Hacking printers

years down the road

Impressum

- Andrei Costin
- Author of MFCUK
  - MiFare Classic Universal toolKit
- Generally interested in:
  - 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:

- *big fat one – because everybody *loves* fineprints

\H1B%-12345X@PJL JOB “HackingPrinters”

- Who & When?
  - Bits of history and present
- Why?
  - Motivation
- What?
  - Market profile
- How & Where?
  - Avenues & techniques
- ?!
  - What’s next and when to expect
  - What did we/industry learn
  - Q&A

01001011 of history

- Phenoelit (2002)
  - First public in-depth research on:
    - PJL vulnerabilities
      - Small password keyspace
      - Non-secured FS access
      - Non-secured access to service functionality (LCD, etc.)
    - Unsecured embedded services on printers (FTP, HTTP, SNMP, etc.)
    - Hacks for HP's proprietary ChaiVM
  - First public release of printer hacking srcs/tools:
    - Hijetter
    - libPJL
    - ChaiPortScan, ChaiCrack

01001011 of history

- Slobotron (2002)
  - Shed light on many aspects of printers hacking:
    - Processors
    - External Languages
    - Internal Languages (PML,EML,VarWare etc)
    - OSes, Using an UNsupported OS
    - Firmware Debugging
    - Remote Firmware Erasing
    - Driver Hacking
    - Applied Printing : Fake Banknotes
    - Touched on hacking HP-printers
  - Essay mainly focused on print-cartridges hacking
  - Claimed that *"TCL can be useful to write data inside protected memory areas if you know the right memory mapping"*
    - Turns out, some vendors even document it ☺
    - @PJL WNVRAM and @PJL RNVRAM

01001011 of history

- Irongeek's "Hacking Network Printers" (2006)
- First and most comprehensive compendium of printer hacking
- Covers wide range of topics:
  - Default passwords
  - Telnet
  - SNMP
  - FTP
  - HTTP
  - Many other tricks

01001011 of present

- "Juste une imprimante" (2010)
- Covers:
  - Lexmark models
  - Mainly Linux-based printers
  - Reverse engineering of the firmware
  - Debugging of the firmware
  - How-to on finding exploits and bugs in those firmwares

01001011 of present

- "Printers gone wild!" (2011)
- Mainly focusing on PJL commands
- A nice kit written in python:
  - printFS
  - pfsScanner
  - pyPJL
  - printJack
  - pyPJLpass

01001011 of present

- Printer to PWND – PRAEDA (2011)
  - Printer data harvesting
  - Written in PERL (migrating to Ruby)
  - Extracts from printer (admin) pages:
    - Various usernames
    - LDAP passwords
    - POP3 passwords
    - SMTP passwords
    - SNMP passwords
    - FTP passwords
    - SMB passwords
  - Tries default admin passwords or auth-bypass exploits

MFPs Exploitation – Why?

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

MFPs Exploitation – Why?

- MFPs interact with (hence can get access to):
  - RFID badges
  - Smart/swipe cards
  - Fingerprints
  - PINs
  - LDAP/domain passwords
  - Aren't these most-wanted things we are hunting after all?

MFPs Exploitation – Why?

- 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

MFPs Exploitation – Why?

- Not so much information in this area (compared to PC or mobile devices)
  - PJL UPGRADE – approx 6 results
  - PJL LPROGRAMENG – 0 results
  - PJL LPROGRAMRIP – 1 result (security paper)
  - PJL DMINFO – approx 300 results
  - PJL DMCMD – approx 75 results
  - Compare with this PDF "/Launch" – approx **55 Mln** results
- Too few known (more or less) public researches
- Recent disclosures mainly focused on web-admin, snmp, XSS and uncontrolled buffer overflows
  - Not too much detailed analysis on OS, kernel and firmware level

“Who’s who”

- Big number of devices – according to Gartner:

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)

- 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

“Who’s who”

- Sadly for exploiter, is very fragmented
- Vendor/arch/OS/device-class/prod-line/etc.
- I see it something like this

MFPs Exploitation – (Mis)use scenarios

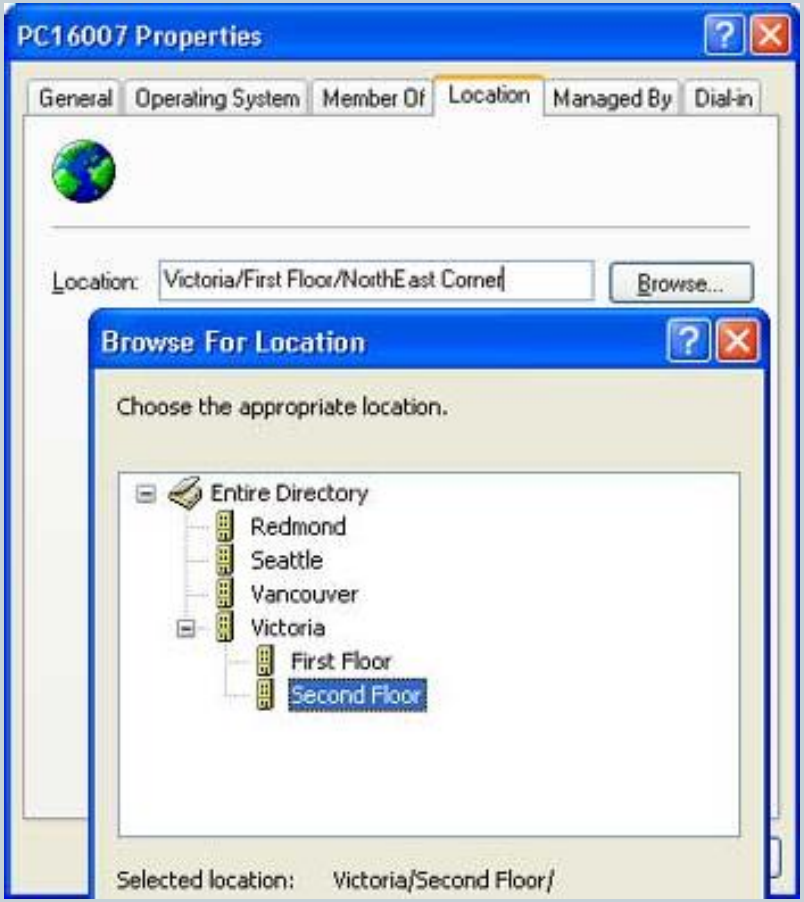
- PDOS aka bricking
  - Some printed documents did it by mistake…
- Idle-time processing
- Malware/upload storage
- “Stealth”/uncleanable command and control
- Unencrypted data theft
- Corporate/enterprise/intelligence assets data theft
- Spam inside/outside networks
- Ransomware
- Espionage
- MFPs attack back (slides below)
- Physical attacks

Geolocation over MFPs

- Geolocation=identification of an object's real-world geographic location
- Geolocation for MFPs
  - MS's Printer Location Tracking (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
  - IETF PWG's IPP Everywhere
    - Uses "geo:" URI scheme
    - Looks like:
      - "printer-geo-location", char[2048], IPP:uri, SM: anyURI maxLen=2048
      - geo:43.220973,-77.417162,128;u=1.83 (u=uncertainty 1.83m)
  - DNS LOC (see the paper)
    - Exciting stuff, though not too many domain admins chose to publish their GPSes ☺
- Comparison: printing subsystem vs mobile-communication networks
  - GSM: MS-assisted with NW-based computation of GPS coordinates
    - PLT: MFP-assisted with AD/PLT-based reverse geolocation lookup
  - GSM: MS-based with NW-assisted computation of GPS coordinates
    - IPP: MFP-based direct "geo:" coding

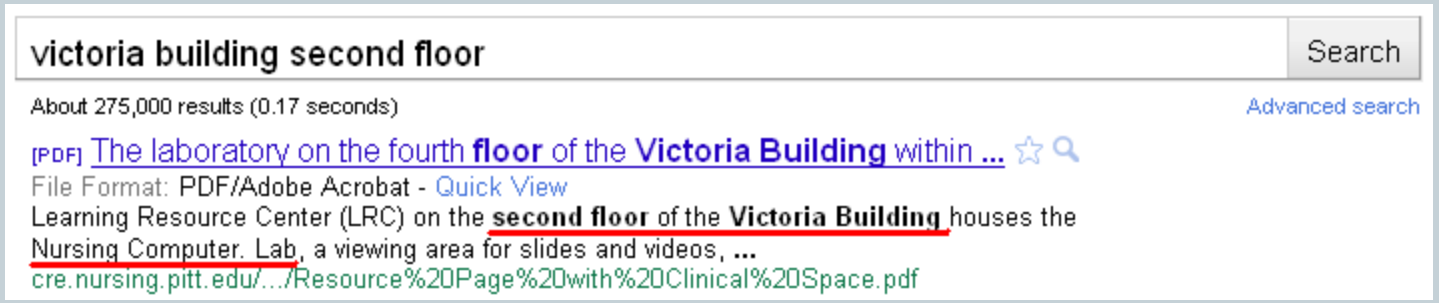
Geolocation over MFPs

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

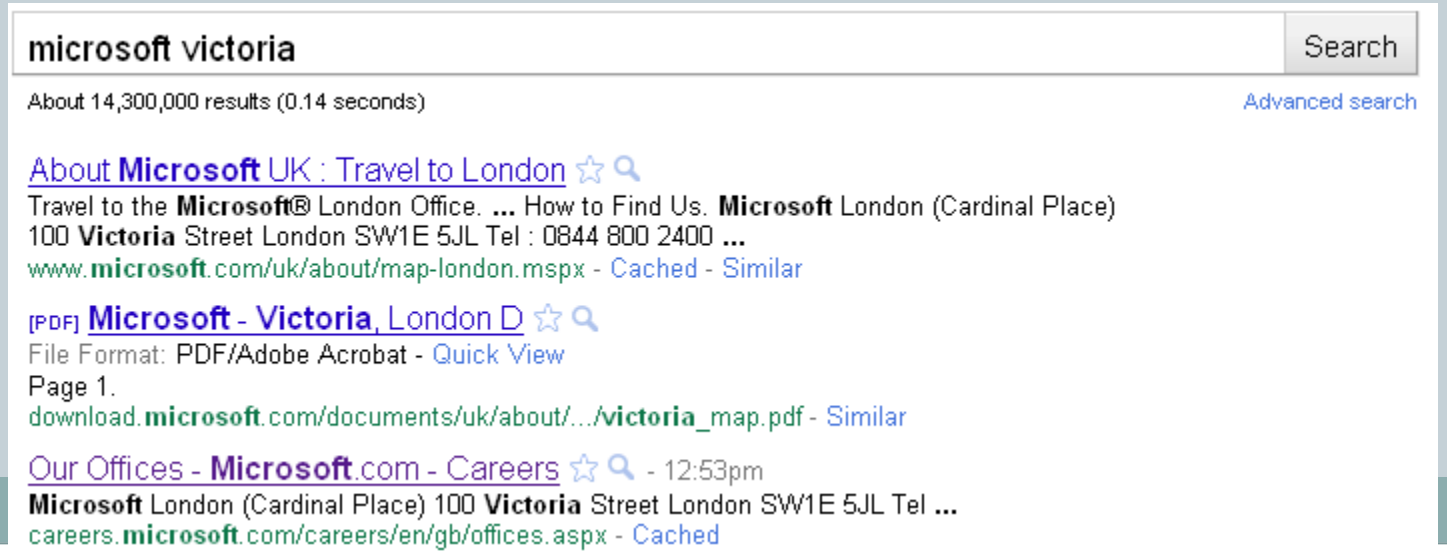


Geolocation over MFPs

- MS magazine – from example to practice:
  - Use: “victoria building second floor” for reverse geolocation lookup – false positive ☹

