Hacking Printers: MIT's Printers Security Analysis

Kritkorn Karntikoon
kritkorn@mit.edu

Cattalyya Nuengsigkapian
cattalyy@mit.edu

Korrawat Pruegsanusak
korrawat@mit.edu

Suchan Vivatsethachai
suchanv@mit.edu

May 16, 2018

Contents

1 Introduction

As MIT students, we print documents almost everyday. With MIT's printers, we print everything from problem sets to lecture notes and even confidential document. But precisely because printing on campus has become very quick and convenient, most of us have not even questioned about the security of MIT printing system. In fact, any of us could immediately perform a simple attack. To print a document, one simply sends it to MIT server printer and fills in a Kerberos name. As a result, an attacker could just order a spam document to any Kerberos they want.

Such attacks in the past motivate us to research into the security of MIT printer and network printer system in general. We have performed a number of attacks on MIT printers, including unlimited printing, document modification, Denial of Service (DoS), and many other possible attacks. Most of the attacks were executed on an MIT printer in MIT IS&T building W92. Some of the attacks apply to every MIT printer, while other attacks can only be performed with only some MIT printers that meet the criteria.

Outline. The remainder of this paper is structured as follow: In Section 2, we provide a basic background of a network printer system and an MIT printer system, which are stepping stones of our attacks and security analysis. In Section 3, we discuss a security analysis of MIT printing system. In Section 4, we describe all of the attacks that we successfully performed. In Section 5, we describe other potential attempts we believe could be performed on MIT printers. Lastly, in Section 6, we give security recommendations that could help prevent some, if not all, of our attacks.

2 Background

In this section, we discuss some important background of network printer system and more details specific to MIT printing system, which will be relevant to further discussion in later sections.

2.1 Network Printer System

Network printing consists of three main layers: Page Description Languages, Printer Control Languages, and Printer Connection Protocols.

2.1.1 Page Description Languages

All documents sent to the printer are translated with a printer driver into one of the page description languages (PDL). Each printer uses different PDLs to determine the appearance of the actual document, and some printers may have different printer drivers to handle more than one PDL. The most common PDLs are PostScript (PS), Portable Document Format (PDF), and Printer Command Language (PCL).

The PDL that is most relevant to our attacks is **PostScript (PS)**, a Turing complete language that has much more capabilities than PDF. Some of our attacks created PS files and planted them in an MIT printer to modify future printed documents on that printer, while leaving the original digital file intact.

Portable Document Format (PDF) is a successor language of PDL, but it is only capable of creating vector graphics. Even though PDF is very popular as a document format used in typical document exchange, it is not very useful in our work.

Printer Command Language (PCL) is a minimalist PDL that is also popular. However, it has limited capabilities and could not be used to exploit printer as well as PS could.

2.1.2 Printer Control Languages

Along with PDL, Printer control languages are used to control printer settings such as the number of copies, tray size, and paper size. However, since page control language controls mostly control external settings of a printer, it is not the main interest of our work.

2.1.3 Printer Connection Protocols

Different protocols are used to send a document to a printer. Each protocol is associated with a port with a fixed number. Our works involve LPD protocol and Raw printing.

Line Printer Daemon (LPD) protocol runs on port 515 with `lpr` command. The files sent consist of both control file and the data file which contains the actual content. LPD could also be used to carry malicious PostScript files to the printer as one of our attack does.

Raw printing runs on port 9100 using TCP to carry data to the printer. The data sent is solely processed by the receiver printer, and the protocol itself only transports data to the destination. The protocol is also bidirectional, that is the printer can send feedback to the user. This makes this protocol vulnerables to many of our attacks described in Section 4.

2.2 MIT Printing System

MIT printers are set up around campus, both in dormitories and academic buildings. All of the printers are Hewlett Packard (HP) printers. The most common models are HP LaserJet 9050n, HP LaserJet 4350n, and HP m605.

MIT uses a centralized network printing. Each printing station consists of a printer and a card reader machine called "omega." When a user orders a print job via the popup user interface, the user must also specify a Kerberos name. Then the document will be sent to the MIT main Pharos server and are kept there for 24 hours under the specified Kerberos name.

To obtain the physical printed document, the user must walk to a nearby printer and swipe their MIT card at the associated omega machine. The omega machine then sends a printing request to the MIT main server. The main server consequently sends the document back to the corresponding printer via TCP protocol to raw port 9100.

3 Security Analysis

In this section, we set up a framework of security policy and user roles and their access levels for printing network in MIT and in general.

3.1 Security Goals: the CIA Triad

The three main principles of information security are the CIA triad – confidentiality, integrity, and availability. In the context of our project, these principles translate to the following goals.

1. **Confidentiality**: the printing content or other files on the printers should not be disclosed to adversaries.

2. **Integrity**: the printing content or other system files should not be modified in an unintended way.

3. **Availability**: the printers should be available to users when needed and adversaries cannot exploit the resource in the system.

3.2 User Roles and Access Levels

To define who the users and adversaries are, and what kinds of actions are authorized, we consider the principals and what roles they have in the system for the general network printer and for the MIT system.

In a general network printer system, the user roles and access levels are as follows.

1. **Administrators**: administrators are responsible for managing the printer settings, especially the security of network.

2. **Authorized users**: each user can print their own job whenever they want, and they have no access to other users' print jobs or printer settings.

3. **Unauthorized users**: individuals who are not involved in the organization should have no access to any component of the printer system.

In the context of MIT printer system, system administrators are IS&T Staff. Authorized users are MIT affiliates, including faculty members, students, and other staff. Unauthorized users are individuals unaffiliated with MIT.

3.3 Attacker Model

To model different types of attackers, we can classify attackers by the level of access that they have.

1. **Physical-access attacker**: the attacker has physical access to the printer and can send malicious files directly into the printer via USB port if enabled. The attacker may also change the settings of the printer if password is not strong enough or even not set at all.

2. **Local attacker**: the attacker is in the same local network as the printer.

3. **Remote attacker**: the attacker is not in the same local network as the printer, but may access the printer if the printer has a public IP address without firewall or via cross-site printing which will be described in further detail in Section 4.

3.4 MIT printers

MIT printers can be found in academic buildings, facility buildings, and all dorms. Most printers except those belong to labs (private printers), require authentication from card swiping (Omega).

