



COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

ANG CUI | SAL STOLFO

{ANG|SAL}@CS.COLUMBIA.EDU

COLUMBIA UNIVERSITY INTRUSION DETECTION SYSTEMS LAB

Update: 12.23.2011 HPSBPI02728 SSRT100692 rev.2

Vendors	2Q10 Unit Shipments	2Q10 Market Share	2Q09 Unit Shipments	2Q09 Market Share	2Q10/2Q09 Growth
1. HP	11,934,950	41.0%	9,757,118	40.2%	22.3%
2. Canon	5,608,371	19.3%	4,942,090	20.4%	13.5%
3. Epson	4,083,638	14.0%	3,399,607	14.0%	20.1%
4. Samsung	1,667,671	5.7%	1,094,660	4.5%	52.3%
5. Brother	1,553,425	5.3%	1,319,257	5.4%	17.7%
Others	4,247,879	14.6%	3,731,497	15.4%	13.8%
Total	29,095,934	100.0%	24,244,229	100.0%	20.0%

Source: IDC Worldwide Quarterly Hardcopy Peripherals Tracker, August 2010

WHEN IN DOUBT, FOLLOW THE \$\$\$

HP IPG: 41% MARKET SHARE, SHIPS **40M UNITS PER YEAR!**

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

23. Are current HP multifunction printers susceptible to viruses and worms?

No, since the majority of viruses and worms exploit vulnerabilities in Windows-based computers. HP MFPs use non-standard operating systems other than Windows. Consequently, they are immune to these viruses and worms. In practice, there have been no known instances of viruses or worms infecting HP MFPs.

In the future HP will likely ship MFPs which include an embedded version of the Windows operating system. However, there are a number of practical reasons why this won't increase the security risk faced by customers.

24. Does this mean that HP MFPs are completely safe from worms and viruses?

No, since it is technically possible for someone to craft a virus or worm that targets the non-standard operating systems shipped with the MFPs. However, HP considers the probability of such an event to be considerably lower. Hackers are more likely to be interested in exploiting vulnerabilities in workstations and servers since they are more widespread and require less expertise.

White Paper: "HP Security Solutions" 2006

THANKS!



Jatin Kataria



Sal Stolfo



Jon Voris

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

INTERNET NEWS MACHINE... (DAY 1)

“Millions of printers open to devastating hack attack, researchers say”
MSNBC

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

INTERNET NEWS MACHINE... (DAY 1)

“Millions of printers open to devastating hack attack, researchers say”
MSNBC

“HP printers can be remotely controlled and set on fire, researchers claim”
ars technica

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

INTERNET NEWS MACHINE... (DAY 1)

“Millions of printers open to devastating hack attack, researchers say”
MSNBC

“HP printers can be remotely controlled and set on fire, researchers claim”
ars technica

“Hackers could turn your printer into a flaming death bomb”
Gawker

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

INTERNET NEWS MACHINE... (DAY 1)

“Millions of printers open to devastating hack attack, researchers say”
MSNBC

“HP printers can be remotely controlled and set on fire, researchers claim”
ars technica

“Hackers could turn your printer into a flaming death bomb”
Gawker

“Can hackers really use your HP printer to steal your identity”

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

INTERNET NEWS MACHINE... (DAY 1)

“Millions of printers open to devastating hack attack, researchers say”
MSNBC

“HP printers can be remotely controlled and set on fire, researchers claim”
ars technica

“Hackers could turn your printer into a flaming death bomb”
Gawker

“Can hackers really use your HP printer to steal your identity and **blow up your house?**”
gizmodo

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

INTERNET NEWS MACHINE... (DAY 2, SMACK DOWN AND SPANKING!)

“HP refutes reports that can be remotely set on fire”
FoxNews

“Hackers can set your house on fire through your older LaserJet printer”
Hitechnology.com

“HP smacks down Columbia University printer fire report”
silobreaker

“HP douses fiery printer hack theory”
Business Recorder

“HP memo spanks Columbia researchers over flaming printers flap”
Allthingsd.com

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

INTERNET NEWS MACHINE... (MY FAVORITE)

“HP HIT WITH LAWSUIT OVER FLAMING-PRINTER HACK”

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

INTERNET NEWS MACHINE... (MY FAVORITE)

“HP HIT WITH LAWSUIT OVER FLAMING-PRINTER HACK”

WIRED!

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

INTERNET NEWS MACHINE... THE NOT TERRIBLE

“SECURITY FLAW IN PRINTERS COULD EXPOSE BUSINESSES TO HACKERS”
HUFFINGTONPOST

“COULD YOUR PRINTER BE A TROJAN HORSE? RESEARCHERS SAY YES!”
CNET

“COLUMBIA RESEARCHERS SHOW REMOTE HP PRINTER HIJACK”
BETANEWS

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

DISCLOSURE: NOVEMBER 21ST

FIRMWARE RELEASE: DECEMBER 23RD

56

P R I N T E R
F I R M W A R E S
H A V E B E E N
U P D A T E D

2 0 0 5 - 2 0 1 1

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

BASED ON MY DISCLOSURE, THESE PRINTER FIRMWARES HAVE BEEN UPDATED

HP LaserJet Enterprise 500 color M551	HP LaserJet P4014	HP LaserJet M9040 Multifunction Printer
HP LaserJet Enterprise 600 M601	HP LaserJet P4015	HP LaserJet 9050
HP LaserJet Enterprise 600 M602	HP LaserJet 4240	HP LaserJet M9050 Multifunction Printer
HP LaserJet Enterprise 600 M603	HP LaserJet 4250	HP 9200c Digital Sender
HP Color LaserJet CM1312 Multifunction	HP LaserJet 4345 Multifunction Printer	HP 9250c Digital Sender
HP LaserJet Pro CM1415 Color Multifunction	HP LaserJet 4350	HP Color LaserJet 9500
HP Color LaserJet CP1510	HP LaserJet P4515	HP Color LaserJet CM3530
HP LaserJet M1522 Multifunction Printer	HP Color LaserJet Enterprise CP4520	HP Color LaserJet 3800
HP LaserJet Pro CP1525 Color Printer	HP Color LaserJet Enterprise CP4525	HP Color LaserJet CP4005
HP LaserJet Pro M1536 Multifunction Printer	HP Color LaserJet Enterprise CM4540	HP Color LaserJet CM6040
HP Color LaserJet CP2025	HP LaserJet Enterprise M4555 Multifunction	HP CM8060 Color Multifunction Printer
HP LaserJet P2035	HP Color LaserJet 4700	HP LaserJet 9040
HP LaserJet P2055	HP Color LaserJet 4730 Multifunction Printer	HP LaserJet M3027 Multifunction Printer
HP Color LaserJet CM2320 Multifunction	HP Color LaserJet CM4730 Multifunction	HP LaserJet M3035
HP LaserJet M2727 Multifunction Printer	HP LaserJet M5025 Multifunction Printer	HP Color LaserJet CP3505
HP Color LaserJet 3000	HP LaserJet M5035	HP Color LaserJet CP3525
HP LaserJet P3005	HP LaserJet 5200n	HP Color LaserJet CP5525
HP LaserJet Enterprise P3015	HP Color LaserJet Professional CP5225	HP Color LaserJet 5550
HP Color LaserJet CP6015	HP Color LaserJet CM6030	

CVE: CVE-2011-4161

SSRT: 100692 rev.2

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

RESEARCH IN CONTEXT. WHO AM I? WHY AM I DOING THIS?

4TH YEAR PH.D. CANDIDATE
INTRUSION DETECTION SYSTEMS LAB
COLUMBIA UNIVERSITY

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

RESEARCH IN CONTEXT. WHO AM I? WHY AM I DOING THIS?

PAST PUBLICATIONS:

- Pervasive Insecurity of Embedded Network Devices. [RAID10]
- A Quantitative Analysis of the Insecurity of Embedded Network Devices. [ACSAC10]
- Killing the Myth of Cisco IOS Diversity: Towards Reliable Large-Scale Exploitation of Cisco IOS. [USENIX WOOT 11]
- Defending Legacy Embedded Systems with Software Symbiotes. [RAID11]
- From Prey to Hunter: Transforming Legacy Embedded Devices Into Exploitation Sensor Grids. [ACSAC11]

4TH YEAR PH.D. CANDIDATE
INTRUSION DETECTION SYSTEMS LAB
COLUMBIA UNIVERSITY

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

RESEARCH IN CONTEXT. PREVIOUS WORK STUDYING EMBEDDED INSECURITY

VULNERABLE EMBEDDED SYSTEM SCANNER

EMBEDDED EXPLOITATION

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

RESEARCH IN CONTEXT. PREVIOUS WORK STUDYING EMBEDDED INSECURITY

VULNERABLE EMBEDDED SYSTEM SCANNER

Continuously Monitoring Internet for Trivially Vulnerable Embedded Devices

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

RESEARCH IN CONTEXT. PREVIOUS WORK STUDYING EMBEDDED INSECURITY

VULNERABLE EMBEDDED SYSTEM SCANNER

Continuously Monitoring Internet for Trivially Vulnerable Embedded Devices

1.4 Million Embedded Devices on the Internet with Default Passwords!

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

RESEARCH IN CONTEXT. PREVIOUS WORK STUDYING EMBEDDED INSECURITY

VULNERABLE EMBEDDED SYSTEM SCANNER

Continuously Monitoring Internet for Trivially Vulnerable Embedded Devices

1.4 Million Embedded Devices on the Internet with Default Passwords!

75,000 Vulnerable HP Printers on the internet. (We'll get back to this)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

EMBEDDED EXPLOITATION: **B**IDIRECTIONAL APPROACH

TOP DOWN: INTERNET SUBSTRATE:

BOTTOM UP: COMMON EMBEDDED DEVICES:

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

EMBEDDED EXPLOITATION: **B**IDIRECTIONAL APPROACH

TOP DOWN: INTERNET SUBSTRATE: **R**OUTERS (BLACKHAT 2011)

BOTTOM UP: COMMON EMBEDDED DEVICES: **P**RINTERS (NOW)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

B I G

QUESTION

CAN EMBEDDED SYSTEMS BE
EXPLOITED ?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HAVE EMBEDDED SYSTEMS BEEN
EXPLOITED ?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HAVE **YOUR** EMBEDDED SYSTEMS
BEEN EXPLOITED?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HAVE **YOUR** EMBEDDED SYSTEMS
B E E N E X P L O I T E D ?

HOW DO YOU KNOW FOR **SURE**?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

YOUR ROUTER/PRINTER
H A S B E E N
0 W N 3 D

CAN YOU REALLY **REMOVE**
T H E M A L W A R E ?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

LET'S TALK



PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HP KOAN: HOW DOES PRINTER UPDATE FIRMWARE?...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HP KOAN: HOW DOES PRINTER UPDATE FIRMWARE?... **PRINT!**

HP LaserJet Printer and Multifunction Printer (MFP) series - Performing a Firmware Upgrade

- Remote firmware update
- Determining the current level of firmware
- Downloading the latest firmware from www.hp.com
- What you should know before downloading firmware to the printer or Multi function Printer (MFP)
- Remote firmware update using FTP through a browser
- Remote firmware update using FTP on a direct network connection (Microsoft Windows)
For Shared Windows Systems
- Using USB
- Updating firmware using "HP Easy Firmware Upgrade" utility
- Remote firmware update using the LPR command
- Remote firmware update using the HP Printer Utility (Macintosh OS X)
- Remote firmware update using FTP on a direct network connection (Macintosh)
- Remote firmware update using HP Web JetAdmin
- Remote firmware update for UNIX systems
- Printer messages during the firmware update
- Troubleshooting a firmware update

From "HP LaserJet Printer and Multifunction Printer (MFP) series - Performing a Firmware Upgrade"

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HP KOAN: HOW DOES PRINTER UPDATE FIRMWARE?... **PRINT!**

Remote firmware update using the LPR command

NOTE: This remote firmware update method is for use in Microsoft Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003.

Complete the following steps to update the firmware by using the LPR command.

1. Type `lpr -P -S -o l -OR- lpr -S -Pbins`, where can be either the TCP/IP address or the hostname of the product, and where is the filename of the .RFU file from a command window.

NOTE: The parameter (-o l) consists of a lowercase "O", not a zero, and a lowercase "L", not a numeral 1. This parameter sets the transport protocol to binary mode.

2. Press `Enter` on the keyboard. The messages described in the section "Printer messages during the firmware update" appear on the control panel.

NOTE: The product automatically restarts the firmware to activate the update. At the end of the update process, the Ready message appears on the control panel.

3. Type `exit` at the command prompt to close the command window.

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HP KOAN: HOW DOES PRINTER UPDATE FIRMWARE?... **PRINT!**

Remote firmware update using the LPR command

NOTE: This remote firmware update method is for use in Microsoft Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003.

Complete the following steps to update the firmware by using the LPR command.

1. Type `lpr -P -S -o l -OR- lpr -S -Pbins`, where can be either the TCP/IP address or the hostname of the product, and where is the filename of the .RFU file from a command window.

NOTE: The parameter (-o l) consists of a lowercase "O", not a zero, and a lowercase "L", not a numeral 1. This parameter sets the transport protocol to binary mode.

2. Press `Enter` on the keyboard. The messages described in the section "Printer messages during the firmware update" appear on the control panel.

NOTE: The product automatically restarts the firmware to activate the update. At the end of the update process, the Ready message appears on the control panel.

