Abstract
In its most basic form, social engineering can best be summarized as the art of manipulation. By convincing another individual to divulge sensitive information or permit access to a restricted location, the hacker’s ruses unsuspecting participants to achieve their goal. In his book, The Art of Deception, Kevin Mitnick, the infamous hacker and one time FBI fugitive, asserts that humans are the biggest threat to security. So, if humans are the Achilles’ heel or weakest link in security, it is only logical that when trying to gather information or gain access, taking advantage of unsuspecting humans is the best place to begin. This research will discuss how the Kevin Mitnick style of social engineering might not be needed when most of the personally identifying information is online. Social engineering might not be able to obtain the same type of information from Data at Rest (DAR) and Data in Motion (DIM). Furthermore the paper will analyze the privacy and identity disclosure in virtual societies, specifically the Xbox 360. Swatting, stolen accounts, kicking, and identity theft will be discussed.

1. Introduction
Although social engineering does not need to be complex, and in some instances is merely a matter of “asking and ye shall receive” (Kevin D. Mitnick, 2002), what if there were easier ways for hackers to obtain sensitive information or make their social engineering attacks more fruitful? When targeting newer technologies such as gaming systems, the weakest link may no longer be humans per se, but rather how humans are required to use these new technologies. Like a hexadecimal Hegelian circle, technology and humans are an infinite loop which continually return upon each other.

Human emotions such as trust, willingness to help others, conformity, fear of getting reprimanded, and personal gain, are often cited as the primary reasons social engineering techniques are so successful (Kevin D. Mitnick, 2002) (Mosin Hasan, Vol.2, No.2, June 2010) (Charles E. Lively, 2003). However, this premise attributes some level of reasoning on the part of the individual being hoodwinked which may not be applicable when applied to gaming consoles which are primarily utilized by teenagers (PEW Internet Project, 2008) who do not possess the same reasoning capabilities as adults (Monisha Pasupathi, Vol 37, May 2001).

According to the Pew Research Center’s Internet and American Life Project, as of 2008, 97% of all teenagers (under 18 years-old) and 53% of adults (over 18 years-old) played video games on a regular basis [4]. Additionally, of the 97% of teens who played video games, 89% did so via gaming consoles such as Microsoft’s Xbox 360 or Sony’s Playstatin 3 (PEW Internet Project, 2008). In a public game room, an adult may be more cautious when disclosing personal information, while a teenager might be more apt to announce that his family is leaving for vacation that upcoming Friday so that everyone listening knows his residence will be unoccupied. Conversely, being over 18 is no guarantee that a user will not fall prey to a social engineering scam or unwittingly reveal personal information which will place him at risk.

In a 2005 study of more than 4,000 Carnegie Mellon University students who utilized social networking sites, Gross and Acquisti found that 89% of all participants used their true names, 90.8% posted an identifiable image on their profile, and 98.5% used their correct date of birth (Acquisti, 2005).

2.0 Swatting
On March 6, 2012, Pennsylvanian East Allen township resident, Lisa Yagerhofer and her family were eating dinner when a state trooper showed up at their front door with his gun drawn and a response team of approximately fifteen law enforcement vehicles on her front lawn (Swatting Hacker Uses Xbox to Trick Police, 2012). The police were responding to a distress call sent to the local 911 system via an instant message which read in part: “Please help. My dad just killed my 4 year old sister. He slit her throat. She's bleeding to death” (Swatting Hacker Uses Xbox to Trick Police, 2012). This is just one of dozens of accounts of Xbox swatting which have made headlines in recent months (Goodin, 6) (Allen, 2012) (Couts, 2011). Anyone who uses the gaming console can fall prey to swatting, as one high-profile Microsoft Xbox
FAT32 found on most legacy computers (David in Xbox is the FATX, an offshoot of the more familiar average personal computers. The file data format used this variation in file formatting is that the Xbox was information sectors found in FAT32. One reason for does not contain the typical backup boot or file system Becker, 2001). Unlike the FAT32 however, the FATX computer - it is actually more powerful than most computer it is designed solely for entertainment as opposed to productivity. Thus, redundancy and legacy support are forfeited in order to increase the system’s speed. Another reason is to protect proprietary data. Microsoft accomplishes this by signing all of Xbox 360’s executable files so that if altered the files will fail to boot. Forensic analyses of Xbox 360 hard drives revealed that while propriety data was signed and encrypted, user data was not (Ashley Podhradsky, 2011).