Since non-private MIT printers obtain printing jobs from the Pharos server, they all are network printers and have IP addresses and Domain Name associated with them. According to [6], each printer name, which is written on the printer itself or the nearby omega, is the same as its reference to Domain Name, i.e. `<printer>-p.mit.edu`. (List of dorm MIT printers `http://kb.mit.edu/confluence/display/istcontrib/List+of+dorm+printers+for+reference`). These sites supply content each printer server through port 80.

In this paper, we will refer MIT printers to non-private MIT printers because we focus mostly on those printers used by majority of students and faculties.

We categorizes MIT printers into two types based on their protection.

1. **Unprotected printers**: by default when no one enable firewall or configuration port protection, all vulnerable ports are opened including RAW port 9100, FTP port 21, telnet port 23, and LPD port 515 as shown in Figure 7.

   Examples of MIT printers are `pharosw91` in IS&T (W92), `avery` in a graduate dormitory (Ashdown), `w51c` in Burton Connor, and five Dell printers in Hayden.

2. **Protected printers**: the firewall configuration that filters IP address and protecting port usually happen together as shown in Figure 2. Most of the MIT printers' ports are protected, and `<printer>-p.mit.edu` only allows the administrator IP address to access. Examples of MIT printers are `ajax` in the 5th floor of the Student Center, `simmons` in undergrad dorm (Simmons), `pulp-fiction` in Senior House.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-16 15:00 EDT
Nmap scan report for 10.240.0.107
Host is up (0.0026s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE    VERSION
80/tcp    open  http       Virata-EmWeb 6.2.1
280/tcp   open  http       Virata-EmWeb 6.2.1
443/tcp   open  ssl/http   Virata-EmWeb 6.2.1
515/tcp   open  tcpwrapped
14000/tcp open  tcpwrapped
```

Figure 1: Open ports of MIT protected printers.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-04-28 04:13 EDT
Nmap scan report for 10.18.3.196
Host is up (0.0019s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        HP LaserJet P4014 printer ftpd
23/tcp    open  telnet     HP JetDirect telnetd
80/tcp    open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
280/tcp   open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
443/tcp   open  ssl/http   HP-ChaiSOE 1.0 (HP LaserJet http config)
515/tcp   open  printer
631/tcp   open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
9100/tcp  open  jetdirect?
14000/tcp open  tcpwrapped
Service Info: Device: printer; CPE: cpe:/h:hp:laserjet_p4014
```

Figure 2: Open ports of MIT unprotected printers.

4 Attacks and Proof of Concept

4.1 Direct and Unlimited Printing

MIT gives each student a printing quota of 3,000 pages per semester. However, we found two simple ways to achieve unlimited printing, thus violating the availability aspect.

First, an adversary could directly connect to the printer via USB connection. Most MIT printers do not block direct printing, even though it is pretty simple to do so. Second, for those printer that leaves port 9100 open, an adversary could simply print the document via this port by using IP address that could be found easily on each printer's control panel.

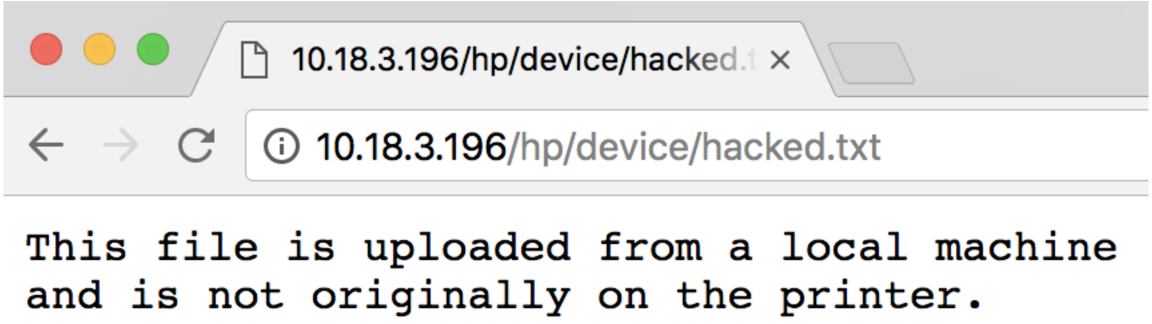
Moreover, opening port 9100 to the public could make the printer vulnerable to Cross Site Printing attack (XSP). The attacker can inject code for printing on any site that is vulnerable to XSS (Cross Site Scripting). Once the printer user run this site, the code will be compiled and let the attacker print while hiding his/her own identity. This can lead to a spamming attack.

4.2 Data Manipulation

4.2.1 Using Printer Job Language (PJL)

1. **Change display message**: This is a simple trick which works because port 9100 is open. The code used to modify the display and the image of the modified display are shown in Figure 4.

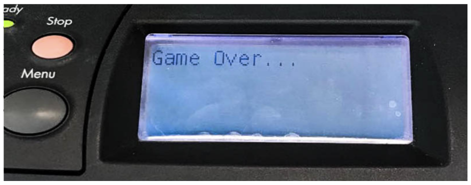
2. **Upload and download**: [8] provides a command line interface that allows us to easily download most files from the printer and upload our own files. Since our test printer has a web interface hosted on the printer, we can upload file onto the '/webServer/home' directory. The files become accessible through a typical web browser, as shown in Figure 3.



10.18.3.196/hp/device/hacked.txt

```
This file is uploaded from a local machine
and is not originally on the printer.
```

Figure 3: A screen capture of a file uploaded onto the test printer. The file becomes accessible through a web browser.



(a) Modified control panel display.

```
$ nc <printer-ip> 9100
@PJL RDYMSG DISPLAY="Game Over..."
```

(b) The code used to execute the attack.

Figure 4: Changing ready message can be easily performed via Port 9100 open port.

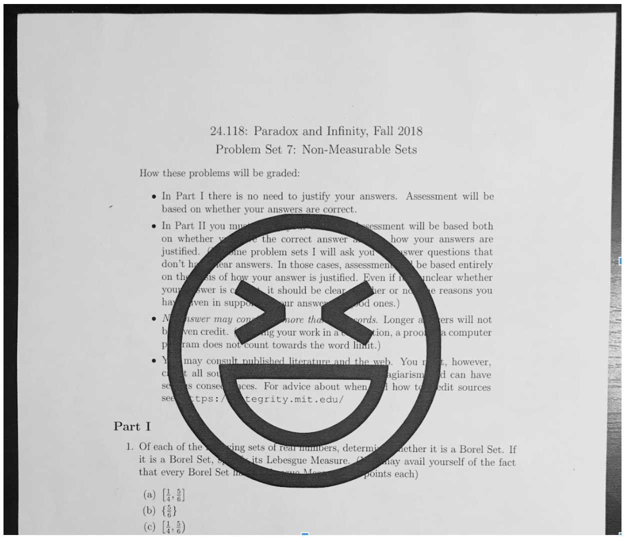
4.2.2 Using PostScript

The paper [8] demonstrates the possibility of manipulating future print jobs by using two techniques to take advantage of the PostScript language. First, we can circumvent the main job server loop by using `startjob` or `exitserver` commands, so that the changes will affect all future jobs until the printer is turned off. Next, such changes can be made by redefining relevant operators, such as `showpage`, the main print operator. This trick leads to the following attacks, which are easily done using the script provided in [8].