3. Type `exit` at the command prompt to close the command window.

YOU SEE WHERE THIS IS **GOING...**

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

LET'S PLAY... STARE AT BINARY BLOB FTW

HP RFU (REMOTE FIRMWARE UPDATE) FILE

```
000000 40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 4D 4F 44 45 4C 3D 48 @PJL COMMENT MODEL=H
000014 50 20 4C 61 73 65 72 4A 65 74 20 50 32 30 35 35 64 6E 0A 40 P LaserJet P2055dn
000028 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 56 45 52 53 49 4F 4E 3D PJL COMMENT VERSION=
00003C 38 33 35 30 34 0A 40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 44 83504
000050 41 54 45 43 4F 44 45 3D 32 30 31 30 30 33 30 38 0A 40 50 4A ATECODE=20100308
000064 4C 20 55 50 47 52 41 44 45 20 53 49 5A 45 3D 37 39 32 39 39 L UPGRADE SIZE=79299
000078 30 36 0A 1B 25 2D 31 32 33 34 35 58 40 50 4A 4C 20 45 4E 54 06
00008C 45 52 20 4C 41 4E 47 55 41 47 45 3D 41 43 4C 0D 0A 00 AC 00 ER LANGUAGE=ACL
0000A0 0F 00 03 62 2D 00 00 00 00 00 79 00 00 AA 55 41 54 00 00 01 \b-
0000B4 20 00 67 FB E9 00 E2 17 03 00 00 00 00 00 67 FD 09 00 00 20 \g
0000C8 E0 00 00 4D 3C 00 68 1D E9 00 00 21 86 00 00 50 91 00 68 3F \M<
0000DC 6F 00 00 20 28 00 00 4D AA 00 68 5F 97 00 00 20 BC 00 00 50 o
0000F0 0C 00 68 80 53 00 00 20 CB 00 00 4C C4 00 68 A1 1E 00 00 20 F
000104 83 00 00 4D BF 00 68 C1 A1 00 00 20 23 00 00 4B 2A 00 68 E1 \M
000118 C4 00 00 1F E1 00 00 4B D8 00 69 01 A5 00 00 20 84 00 00 4D \
00012C 5A 00 69 22 29 00 00 21 1D 00 00 4E 12 00 69 43 46 00 00 21 Z
000140 42 00 00 50 24 00 69 64 88 00 00 24 0D 00 00 54 2D 00 69 88 B
000154 95 00 00 24 35 00 00 54 C1 00 69 AC CA 00 00 23 84 00 00 50 \
000168 E7 00 69 D0 4E 00 00 28 24 00 00 7A 8E 00 69 F8 72 00 00 22 i
00017C CD 00 00 50 D6 00 6A 1B 3F 00 00 21 3E 00 00 52 CF 00 6A 3C P
000190 7D 00 00 1F F3 00 00 4B C0 00 6A 5C 70 00 00 22 11 00 00 51 }

```

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HP RFU (REMOTE FIRMWARE UPDATE) FILE

- **PJL** COMMAND (PRINTER JOB LANGUAGE)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HP RFU (REMOTE FIRMWARE UPDATE) FILE

- PjL COMMAND
- A **SINGLE** PjL COMMAND

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HP RFU (REMOTE FIRMWARE UPDATE) FILE

- PJI COMMAND
- A SINGLE PJI COMMAND
- A SINGLE PJI COMMAND WITH **7MB** OF DATA

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HP RFU (REMOTE FIRMWARE UPDATE) FILE

- PJI COMMAND
- A SINGLE PJI COMMAND
- A SINGLE PJI COMMAND WITH 7MB OF DATA
- A SINGLE PJI COMMAND WITH 7MB OF
COMPRESSED (NOT ENCRYPTED) DATA

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HP RFU (REMOTE FIRMWARE UPDATE) FILE

- PJI COMMAND
- A SINGLE PJI COMMAND
- A SINGLE PJI COMMAND WITH 7MB OF DATA
- A SINGLE PJI COMMAND WITH 7MB OF COMPRESSED (NOT ENCRYPTED) DATA
- DATA IS INTEGRITY CHECKED, BUT IS IT **SIGNED**?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

SO DO HP RFUS USE DIGITAL SIGNATURE?

	attempting to eject the pages.	
CODE CRC ERROR SEND FULL RFU ON PORT	An error occurred during a firmware upgrade.	Contact an HP-authorized service or support provider.
CORRUPT FIRMWARE IN EXTERNAL ACCESSORY For help press ?	The product detected corrupt firmware in an input or output accessory.	Upgrade the firmware. Printing can continue, but jams might occur.
DATA RECEIVED To print last page	The product is waiting for the command to print (such as waiting for a form feed, or when	Press OK to continue.

HP P4010

LOOK THROUGH ERROR MESSAGES... CODE CRC != SIGNATURE

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

STATING THE OBVIOUS:

- LPR / RAW PRINTING HAS NO AUTHENTICATION MECHANISM

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

STATING THE OBVIOUS:

- LPR / RAW PRINTING HAS NO AUTHENTICATION MECHANISM
- PJJL CAN BE EMBEDDED IN POSTSCRIPT (AND LOTS ELSE)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

STATING THE OBVIOUS:

- LPR / RAW PRINTING HAS NO AUTHENTICATION MECHANISM
- PJJL CAN BE EMBEDDED IN POSTSCRIPT (AND LOTS ELSE)
- MALICIOUS RFU = PRINTER MALWARE

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

STATING THE OBVIOUS:

- LPR / RAW PRINTING HAS NO AUTHENTICATION MECHANISM
- PJJL CAN BE EMBEDDED IN POSTSCRIPT (AND LOTS ELSE)
- MALICIOUS RFU = PRINTER MALWARE
- MALICIOUS RFU + DOC FORMAT ATTACK VECTOR

=

SELF-PROPAGATING PRINTER MALWARE, EMBEDDED
SPEAR-PHISHING, ETC

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

NEXT STEP: REVERSE RFU FORMAT

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

NEXT STEP: REVERSE RFU FORMAT

WHAT DIDN'T WORK:

- STARING AT BINARY BLOB
- BINWALK
- COMMON FS HEADERS
- GOOGLING
- ASKING HP, FRIENDS, ADVISER, ETC

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

BRICKING THE PRINTER IS PRETTY EASY...

UNBRICKING THE PRINTER IS ALSO EASY. **HMMM...**

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

BRICKING THE PRINTER IS PRETTY EASY...

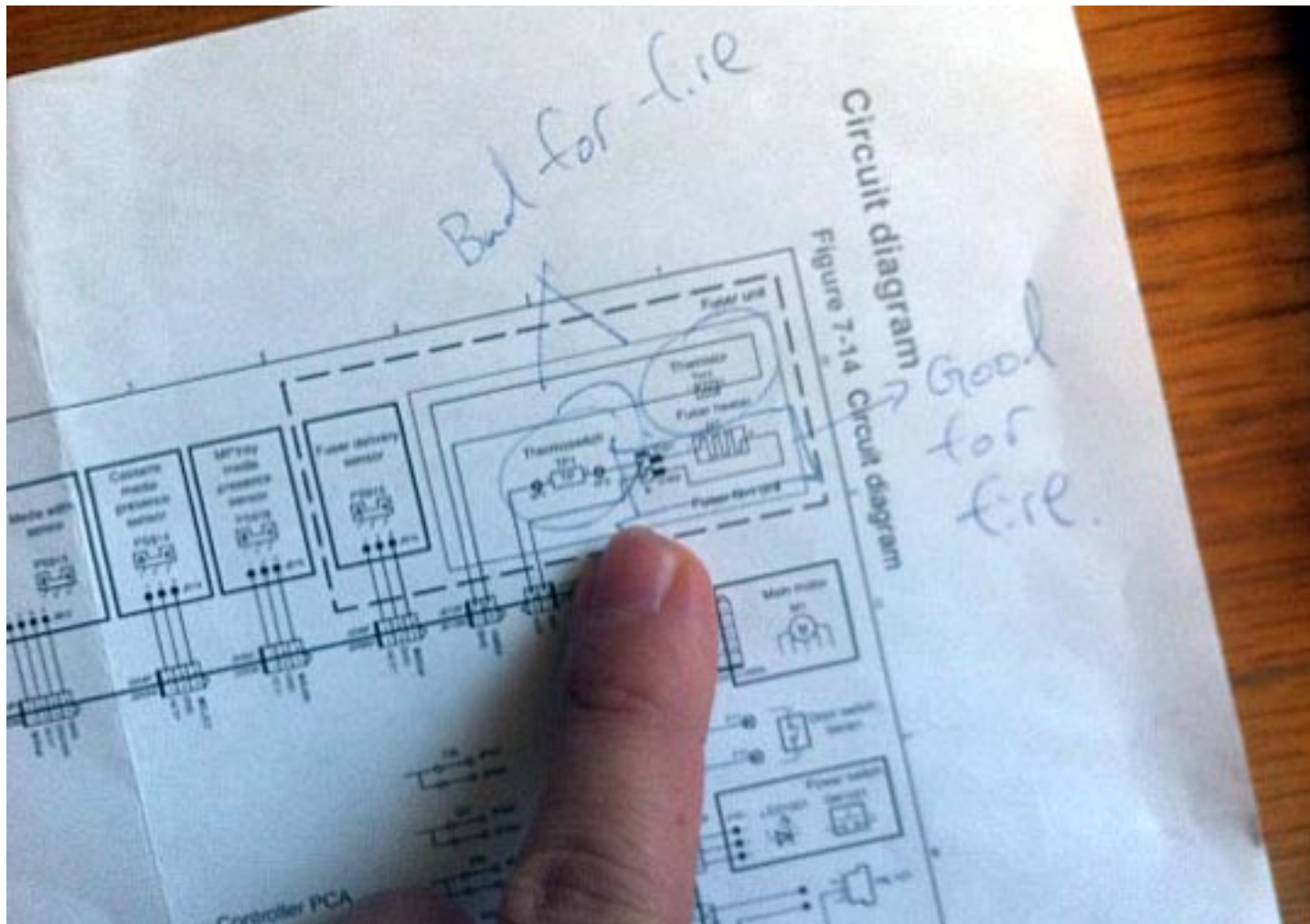
UNBRICKING THE PRINTER IS ALSO EASY. **HMMM...**

IDEA: EXTRACT BOOT CODE, REVERSE RFU PARSER

PRINT ME IF YOU DARE

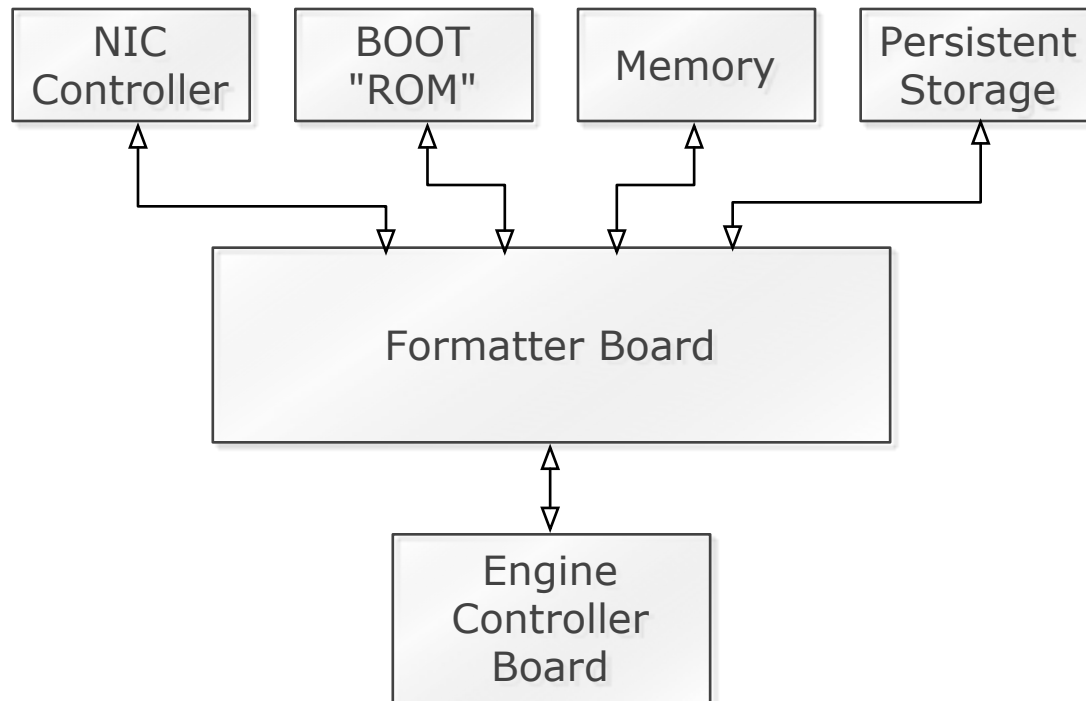
FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

NO FIRE. SRSLY GOIS! MKAY?



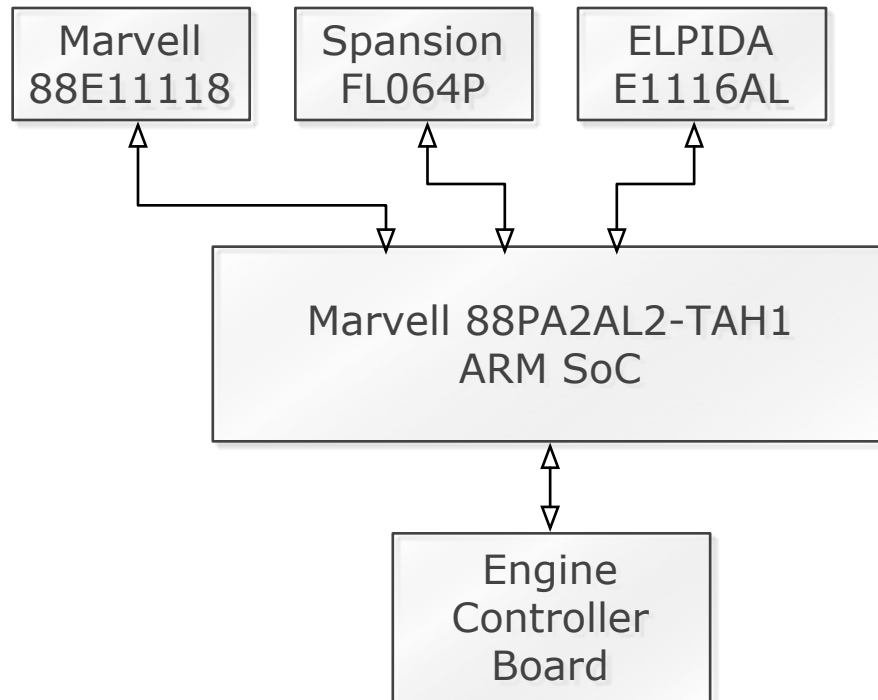
PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE



PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE



- Marvel GigE Transceiver
- Spansion SPI "ROM"
 - 64Mbit Flash Chip
- 128MB DDR2 SDRAM
- ARM SoC (NDA!)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE



2055DN Formatter Board

Main SoC Boots from
SPI-Flash

Marvell SoC (no data sheet)

SPANSION FLASH
(have datasheet!)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