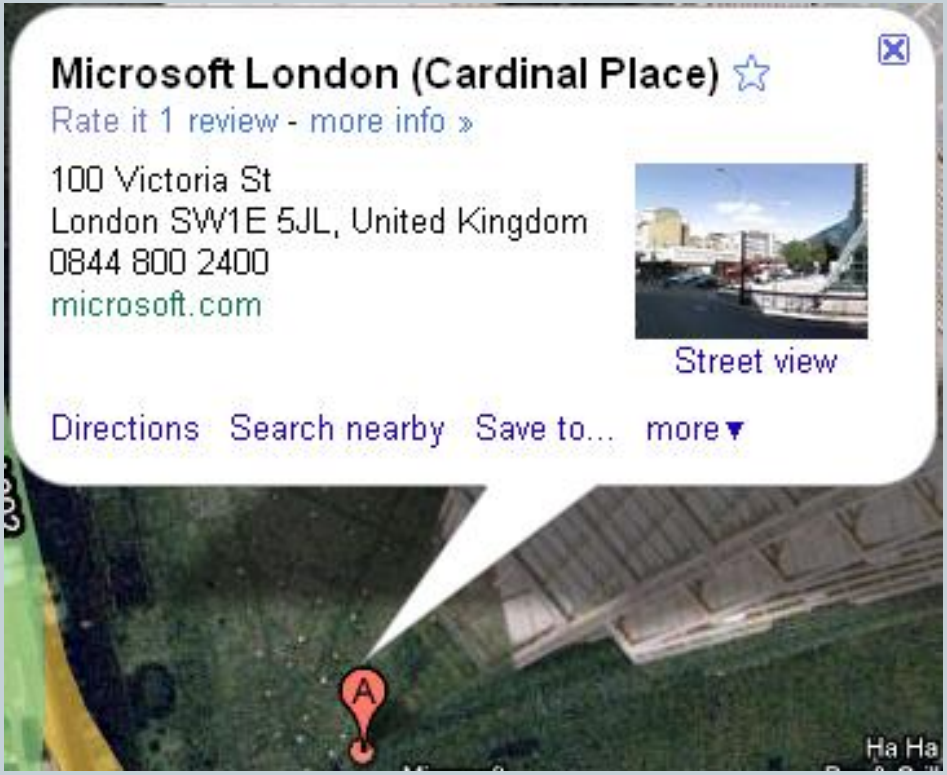


  - Use: “microsoft victoria” for reverse geolocation lookup – first hit ☺!



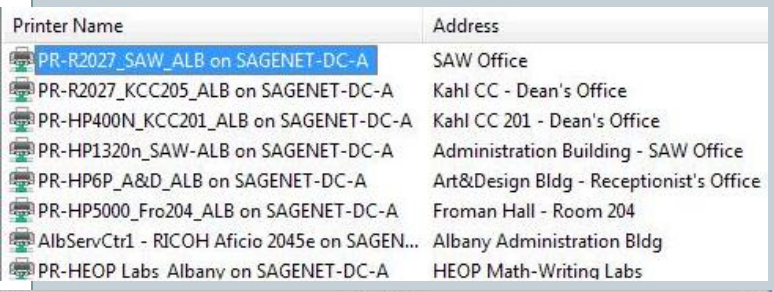
Geolocation over MFPs

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

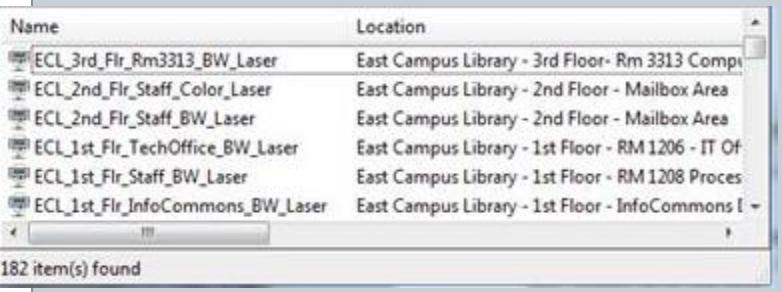


Geolocation over MFPs

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

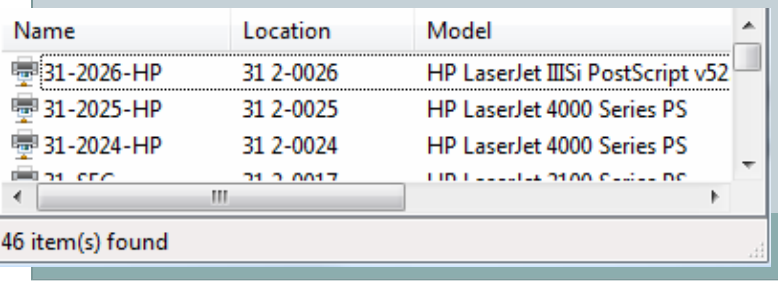


Printer Name	Address
PR-R2027_SAW_ALB on SAGENET-DC-A	SAW Office
PR-R2027_KCC205_ALB on SAGENET-DC-A	Kahl CC - Dean's Office
PR-HP400N_KCC201_ALB on SAGENET-DC-A	Kahl CC 201 - Dean's Office
PR-HP1320n_SAW-ALB on SAGENET-DC-A	Administration Building - SAW Office
PR-HP6P_A&D_ALB on SAGENET-DC-A	Art&Design Bldg - Receptionist's Office
PR-HP5000_Fro204_ALB on SAGENET-DC-A	Froman Hall - Room 204
AlbServCtr1 - RICOH Aficio 2045e on SAGEN...	Albany Administration Bldg
PR-HEOP Labs Albany on SAGENET-DC-A	HEOP Math-Writing Labs



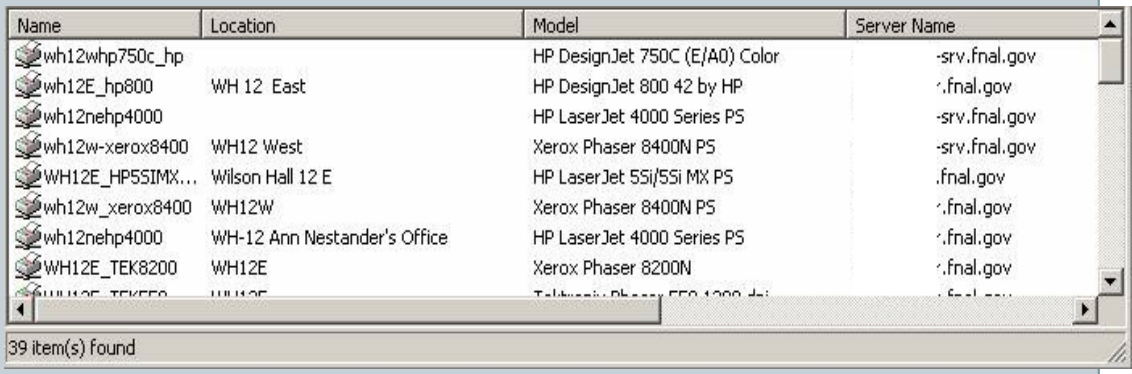
Name	Location
ECL_3rd_Flr_Rm3313_BW_Laser	East Campus Library - 3rd Floor- Rm 3313 Compu
ECL_2nd_Flr_Staff_Color_Laser	East Campus Library - 2nd Floor - Mailbox Area
ECL_2nd_Flr_Staff_BW_Laser	East Campus Library - 2nd Floor - Mailbox Area
ECL_1st_Flr_TechOffice_BW_Laser	East Campus Library - 1st Floor - RM 1206 - IT Of
ECL_1st_Flr_Staff_BW_Laser	East Campus Library - 1st Floor - RM 1208 Proces
ECL_1st_Flr_InfoCommons_BW_Laser	East Campus Library - 1st Floor - InfoCommons [

182 item(s) found



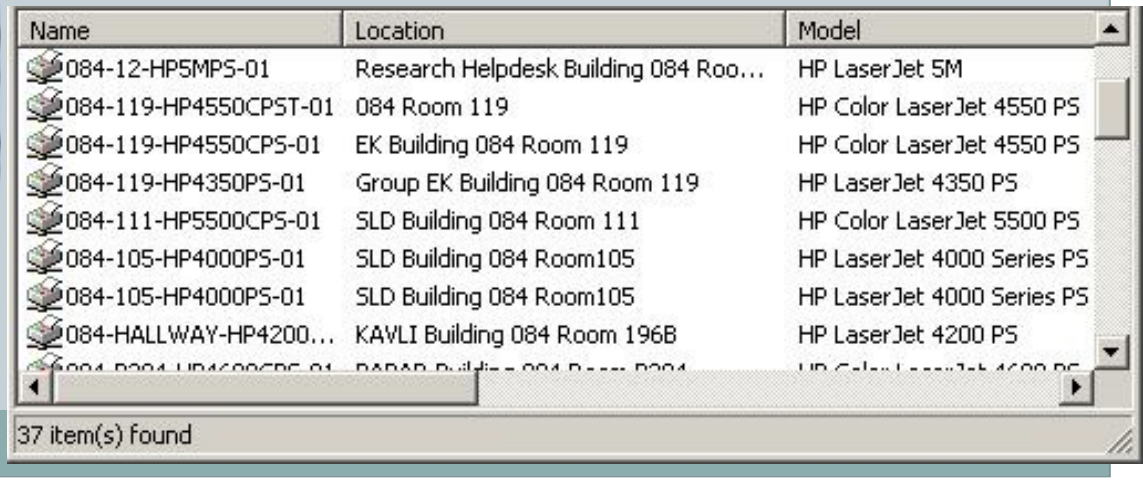
Name	Location	Model
31-2026-HP	31 2-0026	HP LaserJet IIISi PostScript v52
31-2025-HP	31 2-0025	HP LaserJet 4000 Series PS
31-2024-HP	31 2-0024	HP LaserJet 4000 Series PS

