ONLINE GAMING SECURITY

Nathan Schomburg ICTN 4040

Introduction

As the internet has grown gaming companies have worked to build the perfect way for users to interact with each other through online gaming while maintaining user security. Advances in hacking technologies paired with a dramatic growth in online gamers has displayed security flaws thought the industry. Both the Console and PC based online gaming have had their share of security issues. Security for online gaming has become very important recently due to online game purchases and private financial data linked to the accounts. This report will discuss both the current security features online gaming and the issues that have been faced by major online game services.

PC Online Gaming

In the world of PC platform online gaming there are several major players providing games and services to users. The PC platform provides a wide open environment for game development and distribution which allows for more security risks compared to console gaming. Leading all other PC gaming services is Steam followed by the game producer Blizzard. Both of these companies are well known for their online gaming services.

Steam

Steam provides gamer's world wide a marketplace where they can buy and play games online. Like many console based login setups Steam provides a two level system of authentication to ensure a secure gaming experience. By default the account is secured by only the user's account name and login credential. The basic username and password form of authentication has in the recent years fallen to several attacks leaving user information compromised. Most recently Steam user's security has been

threatened by the discovery of the OpenSSL Heartbleed bug, key-logging malware, and phishing attacks. In 2013 it was reported that Steam users have been hacked using a variation of the Ramnit worm. This malware originally used for stealing financial login information through web browser (HTML) injections was modified and used to steal Steam user information during login. This technique of gathering data is known as a man-in-the-browser (MitB) attack. According to The Resource for Security Executives "when a user accesses the Steam Community log-in page and enters his or her username and password, the form is encrypted using the site's public key. To overcome this, Ramnit modifies the form in a way that allows it to capture the password in plain text." To account for this new form of attack Steam has made available to users a second layer of authentication security. Users now have the option to enable a feature called "Steam Guard" which sends a unique authentication code via email which must be entered upon login. This system provides the user a key code in the users email every time a request to login is made. This ensures that there is a sure failsafe for user authentication to the service assuming that the designated email account is secure.

Blizzard Gaming

While Steam is known for being a more secure form of online gaming Blizzard Gaming is known for its lack of security. Blizzard is well known for their Massively Multiplayer Online (MMO) games Diablo, StarCraft, and World of Warcraft. MMO's normally consist of hundreds or thousands of people playing together within one game world allowing players to interact. With this type of gaming where so many people interact together security of user data is crucial. Due to several previous hacking attempts on hundreds of user accounts Blizzard has implemented a second layer of login defense with the implementation of both smartphone and keychain authenticators.

Both of these methods provide the player an 8 digit Authenticator code which they must present during the regular login process on the computer. The mobile authentication app is available for both Android (Example Figure 1) and iPhone which upon installation the user must register the device to the account using the serial code given. This ensures that only devices registered to the specified account are able to generate an authorized key so that the user may gain access. The key generating system has dramatically hardened the authentication process for users to keep others out. Recently though a Trojan that pretends to be Curse Client has been found to be able to bypass the World of Warcraft authentication even with the presence of the authenticator. Although this is a very big security threat users can easily uninstall the virus and download the newly released Battle.Net Launcher by Blizzard which authenticates securely for the moment.

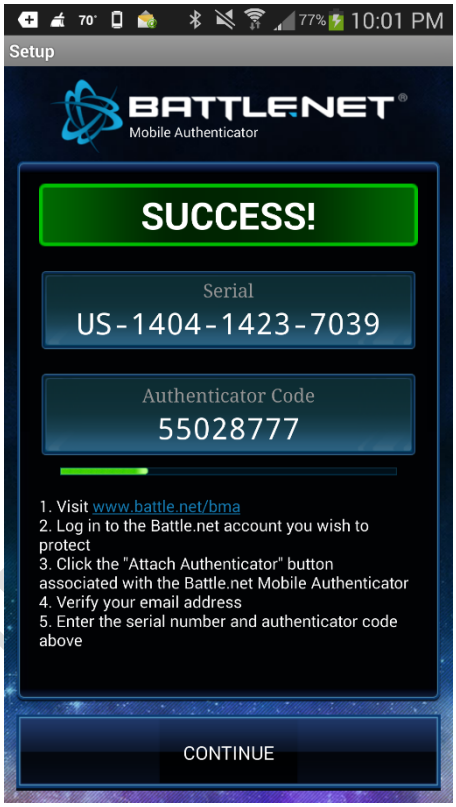

FIGURE 1: ANDROID AUTHENTICATOR

Console Based Online Gaming

Over the past decades Console gaming has grown exponentially becoming the largest form of online gaming on the market. Console online gaming is very similar to PC gaming and but is more secure due lack of open source software. The two leaders in online console gaming are Microsoft's Xbox Live and Sony's PlayStation Network. These companies regulate what software can and cannot run on the devices preventing third party applications to be installed bypassing security features. The operation

system (OS) of the consoles are designed to avoid vulnerabilities through providing a very restrictive online gaming environment. Users may only access the designated servers specified by the vendor for each game in order to play online with others. In order to protect user personal data all important data including financial data is stored in the centralized secure datacenter which is maintained by the associated console vendor. This ensures that personal data is not stored on the individual devices where it could be more easily accessed. However this leaves the company more responsible for user data. Security is very important in online console gaming because almost all of the consoles out require a credit card to be registered to each users account which pay for monthly subscription charges and downloadable content.

