Security Analysis of Xbox 360 Vulnerabilities

Patrick Engebretson
Dakota State University
Madison, SD
pat.engebretson@dsu.edu

Ashley Podhradsky
Dakota State University
Madison, SD
ashley.podhradsky@dsu.edu

D. L. Grahek
St. Thomas More High
Rapid City, SD
Diane.Grahek@rccss.org

A. J. Bierschbach
Madison High School
Madison, SD
Al.Bierschbach@k12.sd.us

Abstract: The growing popularity of using gaming consoles for more than just gaming increases the risk of intrusive activities and related security breaches. Current literature is explored, an online survey of users is conducted, and a security intrusion exercise is performed to study the security vulnerabilities of operational Xbox 360 systems.

Keywords: Xbox; gaming consoles; security;

I. INTRODUCTION

The growing popularity of using gaming consoles for more than just gaming increases the risk of intrusive activities and related security breaches. The purpose of this study is to explore related literature, conduct an online survey of the common practices utilized by Microsoft Corporation's Xbox users, and carry out preliminary intrusive activities on working Xbox 360 gaming consoles. It will include recommendations for Xbox users (particularly teen users) to protect themselves and their Xbox's from invasive activities. The security intrusion exercise was conducted to study the potential of invasive activities within an embedded Xbox 360 system.

II. LITERATURE REVIEW

Vulnerabilities in the Xbox are widespread. The first vulnerability is the unknown backdoors that are opened by modification of the hardware (commonly called "modding"). Modding can consist of re-flashing or replacing the BIOS chip (with a modchip), which will allow the user to play unsigned or unauthentic games and boot from "other" media (XBOX-SCENE, 2012). An additional modification allowed by the new BIOS replacement is the substitution of the Xbox dashboard. The dashboard is a menu-like IOS that the Xbox will boot to if an alternative media source (a CD or DVD) is not available. The Evolution-X is a popular replacement dashboard. A modded dashboard will allow for the installation of a larger hard drive, thus eliminating the need for a CD or DVD, as games can be backed up and played from the new hard drive. The modded dashboard/IOS also has a built-in FTP Server, a configurable menu system, new network capabilities, a flash BIOS utility, and the ability to format, partition, and upgrade the hard drive (XBOX-HQ.com, 2010).

The fiddling with the inside of the Xbox has opened opportunities for pirates to play "backup" games and movies on the systems, as well as given amateur game makers the opportunity to create and play home-brewed software. Unfortunately, this also opens many prospects for backdoor hacking intrusions, and some of these unstipulated activities are illegal, according to the Digital Millennium Copyright Act (Koebler, 2012).

The amplified activity from the hacking community has Microsoft increasingly cautious of the integration of new content partners. Johnson & Wallenstein (2011) reported that the director of security policy of Microsoft's interactive entertainment division pointed out the recent expansion of Xbox Live's content partners, asking that such partnerships "be careful about how they coordinate integration of their systems, lest they leave a backdoor open" (p.6). An example of this concern follows.

Xbox Live vulnerability was brought to the forefront in early 2012, when hackers gathered gamer tags from rounds of games played on Xbox Live. Hackers would then individually "Google" the gamer tags, finding social networking sites linked to the gamer tags. These social sites often would offer up a gamer's Windows Live email address (and potential Windows Live ID). Hackers would then return to Xbox.com and type in the newly-found email address and random password. If they received a message indicating the account does not exist, they would move to another email address. If they received a message that the email address or password was incorrect, the hackers would brute force attack the account with a script of dictionary passwords. After eight tries, Xbox would ask for a CAPTCHA code, but also had an option to "try with another Live ID," allowing hackers to try another 8 times, and so on. A savvy hacker could automate this process. After accessing the Xbox Live account, the user's credit card info, and other content provider info such as Netflix®, was available to the hacker. Hackers could also spend the user's points, make purchases, change the user's gamertag and password, and change the email address associated with the account (Pottinger, 2012). Microsoft is working on this, but there are continued issues with this vulnerability.

