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%)

  https://multifunktionsdruckertest-24.de/entwicklung-des-anteils-von-druckern-und-scannern-in-deutschen-haushalten/
- 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?

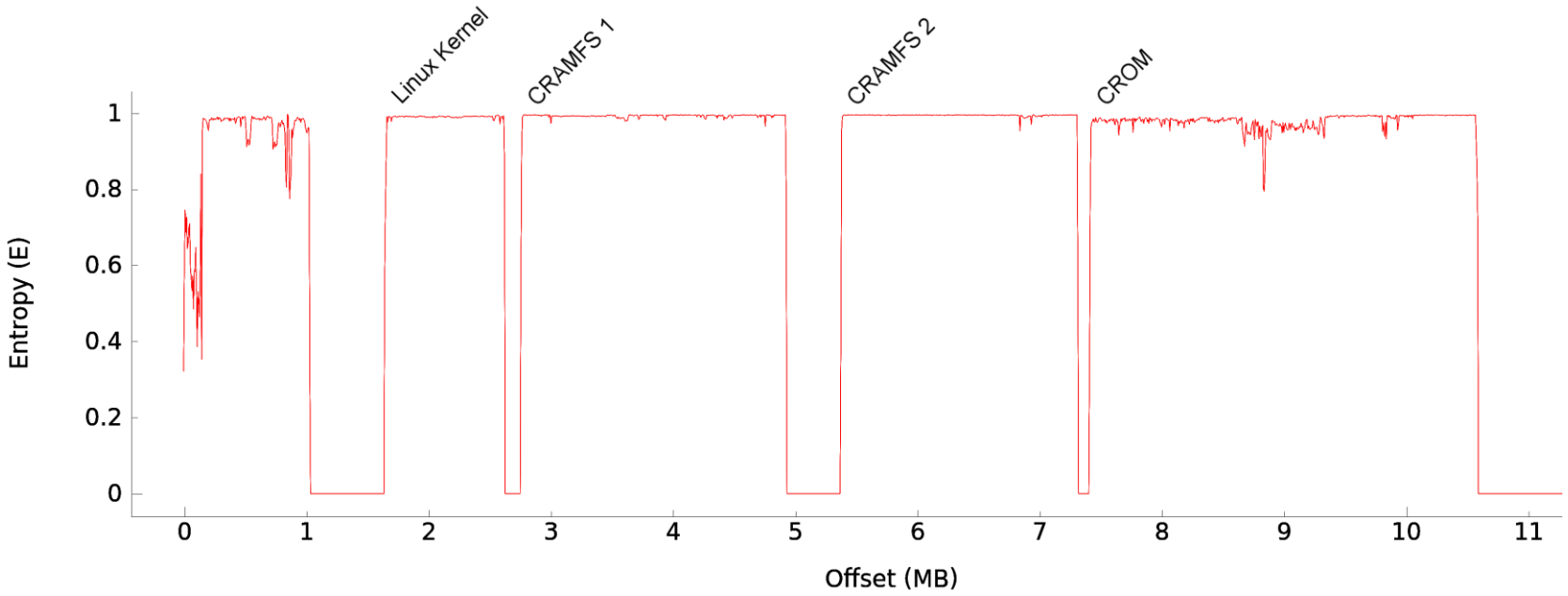
Locally:

- USB
- Hardware access (EEPROM)

Remote:

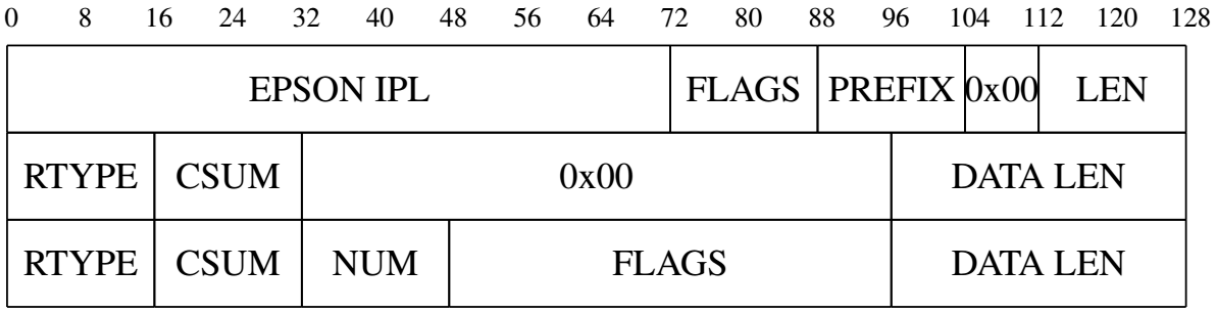
- Network services
- Self-built HTTP Server
- **Firmware updates**

Firmware Structure



IPL-Header

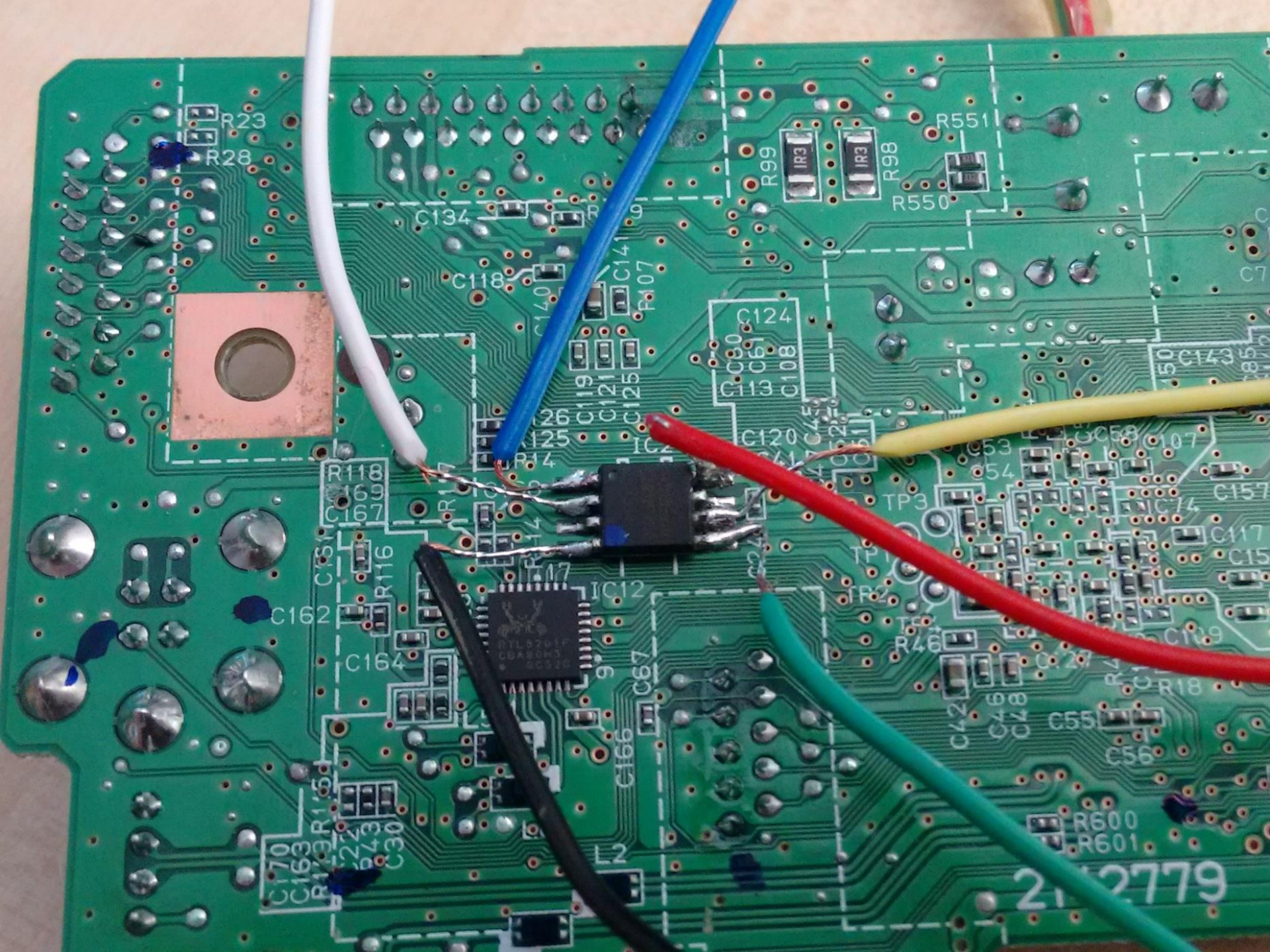
- Describe firmware structure with records
- Records refer to data sections
- Checksums do not cover headers

