Security Reflections on Multifunction Devices

Michael Schaefer
Matthias Luft

{mschaefer,mluft}@ernw.de

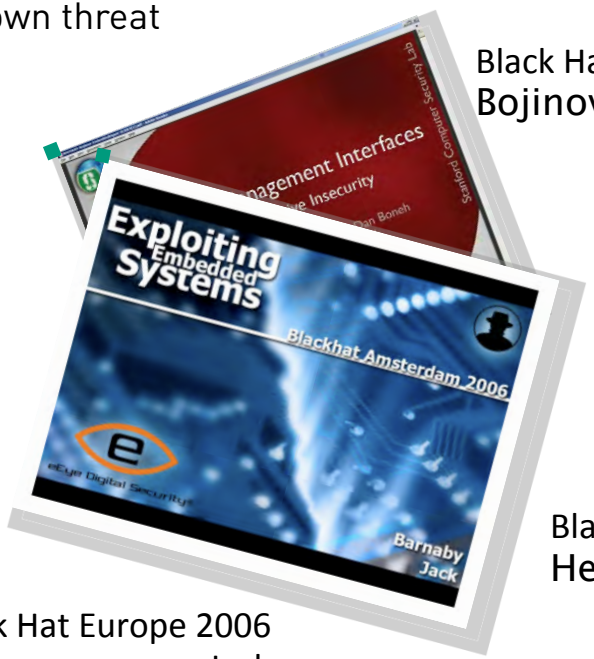
ERNW
providing security.

Agenda

- Motivation
- Multifunction Devices (MFD)
- Role of MFDs in Corporate Networks
- Threats and Vulnerabilities
- *Sisters' Act* of MFD Security
- Conclusions

Why MFD Security?

Because it's a well known threat



Black Hat Europe 2006
Jack

Black Hat USA 2010
Bojinov

Black Hat USA 2010
Heffner

Black Hat Europe 2010
Mende, Rey

Motivation

Printer compromise?

- Why not?

Motivation

Different understanding of MFDs

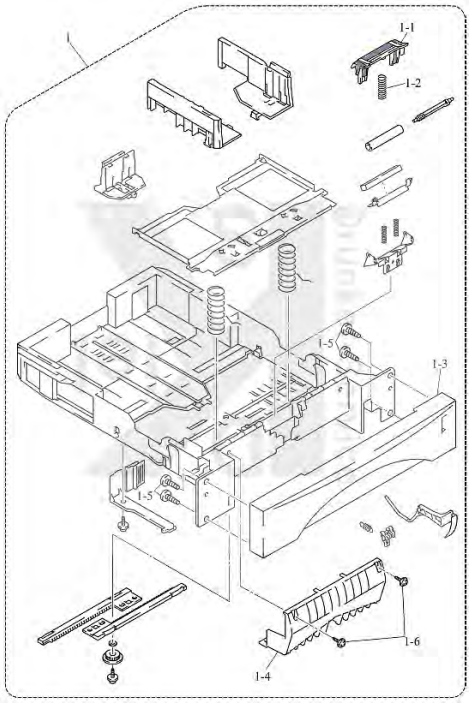
- *Aggregator of sensitive information*
- Multiple attack vectors exist

Definition of MFDs

- Quoting *SANS* (2007):
- *"In today's all-in-one world, you can now obtain single devices that are not only printers, but also*
  - *copiers,*
  - *scanners,*
  - *and fax machines.*
- *These networked multifunction devices (MFDs) are increasingly common in enterprise environments [...]."*

ERNW
providing security.

Their components



- Printing unit
- Image scanner
- Modem for fax communication
- Network interface
- Processor & RAM
- Flash drive (often used for OS)
- Harddrive

Protocols

... and there are a lot!

- SMB
- PJL/PCL/PS/GS
- SNMP
- FTP
- HTTP
- SMTP
- POP3
- Telnet
- ...

Attack vectors!

Typical implementation

- Enterprise level networks
- Small and medium corporate networks
- Access control?
  - Use of MFDs is a critical business use case!
- Dedicated devices for higher management?
  - Some people claim to have seen this, but…

Threats

- When talking about security, it is always important to approach certain assets in a structured way.

Threats

My brother dropped my printer.

- Device compromise
- Physical access
- Information disclosure
- Abuse in context of social engineering attacks
- Eavesdropping

ERNW
providing security.

Vulnerabilities

- Programming flaws
- Lack of hardening
- No encryption
- Insecure file deletion
- Design errors
- Insufficient filtering

Warstories

- 2002:
  - Design errors
  - Code execution in embedded Java VM
- You responded, right? ;-)
  - Again...

