An Artifact from the Past:

The Privacy Vulnerabilities of Network Printers

Josh Simani

COMP116 Final Project

December 13, 2019

I. Abstract

When personal inkjet and laser printers were first made popular in the late 20th century, security was the last thing on the minds of their inventors. As a result, there are now many possible security risks involving today's printers, specifically network printers. Among other things, inherent security risks include malicious parties listening for the files that are sent to printers, which could involve highly sensitive data; hijacking community printers to install a backdoor or virus; and gaining access to a pay-per-page printer to access the printer's functionality without having to pay for it. To explore these risks, I will research the protocols used for printing on most systems, and the possible vulnerabilities that are currently exploitable from these printers. I will be using some of the Tufts University printers as examples.

II. Introduction

Ten to fifteen years ago, printers were used as a means for distributing important documents for just about every official purpose. As email and electronic documents were ushered into normality, many practical uses for physical documents made their transition to the electronic world; however, the use of physical documents is still common practice within the medical and legal fields for extremely sensitive data.

Considering the fact that most personal information is distributed physically between authorized parties (i.e., court documents, medical bills, prescriptions), it would make sense that those parties would take appropriate measures to secure such documents. Unfortunately, that is not always the case; often, the printers used to print this sensitive information are left unprotected and vulnerable to exploitation and attacks from outside sources.

In this paper, I will be exploring the methodologies behind feasible attacks on network printers, and the possible implications of such attacks. I will also offer possible remedies for the vulnerabilities related to network printers.

III. To the Community

I chose this topic to show that something used every day, before the vulnerable IoT devices even came into existence, can also be open to attack and could potentially violate the privacy of people across the country. Printer vulnerabilities are important to recognize because a large portion of people working throughout this country rely on printers for distributing documents containing personal information. If these people have the printer connected to an insecure network, the information they are printing could be vulnerable to attacks.

IV. Printing Languages

There are three main printing languages used to communicate with printers. All three languages are exploitable and can be used to perform various attacks on printers.

The first of the three is PostScript (PS). PostScript is a printing language invented by Adobe Systems between 1982 and 1984. Many of its printing specification features have since been replaced by the PDF standard since its invention, but it is still widely used for sending the page descriptions to laser printers. Since PostScript is a Turing-complete language, being able to gain access to a PostScript interpreter within a printer can be classified as "code execution" vulnerability.[1] An article from *The Register*, an online tech publication, implores its readers to take their printers off of the internet, due to vulnerable PS commands that have existed for over three decades since the time of publication. It details that that possible risks from the language

[1] "PostScript."

include "attackers exfiltrating copies of what is sent to printers, to denial-of-service, code execution, forced resets and even bricking the targets."[2] Indeed most of these attacks were reproducible on Tufts University printers when attempted.

The second common printing language is the Printer Job Language (PJL). PJL was invented by Hewlett-Packard in the early 1980s, and it has since become the standard for printer job control among many different types of printers.[3] It was created in order to give developers "the ability to programmatically switch printer languages, monitor printer status, request the printer model and configuration, change control panel default settings, modify control panel messages, and more."[4] In fact, all of these attacks, and more, were accomplished on Tufts University printers.

The last of the three common printing languages is the Printer Command Language (PCL). Hewlett-Packard introduced this language in 1984 to "provide an economical and efficient way for application programs to control a range of printer features across a number of printing devices."[5] The main purpose of PCL is to define fonts and macros for printing, but due to its limited capabilities, it is somewhat hard to exploit.[6] The main vulnerability discovered from this language was the ability to create a virtual file system, which can be used for file sharing purposes, something that is also reproducible on Tufts University printers.

V. Exploiting Network Printers

These languages are not very useful without a means of communicating with network printers. TCP/IP sockets are needed in order to send these commands to network printers. To

---

[2] Chirgwin, "We Don't Want to Alarm You, but PostScript Makes Your Printer an Attack Vector."
[3] "PJL."
[4] *Printer Job Language Technical Reference Manual*, iii.
[5] *Printer Control Language Technical Reference Manual,* 1-1.
[6] Müller, "Exploiting Network Printers," 8.

facilitate this process, a team at Ruhr-Universität Bochum created a Printer Exploitation Toolkit (PRET) in Python that can inject PS, PJL, and PCL commands to network printers using predefined macros.