In addition to spending the user's points, another study pointed out that hackers could steal credit card information stored on an Xbox 360's hard drive. Researchers from Drexel University and Dakota State University purchased a refurbished Xbox 360 from a Microsoft-authorized dealer and modified the software to find the original owners' files, folders and credit card information on the hard drive (Liebowitz, 2012). An assumed best practice would be to remove and destroy Xbox hard drives before recycling or trading in the device.

Despite the hard drive vulnerability, the file system itself offers resistance to intrusion in its basic structure: It uses a variation of the FAT file system called FATX. FATX is unique to the Xbox, and thus requires familiarity with its distinctive character and organization before intrusion activities can begin. The Xbox FATX file system can be comprised of three or more partitions, all of which serve specific functions within the Xbox. Not only is the concept of the FAT file system quite dated, the Xbox also uses legacy code for several other functions, including some database structures (Bolt, 2011).

The government is also getting involved in the act of collecting information from gaming consoles. The Navy had hired a firm to develop tools for extracting data from gaming consoles. The firm purchased used consoles to create a prototype device to gather both online and offline data. The device will be used to search for console-based messages that may have sensitive intelligence information (Allen, 2012).

Hargreaves & Rabaiotti (2010) investigated the potential to harvest data from game console RAM. Using traditional methods of imaging RAM are not possible due to the unique configuration of the Xbox hardware and software. Most imaging tools rely on the manufacturer of the embedded system to allow such features. It was discovered that exploiting a buffer overflow vulnerability in an identified game allowed code to be executed and the content of the overflowed memory redirected. By executing the exploit within the already authenticated game, it was possible to bypass authentication procedures. Care was taken to move the imaged memory in small 1 MB chunks, as the Xbox would crash if the entire memory image would be moved. The small moved files would then be reassembled to recreate the memory image. It was discovered that accessing certain virtual address spaces also caused crashes. It should be noted that this vulnerability was identified in only one particular game, and patches or updated games would make it difficult to generalize the procedure across the Xbox system.

III. ONLINE SURVEY

A. Methodology

A short online survey of owners of Xbox's was conducted using *Survey Monkey* to identify vulnerabilities created by user practices. Specifically, e-mail solicitations were sent to parents of middle school and high school students at selected rural and urban schools in South Dakota. Approximately 800 families were asked to participate. The survey was completed by 186 parents, demonstrating potential concern that parents have for the security of their homes' Xbox gaming consoles. Section III D. displays the actual results of the online survey.

B. Findings

The survey started by asking owners how long they had owned the Xbox. Over three-fourths of the respondents indicated that they have had the Xbox for at least two years, with almost 27 percent indicating they had owned the Xbox for over five years. Primary users of the Xbox were middle-school and high-school students. Adults accounted for only 19.2 percent of the primary users. 83.1% of owners had purchased a new game for the Xbox within the past year, indicating the popularity of the system and its continuous use in the home. Playing games was rated as the number one use of the Xbox (94.7%). Watching movies and using the Xbox as a Netflix or Hulu-Plus (or similar) portal ranked two and three, respectively.

An Xbox Live account is associated with 77.1% of the Xbox gaming consoles, with 46.6% of those accounts having a credit card associated with the Xbox Live account.

The majority of parents were not aware that the Xbox Live Family Pack subscription included parental controls. Approximately 60 percent surveyed indicated they did not know that social networking sites such as Facebook are accessible through the Xbox gaming console.

Lastly, the survey inquired if users were able to play backed-up games without the game CD installed (i.e. games that would normally require a game CD). 20.3% indicated a positive response to the question.

C. Observations and Recommendations

The survey findings offer these observations and recommendations, with respect to security vulnerabilities. The majority of primary users are high school age and younger. Many young people are not aware of proper security practices, such as the importance of downloading and running updates and using strong passwords that cannot (must not) be shared with others. However, most new games purchased prompt for updating of the console before playing the new game, so it is likely that with over 83% purchasing a new game within the past year, most consoles have received patches and updates at least once in the past year. It is essential that all Xbox users download all updates when prompted.

There are benefits to associating the gaming console with any chosen Xbox Live account (basic or beyond), as it will ensure updates and patches are pushed out to the machine. Beyond the Basic Xbox Live account, a fee is assessed for additional features, such as the ability to participate in online gaming and to use parental controls. There are documented vulnerabilities in the Xbox Live account system, and there is potential risk with associating a credit card with the Xbox Live account.

