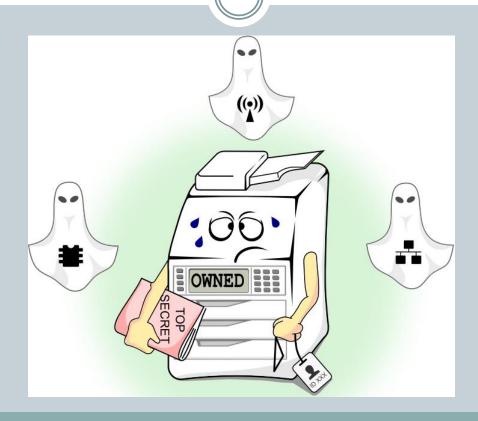
Hacking printers: for fun, profit and (anti)warfare



Impressum

- Andrei Costin
- Author of MFCUK
 - MiFare Classic Universal toolKit
- Day-time programmer (after-8pm type of hobbyist hacker)
 - Not part of printing industry though
- Generally interested in:
 - o Programming/hacking: RFID, GSM, biometrics, embedded
 - Almost everything which:
 - Is connected to networks/communications lines
 - Have smart-cards (contact and contactless)
 - Have crypto involved somewhere down the line
 - × Is or should be secure
 - Corporate/Enterprise IT support software & security
 - TEMPEST and ISS

Abstract

- While more and more new devices (routers, smartphones, etc.) are getting connected to our SOHO/enterprise environments, all-colour hats are getting plenty of focus on their security: defend and harden on one side; exploit and develop malware on the other.
- However, a special class of network devices (specifically network printers/scanners/MFPs), which are networked for more than 15 years, are constantly out of the modern security watchful eye.
- And even though we entrust them even the most confidential documents or the most sacred credentials (LDAP, PINs, RFID badges, etc.), we don't realize closely how weak and unsecured they are, despite the few minor security bulletins that started to pop-up here and there in the recent few months.
- In this presentation, we will try to analyze the reasons why hacking network printers/MFPs is a reasonable and accomplishable idea. Also, we will take a look at current state of (weak) affairs in the vulnerability and security research available. Then we will try to envision types of possible exploitation scenarios, backed-up with a printer remote-exploit demo. We will conclude the presentation with possible solutions and what can be done to protect ourselves as well as our network environments.

Disclaimer*

- No Warranties or Liability. Information is provided as-is, though every effort has been made to ensure the accuracy of the information presented. Author of the presentation is not legally liable under any circumstances for any damages such as but not limited to (including direct, indirect, incidental, special, consequential, exemplary or punitive damages) resulting from the use or application of the presented information.
- Unless explicitly noted in forms such as but not limited to "the XYZ Company says", etc., the opinions expressed in this presentation are solely and entirely my own. They should not be interpreted as representing the positions of any organization (past, present, future, existent, non-existent, public, private, or otherwise) with which I may or may not have been, are or are not, or will or will not be affiliated at some time in the past, present, or future.
- All trademarks and registered names are the property of their respective owners.
- This presentation: © 2010, Andrei Costin. Released under:



*big fat one – because everybody loves fineprints

\H1B%-12345X@PJL JOB "HackingPrinters"

This presentation is about:

- o Hacking "the PC inside printers/MFPs"
 - ▼ Why would someone hack a printer/MFP
 - ▼ How would someone hack "the PC inside printers/MFPs"?
 - ➤ How easy/feasible is MFP *fir* malware creation and exploitation
 - ▼ How to protect yourself and your so-much-loved MFP?
- Laying foundation for further community security research/development/PoC

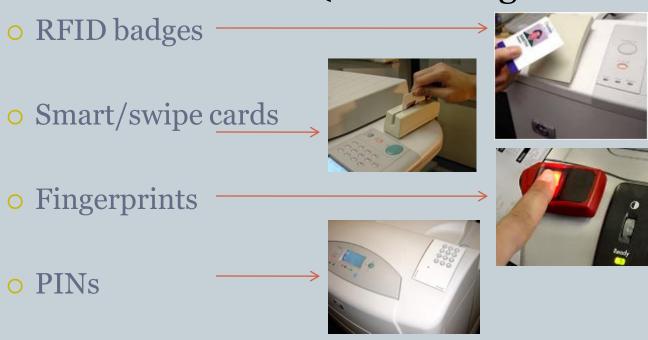
• This presentation is NOT about:

- o Printers' display hack (RDYMSG, OPMSG, STMSG)
- o Printers' embedded web-server hacks (mostly not)
- Printers' SNMP configuration hacks (mostly not)
- o Exhaustive guide to hack every and last MFP (not yet!)

- First, my term for MFP = Mfp, Fax, Printer
- Many would ask "Why would you exploit an MFP?" answer derives from questions below:
 - O How many persons would expect their MFP infected?
 - O How many users/admins/security-auditors audit and hard-secure their/network MFPs?
 - Even if they do, do MFP vendor pay attention to security?
 - o Bottom-line is always "It's just a damn printer/MFP!"
 - O How many persons or anti-malware products could clean such a malware?
 - ➤ Afaik, o(zero) antimalware products for (huge) printers/MFPs market
 - Why not (net/port/vuln)scan the network from a printer which is not suspected/cleanable?
 - Why not hide the malware/payload on a network printer and then make your way through the network/data?
 - o Etc., etc., etc.

- First of all (most) printers/MFPs are already fullblown computers
- Have these to play/own:
 - Some flavor of (RT)OS (VxWorks, LynxOS, Nucleus, Linux)
 - o Embedded Java VM (eg.: ChaiServer)
 - o Embedded Web Server (eg.: Virata EmWeb)
 - o Ethernet/WiFi
 - ➤ Not covering TCP/UDP/IP stack attacks, but there are <u>examples</u>
 - Eventually HDD nice to scan/dump
 - × Eg.: recent <u>CBSNews Investigation Case</u> − with much hype
 - o Eventually SecureJet-like extensions − sweet thing ©!
 - Eventually Fax board

MFPs interact with (hence can get access to):



- LDAP/domain passwords
- Aren't these most-wanted things we are hunting after all?

Looking for confidential documents?

