PWN Xerox Printers (…again)

About Hardware Attacks and (In-) Secure Cloning

Fraunhofer FKIE
Peter Weidenbach, Raphael Ernst

Abstract

Network printers are a worthwhile target for attackers, because they process sensitive information (all your prints) and they are connected to your (trusted) internal network. In this paper we demonstrate how easy it actually is to manipulate a printer. We show two attacks that lead to a remote root-level access to the printer. Since our example printer runs an ordinary Linux system, you can use all these powerful tools that you already have, to do whatever you want to do. Both attacks run on all firmware versions of our printer including its most recent version of January 2016.

1. Introduction

Nowadays network printers can be found in every company. These printers are often used to print sensitive business related data. Sometimes these printers are used to print confidential files as well. In addition these devices are connected to the company's network. To be more precise, most likely printers are part of the "trusted" company's internal network. These facts make printers a worthwhile target for attackers. Two scenarios shall show the obvious security threat:

1) Each print is cached in the memory of the printer for several minutes. Sometimes it is also cached on an internal hard disk. An attacker with access to the printer can steal these prints and all the sensitive information on it.

2) The printer is connected to company's internal networks. So it might attack servers and client PCs in several ways. For example it could explore unprotected file shares, crawl the intranet for interesting data, or start denial of service (DoS) attacks on network services.

In 2012 an exploit [1] was added to Metasploit utilizing the firmware update mechanism to run arbitrary code with root privileges on Xerox Multi-function Printers (MFP). Heiland [2], the author of the exploit, described the attack and the vulnerability in a whitepaper one year later. He reversed the firmware update container and its creation process including the firmware signature creation method. With this knowledge in hand he was able to install a remote shell by creating a firmware update file. Nevertheless, Heiland demonstrated his proof of concept on an out of live product. In addition he states that Xerox was going to harden the update process and its firmware.
In this paper we demonstrate two attacks on a recent Xerox network printer. Both attacks lead to root privileged remote access and show that the printer has severe security weaknesses allowing local and remote attacks.

The rest of this paper is structured as follows. In Section two we describe how we analyzed the firmware and which information we got from it. The third section describes our malicious payload that is going to be installed on the printer. Section four describes how to drop the malicious functionality by attacking the hardware. Afterwards we describe how to remotely install the exploit in section five. Section six deals with minor changes necessary to run our remote exploit on different firmware versions. This section includes a HOWTO find and install recent firmware versions of Xerox printers as well. Section seven deals with related work and section eight provides a conclusion.

2. Analyzing Xerox Printer's Firmware

We used our Firmware Analysis Framework (FAF) to analyze the Firmware update container of a Xerox Phaser 6700 [3] color laser network printer. The Phaser 6700 provides an Ethernet and a USB interface. A Wireless LAN USB adapter is optionally available as well. The printer can be configured via touchscreen or web interface. Username password authentication is available to secure the configuration. Additionally several security features are available: SSLv3, IPsec, 802.1X Authentication, HTTPS, IPPS, SMTP Authentication, SNMPv3, IP Filtering, 256-bit encryption, Image Overwrite, FIPS 140-2.

The analysis shows that the Phaser 6700 is powered by a Wind River Linux probably version 1.4. Beside others, we identified the following software components:

- Apache Web-Server
- Glibc 2.3.6
- OpenSSH 4.3
- OpenSSL 0.9.8
- PHP 5.3.10
- Samba 3.0.37
- WPA Supplicant 0.6.8

Further manual analysis showed that the OpenSSH server is disabled in the xinetd system. We also found a shadow file including the hashed root password.

3. Proof of Concept Attack

As seen in our firmware analysis a SSH server is already installed. Therefore, it should be easy to activate the SSH server and provide a root login. To accomplish this goal three files must be manipulated:

- /etc/xinetd.conf -> activate SSH-Server on startup
- /etc/ssh/sshd.conf -> allow root login[1]
- /etc/shadow -> overwrite or delete root password

After a reboot we should be able to connect to the printer via SSH as root.

