SECURITY THREATS IN ONLINE GAMING

4th Semester Exam

Author: Bianca Helbo Olsen

Supervisor: Michael Claudius

Date: 01/06/17

22911 character (including spaces), 3972 words.

Zealand Institute of Business and Technology
IT Security Elective Course – 4th Semester

Contents

Introduction

Playing games over the internet is a big part of many people's online activities. You trustingly share much personal information with the companies running these games, and it is important to stay secure. With this synopsis, I would like to consider the various kinds of security threats that affect people playing online games, such as Massively Multiplayer Online games, to find the biggest and most common threat and how to protect against it.

Motivation

I've chosen this subject, because it's interesting to me to find out how this widespread hobby could be filled with so many security threats and because video games are a personal hobby and a big part of my life, being secure while online is very important to me.

Problem definition

To dive deeper into this subject, I came up with these questions I will be attempting to answer.

Main question

- What is the biggest security threat in online gaming?

Sub-questions

- How do you most effectively protect yourself against the various security threats in online gaming?
- What value could the hackers be seeking in the player's account?
- What measures do game companies take to protect their costumers?

Method

A list of activities I will do to try to reach the answers to my questions. Note: I will find most of my sources on the internet, but I will try to look mostly at articles after 2010 for a more up-to-date look on the subject.

- Researching
    - Articles and studies on the internet related to the subject.
- Questionnaire
    - To gain insight on how many people have gotten their gaming accounts hacked, and what they've lost.
- Practical work – Potentially considering replicating a Two Factor Authentication.
    - Gaining knowledge on how this security precaution works.

Activities

The time budget is 5 weeks – week 18 to week 22. I will divide the activities into weeks.

I would like to be spending the first week gathering and reading materials and sources and getting a questionnaire send out.

The second week will be for analysing the sources and the questionnaire data.

The third week will be for the practical work.

The fourth week, I will be starting to answer my main and sub-questions with the information found.

The fifth week will be for putting the synopsis together and polishing.

Planning

I have created a table for a better overview of what activities I will be doing during the five weeks, this also includes if there are any specific days to mark for some of the activities. I have made an estimate of how many days of a week I will be spending on each activity. My work week will consist of 7 days.

Weekly Schedule

Week Number	Activity	Days Spend	Specific Date Marks
18	Gathering and reading material. Creating and sending out questionnaire.	6 days 1 day	May 3rd: Questionnaire made and posted.
19	Analysing materials Analysing questionnaire data.	5 days 2 days	May 11th: Looking at questionnaire data.
20	Working on Two Factor Authentication.	7 days	
21	Answering main questions Answering sub-questions.	4 days 3 days	
22	Synopsis writing. Polishing	5 days 1 days + time left on June 2nd.	June 2nd at 11:00: Delivery.

Research

In this section I will lay out and document the knowledge I gained from my research process during the duration of this project. It will be split into parts, each part belonging to some of the activities I have mentioned earlier. Furthermore, I will start forming the answers to my sub-questions based on the research. The main question, I will be discussing at the oral exam.

Reading relevant articles and studies

Searching for and reading several articles and websites helped me in starting to get a good impression of what threats are the most prominent and well-known out there. When trying to be critical of my sources, I looked for articles from as close to 2017 as possible, but looking at none before 2010, to get the most up-to-date and modern view on this as I possibly can. Most of the independent web-pages involving IT and IT-security that I found, agreed on roughly the same types of attacks as the most common or threatening to gamers, and gave useful information about them and examples of instances of these attacks. From reading the articles, I could narrow down the different attacks to some that I find the most relevant and useful for my investigation.

Ransomware

Ransomware in general, is malware, that infects your system and encrypts your files, rendering them unusable by the victim. The hackers will then demand a ransom, like money or bitcoins, from the victim to free them. Although, not a new threat, it is becoming more prominent and as they become more sophisticated, the risk only increases. An example in the gaming community from a few years ago, is TeslaCrypt. It encrypts game related files, like saved games, configurations files etc. TeslaCrypt targets over 40 well-known and popular games[1]. It is, however, no longer operational[2].

