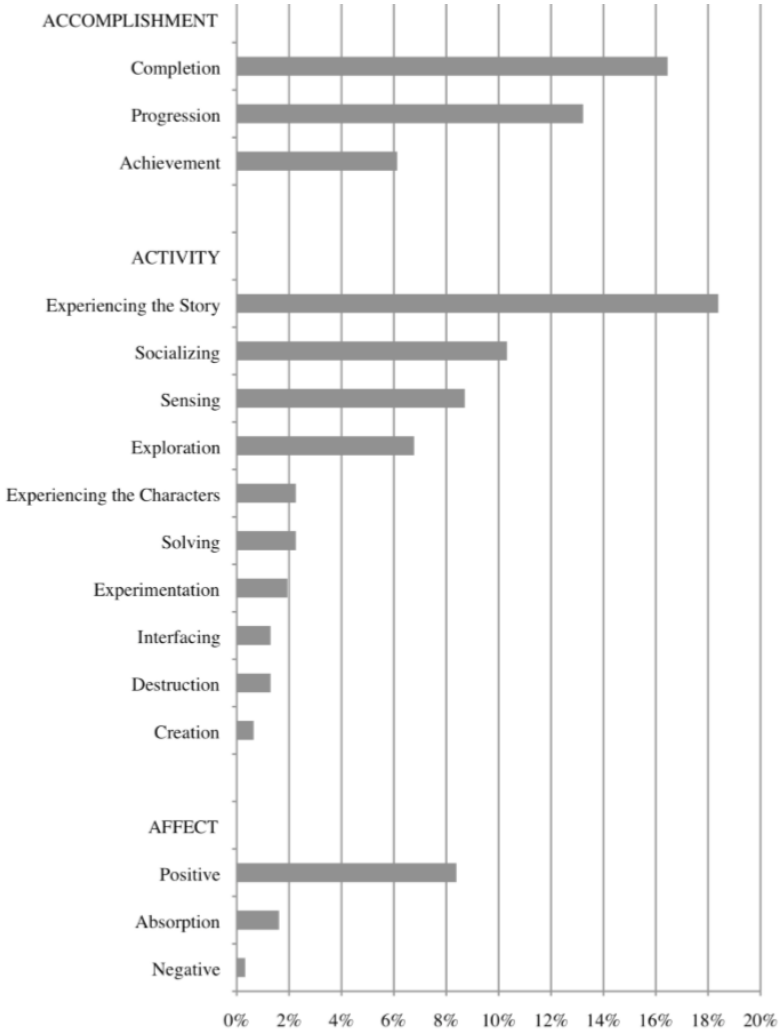


FIGURE 6 "WHAT IN A GAME MAKE YOU WANT TO CONTINUE PLAYING? [53]

The terms were split into groups and another set of data run to see the influence of players demand on the process as seen above.

Though the tests of these papers a varied and never tested further on other target groups the research into continuation desire demonstrate a clear importance of player engagement but rarely or low mentioning of flow, immersion and presence indicating that engagement might have more of an influence on making people continue.

MEASUREMENTS OF PLAY/FUN

In the previous sections of this chapter, continuation desire and engagement were mentioned as a focus upon game creation with the split that motivation still is needed to make people enter the Gameworld and lure them in. They introduce the idea of using Quantitative and Qualitative Methodology for gathering information about measuring fun. But the idea of having fun is a direct relation to the idea of play in our mind so in a paper “Adult Play, Psychology & Design” research is

made into why adults play and though the process clarifies how not only do children and adults play but even Animals play. Though it should be mentioned like their finding that sometimes not everyone wants to play like mentioned in their chapter 3.2 that when working with the idea of play you must keep a focus on the people that are willing to play and have fun instead of the inherit people that individually does not respond well to play currently.

Knowing play exist across all ages was presented as a paper from 2010 “A Model of Flow and Play in Game-based Learning: The Impact of Game Characteristics, Player Traits, and Player States” [54] though its interesting subject for this thesis its interested in chapter 2.3 “Play” aimed at defining play and find a method to work with it as a measurable player stat. Play is the ability to break the rules of the world and have freedom to make your own, like how a game might present the player with the world but it’s the users freedom to choose how to play with it. Much in the way fun gameplay can be part of an educational game in a serious content, the idea of play can be a fun and engaging playfulness enabling maturing in the sense of understanding world, language etc.
During their chapter 4 “Empirical studies” they produced two studies using the first one as a pilot study for creating new measurement scales gabbing a hole in the research area of play.
For their measurements during this pilot test six individual scales were made for the empirical data.
Play experience scale – A scale designed to measure participants estimate of play feeling during the test. Based upon five categories of measurement, 1. Assessment of freedom in the task, 2. Assessment of the task was depended on external aspects. 3. Assessment of how participants felt about how they had to do. 4. Assessment of participants ability to focus at the task at hand and 5. If the participant would qualify the experience as “play”
These sections resulted in the table of questions seen below

	Item	Dimension and Coding
1.	I felt that I was free to use whatever strategy I wanted to while I was using the game	Freedom
2.	I was able to make the game do what I wanted it to	Freedom
3.	The game gave me the freedom to act how I wanted to	Freedom
4.	The game made it difficult to do what I wanted to do	Freedom (R)
5.	I was not worried about someone judging how I performed in the game	No extrinsic
6.	Regardless of how I performed in the game, I knew there wouldnt be a real-world consequence	No extrinsic
7.	My performance in the game was not going to matter outside of the game	No extrinsic
8.	I felt like I had to do well, or the experimenter would judge me	No extrinsic (R)
9.	When I was using the game, it felt like I was playing rather than working	Play-direct
10.	I would characterize my experience with the game as playing	Play-direct
11.	I was playing a game rather than working	Play-direct
12.	Using the game felt like work	Play-direct (R)
13.	When I was using the game, I didnt worry about anything in the real world	Focus
14.	I was able to concentrate on the game without thinking about other things	Focus
15.	When I was using the game, I was focused on the task at hand	Focus
16.	I had a hard time concentrating on the game	Focus (R)
17.	I wanted to do well in the game, ”just because”	Autotelic
18.	When I was using the game, I wanted to do as well as possible	Autotelic
19.	I tried to succeed in the game because I felt like it	Autotelic
20.	During the game, my performance didnt matter to me	Autotelic (R)

FIGURE 5, QUESTIONS FOR THE PLAY EXPERIENCE SCALE [54]

And the method of gathering the results is via a Likert scale

Next the enjoyment scale which they based upon an earlier web enjoyment scale from Lin, Gregor, & Ewing, 2008 "Developing a scale to measure the enjoyment of
web experiences" modified into functioning with their gameplay enjoyment scale instead during gameplay.
And the method of gathering the results is via a Likert scale

Next was the Flow state scale made using nine subscales of definitions around the conception of Flow the none subscales are as followed:

- Challenge/skill balance
- Action-Awareness merging
- Clear goals
- Unambiguous feedback
- Concentration
- Control
- Loss of consciousness
- Transformation of time
- Autotelic experience

And the method of gathering the results is via a Likert scale

Next is the computer playfulness scale developed with a focus on the playfulness trait which is measured based upon seven self-descripted items in question formed as "I am … "these questions are then rated by the participants via a Likert scale.
Two scales more was also developed based on preexisting research and made with a Likert scale.

All these scales and the research behind the area of the trait playfulness and the term play can be used in the focus on how to define fun and the comparing in hacking as a version of gameplay because of even Animals are playing why would some people not be able to do it with hacking and this could be measurable. But when considering play in gaming you must remember the following.

"Whereas paidia (or "playing") denotes a more freeform, expressive, improvisational, even "tumultuous" recombination of behaviors and meanings, ludus (or "gaming") captures playing structured by rules and competitive strife toward goals." – Cited [55] Chapter 4.1

GAMIFICATION

When looking at making a game from something else it's important to realize that the power of games have on an area. With the purpose being focused upon increasing enjoyment and entertainment outcome when using the application its applied to. Therefor this chapter will present some of the knowledge behind the concept of gamification, though not the same as game designing, it is the principle of implementing game design elements into subjects not necessarily in the entertainment or game industry already.

In the paper "From Game Design Elements to Gamefulness: Defining "Gamification"" [55] the term of gamification is being researched and how to use it. Starting out with an origin history of the term the term of gamification is not older than from 2008 where it was documented as used for

the first time, and though there still exist many other variations of the word like “funware” or “playful design” the term gamification today has taken a major part of the terminology of all the other words. But since it’s not that old there is still a bit of debate over meaning and function, here under if gamification is introducing games more into our daily lives, or the other definition about modifying non game related subjects with game design to gain the effects of game engagement etc. from participants. The foundation of gamification is also troublesome since the principle of games is different from play. And yet many areas of gamified application and scenarios are referred to as play more than games. Though research have been made to find the middle ground between the two to identify the games part which is restricted scenario based upon rules and structure with the play side mentioned earlier as openness and freedom. This demonstrates just how unclear the use of gamification still is at the current definitions and only become worse by the point of chapter 4.4 that some authors have even said that a game can be gamified, resulting in that the only real thing not possible to be gamified is designing a game since this already includes the aspects of designing game elements for an application.

When looking at another paper like “Does Gamification Work? — A Literature Review of Empirical Studies on Gamification” [56] a clarification of gamification might become clearer. There it is defined as introducing motivation, getting a new psychologic outcome to more of the same as game productions and lastly the future modification of behavioral outcome

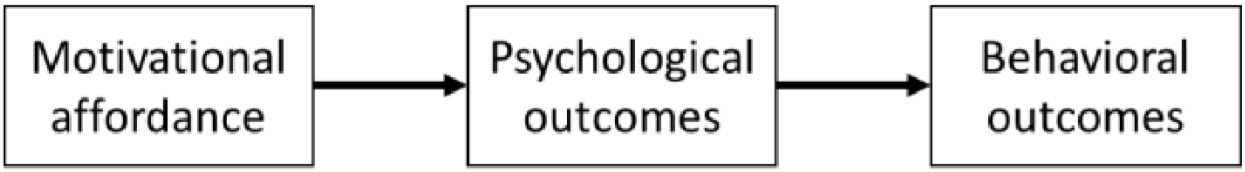


FIGURE 6 GAMIFICATION IN THREE SIMPLE STEPS [56]

And though the gamification term might not be fully evolved yet it’s now as a stage where you can see it being used to modify everything in a fashion of games with the intention of changing people’s motivation and outcome from using their applications.

RESUME

This thesis presented in this chapter a few of the terms used in the game industry to define fun and make it a workable area. Though in the section of “Measurement of play/fun” its presented that games and play is not directly the same. This thesis will support the critics of such separation as the freedom and open world in modern games rarely would be considered as limiting and rule based. It was presented that the principle of gamification though allows for an entity to modify motivation and outcomes of a scenario, application etc. which have become gamified. So, for working with the intend of presenting hacking as a game, this thesis will take great care in any productions and tests to not allow the dynamics of gamification to modify the intended direction. Much in the same way as presenting a test scenario in the world of Virtual Reality can corrupt the data gathered if not needed or presented correctly.

