# PostScript: Danger Ahead?!

Andrei Costin <andrei@andreicostin.com>

Affiliation - PhD student

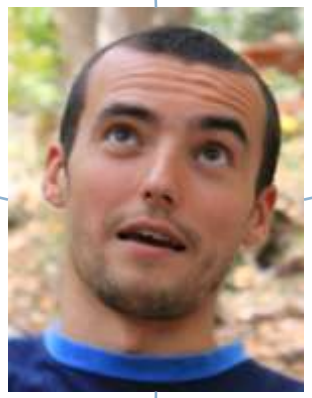
EURECOM
Sophia Antipolis

# whoami: in-between SW/HW hacker

Hacking MFPs (for fun & profit)

Mifare Classic MFCUK


Holistic Security Interest



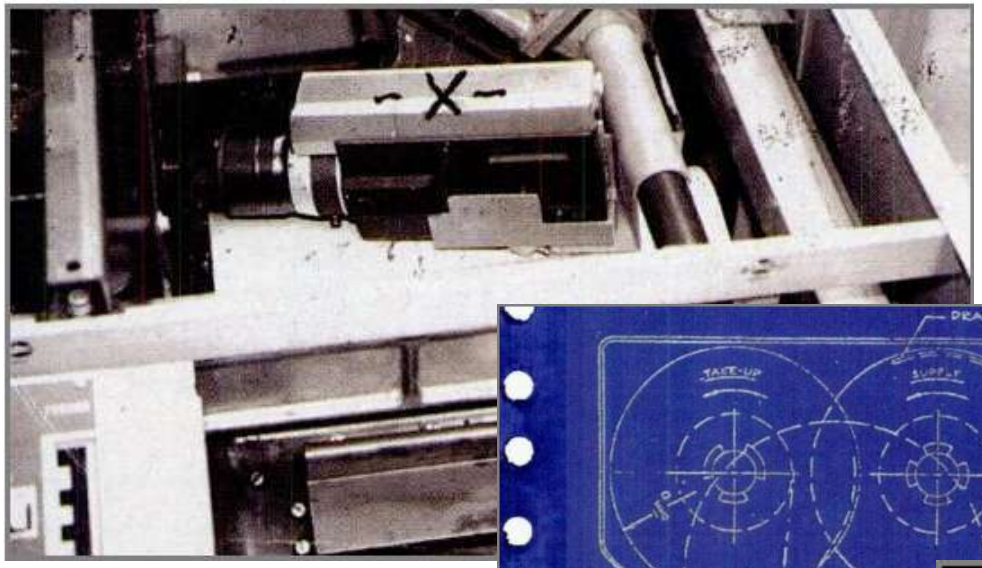
http://andreicostin.com/papers/

# Agenda

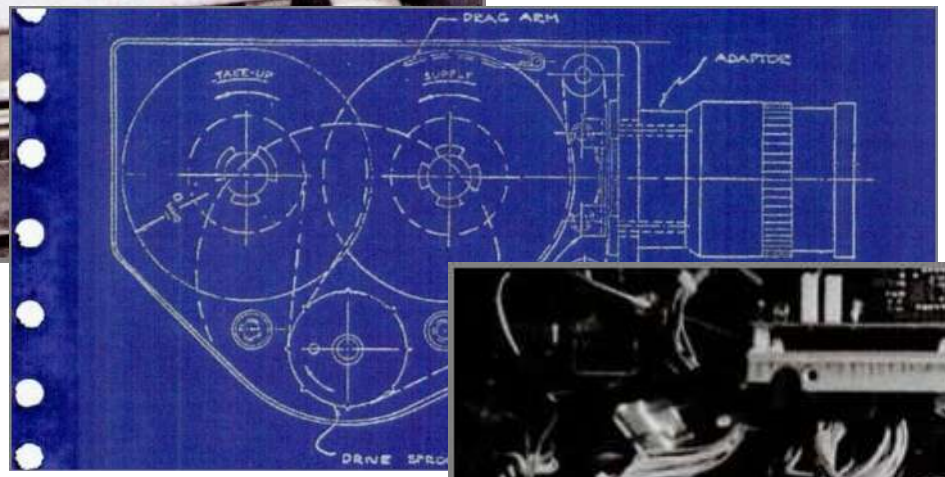
1. Quick refresher
2. What about PostScript?
3. So, what and how did you find?
4. Attacks in a nutshell
5. Solutions and conclusions