Using PRET, when connected to the laser printer in room 118 of Halligan Hall, which is connected to an unsecured network, a malicious user can perform 57 various attacks at the command prompt using PostScript commands,[7] 50 attacks using PJL commands,[8] and 20 attacks using PCL commands.[9] The most notable of these commands are listed below.

Language	Attack	Description
PS	`destroy`	Causes physical damage to the printer's NVRAM by exceeding the guaranteed sustainability of 100,000 flash memory rewrites before any write errors may occur.[10]
PS	`disable`	Allows an attacker to perform a denial of service attack on the printer by entering it into an infinite loop so that it cannot accept new print jobs.
PJL	`display`	Allows an attacker to change the message displayed on the home screen of the printer.[11]
PJL	`env`	Displays all environment variables stored in the operating system of the printer, possibly revealing sensitive information.
PJL	`flood`	Allows an attacker to flood user input on the printer, which may reveal buffer overflows and can cause erroneous messages to be displayed on the home screen of the device.[12]
PJL	`fuzz`	Allows an attacker to perform file system fuzzing, either with path traversal strategies, by putting/appending a file and checking for its existence, or by performing read-only tests for existing files like `/etc/passwd`.
PJL	`offline`	Allows an attacker to take the printer offline and display an error message. This can be used to trick others into thinking that the printer has a paper jam or is out of ink, prompting unnecessary expenses of time and money to "repair" the issue.

[7] See Figure 1.1
[8] See Figure 2.1
[9] See Figure 3.1
[10] Ibid., 17.
[11] See Figure 2.2
[12] See Figure 2.3

PCL	`put`	Allows an attacker to send a file to be stored on a virtual file system. This attack could be used to hijack the printer's memory and use it for file sharing purposes.
PS, PJL, PCL	`print`	Allows an attacker to send a file or ASCII text to the device for printing, possibly bypassing any instituted paywalls necessary to print.
PS, PJL	`reset`	Allows an attacker to manually reset a printer to its factory default settings, allowing possible privilege escalation by removing previously instituted permission checks.
PS, PJL	`restart`	Allows an attacker to manually restart the printer.
PS	`shell`	Allows an attacker to open an interactive PostScript shell, enabling him or her to perform any command conceivable at the time of the attack.

VI. Defenses

The vulnerabilities that are exploitable using PRET carry serious implications. A first step towards preventing these exploitations is to make sure that the printer's firmware is updated regularly so that it is protected against common vulnerabilities that have been previously found and patched. The next ideal step is to simply take the printer offline and only allow it to connect to a device via physical connection. Of course, that is often not a feasible solution for users, so an alternative is to connect the printer to a secure network that is inaccessible to the public. Currently, the printers in Halligan Hall at Tufts University are connected to an unsecured network named "EECS," which does not require a password to join. Simply connecting your printers to a network that requires a password makes it so that unauthorized users cannot establish a connection to the printer to engage in malicious attacks. In addition, turning off the printer when it is not in use would prevent attackers from gaining access at times when the printer is otherwise not being monitored.

The next solution is far more complex and time-consuming, but eliminates the need to restrict current users' abilities to print. Implementing some sort of access control, in which the

printer only accepts requests from a specified set of IP addresses, would eliminate the possibility of attackers connecting directly to the printer. Currently, most printers at Tufts University utilize this method of access control so that it is harder to bypass their paywalls for printing. Doing this, however, may not be an option if certain computers are required to be open to the public.

VII. Conclusion

Since the introduction of laser printers, security features were never a large consideration. Many printers still use the antiquated techniques that were conceived over 30 years ago. With the three standardized printing languages, PS, PJL, and PCL, dozens of the possible attacks outlined could be reproduced by readers with some technical knowledge. The implications of these vulnerabilities are immense and rather unsettling. In recent years, while some have used these vulnerabilities for some rather harmless stunts like printing messages telling people to subscribe to a popular YouTube channel,[13] others have taken advantage of this field of weaknesses with rather malicious intentions. In 2016, a self-described white nationalist "hacktivist" sent anti-semitic and racist fliers containing hate speech and swastikas to printers across the country that were publicly accessible. A notable amount of such printers belonged to colleges and universities.[14]

Unauthorized printing of fliers is a problem, but if attackers are able to do more, like bypassing paywalls or holding printers ransom through denial of service, it could cost companies tens of thousands of dollars in damages. Though printers may appear to be simple machines, they should be given the attention needed to mitigate serious security-related weaknesses.