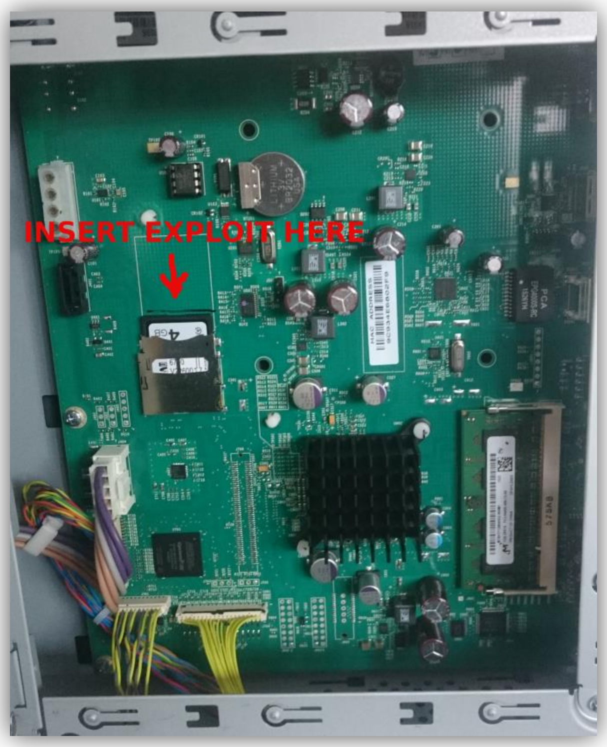
4. The Easy Local Way – Attacking the Hardware

The printer's firmware is stored on and executed from an SD-card. This card can be accessed and replaced via an opening for maintenance at the backside of the printer. The card provides three partitions: An ext3 boot partition, an ext3 Linux root file system and a partition with an u-boot boot-loader.

[1] Login without password is allowed by default on our printer ;-)

Our attack works as follows:

1. Switch off printer
2. Open maintenance opening on the backside and remove SD-card
3. Modify files on SD-card as described in section 3
4. Put the SD-card in the printer again and switch on the printer
5. Close maintenance opening.



The whole attack can be done in less than 5 minutes including the 3 minutes boot process of the printer.

There is no need for tools, because the opening for maintenance is secured with knurled screws. The manipulation of the SD-card can be done with any device capable of mounting an ext3 filesystem and providing a text-editor. This means, you could do it with your android powered smartphone. Therefore, anyone alone with the printer for a few minutes could manipulate it. This may be any employee, cleaning personal, or even a guest.

5. The Easy Remote Way - Exploiting the Cloning Functionality

Heiland [2] described how to exploit the firmware upgrade feature of Xerox printers. He also mentioned that his attack might not work in the future, because Xerox was going to remove the private keys to sign firmware upgrades from the printer's firmware[1].

Therefore, we looked for another feature that is not going to be removed in the future. Cloning is a feature Xerox's printers provide to easily copy the configuration of one printer to another.

In this section we describe the cloning process of the most recent printer firmware on the support website [4]. This is version 081.140.103.22600 of August 2013. In section six we describe minor changes to be done to run the exploit on recent (hard to find) versions of the firmware.

The clone files can be generated in the web interface of the printer. We created a clone file and analyzed its structure with FAF.

The clone file consists of a DLM-Header and a tar.gz archive. The structure of the header is equal to the header of Xerox's firmware upgrade- and patch-file's headers as described by Heiland [2]. The tar.gz archive includes a cloning.sh file and a data folder with several other files. A look at the cloning.sh file provided all information to

[1] By the way, the Metasploit exploit is still running on the newest firmware that is available on the support website [4] of our recent Xerox printer: It is not running on recent versions of the firmware of our printer, which are quite well hidden on the website. We will come to that later.