DEFINING PROBLEM STATEMENT AND THE TESTABLE HYPOTHESIS

Going through the presented research and theories during this thesis. It's now possible to combine this into a final problem statement which it can identify areas of to test in the idea of help. Basing the first idea that hackers and hacking is not actually a case of being evil but instead people that use their knowledge on technology combined with the motivation chapter there exist a foundation that. Though there exist black hats or crackers that aim at breaking security for typical monetary gain or an external motivation like politically. There does exist indications and surveys showing that hacking being performed caused by fun or associated terms based upon entertainment.

As a last step in my confirmation of this being an area to research upon. This thesis attempted to contact several hacking organization and hacker contractors which was found during the original research period. Though it normally ended in a scenario as seen on image hereunder, where systems used to contact was directly hacked by these people.

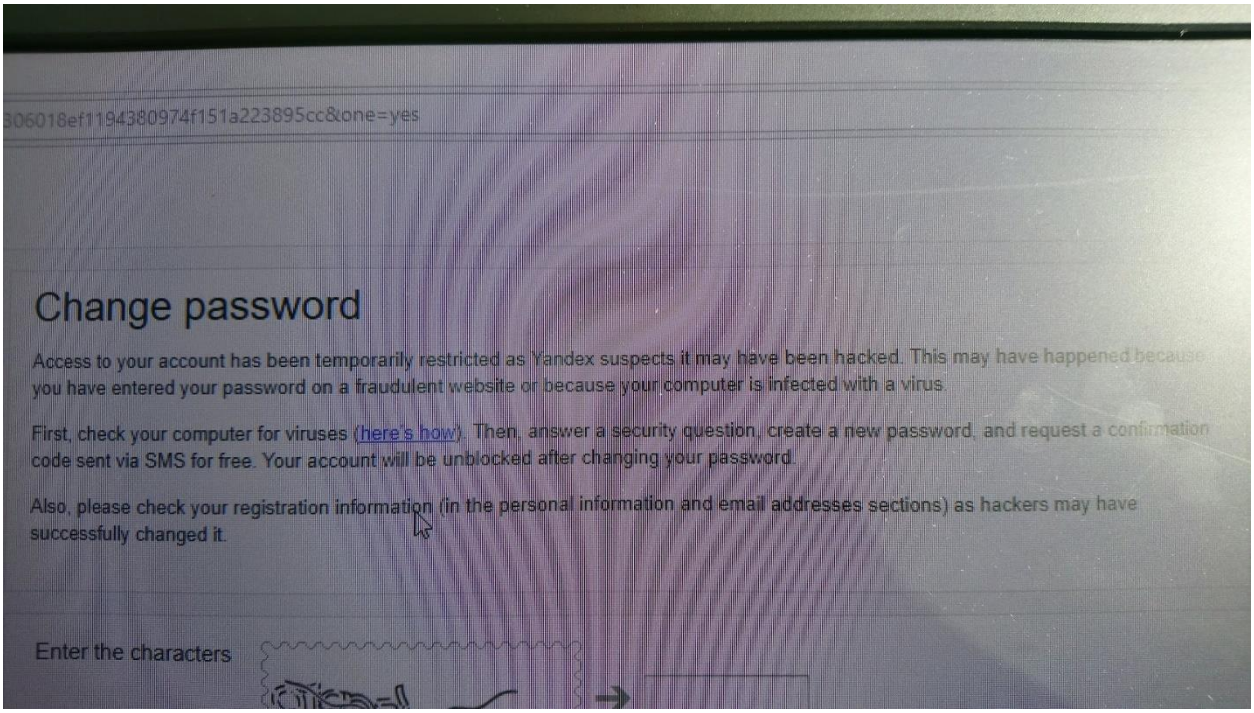


FIGURE 7 PHONE IMAGE, EMAIL SYSTEM YANDEX SHUT DOWN ACCOUNT BECAUSE IT WAS HACKED

But a single group consisting of a student hacker organization existing in Copenhagen, Denmark did respond through a contact person and a questionnaire could be send to the members but had to be delivered quick since the time of year was entering the summer. Nine of the members responded on an online questionnaire, that though early stages of damage use wrong framing as saying "aggressive hacker" instead of using the term "black hat" still respond with some of the same responds as it would expect based on our earlier results (Appendix 1).

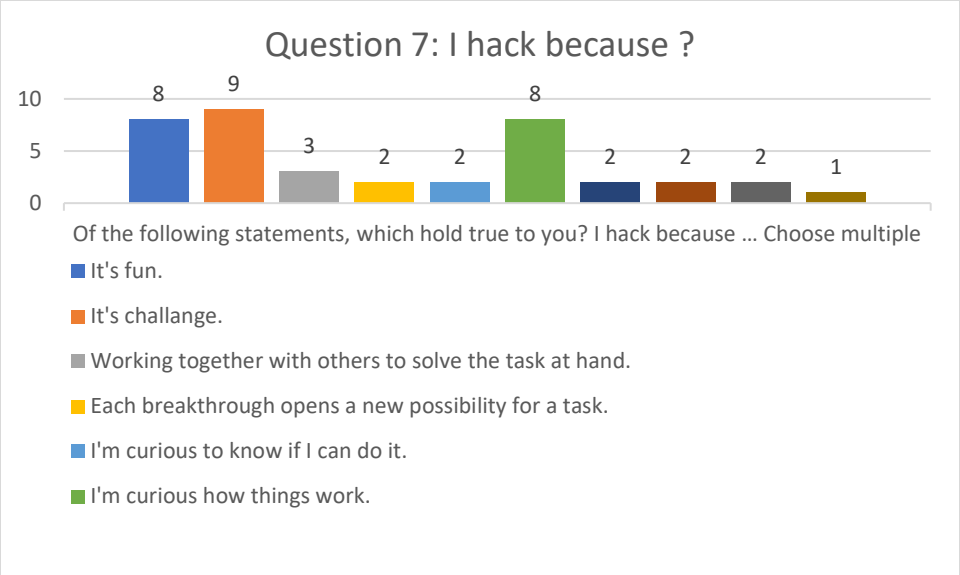


FIGURE 8 APPENDIX 1: QUESTION 7: WHY PEOPLE HACK

Following the answers from the survey with the prior research presented. There exist enough valid data in this thesis. That hacking can be motivated by the term "fun" for some people, which in the industry of gaming and game theory is redefined in terms like Engagement and flow etc. making it a testable and workable motivation for further research.

FINAL PROBLEM STATEMENT

Defining a final problem statement is the next part of the analysis, this is done to narrow the focus of the total field of research so far into the final area of focus.

This thesis presented the motivation behind hacking during background in the form of several sources, combining them together at this point with the questionnaire presented section before, the motivation this thesis focuses upon is that group of hackers is having fun while hacking. This group of hackers should be influenced if their source of fun is modified which is what this thesis will attempt to demonstrate.

This thesis also looked upon a few of the principles behind games, during this the term of fun in games was introduced and how even a serious game can still consist of good entertainment qualified as fun. For this thesis it will from now be looked upon as player engagement, since this was mainly described as the source of players emotions and feelings so as the experience of having fun. With the definition of continuation desire this paper will focus upon this framework and its effect on engagement.

Lastly with this definition of continuation desire it's possible that hacking can clearly be defined as a game not only in the style of fun but that the dynamics of induvial attack styles consist of the OA3 framework and could be made as game mechanics in a possible game design by the principles of gamification.

The possible scenario that hackers is performing their actions because of a level of motivation and engagement in the process of hacking, means that if IT security can be redefined in a method which influence this engagement in

hacking as a badly designed game influence engagement in the gameplay there exist a possible solution that could drastically influence the number of hacks being performed in the world. Even more efficient if this also works reverse since an increasing the fun of hacking for the correct people like those who tries to improve security would result in making it even worse for the other groups attacking because of other motivation sources.

THE FINAL PROBLEM STATEMENT:

If we reduce the accomplishment factor of the continuation desire dynamics from a game simulating a DDoS attack, are we then reducing the player engagement, as they are taking the role of the DDoS attacker, sufficiently to suggest implications for IT security countermeasures for DDoS hacking attacks

DEFINING TESTABLE HYPOTHESES

This problem statement takes the principles about the DDoS attacks and combine them with the theory of continuation desire, which only exist based on people's engagement that have been seen in the research to have a connection to the aspect of fun etc.

To answer the final problem statement, testable and falsifiable hypotheses need to be made based upon the restrictions made with the statement itself.

HYPOTHESIS 1:

Changing a dynamic of the simulation will statistically change people's engagement

HYPOTHESIS 2:

Changing a dynamic of the simulation will statistically change participants continuation desire

HYPOTHESIS 3:

Changing an element of the simulation will make have drastic changes in qualitative responds

ARTIFACT HYPOTHESIS:

A game simulation of a DDoS attack will have qualitative assessment play styles resembling expected DDoS attack styles.

METHODOLOGY

THE ISSUE OF WORKING WITH HACKERS

In the subchapter of comparing games with hacking, its presented that it's possible to look upon fun in the terms of engagement and continuation desire. This is important since getting test participants with a deep knowledge of hacking can be difficult. As presented earlier general reaction to taking contact is returned with being hacked. Though the test participants could consist of hackers with the knowledge but never actually having used their abilities or purely out of white hat hackers, getting a varied test group of these is unrealistically difficult without prior access into the community. Alternatively, much like seen earlier, a single organization/group could be used. This would provide people directly from the field, but any results would arguable be questionable.

Alternatively, it would need a proxy to test on regular people instead of hackers, this is only possible if it follows the rules of inference. Much like how in Denmark the sample group amount of 1000 participants during elections etc. is aimed to suggest the results for the whole population of Denmark. Inference can be used to research on one set of participants and allow the results to transfer to another untested target group. Descriptive inference is what is being used here, as a sample size for unknown variables. This thesis wishes to use the logical illustration of descriptive inference to say a game simulation designed to use the dynamics of hacking. Will function as a conduit between hackers having fun while hacking, to hacker having the fun from the simulation, to regular people's fun while playing the simulation [57].

