**Cyber Security in Video Games**

**a paper submitted by Malcolm Akinje**

**in fulfillment of Comp116 (Cyber Security)**

**Abstract**

In any engineering discipline, to graduate, you must take a course along the lines of public safety or the safety of yourself. Civil Engineers can’t graduate and make bridges for the public to use without taking a public safety course. However, in Computer Science, cyber security is currently one of the least taken topics. Computer Scientist are allowed to handle and manipulate tons of data when it is not even guaranteed that they know how to keep the data hidden if one needs to. Couple that with the video game industry and the world may have a problem on their hands. Today, video games are multimillion-dollar projects with dialogues that can break one thousand pages of text. Characters are more lifelike, reactions are more substantial, and story lines are more complex. The Biggest factor however is that the world is now connected. Online gaming takes this large world that we inhabit and makes it that much smaller. However, these advancements lead to an issue - Security. In single player games, security issues only cheat the player themselves. Security issues in online games cheat everyone. They are unfair to all those involved and violates the “I” in the CIA triad, integrity. This paper will explore security in video games where currently people will use malware to steal others’ accounts, millions of dollars of in game currency is being stolen, and users’ information isn’t safe, all in an industry where these problems are being ignored.

1. **Introduction**

The video game industry can be considered a staple within the United States. According to a study done by the Entertainment Software Association, sixty-five percent of households in America contain at least one person who plays video games regularly. Sixty-seven percent of American households own a device to play video games on. And fifty-three percent of the most frequent gamers will play those games with others, whether those be online multiplayer, or local co-op.[[1]](#footnote-1) According to Michael D. Gallgher, the president and CEO of ESA, “America is a nation of gamers.” It can thus be said with certainty that video games are here to stay in the United States. Although this study shows facts about the use of video games and their prevalence in households, security in the video game industry is overlooked, yet still important.

Confidentiality, Integrity, and Availability are what developers promise end users. According to welivesecurity by ESET, an IT security company, “safety must be considered from the outset to the release.”[[2]](#footnote-2) By that, they mean security must be considered from the first moment data is collected from the user in any form. This includes, but isn’t limited to, email accounts, Facebook credentials, and, credit card information. When developers create an application that uses secure information, the user entrusts the developer to keep their information private. In an interview of Andres Rossi, the CEO of Sismogames, Andres said, “Over the years, [he has] seen all sorts of incidents, from payment-card frauds, to cyber-attacks targeting gamers and the subsequent claim of prizes, to exploitation of servers just for the sake of playing,”, referencing the Sony hacks that happened in 2016.[[3]](#footnote-3) These are blatant incidents that break the C, I, and A in the CIA triad. If they can’t uphold their end of this CIA contract, the video game industry is headed for failure.

1. **To the Community**

The game industry is one of the largest industries in the world today, and based on projections, will only grow from here. in 2017 , the Global Game Market reached over $100Billion and is projected to exceed $180Billion in 2021. The game industry has already surpassed the global box office revenue of 38.3Billion dollars.[[4]](#footnote-4). Because the gaming industry relies on creating immersive experiences, they must create a relationship between the developers and the player, with the game as the medium that unifies both parties. With over 50% of frequent gamers playing online, if this relationship is damaged by a lack of security, online gaming will come to a halt and the industry will only be a fraction of what its full capabilities are. If confidentiality is broken, it is difficult for players to trust an MMORPG(Massive Multiplayer Online Role playing game) to charge their credit card every month for a subscription fee. If integrity is broken and user data is being sold to a third party fewer people would log on to social party games. If availability is broken, people will just flock to a game that is up and running, leaving the former games world like a wasteland, deserted and without people.

1. **Who Causes the Security Issues?**

Security in the video game industry isn’t a black and white issue. While the largest issues are normally found at the hands of the developer, the gamer isn’t completely without blame. There is a positive feedback loop between developers and gamers that lead to security issues at times. Gamers dislike security software, Social Engineering leads to compromised accounts, and the desire to fit in leads to easier social engineering. Developers, for their part, feed off gamers wanting better experiences and not wanting, “bloat ware”. More immersive experiences lead to more development time, increased budget size, and consequently lower attention to security.