---

[13] Hernandez, "Someone Hacked Printers Worldwide, Urging People to Subscribe to PewDiePie."
[14] JTA, "White Supremacist Claims Swastika Printing Hack at US Colleges."

VIII. Proof of Concept / Image Appendix

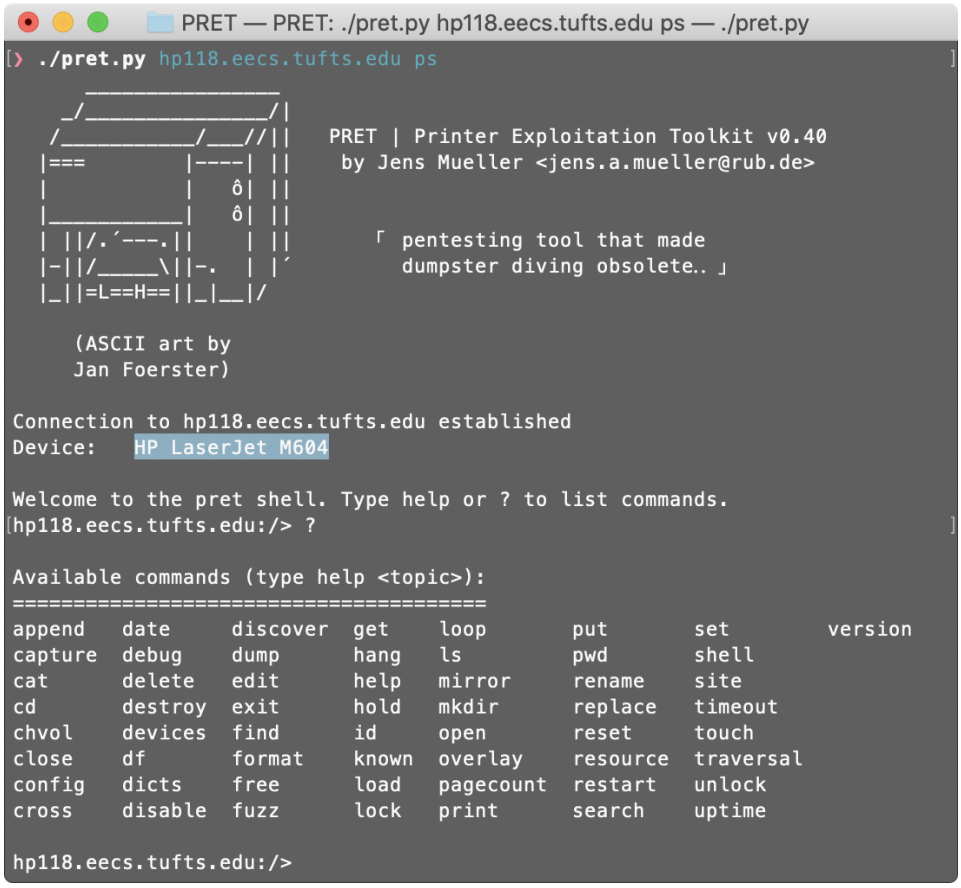

Figure 1.1. A console window running PRET on an HP LaserJet M604 in Halligan Hall using PostScript as a medium for injecting printer commands.