1. **Overlay**: We can overlay a custom Encapsulated PostScript (EPS) file, which contains words or an image, onto every future pages. Figure 5 shows our example of overlaying a smiley face on a problem set.

2. **Text replacement**: Similarly, we can replace a string with another string. The string could be either a single letter or a word. However, our attempts were partially successful. While changing a letter works perfectly fine with a PostScript file, as shown in Figure 6, printing a typical PDF file results in unexpected transition. For instance, replacing ‘1’ to ‘2’ resulted in changing from ‘k’ to ‘n’ instead. This might be because the PDF file was rendered in an intermediate format where each character was not represented with its actual character.

Both attacks could have serious consequences in real life. An adversary could overlay a spam advertisement or simply a blank page as a prank, or replace an amount of money in a contract. An



24.118: Paradox and Infinity, Fall 2018

Problem Set 7: Non-Measurable Sets

How these problems will be graded:

- In Part I there is no need to justify your answers. Assessment will be based on whether your answers are correct.
- In Part II you mu ssessment will be based both on whether y e the correct answer a how your answers are justified. (me problem sets I will ask you swer questions that don't h ear answers. In those cases, assessmen be based entirely on th sis of how your answer is justified. Even if i nclear whether you swer is c it should be clear her or n e reasons you ha iven in suppo ur answe od ones.)
- *N nswer may con more tha ords.* Longer a ers will not b ven credit. ng your work in a tion, a proo a computer p ram does not count towards the word limit.)
- Y may consult published literature and the web. You t, however, c t all sou agiarism d can have se s conse ces. For advice about when how t edit sources see `ttps:/ tegrity.mit.edu/`

Part I

1. Of each of the ing sets of real numbers, determi hether it is a Borel Set. If it is a Borel Set, its Lebesgue Measure. ay avail yourself of the fact that every Borel Set points each)

   (a) $[\frac{1}{4}, \frac{5}{6}]$
   (b) $\{\frac{5}{6}\}$
   (c) $[\frac{1}{4}, \frac{5}{6})$

Figure 5: Overlay attack

adversary might be someone in the same company who has an access to the printer via local network, and the victim might not notice the text replacement in the printed paper.

4.3 Denial of Service (DoS) Attack

In this scenario, an attacker will prevent everyone else from using a printer. Two different approaches we use are Loop forever file and Buffer Overflow.

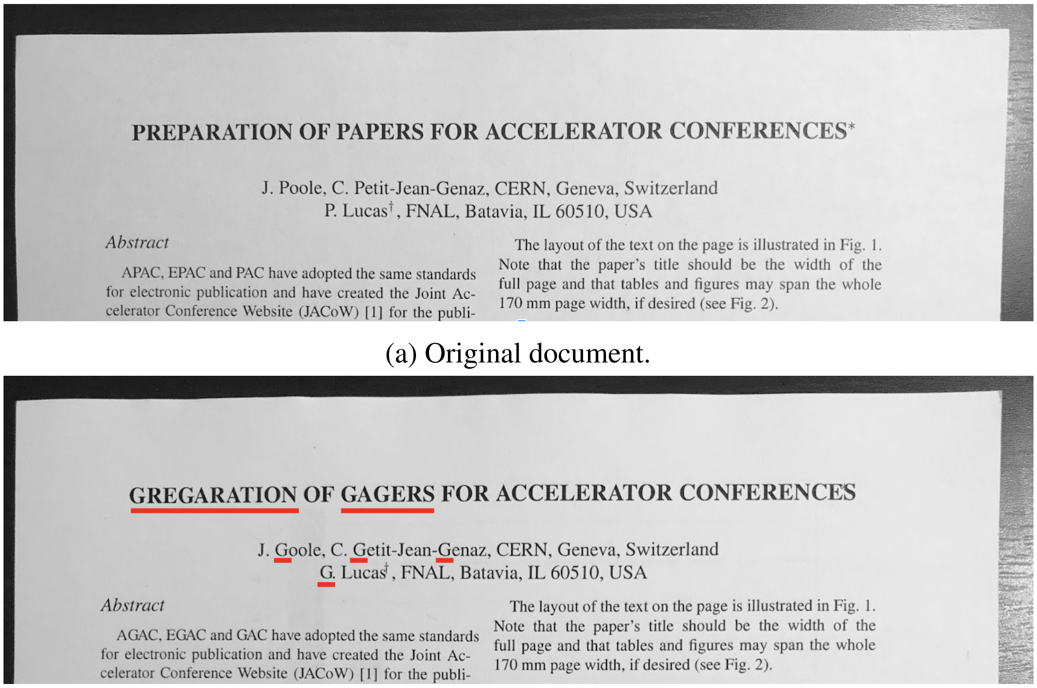
4.3.1 Loop Forever file

Most of the attacks discussed so far rely on the fact that printer port 9100 are opened and insecure. However, this attack requires only the basic ability to print the file. An attacker can print malicious PostScript file and the printer will execute the postscript commands. As discussed in [8], they can supply forever loop file causing the printer to processing the job forever.

We tested this attack on MIT printers. We first tested on an unprotected MIT printer by submitting print file through LPD commands and HP web interface. The malicious PostScript file works as expected: printer keep being stuck in the loop and processing our job indefinitely. However, when we tested in protected printer by sending the PostScript file with LPD command in Athena Machine, the file does not show up on the Omega screen.

4.3.2 Buffer Overflow

As demonstrated in PRET paper [8], we used PRET tool to test buffer overflow by supplying username for printing job ordering via LPD. PRET tested with 150 bytes overflow, for MIT HP printer 4350n, only 80 bytes are enough to make buffer overflow work. Then the printer shuts down suddenly and show error as in Figure 8 .