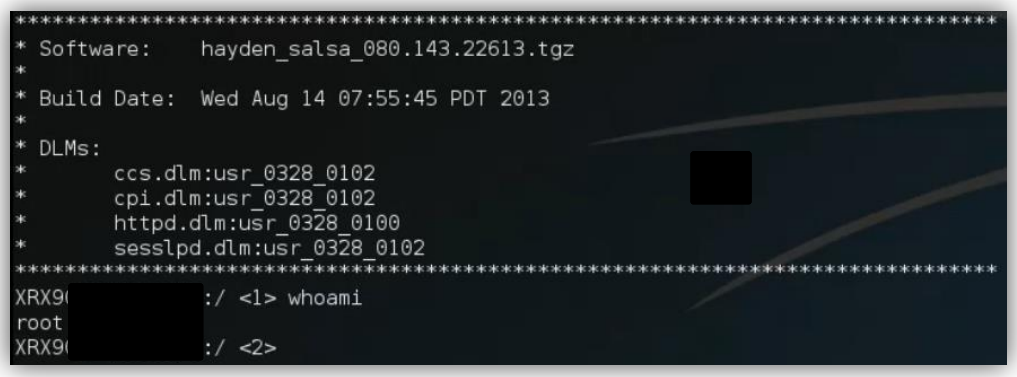
understand the cloning process. Obviously the tar.gz file is extracted to a predefined path in the firmware root file system. Afterwards the cloning.sh is executed. The cloning.sh includes several file copy operations and finally reboots the printer. This information combined with Heiland's information about the dlm-toolkit are sufficient to drop our malicious payload remotely.

In general it seems that the cloning feature works the same way as the upgrade and patch features. Thus, we probably exploit the same vulnerability as Heiland did but with another feature.

Our attack works as follows. We created a clone file and extracted its tar.gz file. Afterwards we added our three exploit files as described in section 3 to the archive and added 3 lines to the cloning.sh that overwrite the corresponding original files of the firmware with our files.

Finally we used the dlm-maker preinstalled on our Xerox printer to create a DLM cloning file with a valid signature.

Installing the clone is very simple. You could either upload the clone file via web-interface, which may require authentication or you send the file unauthenticated to the jetdirect port.

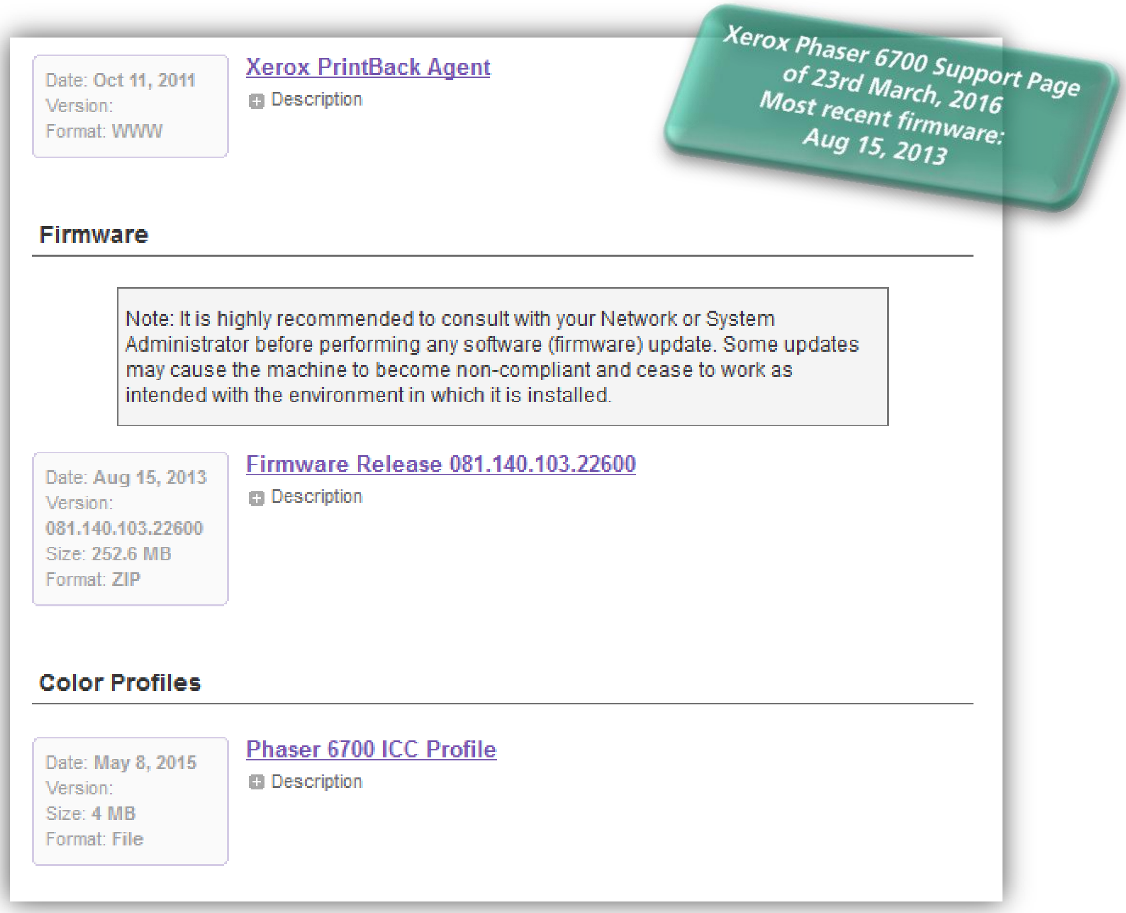


```
********************************************************************************
* Software:    hayden_salsa_080.143.22613.tgz
*
* Build Date:  Wed Aug 14 07:55:45 PDT 2013
*
* DLMs:
*        ccs.dlm:usr_0328_0102                [redacted]
*        cpi.dlm:usr_0328_0102
*        httpd.dlm:usr_0328_0100
*        sesslpd.dlm:usr_0328_0102
********************************************************************************
XRX9[redacted]:/ <1> whoami
root
XRX9          :/ <2>
```

