Fun & Games: an Introduction to Console Forensics

Peter Hannay
School of Computer and Security Science, Edith Cowan University, Perth, Western Australia, Australia

The scope of functionality provided by video game consoles has been consistently expanding to encompass features that were once limited to general purpose personal computers. This expansion poses a unique and interesting problem for those conducting digital forensic investigations as many of these consoles are resistant to traditional forensic acquisition and analysis techniques. In this paper we explore these issues and some possible solutions in an introduction fashion.

Keywords: *digital forensics, forensics, video game, console, gaming, security*

1 Introduction

As video game consoles with web, communication and general computing features become more common it becomes important to consider the forensic issues that may surround these systems. Many modern consoles include not only web browsers and internet access, but also methods for instant messaging, exchanging emails, photos and videos. This functionality leads to a situation in which the ability to forensically analyze these systems would be quite desirable due to the high potential of misuse for such features.

Existing digital forensics investigation software however is typically aimed at the personal computer platforms. A number software packages are now expanding to encompass a number of mobile devices but none at the time of writing have any support for video game consoles. The cause for this lack of support is primarily due to the security features employed by video game console manufacturers in order to prevent unlicensed distribution of software on these platforms.

2 Security Features

Videogame consoles often make use of advanced security measures in an attempt to prevent the use of unlicensed games on the console in question [1]. these security measures cause numerous issues for the forensic investigation of these devices as they attempt to prevent any access to the data located on the device [2]. Historically video game console manufacturers have not been willing to provide the information required in order to access this data and as such there is a need for this to be developed independently if forensic analysis is to be achieved.

The methods of securing video game consoles against unlicensed distribution are quite standard across many video game consoles. These security methods can be broken into two separate and distinct areas. The first of these is the use of proprietary media for distribution. The second is the use of public key cryptography for signature verification. The methods outlined here are both investigated and possible countermeasures discussed. It should be noted that these two distinct methods of security serve different purposes; the first is intended to prevent pirated media from being used with the console, while the second is intended to prevent unlicensed media from being used with the console.

2.1 Media Security

The majority of games consoles make use of optical media as the primary format for games to be distributed, the exception of this is the Nintendo DS which makes use of proprietary flash memory cards.

In order to prevent un-official or burnt media from being used special firmware exists within the optical drives of these consoles that recognizes illegitimate media and reports it as such to the console itself. The disk verification method is typically based around reading specific identifiers from the disk such as the Media ID and disk type flags, which cannot be recorded using standard CD and DVD burners. This layer of security exists entirely within the optical drive itself and as such is independent from all other security within the console [3].

There are a number of methods that allow media security to be defeated on consoles, the most common of these is a modification of the disk drive itself, either by modifying the software on the device or adding additional hardware [4]. In both cases the goal is to change the message received by the consoles motherboard from “invalid media” to “valid media”. In this way the console is essentially fooled into thinking that the media is legitimate as it trusts the disk drive to accurately make this distinction.

The modification can be accomplished in a number of ways, the modification of the drive can be achieved by reflashing the firmware of the optical drive itself with a compromised firmware, thus controlling the internal operation of the drive. Another common method involves the installation of custom hardware which injects code into the running CPU of the optical drive, thus allowing control over the output of the drive. Newer modifications however sit between the optical

	Wii	Wii (Modified)	PSP	PSP (Modified)	Nintendo DS	Nintendo DS (Modified)	PS3	Xbox360
Games (proprietary media)	✓	✓	✓	✓	✓	✓	✓	✓
Games (DLC)	✓	✓	✓	✓	✗	✗	✓	✓
Hard Disk	✗	✗	✗	✗	✗	✗	✓	✓
Internal Flash	✓	✓	✓	✓	✗	✗	✗	✗
Memory Card Support	✓	✓	✓	✓	✓	✗	✓	✓
USB	✓	✓	✓	✓	✗	✗	✓	✓
WiFi	✓	✓	✓	✓	✓	✓		✗
Ethernet	✗	✗	✗	✗	✗	✗	✓	✓
Web Browser	✓	✓	✓	✓	✓	✓	✓	✗
Image Viewer	✓	✓	✓	✓	✓	✓	✓	✓
Video Playback	✗	✓	✓	✓	✗	✓	✓	✓
Desktop Operating System Available	✗	✓	✗	✓	✗	✓	✓	✗

Table 1 - A comparison of console features

drive and the console motherboard itself, intercepting and modifying communication as desired. This final method is very difficult to prevent as it does not rely on the consoles own hardware. In some complete replacements for these optical drives have been used that allow for software to be loaded without physical media at all.