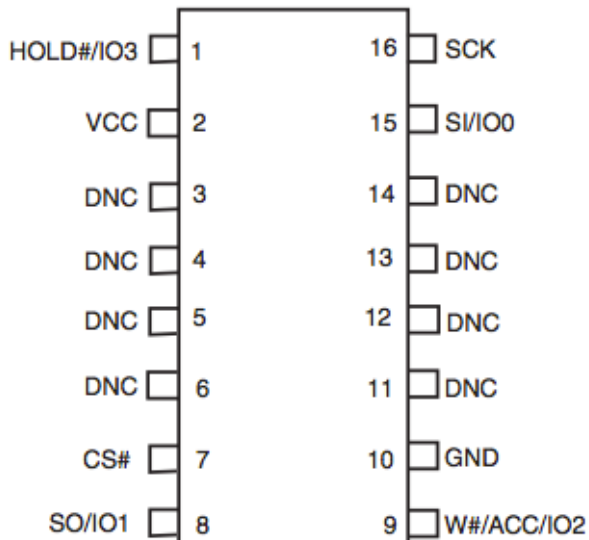
TABLE 5-11. INSTRUCTION SET

Operation	Command	One Byte Command Code	Description	Address Bytes	Mode Bit Cycle	Dummy Bytes	Data Bytes
Read	READ	(03h) 0000 0011	Read Data bytes	3	0	0	1 to ∞
	FAST_READ	(0Bh) 0000 1011	Read Data bytes at Fast Speed	3	0	1	1 to ∞
	DOR	(3Bh) 0011 1011	Dual Output Read	3	0	1	1 to ∞
	QOR	(6Bh) 0110 1011	Quad Output Read	3	0	1	1 to ∞
	DIOR	(BBh) 1011 1011	Dual I/O High Performance Read	3	1	0	1 to ∞
	QIOR	(EBh) 1110 1011	Quad I/O High Performance Read	3	1	2	1 to ∞
	RDID	(9Fh) 1001 1111	Read Identification	0	0	0	1 to 81
Write Control	READ_ID	(90h) 1001 0000	Read Manufacturer and Device Identification	3	0	0	1 to ∞
	WREN	(06h) 0000 0110	Write Enable	0	0	0	0
Erase	WRDI	(04h) 0000 0100	Write Disable	0	0	0	0
	P4E	(20h) 0010 0000	4 KB Parameter Sector Erase	3	0	0	0
	P8E	(40h) 0100 0000	8 KB (two 4 KB) Parameter Sector Erase	3	0	0	0
	SE	(D8h) 1101 1000	64 KB Sector Erase	3	0	0	0
Program	BE	(60h) 0110 0000 or (C7h) 1100 0111	Bulk Erase	0	0 0	0 0	0
	PP	(02h) 0000 0010	Page Programming	3	0	0	1 to 256
Status & Configuration Register	QPP	(32h) 0011 0010	Quad Page Programming	3	0	0	1 to 256
	RDSR	(05h) 0000 0101	Read Status Register	0	0	0	1 to ∞
	WRR	(01h) 0000 0001	Write (Status & Configuration) Registers	0	0	0	1 to 2
	RCR	(35h) 0011 0101	Read Configuration Register (CFG)	0	0	0	1 to ∞
Power Saving	CLSR	(30h) 0011 0000	Reset the Erase and Program Fail Flag (SR5 and SR6) and restore normal operation)	0	0	0	1
	DP	(B9h) 1011 1001	Deep Power-Down	0	0	0	0
	RES	(ABh) 1010 1011	Release from Deep Power-Down Mode	0	0	3	0
(ABh) 1010 1011		Release from Deep Power-Down and Read Electronic Signature	0	0	0	1 to ∞	
OTP	OTPP	(42h) 0100 0010	Programs one byte of data in OTP memory space	3	0	1	1
	OTPR	(4Bh) 0100 1011	Read data in the OTP memory space	3	0	0	1 to ∞

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

Figure 2.1 16-pin Plastic Small Outline Package (SO)

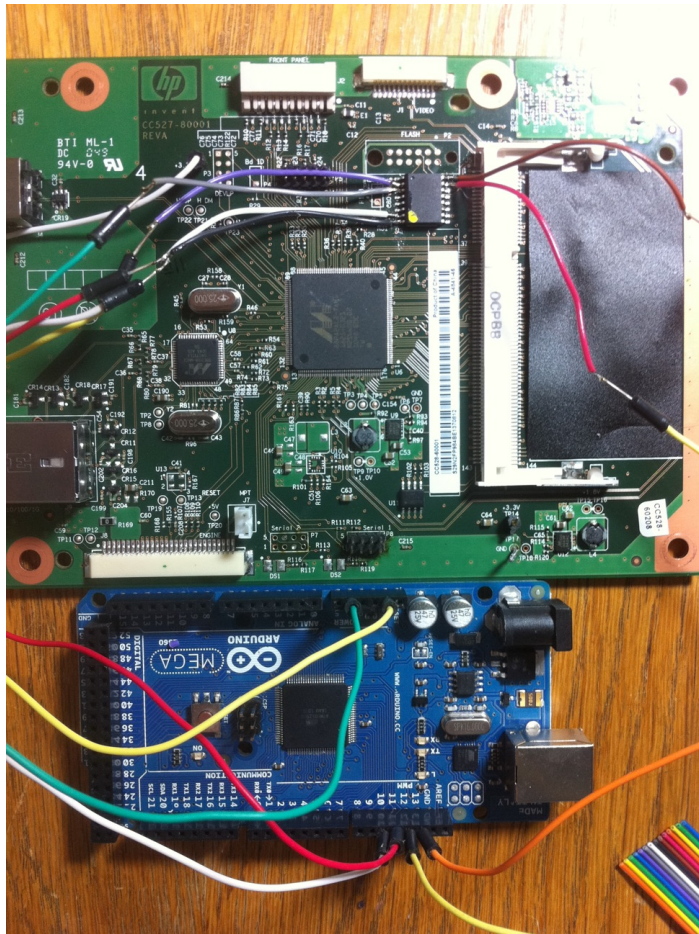


ATTEMPT ONE:

- ARDUINO SPI DUMPER
 - 40 LINES OF AVR CODE
 - SMALL PYTHON CONTROLLER PROGRAM
- MONKEY SOLDERING

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

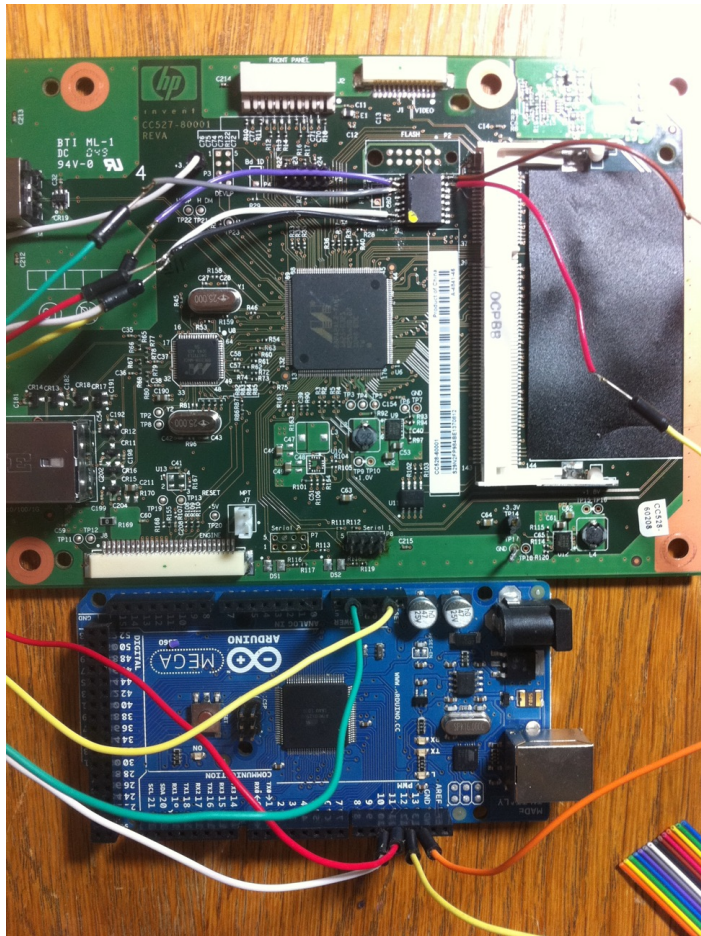


ATTEMPT ONE:

- ARDUINO SPI DUMPER
 - 40 LINES OF AVR CODE
 - SMALL PYTHON CONTROLLER PROGRAM
- MONKEY SOLDERING

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

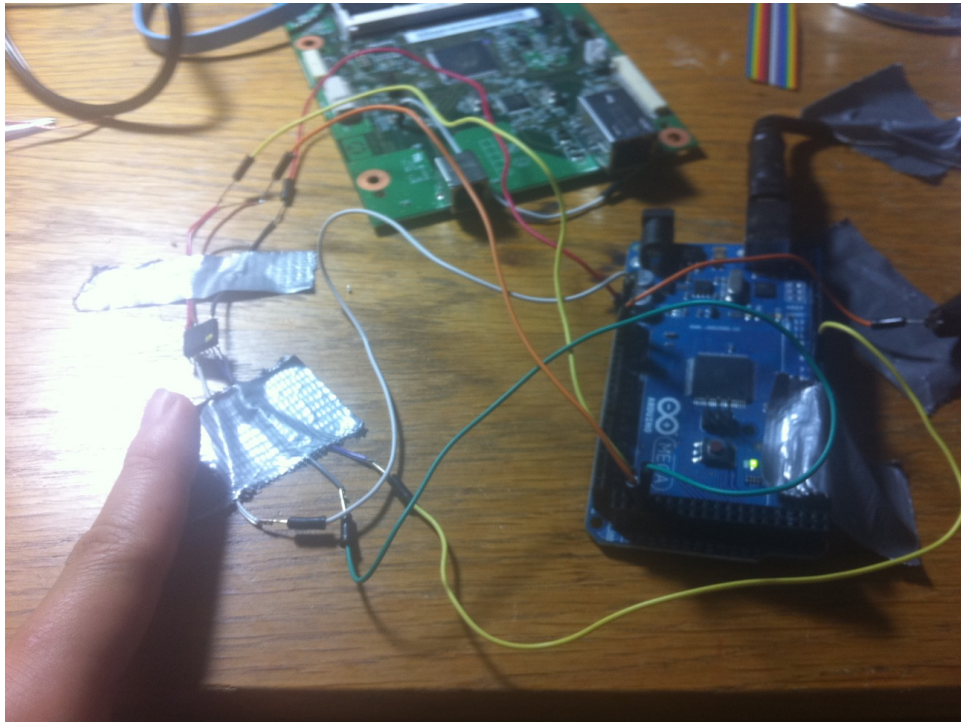


ATTEMPT ONE:

- ARDUINO SPI DUMPER
 - 40 LINES OF AVR CODE
 - SMALL PYTHON CONTROLLER PROGRAM
- MONKEY SOLDERING
- GRADE: **B-**
 - (WORKED, BUT POORLY)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE



ATTEMPT TWO:

- ARDUINO SPI DUMPER
 - 40 LINES OF AVR CODE
 - SMALL PYTHON CONTROLLER PROGRAM
- MONKEY SOLDERING
- **DUCT-TAPE**
- GRADE: **A+**

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

SPI"ROM" DUMP

```
0000002A C BootSPIROM: Starting Image. Entry @ %#x\r\n
00000029 C BootSPIROM: FAIL! imageTableIndex = %d\r\n
0000001D C Cannot start SPI ROM image\r\n
00000011 C <== BootSPIROM\r\n
00000011 C ==> BootEEPROM\r\n
00000033 C BootEEPROM: failed to read image size & checksum\r\n
0000002D C BootEEPROM: imageSize = %d, checkSum = %#x\r\n
0000002F C BootEEPROM: failed to read image from EEPROM\r\n
00000039 C BootEEPROM: invalid checksum. Should be: %#x, is: %#x\r\n
0000001C C Cannot start EEPROM image\r\n
0000000B C BOOTCODE\r\n
00000042 C FLASH 0x%x=0x%x bytes * 0x%x sectors (%x bootcode, %x reserved)\r\n
```

BOOT SPI-ROM FINDINGS:

- NOT ROM (FLASH)
- 8MB CAPACITY
- SMALL BOOT-LOADER
- FACTORY RESET RFU IMAGE (<1 MB)
- RFU PARSER IN BOOT-LOADER

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

SPI"ROM" DUMP

```
20010474 E5 9D 20 54 E5 9F 00 C4 E5 8D C0 00 E1 2F FF 34 T../4
20010484 E1 A0 00 00 EA FF FF 61 00 00 12 00 00 00 0A 60 ..a.....`
20010494 00 00 06 01 20 00 F7 58 AA 55 41 54 00 00 06 02 .... .XUAT....
200104A4 20 00 3A 38 20 01 3B D0 20 00 3B 5C 20 00 3B 70 ..:8 .;.\ .;p
200104B4 02 00 00 00 20 01 DE 14 20 00 3C 04 20 01 64 2C .... .;.<. .d,
200104C4 20 00 3C 14 20 00 3C 0C 20 00 3C 1C 20 00 F7 44 .<. .<. .<. .D
200104D4 20 01 66 20 20 00 3D 4C 00 00 06 05 20 00 3B A0 .f .=L.... .;
200104E4 20 01 64 3C 20 01 10 A0 20 00 3C 44 20 00 3C 7C .d< .. .<D .<|
200104F4 20 00 3C 74 00 00 01 99 00 00 06 04 00 00 06 03 .<t.....
20010504 20 00 3B D0 20 00 3D C4 20 01 13 44 20 00 3D F0 .; .= ..D .=
20010514 00 00 04 05 00 00 80 04 20 00 3E 1C 20 00 3E 3C .....>. .>X
20010524 00 00 06 06 20 00 3C 94 20 00 3D 88 00 00 04 04 ....< .>.....
20010534 20 00 3C 68 00 00 01 CF 00 00 01 8E 20 00 3C D4 .<h.....<
20010544 20 00 3D 18 E9 2D 4F F0 E5 9F 22 14 E2 4D D0 0C .=.-0".M.
20010554 E5 92 30 00 E1 A0 90 00 E3 13 00 02 E1 A0 70 01 0.°....p.
20010564 05 9F 82 00 1A 00 00 76 E2 89 30 04 E1 A0 38 03 .....v0.8.
20010574 E5 9F B1 F4 E5 8D 30 04 E3 A0 A0 00 E5 9F 31 E8 坂0.續.1
20010584 E1 2F FF 33 E1 A0 00 00 E1 A0 00 07 E1 A0 10 09 /3.....
20010594 E3 A0 20 04 E3 A0 30 01 E5 9F C1 D0 E1 2F FF 3C .0./<
200105A4 E1 A0 00 00 E2 50 40 00 0A 00 00 1B E5 9F 21 B0 ..P@.....l
200105B4 E5 92 30 00 E3 13 00 04 0A 00 00 05 E5 9F 01 B0 0.....
200105C4 E1 2F FF 38 E1 A0 00 00 E5 9F 01 A8 E1 2F FF 38 /8.../8
200105D4 E1 A0 00 00 E2 8A A0 01 E3 5A 00 02 9A FF FF E6 ..@.Z..
200105E4 E3 54 00 00 0A 00 00 3F E5 9F 31 74 E5 93 20 00 T.....?it .
200105F4 E5 9F 31 84 E0 02 30 03 E5 53 00 00 1A 00 00 3F 1.0.S.....?
20010604 E5 9F 01 78 E5 9F 11 78 E5 9F 21 78 E3 A0 3D 05 .x.x!x=.
20010614 E1 2F FF 38 E1 A0 00 00 EA FF FF FE E5 9F C1 40 /8..@
20010624 E1 D7 50 B0 E5 9C 30 00 E1 D7 60 B2 E3 13 00 08 P0.~...
20010634 0A 00 00 07 E5 9F 01 38 E1 2F FF 38 E1 A0 00 00 .....8/8..
20010644 FF FF 01 44 E1 A0 10 0E E1 A0 20 06 E1 2F FF 38 n /@
```