[1] http://www.techsling.com/2017/03/top-3-security-threats-online-gamers-avoid/

[2] https://www.welivesecurity.com/2016/08/31/top-5-threats-online-gamers-avoid/

Keyloggers

Keyloggers are malware that monitors and records keyboard use to obtain every stroke, making it possible for hackers to obtain passwords, credit card information, PINs, etc. It's not just a threat to gamers, but every computer user, as they can give the attacker access to bank accounts and social security information[3].

Password Stealers

Scams such as password stealers relies on social engineering to fool the player into giving their access credentials. A popular method is through chatting with the victim[2], asking him to join their team and praising him for his skills, but the victim will be required to follow a link to install an application, such as a voice communication program, to be able to join. The downloaded executable is malware capable of stealing account credentials. Two examples of this malware are 32/PSW.OnLineGames.NNU and Win32/PSW.OnLineGames.OUM. They look for data of well-known games and execute commands from a remote server that tries to destroy any antivirus software on the system. In 2016, the number of detections of Win32/PSW.OnLineGames threats reached over a quarter million[1].

Phishing

Phishing is common and easy to carry out[2], stealing account credentials through fake e-mails which links to fake websites made to look like the original and with a similar domain name and then asking for log in credentials to steal your data to potentially resell or your bank information for your money[4].

The Hacker's Goal

One goal of a hacker could be, to get access to several things[4]: In-game resources, well-developed game characters, paid game accounts or credit card data itself. Credit card information is the most difficult to receive, since most companies keep the information hidden on the account page, by for instance only displaying the last 4 numbers on the card, so even if the hacker gained access to the account, they wouldn't get access to the credit card information. The others are attainable by the methods mentioned earlier in the synopsis. The further you progress in a game, the more cautious you should be with your account as your account or characters could be worth a lot on a black/grey market, as the hackers usually can transfer a character from the account to their own. It is of course possible for the owner of the account to catch and report it in time before the hackers get to transfer anything, and the companies can then make sure to make a password reset on the account to stop the hackers. Many companies have also started sending an email or, via a phone service, a SMS to the costumer if their account is accessed from a country different from the owner's, which can add some extra security to the player.

Threats Against the Companies

Attacks targeting the game company can turn out to be just an inconvenience for the player, but could also be a threat to their personal information. Extortion hacks[5] are when hackers have gained access to the company's sensitive/customer data, and threaten to release it if a certain demand is not met. This could mean, that the company's whole costumer database, that could include sensitive

[3] http://www.bankinfosecurity.com/how-to-beat-keyloggers-a-2999

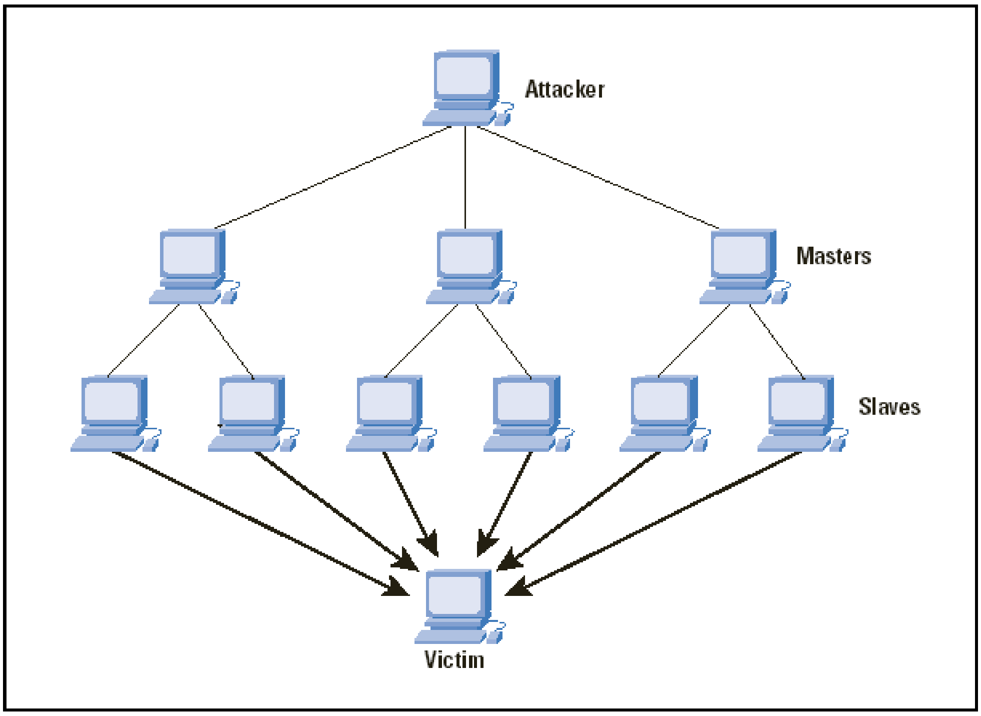
[4] https://blog.kaspersky.com/online-gamer-threats/4474/