46 item(s) found



Name	Location	Model	Server Name
wh12whp750c_hp		HP DesignJet 750C (E/A0) Color	-srv.fnal.gov
wh12E_hp800	WH 12 East	HP DesignJet 800 42 by HP	.fnal.gov
wh12nehp4000		HP LaserJet 4000 Series PS	-srv.fnal.gov
wh12w-xerox8400	WH12 West	Xerox Phaser 8400N PS	-srv.fnal.gov
WH12E_HP5SIMX...	Wilson Hall 12 E	HP LaserJet 5Si/5Si MX PS	.fnal.gov
wh12w_xerox8400	WH12W	Xerox Phaser 8400N PS	.fnal.gov
wh12nehp4000	WH-12 Ann Nestander's Office	HP LaserJet 4000 Series PS	.fnal.gov
WH12E_TEK8200	WH12E	Xerox Phaser 8200N	.fnal.gov

39 item(s) found



Name	Location	Model
084-12-HP5MPS-01	Research Helpdesk Building 084 Roo...	HP LaserJet 5M
084-119-HP4550CPST-01	084 Room 119	HP Color LaserJet 4550 PS
084-119-HP4550CPS-01	EK Building 084 Room 119	HP Color LaserJet 4550 PS
084-119-HP4350PS-01	Group EK Building 084 Room 119	HP LaserJet 4350 PS
084-111-HP5500CPS-01	SLD Building 084 Room 111	HP Color LaserJet 5500 PS
084-105-HP4000PS-01	SLD Building 084 Room105	HP LaserJet 4000 Series PS
084-105-HP4000PS-01	SLD Building 084 Room105	HP LaserJet 4000 Series PS
084-HALLWAY-HP4200...	KAVLI Building 084 Room 196B	HP LaserJet 4200 PS

37 item(s) found

Geolocation over MFPs

- Some even do all the “dirty job” for us (meta over OSM):

Geolocation over MFPs

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

Geolocation over MFPs

- Demo – the map
  - (And this is just public IP based geolocation map….)

Main printer specifications

- Myriad of specs and languages… %)
- UEL – Universal Exit Language
  - Just one command
    - ***<esc>%-12345X*** *(<esc> is 0x1B aka \H1B aka ESCape)*
- PJL – Printer Job Language
  - Developed by HP
  - Job level controls: printer language switching, job separation, environment, status readback, device attendance and file system commands
- PML – Printer Management Language
  - HP's object-oriented request-reply protocol to exchange device management information
  - PML can be used to query SNMP values from a printer device

Main printer specifications

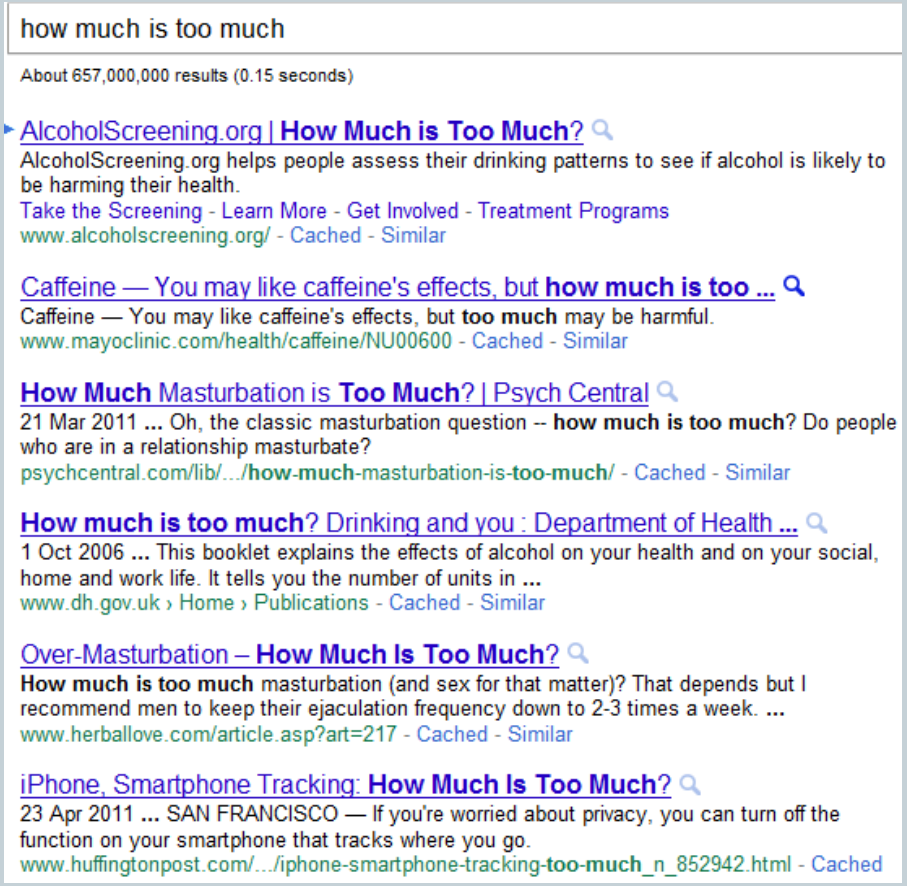
- PS – PostScript Language
  - Developed by Adobe
  - Mostly formatting-control language
- PPD – Adobe PS Printer Description
  - Describe the entire set of features and capabilities available for their PostScript printers
- PCL – Printer Control Language
  - Developed by HP
  - It's more a formatting-control language, like PS
- GPD – Generic Printer Description
  - Windows GDI-based spec, similar to PPD
  - Used for creating unidrv.dll minidrivers for non-PS printers
  - Usually here: *c:\windows\system32\spool\drivers*

Specifications *"fineprints"

- (some) PJL holes:
  - No standard provisions for strong authentication
  - No standard provisions for encryption
    - All usernames, PINs & passwords are in clear-text
      - @PJL SET USERNAME="HackingPrinters"
      - @PJL SET HOLDKEY="1234"
      - @PJL SET **KM**USERKEY2 = "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
    - Also, specs say nothing about N-tries-and-fails scenario actions
      - Again, the wheel…

PJL "Parade"

- PJL – obeys the "HMITM? – more is never enough!"


how much is too much

About 657,000,000 results (0.15 seconds)

AlcoholScreening.org | **How Much is Too Much?**
AlcoholScreening.org helps people assess their drinking patterns to see if alcohol is likely to be harming their health.
Take the Screening - Learn More - Get Involved - Treatment Programs
www.alcoholscreening.org/ - Cached - Similar

Caffeine — You may like caffeine's effects, but **how much is too ...**
Caffeine — You may like caffeine's effects, but **too much** may be harmful.
www.mayoclinic.com/health/caffeine/NU00600 - Cached - Similar

How Much Masturbation is **Too Much**? | Psych Central
21 Mar 2011 **...** Oh, the classic masturbation question -- **how much is too much**? Do people who are in a relationship masturbate?
psychcentral.com/lib/.../**how-much**-masturbation-is-**too-much**/ - Cached - Similar

How much is too much? Drinking and you : Department of Health **...**
1 Oct 2006 **...** This booklet explains the effects of alcohol on your health and on your social, home and work life. It tells you the number of units in **...**
www.dh.gov.uk › Home › Publications - Cached - Similar

Over-Masturbation – **How Much Is Too Much**?
How much is too much masturbation (and sex for that matter)? That depends but I recommend men to keep their ejaculation frequency down to 2-3 times a week. **...**
www.herballove.com/article.asp?art=217 - Cached - Similar

iPhone, Smartphone Tracking: **How Much Is Too Much**?
23 Apr 2011 **...** SAN FRANCISCO — If you're worried about privacy, you can turn off the function on your smartphone that tracks where you go.
www.huffingtonpost.com/.../iphone-smartphone-tracking-**too-much**_n_852942.html - Cached

PJL “Parade”

- @PJL
  - UPGRADE (HP)
  - LPROGRAMENG (Lexamrk)
  - LPROGRAMRIP (Lexmark)
  - DMINFO (HP)
  - DMCMD (HP)
  - WNVRAM ADDRESS=0xDEAD DATA=0xBEEF
  - RNVRAM ADDRESS=0xB00B
  - NVRAMINIT
  - CLEARNVRAM
- @PJL ENTER LANGUAGE
  - PDF
  - TIFF
  - ACL
  - UPGRADE
  - TISDOWNLOAD

PJL “Parade”

- @PJL SUPERUSER
  - SUPERUSER PASSWORD = 12345
  - SUPERUSEROFF
- @PJL EXECUTE
  - SHUTDOWN
  - PRTCONFIG
- @PJL INFO
  - BRFIRMWARE
  - BRFIRMREADY
  - BRFIRMCHECK
- @PJL COMMENT
  - EFIPJL (Minolta)
    - SET PASSWORDUSE=0/1
    - SET PassWord="####“

PJL “Parade”

- @PJL DEFAULT
  - FLASHSYS = ONBOARDFLASHSYS
  - DBGSTATMOD
  - WIRELESSSCAN
  - WIRELESSSETAP
  - WIRELESSRESETCFG
  - NETWORKCONF
  - MAKEMSWRITABLE
  - SYNCNAND
  - CLEARSIINSTALL
- @PJL SET
  - SERVICEMODE=HPBOISEID/EXIT
    - i.e. HP offices in Boise, ID, US
  - DIAGNOSTICS=ON/OFF

PJL “Parade”

- @PJL SET
  - JOBATTR=“@SWDL”
  - BRFIRMMEMVER=“a.b.c.d”
  - SERIALNUMBER=1234
  - USERNAME = “root”
  - HOLDKEY="1234“
  - KMUSERKEY2 = “toor“
  - PCFAXMODE=FAX
  - PCFAXPAS=1234/OFF
  - PCFAXNUM0= "FAX,+1-555-123456,1,0,1“
  - FAXTEL = +1-555-123456

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
- Leaking cryptographic material

