SEMINAR- IT Security

WS 2021

Bleeding-Edge Technology

Written by: Husnain Khan (ite104308)

Date: December 2, 2021

Supervisor: Prof. Dr. Gerd Beuster

Table of Contents

1. Introduction

The term “Bleeding edge” refers to technology that is released in the market for consumer use without undergoing extensive testing and therefore can be variable in results. In other words, bleeding edge technology can pose a certain amount of threat to consumer’s privacy and security as they are usually target of hacking and security breaches (Kenton, 2021). In contrast to bleeding edge, “cutting/ leading edge technology” refers to software that has been well-established in the market and is a step ahead of its competitors therefore is more reliable and poses less threat to consumer’s security (Kenton, 2021).

The question one may ask is why would companies want to release a product in such competitive market without thoroughly testing it first as it could clearly be flawed and lead to negative impact on consumers which may even lead to company losing clients or consumers? It is because this allows companies to test out the software by the consumers and gives them time to fix any glitches that arise in the original software. Along with being cost efficient, another benefit of bleeding edge technology is that it is open to feedback from consumers which companies can use as an asset to modify the technology in order to cater needs of the users to augment their experience of the product. Bleeding edge technology comes with its cost, but has potential to become leading edge once major flaws are taken care off (Kenton, 2021)

In this seminar, the goal is to highlight some of the ways by which security breaches occur in bleeding edge technology, what are some of the software that are more prone to hacking and how can they be made more secure in order to protect privacy of its users. It would be contrary to say that cutting edge technologies are at not risk of security breaches, because there are times when platforms like these are also exploited by hackers and become target of security breaches but certain apps are much more vulnerable and at scrutiny compared to big names. It is because many developers do not pay much attention to security of the product until it is hacked (Anderson, 2008).

The type of security breaches that occur depend on the application that has been hacked but usually involves one of the following. While some security breaches simply open up PCs to botnet recruitment, others can lead to much serious breaches where privacy of consumer could be at risk

such as healthcare data, credit card information and other personal data. Others include breaches from which money can be extracted directly and some to mediate power (Anderson, 2008).

Bleeding edge is generally composed of these 4 types of applications where hackers find innovative ways to attack and these include: online computer games, web applications such as auction sites like eBay, social networking sites such as Facebook, Instagram or other dating websites, cryptocurrencies, electronic elections (Anderson, 2008).

It is becoming more evident that as more people are joining the online web and games, it is creating complex socio-technical systems which lead to more attacks, exploitation such as click frauds and impression spams. (Anderson, 2008). One way to avoid becoming a victim of security breach while still using these applications is to use anonymity, in which user browses under a pseudonym. Anonymity is specifically useful in applications such as electronic elections where users can hide their identity to avoid being bribed or bullied. (Anderson, 2008). As this discussion moves forward, the goal is to emphasize other ways in which these web applications can be used while avoiding being a victim of security breach.

2. Online Computer Games

Online computer games are played by millions of people around the world and are even used to make living off it by many individuals for example by maintaining them to Chinese gold farmers. Some online games have a turnover larger than GDP of some small countries. In 2001, game sales hit $9.4 billion in USA surpassing movie-box office sales (Anderson, 2008). Security breaches in games can lead to huge loss to the companies therefore copy protection before game release is a significant concern and companies invest huge amount of money trying to overcome this issue. After release of the game, another concern developer of the game have is unfair advantage which can lead to biases in the game and over-time consumers loose interest dropping overall demand of the game. There are many types of cheating that can occur in online games that will be highlighted in the next section.

2.1. Common Cheating forms in Online Computer Games

This section will emphasize the common cheating forms that are seen in most online games. This section of the seminar is inspired by (Yan J, 2005).