3**.1 Gamers**

In 2016 ESET did research on the habits of gamers. 83% of people who play games spend, on average, two hours a day on their most played game. In a 7-day week that is 14 hours spent online just on games. This does not include time spent on social media, day to day browsing, and procrastination. With all this time spent online, users could be exposed to many malicious attacks. Although exposing themselves to attacks at a minimum of 14hours a week, only 48% of gamers said they use security software on their gaming computers.[[5]](#footnote-5) 20% said they don’t need to, 13% said they were irritated by popups, 12% said they find security software slows down their computer, and 8% said because it interrupts their gaming experience. Therefore, gamers are not proactive enough in their own security. While expecting developers to adhere to the CIA, they contribute to the security issues on their own systems.

Anti-Virus software is the first line of defense a computer has against malicious intent. By disabling this software, computers become vulnerable to attacks that are easily avoidable. Anti-Virus software prevents malware from performing malicious activity. This can include stealing login credentials, botting and gold/item farming.[[6]](#footnote-6) At the early stages of infection all of this can happen without the gamer being aware. This can lead to banned accounts. If you can prove a compromised account, you may be unbanned. However, with no proof, it may be impossible to retrieve an account.

Another area where gamers cause security issues is normally by being vulnerable to social engineering. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. For attackers targeting gamers, social engineering is used to get the player to unknowingly install software that can steal passwords or install ransomware. Normally, after playing a game with someone, the player may get a message from the attacker asking them to join their team, guild, party etc. They send the player a link telling them that they need to install that software in order to have some form of communication with them. The link will probably be similar to another voice or communication platform like Mumble, TeamSpeak, or Discord. However, once clicked and installed the keylogger has infected the player’s computer and whatever they type can get re-directed to the attacker for them to analyze the player’s typing and finding passwords and other credentials.[[7]](#footnote-7)

A common threat for online gamers is the Win32/PSW.OnLineGames keylogger. Besides its ability to steal credentials and log keys, this piece of malware will search through the filesystem for data on well-known games such as World of Warcraft, Diablo, or League of Legends. A variant of this malware is Win32/PSW.OnLineGames.OUM. This piece of malware receives and executes commands that are sent from a remote server and tries to disable antivirus software. However, as said before, only 47% of gamers keep their antivirus software enabled. Gamers must realize that they play a role in making security an issue in the video game industry. Gamers seem to believe security should be taking a back seat to the experience. However, if gamers prioritize experience over security, so will developers.

**3.2 Developers**

Developers are driven by players. Developers must create something players desire in order to get sales. Lack of sales lead to downsizing or doubling down on the next project. Continuous downsizing, or a failure to ‘double down,’ eventually leads to a company’s termination. Developers are always analyzing what the player wants and how to deliver that experience to them. The video game industry can never stay stagnant because players are continuously demanding more from hardware and software. With a larger demand elsewhere, attention to security wanes. While there is an increase amount being spent on the development on a game, developers have not increased security measures at an equal rate.

Grand Theft Auto IV, developed by Rockstar North, was a critically acclaimed game when it was released in 2008. It was awarded multiple 10/10’s for its story and immersion. Rockstar North’s budget for this game was $100million and was developed in four years.[[8]](#footnote-8) Although described as the most expensive video game ever made, Grand Theft Auto 4 pales in comparison to the budget for Grand Theft Auto 5, its successor. Rockstar North’s Grand Theft Auto 5 was released in 2013 and the development budget was $266million.[[9]](#footnote-9) That is a 266% increase in budget over a 5-year span. With the increase in budget and a greater wait for gamers, the developers wanted to do more. With their new budget, Rockstar North pumped most of the money into developing a game that exceeded all expectations.