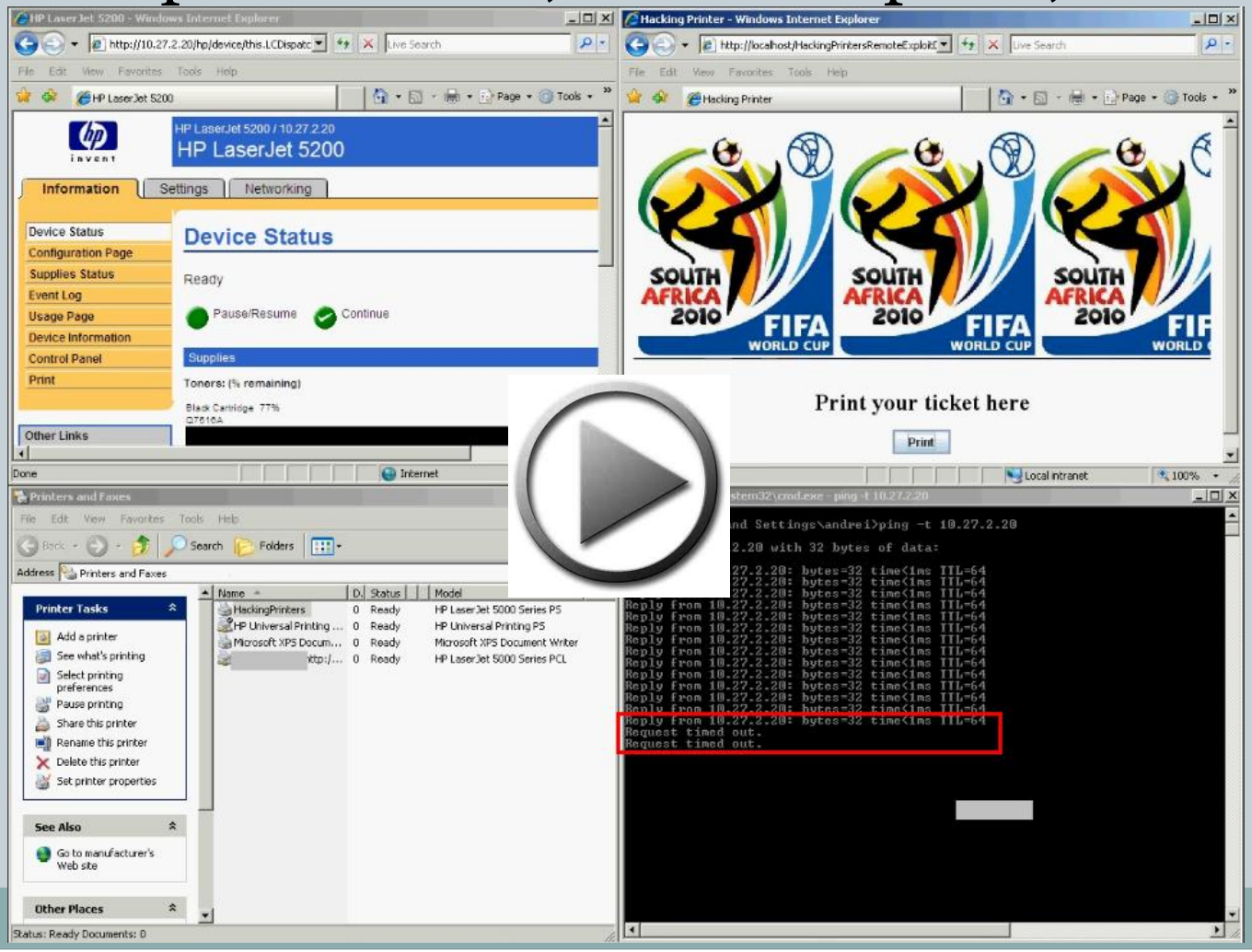
Remote-initiated printing exploit

- 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
  - "mayscript" yes, "scriptable" true, jso = JSObject.getWindow(this), jso.call("startPrintingPPE"...)
- Can be successful using social engineering/nagging
  - 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"
  - Same as phenoelit's trick (BH2002)
    - 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 – *pjl_print_applet.java*
  - PrintService
  - PrintServiceLookup
  - DocPrintJob
  - JobName
  - SimpleDoc
  - … and DocPrintJob.print()