# MFPs carry large abuse potential

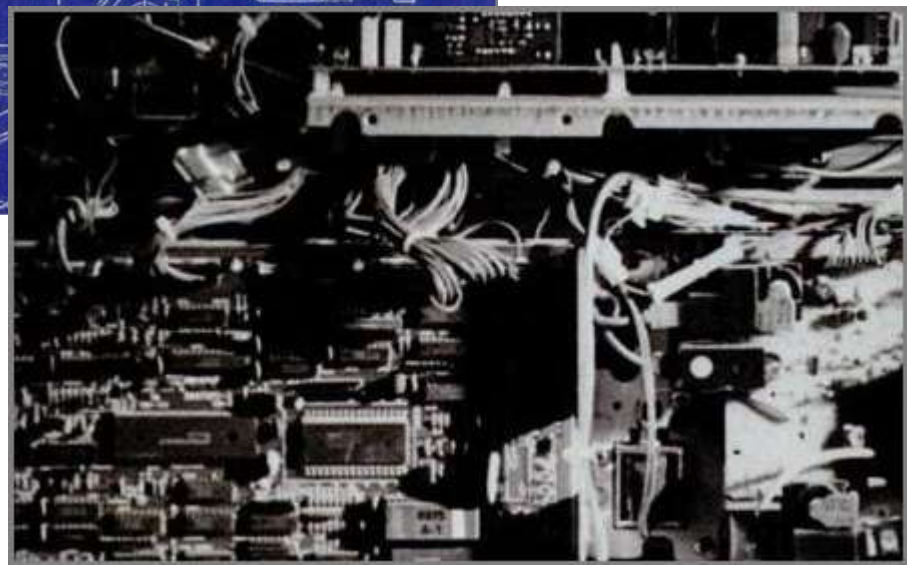
# MFP hacking goes back to the 1960's




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**

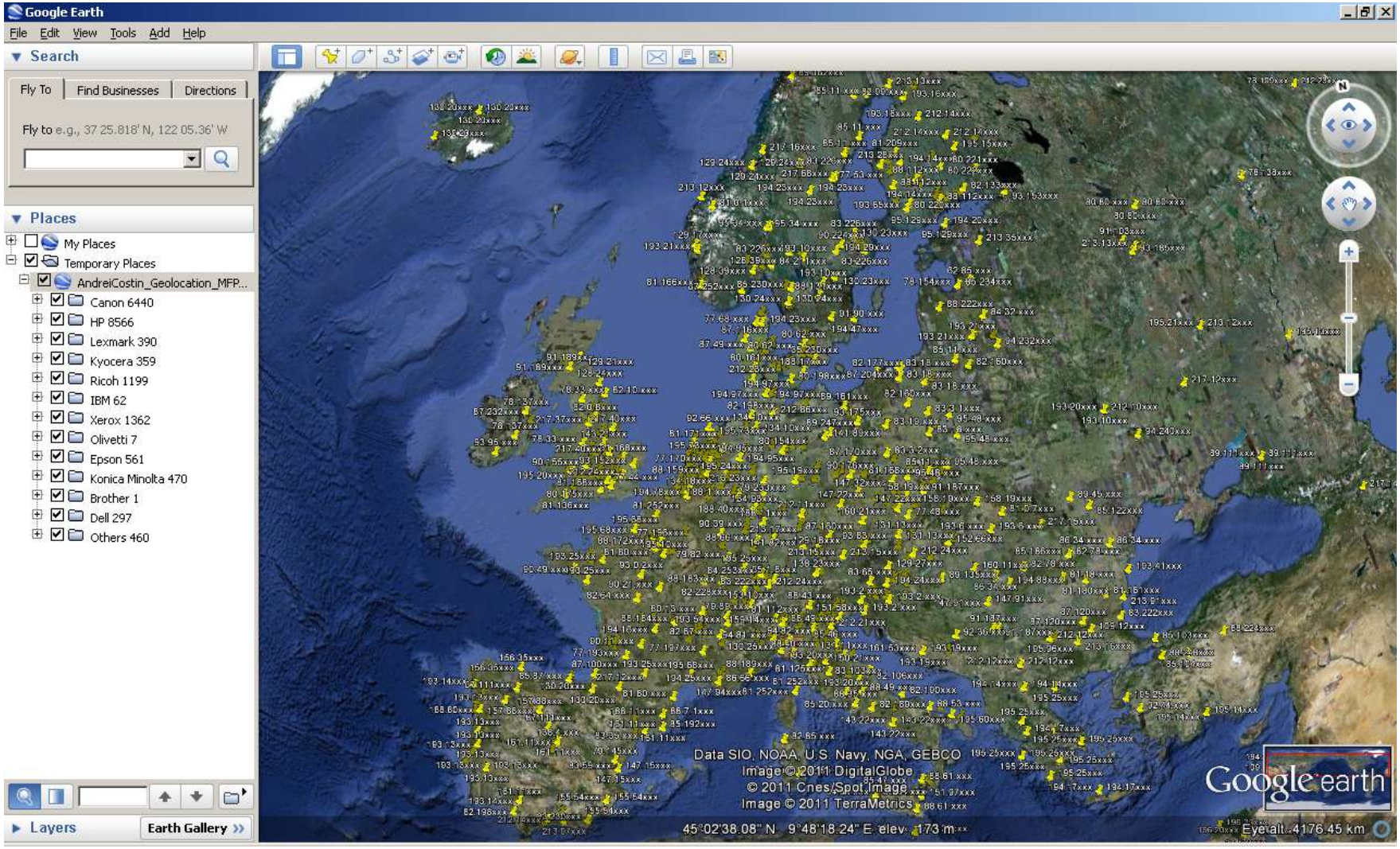
Broader & deeper printer hacking (irongeek)