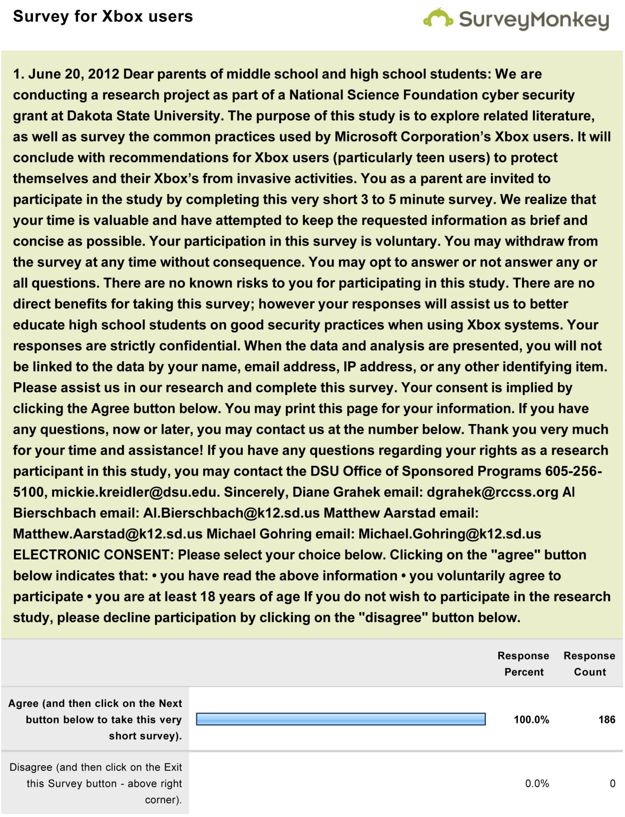
Although most parents surveyed were not aware of the parental controls, additional security features are available, including limiting access to social networking and limiting the amount of time the console can be used.

As for the twenty percent that indicated users were able to play backed-up games without the game CD installed (i.e. games that would normally require a game CD), it could be assumed that at least some of the systems have been modified, or "modded," allowing pirated or home-brewed games and movies to be used on the gaming console. This would also correspond to the approximate twenty percent of the users who indicated that they did not have an Xbox Live account associated with their gaming console. Microsoft has a number of mechanisms in place that detect "modded" systems and will not allow Xbox Live accounts to be associated with a "modded" console. The other explanation could be those parents and families who do not wish to use the Internet access capability on the Xbox.

Xbox recommends that users add extra security proofs to their Xbox Live accounts. Proofs include adding a mobile phone number to their account, adding a trusted PC, having an e-mail address associated with the account and including a secret question with an answer that doesn't match the question. Xbox also recommends using a strong password with a combination of uppercase and lowercase letters, numbers and special characters. A user's Xbox Live account should have a different username and password than other online sites. Users should use caution when using their Windows Live ID on shared computers or in public places. Users should also require their console to ask for their Windows Live ID and password when signing into Xbox Live. Users should set an Xbox Live passcode when anyone wants to use that user's profile on their console (Microsoft, 2012).

Microsoft has a good video on gamer safety, but it is hard to find on the Xbox.com website (Microsoft, 2012). It would be good to have the safety video on one of the main pages of the web site to remind gamers, especially young ones, of proper safety practices while gaming online. It would be advisable to share this video with secondary students in a classroom environment and it is recommended that parents share this with their children.