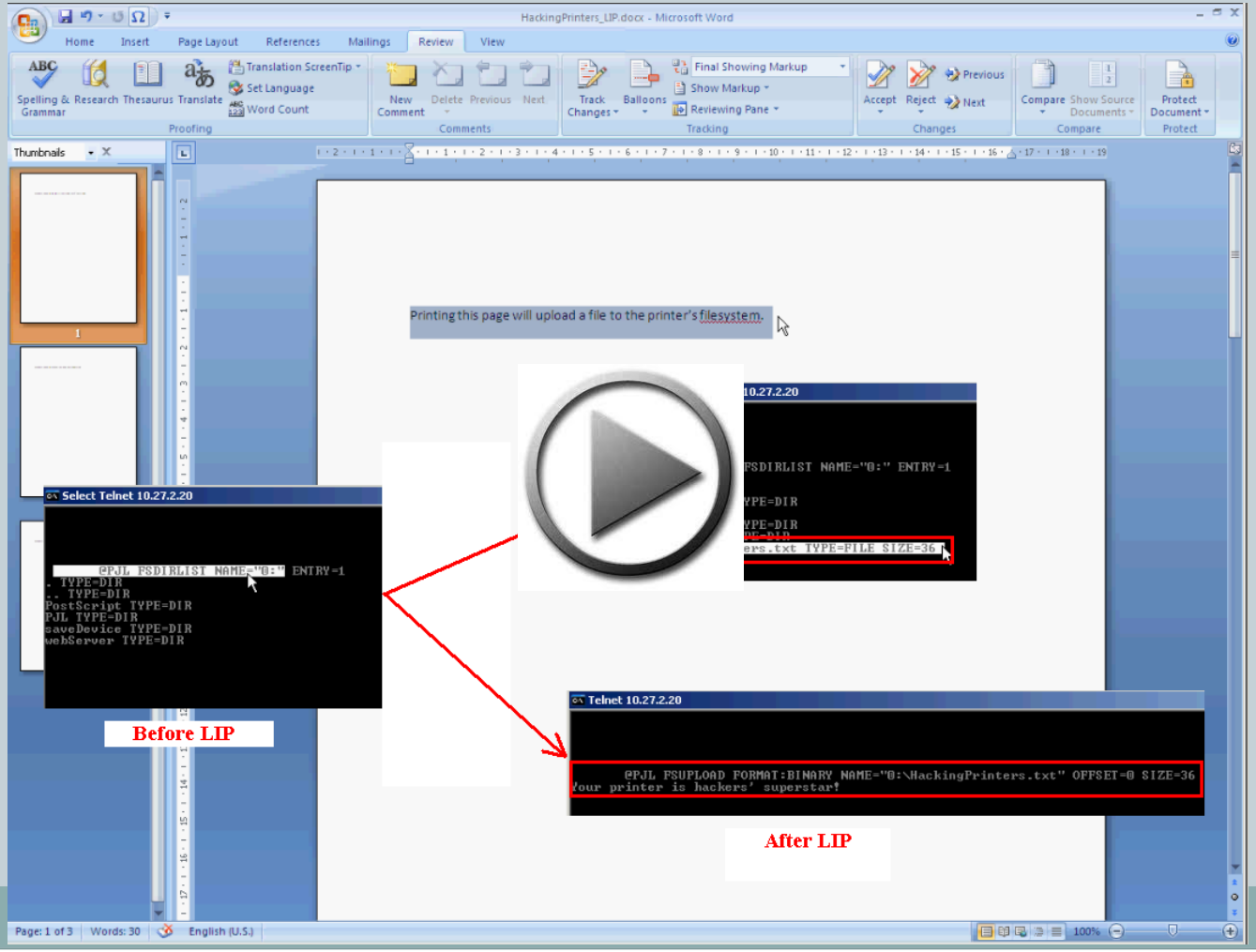
Locally-initiated printing exploit

- MS Word
  - "Print and get your printer owned" type of exploit
  - Will video demo in next slide
- Adobe LiveCycle XDC files (XML files)
  - Used in SAP® environments
  - "Infect"/replace all XDC files with required firmalware payload
    - Doesn't necessarily need admin rights
  - 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>
<seq id="preDoc"><ESC/>%-12345X@PJL RDYMSG DISPLAY=""&#13;&#10;
@PJL UPGRADE SIZE = 1024&#13;&#10;[hex_encoded_payload]<ESC/>%-12345X</seq>
</pdl>
</xdc>
</xdp:xdp>
```

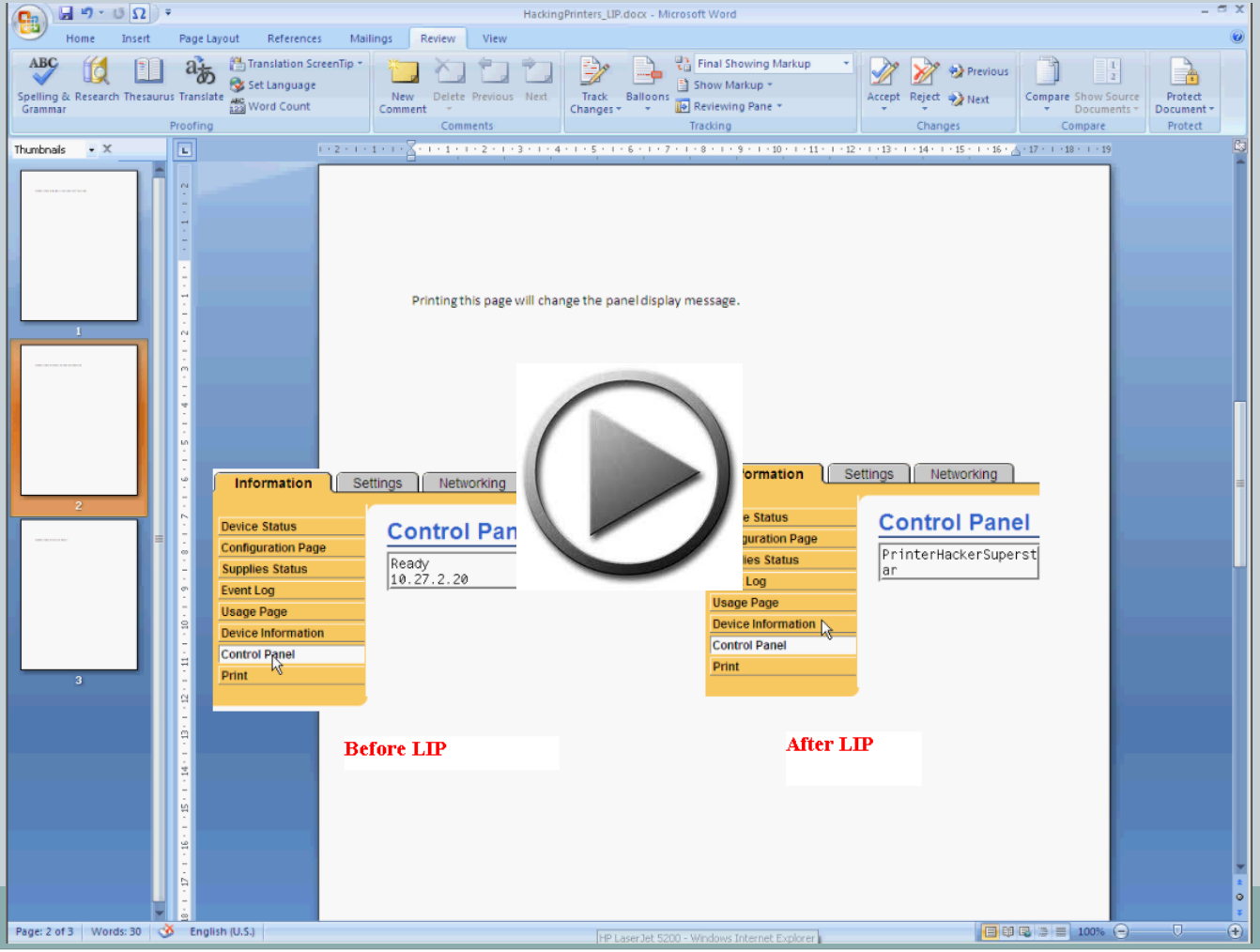
Demo – Locally-initiated printing exploit

- "File upload" PPE over MS Word



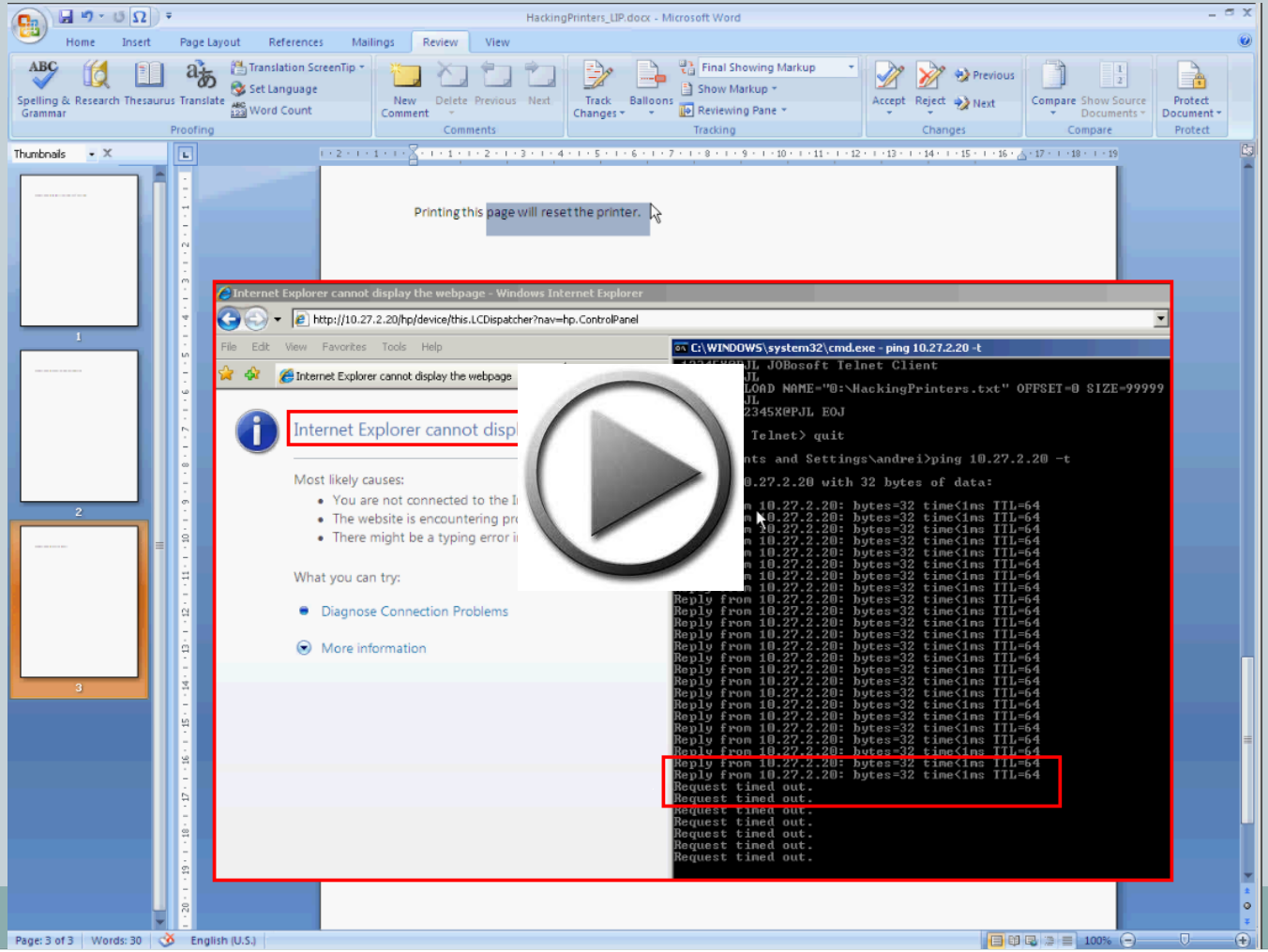
Demo – Locally-initiated printing exploit

- "Printer-display change" PPE over MS Word



Demo – Locally-initiated printing exploit

- "Printer reset" PPE over MS Word

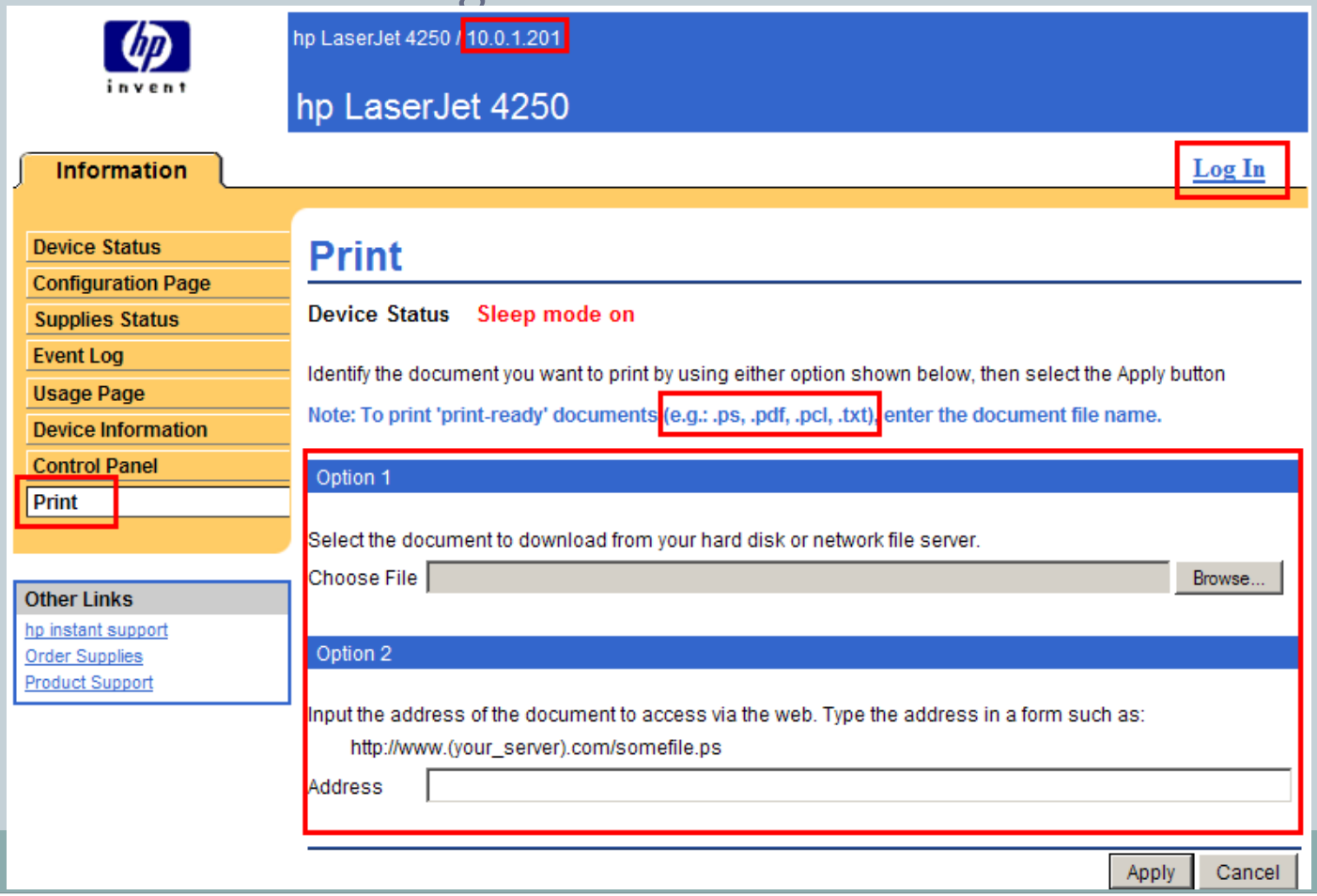


Solutions for remote+local initiated exploits

- How to fix?
  - **Not easy**, since it's PJL design + device vendors' faults
  - 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/filtering printer
    - That will filter out unsafe/suspect payloads (and alert!), producing "safe" docs to print on real devices
      - Unless the virtual printer has bugs/is exploitable itself ☺

Exploiting “test print” access in printers’ EWS

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



Exploiting “test print” access in printers’ EWS

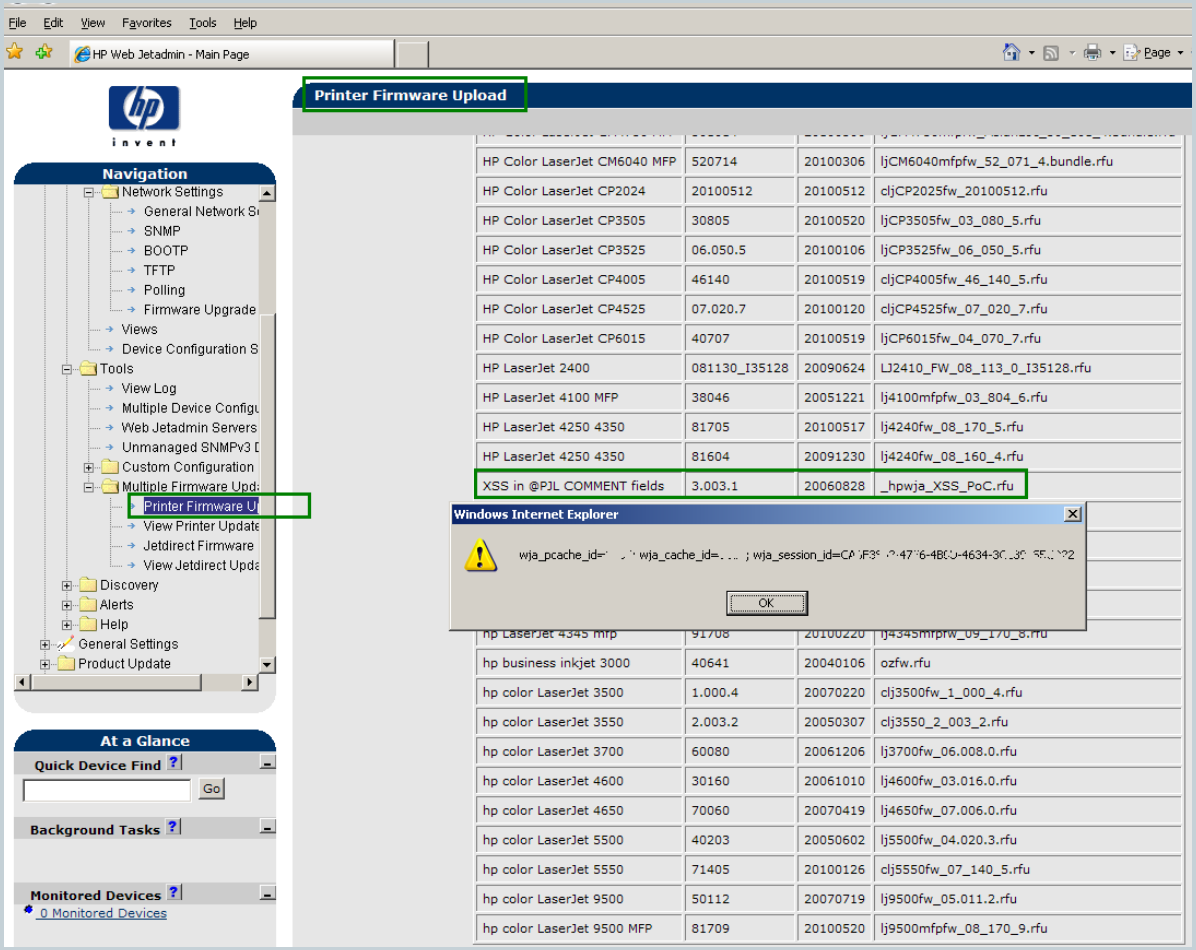
- Accepts file as direct upload :
  - Filters based **only** on extension: txt, pdf, pcl, ps
  - Will **not** accept:
    - *print_my_hexor.**rfu*** or
    - *print_my_hexor.**fmw***
  - Will accept:
    - *print_my_hexor.**pcl!***
    - Yes, in PCL we can embed PJL UPGRADE/equivalent commands
  - Also, **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*

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
  - 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)
- Use XSS as an infection-trigger step in combined MITM+XSS attack

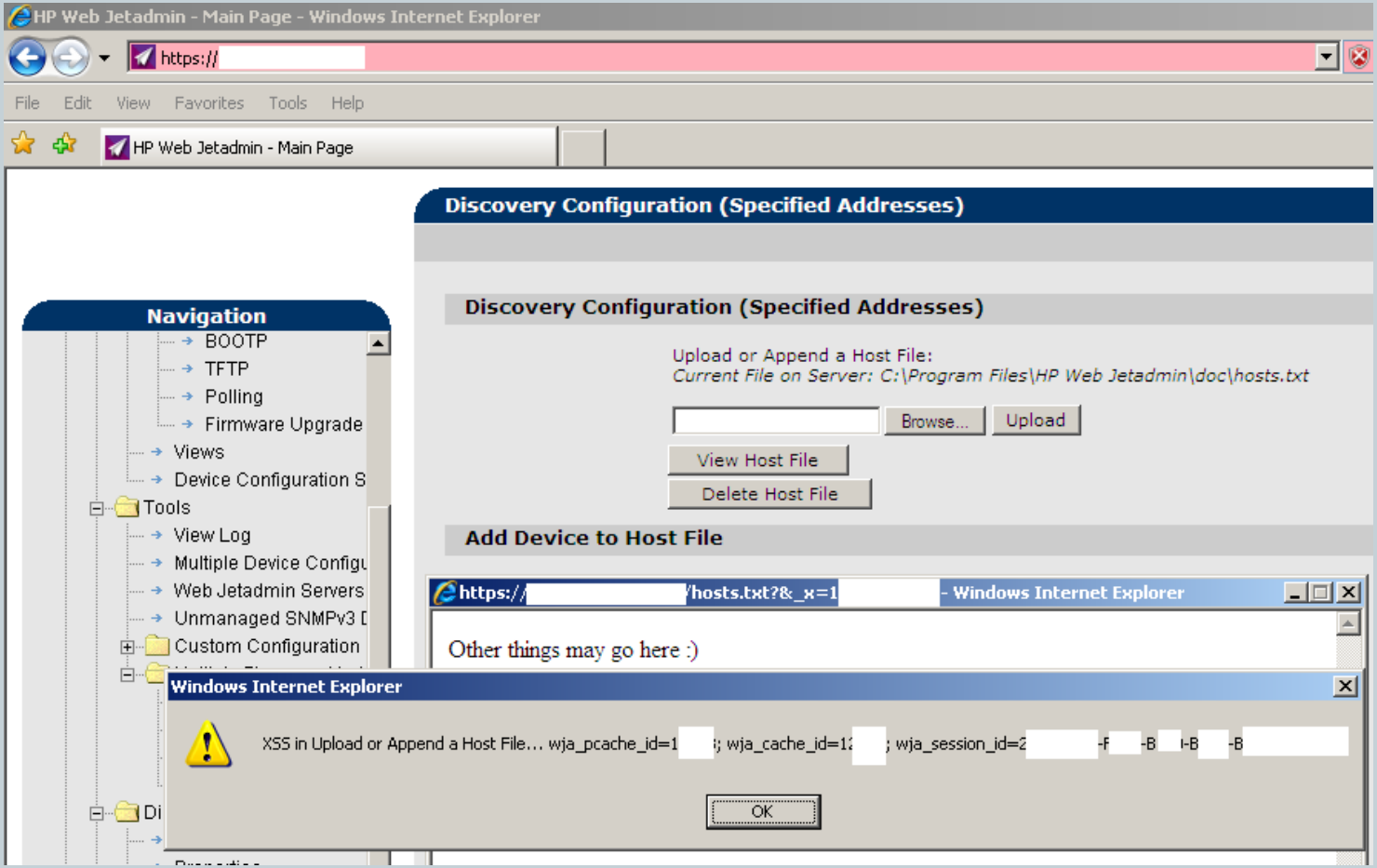
Exploit printer management software

- HP WJA XSS – inside COMMENT field of .rfu file



Exploit printer management software

- HP WJA XSS – in hosts.txt file handling

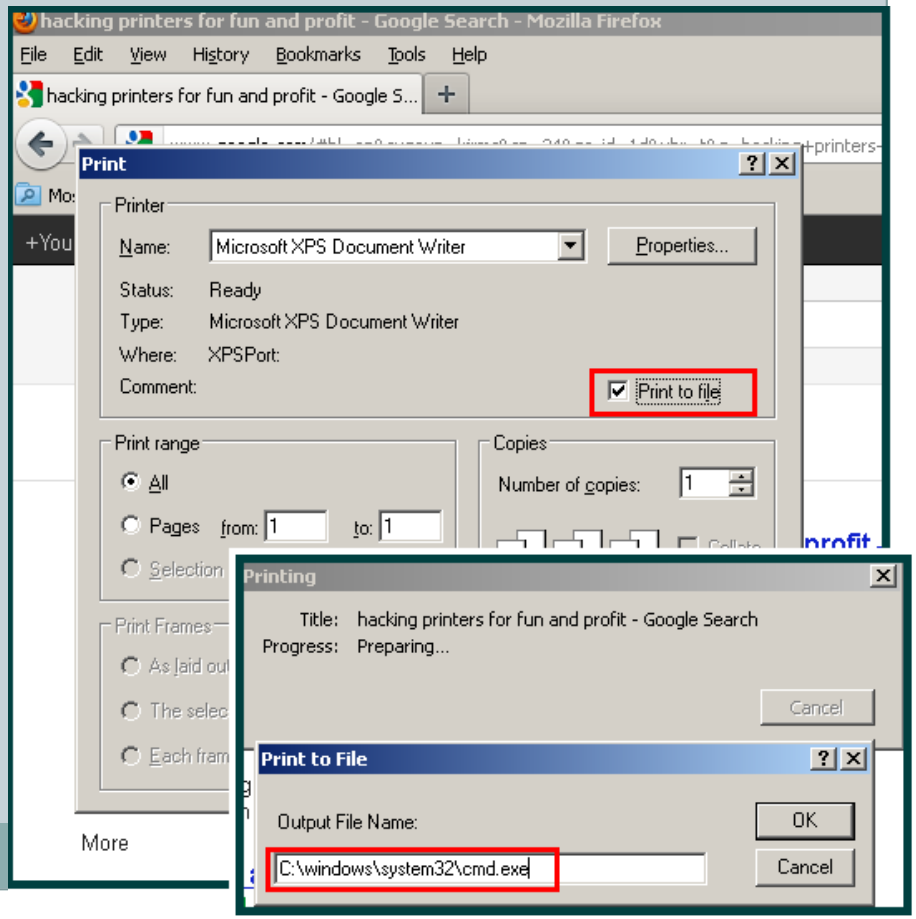


Locally-executed – Apps with rogue firmware

- If all other fail
  - 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:
  - It will be just a printer malware
  - 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

Local host-exploit – DoS and HighPrivTest

- Test if a "jailed" host (eg.: kiosk) is running Admin
  - Select/check "Print to file"
  - Make output file-name as:
    - "c:\windows\system32\cmd.exe"
    - Similar on *nix hosts
  - Consequence1:
    - Keep hacking, might be worthy
  - Consequence2:
    - DoS the host
  - Setback:
    - Cannot yet print executables