PREPARATION OF PAPERS FOR ACCELERATOR CONFERENCES[*]

J. Poole, C. Petit-Jean-Genaz, CERN, Geneva, Switzerland
P. Lucas[†], FNAL, Batavia, IL 60510, USA

Abstract

APAC, EPAC and PAC have adopted the same standards for electronic publication and have created the Joint Accelerator Conference Website (JACoW) [1] for the publi-

The layout of the text on the page is illustrated in Fig. 1. Note that the paper's title should be the width of the full page and that tables and figures may span the whole 170 mm page width, if desired (see Fig. 2).

(a) Original document.

GREGARATION OF GAGERS FOR ACCELERATOR CONFERENCES

J. Goole, C. Getit-Jean-Genaz, CERN, Geneva, Switzerland
G. Lucas[†], FNAL, Batavia, IL 60510, USA

Abstract

AGAC, EGAC and GAC have adopted the same standards for electronic publication and have created the Joint Accelerator Conference Website (JACoW) [1] for the publi-

The layout of the text on the page is illustrated in Fig. 1. Note that the paper's title should be the width of the full page and that tables and figures may span the whole 170 mm page width, if desired (see Fig. 2).

(b) Altered document, with the letter 'P' replaced with letter 'G', with red underline annotations.

Figure 6: Text replacement attack

```
    ./lpdtest.py printer in "`python -c 'print "A"*80'`"
```

Figure 7: example command using PRET tool to attack buffer overflow on LPR command connected via LPD port

4.4 Miscellaneous Attacks

4.4.1 Backdoor in Firmware

We exploit the fact that MIT unprotected printers' file transfer port has weak security. We use metaploit to bruteforce the password of the FTP.

For example, printer HP LaserJet 4350n pharosw91 has weak FTP username: admin and password: admin. According to HP manual [1], user can upload file .rfu through FTP port and the printer will auto update the firmware. This vulnerability from open FTP port and weak password could allow an attackers to easliy force the printer to update the malicious firmware.

This allows attacker to easily upload the malicious firmware and insert backdoor to the printer as shown in [4] or inject malware as shown in [5].

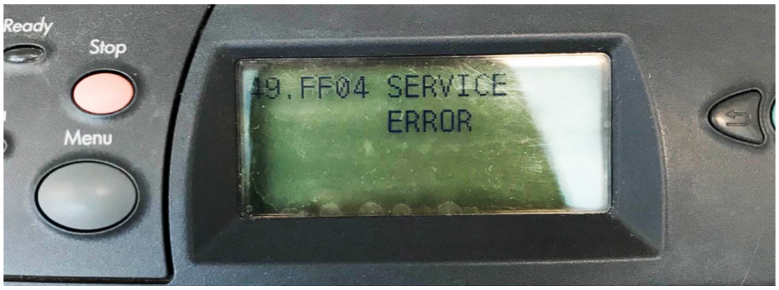
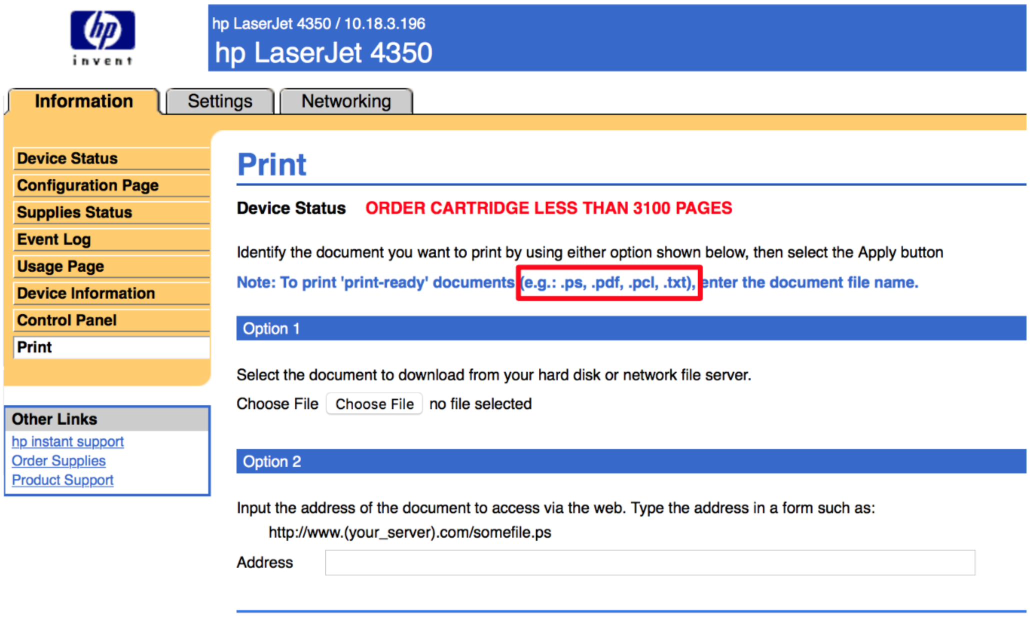


Figure 8: The printer shuts down suddenly after the the buffer overflow attack and display service error.



hp LaserJet 4350 / 10.18.3.196

hp LaserJet 4350

Print

Device Status ORDER CARTRIDGE LESS THAN 3100 PAGES

Identify the document you want to print by using either option shown below, then select the Apply button

Note: To print 'print-ready' documents (e.g.: .ps, .pdf, .pcl, .txt), enter the document file name.

Option 1

Select the document to download from your hard disk or network file server.

Choose File no file selected

Option 2

Input the address of the document to access via the web. Type the address in a form such as:

http://www.(your_server).com/somefile.ps

Address

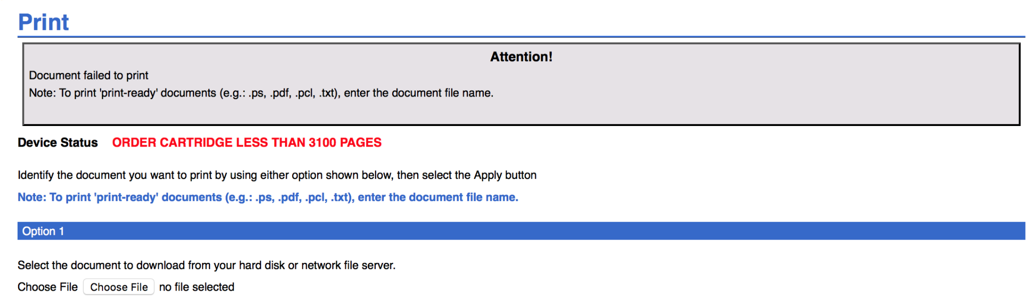
Figure 9: The print page from HP printer LaserJet 4350n specifying what file format are allowed.