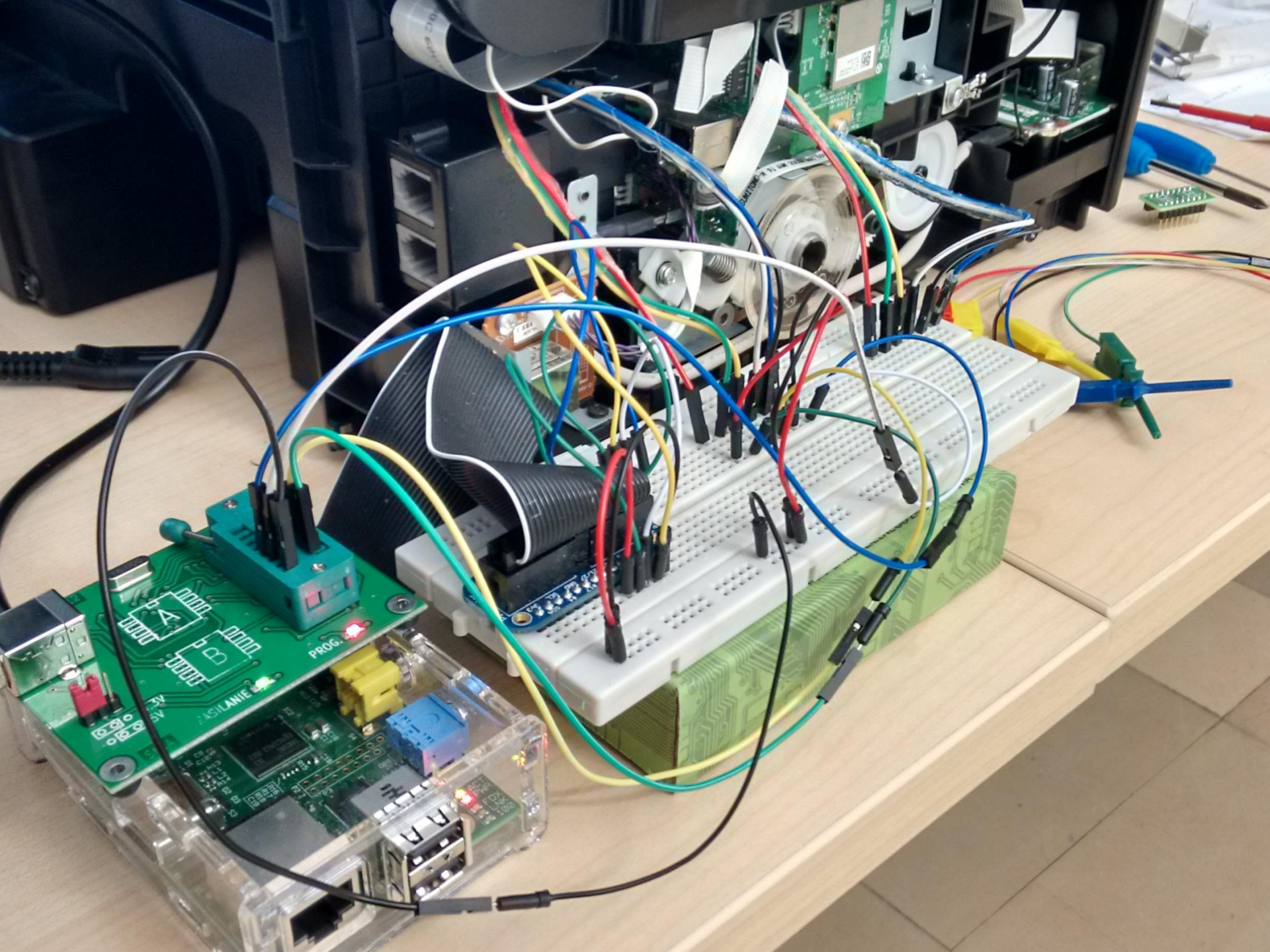


Dumping the Memory

- Readout EEPROM‘s
- Unveil hidden contents
- Understand bootcode & checksums

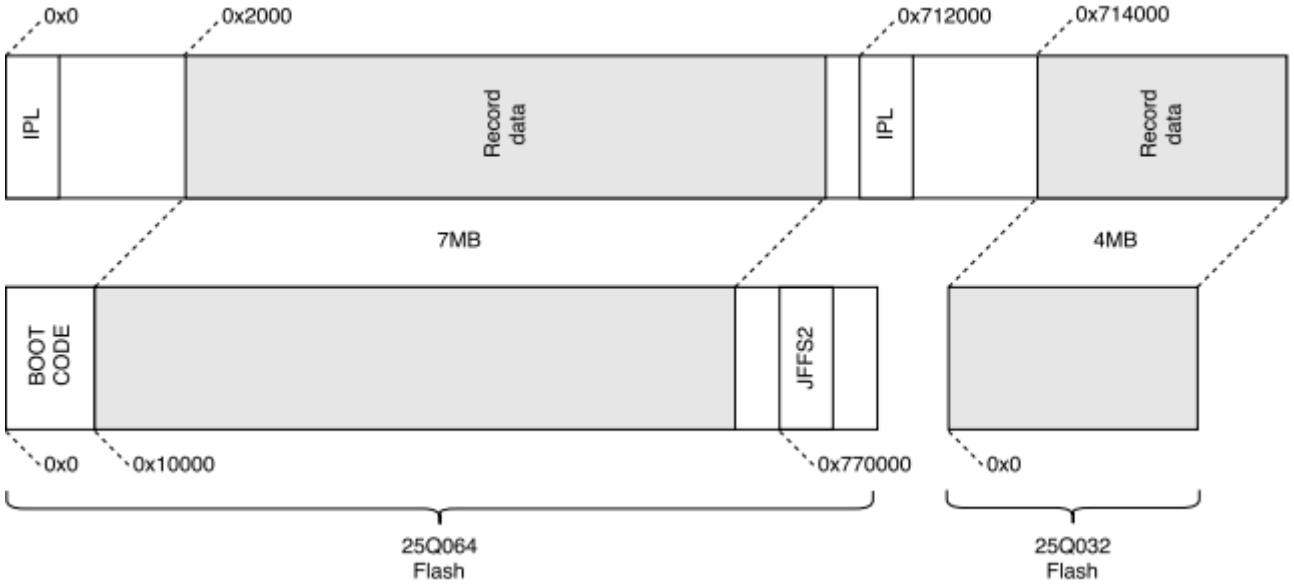
1
2
Click!
OK
3
OK
WF-2540


R23
R28
C134
C118
R551
R99
R98
R550
C124
C113
C120
R118
C167
C116
C162
C164
IC12
C67
C66
R46
C55
C56
R600
R601
L2
C170
C163
C30


PROG.