The Evergreen

Web Vulnerabilities

- XSS, SQLi, Authentication Bypass
  - We don't have to tell, do we?
- Impact:
  - Arbitrary file download
  - Rogue firmware upload
  - IP filter manipulation
  - ...

ERNW
providing security.

Evergreens...

cntd

- SNMP
- Spam Relay
- Default SSL certs
- PostScript exploits
- Phone Home features

Underdogs

- PJL
- Actually, this is *really* lame
- @PJL RDYMSG DISPLAY = “INSERT COIN”

Underdogs

- PJL
- But might be used in social engineering context
- @PJL RDYMSG DISPLAY = “ERROR! Call 555-111”

PJL Cheat Sheet

Short digression

- @PJL ECHO “PJL TEST”
  - *@PJL ECHO “PJL TEST”*
- @PJL FSDIRLIST NAME=“0:\” entry=1 count=255
  - ...
  - *spool_files*
  - ...
- @PJL FSDIRLIST NAME=“0:\spool_files\” entry=1 count=255
  - 0001.jpg
  - 0002.jpg
  - ....
- @PJL FSDOWNLOAD FORMAT:BINARY SIZE=4096 NAME = “0:\spool_files\001.jpg”

ERNW
providing security.

Recent results?

Time for an own lab…

ERNW
providing security.

FTP Download

```
Connected to 10.66.66.10.
220 FTP print service:V-1.10/Use the network password for the ID if updating.
Name (10.66.66.10:uchimata):
230 User uchimata logged in.
Remote system type is ITRON.
ftp> ls
200 Ready command OK.
150 Transfer Start
total   26931500
-r--r--r--   1 root     printer    26931500 Mar  1  1993 c7200-g8ik9s-mz.124-2.XB10.bin
dr--r--r--   1 root     printer           0 Jan  2 03:44 BROTHER
226 Data Transfer OK.
```

FTP Download

```
ftp> cd BROTHER
250 CWD command successful
ftp> ls
200 Ready command OK.
150 Transfer Start
total      53829
dr--r--r--    1 root     printer           0 Jan  2 03:44 .
dr--r--r--    1 root     printer           0 Jan  2 03:44 ..
-r--r--r--    1 root     printer       53829 Jan  2 03:50 02010301.TIF
226 Data Transfer OK.
```

ERNW
providing security.

FTP Download

```
ftp> binary
200 Ready command OK.
ftp> get 02010301.TIF
local: 02010301.TIF remote: 02010301.TIF
200 Ready command OK.
150 Transfer Start
226 Data Transfer OK.
53829 bytes received in 1.14 secs (46.1 kB/s)
```

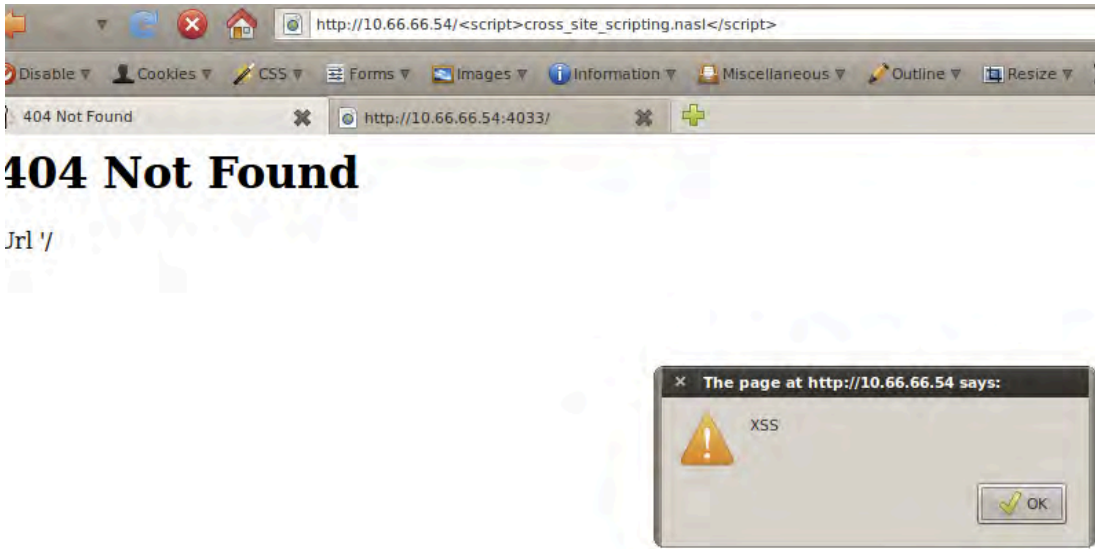
Arbitrary crashes

We didn't even try to fuzz...

- Crash
- Reboot
- Undefined behavior

XSS

Just because it's so mandatory ;-)



ERNW
providing security.