4.4.2 HP Web Interface

Man In The Middle Attack (MITM) HP printers use HTTP POST request to submit the printing job instead of using HTTPS. Therefore, if user use the web interface to print the file, the communication can be eavesdropped and thus exposed to MITM attack.

Unrestricted File Upload Although it explicitly states in the web page that the only accepted printed document extensions are `.ps, .pdf, .pcl, .txt` (the Figure 9), there is no further check on actual type. This can possibly lead to unrestricted file upload where user can upload .exe file for printing job.

We currently doesn't have proof-of-concept on this vulnerability, but we believe that attacker can supply executable file that will be further executed by the printer.



Print

Attention!

Document failed to print

Note: To print 'print-ready' documents (e.g.: .ps, .pdf, .pcl, .txt), enter the document file name.

Device Status ORDER CARTRIDGE LESS THAN 3100 PAGES

Identify the document you want to print by using either option shown below, then select the Apply button

Note: To print 'print-ready' documents (e.g.: .ps, .pdf, .pcl, .txt), enter the document file name.

Option 1

Select the document to download from your hard disk or network file server.

Choose File no file selected

Figure 10: The print page shows error when the printer are not able to print the file we uploaded.

5 Other Attempts

So far, the attacks to control printer using PJL and PostScript (PS) provides us an ability to read and write files and directories, but PJL and PS have rather limited capabilities. Our objective is to be able to execute any LynxOS commands.

5.1 Reverse Engineering Small Binary

In order to perform buffer overflow attack so that we could execute shell code, exploit return to libc or Return to Oriented Programming, we will need to understand how the binary files running on such port work.

We first attempted to reverse engineering very small binary files such as `/bin/ls` with IDA Pro shown in Figure 11.

The reverse engineering approach did not work and we further noticed that first four bytes of the binary was not what we expected from usual ELF file. While the first four bytes of a common ELF file in Linux system are `7f 45 4c 46`, the first four bytes of printer's `ls` are `8f 45 4c 46`, which has an incorrect first byte.

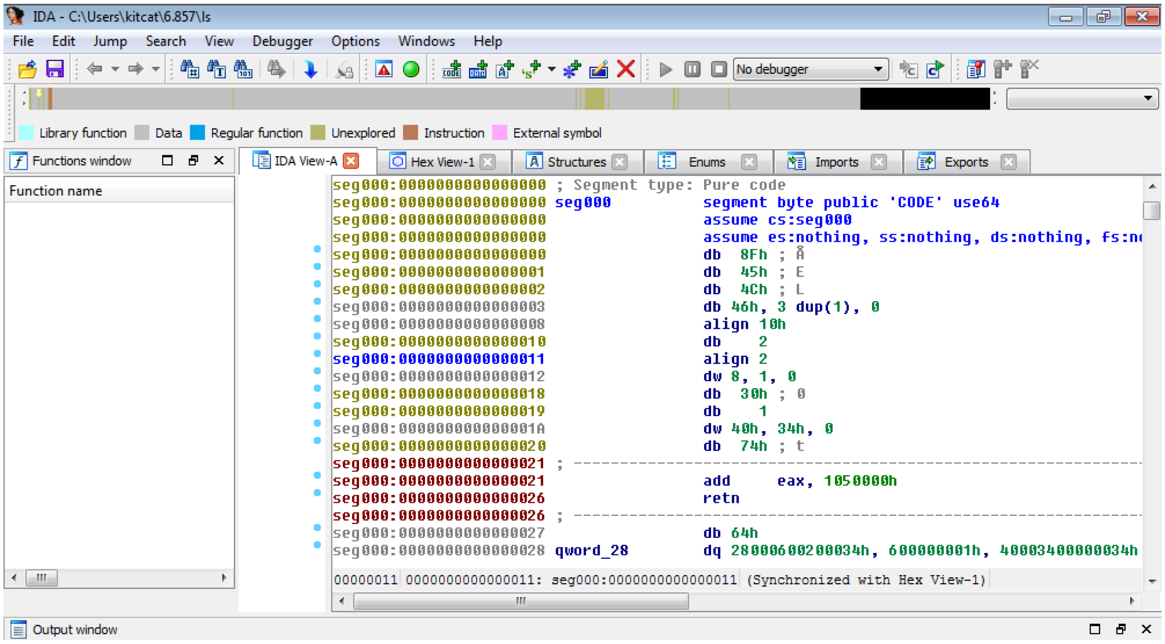
Our assumption is that this is a new ELF file format that is specifically used in this operating system. `.profile` tells us that the printer uses LynxOS, but LynxOS is closed source. Therefore, this reverse engineering process will become much harder for us to achieve within the time constraint for this project.

5.2 Executing Command in Printer OS

We used PRET [8] to exploit via PJL, which allowed us to read and write files and directories in the printer and list all LynxOS available commands, including `cp, df, dlsh, fsck, gdbserver, ls, ps, rc, sh`, as shown in Figure 12.

5.2.1 Attempt 1: Adding our command to `/bin/rc`

After some investigation, we found that `/etc/starttab` shown in 13 seems to be a startup file for the printer, as indicated in the comment "System initialization info," and also executes `/bin/rc`.



```
seg000:0000000000000000 ; Segment type: Pure code
seg000:0000000000000000 seg000          segment byte public 'CODE' use64
seg000:0000000000000000                 assume cs:seg000
seg000:0000000000000000                 assume es:nothing, ss:nothing, ds:nothing, fs:n
seg000:0000000000000000                 db  8Fh ; Å
seg000:0000000000000001                 db  45h ; E
seg000:0000000000000002                 db  4Ch ; L
seg000:0000000000000003                 db 46h, 3 dup(1), 0
seg000:0000000000000008                 align 10h
seg000:0000000000000010                 db    2
seg000:0000000000000011                 align 2
seg000:0000000000000012                 dw 8, 1, 0
seg000:0000000000000018                 db  30h ; 0
seg000:0000000000000019                 db    1
seg000:000000000000001A                 dw 40h, 34h, 0
seg000:0000000000000020                 db  74h ; t
seg000:0000000000000021 ; ---------------------------------------------------------------
seg000:0000000000000021                 add     eax, 1050000h
seg000:0000000000000026                 retn
seg000:0000000000000026 ; ---------------------------------------------------------------
seg000:0000000000000027                 db 64h
seg000:0000000000000028 qword_28        dq 2800060020034h, 600000001h, 400034000000034h
00000011 0000000000000011: seg000:0000000000000011 (Synchronized with Hex View-1)
```

Figure 11: Reverse Engineering the /bin/ls binary with IDA pro.

