Compromising Multifunction Printers

A Case Study of Epson MFP Security

Yves-Noel Weweler
y.weweler@fh-muenster.de
Multifunction Printers

„MFP (Multi Function Product/ Printer/ Peripheral), multifunctional, all-in-one (AIO) ...“

https://en.wikipedia.org/wiki/Multi-function_printer

Typically combine:

• Printer
• Scanner
• Photocopier
• Fax

Today they are small sized computers capable of running fully blown operating systems
Interrogation

How secure are MFP’s and how can an attacker communicate unnoticed with a device?

Motivation:
• Germany (2014): ~ 81 million citizens
  • Ink-jet printer: 22.71 million (~ 28%)
  • Multifunction printer: 21.68 million (~ 26.7%)


• Highly sensible documents
• Connected to access control systems
Epson WF-2540

**Hardware:**
- ARM926EJ-Sid Processor
- 64 MB RAM
- 12 MB EEPROM
- FAX / DATA Modem
- LAN / WLAN / USB

**Software:**
- GNU/Linux Kernel 2.6.18
- BusyBox 1.7.2
- uClibc 0.9.29
- Proprietary binaries
How to Compromise?

Locally:
- USB
- Hardware access (EEPROM)

Remote:
- Network services
- Self-built HTTP Server
- Firmware updates
Firmware Structure
IPL-Header

- Describe firmware structure with records
- Records refer to data sections
- Checksums do not cover headers

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>32</th>
<th>40</th>
<th>48</th>
<th>56</th>
<th>64</th>
<th>72</th>
<th>80</th>
<th>88</th>
<th>96</th>
<th>104</th>
<th>112</th>
<th>120</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPSON IPL</td>
<td>FLAGS</td>
<td>PREFIX</td>
<td>0x00</td>
<td>LEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTYPE</td>
<td>CSUM</td>
<td>0x00</td>
<td>DATA LEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTYPE</td>
<td>CSUM</td>
<td>NUM</td>
<td>FLAGS</td>
<td>DATA LEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Dumping the Memory

- Readout EEPROM’s
- Unveil hidden contents
- Understand bootcode & checksums
Update Process Mechanics

• 1:1 copy of firmware into flash
• Hidden JFFS2 filesystem
• Bootloader not updated by firmware
Firmware

• Taken apart the firmware format
• Decoded checksum algorithm
• Capable of repacking custom firmware
• Capable of compiling own software

Problems:

• No signing
• No encryption
• Poor checksums
Firmware Update Mechanism

- USB
- HTTP (LAN / WLAN)
- ~40 – 45 seconds

Two level process:
1. Enter update mode
2. Upload firmware binary

Problems:
- No authentication
- No CSRF prevention

Diagram:
- Attacker
  - Initialise Update
    - GET /FIRMWAREUPDATE
    - 200 OK
  - Transmit firmware
    - POST /DOWN/FIRMWAREUPDATE/ROM1
    - 204 Content Not Found
- Printer

Yves-Noel Weweler
24. DFN-Konferenz "Sicherheit in vernetzten Systemen"
Remote Exploitation Upgrade

- Victim visits a website and executes a malicious script
- Victim is tricked into updating the printer using CSRF, acting as the attacker
Hidden Communication

Unnoticed communication with a device?

- Utilize integrated modem
- Use FAX connection as a proxy
- Access networks without IP-connectivity

Modem:

- Softmodem
- Hook communication between modem and applications
- Implemented using a kernelmodule
Hooking the Modem

• Man-in-the-Middle-Attack on data channel
• Controlling incoming and outgoing connections
• Reading and writing data
Significance

Vulnerability reaches maximal CVSS-Value of 10

EPSON:
- ~15% market share in 2014
- ~4.9 million printers sold in 2014
- ~343 printer models

Vulnerable devices:
- ~62 printers in the "WorkForce" series
- ~5946 vulnerable devices in the IPv4 range (03/2016)
- "Stylus" series (~211 models) probably also vulnerable

http://www.epson.com/cgi-bin/Store/BuyInkList.jsp
How to protect?

Epson started shipping new firmware at the beginning of 2016

• Update your printers firmware
• Restrict device access
• Block HTTP on port 80 for non administrative users
Summary

How secure are MFP’s and how can an attacker communicate unnoticed with a device?

• Successful penetration of printers
• All devices with network access are vulnerable
• Control over integrated modem
• Modem can be used to transfer data without IP-connectivity
Questions?

Thank you for your attention