- Why taking the trouble for infecting a PC-host on a network (eg. both elements being secured, updated & monitored) just to get a document with strong crypto using long-enough key and then not being able to decrypt it...
- ...when instead wait for it to be in-printer decrypted (eg. SecureDimm) and printed (and I guess secret documents are still being printed on paper occasionally for selected eyes) so you get it decrypted in plain text

- Not so much information in this area (compared to PC or mobile devices)
 - PJL UPGRADE approx 6 results
 - PJL LPROGRAMENG o results
 - PJL LPROGRAMRIP 1 result (security paper)
 - PJL DMINFO approx 300 results
 - PJL DMCMD approx 75 results
 - Compare with this <u>PDF "/Launch"</u> approx 55 Mln results
- Too few known (more or less) public researches
- Recent disclosures mainly focused on web-admin, snmp,
 XSS and <u>uncontrolled</u> buffer overflows
 - Not too much detailed analysis on OS, kernel and firmware level

o Big <u>number of devices</u> – according to <u>Gartner</u>:

Worldwide: Page Printer Vendor Shipment Estimates, 2005 (Thousands of Units)

Company	2005 Shipments	2005 Market Share (%)	2004 Shipments	2004 Market Share (%)	2004-2005 Growth (%)
Hewlett- Packard	10,527,966	49.0	8,828,405	48.7	19.3
Samsung Electronics	1,874,820	8.7	1,901,933	10.5	-1.4
Lexmark	1,268,089	5.9	1,131,213	6.2	12.1
Brother	1,178,039	5.5	1,018,642	5.6	15.6
Canon	1,154,203	5.4	909,492	5.0	26.9
Other Vendors	5,468,926	25.5	4,322,420	24.0	26.5
Total	21,472,043	100.0	18,112,105	100.0	18.6

Source: Gartner Dataquest (February 2006)

- o Theoretically, magnitude of 10 x mlns of devices (24 mlns/yr):
 - Perfectly exploitable & non-easy-cleanable
 - ➤ Always on, no antivirus & firewall running inside of them

ANDREI COSTIN, HACKCON OSLO, 2011

- The Holy Grail would be to own "<u>securities</u> <u>printers</u>"
 - o <u>Currency</u>/financial assets <u>printing</u> machines
 - ▼ Unfortunately limited to very closed circles ⊗ for obvious reasons
 - No updates/patches on internet to poke around
 - o Industrial <u>currency check/count</u> machines
 - × More or less accessible
 - ➤ From <u>BPS 2000/3000</u> Banknote Processing Systems for Central Bank Applications "*The operating system software and all production data* <u>can be</u> authenticated to protect data integrity and guard against tampering (<u>optional</u>)" isn't it just sweet ©
 - Passport/ID printing machines
 - o Eg.: Oberthur, Giesecke&Devrient, others
 - o These are not part of this presentation ⊗... yet ⊚!

ANDREI COSTIN, HACKCON OSLO, 201

Current available public research

- Slobotron on Hacking Printers (2002)
- phenoelit's HP resources (2002)
- Irongeek's "Hacking Network Printers" (2006)
- <u>"Exploiting Printers by Analyzing Their Firmware"</u>
 (2009)
 - Nowhere to find on the net... censored?!
- "Juste une imprimante" (2010)
- Ben Smith's "Printers gone wild!" (2011)
 - o printFS kit
 - o pyPJL kit

MFPs Exploitation – (Mis)use scenarios

- PDOS aka bricking
- Idle-time processing
- Malware/upload storage
- "Stealth"/uncleanable command and control
- Unencrypted data theft
- Corporate/enterprise/intelligence assets data theft
- Spam inside/outside networks
- Ransomware
- Espionage
- MFPs attack back (slides below)

MFPs Exploitation – Physical attacks

- "The <u>paper's speed keeps it from burning</u> as it passes through the fuser assembly". Temp approx: 185 ° C/ 365 ° F
- Attack1: Supply paper impregnated <u>match-head powder/</u>
 <u>KNO3/</u> NH4NO3
- Attack2: Firmware-controlled motors speed + fuser temp + thermo-sensors
 - Supported by default: set fuser to HIGH2, motors auto slows to lower ppm, use thin paper/transparency



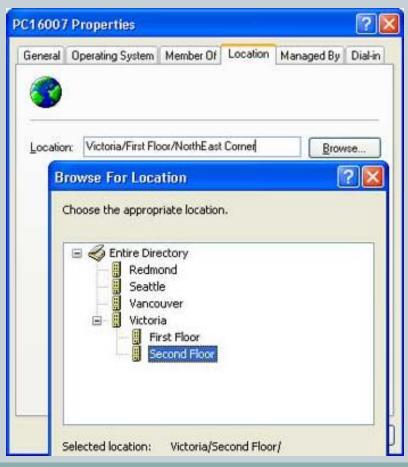
- Geolocation = identification of an object's real-world geographic location
- Geolocation for MFPs
 - o MS's <u>Printer Location Tracking</u> (PLT) (details on next slides)
 - PLT is defined and stored in Active Directory (AD)
 - Non-protocol, description-based, proprietary coding location meta-information
 - Though not intended to, can be used to achieve GPS+ accuracy
 - o <u>IETF PWG</u>'s <u>IPP</u> Everywhere
 - × Uses <u>"geo:" URI scheme</u>
 - × Looks like:
 - "printer-geo-location", char[2048], IPP:uri, SM: anyURI maxLen=2048
 - o geo:43.220973,-77.417162,128;u=1.83 (u=uncertainty 1.83m)
 - o <u>DNS LOC</u> (see the paper)
 - × Exciting stuff, though not too many domain admins chose to publish their GPSes ☺
- Comparison: printing subsystem vs mobile-communication networks
 - o GSM: MS-assisted with NW-based computation of GPS coordinates
 - × PLT: MFP-assisted with AD/PLT-based reverse geolocation lookup
 - o GSM: MS-based with NW-assisted computation of GPS coordinates
 - ▼ IPP: MFP-based direct "geo:" coding

PLT examples:

- o "SLD Bldg o84 Flr 1 Room 111", "C2No5 Block C, 2nd Floor, North Wing, Cubicle o5"
 - ▼ Hard, but not impossible most are just patterns of some kind
- Most organizations have them correct & easy human readable, otherwise PLT is useless
 - Makes decoding easy (even easier with strong apriori knowledge of the target)
- PLT-based geolocation properties:
 - (+) Usually MFPs' location is well defined and fixed
 - ▼ MFPs are by nature very location-static devices
 - o (+) Good accuracy (building, wing, even room granularity) vs IP-only-based
 - (+) Can be 3D approximated (if floor is present in PLT meta-description)
 - (+) Can derive additional meta-information (eg. "Joe Doe's office − 3rd Flr WingN − are we are looking specifically for joe.doe@victim.com?)
 - o (+) Can be used where no public IPs of MFPs are exposed
 - (-) Reverse geolocation sometimes is bogus (hey google, wtf?)
 - o (-) Needs built-in heuristics in malware/C&C to correctly interpret PLT

- Targeted attacks scenarios:
 - o Apriori-built knowledge (for target-specific malware):
 - Target carefully studied (internal domains, shares, naming conventions&patterns)
 - Malware built with gathered heuristic detection + included reverse lookup tables
 - Runtime knowledge (for generic malware):
 - Directly try the luck with access to external
 - × Better, get help from a C&C center for heuristics/GPS-lookups
 - If a (group) of PC(s) under malware control has the same default printer
 - And that printer's PLT reverse-lookups to targeted GPS-location
 - Then we have "target reached"
 - Once the PC-malware or MFP-malware reached the target
 - Activate the attack (physical on printers, network level, OS-level, etc.)
- General conclusion
 - Some malware will have to become more and more target-oriented
 - Malware must and will be self-geolocation-aware
 - Especially where devices are location-static and PLT-like technologies are deployed