A. **Cheating by exploiting mistrust:** involves modification or tampering with configuration data and game code
B. **Cheating by Collusion:** in this form of cheating people collude with each other to gain an advantage over other opponents in the game
C. **Cheating by abusing game procedure:** This form of cheating includes disconnecting from the server once an individual is about to lose
D. **Cheating related to virtual assets:** Some online games involve consumers to acquire assets which they can later trade for money. In such case of cheating, the cheater receives money but ends up not delivering the virtual asset.
E. **Cheating by exploiting machine intelligence:** Cheater can use Artificial Intelligence (AI) to make next moves in the game are obviously much more efficient and superior over a human.
F. **Cheating by modifying client Infrastructure:** Also known as "wall-hack", cheater can modify a wall making it transparent so hidden players can be visible to cheater by modifying device drivers and without changing game code or configuration.
G. **Cheating by denying service to peer players:** Cheater can purposely delay responses and trick peer players into believing something is wrong with the network.
H. **Timing Cheating:** In real time games, cheater can purposely delay move until they become aware of move of all the opponents.
I. **Cheating by Compromising Passwords:** By gaining access to password, cheater can access the data of other opponents in the game.
J. **Cheating by exploiting lack of secrecy:** Cheater can modify, delete or insert game events or commands that are sent over the network in plain-text format
K. **Cheating by Exploiting lack of authentication:** If a game does not have authentication, a cheater can log in from multiple IDs or even collect IDs of legitimate players.
L. **Cheating by Exploiting a bug or loop-hole:** Cheater can discover loop-hole or bug in the game and exploit that to win in the game over other opponents.

M. **Cheating by compromising game servers:** Involves changing game server if access gained to host systems.

N. **Cheating related to internal misuse:** This type of cheating is seen when game operators/ employees or administrators have insight of the game and use it to their advantage to cheat opponents.

O. **Cheating by Social Engineering:** Cheaters acquire IDs and passwords of opponents by making them believe something unusual has occurred with their account.

Table 1. (Yan J, 2005) summerizes common forms of cheating mechanism in online games.

Type	*Label*	*Cheating Form*
Of special relevance to online games	A	Cheating by Exploiting Misplaced Trust
	B	Cheating by Collusion
	C	Cheating by Abusing the Game Procedure
	D	Cheating Related to Virtual Assets
	E	Cheating by Exploiting Machine Intelligence
	F	Cheating by Modifying Client Infrastructure
	H	Timing Cheating
Generic	G	Cheating by Denying Service to Peer Players
	I	Cheating by Compromising Passwords
	J	Cheating by Exploiting Lack of Secrecy
	K	Cheating by Exploiting Lack of Authentication
	L	Cheating by Exploiting a Bug or Design Loophole
	M	Cheating by Compromising Game Servers
	N	Cheating Related to Internal Misuse
	O	Cheating by Social Engineering

Table 1. Common Cheating forms in Online Games

2.2. Bots in FPS and Virtual economical games

Another classic cheating mechanism in online games, specially games that are of First-Person Shooter (FPS) type, where a shooter required to aim on a target usually rely on bots. Aimbots are cheating mechanism where a cheater can enhance their aim compared to normal human or completely have a bot perform all of the target shooting. This is done by tampering with the code

and making up own version of the code which can provide automation and support (Anderson, 2008).

Bots can used in Virtual economical games as well. In these types of games, bots can be used to perform all of the tedious tasks that virtual economies require such as collecting coins and objects which gives significant advantage to the player as they move up in levels much more quickly than a normal player. This is a real problem because some of the virtual economies such as gold-farming are a real source of income in some parts of world such as in China and Romania (Anderson, 2008). These acquired gold-coins via bots can be used to trade in for real money on black market and auction at sites such as eBay.

There are many programs out there to detect aimbots to provide fair play to all the opponents but these aimbots are particularly difficult to detect as they resemble closely to an honest but very skillful shooter (Liu D, 2017). A few ways by which Aimbots can be detecting is by using authentication and encryption mechanisms to protect the original software, or use of guard software such as Punkbuster. Game-guard software such as Punkbuster detects any tampering that occurred in the game-code via anti-virus techniques (Anderson, 2008).