This attack can be prevented by disabling the update feature in the printer's web interface. If disabled neither firmware updates nor cloning files are executed. This procedure is recommended in Xerox's Security Bulletin [5] regarding Heiland's attack. Unfortunately, this bulletin is not listed on the "Phaser 6700 Security Information" site [6]. Maybe Xerox thinks that this device is not vulnerable, because you are able to disable the update process. *Thus, you could hinder the attack known for 4 years, but you are not informed about it.*

6. Dealing with Different Firmware Versions

As mentioned before the firmware version on the printer's support site is quite old. Hints to more recent versions of the firmware can be found on the "Security Information" website of our printer. There you can find several security bulletins as PDF files. In these PDF files you can find links to the more recent versions of the printer's firmware. Unfortunately you are not able to install them, because Xerox changed its update procedure with a firmware released in June 2014. This information can be found by studying the firmware update information of the recent firmware files. With this information in hand, you can search for the firmware of June 2014 and install that one, before you can install the most recent versions of the firmware. Afterwards you contact Xerox personally and they tell you, that they have hidden an even newer firmware version somewhere on their server. So after searching, asking and failing a couple of times you may end up with a printer running the most recent firmware version.



Xerox Phaser 6700 Support Page of 23rd March, 2016 Most recent firmware: Aug 15, 2013

Date: Oct 11, 2011
Version:
Format: WWW

Xerox PrintBack Agent

⊞ Description

Firmware

Note: It is highly recommended to consult with your Network or System Administrator before performing any software (firmware) update. Some updates may cause the machine to become non-compliant and cease to work as intended with the environment in which it is installed.

Date: Aug 15, 2013
Version: 081.140.103.22600
Size: 252.6 MB
Format: ZIP

Firmware Release 081.140.103.22600

⊞ Description

Color Profiles

Date: May 8, 2015
Version:
Size: 4 MB
Format: File

Phaser 6700 ICC Profile

⊞ Description

It follows some notes on the different firmware versions and what to change on our clone exploit to get it running on these particular versions. By the way, the hardware attack is running the same way on all versions.

Firmware Version 081.140.104.17600 of June 2014

Xerox changed its signing mechanism for clone files and updates. This stopped the Metasploit exploit of Heiland [1]. Our exploit is not affected. We just had to generate a new signature with the dlm_toolkit preinstalled on our printer.

Firmware Version 081.140.105.00700 of January 2015 (Introducing Really New Security Issues)

In this version Xerox introduced "secure cloning". They disabled the possibility to process clone files on the jetdirect port. Additionally they added a feature to disable clone imports explicitly. They changed the format of the clone files as well. There is no longer a bash script executed during the cloning process but configuration files that are parsed by tools preinstalled on the printer. Furthermore they changed the extraction path of the tar.gz archive.

So we needed a new entry point and found the CloningManifest.xml. This file is part of the new clone file format. Beside others it defines the paths of the configuration files that are processed by external tools installed on the printer. So a ***simple shell injection*** does the trick to run our clone exploit again.