- MS magazine from example to practice:
 - We know it's microsoft domain



- MS magazine from example to practice:
 - O Use: "victoria building second floor" for reverse geolocation lookup − false positive ⊗

victoria building second floor

Search

About 275,000 results (0.17 seconds)

Advanced search

[PDF] The laboratory on the fourth floor of the Victoria Building within ... 😭 🔍

File Format: PDF/Adobe Acrobat - Quick View

Learning Resource Center (LRC) on the second floor of the Victoria Building houses the

Nursing Computer, Lab, a viewing area for slides and videos, ...

cre.nursing.pitt.edu/.../Resource%20Page%20with%20Clinical%20Space.pdf

o Use: "microsoft victoria" for reverse geolocation lookup − first hit ⊚!

microsoft victoria

Search

About 14,300,000 results (0.14 seconds)

Advanced search

About Microsoft UK: Travel to London 🕸 🔍

Travel to the Microsoft® London Office. ... How to Find Us. Microsoft London (Cardinal Place)

100 Victoria Street London SW1E 5JL Tel: 0844 800 2400 ...

www.microsoft.com/uk/about/map-london.mspx - Cached - Similar

[РОР] Microsoft - Victoria, London D 🏗 🔍

File Format: PDF/Adobe Acrobat - Quick View

Page 1.

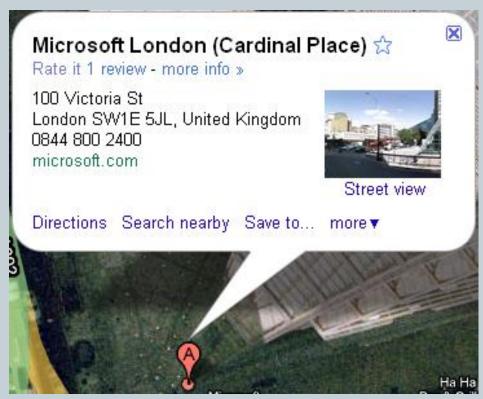
download.microsoft.com/documents/uk/about/.../victoria_map.pdf - Similar

Our Offices - Microsoft.com - Careers 😭 🔍 - 12:53pm

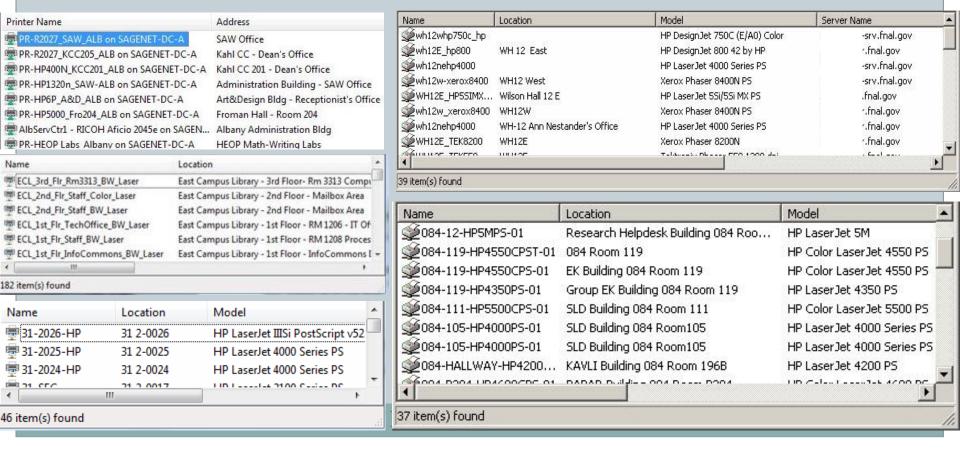
Microsoft London (Cardinal Place) 100 Victoria Street London SW1E 5JL Tel ...

careers.microsoft.com/careers/en/gb/offices.aspx - Cached

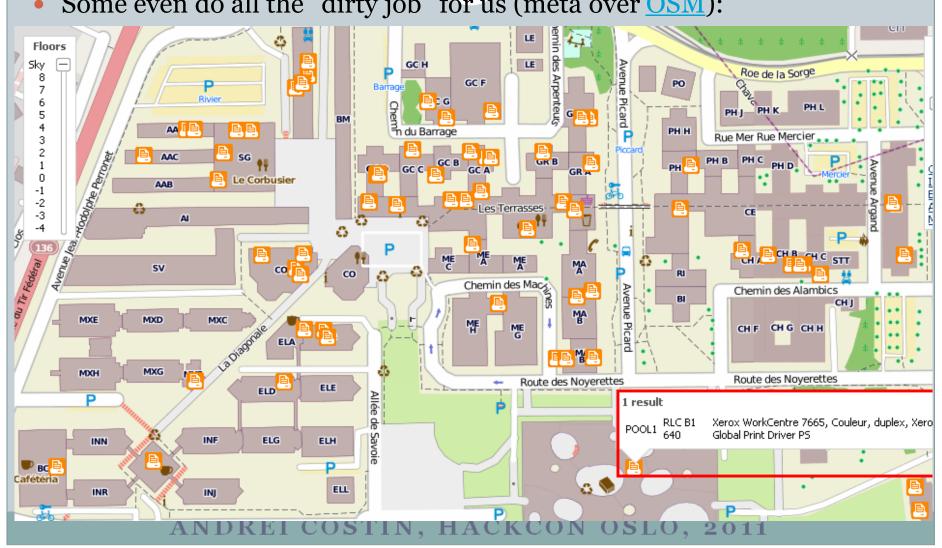
- MS magazine from example to practice:
 - Show me the money.... and the **map!**
 - × lat=51.4970135
 - × lon=-0.1411003



- OMG they are everywhere...
 - o Research labs (nuclear, physics, astronomy), government, big EDUs
- Just few of them:



Some even do all the "dirty job" for us (meta over OSM):



- Visualization (of target/enemy) is powerful!
- Useful if interest lies in specific:
 - o Geo-locations, Device Class, Vendors, Models
- Basic scripting gives us a nice map like below:
 - Live demo (public IP based geolocation map)



- Myriad of specs and languages... %)
- UEL <u>Universal Exit Language</u>
 - Just one command
 - <esc>%-12345X (<esc> is 0x1B aka \H1B aka ESCape)
 - Harmless by itself, lethal in specific combinations
- PJL Printer Job Language
 - Developed by HP
 - Job level controls: printer language switching, job separation, environment, status readback, device attendance and <u>file system</u> <u>commands</u>
 - Have essential security design flaws, hence exploitable
 - Examples:
 - \times <esc>%-12345X@PJLJOB\r\n
 - \times @PJL RDYMSG = "Sample PJL Job"\r\n