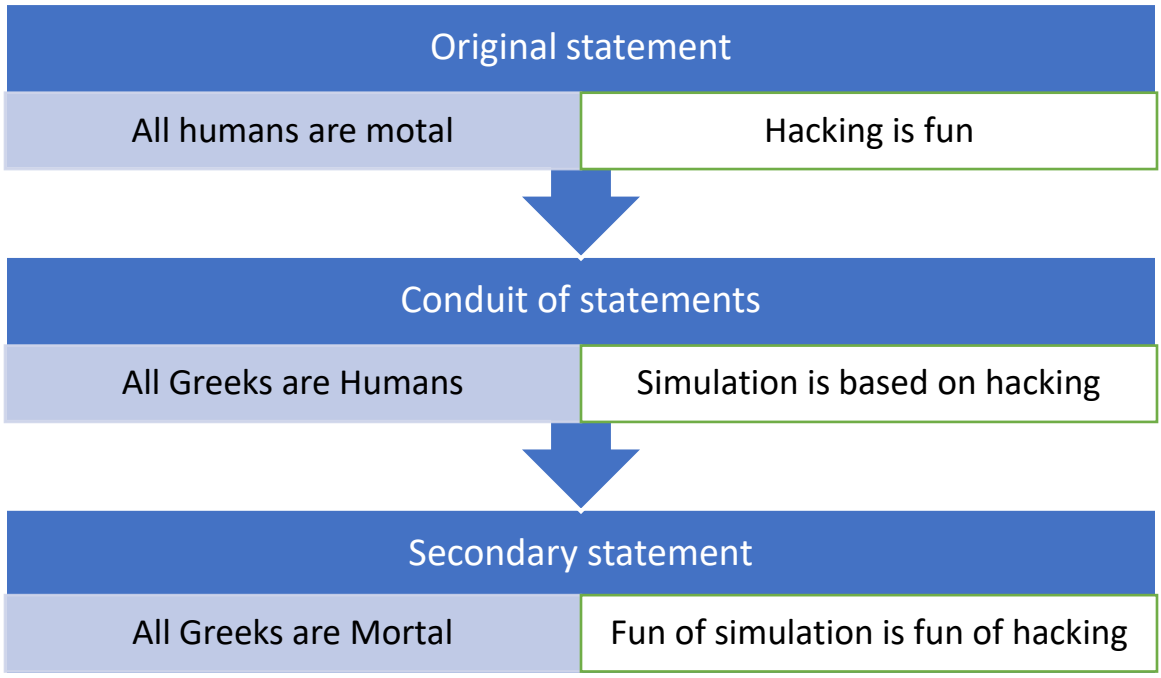


FIGURE 9 THREE PART INFERENCE EXAMPLES (LEFT: EXAMPLE, RIGHT: TEST)

THE NEED FOR A PROXY ENVIRONMENT

The issue of working with hackers illustrated a method using inference to use regular people for the test scenario. This also means that instead of making a technical hacking simulation, this thesis will instead use a test with a regular

a game scenario for people without the expert programming abilities of hackers. which is based upon the dynamics from a DDoS attack and thereby simulating the fun and engagement of the participants in the scenario of hacking.

This is also extremely important since based upon where you are currently are placed hacking rules are different and dynamic. From the Danish law the paragraph 21 have been used in convictions in courts [58].

Which translates into the following:

"Actions that aim to promote or cause the execution of a crime are punished when not enforced as attempts" – Translated from Paragraph 21, the Danish criminal code [59].

The issue can of course be diverted as a scientific experiment but lacking any answers from the Danish criminal court system this method would be a safer approach to the test scenario.

METHODS OF TEST RESULTS

For this thesis it is proposed to use multiple methods of results gathering.

1. Demographic qualitative methods to verify possible changes across Countries and ages.
2. Quantitively methods on player playstyles.
3. Quantitively method of play scale assessment.
4. Qualitative methods of open questions about the simulation.

TARGET GROUP

Trough the research presented not much demographic data of hackers have been found. Therefor this thesis will base is target grouping on the survey made by the nine people answers from the questionnaire to the Danish hacker group.

Their demographics was focused around

- 19 – 35 years
- Highschool education as minimum

METHOD OF TEST

For receiving aspects of fun in the simulation, this thesis does not intend on measuring the amount of fun, but instead modifying a simulation with the intend of changing the results of fun and engagement.

HYPOTHESIS 1:

Changing a dynamic of the simulation will statistically change people's engagement

HYPOTHESIS 2:

Changing a dynamic of the simulation will statistically change participants continuation desire

HYPOTHESIS 3:

Changing an element of the simulation will make have drastic changes in qualitative responds

To answer the three hypothesis requests to help understand the problem statement. This thesis aims to build a split test (also often known as an A/B test), with a control test and an alternative version to check the differences between these tests.

- Split test (Hypothesis 1)
- Ability to play multiple times (hypothesis 2)

DESIGN AND IMPLEMENTATION

This chapter will design and implement the dynamics of a DDOS attacks for game scenario used to test the hypotheses presented earlier in this thesis. To this goal it will go through a detailed explanation of the chosen dynamics of a DDoS attack followed by the areas of the Continuation model earlier explained in chapter of Analysis to find common areas and define the attack style to the model. This will be used to finally make a detailed explanation, to design the test but also find the areas in the attack we can influence for our test scenario.

DDOS DYNAMICS.

Earlier in the thesis we talked about the influence of DDoS attacks and how it works but for a test we need to explain the dynamics an attacker using this style of attack must go through before achieving a successful attack.

BOT NETWORK

Also, often known as a Botnet is one of the methods used to attack with a DDoS attack. Not to be compared with styles like many Anonymous attacks which can be performed singlehandedly by gaining access to a backdoor of a service and attack it from the inside. A botnet can be rented or even bought today for attacking a service and when discussing number of how many needed it's only the more the merrier for attacking a system.

A botnet is typically built up from a group of compromised computers or servers which can then be called to perform tasks remotely and like this an attacker can simply rent or buy the access to these groups and then order them to perform the type of attack which is wanted.

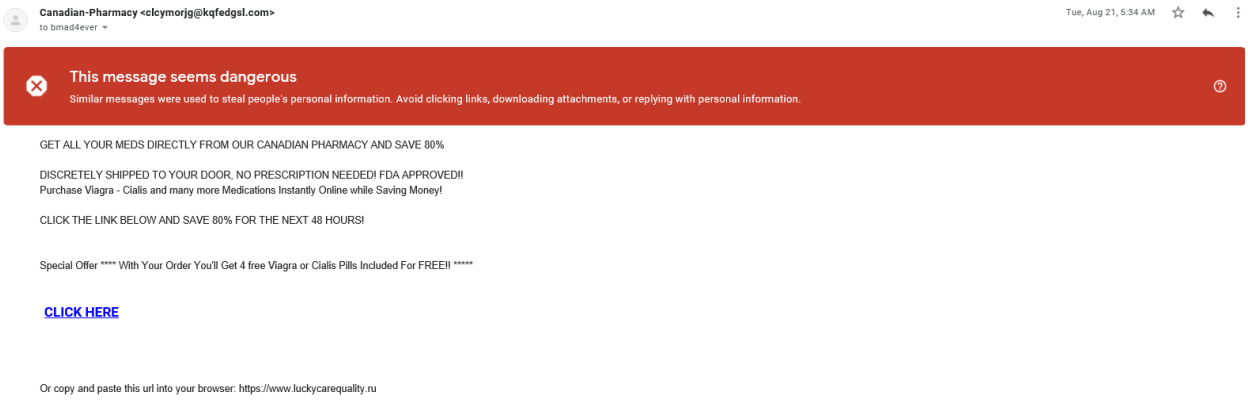


FIGURE 10 EMAIL SENT TO AUTHOR.

Seen above is an example of the phishing emails which most people today have received through their email accounts. This is a simple example of a phishing email send out to achieve different purposes. Most might be in the attempt to gain access to your data in the form of credit card information or directly making you send money. But some is designed for you without considering about it, to open a weakness in the computer or other electronic device for another person or network to later gain access and focus your processor power for a malicious purpose.

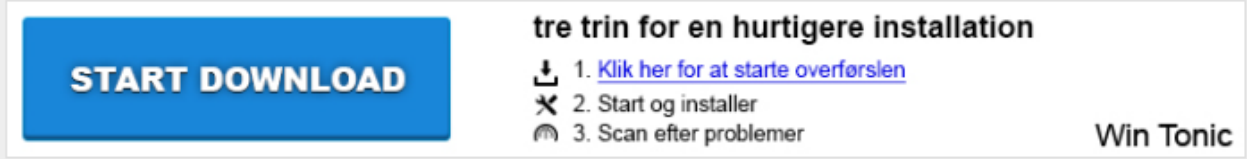


FIGURE 11 PHISHING WEBSITE AD, SIMPLY DOWNLOAD TO GET MALWARE.

Above on figure 13 is an example many people will have seen before. When searching the world wide web, many pages a driven by ad revenue and these can sometimes come from less than trustworthy sources which will attempt to make a user believe that the ad is a computer message or trustworthy source asking you to install a piece of software onto your computer to fix some errors. This can again be many different types of malware, but also for placing a seemingly trustworthy software on your equipment which can be activated from a malicious source for the same purpose as the earlier example.

DETERMINE TIME OF WEAKNESS

If the attacker already rented or gained access to a bot network as mentioned before this area, now the attacker would probably gain the best result from the DDOS attack, and this is normally done at some crucial point in the service.

In 2016 the world popular triple A title Battlefield launched its Beta game before their launch of their new title made by Dice entertainment Battlefield 1. With the last prober launch of a battlefield game being 3 years earlier in 2013 there was a major interest in gaining access and playing the new game. This was the crucial timing in service that attackers could use as the Battlefield servers was already under heavy load from the major number of players standing in line to gain access to the multiplayer beta servers. Launching their DDoS attack at this time shut down the whole service for major amount of the beta players leaving them without the experience of the long-awaited new battlefield 1 game.

Finding patterns and estimating the time of an attack can make an increase in chaos for a user of a service. The more that is waiting in line for a service the more pressure is on the company to fix this issue in a small amount of time.

Fighting the defense

Attacking a service with any form of attack will need you to combat different types of defense systems. Depending on what style of attack being used this can demand different styles of defense systems being activated, this is also why when researching reasons for performing DDoS attacks from monitory gain, it's possible to find cases of it being a simple distraction to deactivate or make the service fight the DDoS instead of the actual attack designed to gain value.

An attacker can use multiple methods of DoS as talked about prior in the thesis to achieve a successful attack, hereunder just one massive attack that crash the whole service but also using a dynamic attack which changes over time to make the service almost incapable of detecting which users is attacking it.

Continuation desire

In the Analysis chapter the Continuation desire research was presented stating the OA3 framework

- Objective
- Activities
- Accomplishment
- Affect

Minecraft example.

Positive example

- Objective build a house of dirt
- Activities is things like digging up enough dirt to do this, protect it etc.
- Accomplishment can be having enough dirt or reaching stages of building the house.
- Affect will be positive affect which result in you adding new objectives like adding a new room or maybe build it out of iron instead.