[5] https://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/

information, could be leaked. An example of this happening recently, is the PlayStation Network leaks were millions of accounts were leaked.[6]

Another more passive threat is the DDoS (Distributed Denial-of-Service) attacks. Very easy to launch and a big nuisance for companies and customers, causing downtime on the services. In the gaming industry, they are aimed at the network layer, bombarding the servers with requests until they slow down or the connections collapse. A rapidly increasing "trend", the reported number of incidents doubled in 2014 and still growing.[7]

Figure 1, DDoS attack[8]



A recent higher profile example, although one of many, is game developer Blizzard Entertainment, owner of one of the biggest player bases, being hit by a DDoS attack in late 2016[9], carried out by hacker group PoodleCorp, targeting Blizzard's ISP. The group publicly announced the attacks on twitter, starting on a Tuesday, asking for 2000 retweets to stop the attack, and a second attack the day after, this time asking for 3000 retweets. Both attacks lasting around 3 hours resulted in a lot of angry players. DDoS attacks on Blizzard Entertainment is a quite common occurrence, targeting authentication servers and ISPs, sometimes several attacks in a month, due to how easy DDoS attacks are to carry out. To try to combat these attacks, Blizzard needs to work with all their network providers and make sure all their servers are protected against the attacks. Because all their games are dependent on the Battle.net servers, this this means, that if they go offline, players are completely locked out of all their games. Although not possible to combat all kinds of DDoS attacks, they can do a couple of things to mitigate them: They could make sure they have all the necessary firewalls and tools to identify phony traffic and a set of back-up servers and a dynamic pool, so that,

[6] http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html

[7] https://www.incapsula.com/blog/ddos-attacks-on-online-gaming-servers.html

[8] http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

[9] http://bestsecuritysearch.com/blizzard-poodlecorp-new-ddos-attacks/

in case of a DDoS attack, they can employ additional servers so they won't be brought down completely.[10]

The company can identify the fake traffic by analysing a couple of traits that points to a bot net is attacking you.[11]

- Bounce rate (entering and leaving): If the bounce rate is extremely high.
- Pages per session: If the pages per session is extremely low.
- Average session duration: If the average session duration is extremely low.
- New sessions: An extremely high percentage of new sessions.

An effective way a company can defend their player base, is by creating a strong authentication method.[12] Examples of Two Factor Authentications in gaming, such as the Steam Guard and Blizzard authenticator added additional security layers against account theft. The standard Blizzard authenticator works as follows: The player obtains either a device or the mobile app that gets linked to the player's account (Battle.net account). When logging in to the service, the player is not only required to enter the username and password for the account, but also the authentication code that they receive from the device or app. The authentication code that the device or app produces, is a user-specific 8-digit code every 15 seconds which remains valid for 2 minutes. If all information is entered correctly, access if granted, if not login fails. Hackers have managed to find ways to working around the authenticator, by installing files on the victim's computer, carrying out a man-in-the-middle-esque attack, possibly using a fake server, intercepting account information and authentication code while giving the player a fake authentication code and getting a small window to enter the correct one. Blizzard later combated this by making an authenticator code only valid once. Additionally, to unlink an authenticator from an account, you must submit two consecutive authenticator codes, thus making it very difficult with for attackers having used the man-in-the-middle methods. Since then, the mobile app has been updated, by instead of having to type in an authenticator code, the login will trigger an authentication request on the app, stating a code, where in the world the request is coming from and when, there is a choice to approve or deny the login request[13]. Since the mobile authenticator is tied to a specific phone, and no longer requires a code to be manually entered, it makes it harder for hackers to obtain.

