Forensic Investigation of the Soft-Modded PlayStation Portable (PSP)

Qin Zhou and Nigel Poole

Faculty of Engineering and Computing, Coventry University
Priory Street, Coventry, CV1 5FB, United Kingdom
{q.zhou,n.poole}@coventry.ac.uk

Abstract. The PlayStation Portable (PSP) is a popular handheld game console. The lack of a hard disk unit within the PSP does not imply a lack of stored data. It incorporates an onboard NAND flash memory and a memory card reader. This paper aims to raise awareness of the presence of custom firmware and identify possible data hiding places in the PSP. It discusses PSP forensics issues and proposes a possible technique for how such a PSP system may be forensically examined.

Keywords: PSP forensics, PlayStation Portable, Custom Firmware, forensic investigation.

1 Introduction

The PlayStation Portable (PSP) is a handheld game console manufactured by Sony Computer Entertainment. It is said that the console is "the most successful non-Nintendo handheld game system ever sold" [1]. Depending on the design version of a PSP system, it incorporates an onboard NAND flash memory offering 32MB or 64MB of storage holding its operating system (also referred to as firmware or system software) and persistent system/user settings like wallpaper or network settings [2]. The content of the onboard memory is hidden from the ordinary users by Sony's official firmware (OFW) but can be accessed with the use of custom firmware (CFW) such as M33 for storing extra data [3]. A reader compatible with Sony's Memory Stick Pro Duo (MS Pro Duo) flash cards is also found on the left edge of the PSP console. A new evolution of PSP, PSPgo is scheduled for release on 1st October, 2009 [4]. PSPgo replaces the UMD drive with 16GB of flash memory to store a variety of content [5].

It is possible to remove the optional extra MS Pro Duo card for external analysis, but the onboard flash memory cannot be easily removed for traditional write-blocked forensic imaging and analysis.

This paper intends to raise the awareness of the availability of CFW and identify places within the PSP memory where data could potentially be hidden. It also discusses PSP forensics issues and proposes a possible solution on how such a PSP system may be forensically examined.

D. Weerasinghe (Ed.): ISDF 2009, LNICST 41, pp. 50–56, 2010.

2 PSP Onboard Flash Memory and Custom Firmware

2.1 Data Storage Areas in the Onboard NAND Flash Memory

According to [6][7], the onboard NAND flash memory of a PSP system (either 32MB or 64MB in size depending on the model of the system) has been divided into three distinct areas: the Initial Program Load (IPL), the IDStorage, and the LFlash (or LFAT). All three areas are encrypted. The LFlash area consists of four FAT12 logical partitions, with Flash0 holding the actual firmware itself, Flash1 containing the system/user settings, Flash2 keeping data required for the PlayStation Network downloads and Flash3 storing extra undefined information. Table 1 shows the LFlash structure of a tested PSP system (Model: PSP2003). The IPL area stores the Initial Program Loader which boots the operating system firmware from the LFlash area. The IDStorage area keeps several hundred system-dependant keys for the PSP system.

Table 1. The LFlash structure of the test PSP system (PSP2003). Here, 1 sector = 512 bytes.

Partition Name	Size in Sectors	Purposes	Used Space	Free Space
Flash0	83936	firmware	24.3MB	16.6MB
Flash1	10208	System / user settings	752KB	4.18MB
Flash2	8160	Data for PlayStation Network downloads	0	3.92MB
Flash3	18656	For downloadable contents?	0	9.04MB

It is worth noting that PSP regularly reads/writes data to Flash1, making an imaging process not repeatable.

2.2 Custom Firmware (CFW)

A PSP system can be soft-modded to run custom firmware (CFW) [8]. CFW such as M33 [3][9] produced by unofficial developers allows users to run third-party software and have full read/write access to the four FAT12 partitions in the LFlash area of the onboard NAND flash memory via the PSP's USB interface. As shown in Table 1, there is typically more than 20MB free space in total available in these partitions which can be used to store extra data. The fact that these partitions can be configured from the Recovery Menu of the CFW such that they are invisible from the PSP's Home Menu makes them the ideal places to hide data. The Home Menu is also referred to as the system menu or the XMB (Cross Media Bar) interface [10].

The test PSP system used in the research was modded using the method of Pandora's battery and magic memory stick described in [3]. M33 CFW was installed on the system.

3 PSP Forensics Issues and Possible Solutions

If a PSP system has not been modded, the examination of the system is simple. An investigator can browse the Home Menu to obtain information about the system, such as system and network settings, web activities, etc.

A MS Pro Duo card found in the PSP system can be easily imaged with the use of a suitable external USB reader and disk imaging tool with a write-blocking mechanism. The fact that a standard FAT32 file system has been used for any memory stick card formatted by the PSP makes the media analysis of stored data straightforward.

Things get more interesting from a forensics point of view if a PSP system has been modded. The following sections explain how such a system may be examined with minimum modification to the system's contents.