    - Needs rogue/malicious driver
      - If driver is there, why bother

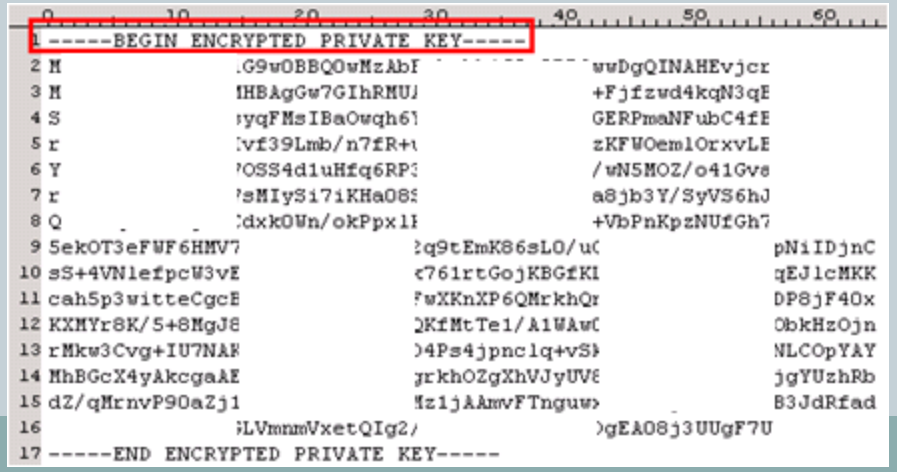


Printing subsystems are broken

- Windows
  - Stuxnet
- *UNIX
  - Possible command injection through print-job name in java
  - Data theft from /tmp/javaprint{%d}.ps

Leaking cryptographic material

- Abuse the leaking cryptographic material
  - root:$1$$I209Z7NcvQAKp7wyCTlia0:10933:0:99999:7:::
  - lp:$1$$RfHkehRv/LWAGZdCEvUU90:10933:0:99999:7:::
  - bcadmin:$1$$YSpLiaVeoDkQidsOLxlm5/:10933:0:99999:7:::
  - engineer:$1$$YSpLiaVeoDkQidsOLxlm5/:10933:0:99999:7:::
  - admin:$1$$I209Z7NcvQAKp7wyCTlia0:10933:0:99999:7:::
  - crypt("password")=$1$$I209Z7NcvQAKp7wyCTlia0



MFPs Fax Exploitation

- Information harvesting
  - fax to a local/international phone number under the control of the attack
  - find which phone numbers are associated with the organization under attack
  - find whether it's a classic PSTN fax number-pool or a FoIP
  - (theory) more advanced/targeted would be to call in back and exploit fax->printer->network->PCs/servers link

MFPs Fax Exploitation

- Money harvesting
  - using PJL and available fax-enabled MFPs, call local/intl premium numbers
  - numbers associated with the attackers/complices
  - the bill is payable by the victim
  - how many organizations have checks and enforce limits/verifications on outgoing numbers?
  - how many assessments do check the fax modules in MFPs for this?

MFPs Fax Exploitation

- COMMAND SET1
  - @PJL SET PCFAXMODE=FAX
  - @PJL SET PCFAXPAS=
  - @PJL SET PCFAXNUM0=
- COMMAND SET2
  - @PJL SET DRIVERTYPE = PCFAX
  - @PJL SET COMPRESS = JBIG
  - @PJL SET FAXCOUNT = 1
  - @PJL SET FAXTEL = +1-555-123456
  - @PJL SET PAGESTATUS = START
  - @PJL SET PAPERWIDTH = 2100
  - @PJL SET PAPERLENGTH = 2970
  - @PJL SET RESOLUTION = 72
  - @PJL SET IMAGELEN = 100

- COMMAND SET1
  - @PJL SET PCFAXMODE=FAX
  - @PJL SET STRINGCODESET=UTF8
  - @PJL SET USERNAME = "test"
  - @PJL SET KMCOETYPE = 2
  - @PJL SET DRIVERJOBID="000802E6DEC304181004320281"
  - @PJL SET PLANESINUSE = 1
  - @PJL SET STRINGCODESET=UTF8
  - @PJL SET JOBNAME = "fax test"
  - @PJL SET KMDRIVER=ON
  - @PJL SET MEDIASOURCE=AUTO
  - @PJL SET QTY=1
  - @PJL SET JOBOFFSET=OFF
  - @PJL SET OUTBIN=DEFAULT
  - @PJL SET BOXHOLDTYPE = PUBLIC
  - @PJL SET RESOLUTION=200
  - @PJL SET PAPER=A4
  - @PJL SET ORIENTATION=PORTRAIT
  - @PJL SET PCFAXPAS=OFF
  - @PJL SET PCFAXDLY=OFF<CR><LF>
  - @PJL SET PCFAXNUM0="FAX,+1-555-123456,1,0,1"
  - @PJL SET CUSTOMPAPER0 = "M,2100,2970"

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
  - 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% ☺
  - On some MFPs, this can be accomplished via Java "applets"
- HP SmartInstall attacks (next slides)

HP 110x/156x/160x series hacks

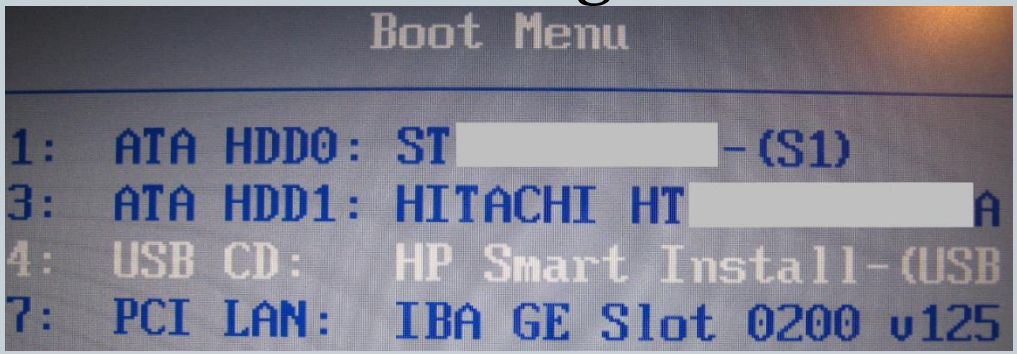
- Firmware hacks
  - It's an Xtensa LX2 based architecture
    - Features JTAG OCD, etc.