2.2 Data Security

The validation of code being executed on a console is quite important to console manufacturers as a large portion of their income comes from the licensing of third party games. In most cases these licensing agreements involve a commission on each title being sold for a platform being paid to the consoles manufacturer; it is due to this that console manufacturers are quite concerned with ensuring that only licensed material can be used with their systems.

These licensing restrictions are most commonly achieved through the use of a public key encryption mechanism known as signing. Whilst common data encryption involves encoding data with a public key so that it can only be deciphered with a matching private key, code signing works in much the reverse way. A digest or hash is made of the code and then this code is encrypted with the console manufacturer's private key, so that it can be decoded by any console that has access to the public key. The decoded digest is then compared with the digest of the code to be executed and if there is a match the execution is permitted to take place, this process is illustrated in figure 1.

There are two main methods used in order to bypass this protection mechanism. The first is to make use of vulnerabilities existing within the console operating system or other software that allows the execution of arbitrary code, such exploits are often found within games or other software available for the console [1]. The other method is to replace the operating system on the device with a version that has been specifically modified to allow the execution of unsigned code [5].

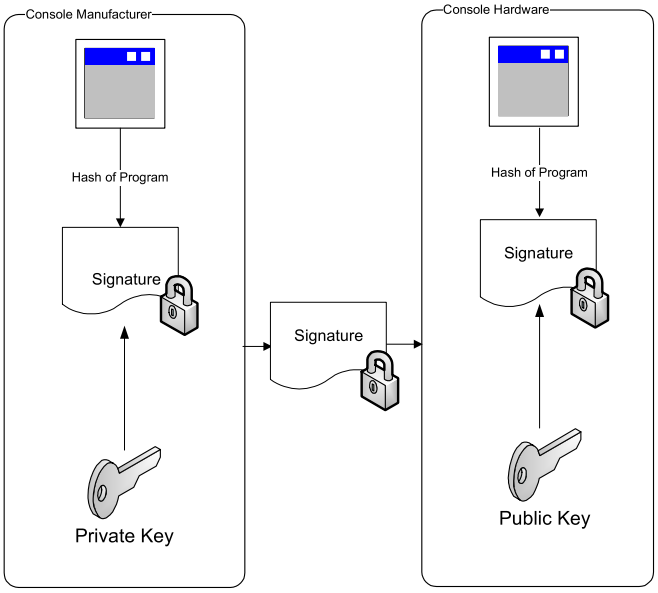

Figure 1 – Illustration of the code signing process

3 Potential Evidence

Given that these devices have a number of features that until recently have been limited to general purpose computers it can be said that there is a wealth of potential evidence available from these devices. This potential evidence is of specific interest due to a number of reasons which will be briefly discussed here.

The security features integral to entertainment console devices are a dual edge sword, whilst they increase the difficulty of forensic acquisition and analysis they also limit the ability of an end user to destroy or modify said evidence. One example of this is that there exists no mechanism to clear the cache or history within the Wii console without erasing the entire contents of the console, which would also lead to the loss of software, save games, addresses books, etc. As such it is quite unlikely that this action would be taken on a regular basis as it would leave the console in a somewhat unusable state.

Potential evidence collected from these consoles could also prove useful in showing that the user was habitual in their criminal behavior, for example possessing illicit images or videos on both a desktop platform as well as a mobile gaming platform may help link the illicit content to a particular user. This is of particular interest as handheld consoles in particular are often personal devices which are not shared with other members of a household, in contrast to desktop computers and the like.

4 Forensic Acquisition

The forensic acquisition of these consoles is severely limited by the aforementioned security features. However the methods discussed to bypass these methods have proven to allow for forensic acquisition and subsequent analysis to take place.