Notice the "UAT" header

Where have I **seen this before**?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

LET'S PLAY... STARE AT BINARY BLOB FTW

HP RFU (REMOTE FIRMWARE UPDATE) FILE

```
000000 40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 4D 4F 44 45 4C 3D 48 @PJL COMMENT MODEL=H
000014 50 20 4C 61 73 65 72 4A 65 74 20 50 32 30 35 35 64 6E 0A 40 P LaserJet P2055dn
000028 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 56 45 52 53 49 4F 4E 3D PJL COMMENT VERSION=
00003C 38 33 35 30 34 0A 40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 44 83504
000050 41 54 45 43 4F 44 45 3D 32 30 31 30 30 33 30 38 0A 40 50 4A ATECODE=20100308
000064 4C 20 55 50 47 52 41 44 45 20 53 49 5A 45 3D 37 39 32 39 39 L UPGRADE SIZE=79299
000078 30 36 0A 1B 25 2D 31 32 33 34 35 58 40 50 4A 4C 20 45 4E 54 06
00008C 45 52 20 4C 41 4E 47 55 41 47 45 3D 41 43 4C 0D 0A 00 AC 00 ER LANGUAGE=ACL
0000A0 0F 00 03 62 2D 00 00 00 00 00 79 00 00 AA 55 41 54 00 00 01 b- UAT
0000B4 20 00 67 FB E9 00 E2 17 03 00 00 00 00 00 67 FD 09 00 00 20 g
0000C8 E0 00 00 4D 3C 00 68 1D E9 00 00 21 86 00 00 50 91 00 68 3F M<h
0000DC 6F 00 00 20 28 00 00 4D AA 00 68 5F 97 00 00 20 BC 00 00 50 o (M h_
0000F0 0C 00 68 80 53 00 00 20 CB 00 00 4C C4 00 68 A1 1E 00 00 20 h S
000104 83 00 00 4D BF 00 68 C1 A1 00 00 20 23 00 00 4B 2A 00 68 E1 M h
000118 C4 00 00 1F E1 00 00 4B D8 00 69 01 A5 00 00 20 84 00 00 4D K i
00012C 5A 00 69 22 29 00 00 21 1D 00 00 4E 12 00 69 43 46 00 00 21 Z i")
000140 42 00 00 50 24 00 69 64 88 00 00 24 0D 00 00 54 2D 00 69 88 B P$ id
000154 95 00 00 24 35 00 00 54 C1 00 69 AC CA 00 00 23 84 00 00 50 $ T i
000168 E7 00 69 D0 4E 00 00 28 24 00 00 7A 8E 00 69 F8 72 00 00 22 i N ($ z i r
00017C CD 00 00 50 D6 00 6A 1B 3F 00 00 21 3E 00 00 52 CF 00 6A 3C P j,? > R j<
000190 7D 00 00 1F F3 00 00 4B C0 00 6A 5C 70 00 00 22 11 00 00 51 } K j\p " Q
```

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

LET'S STARE AT BINARY BLOB FTW

```
000000 40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 4D 4F 44 45 4C @PJL COMMENT MODEL
000012 3D 48 50 20 4C 61 73 65 72 4A 65 74 20 50 32 30 35 35 =HP LaserJet P2055
000024 64 6E 0A 40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 56 45 dn!P@PJL COMMENT VE
000036 52 53 49 4F 4E 3D 38 33 35 30 34 0A 40 50 4A 4C 20 43 RSION=83504!P@PJL C
000048 4F 4D 4D 45 4E 54 20 44 41 54 45 43 4F 44 45 3D 32 30 OMMENT DATECODE=20
00005A 31 30 30 33 30 38 0A 40 50 4A 4C 20 55 50 47 52 41 44 100308!P@PJL UPGRAD
00006C 45 20 53 49 5A 45 3D 37 39 32 39 39 30 36 0A 1B 25 2D E SIZE=7929906!F%
00007E 31 32 33 34 35 58 40 50 4A 4C 20 45 4E 54 45 52 20 4C 12345X@PJL ENTER L
000090 41 4E 47 55 41 47 45 3D 41 43 4C 0D 0A 00 AC 00 0F 00 ANGUAGE=ACL!F!
0000A2 03 F7 67 00 00 00 00 00 79 00 00 AA 55 41 54 00 00 01 ! g!!!!y!! UAT!!!
0000B4 20 00 67 C6 8C 00 E5 89 A8 00 00 00 00 00 67 C7 AC 00 !g !!!!!g !
0000C6 00 20 E0 00 00 4D 3C 00 67 E8 8C 00 00 21 86 00 00 50 ! !!M<!g !! !NP
0000D8 91 00 68 0A 12 00 00 20 28 00 00 4D AA 00 68 2A 3A 00 !h!F!!! (!M !h*:!
0000EA 00 20 BC 00 00 50 0C 00 68 4A F6 00 00 20 CB 00 00 4C ! !!PF!hJ !! !!L
0000FC C4 00 68 6B C1 00 00 20 83 00 00 4D BF 00 68 8C 44 00 !hk !! !!M !h D!
00010E 00 20 23 00 00 4B 2A 00 68 AC 67 00 00 1F E1 00 00 4B ! #!K*!h g!!! !K
000120 D8 00 68 CC 48 00 00 20 84 00 00 4D 5A 00 68 EC CC 00 !h H!!! !MZ!h !
000132 00 21 1D 00 00 4E 12 00 69 0D E9 00 00 21 42 00 00 50 !!!!!N!!!i% !!!B!NP
```

7929906
=
0x790032H

BOOTSPIROM: READS IMAGE SIZE AND CHECKSUM

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

LET'S STARE AT BINARY BLOB FTW

```
000000 40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 4D 4F 44 45 4C @PJL COMMENT MODEL
000012 3D 48 50 20 4C 61 73 65 72 4A 65 74 20 50 32 30 35 35 =HP LaserJet P2055
000024 64 6E 0A 40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 56 45 dn!P@PJL COMMENT VE
000036 52 53 49 4F 4E 3D 38 33 35 30 34 0A 40 50 4A 4C 20 43 RSION=83504!P@PJL C
000048 4F 4D 4D 45 4E 54 20 44 41 54 45 43 4F 44 45 3D 32 30 OMMENT DATECODE=20
00005A 31 30 30 33 30 38 0A 40 50 4A 4C 20 55 50 47 52 41 44 100308!P@PJL UPGRAD
00006C 45 20 53 49 5A 45 3D 37 39 32 39 39 30 36 0A 1B 25 2D E SIZE=7929906!F%
00007E 31 32 33 34 35 58 40 50 4A 4C 20 45 4E 54 45 52 20 4C 12345X@PJL ENTER L
000090 41 4E 47 55 41 47 45 3D 41 43 4C 0D 0A 00 AC 00 0F 00 ANGUAGE=ACL!F!
0000A2 03 F7 67 00 00 00 00 00 79 00 00 AA 55 41 54 00 00 01 ! g!!!!y!! UAT!!!
0000B4 20 00 67 C6 8C 00 E5 89 A8 00 00 00 00 00 67 C7 AC 00 !g !!!!!g !
0000C6 00 20 E0 00 00 4D 3C 00 67 E8 8C 00 00 21 86 00 00 50 ! !M<!g !! !P
0000D8 91 00 68 0A 12 00 00 20 28 00 00 4D AA 00 68 2A 3A 00 !h!F!!! (!M !h*!!
0000EA 00 20 BC 00 00 50 0C 00 68 4A F6 00 00 20 CB 00 00 4C ! !PF!hJ !! !L
0000FC C4 00 68 6B C1 00 00 20 83 00 00 4D BF 00 68 8C 44 00 !hk !! !M !h D!
00010E 00 20 23 00 00 4B 2A 00 68 AC 67 00 00 1F E1 00 00 4B ! #!K*!h g!!! !K
000120 D8 00 68 CC 48 00 00 20 84 00 00 4D 5A 00 68 EC CC 00 !h H!! !MZ!h !
000132 00 21 1D 00 00 4E 12 00 69 0D E9 00 00 21 42 00 00 50 !!!!!N!!!i% !!!B!P
```

7929906
=
0x790032H

Shift for alignment

Hrm....

BOOTSPIROM: READS IMAGE SIZE AND CHECKSUM

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

LET'S STARE AT BINARY BLOB FTW

Type	Value
8 bit signed	
0 bit unsigned	
Hex	Big Endian Overwrite
Offset: 32 Selection: 0	

7929906

=

0x790032H

0x32 bytes header
Payload starts with
"0xAA554154"

Shift again
For alignment

BOOTSPIROM: READS IMAGE SIZE AND CHECKSUM

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

LET'S STARE AT BINARY BLOB FTW

```
000000 00 AC 00 0F 00 03 F7 67 00 00 00 00 00 79 00 00 AA 55  \ \ \ \ g \ \ \ \ y \ \ \ U
000012 41 54 00 00 01 20 00 67 C6 8C 00 E5 89 A8 00 00 00 00  AT \ \ \ \ g \ \ \ \ \ \ \ \
000024 00 67 C7 AC 00 00 20 E0 00 00 4D 3C 00 67 E8 8C 00 00  \g \ \ \ \ \M< \g \ \
000036 21 86 00 00 50 91 00 68 0A 12 00 00 20 28 00 00 4D AA  ! \ \P \h \f \ \ \ \ ( \ \M
000048 00 68 2A 3A 00 00 20 BC 00 00 50 0C 00 68 4A F6 00 00  \h * : \ \ \ \ \P \h J \ \
00005A 20 CB 00 00 4C C4 00 68 6B C1 00 00 20 83 00 00 4D BF  \ \L \hk \ \ \ \ \M
00006C 00 68 8C 44 00 00 20 23 00 00 4B 2A 00 68 AC 67 00 00  \h D \ \ \ # \k * \h g \ \
00007E 1F E1 00 00 4B D8 00 68 CC 48 00 00 20 84 00 00 4D 5A  \ \ \K \h H \ \ \ \ \MZ
000090 00 68 EC CC 00 00 21 1D 00 00 4E 12 00 69 0D E9 00 00  \h \ \ \ ! \ \ \ \ N \ \ \ i % \ \
0000A2 21 42 00 00 50 24 00 69 2F 2B 00 00 24 0D 00 00 54 2D  !B \ \P $ \ \ i / + \ \ $ % \ \ T -
0000B4 00 69 53 38 00 00 24 35 00 00 54 C1 00 69 77 6D 00 00  \i S8 \ \ $ % \ \ T \ \ i w m \ \
0000C6 23 84 00 00 50 E7 00 69 9A F1 00 00 28 24 00 00 7A 8E  # \ \P \ \ i \ \ \ \ \ ($ \ \ z
0000D8 00 69 C3 15 00 00 22 CD 00 00 50 D6 00 69 E5 E2 00 00  \i \ \ \ \ " \ \ \P \ \ i \ \
0000EA 21 3E 00 00 52 CF 00 6A 07 20 00 00 1F F3 00 00 4B C0  !> \ \R \ \ j \ \ \ \ \ \K
```

Hmmm

Looks like

[]
[start addr]
[end addr]
[UAT]
[payload]
[payload]
[.....]

BOOTSPIROM: READS IMAGE SIZE AND CHECKSUM

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

WILL NOT REVEAL CHECKSUM SPECIFICS, BUT...

I STARED, I WON.

IF YOU STARE, YOU PROBABLY WILL WIN TOO...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

SECURITY ANALYSIS

```
.. 0000002F    C    VerifyUSBID: NO MATCH, was %s, should be: %s\r\n
.. 0000003D    C    VerifyUSBID: NO MATCH, USBID sent: %s, USBID should be: %s\r\n
.. 0000004E    C    VerifyFWKey: NVRAM Key: 0x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x...
.. 0000004E    C    VerifyFWKey: Sent Key: 0x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x...
.. 0000003D    C    VerifyFWKey: NO MATCH at byte %d - NVRAM:0x%2x Sent:0x%2x \r\n
.. 00000039    C    VerifyFWKey: Super Secret Bypass of Crypto-Key enabled\r\n
.. 0000005B    C    VerifyPlatformID: ERROR: Invalid ID info version. Should be %d, %d, %d or %d, sent: %d.\...
.. 0000002A    C    ACLBurnFlash: dataLen = %d, offset = %d\r\n
.. 0000002C    C    ACLBurnFlash: Downloading %d bytes to %#x\r\n
.. 0000002D    C    ACLBurnFlash: Boot bank %d, Target bank %d\r\n
.. 00000039    C    ACLBurnFlash: FLASH sector size 0x%x (%x boot sectors)\r\n
```

HRM...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

RFU CONTENT OBSERVATIONS:

- SPECIFIC VERSION OF COMPRESSION LIBRARY HAS
KNOWN ARB-CODE EXECUTION VULNERABILITY.

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

RFU CONTENT OBSERVATIONS:

- SPECIFIC VERSION OF COMPRESSION LIBRARY HAS KNOWN ARB-CODE EXECUTION VULNERABILITY.
- NO MEMORY SPACE SEPARATION
- NO KERNEL-LEVEL SECURITY
- EVERYTHING RUNS AS SUPERVISOR MODE ON CPU
- ANY VULNERABILITY IN ANY (UNPRIVILEGED) CODE WILL LEAD TO FULL COMPROMISE

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

RFU CONTENT OBSERVATIONS:

- SPECIFIC VERSION OF COMPRESSION LIBRARY HAS KNOWN ARB-CODE EXECUTION VULNERABILITY.
- NO MEMORY SPACE SEPARATION
- NO KERNEL-LEVEL SECURITY
- EVERYTHING RUNS AS SUPERVISOR MODE ON CPU
- ANY VULNERABILITY IN ANY (UNPRIVILEGED) CODE WILL LEAD TO FULL COMPROMISE
- BUT THERE IS NO NEED BECAUSE OF THE RFU VULNERABILITY...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

CRAFTING POC ATTACK

- WROTE RFU PACKER (200 LINES OF PYTHON)

```
dyn-168-39-148-169:newfirmware ang$ wc -l packfirmware.py
    200 packfirmware.py
dyn-168-39-148-169:newfirmware ang$ wc -l packfirmware-unittest.py
    48 packfirmware-unittest.py
```

I EVEN WROTE **UNITTESTS!**

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

WRITING VXWORKS ROOTKIT:

- ~3KB OF ARM ASSEMBLY
- PRINT-JOB INTERCEPTOR
- REVERSE IP PROXY
- DEBUG-MESSAGE REDIRECTION (CONSOLE TO TELNET)
- ENGINE-CONTROL CONTROLLER (CAUSE PAPER JAMS, ETC)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

CRAFTING POC ATTACK

- WROTE RFU PACKER (200 LINES OF PYTHON)
 - INPUT: ARBITRARY ELF BINARY
 - OUTPUT: SINGLE PJI COMMAND

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

CRAFTING POC ATTACK

- WROTE RFU PACKER (200 LINES OF PYTHON)
 - INPUT: ARBITRARY ELF BINARY
 - OUTPUT: SINGLE PJI COMMAND
- REWORKED SYMBIOTE TOOL-SET
 - CROSS-COMPILE MALWARE CODE
 - INJECT FUNCTION HOOKS
- INPUT: UNPACKED 2055DN VxWORKS IMAGE
- OUTPUT: MALWARE-INJECTED VxWORKS IMAGE

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE























POC TIME!