3.1 Checking If the System Has Been Modded

First of all, the system information on a PSP system should be checked to decide if the system has been soft-modded. This can be done by navigating to **Settings → System Settings → System Information** from the Home Menu. An original PSP system running OFW should display its system information in the following order:

```
   MAC Address    XX:XX:XX:XX:XX:XX
System Software    Version X.XX (e.g. Version 2.71)
       Nickname    PSP
```

A different presentation order of the system information display suggests that the system has been modded, as illustrated in figure 1. The version of the CFW in the test system was 4.01M33-2.

It is notable that the version of the system software and MAC address can be spoofed by tools like the one in [11] to give false information.

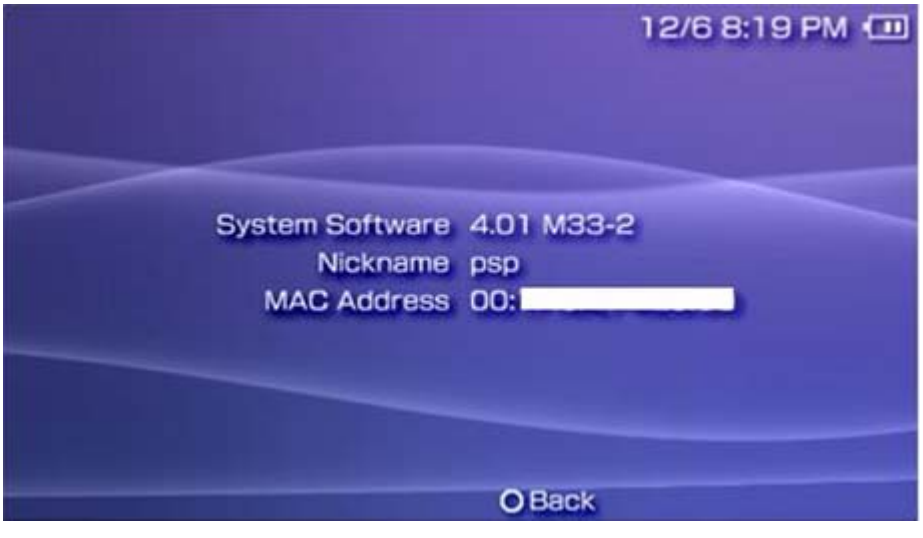

Fig. 1. System information (MAC address deliberately obscured)

3.2 Check If a Custom VSH Menu Is Enabled

If a custom VSH menu [10] such as the M33 VSH menu is enabled, each of the four FAT12 partitions in the LFlash area can be selected as "USB DEVICE" from the menu. Figure 2 shows a device with Flash 3 selected. Once the PSP system is

connected to a PC via the USB connection, the selected flash partition appears as a USB connected memory stick and can be imaged using disk imaging tools such as FTK Imager [12], dd/dcfldd [13], or LinEn [14].

To check if the M33 VSH menu is enabled, one can just press the "SELECT" (or "HOME" in some cases) control to see if an extra menu appears on the screen as illustrated in figure 2.

Fig. 2. M33 VSH menu with Flah3 partition selected for USB connection

If the M33 VSH menu is disabled, the flash partitions can be toggled from the M33 Recovery menu shown in figure 3 and accessed by a PC through the USB interface of the PSP. The M33 Recovery Menu can be accessed by switching off the system, then pressing the "R" control and keeping it pressed while powering on the system.

Fig. 3. M33 Recovery Menu

3.3 Imaging Issues

During the research, an interesting observation was made with regard to flash partition imaging. FTK Imager was found to perform better compared to Linux related imaging tools. FTK Imager only had difficulty in accessing the last sector of each partition during the imaging process while Linux related imaging tools such as dcfldd and LinEn have problems in accessing a number of sectors near the end of each partition. Figure 4 shows 18655 of 18656 sectors were copied successfully by FTK Imager and figure 5 shows only 18640 of them were copied by dcfldd.

```
[Physical Drive Information]
 Drive Model: SONY "PSP" MS USB Device
 Drive Interface Type: USB
 Source data size: 9 MB
 Sector count:    18656

ATTENTION:
The following sector(s) on the source drive could not be read:
        18655
The contents of these sectors were replaced with zeros in the image.

[Computed Hashes]
 MD5 checksum:    e1b3ff5d02ac1954f702d632ca914e8d
 SHA1 checksum:   a55704c52f98ab99b47848e071b5171d653663e0

Image Information:
 Acquisition started:   Mon Jun 15 13:32:19 2009
 Acquisition finished:  Mon Jun 15 13:32:22 2009
 Segment list:
  C:\Q\psp-forensics\psp-flash3-ftk.001

Image Verification Results:
 Verification started:  Mon Jun 15 13:32:22 2009
 Verification finished: Mon Jun 15 13:32:22 2009
 MD5 checksum:    e1b3ff5d02ac1954f702d632ca914e8d : verified
 SHA1 checksum:   a55704c52f98ab99b47848e071b5171d653663e0 : verified
```

Fig. 4. Log file created during imaging of Flash3 by the FTK Imager. It shows 18655 of 18656 sectors were copied successfully.

```
root@masterkey:/# dcfldd bs=512 if=/dev/sdb of=/root/psp/test.dd hash=md5
18432 blocks (9Mb) written.dcfldd:/dev/sdb: Input/output error
Total (md5): 0bd7ebcb31c0f7ad4b2cbb56b7135aeb

18640+0 records in
18640+0 records out
```

Fig. 5. Imaging of Flash3 by dcfldd. 18640 sectors out of 18656 were copied successfully.