 - × ...
 - \sim @PJL EOJ\r\n<esc>%-12345X

- PCL Printer Control Language
 - Developed by HP
 - o Well, actually it's not a control language (PJL is)... name confusion...☺
 - o It's more a formatting-control language, like PS
 - Harmless, but parsers and interpreters could be exploited
 - o Examples:
 - ➤ Usually PCL jobs start with:
 - \circ <esc>E\r\n
 - Sample commands in the job:
 - o <esc>&l1T
 - Toggles the printer's job separation mechanism
 - o <esc>&l3X
 - Instructs to print 3 copies
 - ➤ Mandatory PCL jobs end with:
 - \circ <esc>E\r\n

- PS PostScript Language
 - Developed by Adobe
 - Mostly formatting-control language
 - Also, parsers and interpreters could be attacked
 - o Examples:
 - \times %!PS-Adobe-3.o\r\n
 - × %%LanguageLevel: 2
 - %%BeginFeature: *PageSize A4
 - × 1 1 sub ==
 - × %%EOF\r
- PPD Adobe PS Printer Description
 - Describe the entire set of <u>features</u> and capabilities available for their PostScript printers

• PML – Printer Management Language

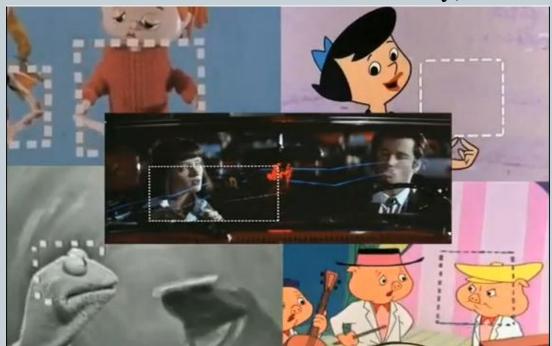
- HP's object-oriented request-reply protocol to exchange device management information
- o PML can be used to query SNMP values from a printer device
- o So... turning SNMP off doesn't solve all problems ☺
- o Examples:
 - ▼ @PJL DMINFO ASCIIHEX="PmlRequest"\r\n
 - ASCIIHEX="PmlReply"\r\n\f
 - ∝ @PJL USTATUS TRAP\r\n
 - ASCIIHEX="PmlTrapRequest"\r\n\f

• GPD – Generic Printer Description

- Windows GDI-based spec, <u>similar to PPD</u>
- Used for creating <u>unidrv.dll</u> minidrivers for non-PS printers
- Something like a customization plugin over unidrv.dll (not a bad idea)
- Usually here: c:\windows\system32\spool\drivers\

Specifications *"fineprints"

- (some) PJL holes:
 - No provisions for standard, secure and vendor/arch/osindependent way for binary/firmware upload/upgrades
 - x Everyone reinvented their own wheel − sadly, most did it wrong...



Specifications *"fineprints"

- (some) PJL holes:
 - No standard provisions for strong authentication
 - No standard provisions for encryption
 - × All <u>usernames</u>, <u>PINs & passwords are in clear-text</u>
 - @PJL SET USERNAME="HackingPrinters"
 - o @PJL SET HOLDKEY="1234"
 - o @PJL SET KMUSERKEY2 = "password"
 - Print job PIN security (@PJL HOLDKEY)
 - × We are in 2010 − we get 0-9999 PIN/password range... ©
 - Ben Smith has a nice PJL password bruteforcer in python
 - x Also, specs say nothing about N-tries-and-fails scenario actions
 - Again, the wheel...

MFPs Exploitation – How to approach?

- Remote-initiated printing (RIP) exploiting channel
- Locally-initiated printing (LIP) exploiting channel
- Exploiting "test print" access in printers' EWS
- Exploit printer management software
- Internal interpreters' exploit
- Locally-executed applications with rogue firmware
- Printer subsystem hacks

Remote-initiated printing exploit

Printing Payload Exploit (PPE) over Java Applets

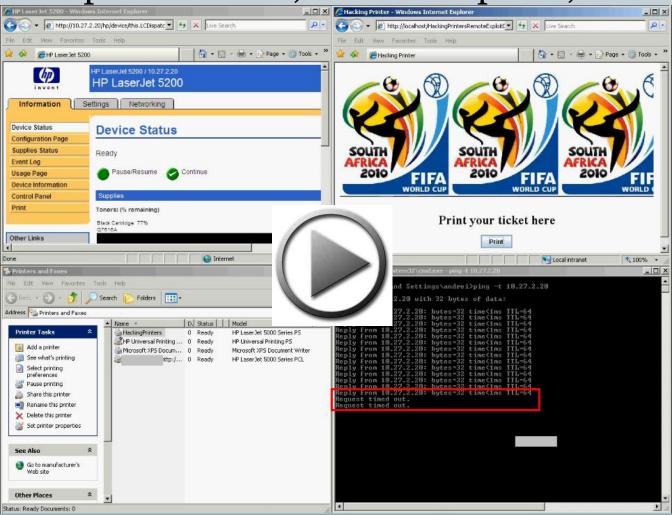
requires some user intervention



- Lure the users to a site and then trick to print
 - Eg: print tickets, print discount coupons, print charity-related stuff, print government/tax related forms/discounts, etc.
- Auto-start printing trick
 - o "mayscript" yes, "scriptable" true, jso = JSObject.getWindow(this), jso.call("startPrintingPPE"...)
- Can be successful using social engineering/nagging
 - o Similar to VBScript F1/Help Keypress Vulnerability

Demo – Remote-initiated printing exploit

Printer exploited: reset, malware upload, etc.



Remote-initiated printing exploit

- Restart (on HPs) is accomplished by
 - @PJL DMINFO ASCIIHEX = "040006020501010301040104"
 - o Same as phenoelit's trick (BH2002)
 - \times SNMP set .iso.3.6.1.2.1.43.5.1.1.3.1 = 4
 - ➤ However, PJL DMINFO is actually "SNMP thru PJL"
- Live code demo pil print applet.java
 - o PrintService
 - PrintServiceLookup
 - DocPrintJob
 - JobName
 - SimpleDoc
 - o ... and DocPrintJob.print()