WRITING VXWORKS ROOTKIT:

SOCKETLIB WAS A LITTLE TRICKY TO FIND, BUT...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

 .PARISJDImerged_pre.elf.rodata:014803B4	00000012	C	sockapi/trclose.c
 .PARISJDImerged_pre.elf.rodata:014803C8	00000006	C	close
 .PARISJDImerged_pre.elf.rodata:014803D0	00000008	C	tfClose
 .PARISJDImerged_pre.elf.rodata:014803D8	0000001B	C	socket has wrong ownership
 .PARISJDImerged_pre.elf.rodata:014803F4	00000022	C	Could not delete socket from tree
 .PARISJDImerged_pre.elf.rodata:01480418	00000023	C	assertion error line %d, file(%s)\n
 .PARISJDImerged_pre.elf.rodata:0148043C	00000011	C	sockapi/trconn.c
 .PARISJDImerged_pre.elf.rodata:01480450	00000008	C	connect
 .PARISJDImerged_pre.elf.rodata:01480468	00000023	C	assertion error line %d, file(%s)\n
 .PARISJDImerged_pre.elf.rodata:0148048C	00000012	C	sockapi/trioctl.c
 .PARISJDImerged_pre.elf.rodata:014804A0	00000008	C	tfioctl
 .PARISJDImerged_pre.elf.rodata:014804A8	00000023	C	assertion error line %d, file(%s)\n
 .PARISJDImerged_pre.elf.rodata:014804CC	00000013	C	sockapi/trlisten.c
 .PARISJDImerged_pre.elf.rodata:014804E0	00000007	C	listen
 .PARISJDImerged_pre.elf.rodata:014804E8	00000023	C	assertion error line %d, file(%s)\n
 .PARISJDImerged_pre.elf.rodata:0148050C	00000011	C	sockapi/trrecv.c
 .PARISJDImerged_pre.elf.rodata:01480520	00000005	C	recv
 .PARISJDImerged_pre.elf.rodata:01480528	00000023	C	assertion error line %d, file(%s)\n
 .PARISJDImerged_pre.elf.rodata:0148054C	00000013	C	sockapi/trrecvfr.c
 .PARISJDImerged_pre.elf.rodata:01480560	00000009	C	recvfrom
 .PARISJDImerged_pre.elf.rodata:0148056C	00000023	C	assertion error line %d, file(%s)\n
 .PARISJDImerged_pre.elf.rodata:01480590	00000011	C	sockapi/trsend.c

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

MYSTERY PROGRAMMER, YOU ARE **AWESOME!**

```
's' .PARISJDImerged_pre.elf.rodata:013DEE30 0000001F C   DBG_OUTPUT [0x%08X] = 0x%08X;\n's' .PARISJDImerged_pre.elf.rodata:013DEE50 00000016 C   ejd Command options:\n's' .PARISJDImerged_pre.elf.rodata:013DEE68 00000036 C     ejd ksh - Routes serial input to EJD ksh console\n's' .PARISJDImerged_pre.elf.rodata:013DEEA4 0000003E C     \nSerial port input now re-directed to JetDirectInside parser\n's' .PARISJDImerged_pre.elf.rodata:013DEEE4 00000041 C     Type 'quit' to redirect serial port back to PARIS debug console\n's' .PARISJDImerged_pre.elf.rodata:013DEF28 00000042 C     DO NOT TYPE 'plugh' - you will end up at inside a small building\n's' .PARISJDImerged_pre.elf.rodata:013DEF6C 00000022 C     with some keys on the ground ...\n's' .PARISJDImerged_pre.elf.rodata:013DEF90 00000010 C     state options:\n's' .PARISJDImerged_pre.elf.rodata:013DEFA0 00000032 C     all - print all accessible state information\n-----
```

LOTS OF OTHER JUICY INFO IN THE UNPACKED IMAGE...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

TECHNICAL DETAILS: MALWARE-INJECTED RFU BUILD PROCESS

- CROSS-COMPILE HOOKS AND PAYLOAD

Builds in OS X

Prereq: arm-elf tool chain
python

```
dyn-209-2-210-2:rootkit ang$ cat Makefile
ARM_AS=/usr/local/arm/bin/arm-elf-as
CARVEBIN=../../src/CarveBin.py
SLICENDICE=../../src/SliceNDice.py

clean:
    rm *.o

assemble:
    ${ARM_AS} -EB -k test.as -o test.o
    ${ARM_AS} -EB -k hook.as -o hook.o
    ${ARM_AS} -EB -k hook_paris.as -o hook_paris.o
    ${ARM_AS} -EB -k hook_snipsnip.as -o hook_snipsnip.o
    ${ARM_AS} -EB -k hook_snipsnip_syslog.as -o hook_snipsnip_syslog.o
    ${ARM_AS} -EB -k hook_snipsnip_icmp.as -o hook_snipsnip_icmp.o
    ${ARM_AS} -EB -k hook_snipsnip_icmp2.as -o hook_snipsnip_icmp2.o
    ${ARM_AS} -EB -k hook_snipsnip_ipv4.as -o hook_snipsnip_ipv4.o
    ${ARM_AS} -EB -k hook_printf.as -o hook_printf.o
    ${ARM_AS} -EB -k hook_icmp.as -o hook_icmp.o
    ${ARM_AS} -EB -k hook_printlog.as -o hook_printlog.o
    ${ARM_AS} -EB -k hook_printintercept.as -o hook_printintercept.o

    ${ARM_AS} -EB -k payload.as -o payload.o
    arm-elf-ld -Ttext 0x15a670c -EB -s payload.o -o payload-linked.o
```

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

TECHNICAL DETAILS: MALWARE-INJECTED RFU BUILD PROCESS

- CROSS-COMPILE HOOKS AND PAYLOAD
- INJECT BINARY INTO UNPACKED VXWORKS IMAGE

```
python ${CARVEBIN} hook1.o
python ${CARVEBIN} print-linked.o
python ${CARVEBIN} printlog-linked.o

slicendice: carvebin
python ${SLICENDICE} uncompressed-0-template uncompressed-0-instance

install: slicendice
cp uncompressed-0-instance ../newfirmware/outbound/uncompressed-0

all: assemble carvebin slicendice install
```


PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

TECHNICAL DETAILS: MALWARE-INJECTED RFU BUILD PROCESS

- CROSS-COMPILE HOOKS AND PAYLOAD
- INJECT BINARY INTO UNPACKED VXWORKS IMAGE
- RUN PACKER WITH ALTERED VXWORKS IMAGE

```
dyn-209-2-210-2:newfirmware ang$ cat Makefile
all:
    python packfirmware.py final-firmware-tramp
    lpr final-firmware-tramp.rfu
```

(AND PRINT TO **PWN**)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

TECHNICAL DETAILS: MALWARE-INJECTED RFU BUILD PROCESS

- POC CODE -> INSIDE A NEW RWX ELF SEGMENT

```
addsection:  
./arm/bin/arm-elf-objcopy -v --add-section .launchpad=newsection --change-section-address
```

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

POC TIME!

TECHNICAL DETAILS: MALWARE-INJECTED RFU BUILD PROCESS

- POC CODE -> INSIDE A NEW RWX ELF SEGMENT

```
addsection:  
./arm/bin/arm-elf-objcopy -v --add-section .launchpad=newsection --change-section-address
```

- CROSS-COMPILE WITH THE RIGHT MEMORY OFFSET...

```
`${ARM_AS}` -EB -k control_tasktest.as -o control_tasktest.o  
arm-elf-ld -Ttext 0x15CBFF0 -EB -s control_tasktest.o -o control_tasktest-linked.o
```

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

DEMO

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE



WE

SACRIFICE
TO THE

DEMO GODS

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

PUTTING POC TOGETHER

OBVIOUS ATTACK VECTORS

- **ACTIVE:** DIRECTLY CONNECT TO 9100/TCP OF TARGET PRINTER
- **REFLEXIVE:** EMBED RFU IN DOCUMENT, AND USE CUPS

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

ACTIVE ATTACK:

While HP has identified a potential security vulnerability with some HP LaserJet printers, no customer has reported unauthorized access. The specific vulnerability exists for some HP LaserJet devices if placed on a public internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade.

SO WHO LEAVES THEIR PRINTERS ON THE INTERNET?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

ACTIVE ATTACK:

While HP has identified a potential security vulnerability with some HP LaserJet printers, no customer has reported unauthorized access. The specific vulnerability exists for some HP LaserJet devices if placed on a public internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade.

SO WHO LEAVES THEIR PRINTERS ON THE INTERNET?

75,000 Vulnerable Printers Online

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

FUN STATS GATHERED BY OUR VULNERABLE EMBEDDED DEVICE SCANNER

- TOTAL VULNERABLE PRINTER COUNT: 76,995

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

FUN STATS GATHERED BY OUR VULNERABLE EMBEDDED DEVICE SCANNER

- TOTAL VULNERABLE PRINTER COUNT: 76,995
- GOVERNMENT PRINTER COUNT: 43, 16 IN THE US

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

FUN STATS GATHERED BY OUR VULNERABLE EMBEDDED DEVICE SCANNER

- TOTAL VULNERABLE PRINTER COUNT: 76,995
- GOVERNMENT PRINTER COUNT: 43, 16 IN THE US
- PRINTERS NAMED “PAYROLL”: 9, ALL EDU’S

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

ACTIVE ATTACK:

While HP has identified a potential security vulnerability with some HP LaserJet printers, no customer has reported unauthorized access. The specific vulnerability exists for some HP LaserJet devices if placed on a public internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade.

DOES THE ACTIVE ATTACK WORK ON WINDOWS?

I have a funny story in my backup slides...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

REFLEXIVE ATTACK:

HP also highlighted the fact that all of its printers from 2009 onwards include digital signing to prevent this type of exploit, but the researchers said that still leaves tens of millions of devices vulnerable.

The security flaw on the pre-2009 machines allows hackers to send customised firmware to a printer that could enable them to render a user's printer useless, waste toner or overheat the device.

WRONG! 2009 DOESN'T MEAN WHAT YOU THINK IT MEANS
(AND APPARENTLY HP NEVER SAID 2009)

Source: <http://www.computerweekly.com/news/2240111721/Pre-2009-HP-printers-vulnerable-to-hackers-say-researchers>

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

REFLEXIVE ATTACK:

HP also highlighted the fact that all of its printers from 2009 onwards include digital signing to prevent this type of exploit, but the researchers said that still leaves tens of millions of devices vulnerable.

The security flaw on the pre-2009 machines allows hackers to send customised firmware to a printer that could enable them to render a user's printer useless, waste toner or overheat the device.

HOW MANY LASERJET UNITS DID HP SHIP IN 2005-NOW?

Source: <http://www.computerweekly.com/news/2240111721/Pre-2009-HP-printers-vulnerable-to-hackers-say-researchers>

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

REFLEXIVE ATTACK:

HP also highlighted the fact that all of its printers from 2009 onwards include digital signing to prevent this type of exploit, but the researchers said that still leaves tens of millions of devices vulnerable.

The security flaw on the pre-2009 machines allows hackers to send customised firmware to a printer that could enable them to render a user's printer useless, waste toner or overheat the device.

HOW MANY LASERJET UNITS DID HP SHIP IN 2005-NOW?

HAVE YOU USED ONE THIS YEAR? (PROBABLY)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REFLEXIVE PS ATTACK

000000	25 21 50 53	2D 41 64 6F	62 65 2D 33	2E 30 0A 25	41 50 4C 5F	44 53 43 5F	45 6E 63 6F	%!PS-Adobe-3.0%APL_DSC_Encoding: UTF8%APLProducer: (Version 10.6.8 (Build 10K549) Quartz PS Context)%Title: (Unknown)%Creator: (Unknown)%CreationDate: (Unknown)%For: (Unknown)%DocumentData: Clean7Bit%LanguageLevel: 2%PageOrder: Special%RBINumCopies: 1%Pages: (attend)%BoundingBox: (attend)%EndComments%BeginProlog%BeginFile: cg-pdf.ps%Copyright: Copyright 2000-2004 Apple Computer Incorporated.%Copyright: All Rights Reserved.%currentpacking true setpacking%cg_md 141 dict def%cg_md begin%L3? language level 3 ge def%bd{bind def} bind def%ld{load def}bd%xs {exch store}bd%xd{exch def} bd%cmmtx matrix def%mark% s
00001C	64 69 6E 67	3A 20 55 54	46 38 0A 25	41 50 4C 50	72 6F 64 75	63 65 72 3A	20 28 56 65	
000038	72 73 69 6F	6E 20 31 30	2E 36 2E 38	20 28 42 75	69 6C 64 20	31 30 4B 35	34 39 29 20	
000054	51 75 61 72	74 7A 20 50	53 20 43 6F	6E 74 65 78	74 29 0A 25	25 54 69 74	6C 65 3A 20	
000070	28 55 6E 6B	6E 6F 77 6E	29 0A 25 25	43 72 65 61	74 6F 72 3A	20 28 55 6E	6B 6E 6F 77	
00008C	6E 29 0A 25	25 43 72 65	61 74 69 6F	6E 44 61 74	65 3A 20 28	55 6E 6B 6E	6F 77 6E 29	
0000A8	0A 25 25 46	6F 72 3A 20	28 55 6E 6B	6E 6F 77 6E	29 0A 25 25	44 6F 63 75	6D 65 6E 74	
0000C4	44 61 74 61	3A 20 43 6C	65 61 6E 37	42 69 74 0A	25 25 4C 61	6E 67 75 61	67 65 4C 65	
0000E0	76 65 6C 3A	20 32 0A 25	25 50 61 67	65 4F 72 64	65 72 3A 20	53 70 65 63	69 61 6C 0A	
0000FC	25 52 42 49	4E 75 6D 43	6F 70 69 65	73 3A 20 31	0A 25 25 50	61 67 65 73	3A 20 28 61	
000118	74 65 6E 64	29 0A 25 25	42 6F 75 6E	64 69 6E 67	42 6F 78 3A	20 28 61 74	65 6E 64 29	
000134	0A 25 25 45	6E 64 43 6F	6D 6D 65 6E	74 73 0A 25	25 42 65 67	69 6E 50 72	6F 6C 6F 67	
000150	0A 25 25 42	65 67 69 6E	46 69 6C 65	3A 20 63 67	2D 70 64 66	2E 70 73 0A	25 25 43 6F	
00016C	70 79 72 69	67 68 74 3A	20 43 6F 70	79 72 69 67	68 74 20 32	30 30 30 2D	32 30 30 34	
000188	20 41 70 70	6C 65 20 43	6F 6D 70 75	74 65 72 20	49 6E 63 6F	72 70 6F 72	61 74 65 64	
0001A4	2E 0A 25 25	43 6F 70 79	72 69 67 68	74 3A 20 41	6C 6C 20 52	69 67 68 74	73 20 52 65	
0001C0	73 65 72 76	65 64 2E 0A	63 75 72 72	65 6E 74 70	61 63 6B 69	6E 67 20 74	72 75 65 20	
0001DC	73 65 74 70	61 63 6B 69	6E 67 0A 2F	63 67 5F 6D	64 20 31 34	31 20 64 69	63 74 20 64	
0001F8	65 66 0A 63	67 5F 6D 64	20 62 65 67	69 6E 0A 2F	4C 33 3F 20	6C 61 6E 67	75 61 67 65	
000214	6C 65 76 65	6C 20 33 20	67 65 20 64	65 66 0A 2F	62 64 7B 62	69 6E 64 20	64 65 66 7D	
000230	62 69 6E 64	20 64 65 66	0A 2F 6C 64	7B 6C 6F 61	64 20 64 65	66 7D 62 64	0A 2F 78 73	
00024C	7B 65 78 63	68 20 73 74	6F 72 65 7D	62 64 0A 2F	78 64 7B 65	78 63 68 20	64 65 66 7D	
000268	62 64 0A 2F	63 6D 6D 74	78 20 6D 61	74 72 69 78	20 64 65 66	0A 6D 61 72	6B 0A 2F 73	