Therefore, we should be able to add our own command to the end of `/bin/rc` to make the printer execute our commands when it starts up. Since the terminal output of `/etc/starttab` cannot be seen anyway, we overcame that issue by redirecting the output to the file that we had a write permission, which we knew from an earlier test, e.g. `/tmp/result`. For example, if we wanted to get the list of the current processes, we would insert `ps > /tmp/running_process` to the end of `/bin/rc`.

However, we wanted to test with the simplest command that already works in `/bin/rc` to make sure that if this attempt failed, the issue came from another step, not the inability to execute our inserted line properly. Therefore, we tested it with the simplest echo lines: `echo "6.857 Game Over..." > /tmp/start-tsmit` at the beginning and `echo "6.857 Game Over..." > /tmp/start-tsmit` at the end, as shown in Figure 14.

We verified that our change correctly overrode the actual `/bin/rc` in the printer. Unfortunately, after we restarted the printer, it reloaded all the binary including `/bin/rc` back to its correct, original version. Before we restarted the printer, the change we modified affect the `rc` file, and `ls` reflected the following information: `- 2276 May 2 2018 (created May 2 13:10) rc`. After we restarted the printer, `ls` showed this information instead: `- 2188 Apr 6 2011 (created May 2 16:26) rc`. This means the file has been changed back to the 2011 version, which is the same year as that of the firmware.

We conclude that the printer reloads every file at the startup, even if this might not be the case for Linux when we modify its startup files. So, this unexpected behavior prevents us from executing our code by modifying `/bin/rc`.

5.2.2 Attempt 2: Replacing `/bin/ls` with other executables

From the first attempt, we realize that we will need to make our attack work without restarting the printer. Otherwise, all binary files will get overridden.

We thought that the PJL command to list directories such as `@PJL FSDIRLIST` may use `/bin/ls` to get the list of directories. Therefore, we tried replacing the `/bin/ls` with `/bin/ps` to make `ps` get executed instead, and hoped that the result from `@PJL FSDIRLIST` would change. However, `@FSDIRLIST` still returned the correct result. Our assumption is that `@FSDIRLIST` does not use `/bin/ls`, or `/bin/ls` might not be used at all.

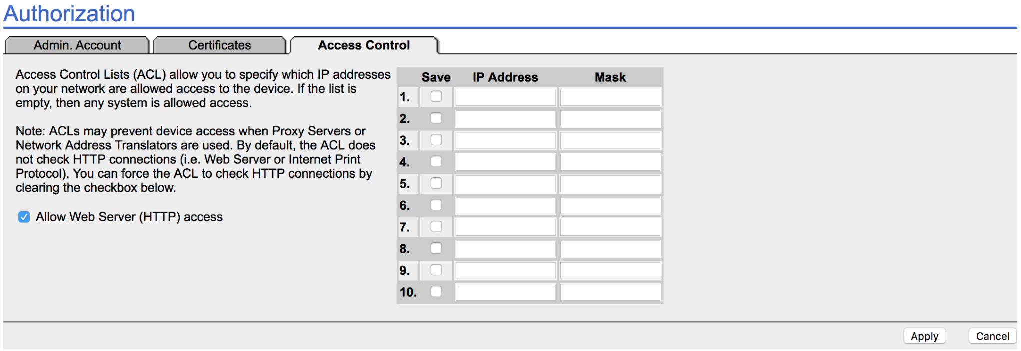
6 Security Recommendations

To prevent printers from attacks mentioned earlier, we would suggest a guideline in this section. The advice is for both administrator and printer company to ensure the security of printers.

6.1 Administrator Advice

In this subsection, we propose a guideline that can be done by the administrator or the owner of printers. Some steps are listed as follows.

1. **Firewall your printer:** A firewall is a network security system that allows user to approve only specific IP address while blocking others. An example of this method is shown in the Figure 15. It is a web interface of a printer on MIT printing network that we worked on. In this interface, users are able to specify the accessibility of their printers via web server by listing all approved IP addresses. With this method, the adversary will not be able to attack you via web server.



Access Control Lists (ACL) allow you to specify which IP addresses on your network are allowed access to the device. If the list is empty, then any system is allowed access.

Note: ACLs may prevent device access when Proxy Servers or Network Address Translators are used. By default, the ACL does not check HTTP connections (i.e. Web Server or Internet Print Protocol). You can force the ACL to check HTTP connections by clearing the checkbox below.

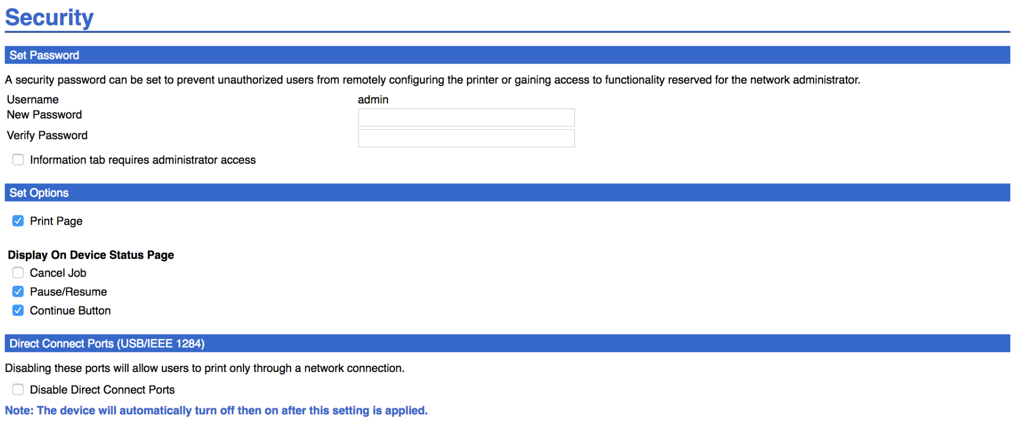
☑ Allow Web Server (HTTP) access

	Save	IP Address	Mask
1.	□		
2.	□		
3.	□		
4.	□		
5.	□		
6.	□		
7.	□		
8.	□		
9.	□		
10.	□		

Figure 15: A web interface of network printer that allow users to block all network access except specific IP addresses. It is an example of a simple firewall that can be done by users.