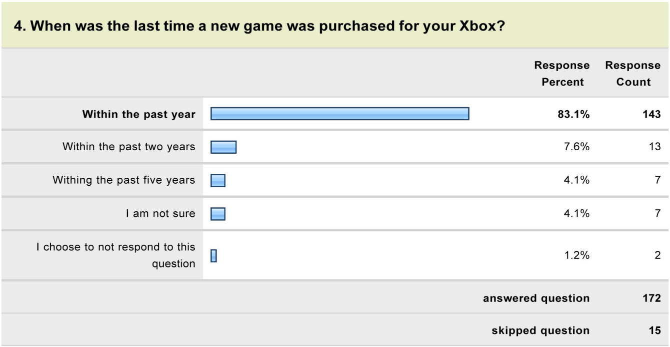
D. *Online Survey Results*



Survey for Xbox users

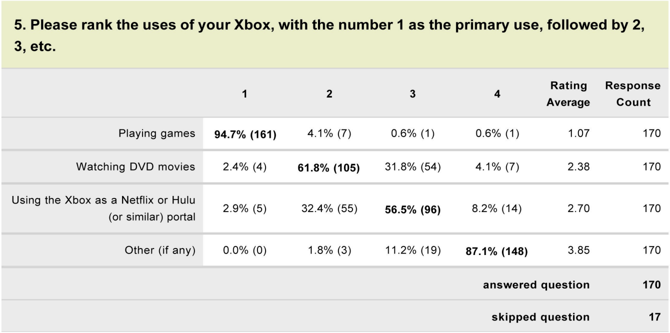
1. June 20, 2012 Dear parents of middle school and high school students: We are conducting a research project as part of a National Science Foundation cyber security grant at Dakota State University. The purpose of this study is to explore related literature, as well as survey the common practices used by Microsoft Corporation's Xbox users. It will conclude with recommendations for Xbox users (particularly teen users) to protect themselves and their Xbox's from invasive activities. You as a parent are invited to participate in the study by completing this very short 3 to 5 minute survey. We realize that your time is valuable and have attempted to keep the requested information as brief and concise as possible. Your participation in this survey is voluntary. You may withdraw from the survey at any time without consequence. You may opt to answer or not answer any or all questions. There are no known risks to you for participating in this study. There are no direct benefits for taking this survey; however your responses will assist us to better educate high school students on good security practices when using Xbox systems. Your responses are strictly confidential. When the data and analysis are presented, you will not be linked to the data by your name, email address, IP address, or any other identifying item. Please assist us in our research and complete this survey. Your consent is implied by clicking the Agree button below. You may print this page for your information. If you have any questions, now or later, you may contact us at the number below. Thank you very much for your time and assistance! If you have any questions regarding your rights as a research participant in this study, you may contact the DSU Office of Sponsored Programs 605-256-5100, mickie.kreidler@dsu.edu. Sincerely, Diane Grahek email: dgrahek@rccss.org Al Bierschbach email: Al.Bierschbach@k12.sd.us Matthew Aarstad email: Matthew.Aarstad@k12.sd.us Michael Gohring email: Michael.Gohring@k12.sd.us ELECTRONIC CONSENT: Please select your choice below. Clicking on the "agree" button below indicates that: • you have read the above information • you voluntarily agree to participate • you are at least 18 years of age If you do not wish to participate in the research study, please decline participation by clicking on the "disagree" button below.

	Response Percent	Response Count
Agree (and then click on the Next button below to take this very short survey).	**100.0%**	**186**
Disagree (and then click on the Exit this Survey button - above right corner).	0.0%	0



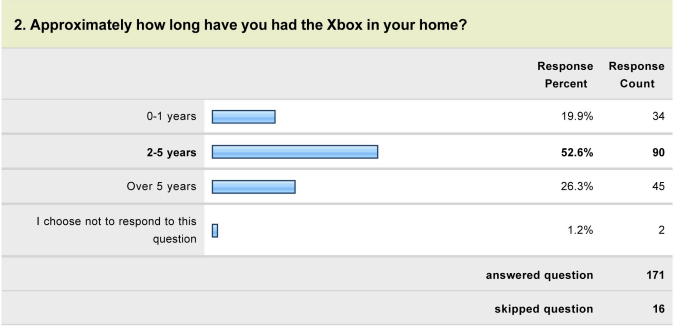
4. When was the last time a new game was purchased for your Xbox?