  - xtensa-linux.org to the rescue
  - Grab Xplorer-2.1.0-windows-installer.exe
  - (Hopefully no) need to reverse the processor overlays configuration
    - Otherwise, it's a big research topic in itself – anyone volunteering?
  - Overlay files + xtensa-linux.org => linux kernel for your printer
  - Binaries are ELFs
    - We love ELFs
  - Spool your kernel as a print-job
    - Using @PJL ENTER LANGUAGE=ACL
  - Lean back, relax and enjoy

HP 110x/156x/160x series hacks

- HP SmartInstall hacks
  - 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 air-gapped networks/PCs
      - 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"
  - Demo
    - Instead of *calc.exe* run *shutdown -r -f* for booting attack (next sld)

HP 110x/156x/160x series hacks

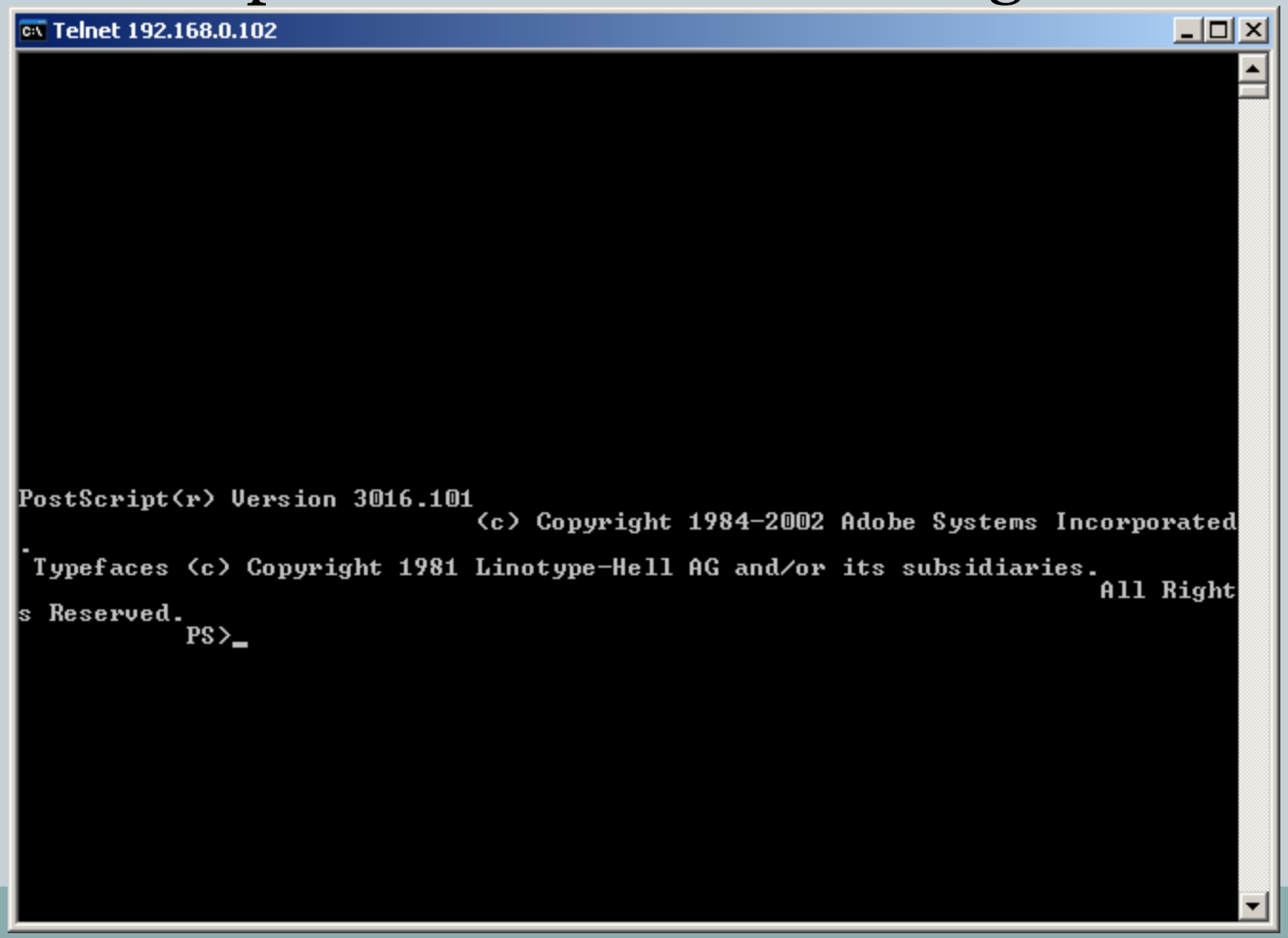
- HP SmartInstall bootloading attack



  - 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 – HPSiB (Happy Printer: Smiling Bootloader)
    - Why not use the printer as safe-boot device?
    - Eg.: recover admin password, have minimalistic Linux, fun, etc.

What's next?

- Sneak video preview of what's cooking ☺



"Secure Thinking" *in quotes*

- HP Security Solutions
  - "*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

"Secure Thinking" *in quotes*

- 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!

"Secure Thinking" *in quotes*

- 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?
    - "…probably…" ?!
      - Nowadays, if you have an OS, a FS and externally connected execution environment, most likely you need internal antivirus/IDS/IPS

"Secure Thinking" *in quotes*

- Final thought on above "secure thinking" quotes
- Remember psybot? To summarize
  - Non-conventional arch – *true* – MIPS
  - Non-conventional OS – *true* - Mipsel Linux
  - Doesn't support antivirus – *true* – "why should we?!"
  - Got owned – *very true* – ~100k devices in a sophisticated command-and-control botnet

---

  - If you need more arguments for securing/cleaning embedded devices, running unconventional 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 crashes/bricks your device…
  - …time to put in practice SDL. we are in 2010, remember?…

Solutions – Printer Vendors' Side

- Authenticate uploader, crypt, sign and verify signature of the uploaded firmware
  - Btw, homebrew or kindergarten crypto is NOT crypto!
  - 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 mandatory strong-password changes 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
  - This point is more to be joke ☺
  - Though, not that there were no surprising developments
- Setup honey-pots for most-spread MFPs EWS :
  - Similar to renowned /etc/passwd
  - Study blackhats/bots actions to train IDS/IPS for MFPs
  - 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
  - The RDYMSG is only annoying
    - Don't SNORT it, 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;)
```