2. **Setting a strong password:** As mentioned earlier, most network printers can be accessed remotely with a password. The simplest thing for users to do is setting a password. As show in the Figure 16, users are allowed to set password easily in the web interface.

Other than the password of the printer, we also need to set a password for FTP port (File Transfer Protocol) as well. As we mentioned in Section 4, we are able to use Metasploit (a tool for Brute Force attack) to obtain a username and password for FTP port of MIT printers. Thus, it would be worth considering setting up a *strong* password for this port as well.



Security

Set Password

A security password can be set to prevent unauthorized users from remotely configuring the printer or gaining access to functionality reserved for the network administrator.

Username	admin
New Password	
Verify Password	

□ Information tab requires administrator access

Set Options

☑ Print Page

Display On Device Status Page

□ Cancel Job

☑ Pause/Resume

☑ Continue Button

Direct Connect Ports (USB/IEEE 1284)

Disabling these ports will allow users to print only through a network connection.

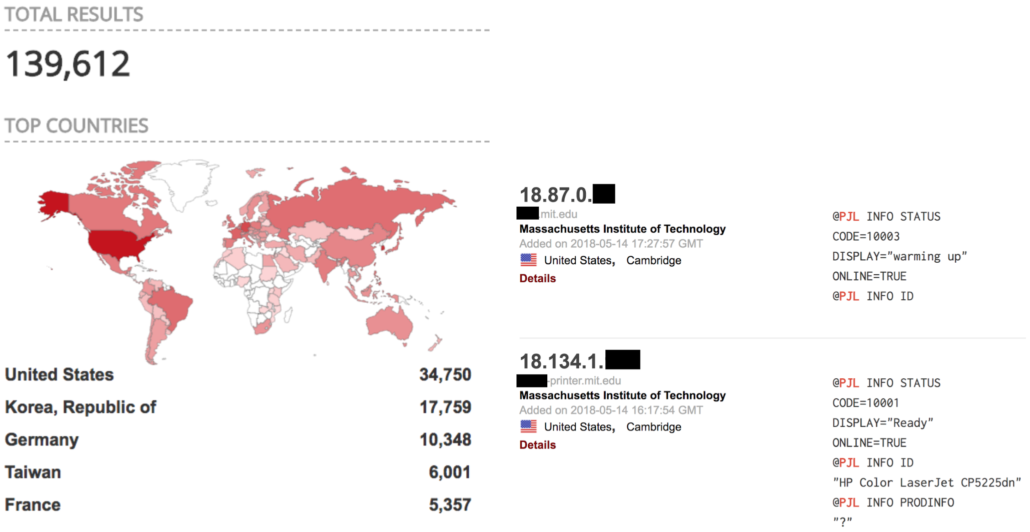
□ Disable Direct Connect Ports

Note: The device will automatically turn off then on after this setting is applied.

Figure 16: A security page from a printer's web interface that allow users to easily set a password, set options, and enable/disable direct connect ports

3. **Update firmware:** When security issues are discovered, most printer manufacturers will send out firmware updates to close security holes. Thus, installing the latest version of firmware will prevent your printers from the most basic network printers issues. Since most printers released after 2010 support web services, these printers can use a direct Internet connection to find and install updates. Another option is to download firmware updates from the manufacturer websites to users' computer and install updates for printers from the computer.

4. **Keep track of port 9100:** As mentioned earlier, port 9100 lead a printer to a lot of malicious attacks. The printer itself already has a timeout to prevent port 9100 being left open, but users can also set the timeout to ensure the security. In addition to that, there is a public site called "Shodan" that shows all the printers that left port 9100 open as shown in the Figure 17. With this tool, users are able to monitor their own printer and ensure that it is not left port 9100 open.



TOTAL RESULTS

139,612

TOP COUNTRIES

United States	34,750
Korea, Republic of	17,759
Germany	10,348
Taiwan	6,001
France	5,357

18.87.0.[redacted]

[redacted].mit.edu

Massachusetts Institute of Technology

Added on 2018-05-14 17:27:57 GMT

United States, Cambridge

Details

```
@PJL INFO STATUS
CODE=10003
DISPLAY="warming up"
ONLINE=TRUE
@PJL INFO ID
```

18.134.1.[redacted]

[redacted]-printer.mit.edu

Massachusetts Institute of Technology

Added on 2018-05-14 16:17:54 GMT

United States, Cambridge

Details

```
@PJL INFO STATUS
CODE=10001
DISPLAY="Ready"
ONLINE=TRUE
@PJL INFO ID
"HP Color LaserJet CP5225dn"
@PJL INFO PRODINFO
"?"
```

Figure 17: An interface of "Shodan." It shows all the printers that left port 9100 open. The left hand side displays the colored map based on the number of printers in each region. The right hand side shows some of the information about printers that can be seen on this site.

5. **Disable direct connect ports:** We described in Section 4 that we are able to have unlimited printing by connecting through USB port. However, this unlimited printing is against MIT policy which limits students' print quota to 3000 pages per semester. To avoid this issue, MIT could check the box for "Disable Direct Connect Ports" which is shown at the bottom of Figure 16.

6.2 Printer Manufacturer Advice

In this subsection, we suggest some solutions that need to be done by printer manufacturers. These solutions require a change in either a system or an interface of printers. Recent printers are designed to detect, protect, and even self-heal automatically. Here, we raise a concern that we found and would be able to improve printers' security.

1. **Password authentication:** The paper [6] indicates that the adversary can factory reset the printer by physical attacks even without knowing the password. With this reset, the adversary can set a new password and gain control over the printer. To avoid this attack, we suggest that the printer should have a password authentication before doing any important action on printer including resetting printers and updating firmware.

2. **Use encryption:** The unencrypted network printers are vulnerable to confidentiality issue. Some attacks are able to capture and access your files. Thus, it is important to use encryption for printer networks, so the print job cannot be intercepted and interpreted by an adversary. Furthermore, many printers also have hard drives to store all documents, and this is also vulnerable to attacks as well. Thus, it would be more secured for the printers to encrypt the data when sending and storing the information.