Questionnaire Data

To try to get some information of how many people have gotten an online game account hacked and if they knew how they got hacked, I created a very short questionnaire to send out to some peers in my network. In this section, I will go through the answers and decide whether they will contribute to finding the answers I am looking for.

17 people responded to my questionnaire and their answers were like so:

In a checklist of what security measures, they use on their PC, 15 people have a Firewall, 16 people have a virus scanner, 1 person has nothing and 1 person selected other.

Out of 17 people, 10 people have had an online gaming account hacked, so only these 10 will have given answers for the rest of the survey.

[10] https://venturebeat.com/2016/08/31/how-blizzard-should-prepare-for-next-wave-of-ddos-attacks/

[11] https://support.flippa.com/hc/en-us/articles/202891420-What-is-fake-traffic-How-can-I-identify-it-

[12] http://www.cs.ru.nl/bachelorscripties/2011/Rens_van_Summeren___0413372___Security_in_Online_Gaming.pdf p. 24

[13] https://us.battle.net/support/en/article/100588

Asking if they know how hackers got access to their account. 7 people did not, but 3 people did.

The 3 people that knew how they were hacked, named these reasons: Keylogger, weak password, third party expansion software (like the Curse Client).

Out of the 10 people that were hacked, 9 people had in-game items (equipment, weapons, etc.), currency and/or characters stolen and 1 had nothing stolen.

I was trying to look for a trend in badly secured computers leading to more hacking, but it seems that the far majority is using a virus scanner and possibly the default windows firewall to protect themselves, but still the majority has been hacked before. Most of the people hacked did not know exactly how the hackers got access to their accounts, but the ones that did know named some of the top reasons that I mentioned earlier in my synopsis, making it clearer that they are big threats to gamers. The answers also confirmed to me that the hackers are very often going for the in-game content of the account, more than the usually well concealed credit card information.

Creating a Two Factor Authenticator

To try to get a better insight on how to two factor authentication work, I wanted to attempt to create an application that simulates the process. I looked into using the services Authy and the Google Authenticator to implement it with a simple Asp.NET web application, but after days of attempting to get it working, I decided to do some research on how the Google Authenticator on phones work instead. By doing this, I should be able to gain some of the same knowledge about 2FA, that I would've gotten by doing more practical work.

The Google authenticator implements the Time-Based One-Time Password (TOTP) that uses the following things[14].

- A unique secret in the form of a sequence of bytes.
- An input derivative of the current time.
- A signing function.

The shared secret is what you need to obtain to set up your account on your phone, either by scanning a QR code or entering the secret manually. The secret is base-32 encoded. For manual entry the secret has the following format.

```
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
```

The input in current time value will be received from the phone. It is of course important that the time on the phone is accurate as the server will essentially repeat what happens on your phone using the current time as known by the server. The server will compare the submitted tokens to all tokens generated in a window of time (a couple of minutes) to account for time it can take you to enter the token and send it to the server.