Another mechanism by which aimbots can be detected is via the use of "AimDetect", which relies on Performance-Skillfulness inconsistency in the player to detect cheating. Recall that cheaters using aimbots are usually significantly better and skillful at aiming but lack other very important game skills such as defending and situation awareness and resemble an average player in those domains. Aimbots also do not help these players to tackle an obstacle which is behind them and therefore a cheater cannot defend themselves when attacked from behind whereas an excellent player presumably performs better in that domain due to cautiousness (Liu D, 2017). Although AimDetect is good at detecting these bots in FPS games, there are ways to evade Aimbot Detectors as well. One of the mechanisms by which cheater can evade Aimbot detectors is via mimicking a normal user behaviour in which initially the cheater performs as an average player and gradually increases performance to mimic improvement and becoming more skillful via practice (Witschel T, 2020).

3. Web Applications

Web applications or websites are at a very high risk of security breaches as they are exclusively run online. Website consist of vast amount of different content ranging from Online search Browsers like Google, Yahoo or MSN to different auction sites like eBay and mail services that include Hotmail and Gmail (Anderson, 2008). Since these websites accept input from many different users, they are prone to many different security breaches such as SQL insertion attacks and Cross-site scripting (XSS). SQL injections and XSS remain a major threat to data-driven web applications. Both these forms of cyber-attacks have potential to steal, edit or destroy database of web applications (Abikoye, 2020).

SQL insertion attack is a type of cyber-attack in which SQL code is inserted into application code which leads to manipulation of the database exposing private information of users to the hacker. This type of security breach is seen in websites that contain personal information of users such as banking websites (Ahuja, 2016). Another mechanism by which security breaches occur in web applications is via cross-site scripting (XSS). This is especially common in websites such as Hotmail, Orkut, Myspace and even PayPal (Anderson, 2008). XSS is similar to SQL insertion in which script code is inserted into web application in form of JavaScript code and has potential to expose valuable data of users to the hacker (Mahmoud, 2017).

One mechanism to that website developers can apply to avoid being attacked by SQL insertion is by improving programing techniques via escaping single quotes, limiting character length input, filtering exception messages (Boyd, 2004) and via forming SQL injection string patterns. Another technique that is successful in detect SQL injections and XSS attacks is by using Knuth-Morris-Pratt (KMP) string matching algorithm that was implemented in PHP scripting language and Apache XAMPP server. It was found that by implemented these techniques, developers can not only prevent the attacks but also block the system using its mac address and generate a warning message once an attack is about to occur (Abikoye, 2020).

3.1. eBay

eBay is an auction site used world-wide to buy and sell different goods and is linked to PayPal, a payment service company. Security breaches at eBay can be very damaging as users link very private data such as their banking information, phone numbers and addresses to their eBay and PayPal accounts therefore security engineering needs to be at the top of the game when it comes to these sites. Despite the fact there are all sort of cyber frauds that happen on eBay.

Starting from the most old-fashioned cyber frauds where underbidders are offered similar items like the ones one sale and after making payment they never receive the item. Some fraudulent account even builds up reputation by first selling good products and building up their ratings and then eventually start to scam customers and do not deliver product after receiving the payment. Another common method of frauds on eBay occurs by hackers hijacking an account with good reviews and rating via phishing or password guessing and use those accounts to scam customers (Anderson, 2008).

This brings us to Phishing, which is a cyber-attack in which user is tricked into clicking on a link, e-mail or open a website which leads to installation of malicious malware in their machine, hijacking the machine and revealing sensitive information such as banking and other credentials to the hacker. Phishing attacks most commonly occur on payment websites like eBay and PayPal according to Figure 1, but can occur in various other type of websites as well (Chouhan, 2018).