3. **Restrict print from web interface:** Instead of sending files through port 9100 or direct connect port, most printers allow users to print through web interface. However, this is also another way for attackers to send a malicious file to your printer. The printer manufacture can improve the security by disabling the option to print form web interface if there is vulnerability issue occurred.

7 Conclusion

To conclude, our group analyzed the MIT printing network and was able to find vulnerabilities for all three aspects of CIA triad - confidentiality, integrity, and availability. With the port 9100 left open and no IP addresses blocking in some MIT printers, we can communicate with the printers and perform various attacks to access files in the printer, modify the content, and gain control over printer. Moreover, we also proposed other attempts which are not based on the ability of PJL and PostScript in Section 5. To avoid most of the attacks mentioned earlier, we propose a guideline for both administrator and printer manufacturer side ranging from basic things as setting password to using encryption when dealing with information.

Acknowledgement

We would like to express our special thanks to Professors Ronald Rivest and Yael Tauman Kalai and the rest of 6.857 staff for the inspiring class and the opportunity to work on this project. We are also grateful to IS&T, particularly, Andy Kalenderian, who was the main point of contact, provided us the test printer, and gave suggestions during the early stage of our project. Lastly, we thank our TA Nicholas Wu who provided helpful guidance.

References

[1] The Hewlett-Packard Company. *HP LaserJet - Update the firmware*. URL: https://support.hp.com/us-en/document/c01711356 (visited on 05/16/2018).

[2] Andrei Costin. *Hacking Printers - 10 years down the road*. 2011. URL: http://andreicostin.com/papers/Conf%20-%20HashDays%20-%202011%20-%20Lucerne%20-%20AndreiCostin_HackingPrinters.pdf (visited on 05/16/2018).

[3] Andrei Costin. *Hacking printers: for fun and profit*. 2010. URL: http://archive.hack.lu/2010/Costin-HackingPrintersForFunAndProfit-slides.pdf (visited on 05/16/2018).

[4] Ang Cui, Michael Costello, and Salvatore J Stolfo. “When Firmware Modifications Attack: A Case Study of Embedded Exploitation”. In: (2013). URL: http://ids.cs.columbia.edu/sites/default/files/ndss-2013.pdf.

[5] Ang Cui and Sal Stolfo. *Print Me If You Dare: Firmware Update Attack and the Rise of Printer Malware*. 2011. URL: http://ids.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf (visited on 05/16/2018).

[6] Emily Do, Huy Pham, and Preksha Naik. “Security Analysis of the MIT Pharos Printing Network”. In: (2016). URL: https://courses.csail.mit.edu/6.857/2016/files/32.pdf.

[7] Adobe Systems Incorporated. *PostScript Language Reference Manual*. 1990. URL: https://www.adobe.com/content/dam/acom/en/devnet/actionscript/articles/psrefman.pdf (visited on 05/16/2018).

[8] Jens Müller et al. “Exploiting Network Printers A Survey of Security Flaws in Laser Printers and Multi-Function Devices”. In: (2016). URL: https://www.nds.rub.de/media/ei/arbeiten/2017/01/30/exploiting-printers.pdf.

[9] Jens Müller et al. “SoK: Exploiting Network Printers”. In: *2017 IEEE Symposium on Security and Privacy (SP)*. May 2017, pp. 213–230. DOI: 10.1109/SP.2017.47.

[10] Aaron Weaver. “Cross Site Printing”. In: (2007). URL: https://helpnetsecurity.com/dl/articles/CrossSitePrinting.pdf (visited on 05/16/2018).

```
 ./pret.py 10.18.3.196  pjl
      ________________
    _/_______________/|
   /___________/___//||   PRET | Printer Exploitation Toolkit v0.40
  |===        |----| ||    by Jens Mueller <jens.a.mueller@rub.de>
  |           |   | ||
  |___________|   | ||
  | ||/.---.||    | ||       pentesting tool that made
  |-||/_____\||-.  | |         dumpster diving obsolete
  |_||=L==H==||_|__|/

     (ASCII art by
     Jan Foerster)

Connection to 10.18.3.196 established
Device:   hp LaserJet 4350

Welcome to the pret shell. Type help or ? to list commands.
10.18.3.196:/> cd ../..
cd *** Congratulations, path traversal found ***
Consider setting 'traversal' instead of 'cd'.
10.18.3.196:/../../bin> ls
-     1212   cp
-     2860   df
-    14684   dlsh
-     6572   fsck
-     2156   gdbserver
-     1436   ls
-     2460   ps
-     2188   rc
-    14684   sh
```

Figure 12: Using PRET's PJL to get binary inside /bin or all commands supported by LynxOS.

```
#
#        System initialization info
#
#Default umask
# Modified by HP to support non-root accessible architecture requirements
#0022
#0002
# Modified by HP to support NFS disk access
0000
#
#Name of single-user shell
/bin/sh
#
#Name of rc file
/bin/rc
#
# Data, stack, and core file limits (in Kbytes)
16384
2048
1024
```

Figure 13: Content in printer's file `/etc/starttab`

```
#!/bin/dlsh

echo "6.857 Game Over..." > /tmp/start-tsmit
echo `\n\n\n\n'

# 4/22/04 Todd Lutz
# Added /hp/bin to get to setdebug command
$#set(path, /bin /etc /hp /hp/bin / . /net)

# disable JVM
#$#set(CHAISERVERROOT,NO_WEBSERVER)
#$#export(CHAISERVERROOT)

#stty crt kill ^U intr ^C eof ^D -tabs

#Add plumbing to automatically load cpb firmware in OS_ONLY system
#that has an MFP attached.
#
if \! $access(x, all, /hp/bin/boot)
  echo `OS_ONLY build -- /hp/bin/boot missing'
  if $access(x, all, /bin/cpbInit)
    /bin/cpbInit
  end
end

echo `
...

# hw_debug & hw_nodebug, not hw_rom
#   need to do this before autoboot in case user CTRL-C's autoboot
if $access(x, all, /bin/bash)
  $#set(HISTSIZE,10)
  $#set(HISTFILE,/hpmnt/.bash_history)
  $#export(HISTSIZE)
  $#export(HISTFILE)
end

# ROM/RAM FULLIMAGE
if $access(x, all, /hp/bin/autoboot)
  ...

if $access(x, all, /bin/sh)
  exec /bin/sh -i
end
echo "6.857 Game Over..." > /tmp/end-tsmit
exit 0
```

Figure 14: Content in printer's file /etc/starttab. "..." means the code is left out due to space constraint.