iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5220

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

Security in Gaming

Dwip Makwana

Abstract: ***Online games need security as they are more popular than story mode games especially multiplayer shooting games. Security in Gaming or Cyber Security in Gaming is a way of securing and avoiding piracy in gaming. It provides various methods through which we can secure game accounts of customers. It provides various and effective measures for both offline and online gaming platforms like consoles, PCs and mobiles. Cyber security in gaming is evolving at a pace far greater than other security domains. It also secures the in-game purchases and currencies used by the player and traded between two users. Gaming security is very important aspect to view as the advancement of gaming industries and technology is higher the tighter the security of the game accounts and server has to be.***

Keywords: Gaming, Gaming platforms, Game purchases, In- Piracy, MODS, DRM, Security, DOOM.

I. INTRODUCTION

Gaming Security or Cyber Security in gaming is a mechanism through which a game account is secured from being hacked or manipulated.

A. Whenever user logs in to play games the server first authorizes you if you input the correct credentials.
B. Then the server issues user an authorization code which is sent to your respective email or mobile number user provided when they had created the account.

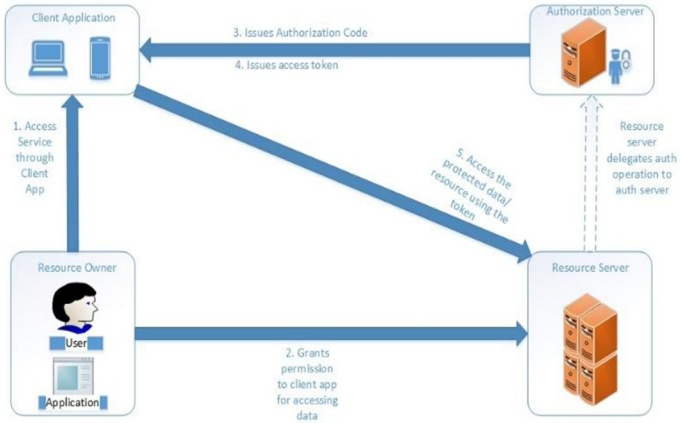


Fig. 1. Account Login Authorization

C. Then when they give the code to the server through client application then user gets access to the server and thus, they can play their respective purchased game. The figure [1] describes how the authorization takes place.
D. This is a type of Kerberos Authentication System used in gaming security framework.

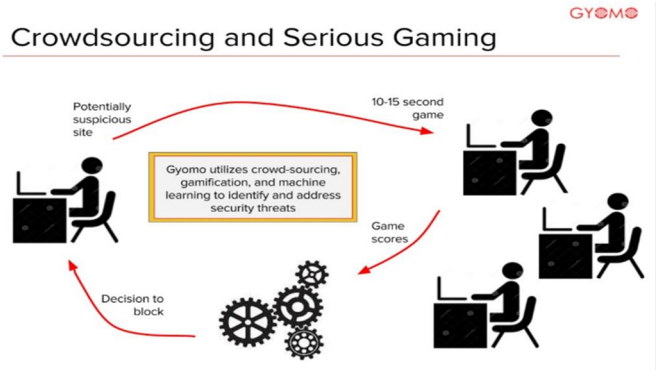


Fig. 2. Crowdsourcing

©IJRASET: All Rights are Reserved

Online gaming offers sessions of duration varying from 10-15 minutes. These sessions are known as "lobby". These sessions can overlap each other or may be created malicious users, resulting in higher than available bandwidth usage. Due to this intrusion by malicious users can lead to denial-of-service attack resulting in crashing of the server. Frequent crashing will lead to dis-satisfaction in the player's community and lead to loss of image of particular gaming company. The figure [2] shows the threat to the lobby or server created for multiplayer gaming online by crowding unnecessary data. This is result of negative crowdsourcing meaning crowding on a particular source for negative purposes which may lead to negative publication regarding continuous play. This decreases the number of downloads of the game or number of playtime and active users in game affecting the profit of the game.

II. IMPORTANCE OF SECURITY

Security is as important as testing or publishing. Cyber security plays an important role in securing the softwares and making the video-games secure. The security has four main pillars- non-repudiation, confidentiality, integrity and availability. These four pillars should be satisfied for an optimum security approach in any software. Each security model depends upon the type of software and its working mechanism. Maintaining security provides good user experience and increases the life of a particular software.