	Response Percent	Response Count
Within the past year	**83.1%**	**143**
Within the past two years	7.6%	13
Withing the past five years	4.1%	7
I am not sure	4.1%	7
I choose to not respond to this question	1.2%	2
answered question		**172**
skipped question		**15**



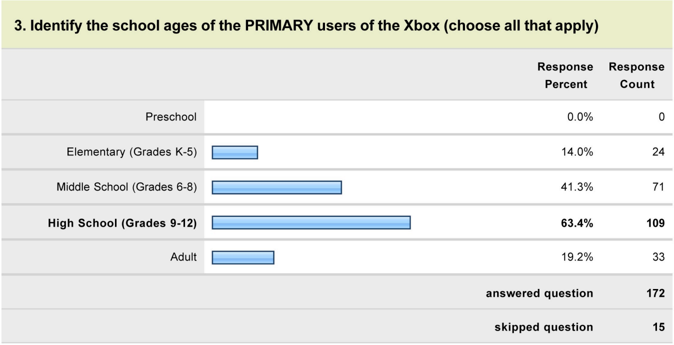
5. Please rank the uses of your Xbox, with the number 1 as the primary use, followed by 2, 3, etc.

	1	2	3	4	Rating Average	Response Count
Playing games	**94.7% (161)**	4.1% (7)	0.6% (1)	0.6% (1)	1.07	170
Watching DVD movies	2.4% (4)	**61.8% (105)**	31.8% (54)	4.1% (7)	2.38	170
Using the Xbox as a Netflix or Hulu (or similar) portal	2.9% (5)	32.4% (55)	**56.5% (96)**	8.2% (14)	2.70	170
Other (if any)	0.0% (0)	1.8% (3)	11.2% (19)	**87.1% (148)**	3.85	170
answered question						**170**
skipped question						**17**



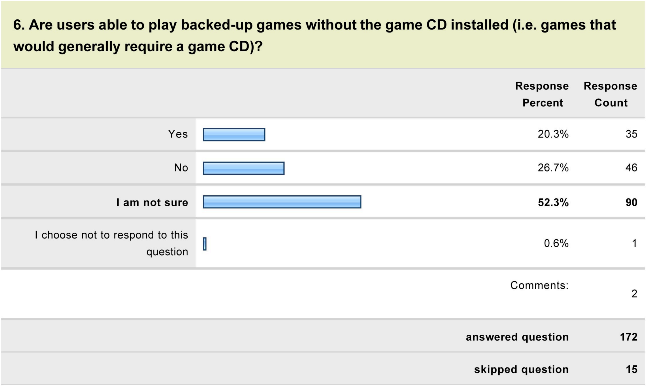
2. Approximately how long have you had the Xbox in your home?

	Response Percent	Response Count
0-1 years	19.9%	34
2-5 years	**52.6%**	**90**
Over 5 years	26.3%	45
I choose not to respond to this question	1.2%	2
answered question		**171**
skipped question		**16**



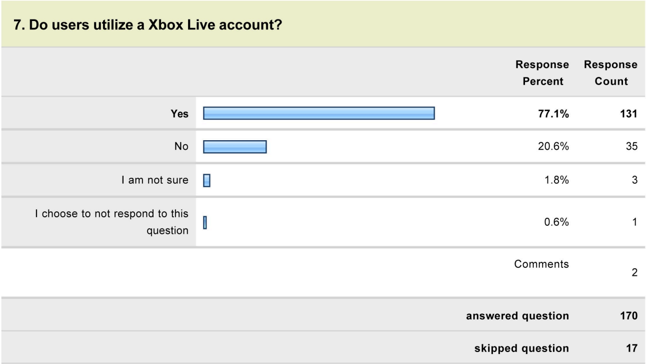
3. Identify the school ages of the PRIMARY users of the Xbox (choose all that apply)

	Response Percent	Response Count
Preschool	0.0%	0
Elementary (Grades K-5)	14.0%	24
Middle School (Grades 6-8)	41.3%	71
High School (Grades 9-12)	**63.4%**	**109**
Adult	19.2%	33
answered question		**172**
skipped question		**15**



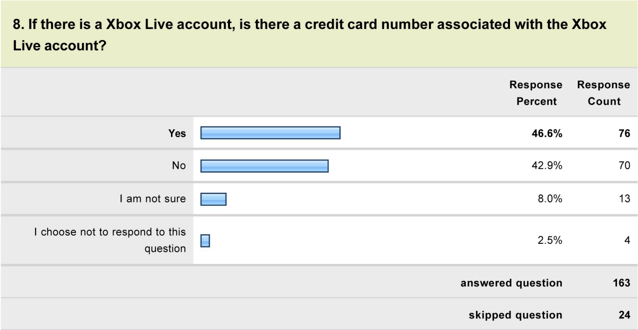
6. Are users able to play backed-up games without the game CD installed (i.e. games that would generally require a game CD)?