Sony PlayStation Network

The PlayStation Network (PSN) is Sony's online gaming service which provides to users of both their PS3 and now PS4 consoles. In the past Sony has had problems keeping user data secure even when it was secured at company datacenters. In 2011 Sony was attacked by what was claimed to be the hacktivist group Anonymous. The group used a Distributed denial of service DDoS attack against the PSN and Sony's music service Qriocity while the personal data of users was breached. This attack resulted in the loss of 77 million users account information. Since then Sony has been forced to shut down their online gaming services multiple times due to data breaches.

Sony has since increased their focus on threat detection of attacks in order to properly respond to any sort of threat.

Microsoft Xbox Live

Of the two main console platforms for online gaming Microsoft's Xbox Live is the most secure. Xbox Live provides user based online services to Microsoft's Xbox 360 and Xbox One consoles. Microsoft has set strict security settings on replacement parts and modifications to the consoles to create an even and secure play surface. Its authentication like all gaming services is user account based. Users are required to login via a Microsoft account which is able to be accessed on all windows devices. The accounts can be configured to request password upon logging into the online service. Recently a major security bug was detected by a five year old boy who was able to bypass a set password by hitting the space button a few times and then hit enter. This bug has now been patched and the devices are now secure.

Conclusion

The world of online gaming is an ever growing and changing environment which must be kept secure to protect gamers worldwide. No matter what way someone chooses play online games there are always inherent data security risk due to the fact that the internet is a shared space and is open to the public. Online gaming will never be fully secure but through vendor attack monitoring and user awareness of security threats we can game safely.

References

"5-year-old Outsmarts Microsoft, Discovers Xbox Security Flaw." *CBSNews*. CBS Interactive, 7 Apr. 2014. Web. 13 Apr. 2014. <http://www.cbsnews.com/news/5-year-old-outsmarts-microsoft-discovers-xbox-security-flaw/>.

Constantin, Lucian. "Attackers Use Ramnit Malware to Target Steam Users." *CSO*. IDG News Service, 19 Aug. 2013. Web. 13 Apr. 2014. <http://www.cso.com.au/article/524098/attackers_use_ramnit_malware_target_steam_users/>.

*Junbaek Ki, Jung Hee Cheon, Jeong-Uk Kang, Dogyun Kim, (2004) "Taxonomy of online game security", Electronic Library, The, Vol. 22 Iss: 1, pp.65 – 73.

Karmali, Luke. "Blizzard Warns of Trojan Bypassing Warcraft Authenticators." *IGN*. N.p., 6 Jan. 2014. Web. 11 Apr. 2014. <http://www.ign.com/articles/2014/01/06/blizzard-warns-of-trojan-bypassing-warcraft-authenticators>.

*McGraw, Gary, and Greg Hoglund. "Online Games and Security." *IEEE Security & Privacy Magazine* 5.5 (2007): 76-79. *IEEE Xplore*. IEEE. Web. 12 Apr. 2014. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4336285>.

Online Console Gaming Statistics. Digital image. *Mmo4arab.com*. N.p., n.d. Web. 13 Apr. 2014. <http://img4.mmo.mmo4arab.com/news/2010/04/21/stats/s1.jpg>.

Rashid, Fahmida Y. "Sony Data Breach Was Camouflaged by Anonymous DDoS Attack." *Sony Data Breach Was Camouflaged by Anonymous DDoS Attack*. N.p., 5 May 2011. Web. 13 Apr. 2014. <http://www.eweek.com/c/a/Security/Sony-Data-Breach-Was-Camouflaged-by-Anonymous-DDoS-Attack-807651/>.

"Steam Guard." *Steam Support RSS Knowledge Base*. Steam, n.d. Web. 12 Apr. 2014. <https://support.steampowered.com/kb_article.php?ref=4020-ALZM-5519#what>.

Younger, Paul. "Steam Has OpenSSL Security Vulnerability. Do Not Use until Fixed." *IncGamers.com*. N.p., 8 Apr. 2014. Web. 11 Apr. 2014. <http://www.incgamers.com/2014/04/steam-has-security-vulnerability-do-not-use-until-fixed>.