4.0 Stolen User Accounts

According to a recent report by Luke Plunkett, contributor at Kotaku Open Forums, there has been a surge over the past few months in hijacked Xbox 360 user accounts (Plunkett, 2012). Victims are unaware that they have been targeted until they are unable to access their accounts (Plunkett, 2012). One such victim, Susan Taylor, started a blog titled Hacked on Xbox to fight back after her Xbox Live account was hijacked earlier this year (Taylor, 2012). On her blog, Taylor encourages other victims to share their stories as well (Taylor, 2012). To date, out of the fifty-nine cases posted, only eight have been resolved by Microsoft (Taylor, 2012). There is no shortage of reports on other gamer sites as well, including Microsoft’s official Xbox Forums, from victims looking for assistance (Microsoft, 2012) (Rubin, 2012). Susan Taylor, who promptly reported the incident to Xbox requesting that they suspend her account, found herself completely helpless because the hijacker had changed her password and security question (Rubin, 2012). Not only did Microsoft fail to lock her account as promised enabling the thief to continue withdrawing money from her PayPal account, but to pour salt to her wound, the thief actually added himself to her buddy list (Taylor, 2012).

When Microsoft was questioned by Dan Crawly, staff writer for Gamesbeat, regarding the theft of his Xbox Live account in December 2011, a spokesperson for Microsoft responded that:

“Customers who use the same identity and log-in details across multiple online sites and services are more vulnerable against these everyday Internet threats” (Crawley, 2011).

Microsoft’s spokesperson further stated that:

“As ever, we advise customers to be vigilant, and provide further advice on account security across Xbox 360, Internet websites and email...” (Crawley, 2011).

These types of statements suggest that the compromised accounts are everyone’s responsibility except for Microsoft. They further imply that if users exercised more caution by utilizing different passwords and identities for their PCs and gaming consoles, they might not fall victim to these types of incidents. Conversely, if Microsoft earnestly believes that these hijackings should be attributed solely to the Internet or careless users, it appears rather contradictory then that they would direct their customers to the Internet to manage their billing accounts as outlined in the Xbox

3.0 Xbox 360 Architecture

While several popular gaming consoles exist, Microsoft’s Xbox 360 is the most popular among American consumers, selling 14.9 million consoles in 2011, eight million more than their top competitor the PS3 (Todd Bishop, 2012). The Xbox 360 enables users to play games and chat with others, instant message, surf the Internet, download game trailers, demos, games, and gaming accessories from Microsoft’s Live Marketplace, rent movies from Netflix, watch movies or television shows with Hulu Plus or Comcast’s Xfinity on demand, access and post on social networking sites such as Twitter and Facebook, and even save to, or retrieve games from, the cloud (Microsoft, 2012). Xbox 360 is even capable of writing its own blog about the user’s daily activities (Meer, 2008).

The Xbox 360 is not only similar to a personal computer - it is actually more powerful than most average personal computers. The file data format used in Xbox is the FATX, an offshoot of the more familiar FAT32 found on most legacy computers (David Becker, 2001). Unlike the FAT32 however, the FATX does not contain the typical backup boot or file system information sectors found in FAT32. One reason for this variation in file formatting is that the Xbox was designed solely for entertainment as opposed to productivity. Thus, redundancy and legacy support are forfeited in order to increase the system’s speed. Another reason is to protect proprietary data. Microsoft accomplishes this by signing all of Xbox 360’s executable files so that if altered the files will
Live Terms of Use (Microsoft, 2011). Furthermore, how careless was Xbox Live’s Policy and Enforcement executive, Stephen Toulouse, when his Xbox Live account was stolen (Ferro, 2012)?

