Hacking MFPs
PostScript(um–you’ve been hacked)

Andrei Costin <andrei@srlabs.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?)

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

http://www.youtube.com/watch?v=KrWFOo2RAnk (there are false claims of some guys)
... 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...
Adobe is the dominant PS implementation

Distribution of Postscript interpreters

- Adobe PS interpreters
- Other PS interpreters

Source: Adobe specification supplement note
PS is built to handle complex processing tasks

- Graphics & patterns
- Complex math
- Web servers
- File systems
- Ray-tracing, OpenGL
- Milling machine
- XML Parsers
- I/O subsystems
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-executive debug enabled
- PS-executive debug disabled/NA
PS> “shell” – how?

- Code demo – telnet 192.168.0.1 9100 and dump this:

```plaintext
1 %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

SECURITY RESEARCH LABS
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 files 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
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

1) Authorization: Basic YWRtaW4yO…

2) HTTP/1.1 200 OK

3) Encoded password sniffed
HTTPS / IPsec secrets are “leaky” as well...
Demo
Attacker has access to printed document details

1) Protected/secret document

2) Printed document details
Demo
Attacker has access to BSD-style sockets...

Two-way BSD-style sockets communication
## Analyzed MFP cannot protect effectively

<table>
<thead>
<tr>
<th>Protection measures</th>
<th>Fail / warn / ok</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege level separation</td>
<td>✗</td>
</tr>
<tr>
<td>Secure password setup</td>
<td>✗</td>
</tr>
<tr>
<td>Secure (basic) auth</td>
<td>✗</td>
</tr>
<tr>
<td>HTTPS, IPSEC secrets protection</td>
<td>✗</td>
</tr>
<tr>
<td>Network topology protection</td>
<td>✗</td>
</tr>
<tr>
<td>In-memory document protection</td>
<td>✗</td>
</tr>
<tr>
<td>Restrict sockets on unprivileged modules</td>
<td>✗</td>
</tr>
</tbody>
</table>
Plenty of Xerox printers share affected PS firmware update mechanism

<table>
<thead>
<tr>
<th>Xerox Phaser 8560DN</th>
<th>Xerox ColorQube 8570DN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xerox Phaser 8560DX</td>
<td>Xerox ColorQube 8570DT</td>
</tr>
<tr>
<td>Xerox Phaser 8560N</td>
<td>Xerox ColorQube 8870DN</td>
</tr>
<tr>
<td>Xerox Phaser 8560DT</td>
<td>Xerox Phaser 7760DN</td>
</tr>
<tr>
<td>Xerox Phaser 8560MFP/D</td>
<td>Xerox Phaser 7760DX</td>
</tr>
<tr>
<td>Xerox Phaser 8560MFP/T</td>
<td>Xerox Phaser 7760GX</td>
</tr>
<tr>
<td>Xerox Phaser 8560MFP/N</td>
<td>Xerox Phaser 7760GXM</td>
</tr>
<tr>
<td>Xerox Phaser 8560MFP/X</td>
<td>Xerox Phaser 4510B B/W</td>
</tr>
<tr>
<td>Xerox Phaser 8500N</td>
<td>Xerox Phaser 4510N B/W</td>
</tr>
<tr>
<td>Xerox Phaser 8500DN</td>
<td>Xerox Phaser 4510DT B/W</td>
</tr>
<tr>
<td>Xerox Phaser 8550DP</td>
<td>Xerox Phaser 4510DX B/W</td>
</tr>
<tr>
<td>Xerox Phaser 6360N</td>
<td>Xerox Phaser 5550B B/W</td>
</tr>
<tr>
<td>Xerox Phaser 6360DN</td>
<td>Xerox Phaser 5550N B/W</td>
</tr>
<tr>
<td>Xerox Phaser 6360DT</td>
<td>Xerox Phaser 5550DN B/W</td>
</tr>
<tr>
<td>Xerox Phaser 6360DX</td>
<td>Xerox Phaser 5550DT B/W</td>
</tr>
<tr>
<td>Xerox ColorQube 8570N</td>
<td>Xerox Phaser 8510</td>
</tr>
</tbody>
</table>
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
- Sent by email
  - Drive-by print

Stage 2 - Printing
- Print attachment
  - Print from web

Stage 3 – Exploiting/spying
- Malware exploits internal netw. or extracts data
  - Spool malicious byte stream
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

<table>
<thead>
<tr>
<th>Actor</th>
<th>Suggested actions</th>
</tr>
</thead>
</table>
| Admins | • 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 |
| Vendors| • Create realistic MFP threat models  
• Do not enable/expose super-APIs |
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 continuous vulnerability patching

Questions?

Andrei Costin andrei@srlabs.de
http://andreicostin.com/papers
Password setup is sniffed by the attacker

1) HTTP request – password clear text

2) HTTP reply

3) Password setup sniffed
Demo
Attacker has access to network topology – no-scan

1) Device discovery (SDP, UPnP)

2) Network topology, attackable devices

SECURITY RESEARCH LABS