**2011**

Revived printer hacking interest

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

# In 2010 we demo'd : mapping public MFPs

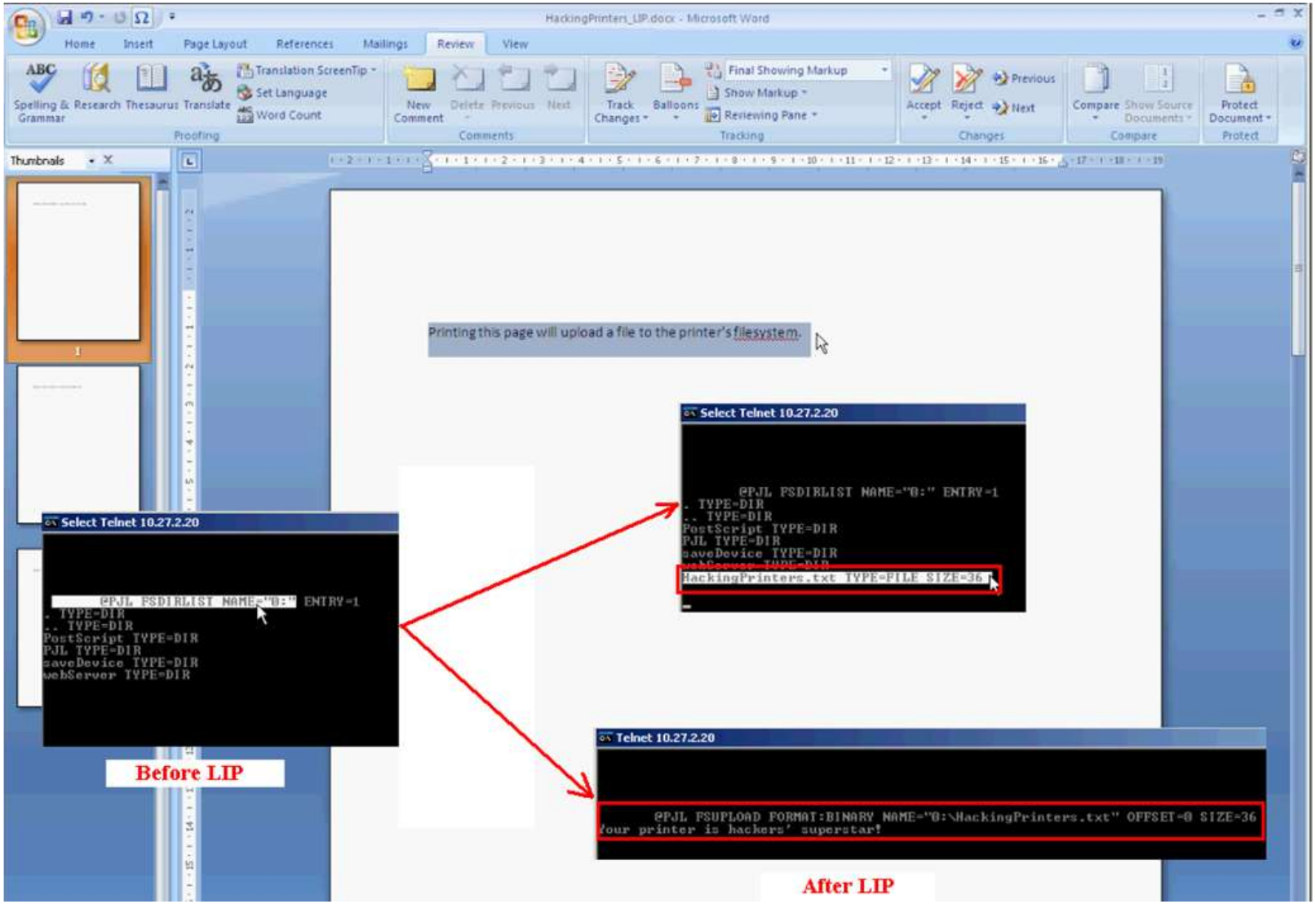



http://www.youtube.com/watch?v=t44GibiCoCM

andreicostin

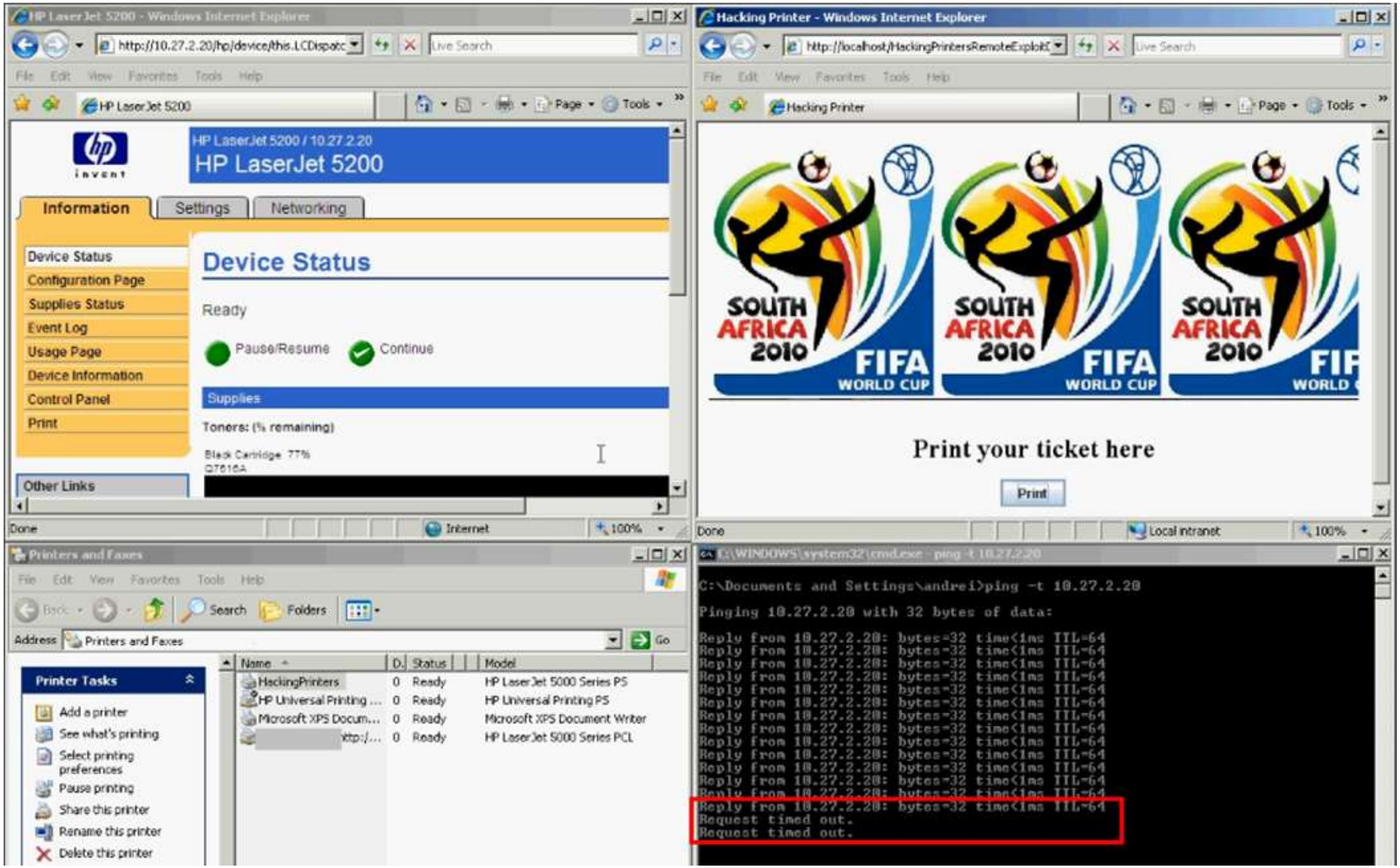
ATHCON

# … and generic MFP payload delivery using Word




http://www.youtube.com/watch?v=KrWFOo2RAnk (there are also some discovery false claims)

# … and generic MFP payload delivery using Java




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

# Agenda

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

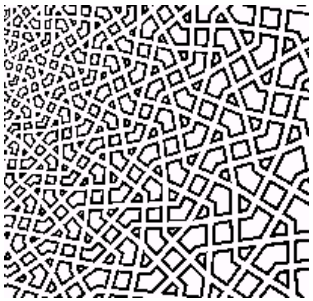
# PostScript who? It's Adobe's PDF big brother

## Adobe PostScript and the **future**

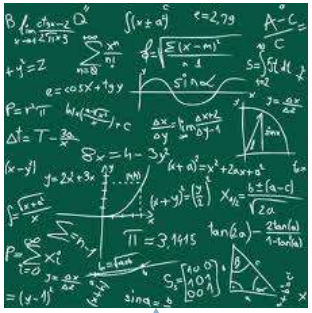
PostScript is a living language. Since introducing PostScript in 1985 as an open standard, Adobe has continually made improvements to the software. This has yielded powerful new capabilities such as Adobe PostScript Fax printers and the coming generation of multifunction products, which will include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

# PS is build to handle complex processing tasks

Graphics & patterns

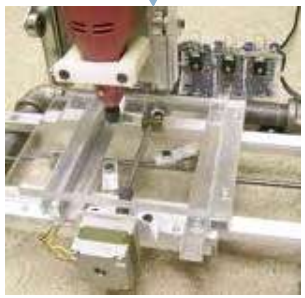


Complex math



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**

# Example
# “Programming language” aspect

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

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

# Example
# “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

# Example
# Real world application – MSOffice crash

# Example
# Real world application – GhostScript autoprn

# Where is PostScript? (Vendor-wise view)

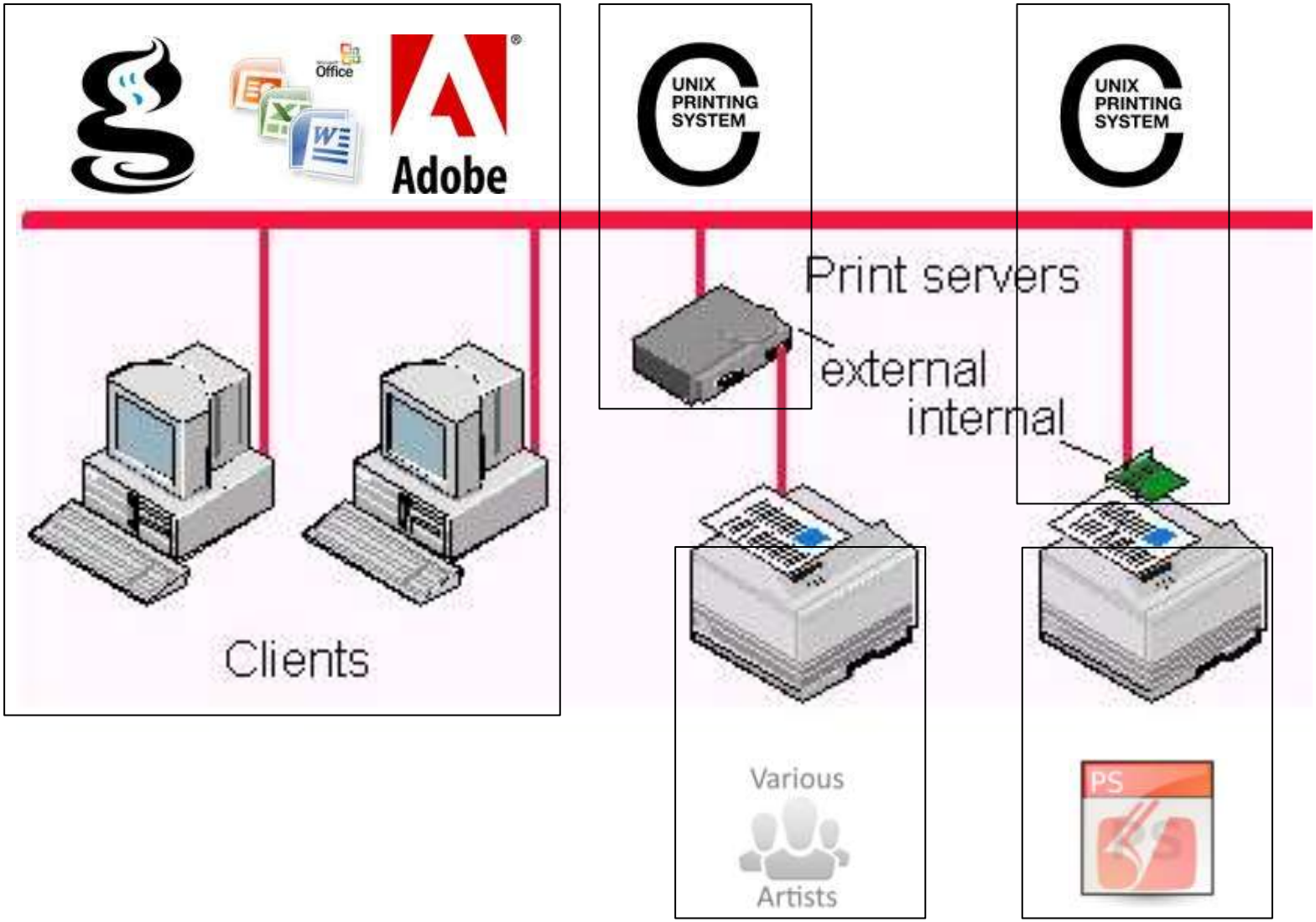

Applications incorporating the PS interpreter



Applications/vendors producing the PS interpreter


The PS interpreter specifications and standards

# Where is PostScript? (Role-wise view)



# 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 firmw
update file that is provided as part of this update package. Firmware update fil
will have a file extension of ".ps". *Shown in the upper red oval.*