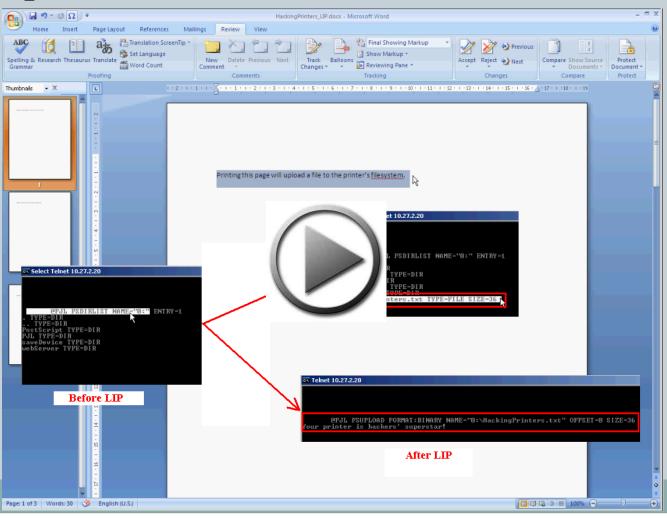
Locally-initiated printing exploit

- MS Word
 - o "Print and get your printer owned" type of exploit
 - Will video demo in next slide
- Adobe <u>LiveCycle XDC files</u> (XML files)
 - Used in <u>SAP®</u> environments
 - o "Infect"/replace all XDC files with required firmalware payload
 - ▼ Doesn't necessarily need admin rights
 - o Good example how to do this is here on page 15

```
<xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
<xdc name="ps_plain" xmlns="http://www.xfa.org/schema/xdc/1.0/">
<pdl>
<pdl>
<seq id="preDoc"><ESC/>%-12345X@PJLRDYMSG DISPLAY=""&#13;&#10;
@PJLUPGRADE SIZE = 1024&#13;&#10;[hex_encoded_payload]<ESC/>%-12345X</seq>
</pdl>
</xdc>
</xdc>
</xdp:xdp></pd>
```

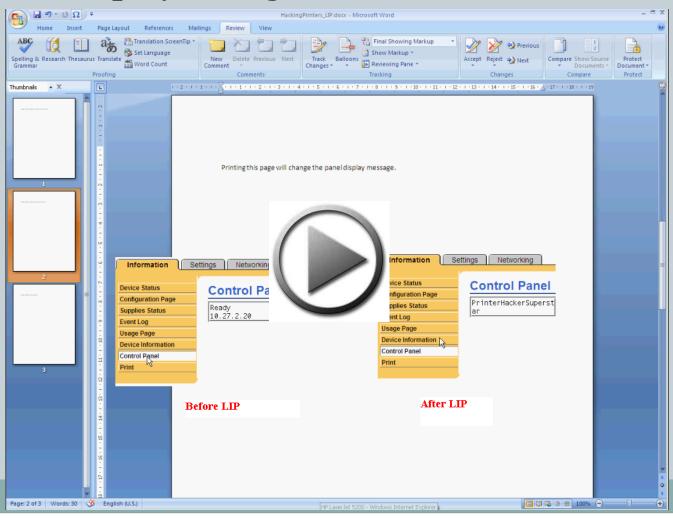
Demo – Locally-initiated printing exploit

"File upload" PPE over MS Word



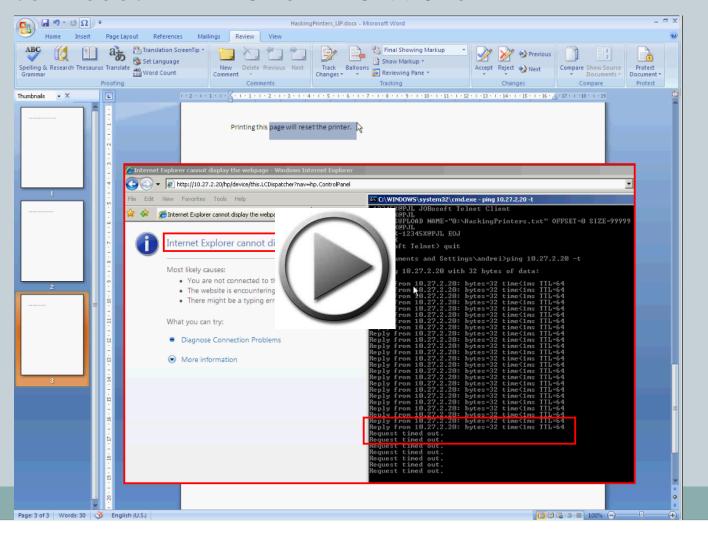
Demo – Locally-initiated printing exploit

"Printer-display change" PPE over MS Word



Demo – Locally-initiated printing exploit

• "Printer reset" PPE over MS Word



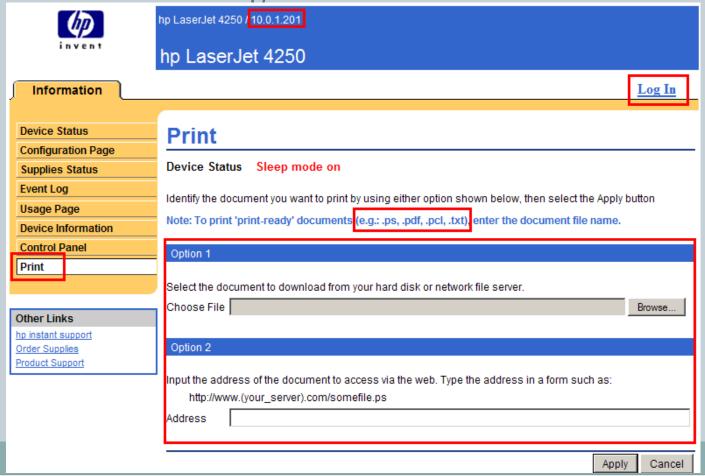
Solutions for remote+local initiated exploits

• How to fix?

- O Not easy, since it's PJL design + device vendors' faults
- o Java, Word, LiveCycle, etc. have no big blame
 - They act as "channels" for delivering the exploits/malware/malicious commands
 - **Rather than fixing channels, better fix specifications and devices**
- Perhaps correct PJL specs + follow standard and safe low-level communication with devices on top of PJL
- Paranoid solution:
 - ▼ Print everything thru a virtual/proxy/<u>filtering printer</u>
 - * That will filter out unsafe/suspect payloads (and alert!), producing "safe" docs to print on real devices
 - Unless the virtual printer has bugs/<u>is exploitable itself</u> ©

Exploiting "test print" access in printers' EWS

- Print is unprotected! (and leaks internal network IP)
 - O Do vendors think diagnostics actions can be harmless?