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REFLEXIVE PS ATTACK

007FA4	35 35 30 20	34 2E 32 34	32 35 34 39	20 36 2E 30	36 31 30 39	36 20 34 2E	38 34 38 30	550 4.242549	6.061096	4.8480
007FC0	30 34 20 37	2E 39 30 35	38 32 35 20	34 2E 32 34	32 35 34 39	20 36 2E 30	36 31 30 39	04 7.905825	4.242549	6.06109
007FDC	36 20 33 2E	30 33 30 35	34 38 20 36	2E 30 36 31	30 39 36 20	30 2E 30 30	30 30 30 30	6 3.030548	6.061096	0.000000
007FF8	20 5D 20 78	53 0A 33 30	32 2E 33 39	38 30 31 20	39 32 2E 39	35 30 39 39	36 20 6D 0A] xStf302.39801	92.950996	mF
008014	28 2B 29 73	0A 65 70 0A	65 6E 64 0A	25 25 54 72	61 69 6C 65	72 0A 25 25	45 4F 4A 0D	(+)s!ep!end!%Trailer!%EOJ%		
008030	0A 1B 25 2D	31 32 33 34	35 0D 0A 1B	25 2D 31 32	33 34 35 58	40 50 4A 4C	20 45 4E 54	!%~12345!%~12345X@PJL ENT		
00804C	45 52 20 4C	41 4E 47 55	41 47 45 3D	41 43 4C 0D	0A 00 AC 00	0F 00 03 D7	9F 00 00 00	ER LANGUAGE=ACL%f	!!!	!!!
008068	00 00 79 00	00 AA 55 41	54 00 00 01	20 00 67 B2	F1 00 E2 17	03 00 00 00	00 00 67 B4	!y! UAT! !g	! !!!!!g	
008084	11 00 00 20	E0 00 00 4D	3C 00 67 D4	F1 00 00 21	86 00 00 50	91 00 67 F6	77 00 00 20	! !M<g ! ! !P !g w!		
0080A0	28 00 00 4D	AA 00 68 16	9F 00 00 20	BC 00 00 50	0C 00 68 37	5B 00 00 20	CB 00 00 4C	(!M !h! ! !P!h7[! ! !L		
0080BC	C4 00 68 58	26 00 00 20	83 00 00 4D	BF 00 68 78	A9 00 00 20	23 00 00 4B	2A 00 68 98	!hX&! !M !hx ! ! #!K*!h		
0080D8	CC 00 00 1F	E1 00 00 4B	D8 00 68 B8	AD 00 00 20	84 00 00 4D	5A 00 68 D9	31 00 00 21	! !K !h ! ! !MZ!h 1! ! !		
0080F4	1D 00 00 4E	12 00 68 FA	4E 00 00 21	42 00 00 50	24 00 69 1B	90 00 00 24	0D 00 00 54	! !N!h N! !B!P!\$!i. ! \$! !T		
008110	2D 00 69 3F	9D 00 00 24	35 00 00 54	C1 00 69 63	D2 00 00 23	84 00 00 50	E7 00 69 87	-!i? ! \$! !T !ic ! ! # !P !i		
00812C	56 00 00 28	24 00 00 7A	8E 00 69 AF	7A 00 00 22	CD 00 00 50	D6 00 69 D2	47 00 00 21	V! !(\$!z !i z! ! " !P !i G! !		
008148	3E 00 00 52	CF 00 69 F3	85 00 00 1F	F3 00 00 4B	C0 00 6A 13	78 00 00 22	11 00 00 51	>!R !i ! ! !K !j!x! ! " ! !Q		
008164	FD 00 6A 35	89 00 00 22	90 00 00 51	68 00 6A 58	19 00 00 22	7C 00 00 50	91 00 6A 7A	!j5 ! ! " ! !Qh!jX! ! ! !P !jz		
008180	95 00 00 24	F0 00 00 55	9D 00 00 00	00 78 9C BC	7D 0D 7C 54	C5 D5 F7 DC	FD CA 26 04	! \$! !U ! ! ! !x } ! !T & !		
00819C	B8 21 41 23	06 58 20 6A	D4 28 37 10	35 2A D6 05	A1 22 62 5C	04 15 95 6A	B4 68 A9 D2	!A#X j (7!5* \ "b\ ! ! j h		
0081B8	1A 2B B6 B4	8F AD 0B 09	10 30 AB E1	1B 91 B8 AB	62 A5 96 B6	51 D1 52 45	5D 84 56 AA	+ %! !0 . b Q RE] V		
0081D4	A4 82 A2 55	2B B2 1F 4C	89 2C 6A 54	AC D4 52 F6	FD 9F 33 73	93 9B 10 6C	7D 9F F7 F7	U+ !L ,jT R 3s ! !}		
0081F0	E6 C7 B0 F7	CE C7 99 39	67 66 CE 9C	39 73 E6 DC	7B C6 4D FC	B6 E1 32 6E	14 F6 9F 4B	9gf 9s { M 2n! K		

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

THIS APPLIES TO HP P2030/P2050 MODELS

- (MANY) OTHER MODELS VULNERABLE
- AT LEAST 3 OTHER (UNSIGNED) RFU FORMATS
- PRINTERS RUNNING LYNXOS, VXWORKS, ETC HAVE SLIGHTLY DIFFERENT RFU FORMATS
- ATTACK VECTORS THE SAME
- RFU FORMATS ARE SLIGHTLY DIFFERENT
 - JUST REPEAT THE SAME EXERCISE!

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

Printer Model	ISA	Operating System
2055	ARM	VxWorks
2030	ARM	VxWorks
2410	MIPS	LynxOS
24x0	MIPS	LynxOS
3000	MIPS	LynxOS
3800	MIPS	LynxOS
4005	MIPS	LynxOS
4100	MIPS	LynxOS
4240	MIPS	LynxOS

Printer Model	ISA	Operating System
5025	MIPS	LynxOS
5035	MIPS	LynxOS
3505	PowerPC!	LynxOS
4250	MIPS	LynxOS
4345	MIPS	LynxOS
4350	MIPS	LynxOS
4600	MIPS	LynxOS
4650	MIPS	LynxOS
4700	MIPS	LynxOS
4730	MIPS	LynxOS
5200	MIPS	LynxOS
5500	MIPS	LynxOS
5550	MIPS	LynxOS
6015	MIPS	LynxOS
9050	MIPS	LynxOS

QUICK UNPACK, GREP FOR "LYNXOS" IN THE ELF IMAGE
DOUBLE CHECK YOURSELF!

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

YOU CAN VERIFY VULNERABILITY OF YOUR PRINTERS EASILY!

1. LOCKDOWN YOUR PRINTER ACCORDING TO HP NIST GUIDE
2. DOWNLOAD RFU FROM HP
3. LPR THE RFU, SEE IF IT WORKS...

http://h30046.www3.hp.com/large/solutions/practical_consideration_WP.pdf

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

GENERAL MITIGATION (**IMMEDIATE**)

- DISABLE RFU UPDATES (POSSIBLE, BUT NOT ON ALL MODELS)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

GENERAL MITIGATION (**IMMEDIATE**)

- DISABLE RFU UPDATES (POSSIBLE, BUT NOT ON ALL MODELS)
- APPLY ACL, PASSWORDS (USE WEB JETADMIN)
- FILTER PRINT-JOB CONTENT ON PRINT-SERVER
- ISOLATE PRINTERS FROM SENSITIVE NETWORKS

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

GENERAL MITIGATION (**IMMEDIATE**)

- DISABLE RFU UPDATES (POSSIBLE, BUT NOT ON ALL MODELS)
 - APPLY ACL, PASSWORDS (USE WEB JETADMIN)
 - FILTER PRINT-JOB CONTENT ON PRINT-SERVER
 - ISOLATE PRINTERS FROM SENSITIVE NETWORKS
-
- **BUT ON THE 2055DN...**
 - RFU UPDATE COULD NOT BE DISABLED USING WJA
 - PJI PASSWORD DID NOT PREVENT “PJI ENTER LANGUAGE=ACL”
 - CANNOT PREVENT RFU ATTACK!
 - HP IS WORKING ON A FIX FOR PRINTERS LIKE THIS...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

GENERAL MITIGATION (**IMMEDIATE**)

- DISABLE RFU UPDATES (POSSIBLE, BUT NOT ON ALL MODELS)
- APPLY ACL, PASSWORDS (USE WEB JETADMIN)
- FILTER PRINT-JOB CONTENT ON PRINT-SERVER
- ISOLATE PRINTERS FROM SENSITIVE NETWORKS

DO THIS QUICKLY. IT'S A RACE!

FIRST THING I'D DO (IF I'M THE BAD GUY):

- DISABLE FURTHER RFU UPDATES
- INJECT MALWARE INTO SPI-FLASH
- **LOCK ALL FLASH PAGES**

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

TABLE 5-11. INSTRUCTION SET

Operation	Command	One Byte Command Code	Description	Address Bytes	Mode Bit Cycle	Dummy Bytes	Data Bytes
Read	READ	(03h) 0000 0011	Read Data bytes	3	0	0	1 to ∞
	FAST_READ	(0Bh) 0000 1011	Read Data bytes at Fast Speed	3	0	1	1 to ∞
	DOR	(3Bh) 0011 1011	Dual Output Read	3	0	1	1 to ∞
	QOR	(6Bh) 0110 1011	Quad Output Read	3	0	1	1 to ∞
	DIOR	(BBh) 1011 1011	Dual I/O High Performance Read	3	1	0	1 to ∞
	QIOR	(EBh) 1110 1011	Quad I/O High Performance Read	3	1	2	1 to ∞
	RDID	(9Fh) 1001 1111	Read Identification	0	0	0	1 to 81
	READ_ID	(90h) 1001 0000	Read Manufacturer and Device Identification	3	0	0	1 to ∞
Write Control	WREN	(06h) 0000 0110	Write Enable	0	0	0	0
	WRDI	(04h) 0000 0100	Write Disable	0	0	0	0
Erase	P4E	(20h) 0010 0000	4 KB Parameter Sector Erase	3	0	0	0
	P8E	(40h) 0100 0000	8 KB (two 4 KB) Parameter Sector Erase	3	0	0	0
	SE	(D8h) 1101 1000	64 KB Sector Erase	3	0	0	0
	BE	(60h) 0110 0000 or (C7h) 1100 0111	Bulk Erase	0	0 0	0 0	0
Program	PP	(02h) 0000 0010	Page Programming	3	0	0	1 to 256
	QPP	(32h) 0011 0010	Quad Page Programming	3	0	0	1 to 256
Status & Configuration Register	RDSR	(05h) 0000 0101	Read Status Register	0	0	0	1 to ∞
	WRR	(01h) 0000 0001	Write (Status & Configuration) Registers	0	0	0	1 to 2
	RCR	(35h) 0011 0101	Read Configuration Register (CFG)	0	0	0	1 to ∞
	CLSR	(30h) 0011 0000	Reset the Erase and Program Fail Flag (SR5 and SR6) and restore normal operation)	0	0	0	1
Power Saving	DP	(B9h) 1011 1001	Deep Power-Down	0	0	0	0
	RES	(ABh) 1010 1011	Release from Deep Power-Down Mode	0	0	3	0
		(ABh) 1010 1011	Release from Deep Power-Down and Read Electronic Signature	0	0	0	1 to ∞
OTP	OTPP	(42h) 0100 0010	Programs one byte of data in OTP memory space	3	0	1	1
	OTPR	(4Bh) 0100 1011	Read data in the OTP memory space	3	0	0	1 to ∞

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

EMBEDDED
DEFENSE
THE
BIGGER
PICTURE

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

DIGITALLY SIGNED FIRMWARE

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

DIGITALLY SIGNED FIRMWARE



SECURE FIRMWARE?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

GENERAL PURPOSE COMPUTING ANALOGY

What if Microsoft said...

Windows is secure because we only allow code signed by Microsoft.
That means you can't run your own anti-virus code, but don't worry....
It's all good!

You would probably say...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

GENERAL PURPOSE COMPUTING ANALOGY

What if **HP** said...

LaserJet is secure because we only allow code signed by **HP**.
That means you can't run your own anti-virus code, but don't worry....
It's all good!

You would probably say...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REAL EMBEDDED DEFENSE!

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REAL

DEFENSE!

- HOST-BASED EMBEDDED DEFENSE NEEDS TO **EXIST**

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REAL

DEFENSE!

- HOST-BASED EMBEDDED DEFENSE NEEDS TO EXIST
- DEFENSE SHOULD BE WELL-KNOWN
- NO MORE OBSCURE SECRET-SAUCE SECURITY

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REAL

DEFENSE!