Now you may say: "OK… but it is really hard to exploit, because you need the admin credentials for the web interface to upload the clone file." Actually you do not need

these credentials, because ***the upload site does not check if you are logged in***. So just prepare a HTTP POST message including your malicious clone file and send it to the upload page directly.
Nevertheless, deactivating the cloning feature prevents this attack.[1]

Firmware Version 081.140.105.20400 of July 2015
The cloning process did not change from version 2015-01. Therefore no further changes are needed to run the exploit.

Firmware Version 081.140.106.01300 of January 2016 (We did not find that our self. Xerox gave it to us)
Exploit is still working.

7. Related Work

In 2013 Heiland [2] published a whitepaper explaining how to exploit the update process of Xerox's Multi-function Printers (MFP). The author reversed the firmware update container and its creation process including the firmware signature creation method. With this knowledge in hand he was able to install a remote shell by creating an own firmware update file. Nevertheless Heiland demonstrated his proof of concept on an out of live product.
In the same year Cui et al [7] presented a similar vulnerability found in HP's Remote Firmware Update functionality. They were able to install malicious firmware updates via print jobs to HP printers.
In 2011 Costin [8] presented a Proof-of-Concept demonstrating malware implemented in postscript. These malicious scripts could be sent as normal print jobs and were executed on the printer. Besides others he showed that information can be stolen from memory via postscript.

8. Conclusion

We demonstrated two attacks on a still in sale Xerox network printer. A hardware based attack, in which we manipulated the firmware storage media itself, and a remote attack exploiting the printer's cloning functionality. Both attacks led to a remote shell with root privileges. At the moment we cannot estimate how many printers are vulnerable to the hardware attack. This attack cannot be prevented in software by now. Nonetheless all Xerox printers that support DLM update and clone packets, are probably vulnerable to the remote attack. The remote attack can be hindered by deactivating the upgrade functionality respectively the clone functionality of the printer. Nevertheless we showed that the security of printers has not evolved much since earlier attacks presented years ago.
In summary even today's network printers can be hijacked with very low effort. On the other hand a hijacked printer gives an attacker a lot of power. He can steal prints, launch DoS attacks or attack the company's internal network by other means.

9. Acknowledgement

This research was supported by German Federal Office for Information Security (BSI).

[1] By the way, we tried to enable the clone feature without authentication as well.
Fortunately it did not work.

Literature

[1] Rapid 7, "Xerox Multifunction Printers (MFP) "Patch" DLM Vulnerability," 7th March 2012. [Online]. Available: https://www.rapid7.com/db/modules/exploit/unix/misc/xerox_mfp. [Accessed 17th March 2016].

[2] D. Heiland, "From Patched to Pwned," 21st February 2013. [Online]. Available: http://h.foofus.net/~percX/Xerox_hack.pdf. [Accessed 9th March 2016].

[3] Xerox Corporation, "Xerox Phaser 6700," [Online]. Available: http://www.office.xerox.com/printers/color-printers/phaser-6700/enus.html. [Accessed 10th March 2016].

[4] Xerox, "Phaser 6700 Support & Drivers," [Online]. Available: http://www.support.xerox.com/support/phaser-6700/downloads/enus.html?operatingSystem=win7x64&fileLanguage=en_GB. [Accessed 23rd March 2016].

[5] Xerox, "Xerox Security Bulletin XRX12-003 Address Postscript and DLM Vulnerabilities," 7th March 2012. [Online]. Available: http://www.xerox.com/download/security/security-bulletin/1284332-2ddc5-4baa79b70ac40/cert_XRX12-003_v1.1.pdf. [Accessed 12th March 2016].

[6] Xerox, "Phaser 6700 Security Information," 2016. [Online]. Available: http://www.office.xerox.com/printers/color-printers/phaser-6700/secu-enus.html. [Accessed 18th March 2016].

[7] A. Cui, M. Costello and S. J. Stolfo, "When Firmware Modifications Attack:," in *20th Annual Network &*, Sand Diego, Californien, USA, Internet Society, 2013.

[8] A. Costin, "Hacking MFPs," in *28th Chaos Communication Congress*, Berlin, Deutschland, Chaos Computerclub e.V., 2011.