Exploiting "test print" access in printers' EWS

- Accepts file as direct upload :
 - o Filters based **only** on extension: txt, pdf, pcl, ps
 - Will **not** accept:
 - *x print_my_hexor.rfu or*
 - x print_my_hexor**.fmw**
 - o Will accept:
 - x print_my_hexor.pcl!
 - x Yes, in PCL we can embed PJL UPGRADE/equivalent commands
 - Also, extension check doesn't enforce content check:
 - Rename print_my_hexor.pcl into print_my_hexor.pdf
 - And here we go again ©
 - Example: use HP_LJ5200_restart.pcl.pdf

Exploiting "test print" access in printers' EWS

- Accepts file as URL link to a printable document:
 - Exploit as in previous direct local upload
- Other interesting uses:
 - Check if printer can access external addresses (cool for commandand-control type of attacks)
 - Might reveal internal/external topology, as well as proxies along the way
 - ▼ If the chain is not properly configured and secured
 - Try to DoS the MFP in two types of <u>slowloris</u>
 - Attacker's http-client "slowloris" es MFP's EWS
 - Attacker's http-server "slowloris" es the MFP's initiated http-clients to our URL-document
 - ➤ Do both from above simultaneously ③
 - o Find race conditions in parsers: direct print, direct URL print, port 9100 print and print-server print; include also PJL/non-PDL cmds

Exploit printer management software

• MITM – HP Example – firmware.glf:

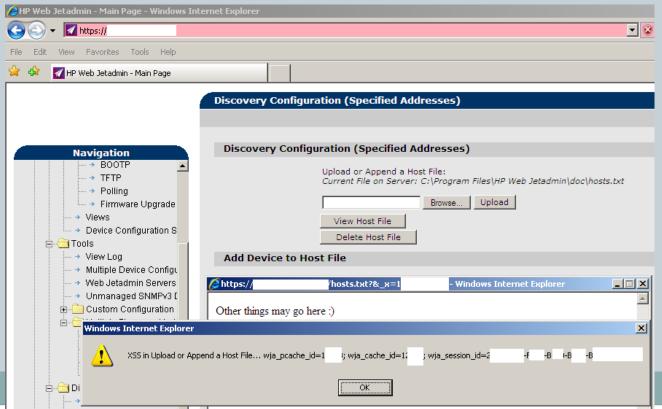
- Contains the links for DLD/RFU firmwares
- Used in WJA, HP Download Manager
- Uses plain HTTP (not even HTTPS), hence not a problem to MITM
- o Once MITMed, malicious DLD/RFU firmware binaries are supplied

Combined MITM+XSS attack:

- MITM and supply malicious firmware binaries (as described above)
- Exploit XSS bugs in admin panel of printer management software
 - ➤ Eg: HP WJA (or alike)
- Use XSS to trigger automatic upgrade of devices
- Two targets in one shot:
 - × Devices infected
 - Web-admin software owned by XSS (can serve other purposes as well)

Exploit printer management software

- Use XSS as an infection-trigger step in combined MITM+XSS attack
 - Eg.: HP WJA has various persistent-XSS bugs, injectable from external channels



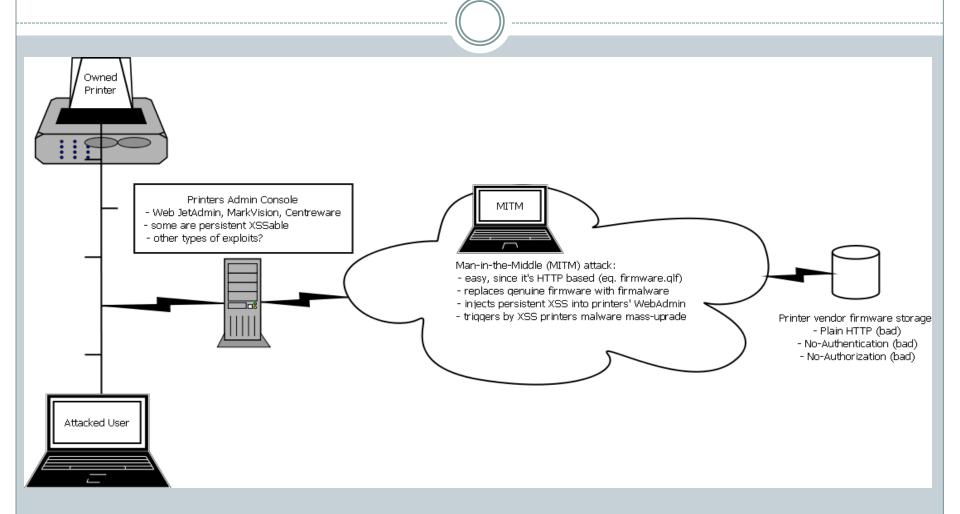
Locally-executed – Apps with rogue firmware

- If all other fail
 - o Because of: fixes in webserver, script-blockers, etc.
- Social engineer the user to "download and play a nice game" application
- Doesn't have to be a PC virus, a valid app will do ok:
 - o It will be just a printer malware
 - o So zero antivirus detection guaranteed still ☺
- Just connect to TCP port 9100 printer job spooler
- Dump the exploit/malware
 - Use @PJL UPGRADE style commands
 - Use @PJL FS* style commands

Locally-executed – Print subsystem hacks

- Find exploit stream for unidrv.dll/pscript5.dll
 - o Get LOCAL SYSTEM privileges (spoolsv.exe)
 - o unidrv/pscript5 dlls called from user space
 - × No need for admin
 - Called locally
 - o Called remotely via shared printers
 - Examples:
 - × Stuxnet, well yeah!
 - Contained oday exploiting <u>spoolsv.exe</u> / <u>StartDocPrinter</u> / policies
 - o Well, oday back in Apr 2009, Carsten have been warning
 - o I've been warning back in Apr 2010
 - o Nobody cared, except perhaps **SIGINTs**-related
- Printing sub-systems are broken...

MFPs attack vectors – Overall diagram



Once MPF is compromised – it attacks back (next)

ANDREI COSTIN, HACKCON OSLO, 2011

MFPs attack back

- Fuzz PC-based SNMP-enabled drivers
 - Exploit the SNMP stacks on the PC
- Produce oday PDF/TIFF crafted documents as a result of MFP activity
 - MFP scanners are internal trusted sources
 - O Victim with 99.99% certainty will open the PDF since:
 - Victim just scanned something
 - ▼ Victim expects the PDF to arrive
 - Victim doesn't believe MFPs can yet be infected
 - This accounts for those 0.01% ©
 - o On some MFPs, this can be accomplished via Java "applets"
- HP SmartInstall attacks (next slides)

MFPs attack back – HP SmartInstall

• HP SmartInstall autorun attack

- o About HP SmartInstall (plug-and-print)
 - Printers with built-in virtual CD-drives containing printer drivers
 - ▼ Is a specifically-wrapped *mkisofs iso 9660/hfs filesystem*
 - Designed to eliminate physical CDs/internet download hassle
 - ▼ Is stored inside some of the printer's NAND flash
 - ▼ Has provisions to be updated (by @PJL proprietary binary proto)
 - ■ "HP SmartInstall" because smart attackers know what they want
 - ▼ Is a possible solution for attacking <u>air-gapped networks/PCs</u>
 - Like some USB sticks did in stuxnet case
 - Need to patch FWUpdate.exe or live-dissect the protocol
 - To bypass FWUpdate's logic that "HP SmartInstall is up-to-date"

Live demo

 \times Instead of *calc.exe* run *shutdown -r -f* for booting attack (next sld)