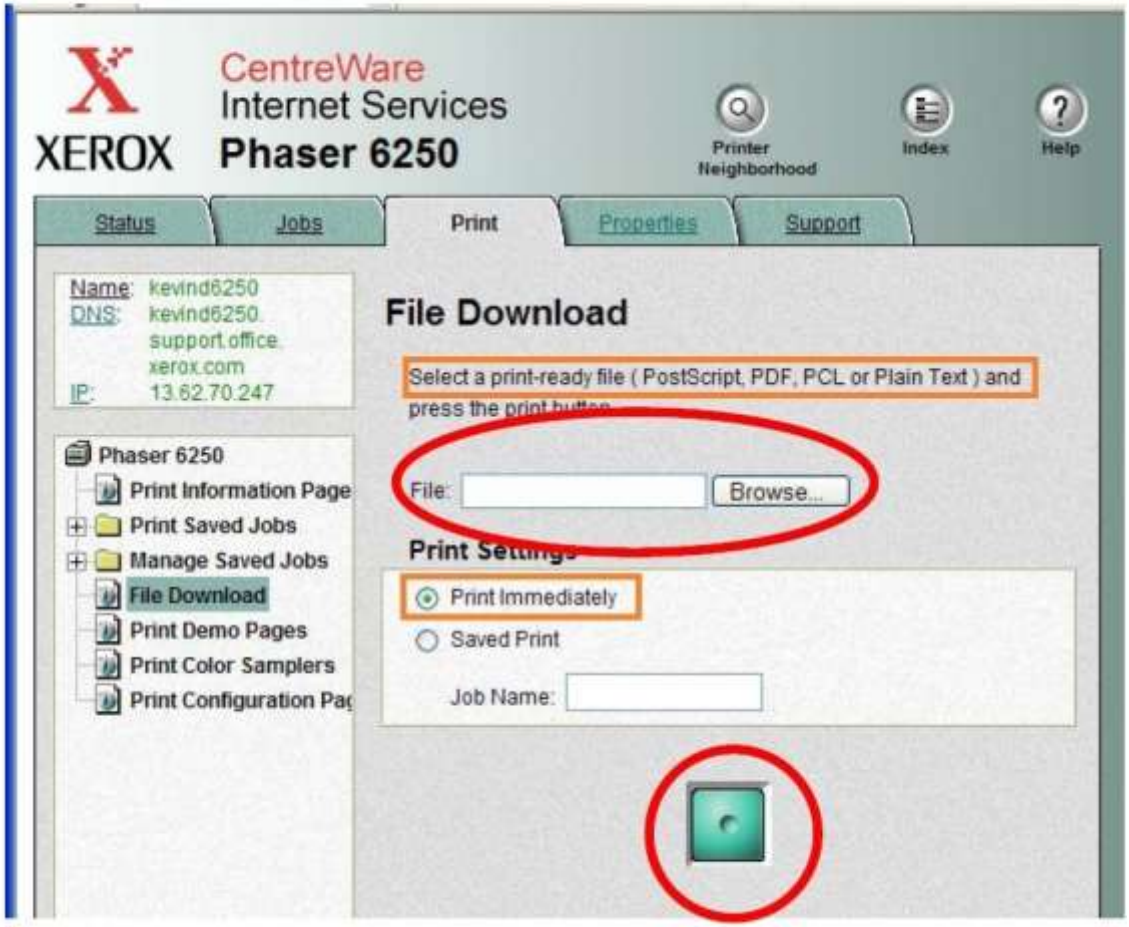
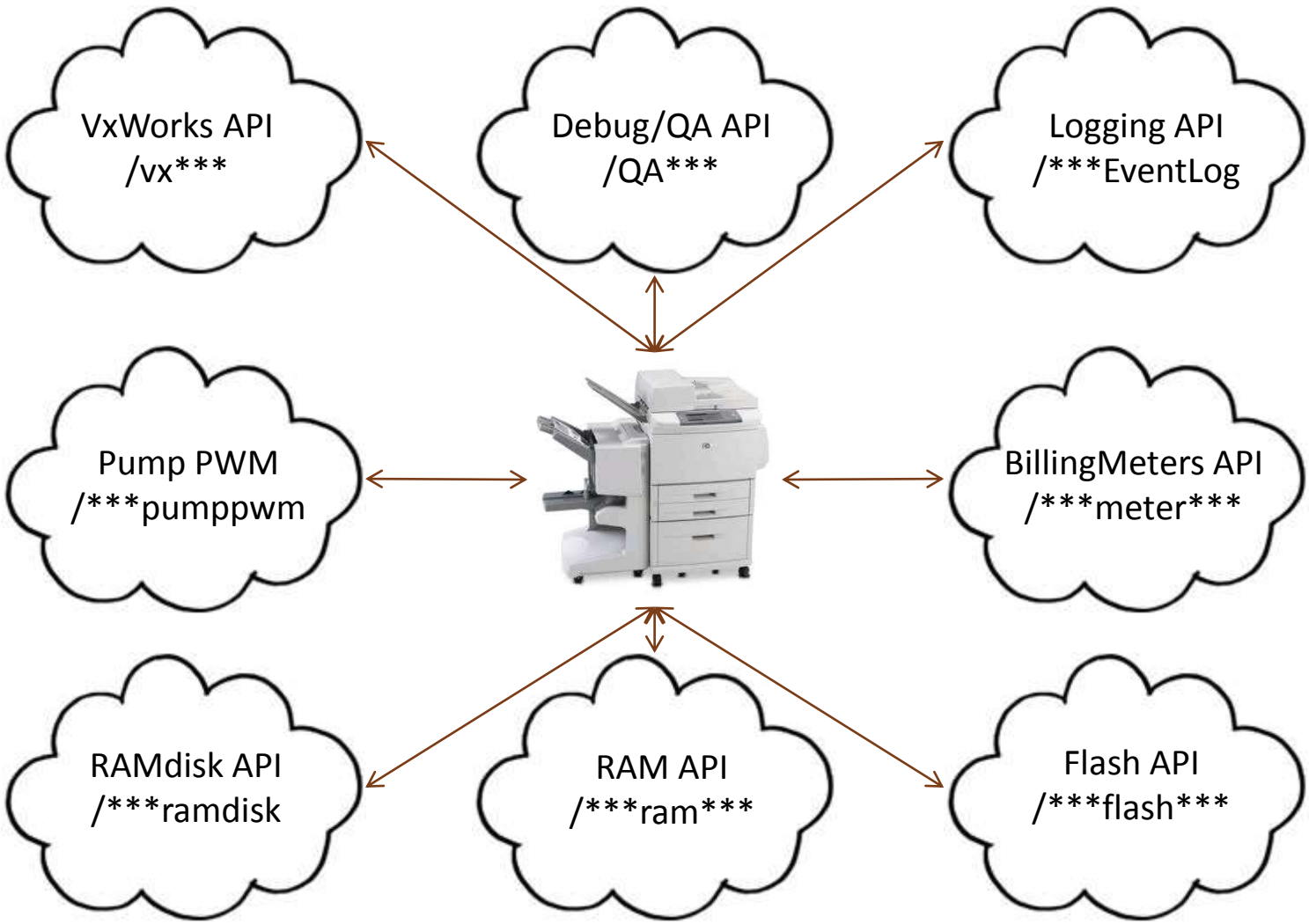
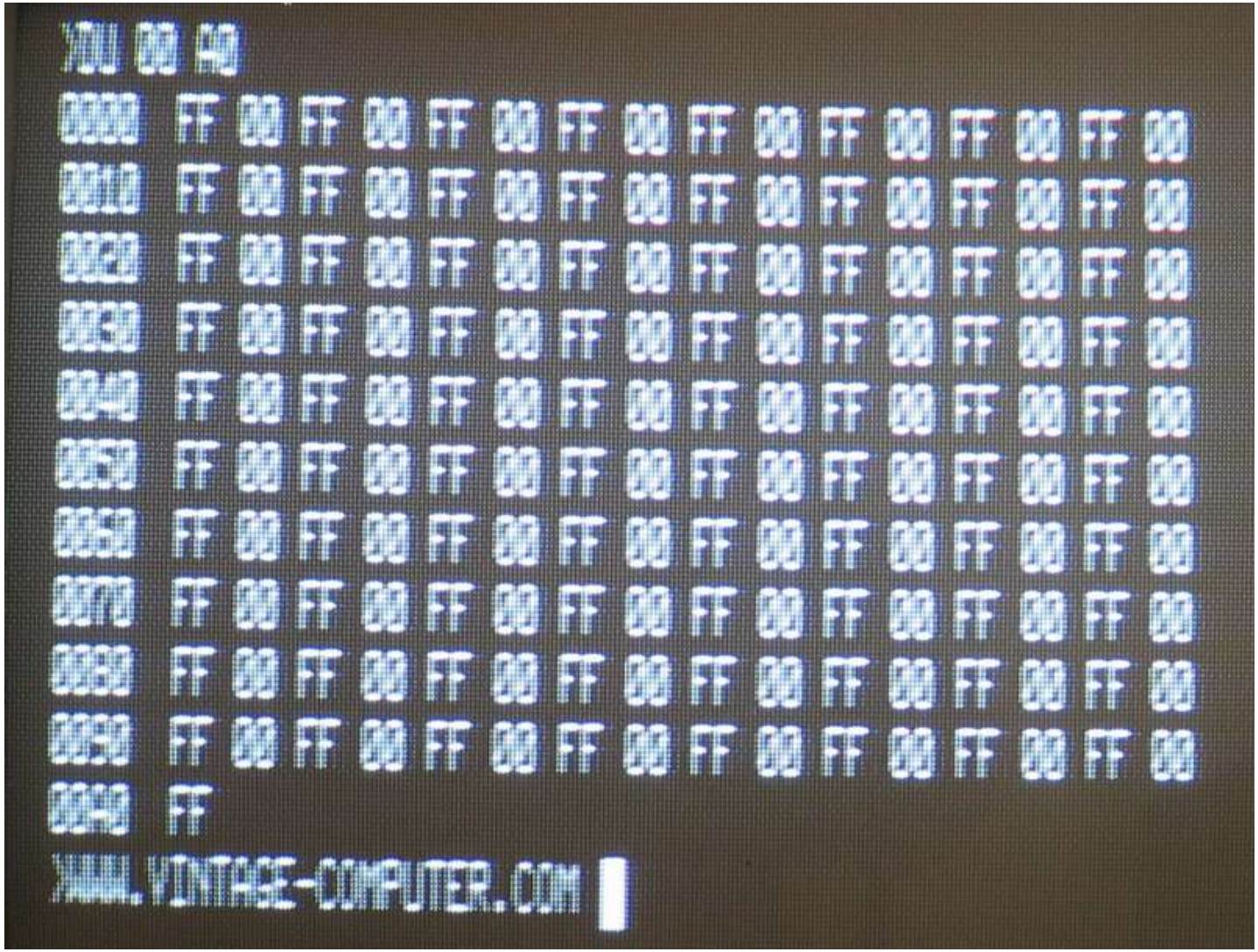