The process of imaging the Flash0, Flash2 and Flash3 partitions is repeatable if a suitable write-blocking mechanism is in place. However the process of imaging Flash1 is not repeatable as the PSP's firmware accesses Flash1 on a regular basis to control settings and update logs.

3.4 NAND Flash Dumping

In addition to imaging individual partitions, it is possible to copy the raw data stored in the onboard flash memory to a removable memory stick in a modded PSP system for external analysis or later restoration. This is a valuable technique since it allows recovery from a number of system problems.

The utility Open Source NAND Dumper V.01for 3.xx [15] is an easy-to-use tool for backing up the raw content of the onboard flash memory. The procedure for executing the NAND dump is explained below:

a) Insert a Memory Stick Pro Duo card to the PSP system's card reader and use the system to format the card.
b) Connect the system to a PC through the USB interface, set the system to the USB mode, use the PC to create a folder \PSP\GAME on the memory stick's root directory and store a copy of the program, Open Source NAND Dumper V.01for 3.xx, in the newly created folder.
c) Exit from the USB mode and perform the NAND dump by navigating to Game → Memory Stick from the Home Menu and clicking the icon of the OPEN NAND DUMPER 3.xx to run the utility.
d) After the NAND dump completes, a file named "nand-dump.bin" can be found at the root directory of the memory stick. The file contains the raw content of the onboard flash memory.

3.5 Media Analysis

The easiest way to perform forensic media analysis of the PSP onboard memory is to examine the image files of its four plain logic FAT12 partitions acquired using the above method. Because three of the four logic partitions (Flash0, Flash2, Flash3) in the LFlash area of the flash memory have been encrypted and analysis of the raw NAND dump data proves to be difficult - it involves extracting the LFlash area, separating the four partitions and decrypting the three encrypted partitions.

4 Conclusions

The main data items of forensic interest within a PSP device reside in its internal flash memory or Memory Stick Pro Duo expansion memory. The memory Stick Pro Duo can be easily removed and attached to a separate PC equipped with a compatible card reader for analysis. The internal flash memory is not normally accessible for detailed analysis from devices running official firmware. Use of custom firmware will allow direct read and write access to this memory space if required. Areas within the flash memory would then become available for hiding sensitive data.

Techniques for identifying the presence of custom firmware on a PSP device, imaging its flash memory partitions and taking a raw dump of the memory have been presented. The underlying structure and function of the flash memory partitions has been described. Combined with conventional forensic analysis tools this enables a detailed examination of a device that potentially holds relevant evidence to be undertaken. Further work could usefully be directed to deducing the detailed structure of the flash memory partitions.

References

1. Matthews, M.: Opinion: What Will The PSP Do In 2009? Gamasutra, http://www.gamasutra.com/php-bin/news_index.php?story=21332
2. Cory1492, 64MB Nand, LAN.ST, http://www.lan.st/showthread.php?t=1435&page=3
3. Devilfish: Intro to Pandora, Custom Firmware & Homebrew Software for PSP. Digital Kaos, http://www.digital-kaos.co.uk/forums/f63/intro-pandora-custom-firmware-homebrew-software-psp-24168/
4. Miller, P.: Engadget & Joystiq live from Sony's E3 2009 keynote. Engadget, http://www.engadget.com/2009/06/02/engadget-and-joystiq-live-from-sonys-e3-2009-keynote/
5. PSP has evolved. Official PlayStation website, http://uk.playstation.com/games-media/news/articles/detail/item160412/PSP-has-evolved/
6. Cory1492, 64MB Nand, LAN.ST, http://www.lan.st/showthread.php?t=1435&page=3
7. Dax Hordes: [TUT]Nand Dumps and Nand Basics[/3r14nd]. Dark-Alex.org, http://www.dark-alex.org/forum/viewtopic.php?f=80&t=1327
8. Softmod. Wikipedia, http://en.wikipedia.org/wiki/Softmod
9. Larrylje: GUIDE: Create Pandora Battery + Magic Memory Stick Using Official/1.50/CFW PSP. Afterdawn.com, http://forums.afterdawn.com/thread_view.cfm/708959
10. Homebrew Jargon Buster. PSP Homebrew, http://www.psp-homebrew.eu/faq/jargon.php#XMB
11. Davee: Unlimited Character Version and Mac Address Spoofer. Davee's DavSite, http://davee.x-fusion.co.uk/
12. FTK Imager, AccessData, http://www.accessdata.com/
13. dcfldd, http://dcfldd.sourceforge.net/
14. LinEn, Guidance Software, http://www.digitalintelligence.com/software/guidancesoftware/encase/
15. Open Source PSP NAND Dumper v0.1, http://www.psp-hacks.com/file/1313