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

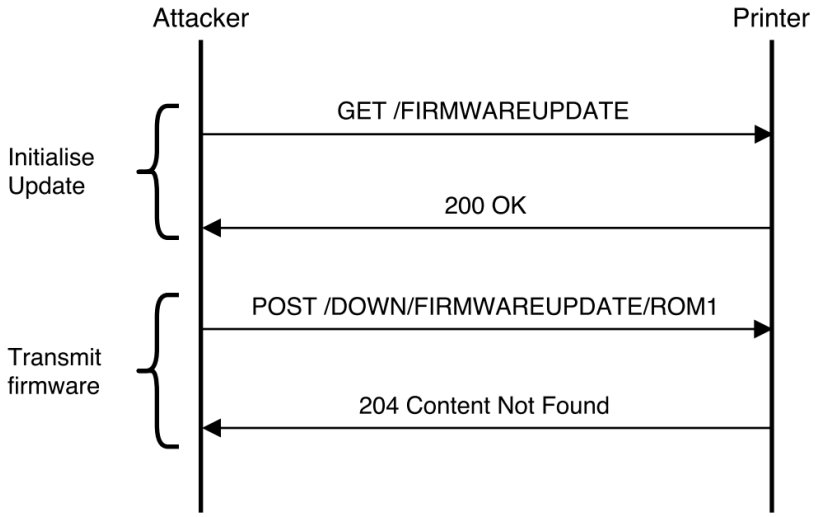
- USB
- HTTP (LAN / Wi-Fi)
- ~40 – 45 seconds

Two level process:

1. Enter update mode
2. Upload firmware binary

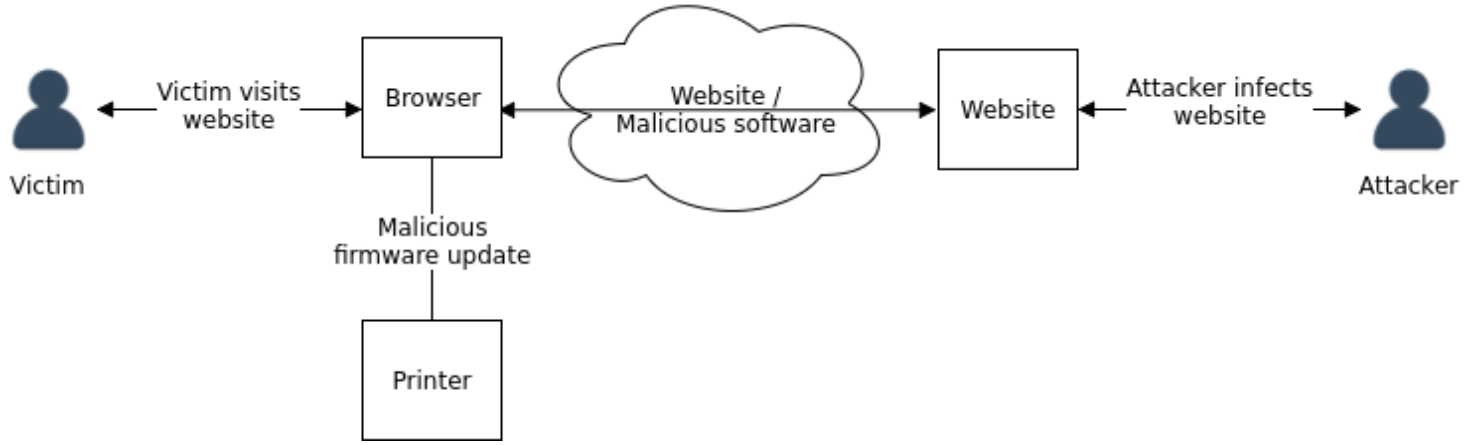
Problems:

- No authentication
- No CSRF prevention



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?

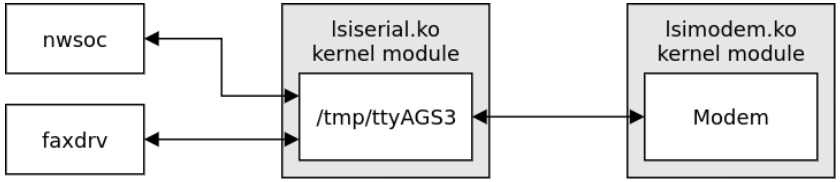
- Utilize integrated modem
- Use FAX connection as a proxy
- Access networks without IP-connectivity

Modem:

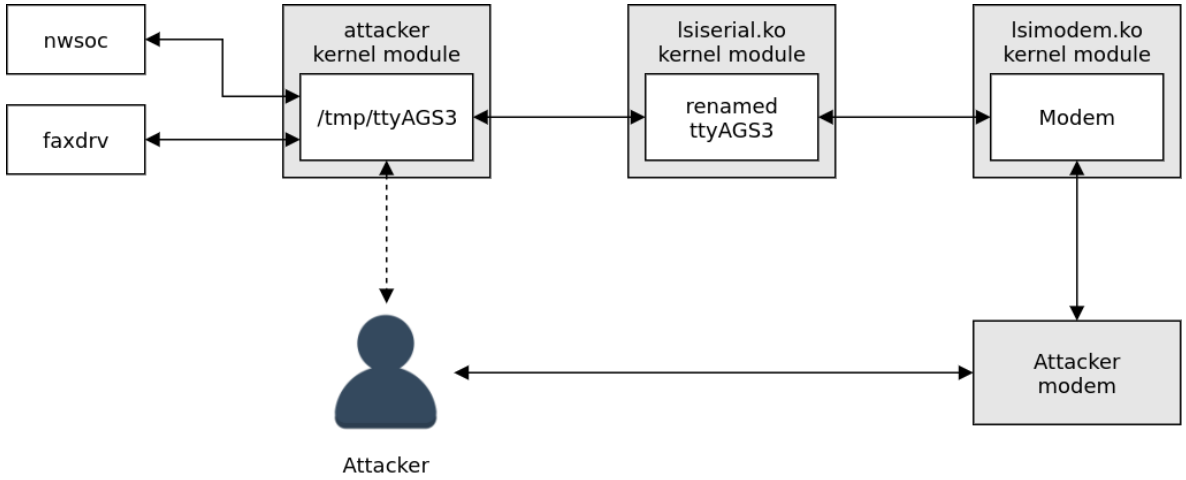
- Softmodem
- Hook communication between modem and applications
- Implemented using a kernelmodule

Hooking the Modem

Original

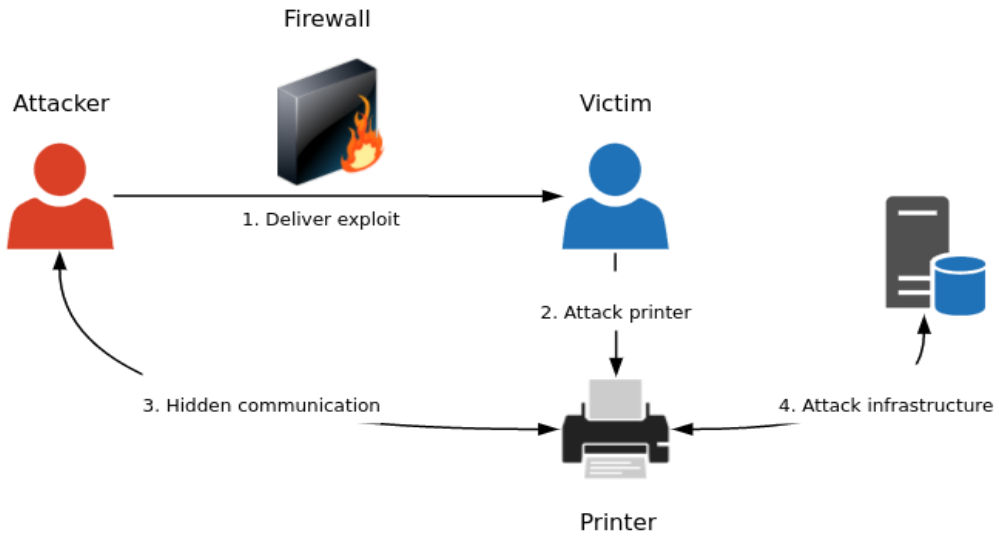


Compromised



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

http://www.epson.com/cgi-bin/Store/BuyInkList.jsp

Vulnerable devices:

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

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