**Figure 4: Select the firmware update file and press the green button to send it.**

# This is too good to be true….



# Memory dumping reveals computing secrets



# Demo

Home - Phaser 8560N - Mozilla Firefox

File Edit View History Bookmarks Tools Help

New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | Home - P...

192.168.0.103 | gibraltar offshore

Most Visited | Getting Started | Latest Headlines | Keep It!

CentreWare
Internet Services
**Phaser 8560**

Printer Neighborhood | Index | Help

Ready

Name: Phaser 8560N
DNS: Unknown
IP: 192.168.0.103
Contact:
Location:
Status: Ready

Refresh Status

**Features**
- √ Premium color printing - up to 2400 FinePoint
- √ Fast printing up to 30 ppm and unrivaled 6 seconds to first page
- √ Outstanding performance with 600 MHz processor
- √ Easy to load solid ink consumables
- √ True Adobe PostScript 3
- √ Easy installation and use with Phaser Software

**Optional Features**
**(√ = installed on this system)**
- Automatic two-sided printing
- 525-Sheet feeder
- Advanced Features
- √ Network Interface

**Printer Drivers**
Install Printer Drivers

Status
Jobs
Print
Properties
Support



XEROX

Record
Stop
Pause

# Admin restriction fail to prevent memory dumping

# Demo

Protected Object - Mozilla Firefox

File Edit View History Bookmarks Tools Help

New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | New Tab | Protected... | Base64 Onlin...

192.168.0.103/securitysettings.html

motobit base64

Most Visited | Getting Started | Latest Headlines | Keep It!

## Protected Object

This object on the RomPager server is protected.