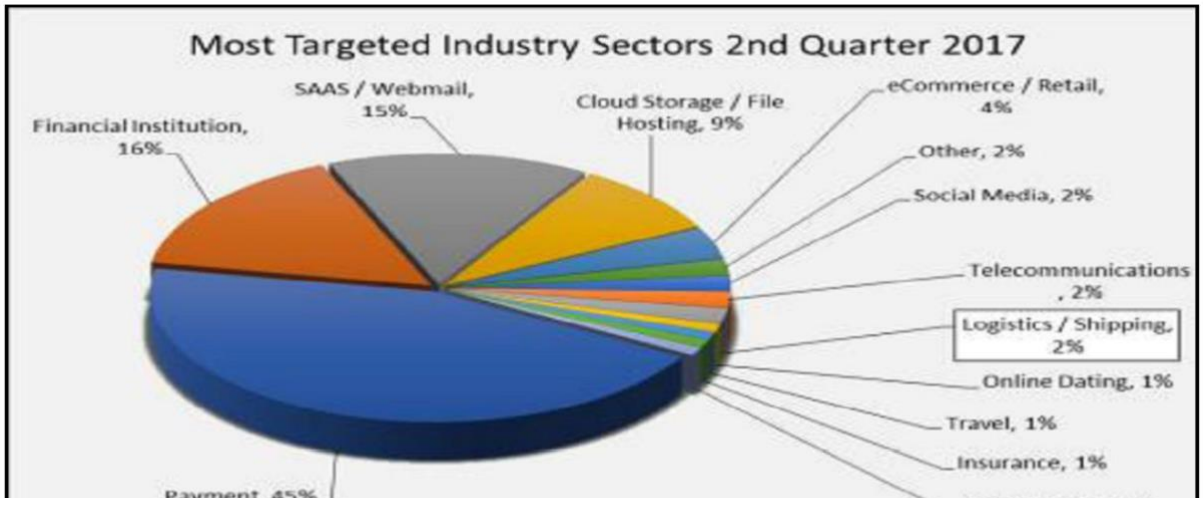

Figure 1. Industries most commonly targeted by Phishing

Another phishing scam in which hackers utilize a bug in “Forgot Password” process of eBay in which instead of sending new password information to user’s email, the attacker intercepts “reqinput” value to the change the password of the user to new value set by the hacker (Sidhu,

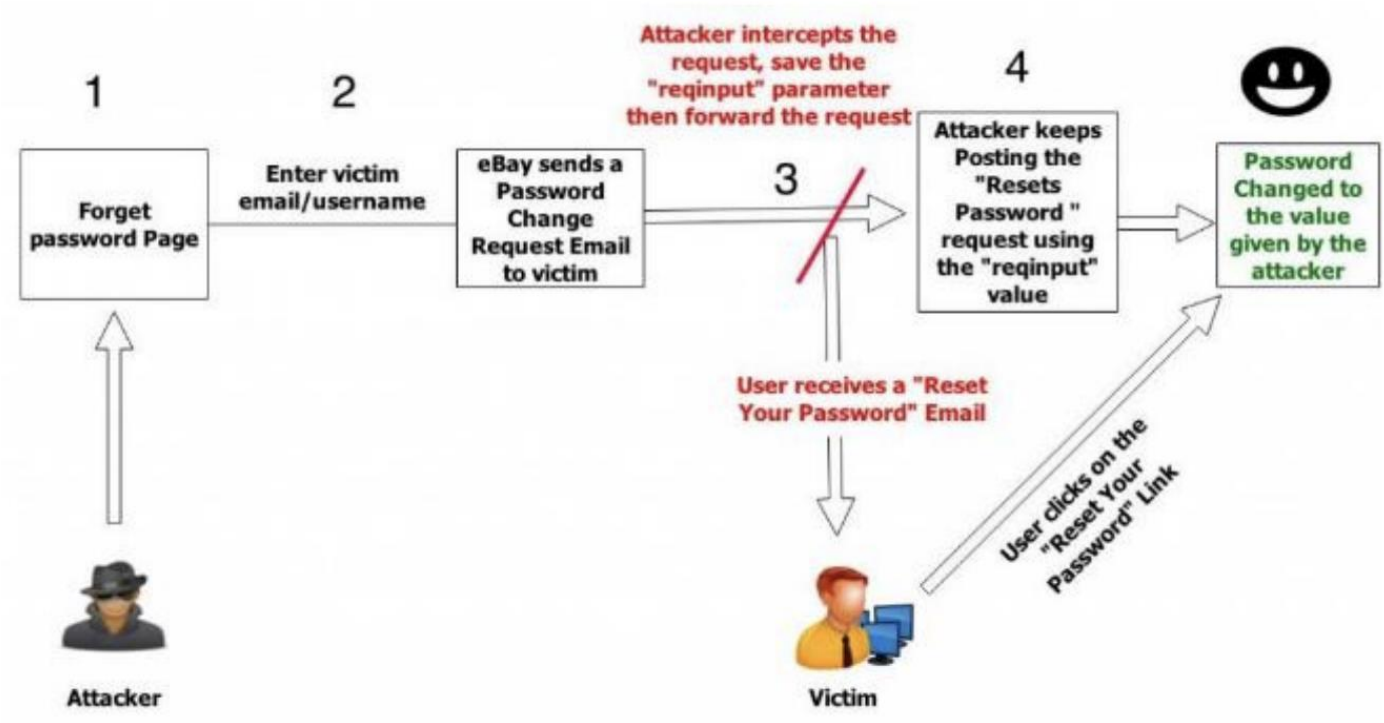

Figure 2. Phishing scam utilizing bug in "Forgot Password" in eBay

3.2. Social Networking Sites

Social networking sites include many different platforms such as Facebook, Instagram which link people to their family and friends and some sites are exclusively for means of communication of professionals such as LinkedIn. Social networking sites provide a mean to meet new people, make friends, find partners and meet other professionals

Social media users to add a lot of private information about their lives on these platforms and while it is means of connecting individuals to their friends and family and help individuals make new friends, it can also impact negatively when you private information gets leaked to people you do not want to share that information with. Starting from “Friends of friends” on Facebook, every

time someone tags you for example on Facebook, your page gets linked to their friends' accounts as well and now their friends are also able to see your post/ pictures. Some sites allow you to make friends based on mutual acquaintances (for example Facebook suggesting "People you may know") while other social networking sites allow you to meet people based on age, location, sex and sexual orientation such as Tinder (Anderson, 2008). Most of the users on social networking sites are of young age and they can be particularly target of privacy leaks specially teenagers as they less aware of what consequences can their posts have. Young people specially teenagers can end up revealing too much about their private lives on social sites, it can end up attracting sexual predators (Anderson, 2008). There has also been rise seen in cyber-bullying where the bully is anonymous and much more aggressive than bullies in person. It has led to increased suicide rates specially in teenagers therefore it is very important we monitor what kind of content our children are viewing online and who they interact with on social media as their security and safety is upmost concern for any parent. Concept of anonymous online chat rooms is even more hazardous as bullies can be a lot more aggressive and hostile on those compared to social networking sites because they do not fear the associated reputation risk (Anderson, 2008).

This brings us to how can we as an individual make social media and social networking sites safer for us as and protect our private data while still being able to share our life with family and friends? Talking about Facebook, there are changes one can make in their settings account and make the account more private to share it only with friends, and also refrain from posting content that might harm an individual in future when certain agencies like employment firm might see as inappropriate while checking social media accounts during hiring process. But the problem still arises when an individual is "tagged" in a photo or event from a common friend, the person has a choice to "opt in or opt out" of the tag but if for some reason person does not check their social media frequently or is not familiar with the access control options, and the tag remains it can be devastating in some cases. For example, "On New Year's Day 2008, following the assassination of Benazir Bhutto in Pakistan, the UK press published a photo of her son and political heir Bilawal Bhutto, dressed up in a devil's costume with red horns for a Halloween party, which was found on the Facebook site of one of his student friends" (Anderson, 2008). This type of situation can obviously create a lot of controversy and have negative impact on not only the person but also in this case on their political career.

Another problem that occurs is when individual's account gets hacked, or your confidential information from a friends account get leaked. Spamming is also a huge issue with social network accounts. According to a study at Indiana University where an experiment was performed by sending phish to students on university email vs social network accounts. While 16% students became a target of phishing when email was sent to university email vs 72% individuals when sent to social network accounts (Anderson, 2008).