  - 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:!"|0A|"; 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 printers-related 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:
  - Device and antimalware vendors seem to ignore the issues… yet
- MFPs are more than “dummy printers” – these are full-blown machines with great power and connectivity
- MFPs tend to interact with same (or even bigger) number of technologies as computers:
  - Eth
  - WiFi
  - RFID
- MFPs have access to almost same set of secrets as PCs

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"

- ?

- !

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

- Print-in-touch:
  - lpr –Phoneypot-printer@andreicostin.com –Y –J "Hacking Printers" –T "Comments/suggestions/collaboration" –m andrei@andreicostin.com –m zveriu@gmail.com -- -
- Till next time… keep your MFPs safe as golden:

Bonus

- Below are some detailed slides for readers interested in specific sub-topics

Geolocation over MFPs

- PLT examples:
  - "SLD Bldg 084 Flr 1 Room 111", "C2N05 – Block C, 2nd Floor, North Wing, Cubicle 05"
    - 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
  - (+) 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?)
  - (+) Can be used where no public IPs of MFPs are exposed
  - (-) Reverse geolocation sometimes is bogus (hey google, wtf?)
  - (-) Needs built-in heuristics in malware/C&C to correctly interpret PLT

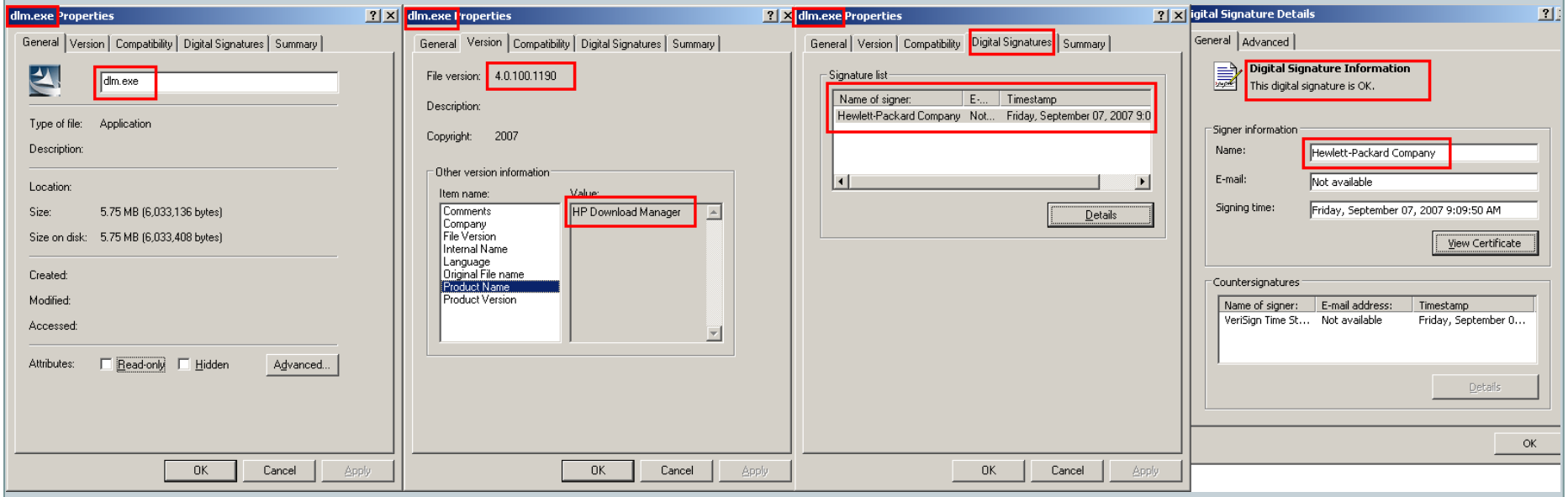
Geolocation over MFPs

- Targeted attacks scenarios:
  - 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

Privacy/transparency concerns

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



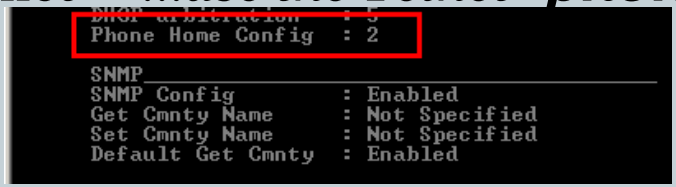
Privacy/transparency concerns

- Important note:
  - It's not managing a PC-backdoor
  - It is managing an MFP/JetDirect-backdoor
  - *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 AMD K8 Microcode backdoor update feature

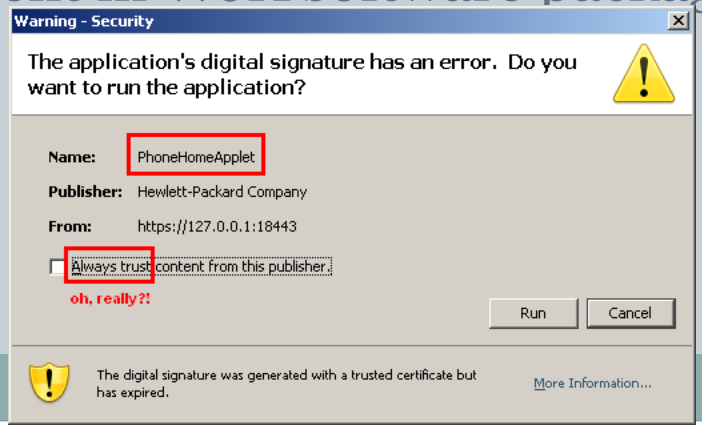
Address	Length	Type	String
".rdata:0045...	0000002A	C	FirmwareFileManager::CreateDiscDictionary
".rdata:0045...	00000030	C	FirmwareFileManager::GetFirmwareImageFileHeader
".rdata:0045...	00000033	C	FirmwareFileManager::IsMicroCodePartitionAvailable
".rdata:0045...	00000026	C	FirmwareFileManager::ReadBackDoorfile
".rdata:0045...	0000002E	C	FirmwareFileManager::ReadFirmwareBackDoorFile
".rdata:0045...	00000031	C	FirmwareFileManager::ReadFirmwareImageHeaderFile
".rdata:0045...	00000027	C	FirmwareFileManager::getCurrentVersion

Privacy – What about PhoneHome feature?

- Phone Home feature in HPs
  - Present in EWS of devices (telnet/web/snmp interfaces)
    - SNMP MIB is 1.3.6.1.4.1.11.2.4.3.7.31.0
      - *"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)"*
    - telnet - *"...use the Telnet "**phone-home-config**: 0" ..."*



  - Present in WJA software package



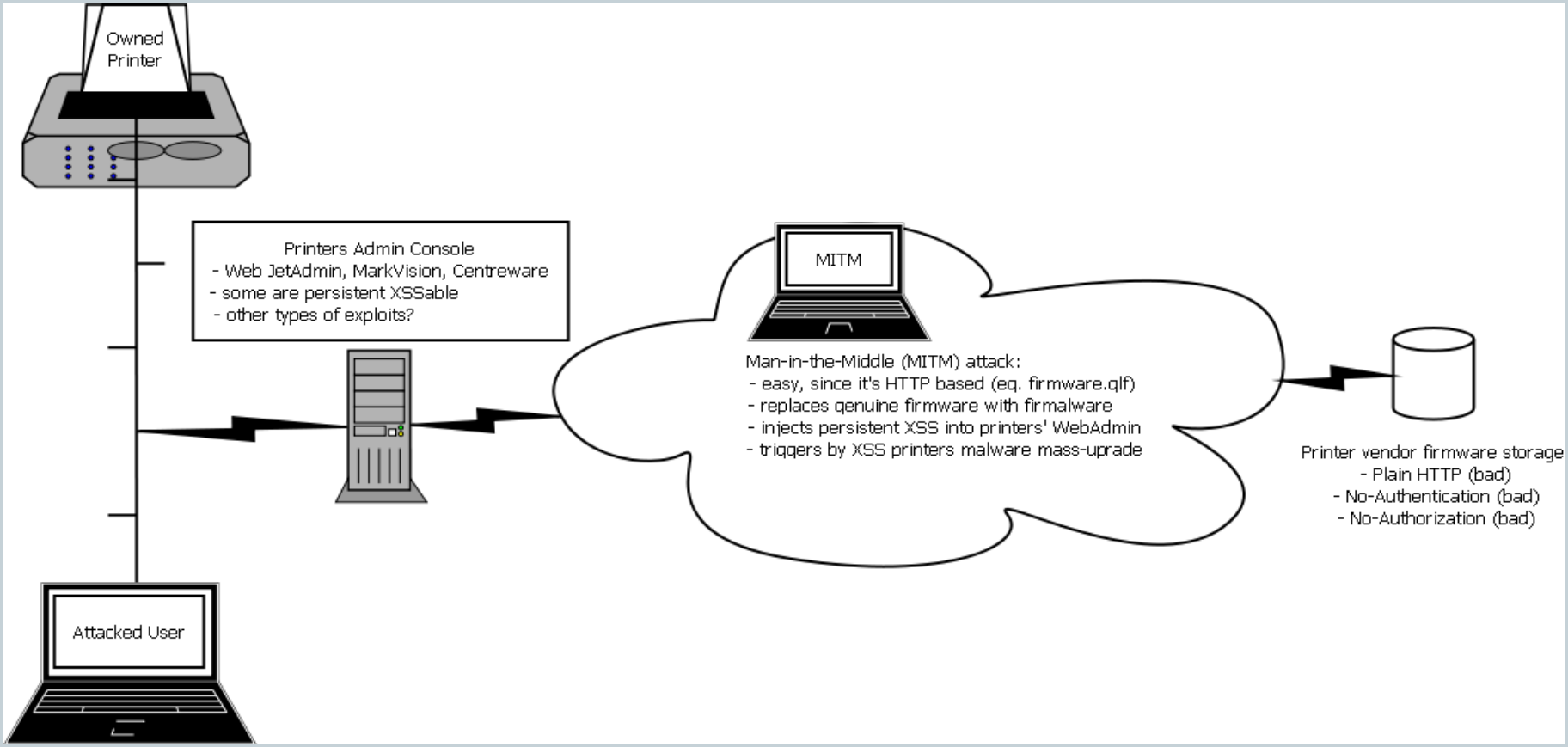
Privacy – Some thoughts

- PhoneHome (1.3.6.1.4.1.11.2.4.3.7.31.0) privacy 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 ☺
- PhoneHome + JetDirect Firmware Backdoor
  - 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!**

Locally-executed – Print subsystem hacks

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

MFPs attack vectors – Overall diagram



- Once MPF is compromised – it attacks back (next)

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 command-and-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 slowloris
    - 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 ☺
  - Find race conditions in parsers: direct print, direct URL print, port 9100 print and print-server print; include also PJL/non-PDL cmds