The only apparent link between the victims of these account hijackings is that they utilized Xbox Live (Ferro, 2012). Exactly how they are being selected as targets is unknown at this time. However, malicious hackers are not the only individuals users need to be wary of. The Xbox Live Terms of Use clearly state that by using Xbox Live consumers are consenting to permit Microsoft to automatically upload data about their computers as well as how they use the service (BBC, 2009). What is even more discerning is that users are also giving their consent to allow Microsoft to share data about them, including but not limited to, their name, gamertag, motto, avatar, and any other PII provided (BBC, 2009)” with Microsoft’s “affiliates, resellers, distributors, service providers, partners, and/or suppliers (BBC, 2009)”.

5.0 Kicking

Kicking is a quasi-hacking technique where an Xbox user is “kicked” off of Xbox Live by another player in the room. Utilizing free tools such as OXID’s Cain and Able (OXID, 2012) password recovery tool, the hacker is capable of gaining access to another gamer’s IP and MAC addresses which he then exploits to repeatedly kick the gamer off every time he tries to connect to a game room (Images 1-3). Although typically viewed as merely a form of malicious harassment, the information obtained can be used to perform more serious spoof attacks and should not be taken lightly. Once the attacker has gained access to the target’s IP address, he can then ascertain what city and state the player is located in, the name of their service provider, send a virus directly to the target’s machine, or employ further reconnaissance techniques using tools such as Nmap (Nmap.org, 2012) to secure even more sensitive data.

These booting services are also being sold to players who are seeking to get revenge on other gamers (BBC, 2009). What is problematic about this type of attack is that it does not target Xbox directly, but rather the victim’s internet connection (BBC, 2009). For approximately $20.00, some hackers are even willing to remotely access their customer’s PC and set these hacking tools up for them permitting the client to target players independent of the hacker (BBC, 2009). For an even larger fee, these hackers will add the compromised machine to a botnet enabling them to perform more powerful buffering or Denial of Service attacks against the targeted IP address (BBC, 2009).

Microsoft defines three categories of NAT on their consoles—open, moderate, and closed. These attributes, or policies, control the amount of user access to Live services. The ports used are UDP (User Datagram Protocol) ports 3074, 5060, and 5061 (CAI Networks, 2000). Considering that UDP is a connectionless protocol, this could provide hackers with additional vulnerabilities to exploit, recalling that the hacker is targeting the player’s internet connection not the actual gaming console, such as UDP 5060 and weak SIP or Brute Force Attacks. Thus, when gamers who are not familiar with NAT or VoIP weaknesses change their settings in an effort to host games with other players, they are unknowingly introducing more vulnerabilities into their systems.
Repeatedly Kicking a player out of a game room primes the victim so he can be easily manipulated by the hacker. Either by posing as a Microsoft employee who can assist in “fixing” the connection problem or as a helpful gamer who just happens to be computer savvy, the target may naively provide personal information or even permit the “good Samaritan” access to his system to fix what he might believe is a technical problem. Although an adult might not fall prey to these types of ruses as easily, an adolescent, who does not have the same reasoning abilities as an adult, or may fear he has done something to his system, may be easily swayed (Monisha Pasupathi, Vol 37, May 2001).

6.0 Identity Theft and Used Consoles

With the continual emergence of new gaming bundles and sleeker systems, more users will be selling or trading their current consoles either because they are outmoded or to financially offset the cost of acquiring a newer system. In addition to selling the system in its entirety, some users may elect to sell or swap the hard drive independent of the console. Oftentimes, after acquiring numerous games, storing countless media files, or amassing a plethora of other data, the user may seek to change a drive out of necessity because a larger drive is required.