MFPs attack back – HP SmartInstall

HP SmartInstall bootloading attack

```
Boot Menu

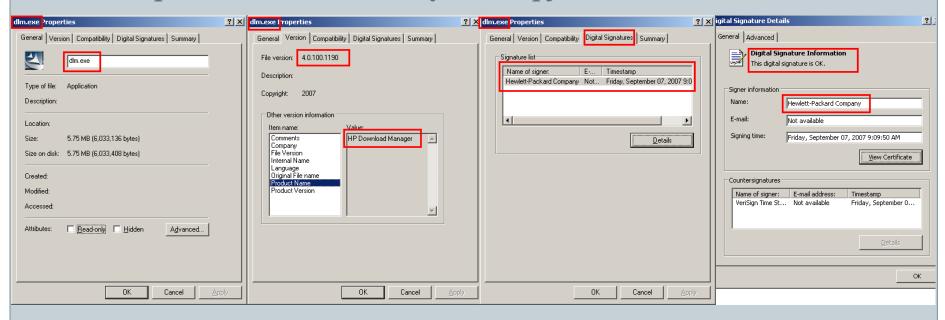
1: ATA HDDO: ST - (S1)
3: ATA HDD1: HITACHI HT A
4: USB CD: HP Smart Install-(USB 7: PCI LAN: IBA GE Slot 0200 v125
```

Attack

- ▼ Flash into HP SmartInstall NAND a "hackers swiss-knife" ISO
- × Prerequisite: USB CD-drive is the highest priority boot device
- × ISO: silently boots, dumps data (hives with passwords, etc.), the minimalistic TCP/IP sends dumps to the attacker
- Feature <u>HPSiB</u> (Happy Printer: Smiling Bootloader)
 - Why not use the printer as safe-boot device?
 - **Eg.:** recover admin password, have minimalistic Linux, fun, etc.

Privacy/transparency concerns

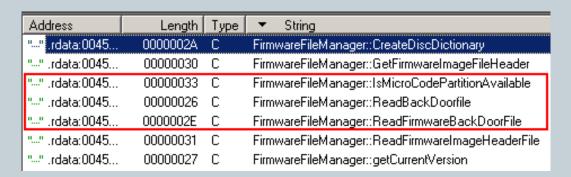
- Not satisfied with <u>printer tracking dots</u>?
- Satisfaction guaranteed with:
 - HP Download Manager a story from backstagedoor
 - Will present minimal analysis of hpjdwnld.exe



Privacy/transparency concerns

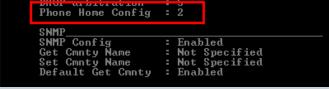
o Important note:

- × It's <u>not</u> managing a PC-backdoor
- x It is managing an MFP/JetDirect-backdoor
- *x strings* utility is enough to spot it
- Checks for %INST_DIR%\upgrades\jetdirect\SpecialUpgrades.txt
- Checks special firmware files for ShortStack/CodeImage microcodes
- ➤ If you have samples for above 2 items, please share them!
- ➤ Possibly similar to <u>AMD K8 Microcode backdoor update feature</u>



Privacy – What about PhoneHome feature?

- Phone Home feature in HPs
 - Present in EWS of devices (telnet/web/snmp interfaces)
 - × SNMP MIB is <u>1.3.6.1.4.1.11.2.4.3.7.31.0</u>
 - "Use an SNMP management or command line utility to set the object identifier (OID) .1.3.6.1.4.1.11.2.4.3.7.31.0 to zero (0)"
 - x telnet "...use the Telnet "phone-home-config: o" ... "



Present in WJA software package



KCON OSLO, 2011

Privacy – Some thoughts

- PhoneHome (1.3.6.1.4.1.11.2.4.3.7.31.0) <u>privacy</u> statement says:
 - "If permitted to do so, HP will collect this information as statistical data only and use it to improve product features and services. Personal data is not collected in accordance with HP privacy policies"
 - Well, name implies something else
 - We want all its juicy details ©
- <u>PhoneHome</u> + JetDirect Firmware <u>Backdoor</u>
 - Can be easily misused by HP
 - Raises (at least should!) privacy concerns
 - Not very well documented by vendors
 - Can be misused by malicious attackers
 - After all, multiple naming FAIL!

Printer debugging (or lack of it)

- syslogd messages examples
 - o Most *syslogd*'s are not very debugging-friendly

Syslogs				
TimeStamp	Agent	Facility	Level	Alert
Fri Aug 27	10.27.2.20	lpr	informational	<54> printer: error cleared
Fri Aug 27	10.27.2.20	lpr	error	<51> printer: offline or intervention needed
Fri Aug 27	10.27.2.20	lpr	informational	<54> printer: error cleared
Fri Aug 27	10.27.2.20	lpr	informational	<54> printer: peripheral low-power state
Fri Aug 27	10.27.2.20	lpr	informational	<54> printer: ready to print
Fri Aug 27	10.27.2.20	lpr	warning	<52> printer: powered up
😿 Fri Aug 27	10.27.2.20	lpr	debug	<55> printer: syslog started
Fri Aug 27	10.27.2.20	lpr	error	<51> printer: offline or intervention needed
Fri Aug 27	10.27.2.20	lpr	informational	<54> printer: ready to print
Fri Aug 27	10.27.2.20	lpr	warning	<52> printer: powered up
V Fri Aug 27	10.27.2.20	lpr	debug	<55> printer: syslog started
Fri Aug 27	10.27.2.20	lpr	error	<51> printer: offline or intervention needed

HP Security Solutions

- o "Q23. 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"
 - ➤ Well, PoC-community or some haxor or some IT-criminals might change that "in practice" then!
- "Firmware generally behind software in terms of secure development & deployment" – more than true
 - ▼ Wonder if HP's SecLab PhlashDance ever reached HP's MFP R&D

Sharp Security Suite

- "Sharp MFP products use unique embedded firmware and are not based on Windows operating systems. Therefore, Sharp MFP's internal systems are not subject to the same Virus vulnerability as Microsoft operating systems. We believe this approach provides the internal systems of our products with protection against common Windows executable viruses and other similar infectious software programs."
 - ➤ Well, possibly are vulnerable to *other* (i.e. not same) virus vulnerabilities!

- Lexmark MFP Security, Samsung MFP Security
 - "In other areas, the security considerations around printers/MFPs are substantially different: they generally don't run conventional operating systems, they don't have network file shares that need to be secured, they probably don't need or support antivirus software, etc."
 - × Who did copy from who that text? Or they just assumed *the leader* is right and mutually-copy-pasted?
 - x "...probably..." ?!
 - Nowadays, if you have an OS, a FS and externally connected execution environment, most likely you need internal antivirus/IDS/IPS

- Final thought on above "secure thinking" quotes
- Remember <u>psybot</u>? To summarize
 - Non-conventional arch *true* MIPS
 - o Non-conventional OS − *true* Mipsel Linux
 - Doesn't support antivirus *true* "why should we?!"
 - o Got owned − *very true* − ~100k devices in a sophisticated command-and-control botnet
 - o If you need more arguments for securing/cleaning embedded devices, running <u>unconventional</u> OS+arch which do not support secure/antimalware standards/frameworks
 - ▼ Perhaps security is your *lowest priority hobby* my \$0.02...