The increase in spending on development did not come without a cost. With more time spent in development and making the game, security took a back seat. Even today, new exploits are found. In 2017, an exploit allowed players to steal millions from other players.[[10]](#footnote-10) While this may not violate the C or the A in the CIA triad, the I was violated. The integrity of the game was hurt because players spend hours of their lives to gain this virtual currency. For a player to be able to steal currency and make other players hours pointless hurts the community and even caused many players to logout until the exploit was fixed. The following sections will explore more in depth the consequences that have happened when developers don’t spend the appropriate amount of time and money on security.

1. **What Security Issues Lead To**

In 2016, the video game industry was targeted. It was described as “the year the video game industry realized it’s cyber security problem”.[[11]](#footnote-11) Due to a lack of care and time spent, the industry was victimized and abused throughout that year.

**4.1 DDOS of Sony, Microsoft, Pokemon GO**

A Distributed Denial of Service (DDOS), is a type of Denial of Service attack where multiple infected systems, are used to target another system in an attempt at taking up all the target computers resources. Once the resources are depleted, the computer, or sever, becomes unresponsive. This breaks the A, availability, in the CIA triad.

In 2016, video game companies were the greatest targets of DDOS attacks.[[12]](#footnote-12) Sony’s PlayStation, Microsoft’s Xbox Live, Digital Extremes’ Warframe, Niantic’s Pokemon GO, and the Mirai botnet against Dyn are just a few of the recipients of one of the many DDOS attack that occurred by the end of August 2016. [[13]](#footnote-13) Upon a successful DDOS, a games server must be taken down. This can cause outages to the game for several hours. During this time, a company is losing money. According to threatpost.com, a DDOS can cause a company to lose twenty thousand dollars per hour of downtime.[[14]](#footnote-14) This figure can immediately skyrocket if any personal information is leaked and/or if virtual currency is stolen during the attack. For many of the games listed, this was not the issue. Many of the games were DDOSed as a wakeup call. The goal of the DDOS attacks on Microsoft’s Xbox Live, Niantic’s Pokémon GO, and Minecraft were to demand better cyber security. The grey hats, as they referred to themselves, were disgusted with how our information as end users were being stored. By not protecting themselves against DDOS’s, gaming companies were both failing CIA triad and through that, failing the consumer.

* + 1. **EA Currency**

Another issue that occurred up when security was not correctly handled was when the FBI had to intervene with an issue at EA. In 2016, hackers were found guilty of mining $16million worth of in-game currency from EA’s title FIFA.[[15]](#footnote-15) FIFA Coins are the in-game currency used in FIFA to get players for your online squads. You can play matches to get FIFA coins, or you can spend real money to buy them in game. This leads to third-party marketplaces, a sort of black market, for FIFA coins in Europe and China. Anthony Clark, one of the hackers, made $15 to $18 million dollars after mining the FIFA coins and selling them to the black-market dealers. According to an unsealed FBI indictment, Anthony Clark and the other hackers built a tool that would send false request to EA’s servers to spoof matches. [[16]](#footnote-16) By sending these request, they were able to mimic the result of thousands of matches in a short period, garnering them the large amount of FIFA coins.

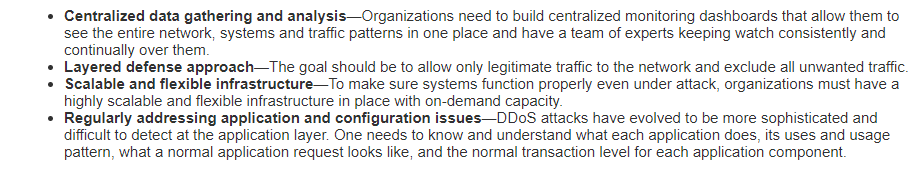
Although no confidential information was lost, EA took a large hit during this hack. Because their in-game currency is a part of their business model, EA took a large financial loss. EA was expected to only give out that many coins to one account after an either exorbitant amount of money was paid, or amount of time was put into the game. This violates the I in the CIA triad because now, $15million dollars’ worth of FIFA coins that were unearned are now in the market being sold at a lower price than others paid for.

1. **Solutions and a Call to Action**

Security is a must. From a company’s standpoint, it is not worth both the financial risk and the loyalty of their fanbase to make security not an issue. From a gamer’s standpoint if your computer is compromised, you can’t play the games you want anyway. This call to action is meant as a way to increase security for everyone involved across the video game industry.

* 1. **Developers! You Made a Promise**

Developers, you made an oath to the consumer to uphold the CIA triad. Always keep in mind Confidentiality, Integrity, and Availability. Confidentiality – keep your users’ information safe. That means spend the time to make sure that no leaks can happen, make sure common threats are fixed. Run server scans. Hire people to hack your servers and pay them when they do find an exploit. Bug Bounty programs are a great way to reward those who are looking out for your benefit. Integrity – keep your games values safe. EA should not have had $18million dollars’ worth of FIFA Coins stolen. It undermines every person who has put their own hours, or even their own money, into the game. Why should they pay or play for something that someone else can get for free or a reduced price? Availability – DDOS’s can be prevented. External solutions can entail paying your ISP to stop attacks before they happen. DNS redirection can redirect inbound internet traffic to a cleanser that can detect attack and filter traffic to data centers. If you don’t want to pay for the problem to be fixed externally, internal solutions are also available. 24/7 monitoring is needed and the ISACA, Information Systems Audit and Control Association, recommends:

[[17]](#footnote-17)

* 1. **Gamers! Help the Developers Out**

Gamers, It isn’t just the developers job to make security an issue. It is disheartening that only 47% of us have antivirus enabled on our gaming devices. If you want developers to make security a bigger issue on their list, we need to make it a bigger issue on ours. They focus on what we want. If most of their users don’t value security, or at least look like they don’t value security, in their mind, security won’t be as large an issue. Firewalls and antivirus software are needed. It makes developers jobs easier and will allow us to have a first line of defense at tracking malware instead of putting the entire burden on the developers. IGN, one of the largest video game news and review sources, normally publishes an article each year on best antivirus.[[18]](#footnote-18) The fix for social engineering is to pay attention to what you download, where you go, and what you are clicking. Stay away from weird links. If you must check, run the link through VirusTotal. If a deal looks to good to be true, it probably is. In end, for gamers, before doing anything that could compromise your computer in any fashion, take a step back and ask is what your doing seem normal and does this seem right. If you are uncomfortable with something don’t do it.

1. **Conclusion**

The video game market is rapidly growing. We are growing at a pace that most didn’t expect and because of that, we are targeted. Attackers see opportunity, not a completely new industry, but a new audience: online gamers. Sending information is easy to do, but protecting that information is what allows us to continue sending more. Online games have made the world that much smaller. At a mere click of a button, gamers from all places are connected, and cyber security within video games allow that connection to be maintained. However, violations in security lead to the opposite of what online games are supposed to do. Companies we run can lose thousands of dollars per hour, and the trust between developers and gamers are broken. Cyber security in video games isn’t just a developer problem. From the developer to the end user, it is everyone’s job to maintain this connection and allow the world to be that much of a smaller place.

Works Cited

Buckley, Sean. “'FIFA' Hackers Guilty of 'Mining' $16 Million from EA.” *Engadget*, 17 Nov. 2016, www.engadget.com/2016/11/17/fifa-hackers-guilty-of-mining-16-million-from-ea/.

Burger, Andrew. “DDoS Attack Data: Gaming Companies Were the Biggest Target.” *Telecompetitor*, 9 June 2016, www.telecompetitor.com/akamai-gaming-companies-targeted-half-ddos-attacks/.

Cloudbric. “A Year in Review: The Top Ten Cyber Attacks of 2016 in the Gaming Industry.” *Cloudbric*, Cloudbric, 23 Mar. 2018, www.cloudbric.com/blog/2016/12/a-year-in-review-the-top-ten-cyber-attacks-of-2016-in-the-gaming-industry/.

Das, Samburaj. “DDoS Attacks Can Cost Businesses Up to $2.5M Per Attack, Report Says.” *Threatpost | The First Stop for Security News*, 2 May 2017, threatpost.com/ddos-attacks-can-cost-businesses-up-to-2-5m-per-attack-report-says/125357/.

Entertainment Software Association. “Two-Thirds of American Households Regularly Play Video Games.” *The Entertainment Software Association*, 19 Apr. 2017, www.theesa.com/article/two-thirds-american-households-regularly-play-video-games/.

Gibson, Ellie. “GTA IV Is Most Expensive Game Ever.” *Eurogamer.net*, Eurogamer.net, 25 Feb. 2010, www.eurogamer.net/articles/gta-iv-is-most-expensive-game-ever-made.

Kumar, Ajay. “DDoS Attacks—A Cyberthreat and Possible Solutions.” *ISACA Journal*, vol. 4, 2013, www.isaca.org/Journal/archives/2013/Volume-4/Documents/13v4-DDoS-Attacks.pdf.

Newzoo. “Newzoo's Key Numbers | Games, Esports, Mobile.” *Newzoo*, 20 Apr. 2018, newzoo.com/key-numbers/.

Norem, Josh. “The Best Antivirus.” *IGN*, IGN, 23 Apr. 2018, www.ign.com/articles/the-best-antivirus-2.

Porolli, Matias. “Top 5 Threats for Online Gamers and How to Avoid Them.” *WeLiveSecurity*, ESET, 31 Aug. 2016, www.welivesecurity.com/2016/08/31/top-5-threats-online-gamers-avoid/.

Sassone, Santiago. “Why Security Is a Transversal Issue for Video Games Development.” *WeLiveSecurity*, ESET, 12 July 2017, www.welivesecurity.com/2016/08/16/security-transversal-issue-video-games-development/.

Schreier, Jason. “FBI Says Alleged Hackers Used FIFA To Steal Millions From EA.” *Kotaku*, Kotaku.com, 14 Nov. 2016, kotaku.com/man-goes-on-trial-for-allegedly-stealing-millions-from-1788948231.

Serrels, Mark. “Grand Theft Auto V Is The Most Expensive Video Game Ever Made.” *Kotaku Australia*, Kotaku Australia, 9 Sept. 2013, www.kotaku.com.au/2013/09/grand-theft-auto-v-is-the-most-expensive-video-game-ever-made/.

welivesecurity, Editor 13. “Security Takes a Backseat for Uninterrupted, Video Game Marathons.” *WeLiveSecurity*, ESET, 13 Sept. 2016, www.welivesecurity.com/2016/09/13/security-takes-backseat-uninterrupted-video-game-marathons/.

Zwiezen, Zack. “New GTA Online Exploit Lets Hackers Steal Millions From Other Players.” *Kotaku*, Kotaku.com, 11 Apr. 2017, kotaku.com/new-gta-online-exploit-lets-hackers-steal-millions-from-1794231142.

1. Entertainment Software Association. “Two-Thirds of American Households Regularly Play Video Games.”*The Entertainment Software Association*, 19 Apr. 2017, www.theesa.com/article/two-thirds-american-households-regularly-play-video-games/. [↑](#footnote-ref-1)
2. Sassone, Santiago. “Why Security Is a Transversal Issue for Video Games Development.” *WeLiveSecurity*, ESET, 12 July 2017, www.welivesecurity.com/2016/08/16/security-transversal-issue-video-games-development/. [↑](#footnote-ref-2)
3. Sassone, Santiago. “Why Security Is a Transversal Issue for Video Games Development.” *WeLiveSecurity*, ESET, 12 July 2017, www.welivesecurity.com/2016/08/16/security-transversal-issue-video-games-development/. [↑](#footnote-ref-3)
4. Newzoo. “Newzoo's Key Numbers | Games, Esports, Mobile.” *Newzoo*, 20 Apr. 2018, newzoo.com/key-numbers/. [↑](#footnote-ref-4)
5. welivesecurity, Editor 13. “Security Takes a Backseat for Uninterrupted, Video Game Marathons.”*WeLiveSecurity*, ESET, 13 Sept. 2016, www.welivesecurity.com/2016/09/13/security-takes-backseat-uninterrupted-video-game-marathons/. [↑](#footnote-ref-5)
6. welivesecurity, Editor 13. “Security Takes a Backseat for Uninterrupted, Video Game Marathons.”*WeLiveSecurity*, ESET, 13 Sept. 2016, www.welivesecurity.com/2016/09/13/security-takes-backseat-uninterrupted-video-game-marathons/. [↑](#footnote-ref-6)
7. Porolli, Matias. “Top 5 Threats for Online Gamers and How to Avoid Them.” *WeLiveSecurity*, ESET, 31 Aug. 2016, www.welivesecurity.com/2016/08/31/top-5-threats-online-gamers-avoid/. [↑](#footnote-ref-7)
8. Gibson, Ellie. “GTA IV Is Most Expensive Game Ever.” *Eurogamer.net*, Eurogamer.net, 25 Feb. 2010, www.eurogamer.net/articles/gta-iv-is-most-expensive-game-ever-made. [↑](#footnote-ref-8)
9. Serrels, Mark. “Grand Theft Auto V Is The Most Expensive Video Game Ever Made.” *Kotaku Australia*, Kotaku Australia, 9 Sept. 2013, www.kotaku.com.au/2013/09/grand-theft-auto-v-is-the-most-expensive-video-game-ever-made/. [↑](#footnote-ref-9)
10. Zwiezen, Zack. “New GTA Online Exploit Lets Hackers Steal Millions From Other Players.” *Kotaku*, Kotaku.com, 11 Apr. 2017, kotaku.com/new-gta-online-exploit-lets-hackers-steal- millions-from-1794231142. [↑](#footnote-ref-10)
11. Cook, Matthew. “2016: The Year the Video Game Industry (Finally) Realized Its Cybersecurity Problem – Panopticon Laboratories.” *Panopticon Laboratories*, 13 Dec. 2016, www.panopticonlabs.com/2016-the-year-the-video-game-industry-finally-realized-its-cybersecurity-problem/. [↑](#footnote-ref-11)
12. Burger, Andrew. “DDoS Attack Data: Gaming Companies Were the Biggest Target.” *Telecompetitor*, 9 June 2016, www.telecompetitor.com/akamai-gaming-companies-targeted-half-ddos-attacks/. [↑](#footnote-ref-12)
13. Cloudbric. “A Year in Review: The Top Ten Cyber Attacks of 2016 in the Gaming Industry.” *Cloudbric*, Cloudbric, 23 Mar. 2018, www.cloudbric.com/blog/2016/12/a-year-in-review-the-top-ten-cyber-attacks-of-2016-in-the-gaming-industry/. [↑](#footnote-ref-13)
14. Cloudbric. “A Year in Review: The Top Ten Cyber Attacks of 2016 in the Gaming Industry.” *Cloudbric*, Cloudbric, 23 Mar. 2018, www.cloudbric.com/blog/2016/12/a-year-in-review-the-top-ten-cyber-attacks-of-2016-in-the-gaming-industry/. [↑](#footnote-ref-14)
15. Buckley, Sean. “'FIFA' Hackers Guilty of 'Mining' $16 Million from EA.” *Engadget*, 17 Nov. 2016, www.engadget.com/2016/11/17/fifa-hackers-guilty-of-mining-16-million-from-ea/. [↑](#footnote-ref-15)
16. Schreier, Jason. “FBI Says Alleged Hackers Used FIFA To Steal Millions From EA.”*Kotaku*, Kotaku.com, 14 Nov. 2016, kotaku.com/man-goes-on-trial-for-allegedly-stealing-millions-from-1788948231. [↑](#footnote-ref-16)
17. Kumar, Ajay. “DDoS Attacks—A Cyberthreat and Possible Solutions.” *ISACA Journal*, vol. 4, 2013, www.isaca.org/Journal/archives/2013/Volume-4/Documents/13v4-DDoS-Attacks.pdf. [↑](#footnote-ref-17)
18. Norem, Josh. “The Best Antivirus.” *IGN*, IGN, 23 Apr. 2018, www.ign.com/articles/the-best-antivirus-2. [↑](#footnote-ref-18)