- HOST-BASED EMBEDDED DEFENSE NEEDS TO EXIST
- DEFENSE SHOULD BE WELL-KNOWN
- NO MORE OBSCURE SECRET-SAUCE SECURITY
- DEFENSE SHOULD BE **DECOUPLED** FROM OS

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REAL

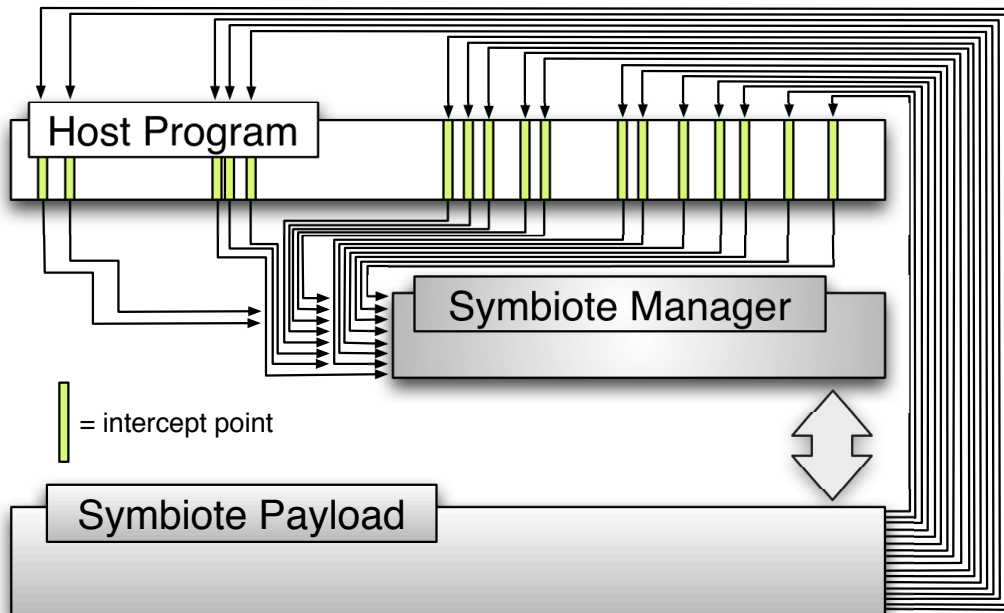
DEFENSE!

- HOST-BASED EMBEDDED DEFENSE NEEDS TO EXIST
- DEFENSE SHOULD BE WELL-KNOWN
- NO MORE OBSCURE SECRET-SAUCE SECURITY
- DEFENSE SHOULD BE DECOUPLED FROM OS
- OS FORTIFICATION IS GOOD
 - BUT SHOULD NOT REPLACE **INDEPENDENT SECURITY SOFTWARE!**

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REAL EMBEDDED DEFENSE EXISTS TODAY!



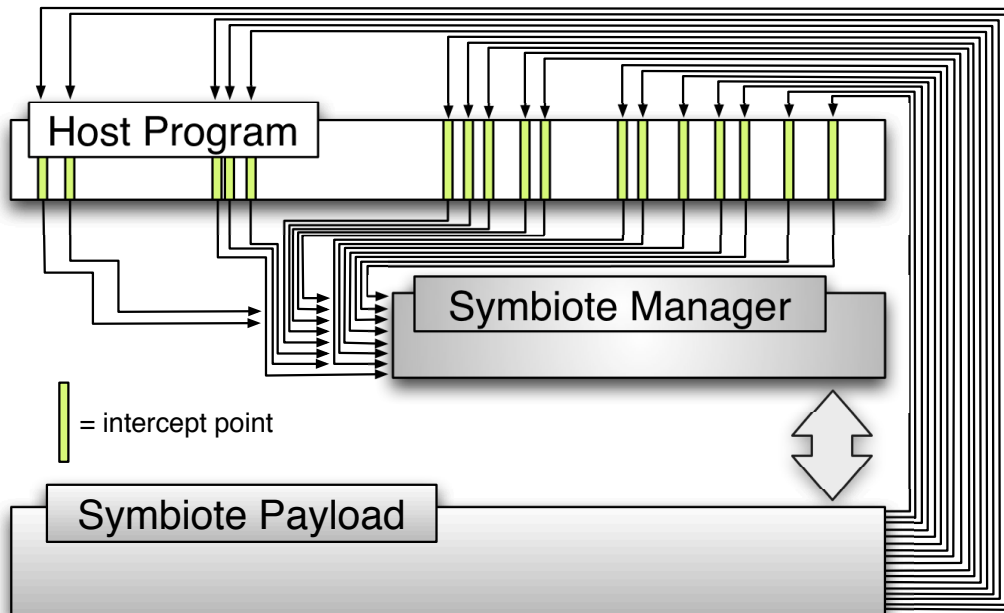
TESTED ON CISCO IOS

- CUI, STOLFO RAID 2011
- CUI, KATARIA, STOLFO ACSAC 2011
- CUI, KATARIA, STOLFO BLACKHAT 2011

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REAL EMBEDDED DEFENSE EXISTS TODAY!



TESTED ON CISCO IOS

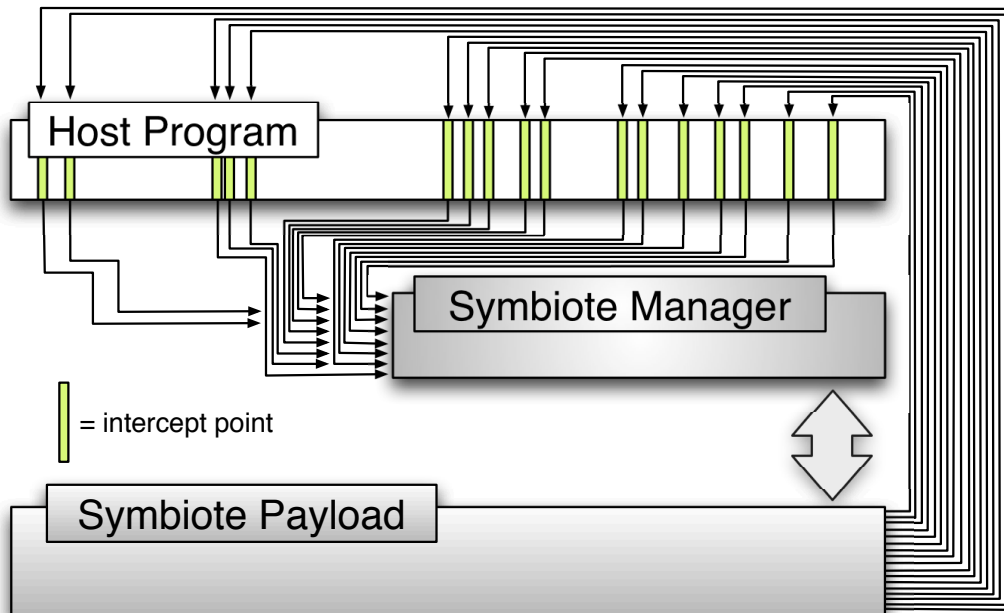
- CUI, STOLFO RAID 2011
- CUI, KATARIA, STOLFO ACSAC 2011
- CUI, KATARIA, STOLFO BLACKHAT 2011

Want a router sensor? [Email me!](#)

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

REAL EMBEDDED DEFENSE EXISTS TODAY!



TESTED ON CISCO IOS

- CUI, STOLFO RAID 2011
- CUI, KATARIA, STOLFO ACSAC 2011
- CUI, KATARIA, STOLFO BLACKHAT 2011

APPLIED HP (**HOPEFULLY**)

- COMING IN 2012!

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

23. Are current HP multifunction printers susceptible to viruses and worms?

No, since the majority of viruses and worms exploit vulnerabilities in Windows-based computers. HP MFPs use non-standard operating systems other than Windows. Consequently, they are immune to these viruses and worms. In practice, there have been no known instances of viruses or worms infecting HP MFPs.

In the future HP will likely ship MFPs which include an embedded version of the Windows operating system. However, there are a number of practical reasons why this won't increase the security risk faced by customers.

24. Does this mean that HP MFPs are completely safe from worms and viruses?

No, since it is technically possible for someone to craft a virus or worm that targets the non-standard operating systems shipped with the MFPs. However, HP considers the probability of such an event to be considerably lower. Hackers are more likely to be interested in exploiting vulnerabilities in workstations and servers since they are more widespread and require less expertise.

QUESTIONS!?

White Paper: "HP Security Solutions" 2006



COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK



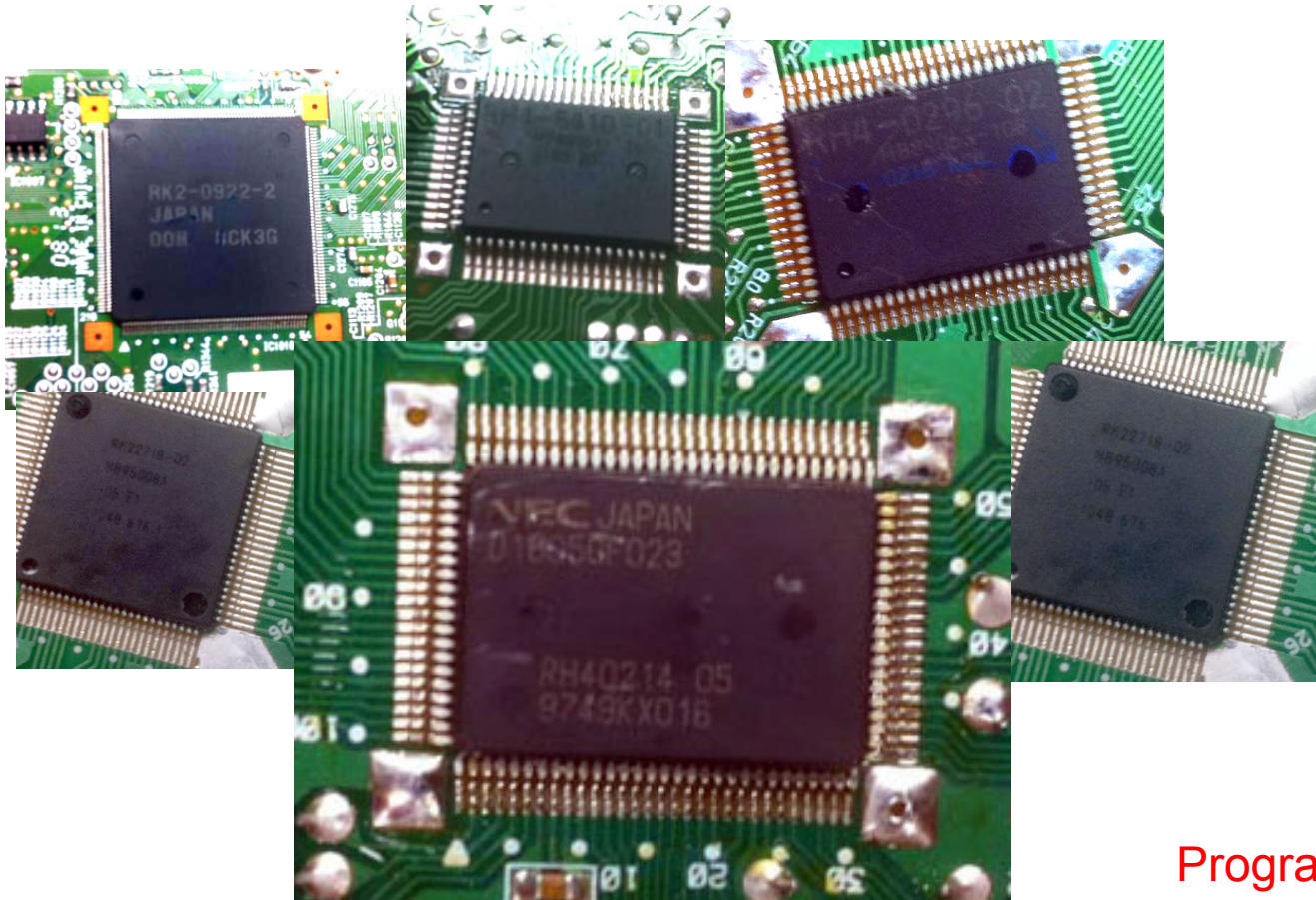
IN LOVING MEMORY OF
BAMBAM
3.12.2008 - 12.7.2011

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

ENGINE CONTROLLER:

NEC MICROCONTROLLER ON ALL MODELS I LOOKED AT.



NEC

RH4-0296-02

RH4-5410-01

RH4-0214-05

RK2-0922-02

RK2-2718-02

Programmable Via RFU!

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

ENGINE CONTROLLER:

NEC MICROCONTROLLER ON ALL MODELS I LOOKED AT.

```
f.rodata:013EC2F4 00000027 C ENG: Elabel NOT ready - Reg SR45 0x%X\n
f.rodata:013EC31C 0000002A C ENG: Elabel response not ready, timedout\n
f.rodata:013EC348 00000026 C ENG RFU: cmd=0x%04X; response=0x%04X\n
f.rodata:013EC370 0000001C C ENG RFU: put into RFU mode\n
f.rodata:013EC38C 00000037 C ENG RFU: start RFU send. size=0x%X=%ld 2-byte chunks.\n
f.rodata:013EC3C4 00000025 C ENG RFU: sent %ld words out of %ld \n
f.rodata:013EC3EC 00000044 C ENG RFU: RFU download done, EEC86 result: 0x%04X, response: 0x%04X\n
f.rodata:013EC430 0000001F C ENG RFU: wait for engine init\n
f.rodata:013EC450 00000019 C ENG RFU: engine initing\n
f.rodata:013EC46C 00000018 C ENG RFU: engine init done\n
f.rodata:013EC488 0000001A C ENG RFU: engine RFU done\n
f.rodata:013EC4A4 00000016 C FWDL: start download\n
f.rodata:013EC4BC 00000019 C FWDL: send fw to engine\n
f.rodata:013EC4D8 0000000C C FWDL: done\n
```

NEC

RH4-0296-02

RH4-5410-01

RH4-0214-05

RK2-0922-02

RK2-2718-02

GREAT PLACE FOR MALWARE TO HIDE...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

SEARCH FOR “HP COLUMBIA PRINTER”

[HP LaserJet printers pose massive security risk, say Columbia ...](#)

[www.theverge.com/.../hp-laserjet-printers-pose-massive-security-risk-...](#)

Nov 29, 2011 – MSNBC is reporting a security flaw that could affect millions of **HP LaserJet printers**. According to Ang Cui and Salvatore Stolfo of **Columbia ...**

[Printer Locations - Columbia University](#)

[www.columbia.edu](#) > Facilities > Printing

Block all [www.columbia.edu](#) results

60+ items – CUIT and Libraries **Printer** Locations Barnard **Printer** Locations ...