Now let's look at some of the security measures developers of social networking site can take in order to protect user's data. Although these do not assure that breaches will not occur, but they definitely provide extra cover to maintain user's privacy. This section is inspired by (Shevchuk, 2019). A few of these security measures include:

1) **Two-factor authentication:** helps protect user's account by a second form of authentication for example a phone number (This is used in many applications including social networking sites as well as banking).
2) **Private account:** only friends can see posts and all of user's information is private
3) **Login notification:** sends user a notification via email usually when login occurs from unknown location or unknown device.
4) **Security check-up:** allows user to have a few trusted devices where verification is not required with each login.
5) **Trusted contacts:** This allows user to send a virtual key of social media account to 3 friends from the contact list.
6) **Identification code:** allows to process two-factor authentication
7) **Password strength checker:** this security measure is in place so individuals do not make passwords that can be easily hacked. The password is only accepted when it meets certain criteria.
8) **Password breaches checker:** This alerts user when password breaches or attempt of password breach has been placed (for example: multiple wrong tries on a password)
9) **Email breaches checker:** alerts user if email breach occurs.
10) **Periodic password changes:** sends users notification to change password after a certain amount of period has passed.

11) **External application/site access checkup:** limits third party access to social media accounts.

These security measures are utilized by different social media applications in order to protect user's data. The chart below provides a comparative analysis of which of these safety measures are used by Facebook, YouTube, and Instagram and are part of their default safety protocols (Shevchuk, 2019). While looking at the data in the chart below (Table 1.), one can conclude that Facebook provides its users with most security measures while Instagram accounts have least cover making them more vulnerable to security breaches.

TABLE I. COMPARATIVE ANALYSIS OF SOCIAL MEDIA SECURITY TOOLS

Security tools	**Social media**		
	Facebook	***YouTube***	***Instagram***
Two-factor authentication	+	+	+
Private account	+	+	+
Login notification	+	+	-
Security checkup	+	+	-
Trusted contacts	+	-	-
Identification code	+	+	+
Password strength checker	+	+	+
Password breaches checker	-	-	-
E-mail breaches checker	-	-	-
Periodic password changes	-	-	-
External application/site access checkup	+	+	-

4. Elections

Election process for any country and democratic parties can be very stressful. The primary goal of any elections be it small scale such as municipal elections or Federal/ Presidential elections, is to have fair results where democracy wins and people's voice is heard. But election campaigns and its results are in today's world is drastically manipulated ne only by media but also social media and are also target of security breaches frequently.

Election process is one of the process where anonymity is required to be maintained throughout to avoid vote-buying and intimidation. As the election process moves to electronic voting and the two major issues that arise include satisfaction of voters that their vote will be counted properly along with their anonymous status which depends combination of both excellent physical and computer-security mechanisms (Anderson, 2008). When it comes to electronic voting and political campaigns moving to social media, there are issues that arise from election security breaches to fake news propaganda that will be further investigated in this section of the seminar.

4.1. Computational Propaganda and Fake news media

Starting from simply social media, it has great influence on how a party or it's campaign can be perceived for example opponent parties or even other countries can use bots, fake social media accounts, memes to spread misinformation which can heavily affect the results of any election. This type of misleading information campaigns has been observed in many countries during election process such as Brazil, UK, France, USA, and Ukraine (Tenove, 2018).

It is observed that fake news is propagated on social media via use of algorithms, automation, sockpuppet accounts and bots. The type of bots used include Dampener bots, whose job is to supress messages and Amplifier bots that make messages appear much more popular than they really are on social media accounts. Bots are primarily used on twitter to rebroadcast content. On the other hand, sockpuppet accounts are human operated fake accounts that post fake messages for example a Russian-controlled account "United Muslims of America" whose motive was to

pressure US politicians and US forgein policy, along with accounts such as " pro-Trump" to amplify messages on social media were used in 2016 USA Federal Elections (Tenove, 2018)

4.2. Cyberattacks on Databases

Another mechanism of affecting political electoral campaigns that has specially gained a lot of popularity in recent times is hacking and leaking private emails, and conversations of political candidates and use it against them to influence public. This is usually done by hacker gaining access to digital devices, data servers and social media accounts. This was seen in case of Hilary Clinton election campaign in USA presendital elections of 2016 where emails were leaked during to influence her reputation. Another example includes data leak of emails and documents 2 days before election in 2017 French presidential elections campaign of Macron (Tenove, 2018).