Negative example

- Objective is again to build a house of dirt.
- Activity is to gather the dirt and protect it etc.
- Negative affect is added when you fail to defend against a creeper (exploding creature) which get too close to house progress and destroy it all.
- This negative affect gives you knew objectives to rebuild in a new scenario which is better defended.

HACKING AS CONTINUATION DESIRE

The individual parts work both alone but is connected. Like mentioned before a botnet is often needed. The reason this is needed is to use the strength of this botnet when attacking the servers.

Under here you will see some of the thought behind the individual mechanics

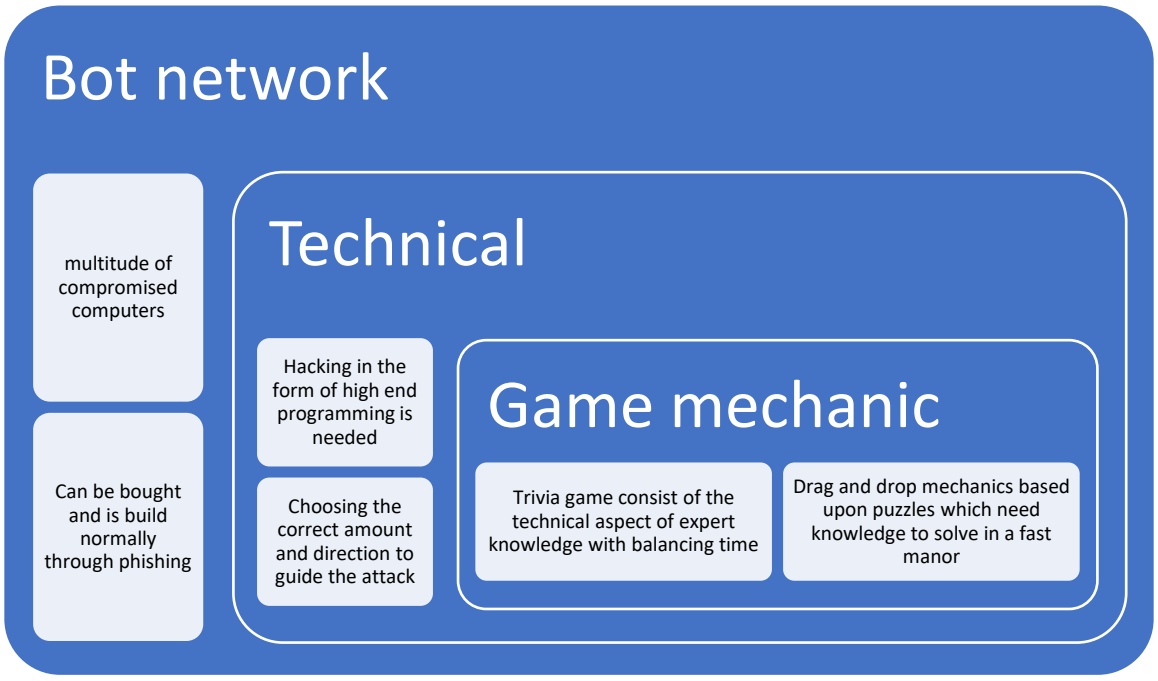


FIGURE 12 A BRAINSTORM THOUGHT PROCESS BUBBLE EXAMPLE

Through the brainstorming of the different aspects of what a botnet exists of and need. It was decided that Quizzing or trivia-based system was the best for a non-technical person to still rely on common and expert knowledge without restricting people from not being engaged caused by dislike of mechanics.

Real DDOS	Game equivalent
Botnet	Botnet Strength score
Compromising devices	Quiz questions
Spam/rejection of phishing	Detection meter
Speed and strength of attack	Timer of game
Determine attack strategy	Simon says
Server/service/ Access point of overall service	Individual blinking lights in Simon says
Shutting down server/service point/ access point	Holding light in Simon says as predicted to blink
Successful DDOS	Shutting down all blinking lights
Failed DDOS	Detection meter full

Another set of brainstorming exercises was made to determine some functionalities and game mechanics which could exist together with the new trivia based idea.

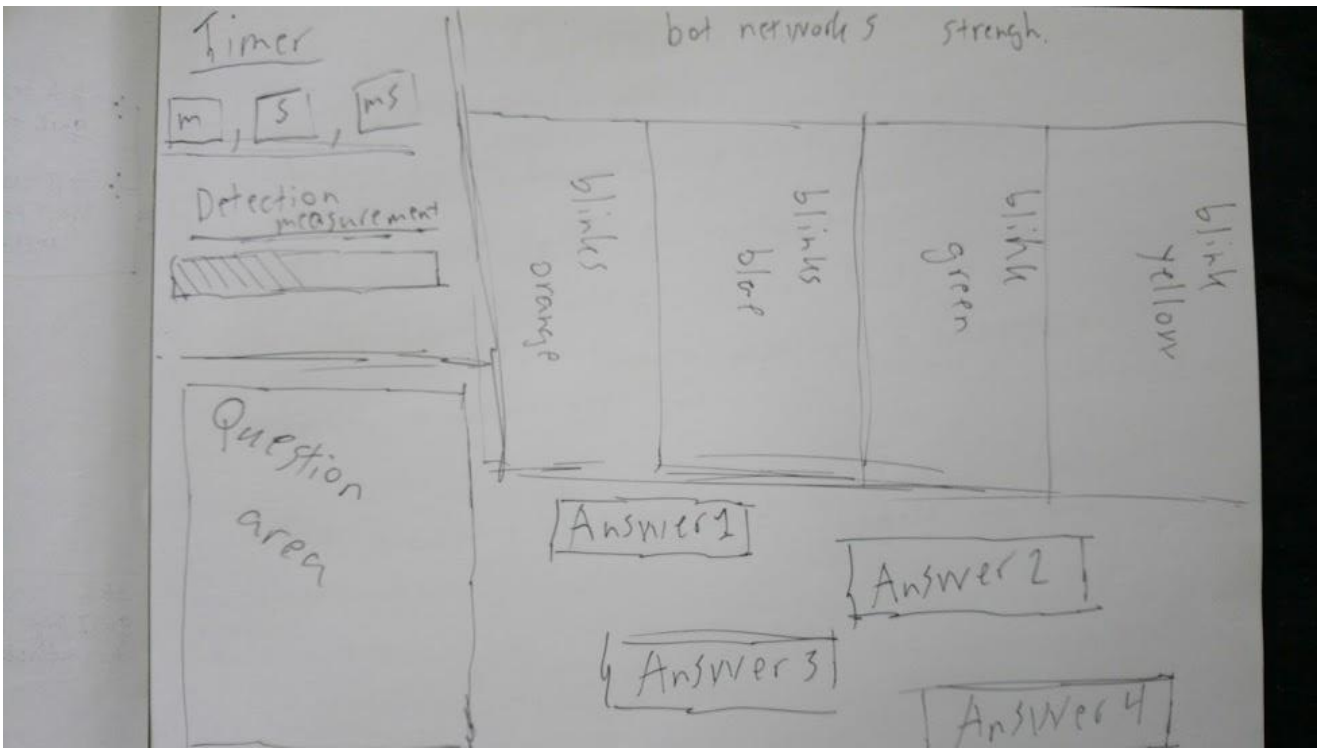


FIGURE 13 THE DRAWING OF 1ST ITERATION DESIGN IDEA

Design ideas was generated in different styles and amount with the focus around trivia being the programming of the hack while a secondary game needed to exist as a directional attack.

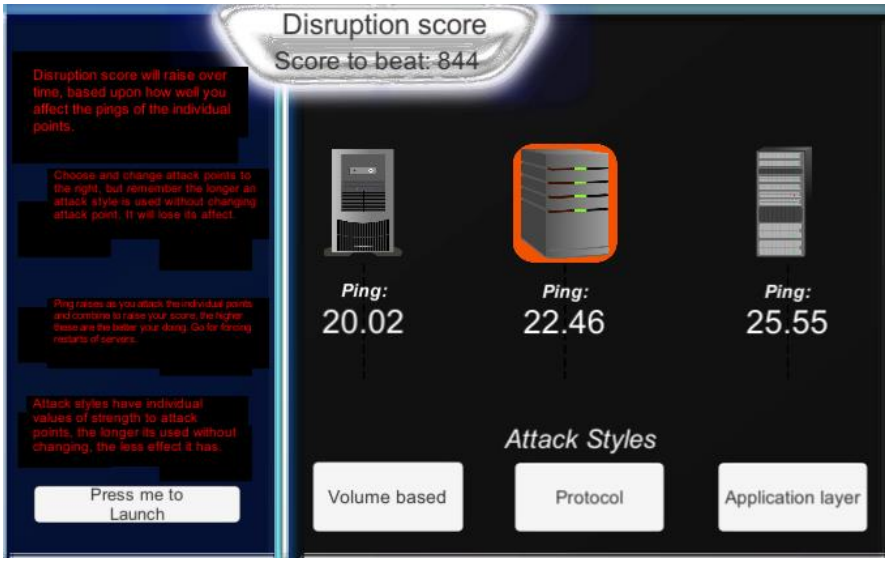


FIGURE 14 CLICK THE SERVER AND DETERMINE ATTACK STYLE OF YOUR DDOS

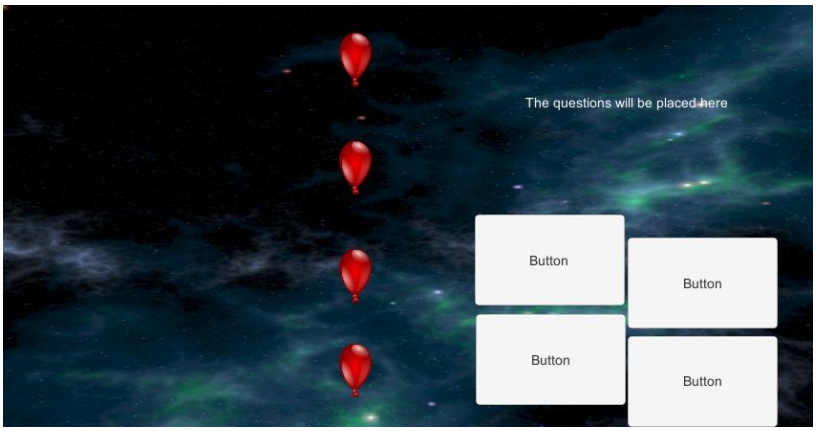


FIGURE 15 ARROW GAME, TRIVIA ANSWERING TO BLOCK THE BALLONS

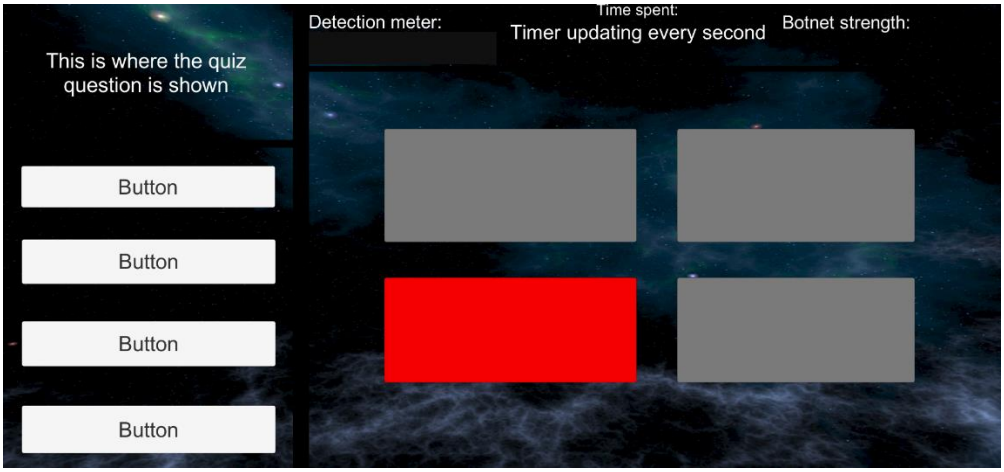


FIGURE 16 SIMON SAYS, DETECT THE PATTERNS

Though most of them had potential because of the dynamics they based upon, it was difficult for them to be usable in a split test scenario.

FINAL PRODUCT IDEA

The final product idea was based upon the principle of having the trivia game work as a charger, unlocking the speed of the attack slowly as you answer correctly.

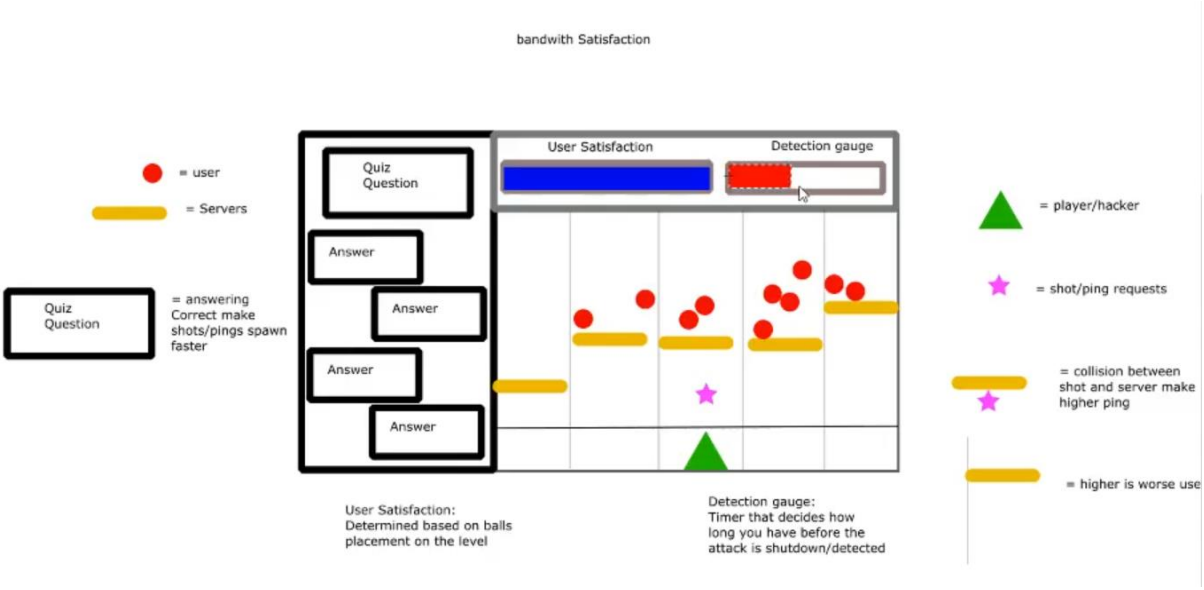


FIGURE 17 IMAGE TAKEN FROM PRESENTATION MOVIE OF THE IDEA

A presentation movie was produced and shown to three individuals who reacted with an understanding of the reasoning of the game mechanics chosen. It was all based upon a flood ping attack of the same style used against Sony Pictures in 2014. Not aimed at shutting server down but instead annoying users enough for them to leave.

GAME MECHANIC	REAL ATTACK
TRIVIA	Bot network
SHIP	Targeting server
SHOTS	Ping request
PLATFORMS	Servers
RAISED PLATFORM	Raised server bandwidth

A couple of modification was made to produce a timer and a short storyline which allowed the introduction of a tutorial.

FIGURE 18 IMAGE OF FINAL TEST A

Now the mechanic to modify based upon the accomplishment factor was in the movie presented as the users, and this kept onto the actual game.

FIGURE 19 IMAGE OF FINAL TEST B

OPENTDB

The trivia questions needed to be of a multitude of different styles and possible answers. Therefor instead of generating a list based upon personal knowledge. A license was looked for to get trivia questions for free.

Though after a while a serious of nicely written no came into the mailbox and the choice was made to use an open source trivia database, with the cost of questions being much harder.

https://opentdb.com/

The only real open trivia question database was found and 250 questions with 150 easy, 50 medium and 50 hard was generated for the game to use.

TESTING

For testing there was a couple of methods used, mostly presented during the methodology chapter there was a questionnaire referring to the demographics of the participants. Gameplay data had to be logged for later statistical testing of engagement based upon click frequency and playstyles.

After these two external questionnaires was also build, the first based upon the already presented play score questionnaire [54] during the Analysis sub chapter Measurements of play/fun .

The methodology chapter covers most of the reasoning for why the proxy environment is needed and design and implementation present how it's made this chapter will focus upon the two aspects of pre-launch testing and launching the artifact online

SMOKE TESTING

As the game artifact was designed for going online. There was no personal oversight if the test acted wrongly during a test participants interaction, for this purpose smoke testing was performed to check that the system could handle all its major functionalities without oversight for a long period of time.

Setting a macro to run and leaving the system to play nonstop for a total of 3 hours before returning showed a fully functional game still going through the level without break.

The smoke test was not in vain though, looking through the 3-hour debug log from Unity it was discovered that the PlayerID which was designed to chain information together. Was not being updated correctly and had repeats of the same playerID

PERFORMANCE TEST

As the test was online, there was no guarantee that the data collection would receive singular results or that it would be results in an expected fashion from the participants. Therefor five individual macro recordings were setup to play the game while being physically played at the same time by the author. Indented to verify the performance of the data receiving system would not crackle under any situation.

END–TO-END TESTS

As there was no supervision while playing this test it was important that that every device and situation was tested by a pre-testing situation. Leaving it to independent people to test it which had the prior experience to tell if something was wrong. This test revealed that though a long time had been used on the ability for the application to be run on any device the Unity WebGL plugin for mobile browsers had broken from the developers' side during the production of this artifact. Leaving no choice than remove mobile devices from supported applicants.

SPREADING THE TEST

For getting the test out into the participants hand it went through three stages of methods of distribution before ending the test.

First stage was spreading through social medias this included reddit, Facebook and forums of different origins

Hereis an example posted on a survey group

"So a bit of a different survey here that everyone can take, because its linked with a game. The game is built upon the dynamics of hacking and therefor I need as many test participants to answer my questions and play the game as I can. Just simply go to the link and start the game from your browser.

Thank you in advance

"

Though these posting did bring a few test participants into the game it was slow and inefficient.

Next stage was personal connections through social media, trying to get people of distant relationship to spread it amongst their friendship circle. Retaining from using direct or personal current friendship, family or promising rewards to not influence the results that would be received.

These posts normally requested acquaintances on social media to spread the game amongst their own friend circle in hope of getting more people for my master thesis.

Amongst the people received several offers returned this method of people willing to bring the game to events, here under a person bringing it to a workshop in Norway with 30 people. Another willing to bring it during a game bar in Aarhus for demoing. More examples exist and by the End of August a total of 400 participants had been promised from people bringing it to different places.

As people reported back that they had to take back their word about bringing the game to even the last final push for more people was made by physically move out to handout actual cards with a link to the game.

FIGURE 20 THE IMAGE OF A PAPER CARD HANDED OUT TO PEOPLE ACROSS COPENHAGEN

RESULTS

In this chapter the results of each individual area of the test will be presented by themselves for better overview to the discussion.

Before anything else every outlier or biased data was removed from the dataset here under four bots and two people with too much inside information of the test scenario.

All data from this point is measured in observational methods or using Office Excel for simple statistics and MATLAB for statistical analysis.

In total there was 58 test participants after scrubbing bad data which launched the game (N = 58).

Because of the test setup being online and unsupervised some people did not finish the questionnaires after the game resulting in less results after the gameplay was over.

This resulted in a total output of data as follows.

DATA ORIGIN	AMOUNT OF DATA INPUTS	AMOUNT OF PEOPLE /DATA ANSWERED
DEMOGRAPHIC QUESTIONS	413	58
GAMEPLAY LOGGING	3762	627
PLAY SCALE QUESTIONNAIRE	245	35
QUALITATIVE FEEDBACK	245	35

With a total amount of
25 playing test A
33 playing test B

QUALITATIVE DEMOGRAPHICS FINDINGS

As seen below here the general target demographics was well preserved with the intention of getting a sample group equal to what was seen from earlier in the survey presented to a hacker group.

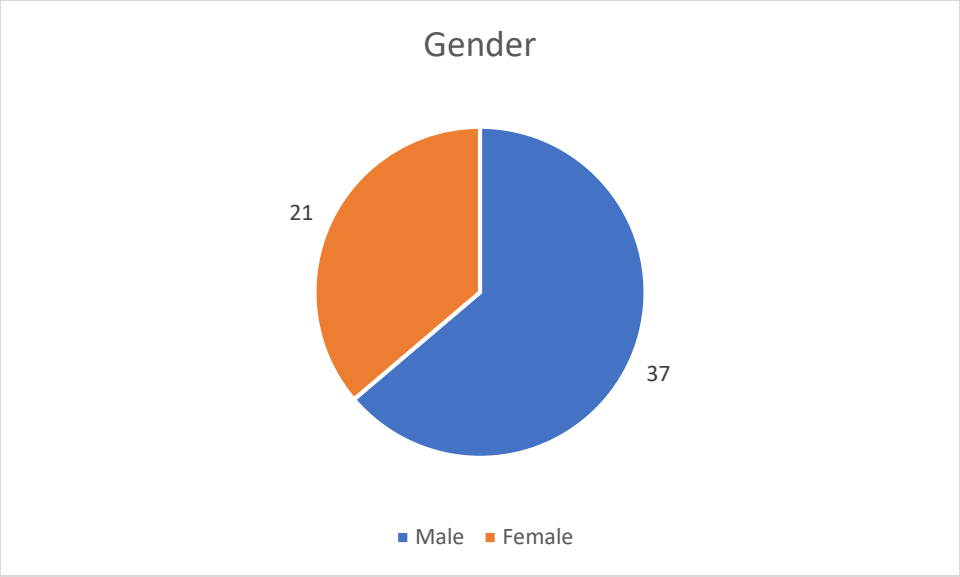


FIGURE 21 GENDER DIAGRAM.

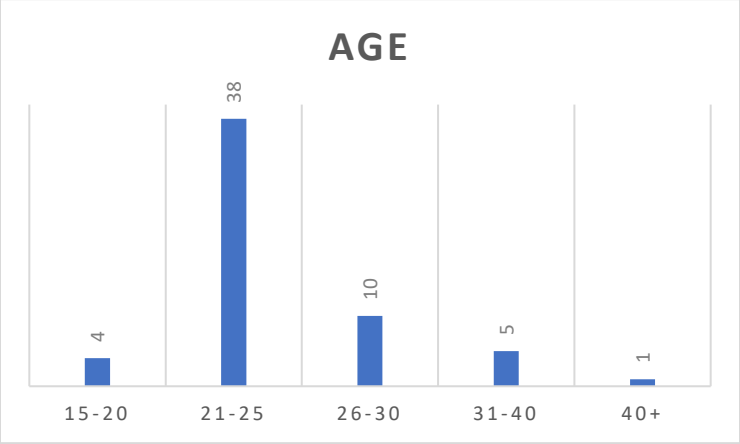


FIGURE 22 AGE PILLARS

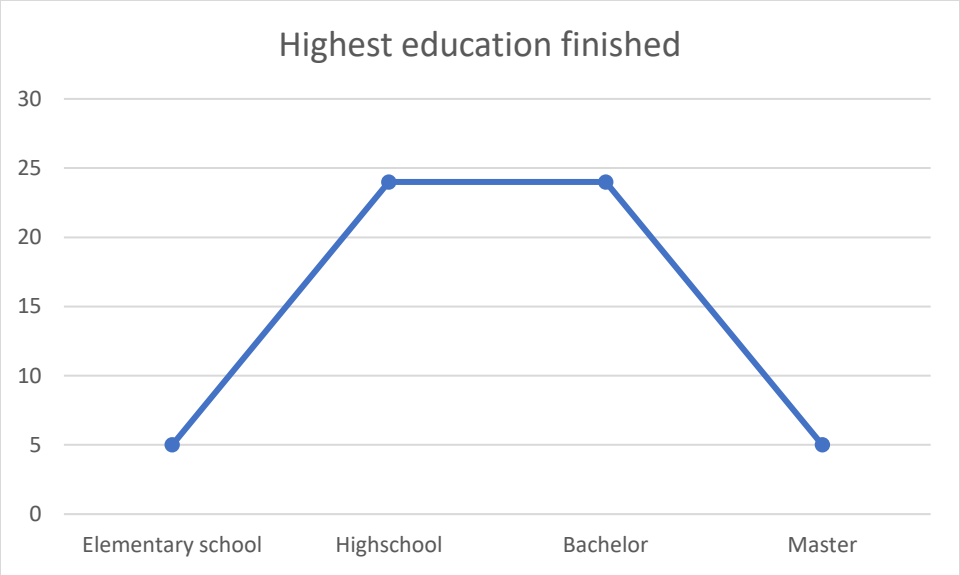


FIGURE 23 HIGHEST EDUCATION FINISHED

Though there exist five high school students and the five people outside the area of age for the target group, this thesis will continue with them staying in the data pool as it is deemed their contribution to the low data pool have more value than their cost on possible results.

GAME PLAY LOGS FINDINGS.

First moving through the gameplay logs to identify if any users took advantage of the pause menu as a game element or left mid through a data commit, which can be noticed by the timestamps having an unregular difference. Because its sending data through google form each timestamp is not perfect but should have between 30 to 59 seconds between them, less and something is wrong, or someone left and more there is an irregularity.

1. Qualitatively scanning of irregularity in timestamps yield no results.
2. Using Excel IF statement to find irregularity in timestamps yield no results.

BASIC STATISTICS

The gameplay logs are committed to send with a 30 second delay between every data point unless specific scenarios arise (like quitting game early), in these 30 seconds every click made in the game is logged with what they did and send as a combined string in the form of CVS style using “,” and “;” to separate data. Each commit also include time, level played, playerID, and how many users they have made leave in the game.

Here is presented some of the simple statistics found from the excel sheet

	Test A	Test B
Inputs of data received	301	177
Total clicks made	3950	2222
Average clicks per timestamp	13,12	12,56
Median of clicks per timestamp	7	7
Players began level 1	25	33
Player went to level 2	10	14
Player went to level 3	6	5

STATISTICAL DIFFERENCES

This part is aimed to monitor statistical differences in gameplay log files between the two tests aimed at providing knowledge toward the hypotheses.

This area will focus on the two null hypotheses

H0: There is no statistical difference between click rate received

After cleaning the data of outlier as earlier and making only the clicks counted for each data input separated into the two individual tests which end with two variables

ClickrateAClean = 300 inputs

ClickrateBClean = 180 inputs

Before running statistical difference on the results, its needed to identify if the datasets are parametric (Normally distributed)

For this purpose, a One-sample Kolmogorov-Smirnov test is performed on each of the datasets.

```
>> kstest(ClickRateAClean)

ans =

  logical

   1

>> kstest(ClickRateBClean)

ans =

  logical

   1
```

FIGURE 24 ONE-SAMPLE KOLMOGOROV-SMIRNOV TEST PERFORMED IN MATLAB

In both cases h = 1, which indicates a rejection of the null hypothesis that the data originate from a standard normally distribution. At the default 5% significance level.

With nonparametric results combined with an unequal sample size in the two datasets, the test parameters demand the need for a Wilcoxon rank sum test is performed to test the null hypothesis.

H0: The two sets of data exist from a continues distribution with equal medians.

```
>> [p,h,stats] = ranksum(ClickRateAClean,ClickRateBClean)

p =

    0.8951


h =

  logical

   0


stats =

  struct with fields:

       zval: 0.1318
    ranksum: 7.1892e+04
```

FIGURE 25 RUNNING A WILCOXON TEST THROUGH MATLAB

Running the Wilcoxon with the default two tailed, 5% significance and p value set to exact. The null hypothesis is not rejected with a p well over the 5% and H value showing hypothesis test showing failure to reject it.

Next is performed an analysis on the playstyles of participants between the two tests.

H0: There is no statistical difference between playstyles of the two tests

First the data is scrubbed and separate it into individual data sets as before.

This result in two datasets

PlaystyleA = 312 * 2 inputs

PlaystyleB = 315 * 2 inputs

Again, checking both datasets for normal distribution

```
>> kstest(PlaystyleA)

ans =

  logical

   1

>> kstest(PlaystyleB)

ans =

  logical

   1
```

Both being rejected of the null hypothesis that they exist from a normal standard distribution.

Since both datasets is nonparametric and unequal in amount the Wilcoxon rank sum test is performed on these data sets, but since the Wilcoxon MATLAB version only works with vectors separating the data into induvial assessment of playstyles of quiz, and player ship movement is needed instead of combined.

First presented is the null hypothesis that player ship movements are from a continues distribution with equal means.

```
>> [p,h,stats] = ranksum(PlaystyleA(:,1),PlaystyleB(:,1))

p =

   2.4756e-09


h =

  logical

   1


stats =

  struct with fields:

       zval: 5.9631
    ranksum: 111214
```

FIGURE 26 WILCOXON TEST RUN ON PLAYSTYLES OF SHIP MOVEMENT.

The low p value in addition to h = 1 indicate a rejection of the null hypothesis that players movement of ships come from a continuous distribution with equal mean.

Next, the same is done for player usage of the quiz element

```
>> [p,h,stats] = ranksum(PlaystyleA(:,2),PlaystyleB(:,2))

p =

    0.3471


h =

  logical

   0


stats =

  struct with fields:

       zval: -0.9403
    ranksum: 9.5852e+04
```

FIGURE 27 WILCOXON TEST RUN ON PLAYSTYLES OF QUIZ USAGE.

Here again as seen earlier the P value is higher and h = 0 indicate a failure to reject the null hypothesis that the players quiz usage comes from a continuous distribution with equal means.

GAMEPLAY OBSERVATION

Looking through the inputs of data from different participants there exist outliers in the number of clicks per data received.

Presented earlier was an average click rate of around 13 clicks per 30 seconds. But some players use different styles of receiving desired results.

Information of playstyles is separated here into people clicking more than 30 times per data input meaning minimum of one time every second. On other hand some participants might consider their moves for longer so another datapoint will be clicking less than 4 times per data input resulting in waiting more than 10 seconds per click.

Over 30 clicks per input of data	**51**
Less than 4 clicks per input of data	56

PLAY SCALE QUESTIONNAIRE FINDINGS.

After the player had decided to finish with the game they were presented with two questionnaires more. The first based upon questions from a Play scale experiment.

This section is aimed at running statistical analysis on the test result to figure out if the answers between test A and test B is considered statistically to be the same distribution.

Launching with scrubbing the data and separating the results into A and B data sets the next parameter is running KS test again with MATLAB to check for normal distribution (parametric)

```
>> kstest(TestAanswers)

ans =

  logical

   1
```

FIGURE 28 KSTEST RUN IN MATLAB ON THE ANSWERS FROM TEST A

```
>> kstest(TestBanswers)

ans =

  logical

   1
```

FIGURE 29 KSTEST RUN IN MATLAB ON THE ANSWERS FROM TEST B

This result in using Wilcoxon test as the data sets is non parametric and is unequal amounts.

```
>> for m = 1:5
ranksum(TestAanswers(:,m),TestBanswers(:,m))
end

ans =

    0.4460


ans =

    0.0686


ans =

    0.2196


ans =

    0.6726


ans =

    0.0575
```

FIGURE 30 RANKSUM WILCOXON MADE WITH MATLAB

As seen through the results of p values from the h = 0 in all of them. This means that the answers provided by the test participants is not statistically different between the A and B test.

QUALITATIVE FEEDBACK FINDINGS.

During the Qualitative feedback the writer opens the game to replicate the reported issues and mentioning's for better understanding.

QUESTION 1: GLITCHES AND BUGS

Couple of minor bugs happened with the quiz, the code making questions not being shown again can break resulting in someone seeing it three times. Including sometimes Text on questions does not appear in the online version. Bars (servers) got stuck as part of a physics engine glitch.

QUESTION 2: LEARNED ANYTHING ABOUT HACKING

This is a trick question since the game is based as a simulation able to be played by everyone if a person felt like they had learned something unexpected it would be a sign of biased info or a person to look towards.

The answers do indicate though an expectation of people wishing to see or learn something during the gameplay.

QUESTION 3: DID YOU EXPERIENCE FUN WHILE PLAYING ?

There are some answers which stand out between the no answers which show a bit of promise towards the earlier research and the indications of how people are playing.

"Not really, more of a "I HAVE TO BEAT THIS" kind of feeling."

"Yes, it was an interesting premise."

But an overwhelmingly negative reaction from people being confused and finding the game elements too slow or badly made.

Interestingly the foundation of using quizzes as coding might have been a success but the ship part being the confusing addition.

"Yes, the question was the fun part. The ship not so much."

"Yes, love quizzes"

QUESTION 4: EXPERIENCE IT WAS LACKING SOMETHING FOR A GAME

"Maybe more engagement in the form of a story"

This is interesting considering this thesis have already presented research which indicate of this narrative engagement being a game element which have drastic effect on engagement.

"The actual gameplay didn't really feel connected to the instructions, and I wasn't able to raise the green part as I think I should have? Because of the time it took to read each question I was only able to raise one blue thing at a time, but I didn't really understand why I had to raise them. The small explosions that were above the blue things gave absolutely no sense to me."

This person received the b test and is reacting confused mainly because handling the multitude of objects at the same time, but more interestingly the blue explosion he refers to is users leaving which in the B test would be expected to be confusing since you did not know they even existed.

Overall the results are again about confusion about what to do and better control schemes forward moving.

Question 5: reason for stopping playing

The answers here are as expected mostly no and that they gave up on moving forward or lost interest with the difficulty. Also a few mentions are about having plans or something else which when looking at their playtime did not affect any of the overall test results.

Discussion

With the overall test results now presented, this discussion chapter aims at providing the reader with a discussion of the combined results with the presented research earlier and compare them to the hypotheses presented as part of the problem statement.

During the result it was shown that none of the quantitative data was normally distributed aka non-parametric forcing this thesis to use Wilcoxon tests

This test is not necessary the most wished test to use but does present us with clear p values to identify that only a singular result was statistically different. This thesis aimed at providing results for three hypotheses where two of them was focused upon statistical change of the test participants.

And since most of this data is very clearly showing that it is conclusive this discussion will focus mainly upon the errors and possible changes needed which can be found from the qualitative research.

This discussion will from here be split into two sections to provide the user with a post mortem style discussion of three areas that the thesis saw as well done versus three flawed areas.

Success

This thesis aimed at any reader would have to reteach the meaning of being an actual hacker and what the term of hacking entailed. This was done by a singular chapter using a red thread in the form of history of the terms followed by a cruel reminder of the damage it can cause. This is seen as a success considering that the regular person has been taught the meanings of these terms through the policies of policing and the modern media, but the terms have a much deeper meaning.

This thesis also presented the motivation of hackers in a fashion which is very difficult to find in the first place. The current research and aims of organizations are normally attacking this trait of hacking in a fashion where even a white hat would be shamed by the public. Finding basis for motivation of hacking is difficult and most of the knowledge found is either too old or is found untrustworthy. So, through some alternative means and a few newer articles which finally look upon hacking motivations it was possible to document enough to present the idea that hackers have motivations outside the area of being criminal beings.

Last this thesis aimed at using interference instead of the nonhuman simulations or limited test participants normally found in this area of research. Though the test itself will exist in the flawed area the logic behind using target grouping and simulation of hacking in theory could provide the field of hacking research with a much-needed human touch in participants.

FLAWS

The artifact itself was flawed. As a game production normally takes either longer time or need more man power than a singular master student it should have been predicted that the results would receive a drastic negative feedback from participants lacking the standard of games today and another artifact or scenario could have been devised. It must be mentioned though that both sides of A and B test was flawed in the same fashion, so the results are impacted equally for both test scenarios.

The publishing of the game test on a web-based scenario could in theory function but, the alone scenario of it being made as a student project reduces peoples urge to try it. But more over the internet is a hard thing to predict which is also why there is research areas like “the internet of things” focused upon understanding the movement and flow of internet activity. Without extra research into how a product like this should create its own flow on the internet the test scenario will have to get a personal touch making the aspect of openness restricted by the choices of the authors like a physical test.

Last Is the flaw of doing this project as a master thesis. Through the research made and the conversations had with people in the industry etc. This area is much larger, and this research thesis was only able to work in it by taking a direct focus on a singular hacking term as the artifact focus and leave the rest for later research. Even with this in mind producing anything more than indication of possible results in the field of hacking would take a major insight into the world from not only the side of this thesis but also the side of the hackers.

LAST INSIGHTS

It should be noted that though this research might be interesting and promising no matter the results. The test scenario done in this thesis only produced a total of 58 participants. Inference which is used to bind regular participants results with hackers also is what allows science and social publications to generalize across a bigger group of people based upon a sample size. Even without cleaning the data this thesis was unable to produce a sample size large enough to show any results and as maximum can only be considered an indication of what to expect in future research.

CONCLUSION

This thesis presented a background of research to build a final problem statement about demonstrating the fun an aspect of hacking through a game simulation tested on regular people.

The thesis was unable to get enough participant to achieve actual results that can be scaled up but does have an indication of what results could look like.

The problem statement was accompanied with three individual hypotheses.

HYPOTHESIS 1:

Changing a dynamic of the simulation will statistically change people's engagement

HYPOTHESIS 2:

Changing a dynamic of the simulation will statistically change participants continuation desire

HYPOTHESIS 3:

Changing an element of the simulation will make have drastic changes in qualitative responds

Hypothesis 1 (H1): the first hypothesis was aimed at engagement as fun, though the qualitative results show a few people toying with the game mechanics and there exist answers that demonstrate engagement, the overall statistical analysis of results is a clear indicator of failing to reject a null hypothesis leaving the alternative H1 hypothesis unlikely in the current research scope.

Hypothesis 2(H2): The second hypothesis was aimed at continuation desire and was meant to be measured between people playing time and wish to go forward in the challenges. Though qualitatively you can see minor changes as example the drop off over time is much less during Test A than Test B, statistically there is no difference between A and B test leaving the lack of test participants again to be a dying factor for the qualitative value.

Hypothesis 3 (H3): The third hypothesis was aimed to illustrate that no matter the statistics the test participants will experience the break in absorption when playing a game missing an expected mechanic. This Hypothesis was partly accepted based upon the test result from the 35 answers. Though still too few to say it's a clear rejection of a null hypothesis, it does show a possible future of the project.

ARTIFACT HYPOTHESIS:

A game simulation of a DDoS attack will have qualitative assessment play styles resembling expected DDoS attack styles.

Looking through our results one might notice that the simulation game allowed people to change tactics and without hinting the players automatically modified their styles of "programming" from spear phishing compromised computer via using longer time on getting answers correct on quiz, to spamming it out as the email services know much too well since 1/10 is still a lot if you send a 100 a second. Noticing people's movement of the ship also included

a few trying to lift the server in specific manner while others seemed to have used a more strategic plan for dealing with the users.

For the end of this thesis, the results toward the final problem statement

If we reduce the accomplishment factor of the continuation desire dynamics from a game simulating a DDoS attack, are we then reducing the player engagement, as they are taking the role of the DDoS attacker, sufficiently to suggest implications for IT security countermeasures for DDoS hacking attacks

Seems to be focused a lot on the rejection of the problem. Though there seems to be foundation to being able to present hacking as a game, using game theories to measure their motivation of fun was in this thesis rejected overall.

SUGGESTIONS FOR FUTURE RESEARCH

If there should be a person or group who wished to use this thesis as an idea or foundation to continue in the line of fun in hackers. There is a couple of observations from this thesis which could be possible improvement of others.

1. Web based testing functions well if made correctly, including an ability to spread the test easier seemed to be an issue in this case.
2. Using test results from other sources might be a method to look at game design as hacking, this paper demonstrates its possible to build a game of the dynamics in hacking so its possible there already exist scenarios where the dynamics exist.

REFERENCES

[1] Sharpened productions, 2018. [Online]. Available: https://techterms.com/definition/hacker.

[2] Oxford, 2018. [Online]. Available: https://en.oxforddictionaries.com/definition/hacker.

[3] T. Jordan, »A genealogy of hacking,« *Convergence,* pp. 528--544, 2016.

[4] C. Perrin, »Hacker vs. cracker,« 2018. [Online]. Available: https://www.techrepublic.com/blog/it-security/hacker-vs-cracker/.

[5] cambridge college, 2018. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/hacking.

[6] R. a. o. Barber, »Hacking techniques: The tools that hackers use, and how they are evolving to become more sophisticated.,« Elsevier, 2001.

[7] »What Is 'Brute Force' Dictionary Hacking?,« 2018. [Online]. Available: https://www.lifewire.com/brute-force-dictionary-hacking-4061418 .

[8] »Why everything is hackable,« 2017. [Online]. Available: https://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security.

[9] D. Elsom, »Five of the worst cases of cyber crime the world has ever seen – from data theft of one BILLION Yahoo users to crippling the NHS,« 31 6 2017. [Online]. Available: https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/.

[10] K. Friesland, »10 of the Worst Cyber Crimes in History,« 20 10 2017. [Online]. Available: https://www.technadu.com/biggest-cyber-crimes/9094/.

[11] L. Newman, »Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts,« 2018. [Online]. Available: https://www.wired.com/story/yahoo-breach-three-billion-accounts/.

[12] Norton, »CyberCrime,« 2018. [Online]. Available: https://www.nortonsecurityonline.com/security-center/cybercrime.html.

[13] »What Is a Computer Worm?,« [Online]. Available: https://www.nortonsecurityonline.com/security-center/computer-worms.html.

[14] Norton security, »Malware - Viruses, Worms, Trojan Horses, Spyware, Bots, Rootkits, Ransomware,« [Online]. Available: https://www.nortonsecurityonline.com/security-center/malware.html.

[15] Noton security, »Computer Viruses,« [Online]. Available: https://www.nortonsecurityonline.com/security-center/computer-viruses.html.

[16] G. Torres, »What is a computer virus?,« 18 12 2017. [Online]. Available: https://avg-2683519.hs-sites.com/en/signal/what-is-a-computer-virus.

[17] Norton security, »About Phishing,« [Online]. Available: https://www.nortonsecurityonline.com/security-center/phishing.html.

[18] J. Regan, »What is Phishing? The Ultimate Guide to Phishing Emails and Scams,« 16 2 2018. [Online]. Available: https://avg-2683519.hs-sites.com/en/signal/what-is-phishing.

[19] Symantec, »DOS attacks explained,« [Online]. Available: DOS attacks explained.

[20] J. Regan, »The ultimate guide to Denial of Service (DoS) attacks,« 3 7 2018. [Online]. Available: https://www.avg.com/en/signal/what-is-ddos-attack.

[21] GrayHat4Life, »7 Types of Hackers You Should Know,« 9 9 2015. [Online]. Available: https://www.cybrary.it/0p3n/types-of-hackers/.

[22] Symantec , »What is the Difference Between Black, White and Grey Hat Hackers?,« [Online]. Available: What is the Difference Between Black, White and Grey Hat Hackers?.

[23] I. A. Hamilton, »The boss of 'Fortnite' spent days attacking Google for scoring 'cheap PR points' by exposing a flaw in the game's security,« 18 8 2018. [Online]. Available: https://nordic.businessinsider.com/epic-games-ceo-tim-sweeney-attacks-google-over-fortnite-bug-2018-8?r=US&IR=T.

[24] E. Kovacs, »Tesla Increases Bug Bounty Payout After Experts Hack Model S,« 10 8 2015. [Online]. Available: https://www.securityweek.com/tesla-increases-bug-bounty-payout-after-experts-hack-model-s.

[25] N. Murray, Instruktør, *Bill Nye saves the world (Season 2, Ep 2).* [Film]. 2017.

[26] B. Knappenberger, Instruktør, *We are legion: the story of the hacktivists.* [Film]. 2012.

[27] J. Regan, »The Most Dangerous Hackers Today,« 24 7 2018. [Online]. Available: https://avg-2683519.hs-sites.com/en/signal/the-most-dangerous-hackers-today.

[28] Y. a. L. X. a. P. M. a. C. Y. Lu, »Social network analysis of a criminal hacker community,« *Journal of Computer Information Systems*, pp. 31--41, 2010.

[29] Urban dictionary, »Trolling,« 2 1 2014. [Online]. Available: https://www.urbandictionary.com/define.php?term=Trolling.

[30] B. W. J. B. C. D. Karim R. Lakhani, *The Boston Consulting Group Hacker Survey.*

[31] R. F. O. a. R. K. M. a. K. R. G. A. a. P. A. G. a. S. A. J. A. a. V. P. B. V. Cayubit, »A Cyber Phenomenon: A Q-Analysis on the Motivation of Computer Hackers,« *Psychological Studies*, pp. 386--394, 2017.

[32] Symentec, »Internet security threat report,« 2018. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

[33] Microsoft, »Beskyt min computer med Windows Defender,« 7 6 2018. [Online]. Available: https://support.microsoft.com/da-dk/help/17464/help-protect-my-computer-with-windows-defender.

[34] T. Klosowski, »Gmail Now Tells You Why Email Ends Up in Your Spam Folder,« 20 3 2012. [Online]. Available: https://lifehacker.com/5894793/gmail-now-tells-you-why-email-ends-up-in-your-spam-folder.

[35] E. Kavanagh, »Botnets: One Down, But How Many Are Still Out There?,« 2018. [Online]. Available: https://www.nortonsecurityonline.com/blog/botnets-one-down-but-how-many-are-still-out-there/.

[36] Bullguard, 2018. [Online]. Available: https://www.bullguard.com/da/landing-pages/ppc/antivirus-offer.aspx?&utm_medium=cpc&utm_source=google&utm_content=Offer&utm_campaign=NonBrand_DK&utm_term=antivirus%20software&gclid=EAIaIQobChMI-PzAkuSo3QIVj1QYCh2B6wRAEAAYAyAAEgKaXvD_BwE.

[37] Symantec, 2018. [Online]. Available: https://www.symantec.com/.

[38] Norton Security, »Norton Security – Comparison to other Security Software Vendors,« 2018. [Online]. Available: https://www.nortonsecurityonline.com/norton-comparison.html.

[39] Microsoft, »Azure DDoS Protection Standard overview,« 29 03 2018. [Online]. Available: https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview.

[40] »How to Clean a WordPress Hack,« 31 1 2018. [Online]. Available: https://sucuri.net/guides/how-to-clean-hacked-wordpress.

[41] »How to Fix a Hacked WordPress Site,« 11 4 2018. [Online]. Available: https://www.tripwire.com/state-of-security/security-awareness/fix-hacked-wordpress-site/.

[42] A. Etzioni, »Cybersecurity in the private sector,« *Issues in Science and Technology*, pp. 58--62, 2011.

[43] Game-Sec, »Conference on Decision and Game Theory for Security,« 2018. [Online]. Available: http://www.gamesec-conf.org/papers.php.

[44] M. H. a. Z. Q. a. A. T. a. B. T. a. H. J.-P. Manshaei, »Game theory meets network security and privacy,« *ACM Computing Surveys (CSUR)*, p. 25, 2013.

[45] A. Gueye, »A game theoretical approach to communication security,« UC Berkeley, 2011.

[46] R. a. L. M. a. Z. R. Hunicke, »MDA: A formal approach to game design and game research,« i *Proceedings of the AAAI Workshop on Challenges in Game AI*, 2004, p. 1722.

[47] K. a. A. N. Mitgutsch, »Purposeful by design?: a serious game design assessment framework,« i *Proceedings of the International Conference on the foundations of digital games*, ACM, 2012, pp. 121--128.

[48] U. a. C. M. a. V. P. Ritterfeld, Serious games: Mechanisms and effects, Routledge, 2009.

[49] H. L. a. T. E. G. O'Brien, »What is user engagement? A conceptual framework for defining user engagement with technology,« *Journal of the American society for Information Science and Technology*, pp. 938--955, 2008.

[50] S. a. H. M. S. Osborne, »Effective employee engagement in the workplace,« *International Journal of Applied Management and Technology*, p. 4, 2017.

[51] H. a. B. T. Schønau-Fog, »"Sure, I Would Like to Continue" A Method for Mapping the Experience of Engagement in Video Games,« *Bulletin of Science, Technology \& Society*, pp. 405--412, 2012.

[52] D. a. J. H. A. a. D. A. a. S.-F. H. Stankevicius, »A Factor-Based Exploration of Players Continuation Desire in Free-to-Play Mobile Games,« *Artificial Intelligence and Interactive Digital Entertainment ConferenceArtificial Intelligence and Interactive Digital Entertainment*, pp. 36--42, 2015.

[53] H. Schoenau-Fog, »The Player Engagement Process-An Exploration of Continuation Desire in Digital Games.,« *DiGRA Conference*, 2011.

[54] D. Pavlas, »A Model Of Flow And Play In Game-based Learning The Impact Of Game Characteristics, Player Traits, And Player States,« 2010.

[55] S. a. D. D. a. K. R. a. N. L. Deterding, »From game design elements to gamefulness: defining gamification,« i *Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments*, ACM, 2011, pp. 9--15.

[56] J. a. K. J. a. S. H. Hamari, »Does gamification work?--a literature review of empirical studies on gamification,« i *2014 47th Hawaii international conference on system sciences (HICSS)*, IEEE, 2014, pp. 3025--3034.

[57] L. B. a. H. K. M. a. K. R. Andersen, »Metoder i statskundskab,« Rosinante\&Co., 2010, p. 32.

[58] L. Jacobsen, »Hackersagen: Her er paragrafferne som de to hackere er blevet dømt efter,« 30 10 2014. [Online]. Available: https://www.computerworld.dk/art/232305/hackersagen-her-er-paragrafferne-som-de-to-hackere-er-blevet-doemt-efter.

[59] Danish criminal law, »Straffeloven paragraf 21,« [Online]. Available: https://www.foxylex.dk/straffeloven/21/.

APPENDIX

HACKER QUESTIONNAIRE APPENDIX 1:

Tidsstempel Gender Age Highest finished education What type of hacker would you classify yourself as ? How long have you been a hacker ?On a scale where 1 is reading source code from a website and 10 is crippling world economy, what would you rate your own ability as Of the following statements, which hold true to you? I hack because … Choose multiple Of these following expressions, which do you see yourself in? When I hack I will … Choose multiple

28/05/2018 11.12.01 Male 30 + Bachelor degree Ecucational based hacker 5 to 10 years 4 It's fun., It's challange., Working together with others to solve the task at hand., Each breakthrough opens a new possibility for a task., I'm curious to know if I can do it., I'm curious how things work., I can use it across other work tasks. Lose track of time., Explore beyond the original assignment., Lose awareness of my surroundings, Get wound up about the task., Keep going feeling like I cannot stop before finished., Keep working longer than I planned.

28/05/2018 11.21.45 Male 25-30 Bachelor degree Friendly hacker 5 to 10 years 7 It's fun., It's challange., I already work with technical IT security including research and root cause analysis. Explore beyond the original assignment., Get wound up about the task., Keep going feeling like I cannot stop before finished., Keep working longer than I planned., lose the feeling of being tired.

28/05/2018 11.36.18 Male 30 + Middle school Friendly hacker 10+ years 8 It's fun., It's challange., Each breakthrough opens a new possibility for a task., I'm curious how things work., I believe it can make me better for a future job., I want to earn money from it. Take notes to improve my future work., Keep working longer than I planned.

28/05/2018 11.54.35 Female 19-24 High school A mix of educational, curious, friendly, white hat hacker 1 to 3 years 3 It's fun., It's challange., Working together with others to solve the task at hand., I'm curious how things work. Ask for help across multiple sources to finish the assignment., I get tired as fuck.. but it's fun and interesting

28/05/2018 16.57.05 Male 30 + Kort videregående Staten sponsored 10+ years 6 It's fun., It's challange., I'm curious how things work., I want to earn money from it. Take notes to improve my future work., Explore beyond the original assignment., Keep going feeling like I cannot stop before finished., Keep working longer than I planned.

28/05/2018 21.48.51 Male 25-30 Bachelor degree Ecucational based hacker 3 to 5 years 7 It's fun., It's challange., Working together with others to solve the task at hand., I'm curious how things work., I can use it across other work tasks. Take notes to improve my future work., Keep going feeling like I cannot stop before finished.

31/05/2018 11.31.35 Male 30 + Master's degree Ecucational based hacker 5 to 10 years 7 It's fun., It's challange., I'm curious how things work. Lose track of time., Take notes to improve my future work., Explore beyond the original assignment., Lose awareness of my surroundings, Get wound up about the task., Keep going feeling like I cannot stop before finished., lose the feeling of being tired.

31/05/2018 13.51.21 Male 25-30 Master's degree Ecucational based hacker 3 to 5 years 6

It's fun., It's challange., I'm curious how things work., I believe it can make me better for a future job. Lose track of time., Keep going feeling like I cannot stop before finished., Keep working longer than I planned., lose the feeling of being tired.

04/06/2018 14.43.29 Male 19-24 High school Ecucational based hacker Less than a year 3

It's challange., I'm curious to know if I can do it., I'm curious how things work. Take notes to improve my future work., Get wound up about the task., Keep going feeling like I cannot stop before finished., Keep working longer than I planned.