The signing function used is HMAC-SHA1. Using HMAC allows us to verify authenticity – only users knowing the secret can generate the same output for the same input (time). The algorithm can look something like this14[14]:

```
hmac = SHA1(secret + SHA1(secret + input))
```

[14] https://garbagecollected.org/2014/09/14/how-google-authenticator-works/

Looking more into this algorithm, we'll first need to base-32 decode the secret. Since google presents it with spaces and in lowercase to make it more readable, but base-32 does not allow spaces and only allows uppercase, we'll need to account for that:

```
original_secret = xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
secret = BASE32_DECODE(TO_UPPERCASE(REMOVE_SPACES(original_secret)))
```

Next, we will need the current time for the input. In this example, they use UNIX time.

```
input = CURRENT_UNIX_TIME()
```

Since Google Authenticator codes are viable for some time before changing to the next value, we need to account for that. The default amount of time a code is viable is 30 seconds. We can simply do an integer divide by 30 to get a value that will remain stable in a 30 second time window. We don't really care if the value has a particular scale, as long as the value is reproducible on both sides.

```
input = CURRENT_UNIX_TIME() / 30
```

Lastly, we apply the signing function:

```
original_secret = xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
secret = BASE32_DECODE(TO_UPPERCASE(REMOVE_SPACES(original_secret)))
input = CURRENT_UNIX_TIME() / 30
hmac = SHA1(secret + SHA1(secret + input))
```

This will in theory provide effective Two Factor Authentication, but the resulting HMAC value will be a standard length SHA1 value, which is 20 bytes or 40 hex characters, which is far to long for anyone to want to type in. So, we will want to convert it down to 6-digits, far easier for users to enter.

To convert SHA1 to a 6-digit number. We will use the last 4 bits of the SHA1 (a value ranging from 0-15) to index into the 20-byte value and use the next 4 bytes at that index, so we'll get:

```
four_bytes = hmac[LAST_BYTE(hmac):LAST_BYTE(hmac) + 4]
```

We can now turn these into a standard 32 bit unsigned integer:

```
large_integer = INT(four_bytes)
```

This will still be a large number, so we will need to slim it down a bit further. We can get a guaranteed 6-digit number by using the remainder of dividing the first by the first 7-digit number:

```
large_integer = INT(four_bytes)
small_integer = large_integer % 1,000,000
```

This will be our final value, and here's the whole process together:

```
original_secret = xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
secret = BASE32_DECODE(TO_UPPERCASE(REMOVE_SPACES(original_secret)))
input = CURRENT_UNIX_TIME() / 30
hmac = SHA1(secret + SHA1(secret + input))
four_bytes = hmac[LAST_BYTE(hmac):LAST_BYTE(hmac) + 4]
large_integer = INT(four_bytes)
small_integer = large_integer % 1,000,000
```

This could be an example of how a 2FA works with a TOTP.

Conclusion

From the research I've done to answer my questions, I've concluded the answers to the three sub-questions here. The main question will be presented in-depth and reflected on at the oral exam.

How do you most effectively protect against the security threats in online gaming?

Besides the obvious facts of having a good anti-virus program and protecting your own account information by not handing it out to strangers and untrusted sources, the best way to protect your gaming accounts is by making use of the Two Factor Authentication services that most companies provide now and by using their phone services. That way you will get easily notified if someone unauthorised is trying to access your account and can easily act against it. It also makes it a lot harder for a hacker to even gain access to your account in the first place, as they don't have easy access to the authenticator codes.

What value could the hackers be seeking in the player's account?

It seems that, if the hacker has gotten access to a game account, they mostly are aiming for the in-game items, such as the characters themselves and their equipment they own, rather than the credit card information, which is well hidden.

What measures do the companies take to protect their costumers?

They are adding more and more services to help protect the costumers' accounts, and letting the costumers know when their accounts are subjects to suspicious activity. The authenticators mentioned earlier, and the SMS protection services are becoming more and more widespread, all in all helping if the customers are willing to use them.

As for attacks on the company that also affect the customer, e.g. DDoS attacks, in the instance of Blizzard Entertainment, I cannot find much information about anything being done, as it is still easy to carry out and frequent.

Reflection

After nearing the end of the synopsis writing, I want to reflect on my learning experience and my methods used in the process.

Learning experience

There was of course some pre-existing knowledge on this subject, but I still do feel like I've learned a lot. I got to dive deeper into some of the hacker's method in attaining account information and some quite recent and significant examples of these attacks that I had never heard of before.

A couple of things I thought I knew a lot about turned out to take up the most of my research time: DDoS attacks. Since we've gone through it during the teaching, I didn't expect to put much time into researching that, but ended up spending several days investigating specific examples of DDoS attacks and how companies protected against them.