4.3. Direct- Recording Electronic (DRE) Voting System

DRE is a voting system by which participants can voice their opinion and cast their vote electronically which might seem more functional than standing in long line-ups but this method can be very unreliable as it can potentially be at risk of major security breaches. Looking back in the history, John Hopkins investigated the DRE machines and software Diebold used in 2002 elections and found out that the security flaws were beyond expected, voters were able to caste unlimited votes, and employees working from the inside were able to identify voters sabotaging anonymity and the system can many bugs and loop-holes allowing it to be attacked by hackers (Anderson 2020). In 2007, similar study performed by Florida State University also concluded even more weaknesses in Diebold equipment which included data encryption issues, buffer overflows, SQL injections, and undocumented backdoors (Anderson, 2008). Given all these loopholes in electronic voting system, electronic abuse is prone to occur at election time and can be used by influential and authoritative individuals to stay in power.

Another E-voting system known as Helios 2.0 used in elections that was targeted for hacking led upgrade to Helios 3.0. Helios 2.0 was targeted for hacking by utilizing a bug in the software. Web browser and JavaScript plays important role for functionality of Helios. A malicious candidate

could trick voters into accepting hacked ballot and win election that was managed by Helios (Estehgari, 2010).

5. Cryptocurrency

Cryptocurrency industry has been developing fast in the recent years which include many such as Bitcoin, Ethereum, Dogecoin, Chain-link, Stellar and the list goes on. Cryptocurrencies are now available in market as many different forms of payment such as retail goods, international transactions, and even available through ATM (Limba, 2019). Cryptocurrency hacks and scams are a major concern and because after hacking these currencies can be sold on the black market for cash. It is somewhat easier to manipulate with cryptocurrencies because these exchanges are not recorded on blockchain so the insiders can manipulate the quotes and leave gaps or leak out. (Hong, 2019). Cryptocurrency are at major risk of scamming as well. An article published by BBC news on November 2, 2021 describes a scam of digital token inspired by popular south Korean Netflix series Squid Game, where buyers were scammed and lost $3.38 Million. While some economists suggest cryptocurrencies will be the currency of future, there is still a lot of work that needs to be done to protect user's data and establishing a safe platform where users are not targeted by scammers and fall for fraud.

6. Conclusion

In conclusion, bleeding edge technology is technology that is prone to cyber-security breaches and attacks because there could be loopholes and bugs in the software because developers haven't done through testing on these applications as they are fairly new. Some of the applications that consist of bleeding edge include Online Computer Games, Web applications such as eBay, social networking sites, electronic elections and cryptocurrencies. Attackers can hack private data of users through these accounts such as emails, chats, banking information and other private information and use it against them on many different platforms. Looking at online computer games, cheaters tamper with code of the game giving them unfair advantage at game which eventually drops over-all ratings of the game as people lose interest. Some games offer coins and other rewards that can be exchanged for real cash therefore cheating in these kinds of games cheating can be very dreadful. A few ways by which cheaters get an upper hand on games is via

use of Aimbots which enhance their aim compared to normal human in shooting games. Bots can also be used to perform other tasks that such as doing all the labor work in games consisting of virtual economies. There are ways to detect these bots in order to provide fair play to all the players such as Aimbot, guard software such as Punkbuster and via authentication and encryption mechanism. Web applications such as emails, dating websites, social networking sites including Facebook and Instagram can also be target of many security breaches which can lead to serious consequences as user's private chats and pictures can be leaked. Mechanism by which security breaches occur on these websites include SQL insertion attacks, and Cross-site scripting. Both SQL insertion attacks and XSS are type of attacks in which malicious code id inserting into the software's code exposing private information of the user. A few other mechanisms by which security breaches occur include Phishing in which cyber-attack occurs when user clicks on the link sent to email leads to download of malware in their machine which hijacks the PC of the person. Cyberattacks are not only confined to web applications and games but also can occur via elections compromising integrity of a fair election. A few ways by which computer technology can be used to compromise fair election is by propagating fake news about certain parties via using bugs in the social media apps via help of bots to amplify memes and messages. Another common method becoming popular is recent times in elections around the world is leakage of private information of candidates just before election to jeopardize their popularity. There are also flaws in the web applications that conduct electronic voting such as Diebold equipment noted to have many bugs included encryption issues, SQL injections and buffer overflows. These bugs in the software provide an opportunity for hackers to attack the electronic voting system and manipulate the results of the election. This brings us cryptocurrencies, which include Bitcoin and Ethereum, these are gaining a lot of popularity in recent times but there have been cases scams that occur and people fall for fraudulent currencies where scammers take all their money.