A quick look on eBay provides a small snapshot of how many systems are sold daily. As of the date of this report, there were over 3,705 Xbox 360 gaming systems for sale in the United States alone (eBay, 2012). These listings are subject to change by the minute and do not include Xbox hard drives being sold without a console. It is relevant to note, that when purchasing used gaming systems from online auction sites, identity thieves gain somewhat of an additional advantage – the seller’s name and mailing address appears right on the package when it arrives. Likewise, if acquired from a classified forum such as craigslist (Craigslist, 2012) unscrupulous individuals can amass the seller’s name, telephone number or email address, and various other tidbits of information by way of social engineering.

Typically, when an individual decides to sell or trade their Xbox console or hard drive they delete, or erase their personal data and history believing the information is permanently gone. However, this common practice does not technically remove data from the console - it merely alters it (Podhadsy, 2011). When data is deleted, it is not really erased; in fact, it is not even necessarily moved. In most cases, the information or file stays exactly where it was. What changes is the path and filename of the data known as the directory entry. The first letter of the file is modified and marked with a character indicating it is available to be rewritten. There it will stay intact until new data is written over the existing data (overwriting).

More knowledgeable Xbox users may opt to reformat the console’s hard drive in order to destroy sensitive information. Theoretically, when an Xbox drive is reformatted, every available block of space is filled with zeros, or ASCII NUL bytes (0x00). Successfully overwriting a drive is not only contingent upon both the logical and physical condition of the drive, but the methodology utilized as well. It would be problematic at best to say, with any degree of certainty, that all information can be eradicated.

According to Microsoft’s Online Xbox 360 Support tutorials, once the Xbox console is reformatted, “…all of the information saved on that device is erased and cannot be recovered (Microsoft, 2012).” However, this is rather misleading.

7.0 Preparing Hard Drive for Examination

Researchers took a new Xbox 360 Elite containing a Hitachi 120 GB hard drive and created two Xbox Live gamertags. This was in addition to the automatically assigned gamertag Microsoft provides new users (i.e.: Player1). Two of these user profiles, including the one automatically assigned, were deleted. The third remained intact. Each of the two profiles created were used for a brief period of time to play games and access Xbox Live services. All the deleted gamertags were removed following Microsoft’s recommendations:

1. Go to Settings, select System.
2. Select Storage.
3. Select All Devices.
4. Select Gamer Profiles.
5. Select the gamertag that you want to delete.
6. Select Delete.
7. Select Delete Profile and Items (this option deletes the profile and all saved games and achievements affiliated with that profile) (Microsoft, 2012).

7.1 Imaging the Drive
The current standard for authenticating evidence is to preserve the original hard drive by imaging, or creating a bit-by-bit copy of the drive to work from (Nelson, 2008). This ensures that the original evidence has not been accidently altered or tampered with. However, when working with the Xbox 360 drive, this can be rather challenging.

Some of the complications encountered when trying to image an Xbox 360 drive can be attributed to the drive’s FATX file format as well as the unknown or proprietary structure of the drive. The hard drive was imaged with DrDD, FTK Imager, and in Linux. All three utilities yielded illegible sectors. Thus, in order to view the the hard drive, researchers utilized gamer modification tools. By employing modification utilities the HD could be opened directly and files of interest extracted and examined in a hex editor.

7.2 Hash Checksums
In light of the difficulty in obtaining a forensically sound image of the drive to work from, repeated MD5 and SHA-1 checksums were performed to ensure the integrity of the study drive. Using both FTK Imager and Linux, checksums were continually recorded. While this is not atypical in an examination to ensure the validity of any evidence discovered, it was also necessary in this case to monitor the dependability of non-forensic tools utilized as well.