Second Life, a 2003 published multiplayer online roleplaying game is free to play. There are some features which differ from other online games like copy-right of their creation, earning money, sell and buy inventory items, virtual land, etc.

III. RELATED WORK

In the website [1] the author Frank Siemons suggested that the accounts of user in which a game is attached can get hacked by various methods losing identity and thus having financial loss as now a days a single game is also worth of many dollars. Many gaming companies like DICE and VALVE and even ROCKSTAR GAMES are enhancing the stability and security of their network and gaming systems by providing their own anti-cheat softwares in order to enhance the gaming user experience. Further adding he claimed that cheaters can damage the fun of an online multiplayer game and if the damage to a famous or renowned game is large enough and its upcoming sequels. Many anti-cheat softwares or techniques have been integrated in-game.

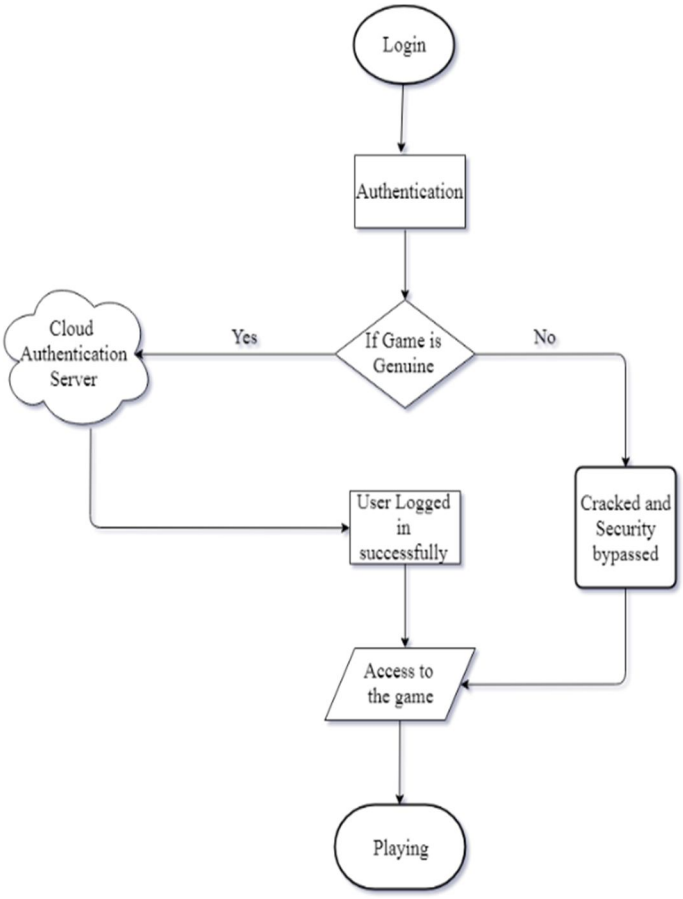


Fig. 3. Login steps for authentication in games

©IJRASET: All Rights are Reserved

In 2011, author Rens van Summeren giving a new dimension to account theft by describing that Brute force or Dictionary attacks and malicious software are another way to get access to accounts if the target authentication system does not adequately protect against this. He also talks about social engineering describing that hackers try to take game IDs by using phishing techniques. Players may assume that something is happened to account or the account needs to be more secured, making attackers successful to get game accounts [2]. He also mentioned about cheating that as long as game are existing, cheating will be done or attempted.

The view of the security company "OneSpan" for gaming security, believe that gamers should have optimal gaming experience and game must be UI friendly [3]. They suggest that selecting a solution that offers simplicity of design, tough integration and proper support to avoid the delays that are not affordable and poor experience for the player. Further adding Strong security across large gamer populations with expectations by users for a streamlined login experience is daunting at best. They brief on how to protect gamers' identities and prevent account takeover using two-factor authentication to ensure user identity's validation. Account hacking poses a real threat which may remove gaming applications' customer trust completely.

The company PWC stresses on 2 points mainly for security in gaming as follows;

A. Connecting the player, Understanding the risks and protecting data. In connecting player, they describe that the next generation of players are tech-savvy and able to merge in person and virtual activities more readily than ever before [5].

B. Protecting data, they proposed that by putting up a wall around confidential information is no longer a simple or completely secure solution—especially as the gaming industry collaborates more to align offerings with a player-centric model.