	Response Percent	Response Count
Yes	20.3%	35
No	26.7%	46
I am not sure	**52.3%**	**90**
I choose not to respond to this question	0.6%	1
Comments:		2
	answered question	**172**
	skipped question	**15**



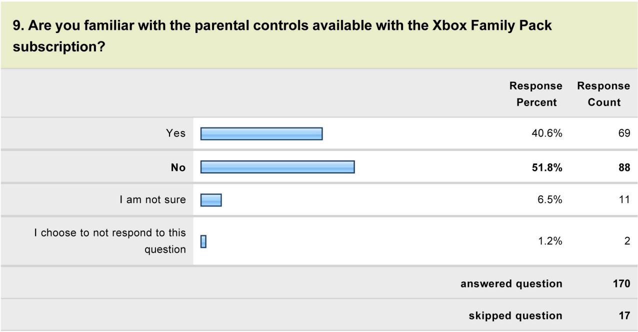
7. Do users utilize a Xbox Live account?

	Response Percent	Response Count
Yes	**77.1%**	**131**
No	20.6%	35
I am not sure	1.8%	3
I choose to not respond to this question	0.6%	1
Comments		2
	answered question	**170**
	skipped question	**17**



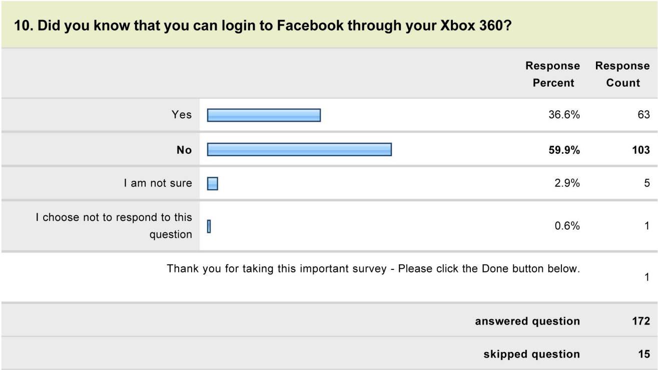
8. If there is a Xbox Live account, is there a credit card number associated with the Xbox Live account?

	Response Percent	Response Count
Yes	**46.6%**	**76**
No	42.9%	70
I am not sure	8.0%	13
I choose not to respond to this question	2.5%	4
	answered question	**163**
	skipped question	**24**



9. Are you familiar with the parental controls available with the Xbox Family Pack subscription?

	Response Percent	Response Count
Yes	40.6%	69
No	**51.8%**	**88**
I am not sure	6.5%	11
I choose to not respond to this question	1.2%	2
	answered question	**170**
	skipped question	**17**



10. Did you know that you can login to Facebook through your Xbox 360?

	Response Percent	Response Count
Yes	36.6%	63
No	**59.9%**	**103**
I am not sure	2.9%	5
I choose not to respond to this question	0.6%	1
Thank you for taking this important survey - Please click the Done button below.		1
	answered question	**172**
	skipped question	**15**

IV. Security Intrusion Exercise

A. Methodology

In addition to the online survey, a security intrusion exercise was conducted to study the potential of invasive activities within four working Xbox 360 systems. The security intrusion exercise was performed by undergraduate and graduate information security students in a university setting. The students first made an online inquiry and found that XboxLive.com lists ports 53, 80, 88, and 3074 as needing to be open for traffic on a network. Information gathering tools used included nmap, ping, arp, dsniff, arpspoof, and *Wireshark®.* Simple penetration tools typically used for Windows or Linux were tried as well. Unless otherwise noted, most intrusion tools were ran from a standard Ubuntu (Linux) installation.