8.0 The Investigation
While there were several groups of nulls, the drive did not exhibit signs of being overwritten as there were no large sections of zeros in non-program specific files. It is always problematic at best however to declaratively state that an Xbox drive has not been reformatted without further studies as each operating system has its own unique way of performing this process and while the Xbox does share some similarities with a PC, it cannot truly be measured using the same criteria (Computer Gyaan, 2010).

Using Modio, the hard drive was then opened to see if either of the deleted user names could be recovered. Modio can be extremely handy for viewing image files on the fly without needing to export them first using another program. Because hardware write blocking is necessary when utilizing Modio as data can be overwritten with software write blocking, Thermaltake’s BlackX docking station with hard write blocking capabilities was employed.

Upon opening the drive, three players were noted. The two deleted accounts, which were represented by strings of zeros (Image 4) were discovered. The third gamertag, HakinLuger was present, complete with the user’s avatar. A preliminary examination of player HakinLuger’s downloads reveals games (Kinect Adventures, Halo, and Call of Duty) as well as the services he utilized through Xbox Live such as Netflix and Hulu Plus (Image 5).

**Image 4– Accounts either active or deleted on the hard drive**
A quick search for HakinLuger at XboxGamerTag.com (Xbox Gamertag, 2012) confirms the games found on the drive and reveals that our gamer had a preference for sports games (Image 6). Xbox GamerTag is a free gaming search engine that enables visitors to obtain anyone’s profile, including, but not limited to, recent games played, achievements, game scores, and avatar (Xbox Gamertag, 2012). From an investigative purpose, because the site provides the date and time a game was last played, it could be used in collaboration with other data when trying to place, or eliminate, a suspect in the same game room with the victim. From a social engineering perspective, these types of databases provide a multiplicity of data to exploit making their job easier.

David Collins, a computer scientist at Sam Hoston State University in Texas and distributed by Protowise Labs (Protowise Labs, 2011). XFT 2.0 features both FATX and XTAF (derived from MS-DOS) file system recognition, file hashing, displays deleted files (but does not recover them), and file type identification. It is designed to run on Windows operating systems and features a user-friendly interface, although when tested on both Windows XP and WIN 7, the utility did not run as smoothly on the later (Dr. Ashley Podhradsky, 2011). In order to examine the drive with XFT 2.0, the HD first had to be imaged with DrDD. Unfortunately, although XFT recognizes the FATX file structure, the host machine running Windows does not.

Utilizing XFT, the second gamertag, which was created, used, and then deleted, was revealed (POD H RAD SKY). Because XFT does not recover deleted files, researchers were unable to obtain detailed data about the gamertag by examining the drive. However, the user’s profile was available at XboxGamerTag.com (Image 7). The second deleted gamertag which was automatically created by Microsoft was never recovered. This might be due to the fact that it was never utilized.

While examining the hard drive with XFT 2.0, another deleted gamertag was found (Reaver95) which researchers did not create (Image 8). Reaver95 was a guest who logged on to our Xbox using his own gamertag to play. With nothing more than his gamertag, researchers performed an internet search and within twenty minutes a remarkable amount of personally identifiable information was ascertained on Reaver95’s (Image 9) including:

- Favorite Xbox 360 game, scores, and last logon date (Microsoft, 2012)
- Location (Microsoft, 2012)
What is so alarming about this is that there was no need to hack an account or employ social engineering techniques to amass this information. With as little as a gamertag, enough PII was gathered to either steal Reaver95’s identity, perform an extremely sophisticated social engineering attack, or to sell his identity on the black market (Ferro, 2012).

Another gamertag found on the hard drive was BryanOban1701 (Image 10). This player was not on our gamer’s buddy-list or in a cache file which would indicate that he was playing in the same game room with HakinLuger, but was located in a Dashboard file. An Internet search of gamertag BryanOban1701 revealed that he and HakinLuger shared a mutual buddy on Xbox Live named Maliki67 (Image 11) (Xbox Live Score, 2012). This finding suggests that parallel to Facebook, Linked-in, and other social networking sites, Microsoft connects users who share something in common with one another.
9.0 Requested: Safeguarding PII

As society continues to have a greater dependency on non-traditional computing devices, including virtual worlds and social networking, there are new risks introduced. Social networking and virtual world have become a popular medium for both communication and hackers who want to employ social engineering tactics. By employing social engineering schemes, criminal activities are more successful because it affords higher rates of success and considerably lower chances of getting caught and prosecuted.