New theory was built against the paper by author Frank Siemons as mentioned above in understanding the risks by talking about the factors such as new innovations, pairing of existing and newer systems, and increasing collaboration across businesses only adds to the complexity of the risk landscape.

In 1997, when gaming was in incubation stage, authors Andrew Kirmse, Chris Kirmse believed that persistent world architecture in gaming laying information. These persistent worlds share the same basic architectural features. To play the game, a user either installs client software from a CD-ROM or downloads it from the Internet. They gave a new perspective about the client software which contains code that communicates with the game server using their own set of protocols designed for the client application activating the game [4]. Large static data, such as graphic files, sounds, music, and level layout are typically part of the initial installation onto the client they mentioned.

IV. SECURING THE GAMING ENVIRONMENT

The biggest threat and drawback in Gaming Security is the MODS created in any games which ruins the gaming experience to the legitimate users. Some games have their code open-source so the codes are available online. Some great programmers with bad intention take this code and manipulate and create MODS for games. Some MODS are available online free to download that becomes the reason of becoming viral and increasing the number of moded users and messing the gaming experience. The code should not be open-source and even the game files after installation can be encrypted or prevented from unauthorized access. In this way the creation of the MODS that defies the experience of real gaming will be prevented. Mainly the games are protected with DRM (Digital Rights Management) technology which has access control over softwares that has certain copyrights mainly in game industry. It most used technology by huge game handles like Steam and Origin which serves to anti-piracy. Initially the DRM was a blast as no crackers could crack it but as time went the crackers finally managed to bring down DRM. DRM also have some cons as it brings decreased performance and uncertainties in severs with it as installed. The DRM evaluates access by the user's purchased mode and then it gives access to games which requires total internet connection even in single player games. It doesn't allow outside environment or entity to access the purchase of any service. The main threat to online gaming is the cheats used in-game. The cheat scripts used by cheaters or hackers bypass the certain rules of games for e.g. if it is a first-person shooting game then the hackers' script that they can shoot through walls while it is not possible for normal users. In this way they lead the game giving problems to legit players. Many anti-cheat algorithms by big gaming industries have been implemented in their client application and in-game but they are not that much effective. Various players have different way to play the games. One uses stealth mode while other goes open fire. So here AI [Augmented Reality] can be used as they can learn how the player plays and uses the game features and tools. If the account gets hacked the hacker's way of play is different so the location can be banned by anti-cheat or the account itself can be banned. According to an article on CISOMAG [10] hacker's background mainly consists of young gamers which commit cybercrime. The research assured that cybercrime skills developed through video games was acquired by 82% of teens and young adults which became an unofficial employee of criminals.

©IJRASET: All Rights are Reserved

From last 2-3 years on every website, whenever the user sign-in into their account the company or websites suggest to setup two step verification for their security but human nature makes them to just skip this step. In this way hackers through SQL Dump and SQL Injection extract their passwords from the websites and sell them in the black market of game accounts. Services like Uplay and Origin that are provided by one of the biggest gaming industries "Ubisoft" and "Electronic Arts" are not able to recognize the login session between the legit customer and hacker. The hacker then changes the password of account and sells it and the original customer can't login and thus faces issues. The two-factor authentication should be made compulsory like other credentials while creating account so as to protect the account.

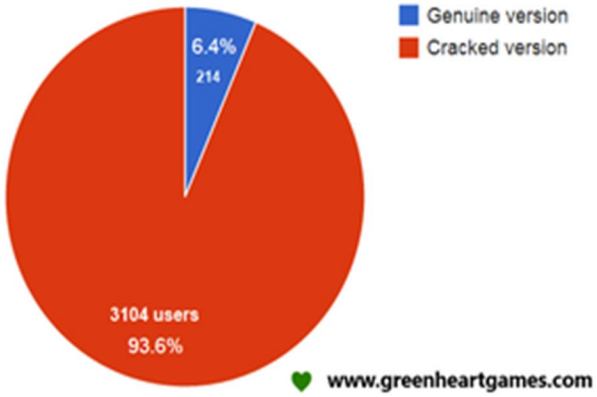


Fig. 4. Cracked version V/S Genuine version

Pirated or cracked games are also a major downfall in gaming industry. Though pirated games do not have full access to the game features, players download them as they contain the main story of the game. These games don't have internet access as game companies detect pirated games through internet. Players who don't have enough money to buy the games which costs around $50-$60 per game waits for pirated copy and uses it once the games are cracked. This promotes piracy in gaming and also an underground market of buying & selling of illegal accounts of games. These markets are often created on telegram as it is a powerful social app for anonymity of users. These accounts are sold by getting accounts from internet through software called "SQL Dumper" and are verified and filtered on a large scale by a method known as "Leeching". 93.6% of gamers worldwide uses cracked version of a particular game. One of the big reasons the game industry is in the eye is that the hackers or criminals makes profit easily by having a business of in-game items.