Methods and planning

Researching went well and there seems to be an abundance of material of this subject on the internet. Since they were all articles from websites, it did however take a lot of time going through the sources and deeming if they were trustworthy or not. I made sure that I stuck with recent, as recent as possible, articles and that the sources and authors were at least somewhat experienced in the field of gaming.

The questionnaire was meant to give me some information on how peers in my network got hacked and what they lost. It turned out to be a challenging task to set up, but I did manage to get some results, although it wasn't as useful information as I could've hoped for. If I ever do decide to use a questionnaire for data again, I will put even more thought into the questions asked and make sure to get even more data, because it was a bit on the low side.

The practical work I set out to do, turned out to be a failure. Creating a 2FA myself, was a bit too much of a task for me, for the time I set aside for it. I tried following tutorials that I just couldn't get to work, so I was running out of time and decided to switch method and research how it works instead, so I would at least have some information to use on this very important subject.

As mentioned I feel like I could've been a little more realistic with my planning and spend way less time on the questionnaire, and more time on the 2FA. I also ended up doing my writing along-side of the researching, as this was what I preferred, so there is an entire week that was a mix of everything. I will keep this in mind.

Overall, I feel like it has been a very successful process and I feel like I've gotten my answers to the questions I asked. Although there were hiccups, I still managed to reach most of my goals.

Literature

Matías Porolli, *Top 5 threats for online gamers and how to avoid them*, Aug 31, 2016, https://www.welivesecurity.com/2016/08/31/top-5-threats-online-gamers-avoid/

Alyssa Sellors, *Top 3 Security Threats to Online Gamers, and How to Avoid Them*, Mar 21, 2017, http://www.techsling.com/2017/03/top-3-security-threats-online-gamers-avoid/

Linda McGlasson, *How to Beat Keyloggers*, Oct 11, 2010, http://www.bankinfosecurity.com/how-to-beat-keyloggers-a-2999

Serge Malenkovich, *Top 5 Threats for an Online Gamer*, Apr 14, 2014, https://blog.kaspersky.com/online-gamer-threats/4474/

Kim Zetter, *The Biggest Security Threats We'll Face in 2016*, Jan 1, 2016, https://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/

Shane Richmond, *Millions of internet users hit by massive Sony playstation data theft*, Apr 26, 2011,

http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html

Igal Zeifman & Nabeel Hasan Saeed, *It's Not a Game: The Ever-Growing Risk of DDoS Attacks to Online Games*, Jul 1, 2015, https://www.incapsula.com/blog/ddos-attacks-on-online-gaming-servers.html

Charalampos Patrikakis, Michalis Masikos, & Olga Zouraraki, *Distributed Denial of Service Attacks - The Internet Protocol Journal - Volume 7, Number 4, Dec, 2004*, http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

Gergana Ivanova, *Blizzard Entertainment Suffered new DDoS Attacks*, Sep, 2016, https://bestsecuritysearch.com/blizzard-poodlecorp-new-ddos-attacks/

Aurangzeb A. Durrani, *How Blizzard should prepare for next wave of DDoS attacks*, Aug 31, 2016, https://venturebeat.com/2016/08/31/how-blizzard-should-prepare-for-next-wave-of-ddos-attacks/

Joseph C, *What is fake traffic? How can I identify it?*, Sep 30, 2016, https://support.flippa.com/hc/en-us/articles/202891420-What-is-fake-traffic-How-can-I-identify-it-

Rens van Summeren, *Security in online gaming – Bachelor Thesis Information Science*, Jan 26, 2011, http://www.cs.ru.nl/bachelorscripties/2011/Rens_van_Summeren___0413372___Security_in_Online_Gaming.pdf

Blizzard Support, *Battle.Net Authenticator*, last updated Dec, 2016, https://us.battle.net/support/en/article/100588

How Google Authenticator Works, Sep 14, 2014, https://garbagecollected.org/2014/09/14/how-google-authenticator-works/