One way users can protect themselves is by using prepaid Xbox Live membership cards as opposed to using credit cards or PayPal. Unfortunately, accounts that do not enter a credit or debit card are unable to utilize Microsoft’s 2 year Xbox Live Gold subscription as pre-paid cards and PayPal are not accepted forms of payment (Microsoft, 2012). A 2-year Xbox Live Gold subscription enables Xbox Live users to rent movies through Netflix, chat, watch shows with Hulu Plus, and participate in multiplayer gaming at substantial discount (Microsoft, 2012).

Like their counterpart in Virtual World, Microsoft’s Xbox points can be traded-in by users to enhance their gaming experiences. On Xbox, points can be used to rent movies, download game extras such as maps, levels, vehicles, and purchase avatar accessories. In lieu of purchasing Microsoft points through the console using a credit card, a safer alternative is for users to purchase a Microsoft points cards from their local video store.

As with any technology, users should always check, and if necessary, change, their device’s default settings. Interestingly, Xbox Live safety and privacy default settings are automatically set according to the birthdate entered by the user when setting up his account (Microsoft, 2012). The default settings for an adult permits anyone to access the player’s game history, online status, and friend’s list (Microsoft, 2012).

Xbox Live subscribers should not use the same username or email address for their Xbox Live accounts as they do for other membership based accounts. Creating separate Hotmail and Messenger accounts exclusively for Xbox Live may deflect reconnaissance activity. Because PayPal is linked to the user’s bank account and credit card, using PayPal should be avoided. Although Microsoft details how to change default settings to protect player privacy on their website, it appears to be geared more toward protecting minors (Microsoft, 2012). Finally, to deter hackers from listening in on conversations users should set up private game rooms (referred to as parties) and utilize the privacy settings on their headsets.

10.0 Future Work

In May of 2012 Microsoft announced that it was testing a version of Internet Explorer with the goal of integrating the browser directly into the Xbox platform. (Murph, 2012). While many gamers view the additional applications and functionality as a benefit, there may be a potential downside. GFI recently published a list of the most vulnerable applications. (Florian, 2012). The list was compiled by reviewing the 3532 vulnerabilities reported to the National Vulnerability Database (NVD) in 2011. Internet Explorer was number 11 in the list of “the most targeted applications in 2011”. The NVD utilizes the Common Vulnerability Scoring System version 2 (CVSS) to label vulnerabilities on a Low, Medium, or High scale. Scores range from 0-10. Vulnerabilities scoring between a 7.0 and 10.0 are labeled as “High”. Of the 45 Internet Explorer vulnerabilities reported to the NVD, 31 were designated as “High” (Florian, 2012). The continual expansion of Xbox platform and inclusion of applications like Internet Explorer are sure bring additional security concerns.

11.0 References


Monisha Pasupathi, U. M. (Vol 37, May 2001). *Seeds of wisdom: Adolescents' knowledge and*
judgment about difficult life problems. 
 DEVELOPMENTAL PSYCHOLOGY, 351-361.


http://www.gobison.com/ViewArticle.dbml?DB_OEM_ID=2400&ATCLID=659643


http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1526403,00.html

Protowise Labs. (2011). XFT 2.0 Game Console Forensics is Released. Retrieved 5 22, 2012, from XFT 2.0 Game Console:
http://protowise.com[tag=xft-xbox-forensics


http://www.hackedonxbox.com/


https://sites.google.com/site/whsclassof01/classmateupdates


http://www.xboxlivescore.com/profile/Maliki67