B. Findings, Observations, and Recommendations

An nmap scan found that on one Xbox, an additional port, 1032, was open and being used for 1ad3 web services, but only during one Xbox Live session. Other scans indicated a mere 1,697 ports were identified as functional (but filtered) on a typical Xbox 360 system - another indication of the Xbox system's limited scope. Attempts to ping the Xbox systems using ICMP protocols were not successful. It is unknown if ICMP protocols are enabled in the Xbox operating system. A simple arp –a inquiry from a Windows 7 laptop resulted in the harvesting of the MAC addresses associated with the four Xbox systems. Penetration tools typically used for Windows or Linux were tried, but proved ineffective. More time would have allowed for additional strategies in this area.

During a network play session of *Call of Duty MW3* (not using Xbox Live), there were no identified open ports scanned. Despite not using Internet play with Xbox Live during this session, an extensive amount of encrypted packet traffic was constantly being sent to Microsoft by all four systems, as observed by *Wireshark®.* More analysis is needed of these packets to determine the function and readability of the traffic. Arp spoofing was successfully performed during this network play session on one of the systems, and the spoofed Xbox system continued to send packets to Microsoft. Upon ending the network game and moving the four systems to sign on to Xbox Live, the arp poisoning was immediately detected by Microsoft, and the poisoned system could not sign in to Xbox Live until the spoofing was removed. After an Xbox Live session of *Call of Duty MW3* was underway, a different Xbox system was arp poisoned, and within a very short time it was detected by Microsoft and the game was abruptly ended on the system, and the system was logged off of Xbox Live. Removal of the spoof allowed the gamer to sign in and resume play.

V. CONCLUSION

The nature of the Xbox operating system and its narrow functionality also limits the ability to intrude into a working system. The success in arp spoofing could result in redirection and the use of certain denial-of-service activities at the network level. Basic information gathering tools are effective, and vulnerabilities can be assumed as all information gathered has potential to be used in more invasive activities. Online activities and the use of the Xbox Live account for social networking and additional entertainment options reinforces the need for increased vigilance and the use of sound security practices by Xbox users.

REFERENCES

[1] Allen, B. (2012, April 11). US Government Hires Firm to Hack Video Game Consoles. Retrieved June 11, 2012, from TechnologyTell.com: http://www.technologytell.com/gaming/91745/us-government-hires-firm-to-hack-video-game-consoles/

[2] Bolt, S. (2011). XBOX 360 Forensics. Burlington, MA: Elsevier.

[3] Hargreaves, C.J. & Rabaiotti, J.R. (2010, May). Using a software exploit to image RAM on an embedded system. Digital Investigation, 6(3), 95-103. doi: 10.1016/j.diin.2010.01.05

[4] Johnson, T. & Wallenstein, A. (2011, December 8). Bizzers beware of hack attacks. Symposium conducted at Entertainment Content Protection Summit, Los Angeles.

[5] Koebler, J. (2012). Hackers take on Sony, Microsoft. U.S. News Digital Weekly, 4(9), 7.

[6] Liebowitz, M. (2012, March 30). Your old Xbox could be stealing your credit card. Retrieved June 11, 2012, from MSNBC: http://www.msnbc.msn.com/id/46909290/ns/technology_and_science-security/t/your-old-xbox-could-be-stealing-your-credit-card/

[7] Microsoft. (2012). Get the Most of Xbox with Xbox 101. Retrieved July 3, 2012, from Xbox.com: http://www.xbox.com/en-US/community/xbox101

[8] Microsoft. (2012). Xbox Live Account Security Checklist. Retrieved June 29, 2012, from Xbox.com: http://www.xbox.com/en-US/Live/Account-Security/Security-Checklist

[9] Pottinger, A. (2012, January 12). Xbox Live vulnerability exposed! Microsoft ignored the truth. Retrieved June 6, 2012 from http://analoghype.com

[10] XBOX-HQ.com. (2010). Xbox Homebrew. In EvolutionX. Retrieved June 8, 2012 from http://www.xbox-hq.com/html/modules.php?name=Xbox_Homebrew&op=view&gid=81

[11] XBOX-SCENE. (2012, March). The beginner's guide to XBOX modification (v0.2). Retrieved June 7, 2012 from http://www.xbox-scene.com/articles/beginnersguide.php