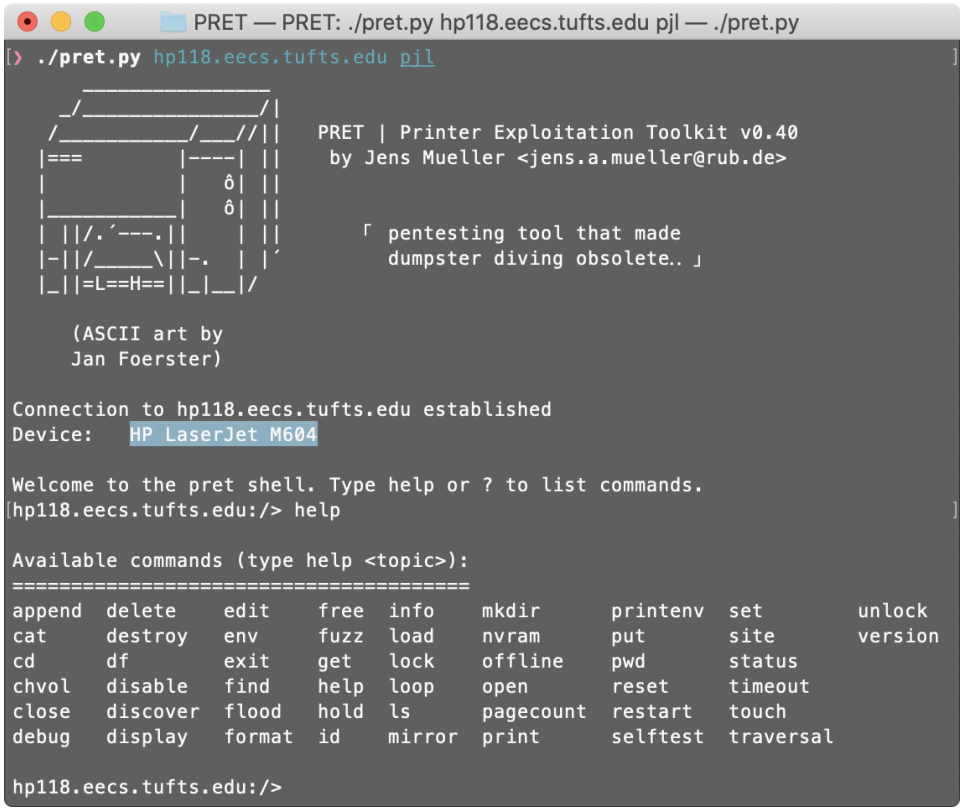

Figure 2.1. A console window running PRET on an HP LaserJet M604 in Halligan Hall using PJL as a medium for injecting printer commands.

Figure 2.2. A snapshot of the printer's display after running the `display` macro in PJL mode in PRET to change the printer's home screen dialog.

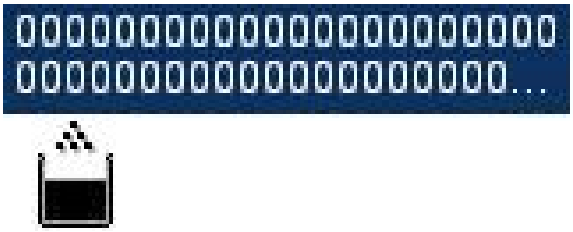

Figure 2.3. A snapshot of the printer's display after running the `flood` macro in PJL mode in PRET to flood user input on the printer.

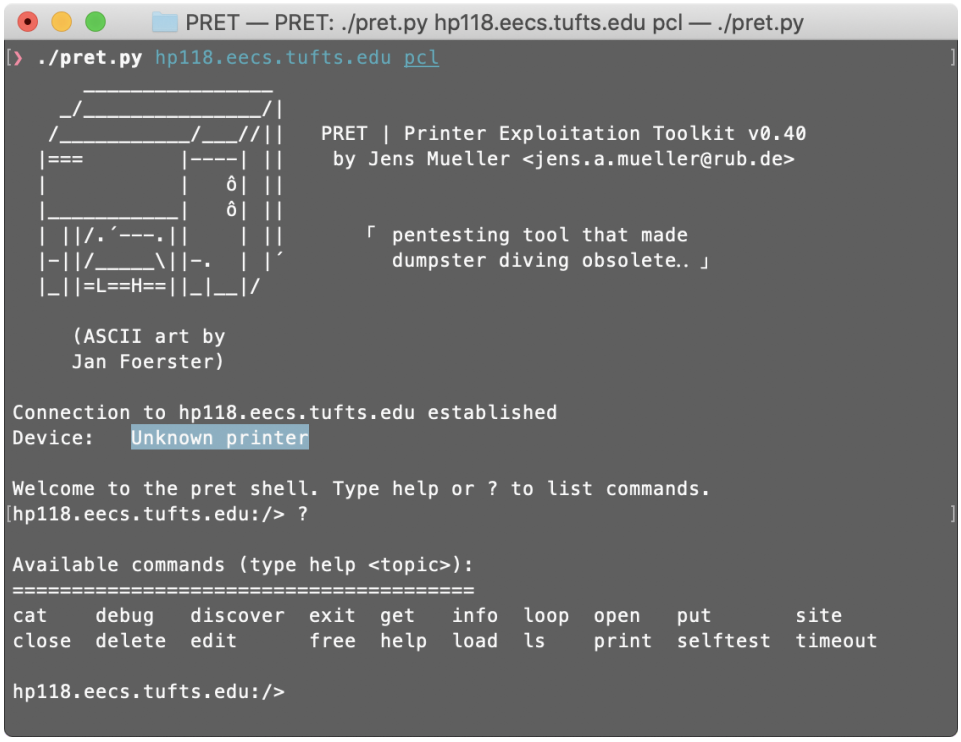

Figure 3.1. A console window running PRET on an HP LaserJet M604 in Halligan Hall using PJL as a medium for injecting printer commands.