NINJa hostname	Location	Printer Model/Driver
avery200a-ninja.atg.columbia.edu	Avery 200	HP LaserJet P4015 PS
avery200b-ninja.atg.columbia.edu	Avery 200	HP LaserJet P4015 PS

[Computer FAQ](#)

[www.math.columbia.edu/general/main/computerfaq/index.html](#)

421: lp421.math.columbia.edu 128.59.192.100 **HP Laserjet 4515. 509 Color Printer:**
lp509.math.columbia.edu 128.59.192.101 **HP Color Laserjet 3000 ...**

[Columbia University Researchers Reveal Flaw in HP Printers That ...](#)

[www.theblaze.com/.../your-printer-could-be-the-next-target-of-a-hac...](#)

Nov 29, 2011 – It seems computers get all the action when it comes to hackers' target of choice, but that could very well change. According to an exclusive ...

[HP Refutes Reports That Printers Can Be Remotely Set On Fire ...](#)

[www.foxnews.com/.../hackers-can-set-your-hp-printer-on-fire-resear...](#)

Nov 29, 2011 – Reports based on research by a team of **Columbia** University computer science professors, claimed that **HP's laser printers** can be sent new ...

Please don't attack us.

We surrender!

-(

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

OFFENSIVE POTENTIAL

WE INTENTIONALLY DID NOT “WEAPONIZE” THIS ATTACK

BUT CAN THIS BE DONE PRACTICALLY ON WINDOWS?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

OFFENSIVE POTENTIAL

SPEAKING OF MS WORD...

Field codes: Print field

Applies to: Microsoft Office Word 2003

{ PRINT "PrinterInstructions" }

[+ Show All](#)

Sends printer-control code characters to the selected printer.

Microsoft Word displays a result only when the document is printed. For appropriate printer codes, consult your printer manual.

[+ Learn more about using the PRINT field to embed PostScript commands in a document](#)

NOTE The PRINT field works well with a PostScript printer or a Hewlett-Packard LaserJet printer, but it may not work properly with another type of laser printer. The PRINT field works with a dot-matrix printer only if the printer supports the PassThrough command.

Did this article help you?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

Field codes: Print field

Applies to: Microsoft Office Word 2003

{ **PRINT** "*PrinterInstructions*" }

[+ Show All](#)

Sends printer-control code characters to the selected printer.

Microsoft Word displays a result only when the document is printed. For appropriate printer codes, consult your printer manual.

[+ Learn more about using the PRINT field to embed PostScript commands in a document](#)

NOTE The PRINT field works well with a PostScript printer or a Hewlett-Packard LaserJet printer, but it may not work properly with another type of laser printer. The PRINT field works with a dot-matrix printer only if the printer supports the PassThrough command.

Did this article help you?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

OFFENSIVE POTENTIAL

SPEAKING OF MS WORD... (FUNNY STORY)

WHEN LOW ON MAN-POWER, OUTSOURCE!

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

☆ **Albert Mah** to me, hemin.merchant, MSSolve, Ross

[show details](#) Oct 28

[Reply](#)

Hi Ang and Hemin,

My name is Albert Mah, a Support Escalation Engineer on the Word team. You were previously working with Ross Lindgren, who assigned your case to me and I will now be your main point of contact.

111101383378206 WD2007: Problem with Hexadecimal in .PRN file

As I understand it, you want to include approximately 7MB of raw PJI data in a Print field and sent it to a printer. However, your finding that the hex sequence

- a) "BF FA FE 00 00 00" is being inserted into the .prn file when using an HP PCL6 driver
- b) "1B 2A 6F 34 57 0A 06 00 01 1B 2A 6F 34 57 0A 06 00 00" is being inserted into the .prn file when using an HP PCL5 or PS driver.

At this point, I'm investigating whether this sequence is being inserted by Word or not.

I'll keep you posted on any new developments.

Have a great Halloween weekend!

Thank you for using **Microsoft** Customer Service and Support (CSS),

Albert Mah

Support Escalation Engineer | Commercial Technical Support

Office: [\(469\) 775-6465](tel:(469)775-6465)

Fax: [\(555\) 775-6738](tel:(555)775-6738)

Bridge [\(866\) 500-6738](tel:(866)500-6738) Passcode: 9866716

almah@Microsoft.com

microsoft.com/

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

OFFENSIVE POTENTIAL

SPEAKING OF MS WORD... (FUNNY STORY)

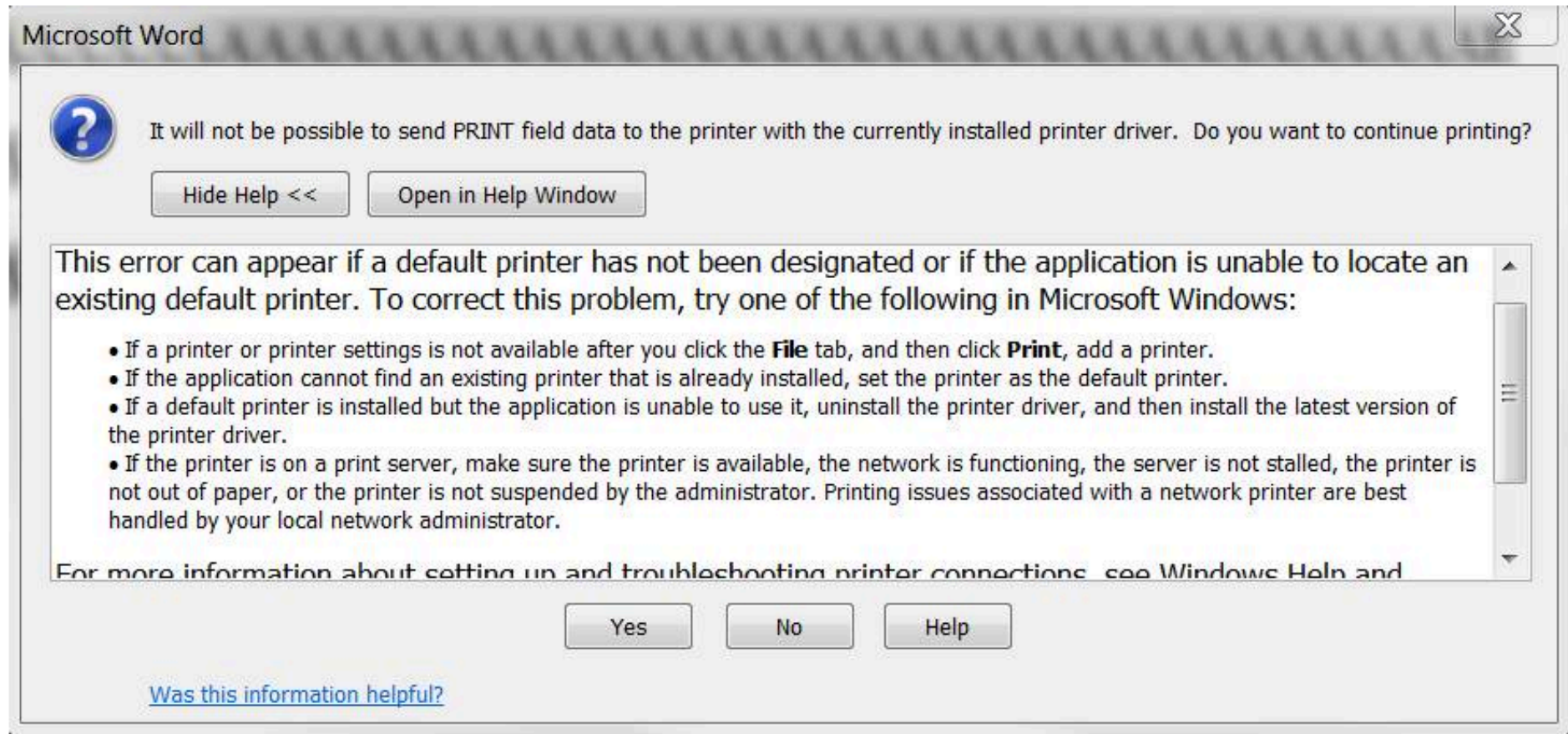
WE CAN TALK ABOUT IT NOW BECAUSE...

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

2. HP also released its latest Universal Print Driver (UPD) PCL6 (version 5.4) driver on December 1st.

We installed the driver, and when we attempted to print the sample document to .prn file, we get the error:

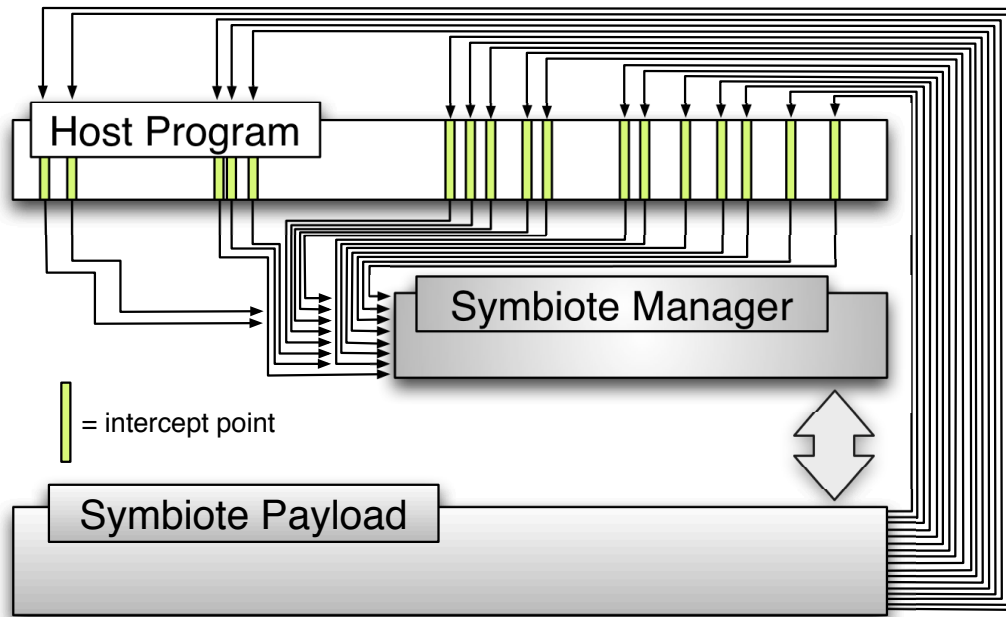


PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HOW IT ALL STARTED...

APPLYING SOFTWARE SYMBIOTE DEFENSE TO PRINTERS



APPLIED TO CISCO IOS

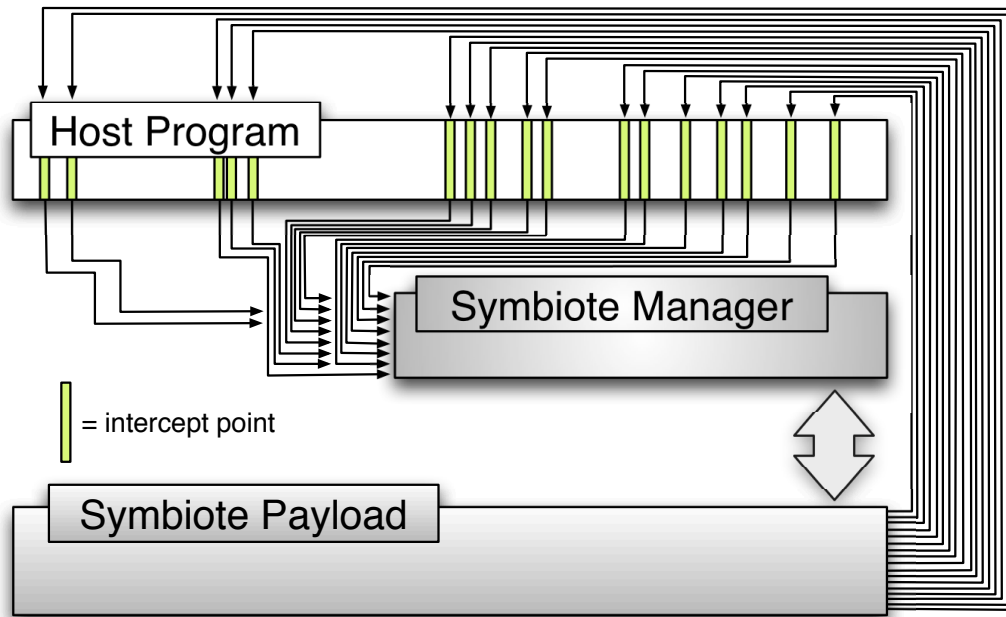
- CUI, STOLFO RAID 2011
- CUI, KATARIA, STOLFO ACSAC 2011
- CUI, KATARIA, STOLFO BLACKHAT 2011

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

HOW IT ALL STARTED...

APPLYING SOFTWARE SYMBIOTE DEFENSE TO PRINTERS



APPLIED TO CISCO IOS

- CUI, STOLFO RAID 2011
- CUI, KATARIA, STOLFO ACSAC 2011
- CUI, KATARIA, STOLFO BLACKHAT 2011

BUT CAN IT BE DONE TO
NOT-A-ROUTER?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

FOR THE SYMBIOTE TO WORK, YOU NEED TO:

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

FOR THE SYMBIOTE TO WORK, YOU NEED TO:

- UNPACK EXISTING FIRMWARE

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

FOR THE SYMBIOTE TO WORK, YOU NEED TO:

- UNPACK EXISTING FIRMWARE
- ANALYZE UNPACKED BINARY

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

FOR THE SYMBIOTE TO WORK, YOU NEED TO:

- UNPACK EXISTING FIRMWARE
- ANALYZE UNPACKED BINARY
- INJECT SYMBIOTE MANAGER AND PAYLOAD

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

FOR THE SYMBIOTE TO WORK, YOU NEED TO:

- UNPACK EXISTING FIRMWARE
- ANALYZE UNPACKED BINARY
- INJECT SYMBIOTE MANAGER AND PAYLOAD
- REPACK FIRMWARE

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

QUANTITATIVE SCOPE

ACTIVE ATTACK:

While HP has identified a potential security vulnerability with some HP LaserJet printers, no customer has reported unauthorized access. The specific vulnerability exists for some HP LaserJet devices if placed on a public internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade.

WHO EXACTLY IS A “TRUSTED PARTY” ON YOUR NETWORK?

PRINT ME IF YOU DARE

FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

FOR THE SYMBIOTE TO WORK, YOU NEED TO:

- UNPACK EXISTING FIRMWARE
- ANALYZE UNPACKED BINARY
- INJECT SYMBIOTE MANAGER AND PAYLOAD
- REPACK FIRMWARE

BUT FIRST, YOU HAVE TO BE ABLE TO MODIFY
THE FIRMWARE ON THE TARGET DEVICE...