Solutions – Printer Vendors' Side

- First, accept that present day printers (especially network ones) are:
 - Full-blown computers themselves
 - A security target/threat
 - To be considered as part of Secure Development/Testing/Audit Lifecycles
- Fix those specs and parsers (PJL, PCL, PML, PDF, PS)
- Fix those damn web/telnet/ftp/snmp/etc. interfaces
- If first random 200 bytes fuzz string <u>crashes/bricks</u> <u>your device</u>...
 - o ...time to put in practice **SDL**. we are in 2010, remember?...

Solutions – Printer Vendors' Side

- <u>Authenticate uploader, crypt, sign and verify signature</u> of the uploaded firmware
 - O Btw, homebrew or kindergarten crypto is NOT crypto!
 - o Or make (some) implementations FOSS so open and secure standards can be implemented (oh, these utopist ideas...)
- Be fair!
 - Transparent and backdoor-free systems/software
- Collaborate with antimalware vendors for your platforms
 - Could win you a nice marketing step
- Last but not least remove default passwords and make <u>mandatory strong-password changes</u> as part of the initial setup procedures/installations

Solutions – Antimalware Vendors' Side

Collaborate with vendors and security community

- Make vendors understand those MFPs are real exploitable targets
- Also, it could be a good marketing step "First antimalware on printers/MFPs"
- Develop open and secure practices/protocols for in-printer antivirus management and updates

If above collaboration does not work

- Sponsor high-profile MFP exploit botnet volunteers are out there
- You have your foot in the "MFP antimalware market" `s door
- o This point is more to be joke ☺
- o Though, not that there were no surprising developments

Setup honey-pots for most-spread MFPs EWS :

- Similar to renowned <u>/etc/passwd</u>
- Study blackhats/bots actions to train IDS/IPS for MFPs
- o Get samples of firmalware or exploit payloads (PJL, PS, PCL)
- ... even though AV concept is being considered obsolete

Solutions – Admins' Side

- Develop and follow secure periodic practices and checklists for all your MFPs/printers
- Use and analyze extensive logging using MFPs management platforms
- Properly isolate MFPs on appropriate network segments
- Perhaps implement stricter domain-level printing policies
- Well, last but not least don't leave those default accounts/passwords on

Solutions – IDS/IPS

- Update and improve printer-based IDS/IPS sigs
 - Addresses to antimalware and admin side

- Dilemma
 - Start filtering in paranoid mode, but...
 - Can impact a scheduled mass upgrade of net-administered MFPs
 - Can impact pretty valid print jobs
 - Where should the balance be...?
 - Real solution is to fix the specs

Solutions – IDS/IPS

- Snort IDS signature samples
 - o The RDYMSG is only annoying
 - ➤ Don't <u>SNORT it</u>, cron it on repetitive (RDY/OP/SYS)MSG reset

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 9100 (msg:"POLICY HP
JetDirect LCD modification attempt"; flow:to_server,established;
content:"@PJL RDYMSG DISPLAY ="; classtype:misc-activity;
reference:bugtraq,2245; reference:arachnids,302; sid:568; rev:5;)
```

- o PDOSing is not fun anymore is already a concern
 - * Though this **SNORT** rule sucks. Do you see why?

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 9100 (msg:"ET EXPLOIT Xerox
WorkCentre PJL Daemon Buffer Overflow Attempt";
flow:established,to_server; content:"ENTER LANGUAGE ="; depth:50;
nocase; isdataat:55,relative; content:!"|OA|"; within:55;
pcre:"/ENTER\x20LANGUAGE\x20\x3D.(55)/smi"; classtype:attempted-admin;
reference:url,www.securityfocus.com/bid/38010
<http://www.securityfocus.com/bid/38010>; sid:18000211; rev:1;)
```

- The real pain is MFP malware (PJL UPGRADE types)
 - Your pride starts having pains in your back... unless fixed
 - pcre:"/ENTER[\x20]+LANGUAGE..."

Solutions – Users' Side

- Stay updated to latest firmware of the printer's vendor
 - Make sure you choose a security-aware vendor (but skip the marketing BS between the lines)
- Don't print anything from untrusted sources
 - Well, this is hard... everybody is untrusted today
- Don't open unknown files
 - Not guaranteed that malware detection is triggered for printersrelated malware
 - Important point exploits the MFP, no need for admin rights on PC!
- Log and monitor printers' activity
 - Connects from it's IP
 - Paranoid mode USB data filter from the printer to host PC
 - You never know what bugs do printer's driver have on the PC
- Use safe virtual printers to produce malware-free docs

Conclusions

- As PoC shown, printers are exploitable
- Specs have holes and are outdated for the new IT security realities:
 - O Device and antimalware vendors seem to ignore the issues... yet
- MFPs are more than "dummy printers" these are fullblown machines with great power and connectivity
- MFPs tend to interact with same (or even bigger) number of technologies as computers:
 - o Eth
 - WiFi
 - o RFID
- MFPs have access to almost same set of secrets as PCs

Credits/Props/Recommended reading

- Slobotron on Hacking Printers (2002)
- phenoelit's HP resources (2002)
- <u>Irongeek's "Hacking Network Printers"</u> (2006)
- <u>"Exploiting Printers by Analyzing Their Firmware"</u>
 (2009)
 - Nowhere to find on the net... censored?!
- "Juste une imprimante" (2010)
- Ben Smith's "Printers gone wild!" (2011)
 - o printFS, pyPJL, bruteForcePJL kit

Credits/Props/Recommended reading

- "Vulnerabilities in Not-So-Embedded Systems"
- "Network Printing" book
- MFP Security for Enterprise Environments
- SANS Auditing and Securing Multifunction/MFP
 Devices
 - Amuzing note: "Using this port and the right utility you can, among other things, *change what shows up on the LCD display*. Modification of the LCD panel, either causing confusion ("Out of Service") or opening the door for social engineering purposes ("Error. Call 555-5151.")."
- cyrtech.de

@PJL COMMENT = "Insert coins to continue"

• 3





\H1B%-12345X@PJL EOJ "HackingPrinters"

• Print-in-touch:

o lpr <u>-Phoneypot-printer@andreicostin.com</u> -Y -J "Hacking Printers" -T "Comments/suggestions/collaboration" -m <u>andrei@andreicostin.com</u> -m <u>zveriu@gmail.com</u> -- -

• Till next time... keep your MFPs safe as golden:

