



PostScript: Danger Ahead?!

Andrei Costin <andrei@andreicostin.com>

Affiliation - PhD student



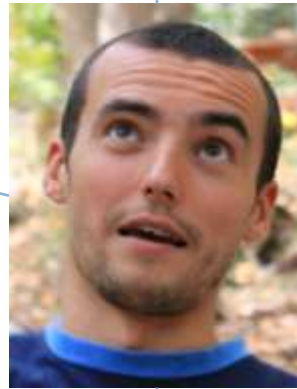
whoami: in-between SW/HW hacker

Hacking MFPs (for fun & profit)

Mifare Classic MFCUK



Holistic
Security
Interest



<http://andreicostin.com/papers/>

Agenda

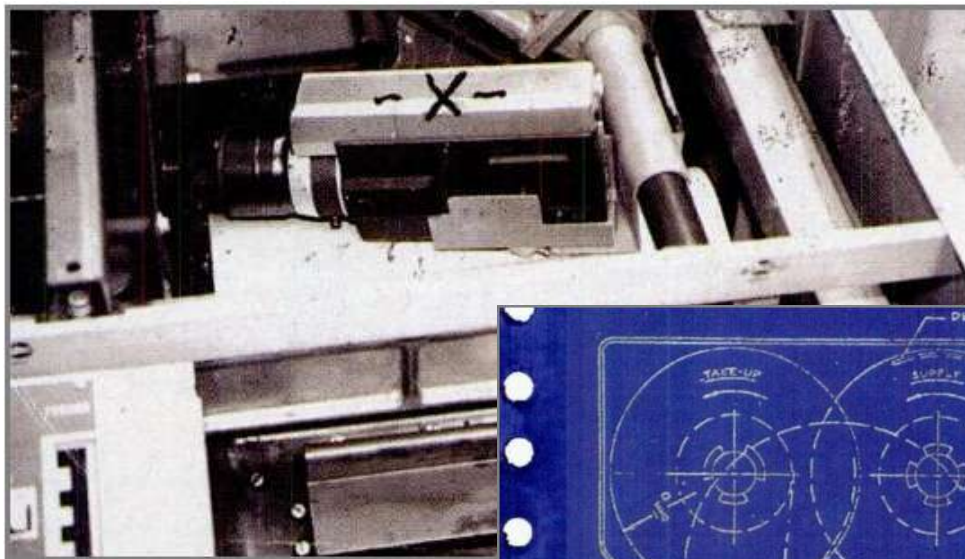
Quick refresher

2. What about PostScript?
 3. So, what and how did you find?
 4. Attacks in a nutshell
 5. Solutions and conclusions
-

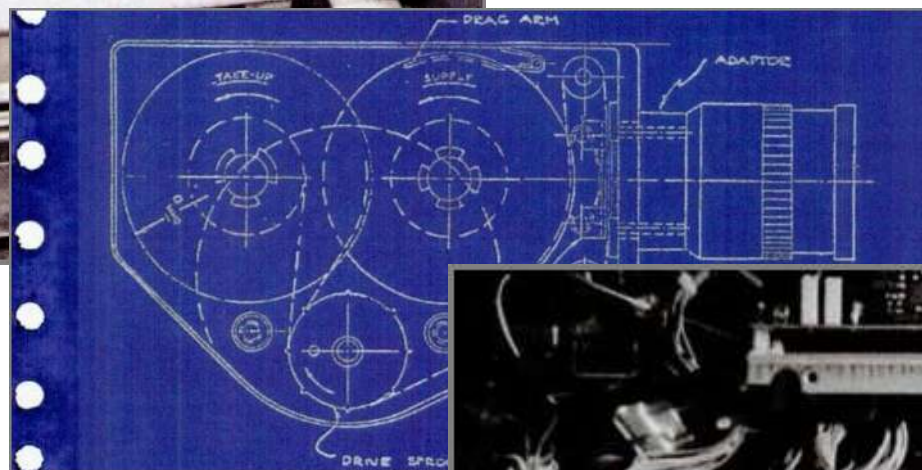
MFPs carry large abuse potential



MFP hacking goes back to the 1960's



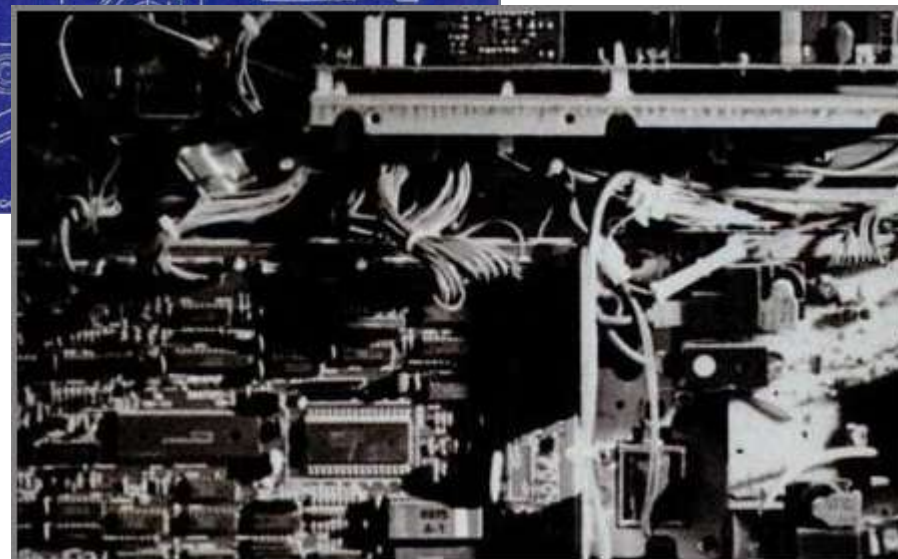
The “micro”-film camera, marked X



Patent drawing, 1967

Electronics/hardware hacking

“Spies in the Xerox machine”



Modern printer hacking goes back almost a decade

2002

Initial printer hacks
(FX/pH)

2006

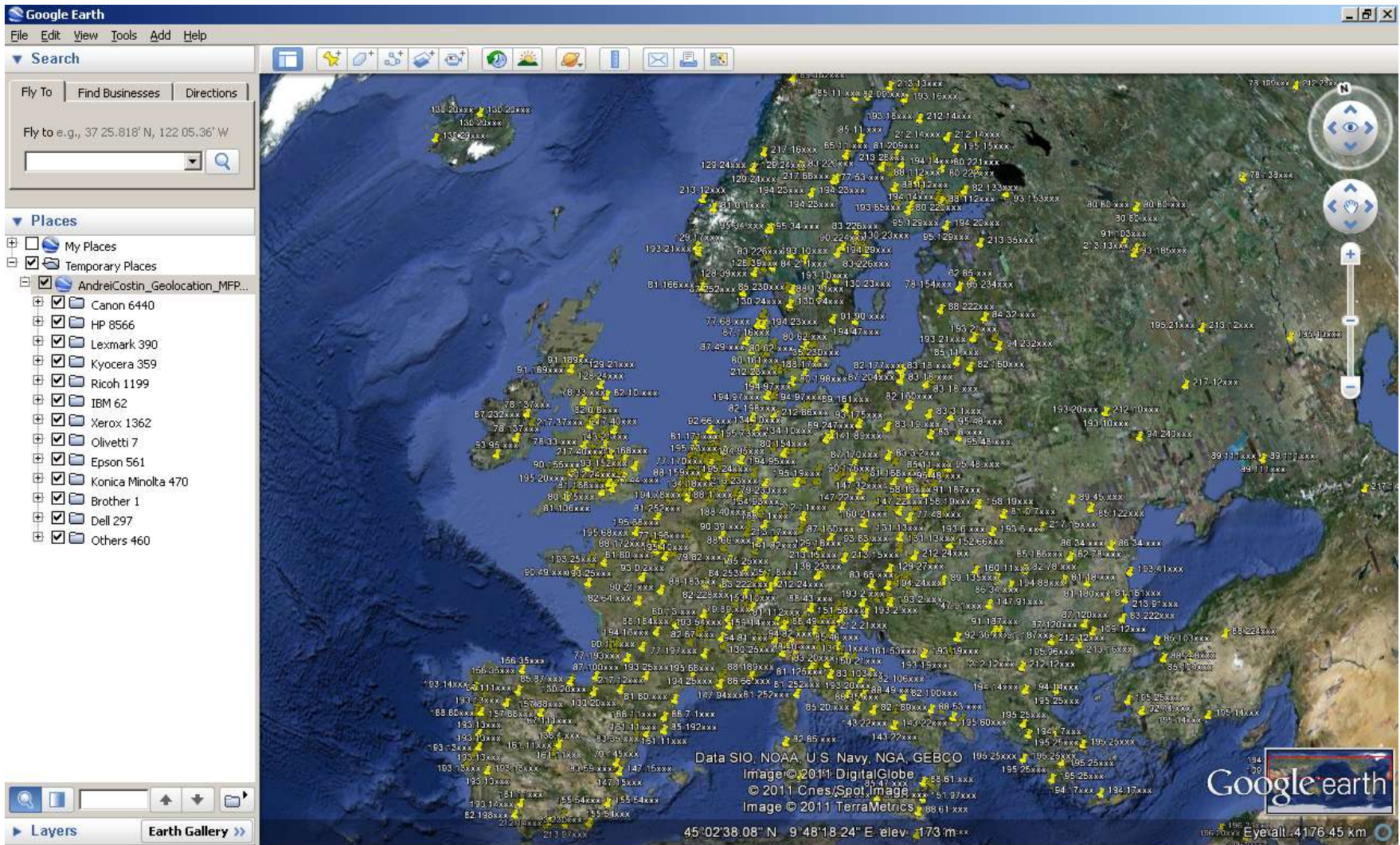
Broader & deeper
printer hacking
(irongeek)

2010-2012

Revived printer hacking
interest

This talk focuses mainly on
remote code execution
inside MFPs/printers

In 2010 we demo'd : mapping public MFPs



<http://www.youtube.com/watch?v=t44GibiCoCM>

... and generic MFP payload delivery using Word

The screenshot shows a Microsoft Word document titled "HackingPrinters_LIP.docx". A comment box in the document reads: "Printing this page will upload a file to the printer's filesystem." Below the document, three terminal windows illustrate the LIP (Language Independent Protocol) process:

- Before LIP:** A terminal window titled "Select Telnet 10.27.2.20" shows a list of printer capabilities. The line "HackingPrinters.txt TYPE=FILE SIZE=36" is highlighted with a red box.
- After LIP:** A terminal window titled "Telnet 10.27.2.20" shows the LIP command being sent: "GPJL FSPHLOAD FORMAT=BINARY NAME='0:\HackingPrinters.txt' OFFSET=0 SIZE=36 /our printer is hackers' superstar!". This line is also highlighted with a red box.

Red arrows point from the "Before LIP" terminal to the "After LIP" terminal, and from the "Before LIP" terminal to the terminal window above it, which shows the command being prepared.

<http://www.youtube.com/watch?v=KrWFOo2RAnk> (there are false claims on this discovery)

... and generic MFP payload delivery using Java

The screenshot displays a Windows desktop environment with three open windows:

- HP LaserJet 5200 - Windows Internet Explorer:** Shows the printer's web interface. The address bar contains `http://10.27.2.20/hp/device/this.LCDispac`. The page title is "HP LaserJet 5200 / 10.27.2.20 HP LaserJet 5200". The "Device Status" section shows "Ready" with "Pause/Resume" and "Continue" buttons. The "Supplies" section shows "Toner: (% remaining) Black Cartridge 77% Q7615A".
- Hacking Printer - Windows Internet Explorer:** Shows a page titled "Hacking Printer" with a URL of `http://localhost/HackingPrintersRemoteExploit`. The page features three "South Africa 2010 FIFA World Cup" logos and a "Print your ticket here" button.
- Printers and Faxes:** Shows a list of installed printers:

Name	D.	Status	Model
HackingPrinters	0	Ready	HP LaserJet 5000 Series PS
HP Universal Printing ...	0	Ready	HP Universal Printing PS
Microsoft XPS Docum...	0	Ready	Microsoft XPS Document Writer
xtp:/...	0	Ready	HP LaserJet 5000 Series PCL
- Command Prompt:** Shows a ping command being executed:

```
C:\WINDOWS\system32\cmd.exe - ping -t 10.27.2.20
C:\Documents and Settings\andreiodping -t 10.27.2.20
Pinging 10.27.2.20 with 32 bytes of data:
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Reply from 10.27.2.20: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
```

The last two lines, "Request timed out.", are highlighted with a red box.

<http://www.youtube.com/watch?v=JcfxvZml6-Y>

Agenda

1. Quick refresher

▶ What about PostScript?

3. So, what and how did you find?

4. Attacks in a nutshell

5. Solutions and conclusions

PostScript who? It's Adobe's PDF big brother

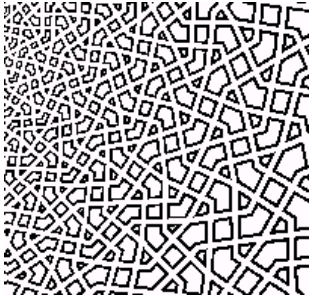
Adobe PostScript and the **future**



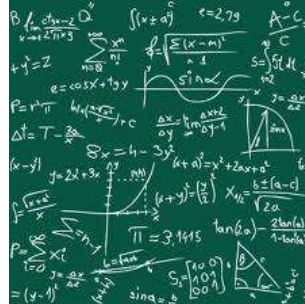
PostScript is a living language. Since introducing PostScript in 1985 as an open standard, Adobe has continually made improvements to the software. This has yielded powerful new capabilities such as Adobe PostScript Fax printers and the coming generation of multifunction products, which will include fax, copying, and

PS is build to handle complex processing tasks

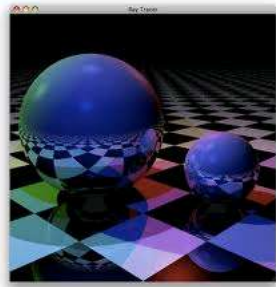
Graphics & patterns



Complex math



Web servers



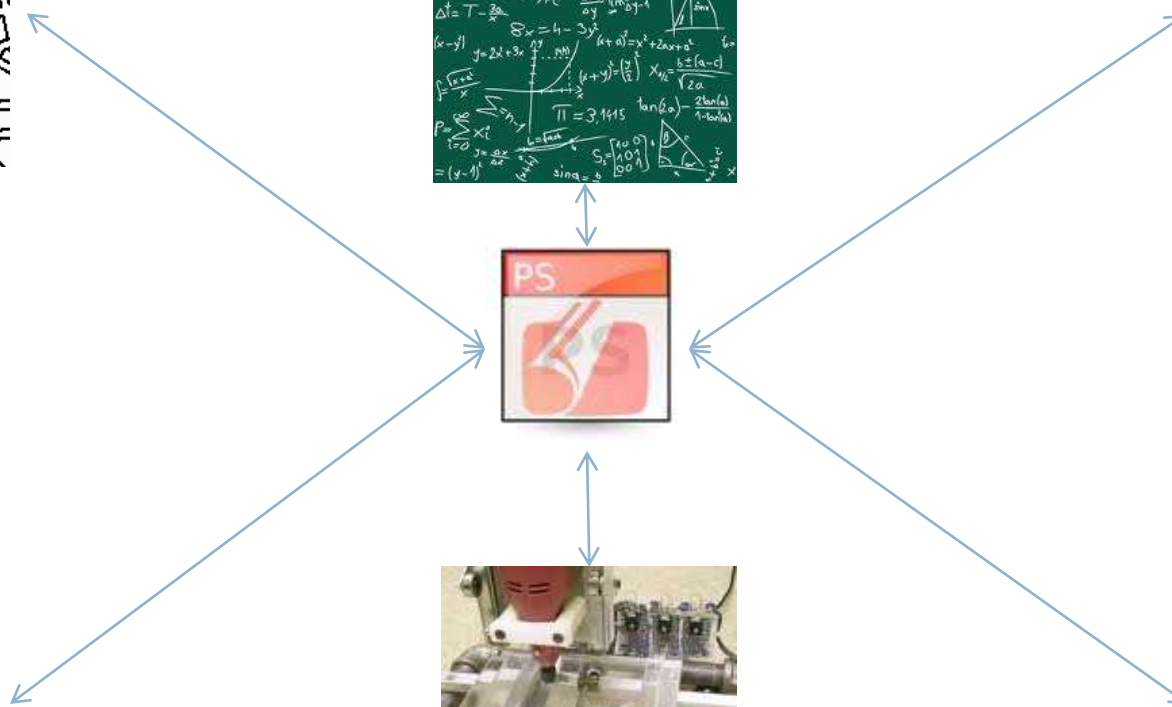
Ray-tracing, OpenGL



Milling machine



XML Parsers



Then, what exactly is PostScript?

- PostScript IS NOT just a static data stream like



- PostScript IS a
 - Dynamically typed & concatenative
 - Stack-based
 - Turing-complete
 - **Programming language**
 - What does it all mean? Exactly!

What happens when printing PS?

- User writes the doc and hits Print
 - PS printer driver transforms it to PS stream for specific device
 - PS data stream on PRN

- User Opens a PS file from email/hdd
 - PC-based PS interpreter processes it
 - PS data stream executes on PC

- In both cases, PS data stream IS A PS program
 - **Program != static data**

Demo

“Programming language” aspect

- Programming languages 101:
 - Control statements
 - if/else
 - loop
 - while

- Simplest DoS attack is an “infinite loop”
 - `!%`
 - `{ } loop`

Demo

“Dynamically typed concatenative” aspect

- You wonder why your smart IDS/IPS rules stopped working?
- Here is why:
 - `ps_dynamic_statement_construction_and_execution.ps`
- Solution:
 - Bad news: Need dynamic execution sandbox
 - Good news: It’s coming in upcoming weeks

Demo

Real world application – MSOffice PS crash

- Submitted to MS
- Apparently this one is not exploitable as in smash stack attacks
- But it opens an interesting perspective on MS Office...

Demo

Real world application – GhostScript autoprn

- One got to love custom extensions
- Send a print-job stream directly by mere opening the file
- Requires more investigation, but perspective is interesting...

Dynamic document forging/generation + SocEng

```
0 10 20 30 40 50 60 70
1 product
2 (GPL Ghostscript) eq
3 {
4 userdict begin
5 DisplayImage
6 0 0
7 574 960
8 12
9 574 960
10 0
11 0
12 62 689A5F659761649764679A63 65985E6093 6060946565996161956262966062955E60935C5F92
13 ...
14 }
15 {
16 % The malicious stuff goes here
17 }
18 ifelse
```

Computer side

The printer driver encountered an unexpected error – it has been logged.

Please print this document directly using printer convenient user interface.



Printer/MFP side



Dynamic document forging/generation + SocEng

User computer

User printout

Page 128 of 1024

Page 128 of 1024

...(some legal clauses trololo)...

...(some legal clauses trololo)...

The customer X agrees, by signing the printout, The customer X agrees, by signing the printout,

to pay 100 EUR to the vendor Y

to pay 1000 EUR to the vendor Y

...(some more legal clauses trololo)...

...(some more legal clauses trololo)...

Where is PostScript? (Vendor-wise view)



Applications incorporating the PS interpreter

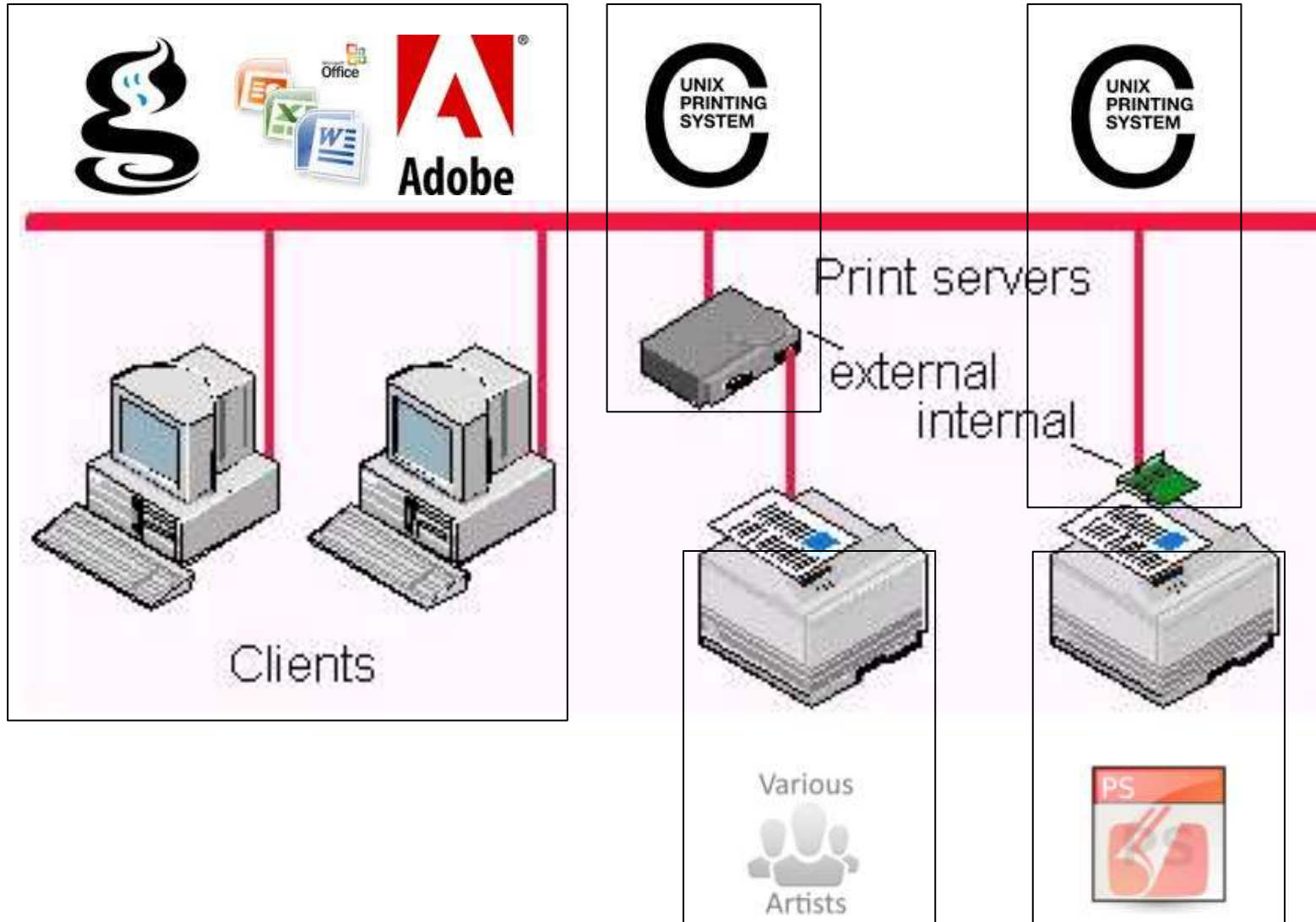


Applications/vendors producing the PS interpreter



The PS interpreter specifications and standards

Where is PostScript? (Role-wise view)



PostScript Web 2.0 Style

- PostScript made it into the web as well
- Around 20+ services found to be vulnerable to various degrees
 - Google was one them -> Bounty reward 😊
- Some fun facts
 - Effective for host exploitation and information gathering
 - Some ran GS as root user
 - Some ran GS without -dSAFER
 - All of them ran vulnerable GS versions
 - Heap and stack overflows
- More details to come...

Agenda

1. Quick refresher
 2. What about PostScript?
 3. What else was found?
 4. Attacks in a nutshell
 5. Solutions and conclusions
-

A PS-based firmware upload was required

Click the “Browse” button. In the resulting file open window, select the firmware update file that is provided as part of this update package. Firmware update file will have a file extension of “.ps”. *Shown in the upper red oval.*

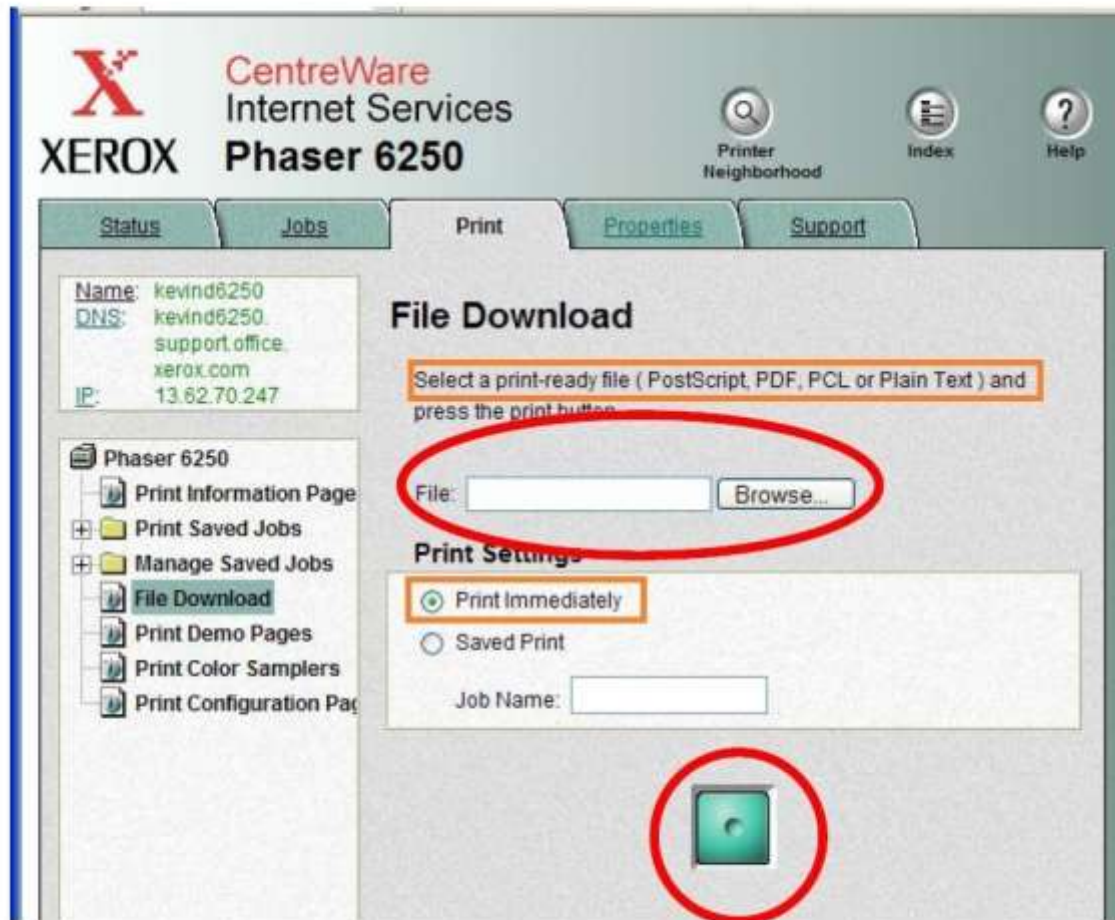
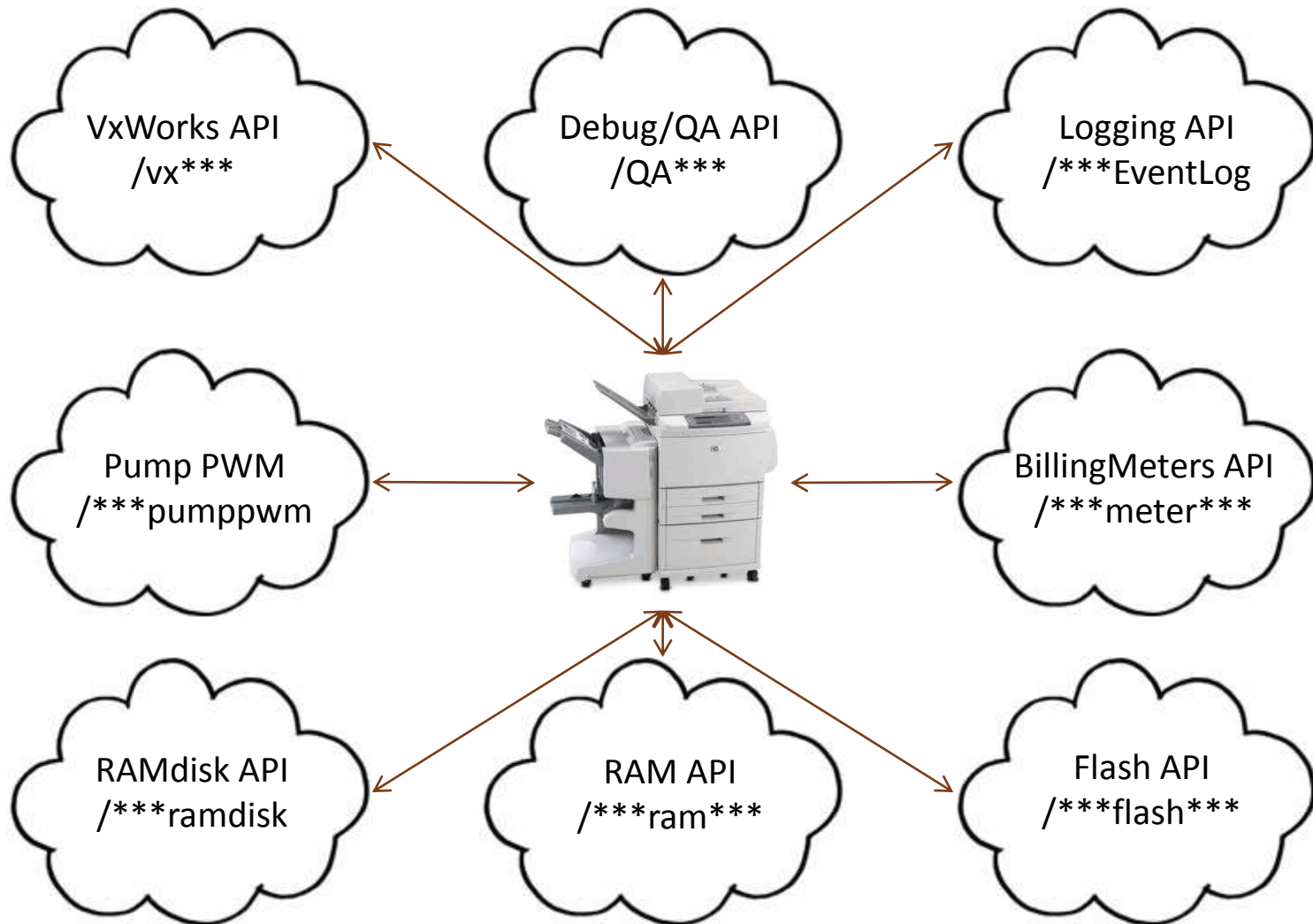


Figure 4: Select the firmware update file and press the green button to send it.

This is too good to be true....



Memory dumping reveals computing secrets

```
YOU 00 40
0000 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
0010 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
0020 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
0030 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
0040 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
0050 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
0060 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
0070 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
0080 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
0090 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00
00A0 FF
WWW.VINTAGE-COMPUTER.COM
```

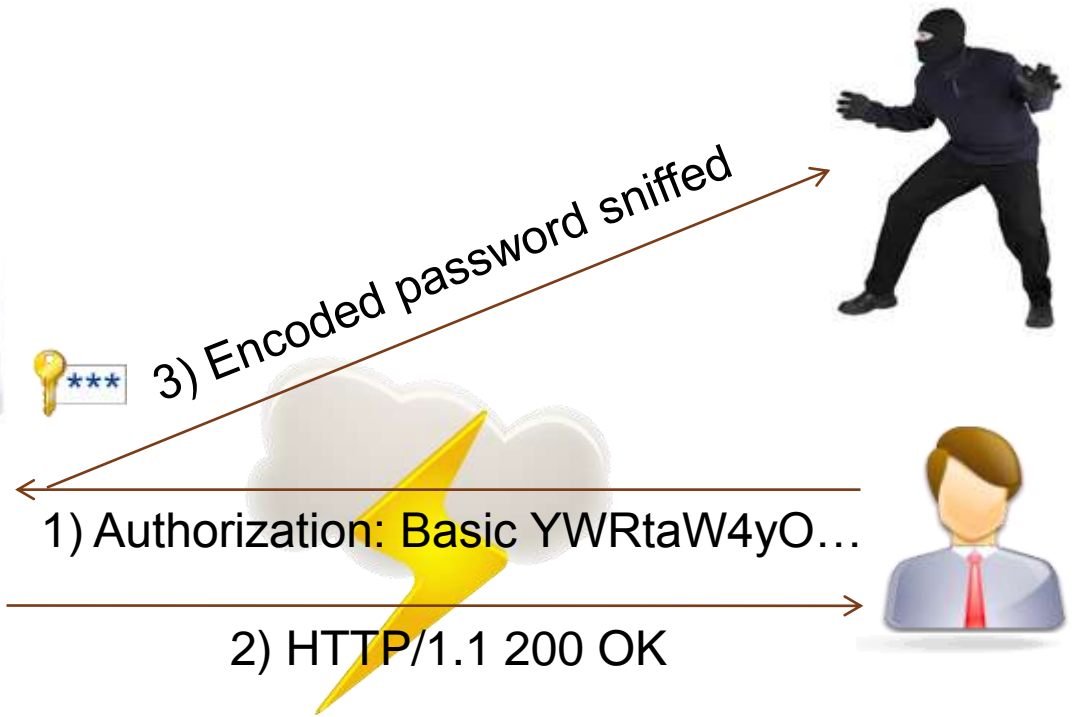
Admin restriction fail to prevent memory dumping



Password setup is sniffed by the attacker



Basic auth password can be dumped



HTTPS / IPsec secrets are “defaulty” & “leaky”

```
0 10 20 30 40 50 60 70
1 IPsec AUTHKEY
2 66306630663066306630663066302222
3
4 /ramDrv/./ssl/private/clientkey.pem
5 BJBgkqhkiG9wOBBQwPDAbBgkqhkiG9wOBBQwwDgQIt/VXBECuFwMCaggA
6 MBOGCWCGSAFlAwQBAgQQObFFTwd+A7+9U31Ngp/bgSCAoDoth9xVw1UwwLGrnPX
7 .....
8 .....
9 .....
10 /zT8zr+wt1OHxSBj6WFqVXOwNFPkcsqfuUXxVJ+HcuaUuUpTsTle1BSDC2m5MM76
11 h1Tx0/Z9/pfF09zFXqOEdOukc3wR1U76b56fhupORKtyH9woAgT8a4pb8hYPUgsJ
12
```



0x663066306630663066306630663066302222

Attacker has access to printed document details



2) Printed document details



1) Protected/secret document



Attacker has access to network topology – no-scan



2) Network topology, attackable devices

1) Device discovery (SDP, UPnP)



Attacker has access to BSD-style sockets...



Two-way BSD-style sockets communication



Analyzed MFP cannot protect effectively

Protection measures

Privilege level separation



Secure password setup



Secure (basic) auth



HTTPS, IPSEC secrets protection



Network topology protection



In-memory document protection



Restrict sockets on unprivileged modules



Fail / warn / ok

Plenty of Xerox printers share affected PS firmware update mechanism

Xerox Phaser 8560DN	Xerox ColorQube 8570DN
Xerox Phaser 8560DX	Xerox ColorQube 8570DT
Xerox Phaser 8560N	Xerox ColorQube 8870DN
Xerox Phaser 8560DT	Xerox Phaser 7760DN
Xerox Phaser 8560MFP/D	Xerox Phaser 7760DX
Xerox Phaser 8560MFP/T	Xerox Phaser 7760GX
Xerox Phaser 8560MFP/N	Xerox Phaser 7760GXM
Xerox Phaser 8560MFP/X	Xerox Phaser 4510B B/W
Xerox Phaser 8500N	Xerox Phaser 4510N B/W
Xerox Phaser 8500DN	Xerox Phaser 4510DT B/W
Xerox Phaser 8550DP	Xerox Phaser 4510DX B/W
Xerox Phaser 6360N	Xerox Phaser 5550B B/W
Xerox Phaser 6360DN	Xerox Phaser 5550N B/W
Xerox Phaser 6360DT	Xerox Phaser 5550DN B/W
Xerox Phaser 6360DX	Xerox Phaser 5550DT B/W
Xerox ColorQube 8570N	Xerox Phaser 8510

Agenda

1. Quick refresher
2. What about PostScript?
3. So, what and how did you find?

▶ Attacks in a nutshell

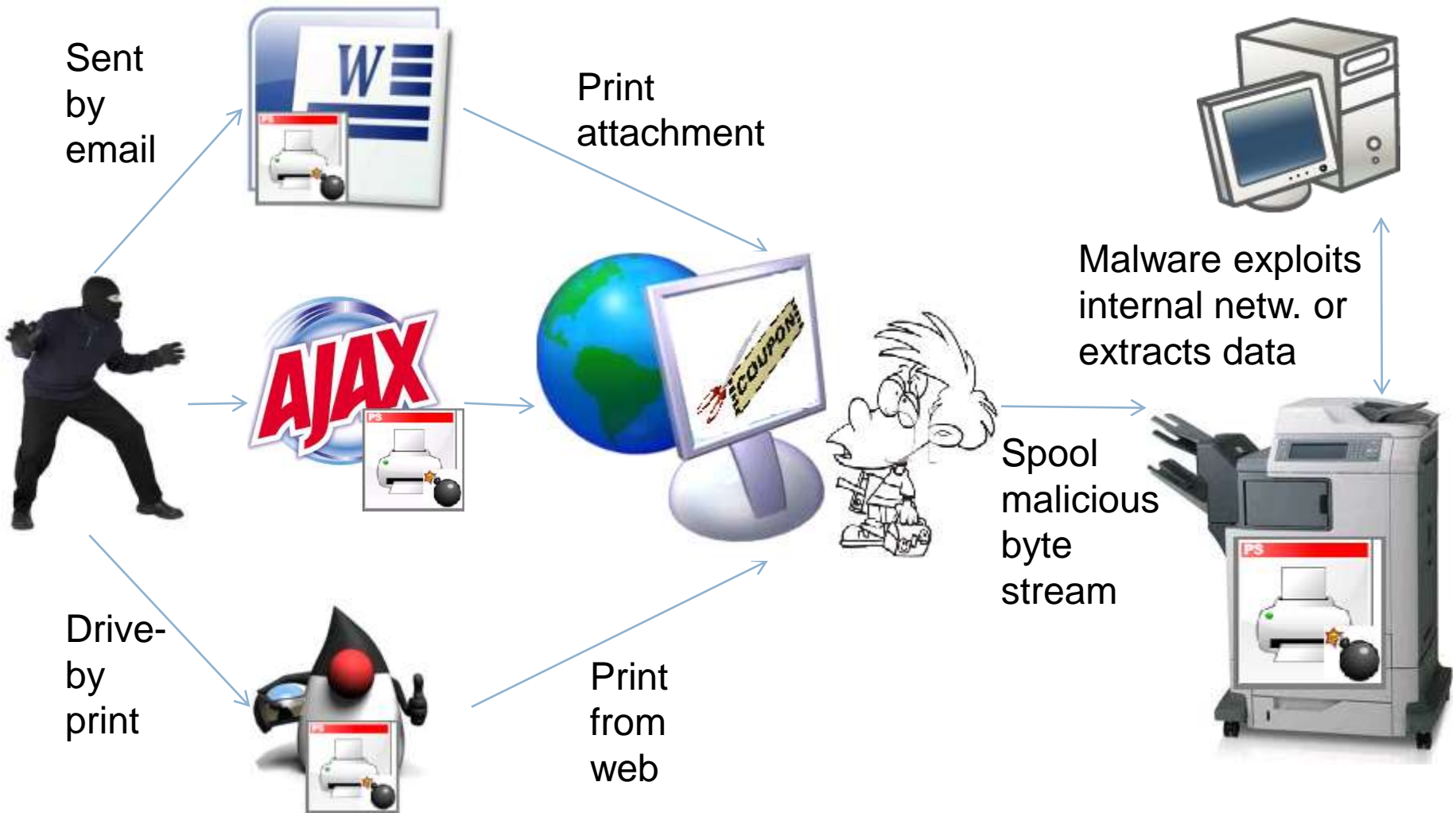
5. Solutions and conclusions
-

Remote attacks can be used to extract data

Stage 1 – SocEng

Stage 2 - Printing

Stage 3 – Exploiting/spying



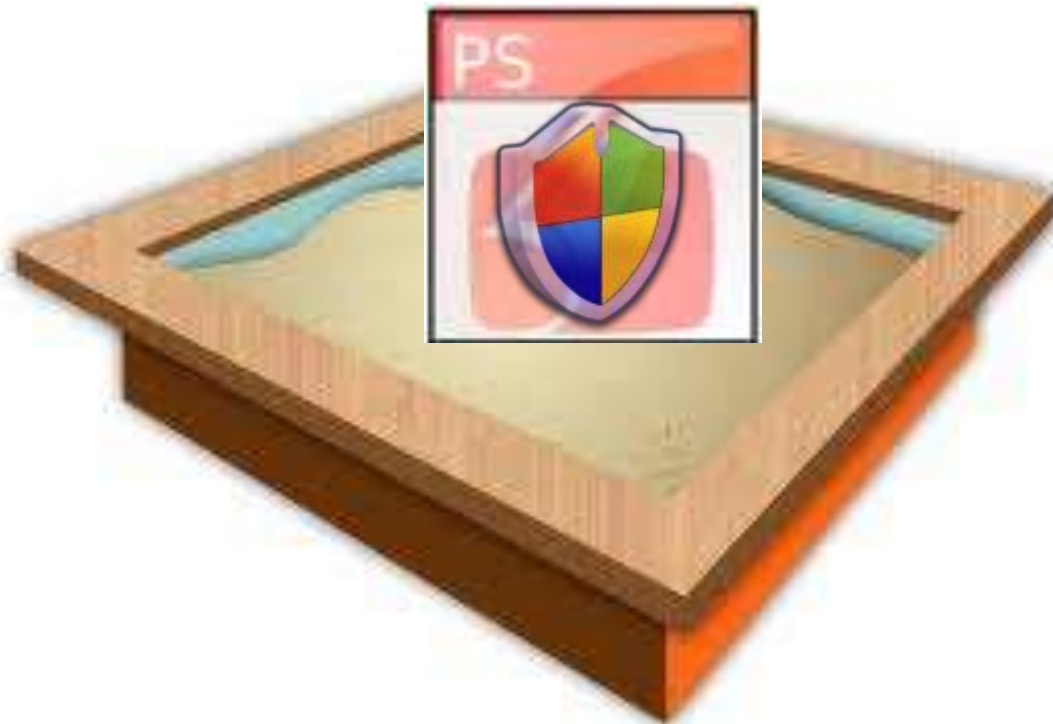
Agenda

1. Quick refresher
2. What about PostScript?
3. So, what and how did you find?
4. Attacks in a nutshell

▶ What's next, solutions, conclusions

What's next? Upcoming weeks

- **Secure PostScript Execution/Interpreter Sandbox**
- Set of online/offline tools for analysis & reporting
- Wepawet-like, but for PostScript related data
- Perhaps have it part/along of IDS/IPS/AV/PrintServer data-flows



What's next? PS + MSF + FS + Sockets = PWN!



Solutions

Actor

Suggested actions

Admins

- **Disable PS processing on printers**
- **Route print-jobs thru sandboxed print-servers**
- **Replace PS drivers with PCL ones (well...)**
- **Disable [Language Operator Authorization](#)**
- Look for security bulletins and patch
- Sandbox printers in your network
- Include MFPs in security audit lifecycle

Users

- Do not print from untrusted sources
- Be suspicious on PostScript files

Vendors

- Create realistic MFP threat models
- Do not enable/expose super-APIs

Acknowledgements

The Xerox-related PostScript work & research done under support of



Thanks/resources

[Xerox Security Team](#)

Positive responses, active mitigation

www.tinaja.com

Insanely large free postscript resources dir

www.anastigmatix.net

Very good postscript resources

www.acumentraining.com

Very good postscript resources

Personal thanks

[Igor Marinescu](#), MihaiSa

Great logistic support and friendly help

Take aways

- MFPs are badly secured computing platforms with large abuse potential
- Upcoming MFP attack could include viruses in Office and PS documents that extract organization data
- Securing the MFP infrastructure requires better segmentation, strong credentials, and continious vulnerability patching
- **Check upcoming research papers**
- **Check www.youtube.com/user/zveriu**

Questions?

Andrei Costin andrei@andreicostin.com
<http://andreicostin.com/papers>