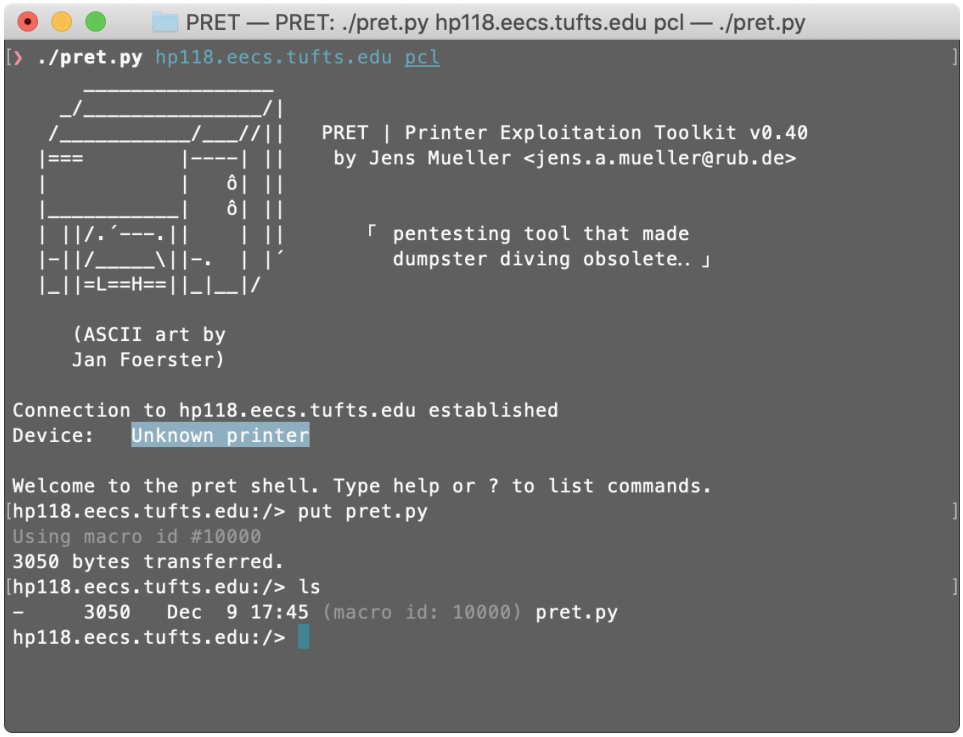

Figure 3.2. A console window running PRET on an HP LaserJet M604 in Halligan Hall using PJL as a medium for injecting printer commands, showing the contents of the printer's virtual file system after running `put` to upload a file to it.

IX. Works Cited

Chirgwin, Richard. "We Don't Want to Alarm You, but PostScript Makes Your Printer an Attack Vector." *The Register*. January 31, 2017. https://www.theregister.co.uk/2017/01/31/postscript_bug/.

Hernandez, Patricia. "Someone Hacked Printers Worldwide, Urging People to Subscribe to PewDiePie." *The Verge*, November 30, 2018. https://www.theverge.com/2018/11/30/18119576/pewdiepie-printer-hack-t-series-youtube.

JTA. "White Supremacist Claims Swastika Printing Hack at US Colleges." *The Times of Israel*, March 30, 2016.

Müller, Jens. "Exploiting Network Printers: A Survey of Security Flaws in Laser Printers and Multi-Function Devices." Ruhr-Universität Bochum, 2016. https://www.nds.ruhr-uni-bochum.de/media/ei/arbeiten/2017/01/30/exploiting-printers.pdf.

Hacking Printers. "PCL." Wiki, January 31, 2017. http://hacking-printers.net/wiki/index.php/PCL.

Hacking Printers. "PJL." Wiki, June 6, 2017. http://hacking-printers.net/wiki/index.php/PJL.

Hacking Printers. "PostScript." Wiki, January 31, 2017. http://hacking-printers.net/wiki/index.php/PostScript.

Printer Control Language Technical Reference Manual. HP Inc., 1992. http://www.hp.com/ctg/Manual/bpl13210.pdf.

Printer Job Language Technical Reference Manual. HP Inc., 1997. http://h10032.www1.hp.com/ctg/Manual/bpl13208.pdf.