Return to last page

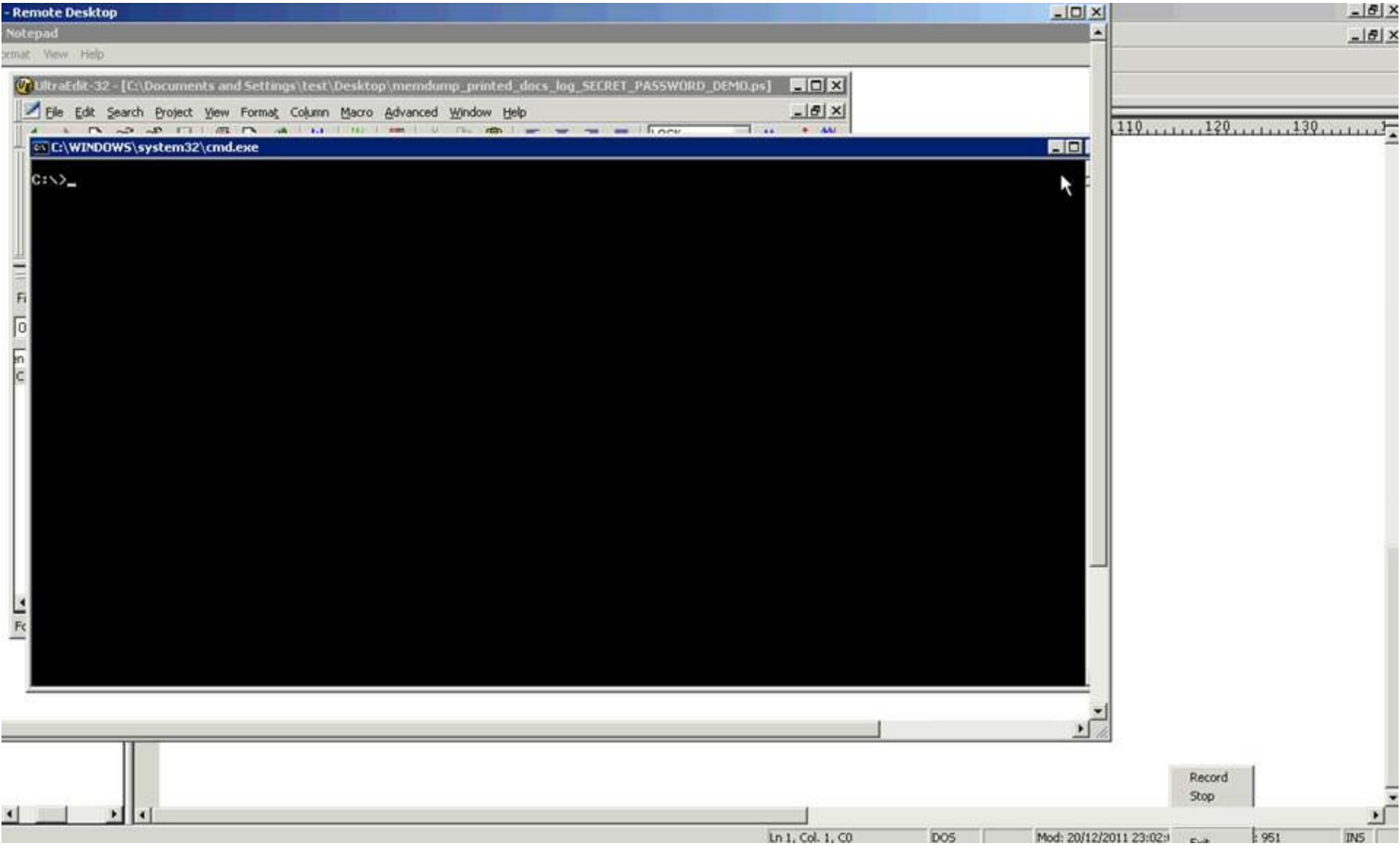
# Basic auth password can be dumped

# HTTPS / IPsec secrets are “leaky” as well…

```
1  IPSec AUTHKEY
2      66306630663066306630663066302222
3
4  /ramDrv/../ssl/private/clientkey.pem
5      BJBgkqhkiG9w0BBQ0wPDAbBgkqhkiG9w0BBQwwDgQIt/VXBECuFwMCAggA
6      MB0GCWCGSAFlAwQBAgQQ0bFFTwd+A[illegible]+9U31Ngp/bgSCAoDoth9xVwlUwwLGrnPX
7      ..............................[illegible]..............................
8      ..............................[illegible]..............................
9      ..............................[illegible]..............................
10     /zT8zr+wt1OHxSBj6WFqVXOwNFPkcsqfuUXxVJ+HcuaUuUpTsTlelBSDC2m5MM76
11     hlTx0/Z9/pfF09zFXqOEdOukc3wRlU76b56fhupORKtyH9woAgT8a4pb8hYPUgsJ
12
```

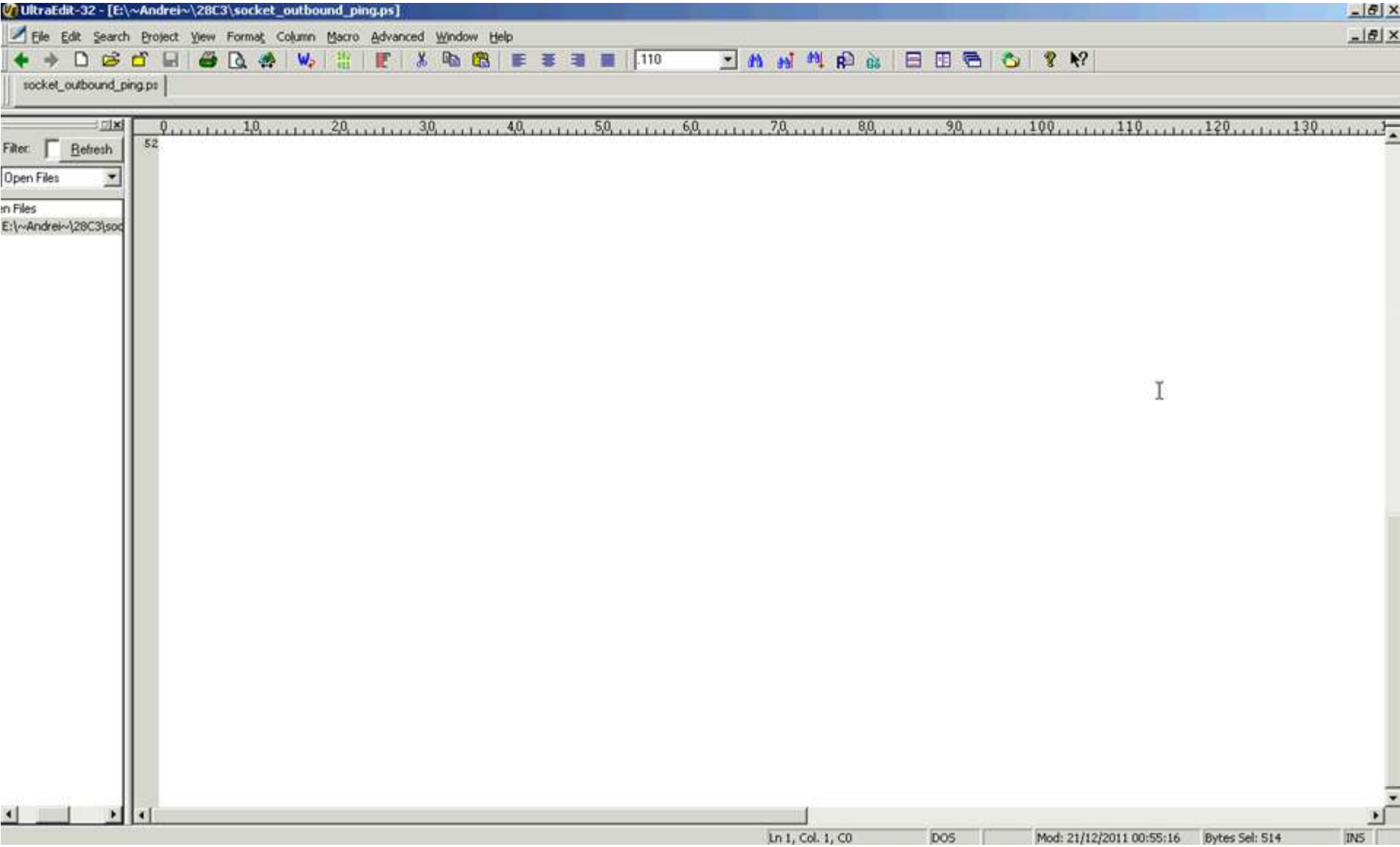
0x66306630663066306630663066302222

# Demo


Remote Desktop
Notepad
UltraEdit-32 - [C:\Documents and Settings\test\Desktop\memdump_printed_docs_log_SECRET_PASSWORD_DEMO.ps]
File Edit Search Project View Format Column Macro Advanced Window Help
C:\WINDOWS\system32\cmd.exe
C:\>_
Record
Stop
Ln 1, Col. 1, C0
DOS
INS

# Attacker has access to printed document details

# Demo


UltraEdit-32 - [E:\~Andrei~\28C3\socket_outbound_ping.ps]
File Edit Search Project View Format Column Macro Advanced Window Help
socket_outbound_ping.ps
Filter: Refresh
Open Files
Ln 1, Col. 1, C0
DOS
Mod: 21/12/2011 00:55:16
Bytes Sel: 514
INS

# Attacker has access to BSD-style sockets…


Two-way BSD-style sockets communication

# Analyzed MFP cannot protect effectively

| Protection measures | Fail / warn / ok |
|---|---|
| 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 | ⛔ |