V. CASE STUDY: DOOM ETERNAL

The famous but rather erroneous AAA title DOOM that was developed by Bethesda Studios was crashed and mocked recently when their latest game DOOM ETERNAL accidently released a DRM-free version. The players which where depended on cracked games were able to get their hands-on before the company patched the games. The crackers were so fast enough that they managed to rig DRM-free version inside the folders of the game and cracked it. The cracked version was distributed before even game company could patch it and re-release it. Besides this rant, Bethesda Studios has generated a nice amount of revenue by DOOM ETERNAL as it has less microtransactions which makes it a neat and un-biased game against the wealthy gamers.

VI. CONCLUSION AND FUTURE WORK

Most of games are delayed for security purposes but are cracked after a month or two. Gaming companies can encrypt their file with their own encryption algorithms which are confidential. Investing time in encryption and creating new file extensions makes it difficult for integrity contamination. MODS supportive scripts can be avoided by maintaining source code security and delivering high secured compression to the game files.

The two-factor authentication should be made to compulsion as I mentioned above so as to eradicate the ease of access of unidentified hacker and criminals to the game accounts. While game companies can also increase their backend security by encryption or making online access compulsory to play as now-a-days internet is available globally even in remote areas.

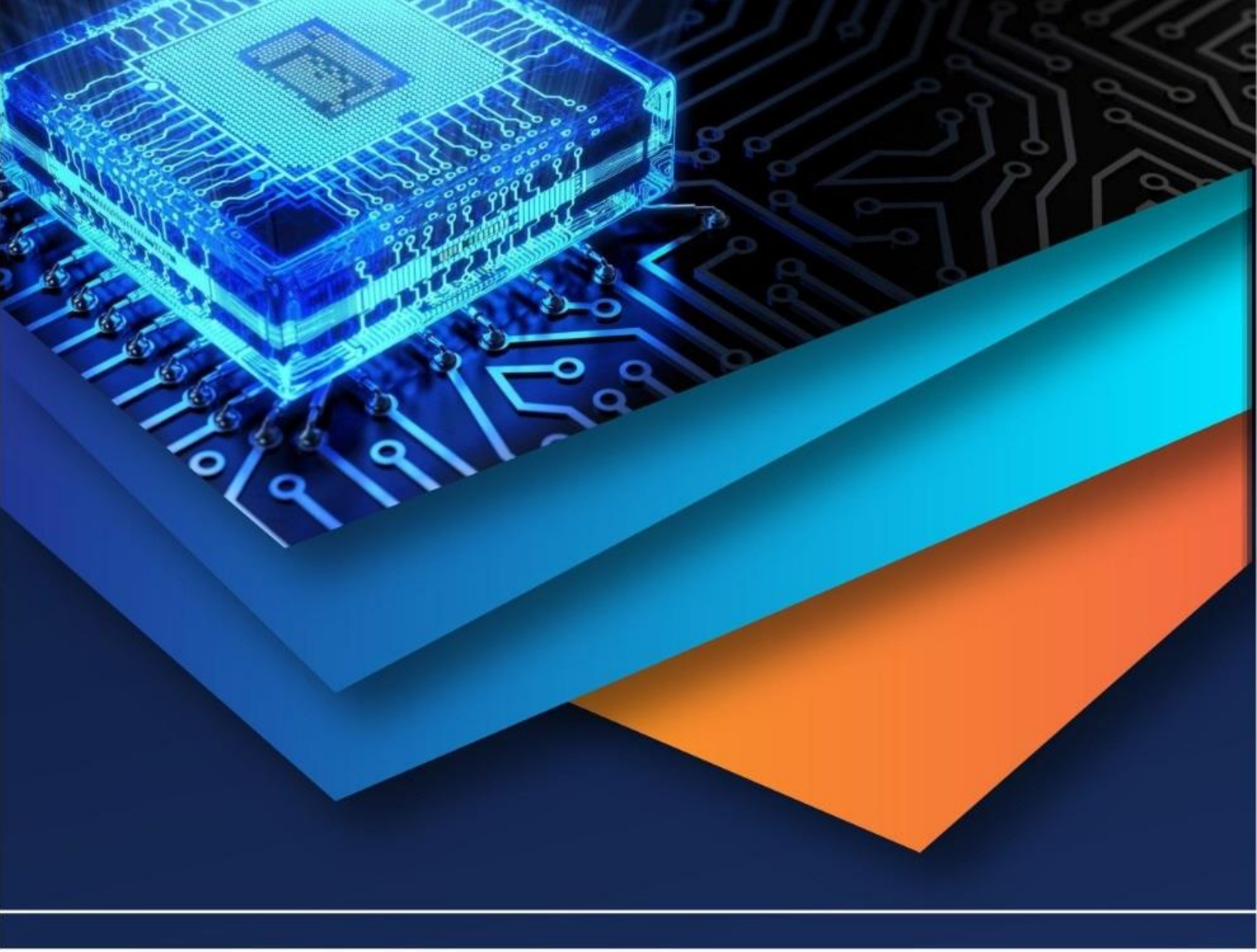
Lastly, the prices of the games can be narrowed a little bit for an efficient sales market. Players will not be motivated for playing pirated games and will be able to have full features of the game. Dropping prices especially in PC games can affect the piracy at a vast rate. The DLCs [downloadable content/extended storyline] can be given as free content to the users who buy the genuine game rather than pirated game accounts from the black market.