In each instance when it has become possible to run arbitrary code on a console there exists the possibility to create a piece of software that will record a bit stream copy of the data contents of the console in question. In addition to this, depending on the exploit method used, it may be possible to preview forensic information on the console itself prior to acquisition. Of course the feasibility of this technique is also dependant on the capabilities of the individual console in question.

Of course in some cases the traditional method of removing the storage medium and performing external analysis may also be possible, however this is specific to the individual console in question and is not possible in many cases due to the use of encryption on storage media, in some cases this also extends to the use of encryption on internal flash chips [6].

5 Current Findings & Ongoing Research

Current research carried out by the author on a number of consoles has shown that it is possible to perform bit stream acquisition of the data contents of the Wii and PSP consoles without making changes to the internal memory of these devices. In subsequent analysis the following information has been retrieved from both systems:

- Web history
- Saved images
- Saved video (PSP Only)
- Times/dates of device use

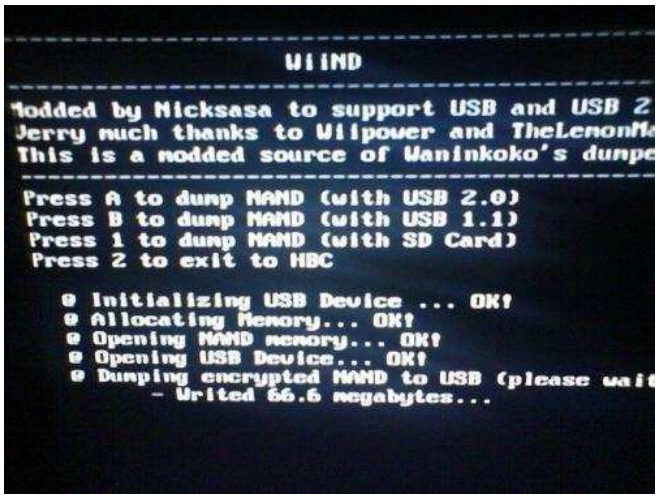

Figure 2 - The use of a custom tool to aquire the Wii console

It should be noted that in all cases this information has been stored in a proprietary and console specific manner. An example of this is that even though the Wii makes use of the opera browser, all web history is stored in a single non-

standard file that bears no resemblance to the storage method used by the desktop version of the Opera web browser. It is due to this that existing forensic software is of limited use even after the acquisition phase is complete. In essence console forensics is in the same state that mobile phone forensics once was, each device must be individually evaluated and reverse engineered in order for analysis to be conducted.

6 Conclusions

Video game consoles have expanded beyond their original scope as devices for playing games. These devices are now central hubs for communication, entertainment and internet access. In essence these devices are bringing the internet and general computing to the lounge room as well as the pocket.

The potential for evidence from these devices has become obvious as usage patterns extend from the desktop, to portable devices, to the lounge room and indeed the workplace. The potential for an overarching pattern of behavior to be established across many devices is reaching critical mass as all these devices become connected to the cloud.

Currently the same security that seeks to ensure profits for the video game console developers is also proving to hinder the ability of forensic examiners to utilize evidence from these devices. However through the use of techniques developed by hackers to allow arbitrary code execution on these platforms it has become possible to acquire data from these devices in an efficient and effective manner. The use and development of these techniques for forensic use is ongoing and appears to be extremely promising.

7 References

[1] Shi, W., et al. Attacks and risk analysis for hardware supported software copy protection systems. 2004: ACM New York, NY, USA.

[2] Turnbull, B., Forensic Investigation of the Nintendo Wii: A First Glance. Small Scale Digital Device Forensics, 2008. **2**(1).

[3] Bushing. The State of the Wii. in 24C3. 2007.

[4] Chetan. technology: How do 1st generation Wii Chips work? 2009 [cited 2009 4th, April]; Available from: http://chetudrives.blogspot.com/2008/02/how-do-1st-generation-wii-chips-work.html.

[5] Huang, A., Keeping secrets in hardware: the Microsoft Xbox (TM) case study. Massachusetts Institute of Technology, Artificial Intelligence Laboratory, Cambridge, MA, Tech Report AIM-2002-008, 2002.

[6] Vaughan, C., Xbox security issues and forensic recovery methodology (utilising Linux). Digital Investigation, 2004. **1**(3): p. 165-172.