# Plenty of Xerox printers share affected PS firmware update mechanism

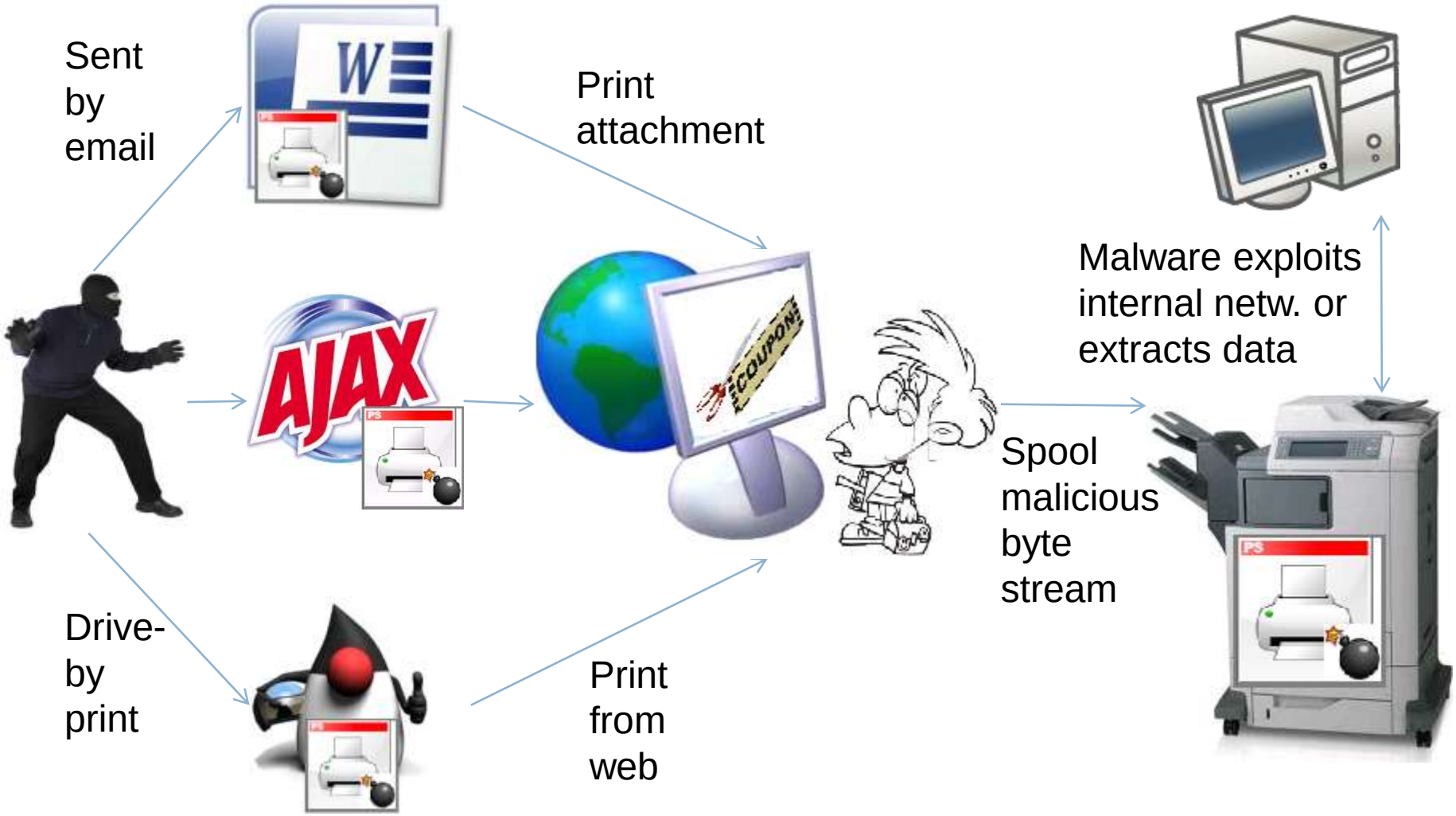
| | |
|---|---|
| Xerox Phaser 8560DN | Xerox ColorQube 8570DN |
| Xerox Phaser 8560DX | Xerox ColorQube 8570DT |
| Xerox Phaser 8560N | Xerox ColorQube 8870DN |
| Xerox Phaser 8560DT | Xerox Phaser 7760DN |
| Xerox Phaser 8560MFP/D | Xerox Phaser 7760DX |
| Xerox Phaser 8560MFP/T | Xerox Phaser 7760GX |
| 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?
4. 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**

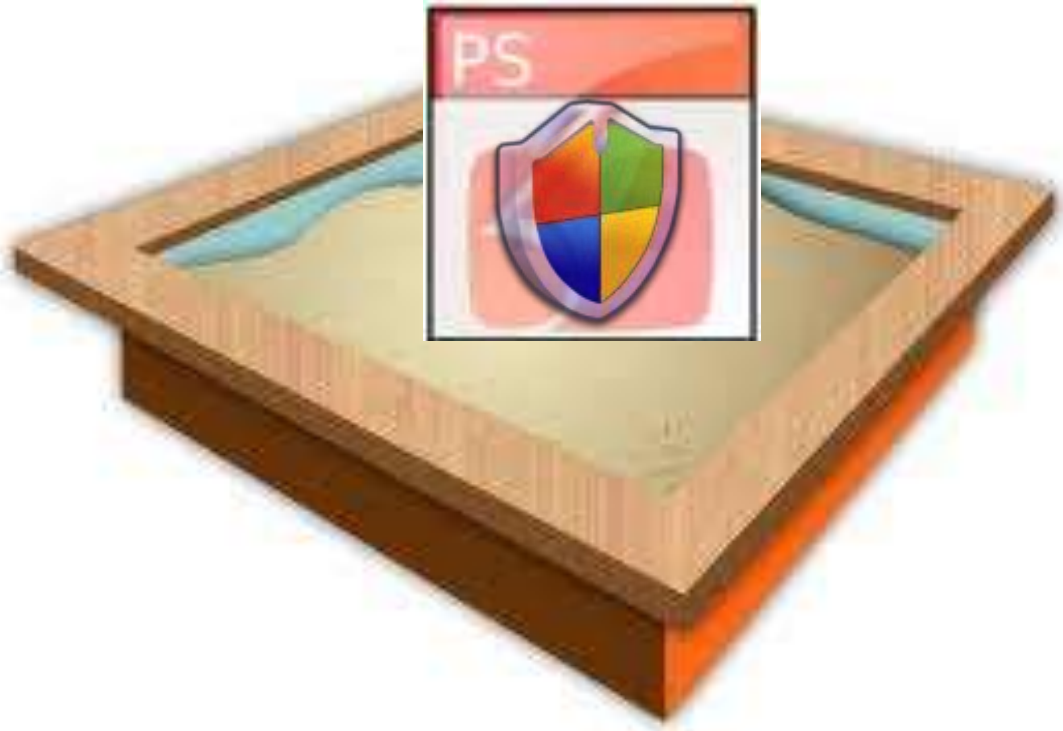


# Agenda

1. Quick refresher
2. What about PostScript?
3. So, what and how did you find?
4. Attacks in a nutshell
5. 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**<br>• **Route print-jobs thru sandboxed print-servers**<br>• **Replace PS drivers with PCL ones (well…)**<br>• Disable Language Operator Authorization<br>• Look for security bulletins and patch<br>• Sandbox printers in your network<br>• Include MFPs in security audit lifecycle |
| Users | • Do not print from untrusted sources<br>• Be suspicious on PostScript files |
| Vendors | • Create realistic MFP threat models<br>• Do not enable/expose super-APIs |

# Acknowledgements

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

SECURITY RESEARCH LABS

# 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

# Questions?

**Andrei Costin** andrei@andreicostin.com
http://andreicostin.com/papers

# Backup slides zone

# Demo

Administrative Security Settings - Phaser 8560N - Mozilla Firefox

File Edit View History Bookmarks Tools Help

192.168.0.103/securitysettings.html

Most Visited Getting Started Latest Headlines Keep It!

Clone Printer

| | Admin | Key User | Any User |
|---|---|---|---|
| **Administration** | | | |
| Modify Configuration Web Pages | ✓ | ☑ | ☐ |
| View Configuration Web Pages | ✓ | ☑ | ☐ |
| View Home & Status Web Pages | ✓ | ☑ | ☐ |
| Manage Job Accounting | ✓ | ☑ | ☐ |
| Delete Font File | | | |
| **Web Server Pri** | | | |
| Print Demo Pac | | | |
| File Download | | | |
| **Printer Neighbc** | | | |
| Modify Preferer | | | |
| View Preferenc | | | |
| Initiate Printer Search | ✓ | ☑ | ☐ |
| Initiate Status Refresh | ✓ | ☑ | ☐ |
| Generate Reports | ✓ | ☑ | ☐ |

**Authentication Required**

A user name and password are being requested by http://192.168.0.103. The site says: "View Configuration Web Pages"

User Name:

Password:

OK Cancel

**Language Operator Authorization**

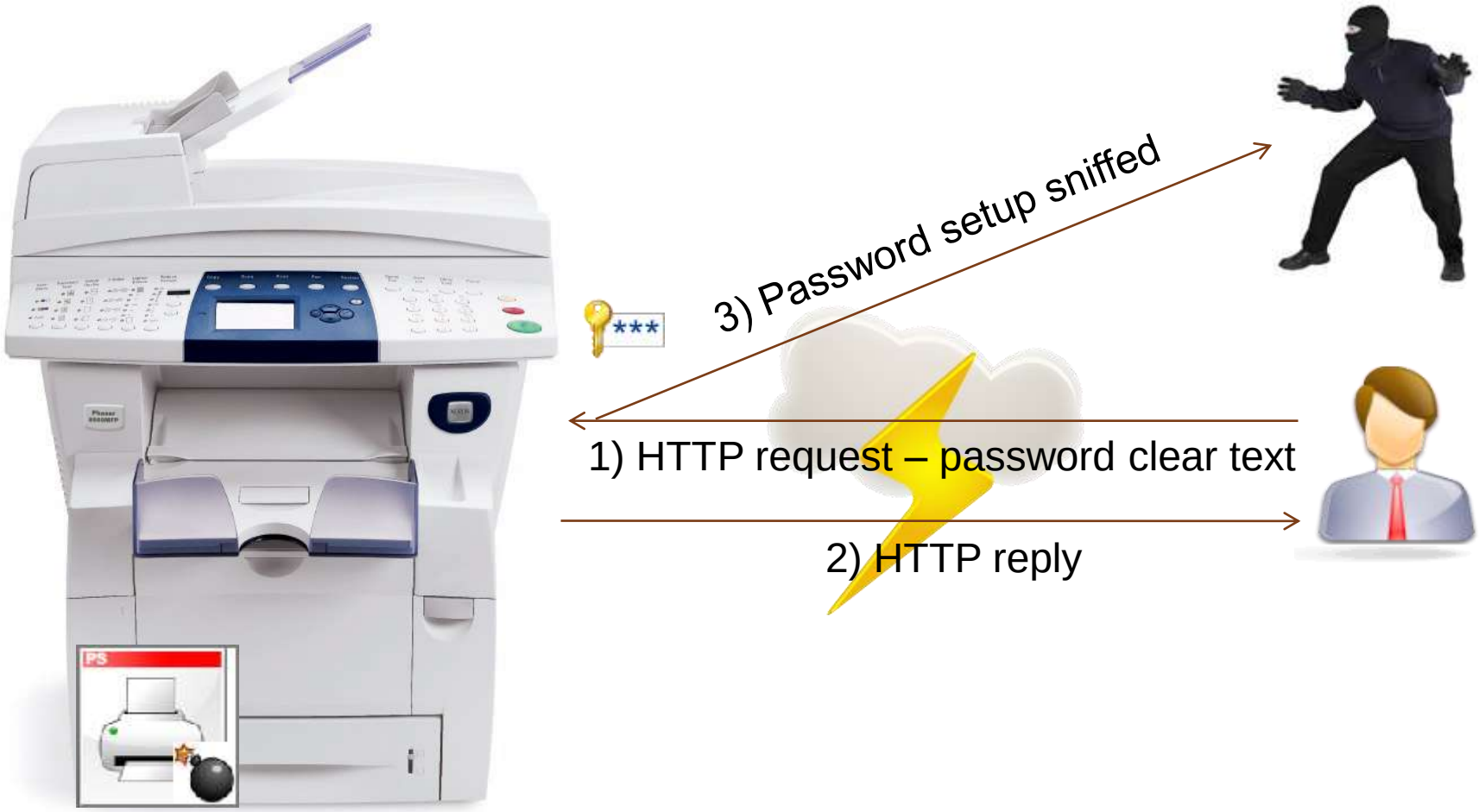
Some printer languages are capable of modifying the device configuration. Uncheck the box to prevent configuration changes by printer language operations.

Allow printer configuration changes by language operations ☑

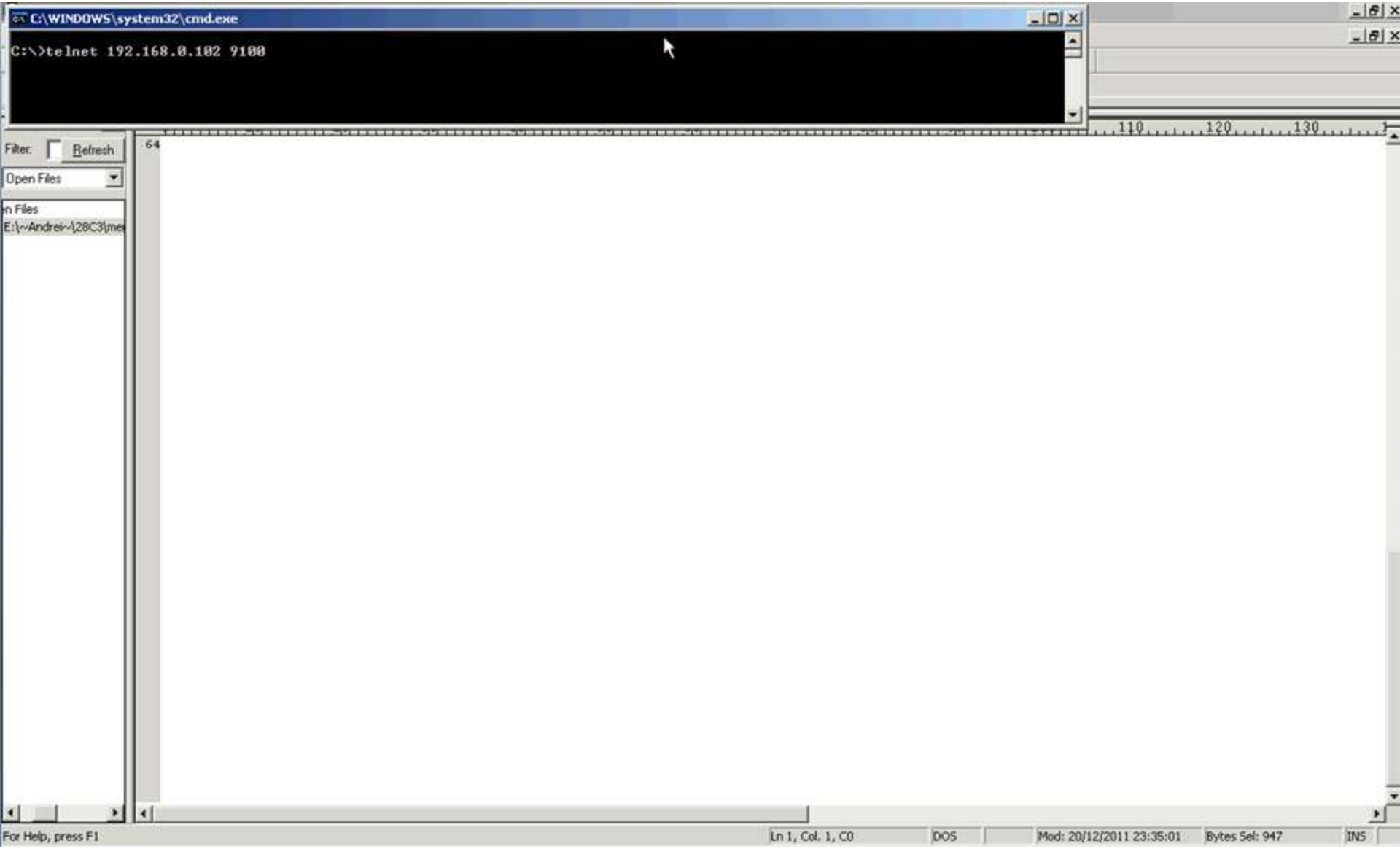
Save Changes Discard Changes

Waiting for 192.168.0.103...

# Password setup is sniffed by the attacker



# Demo


C:\WINDOWS\system32\cmd.exe
C:\>telnet 192.168.0.102 9100
Filter:
Refresh
Open Files
For Help, press F1
Ln 1, Col. 1, C0
DOS
Mod: 20/12/2011 23:35:01
Bytes Sel: 947
INS

# Attacker has access to network topology – no-scan

2) Network topology, attackable devices

1) Device discovery (SDP, UPnP)