©IJRASET: All Rights are Reserved

REFERENCES

[1] Frank Siemons, "Security Considerations in Games Platforms". https://resources.infosecinstitute.com/security-considerations-in-games-platforms/#
[2] Rens van Summeren, "Security in online gaming". https://www.cs.ru.nl/bachelors-theses/2011/Rens_van_Summeren___0413372___Security_in_Online_Gaming.pdf
[3] Vasco AKA One Span, "Gaming anti-hack solutions". https://www.vasco.com/solutions/gaming-anti-hack-solutions
[4] Andrew Kirmse, Chris Kirmse, "Security in Online Games". https://www.gamasutra.com/view/feature/131620/security_in_online_games.php
[5] PwC Canada's gaming Practice, "Cyber Security in gaming". https://www.pwc.es/es/publicaciones/entretenimiento-y-medios/assets/ciberseguridad-juego-online.pdf
[6] Figure 1.0," Sadruddin Md". https://iteritory.com/oauth-tutorial-understand-oauth2-0-in-simple-step-by-step-lesson/
[7] Figure 1.1," *Wefunder Inc*." https://wefunder.com/gyomo/
[8] Figure 1.3, Jared Newman," *Game Dev Tycoon battles digital piracy with digital piracy*." https://www.pcworld.com/article/2036606/game-dev-tycoon-battles-digital-piracy-with-digital-piracy.html
[9] "Anja Beyer", Security in Online Games - Case Study: Second Life https://www.aaai.org/Papers/FLAIRS/2007/Flairs07-110.pdf
[10] "CISOMAG" Gaming industry suffered 12 billion cyber-attacks in past 17 months https://www-cisomag-com.cdn.ampproject.org/v/s/www.cisomag.com/gaming-industry-suffered-12-billion-cyber-attacks-in-past-17-months/amp/?usqp=mq331AQFKAGwASA%3D&amp_js_v=0.1#aoh=15894843053934&referrer=https%3A%2F%2Fwww.google.com&amp_tf=From%20%251%24s&ampshare=https%3A%2F%2Fwww.cisomag.com%2Fgaming-industry-suffered-12-billion-cyber-attacks-in-past-17-months%2Famp%2F%23aoh%3D15894843053934%26referrer%3Dhttps%253A%252F%252Fwww.google.com%26amp_tf%3DFrom%2520%25251%2524s
[11] "Kevin Townsend" Gamers and gaming security https://blog.avast.com/cybersecurity-risks-all-gamers-should-know
[12] "Toby Arguello" Bethesda Accidentally Released A DRM-Free Version of DOOM Eternal https://screenrant.com/bethesda-releases-doom-eternal-drm-free/

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)