In end, Bleeding edge technology has setbacks because it is still under-development, but once the bugs are fixed, it has potential to compete with other major competitors that are now leading edge and can provide vast medium of opportunities to its users to enhance their overall digital experience.

7. References

1. Anderson, R. (2008). *Security engineering: a guide to building dependable distributed systems. (Chapter 23: Bleeding Edge).* John Wiley & Sons. (Page 3, 4, 7, 8, 11,14, 15)

2. Yan, J., & Randell, B. (2005, October). A systematic classification of cheating in online games. In *Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games* (pp. 1-9). (Page 5)

3. Liu, D., Gao, X., Zhang, M., Wang, H., & Stavrou, A. (2017, June). Detecting passive cheats in online games via performance-skillfulness inconsistency. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 615-626). IEEE. (Page 7)

4. Witschel, T., & Wressnegger, C. (2020, April). Aim low, shoot high: evading aimbot detectors by mimicking user behavior. In *Proceedings of the 13th European workshop on Systems Security* (pp. 19-24). (Page 7)

5. Ahuja, BK, Jana, A., Swarnkar, A., & Halder, R. (2016). On preventing SQL injection attacks. In *Advanced Computing and Systems for Security* (pp. 49-64). Springer, New Delhi. (Page 8)

6. Boyd, SW, & Keromytis, AD (2004, June). SQLrand: Preventing SQL injection attacks. In *International conference on applied cryptography and network security* (pp. 292-302). Springer, Berlin, Heidelberg. (Page 8)

7. Mahmoud, S. K., Alfonse, M., Roushdy, M. I., & Salem, A. B. M. (2017, December). A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques. In *2017 Eighth International Conference on Intelligent Computing and Information Systems (ICICIS)* (pp. 36-42). IEEE. (Page 8)

8. Abikoye, O. C., Abubakar, A., Dokoro, A. H., Akande, O. N., & Kayode, A. A. (2020). A novel technique to prevent SQL injection and cross-site scripting attacks using Knuth-Morris-Pratt string match algorithm. *EURASIP Journal on Information Security*, *2020*(1), 1-14. (Page 8)

9. Chouhan, R., Arora, S., Thakur, R., & Hyde, A. (2018). Anti-phishing measures against phishing attack in the state of art. (Page 8, 9)

10. Sidhu, J., Sakhuja, R., & Zhou, D. (2016). Attacks on eBay. (Page 10)

11. Shevchuk, R., & Pastukh, Y. (2019, June). Improve the security of social media accounts. In *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 439-442). IEEE. (Page 12, 13).

12. Tenove, C., Buffie, J., McKay, S., & Moscrop, D. (2018). Digital threats to democratic elections: how foreign actors use digital techniques to undermine democracy. (Page 13, 14)

13. Estehghari, S., & Desmedt, Y. (2010). Exploiting the Client Vulnerabilities in Internet E-voting Systems: Hacking Helios 2.0 as an Example. *EVT/WOTE*, *10*, 1-9.
14. Limba, T., Stankevičius, A., & Andrulevičius, A. (2019). Towards sustainable cryptocurrency: Risk mitigations from a perspective of national security. (Page 15, 16)

15. Hong, S. (2019). Survey on analysis and countermeasure for hacking attacks to cryptocurrency exchange. *Journal of the Korea Convergence Society*, *10*(10), 1-6. (Page 16)

16. "Squid Game Crypto Token Collapses in Apparent Scam." *BBC News*, BBC, 2 Nov. 2021, https://www.bbc.com/news/business-59129466. (Page 16)

17. *Kenton, W. (2021). Bleeding Edge Technology*. (n.d.). https://www.investopedia.com/terms/b/bleeding-edge-technology.asp (Page 2)