Forensic

- Hard drive disassembly
  - And it's so easy...
- Recovery of documents
  - Even easier? ;-)

Disassembly

Disassembly

This was even a hard one

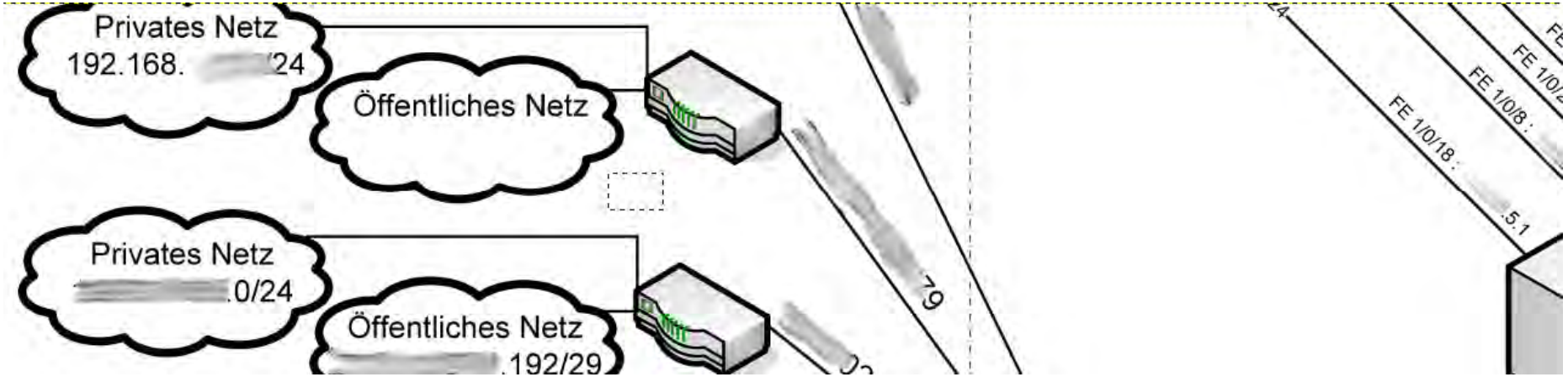
Reconstructing

```
0a 25 c7 ec 8f a2 0a 35  |%PDF-1.4.%.....5|
3c 2f 4c 65 6e 67 74 68  | 0 obj.<</Length|
69 6c 74 65 72 20 2f 46  | 6 0 R/Filter /F|
64 65 3e 3e 0a 73 74 72  |lateDecode>>.str|
d9 92 1c c5 15 f5 f3 58  |eam.x..\.......X|
be 84 1d 0e b3 19 64 43  |...S.........dC|

49 46 00 01 01 00 00 01  |......JFIF......|
43 52 45 41 54 4f 52 3a  |.......<CREATOR:|
20 76 31 2e 30 20 28 75  | gd-jpeg v1.0 (u|
20 4a 50 45 47 20 76 36  |sing IJG JPEG v6|
69 74 79 20 3d 20 31 30  |2), quality = 10|
```

- Punchline:
  Files are recoverable, even though they're not visible at first glance
  - Still surprising? Srsly? ;-)
- Not only talking about scanned documents
- There is a reason for large hdds…

Reconstructing



Reconstruction

cntd

- How about leased MFDs?
  - Or refurbished hard drives/MFDs sold?

World hasn't change

- At least, regarding printer vulnerabilities
- So, what now?

ERNW
providing security.

Seven Sisters

ERNW
providing security.

Seven Sisters

Access Control

Secure Management

Hardening

Isolation

Encryption

Restriction

Visibility

Access Control

- Secure Passwords
- Don’t forget community strings!

Isolation

- Dedicated MFD/printer/fax VLAN?

ERNW
providing security.

Restriction

- Filter traffic to printer VLAN
- Decide which printing protocol is needed!

Encryption

- Hdd encryption
  - ATA password
- Transport encryption

Hardening

- Disable protocols
- Replace default passwords
- Enable disk wiping/secure delete

Hardening

cntd

- Patch management?
  - CVE-2010-0548
  - CVE-2010-0549
  - CVE-2010-2063
- Web interface access necessary?
  - If not: disable it or use mgmt vlan!

Hardening

cntd

- Disable PXE boot
- Enable deletion of spool files

ERNW
providing security.

Secure Management

- HTTPS
- Mgmt VLAN
- LDAP user authentication

ERNW
providing security.

Visibility

- Print job logging
- LDAP/AD integration

Why isn't it happening?

- Hardening guides exist
  - Even from the manufacturers!
- Align your processes!
- Also think about maintenance access
- Where to store scanned files?

ERNW
providing security.

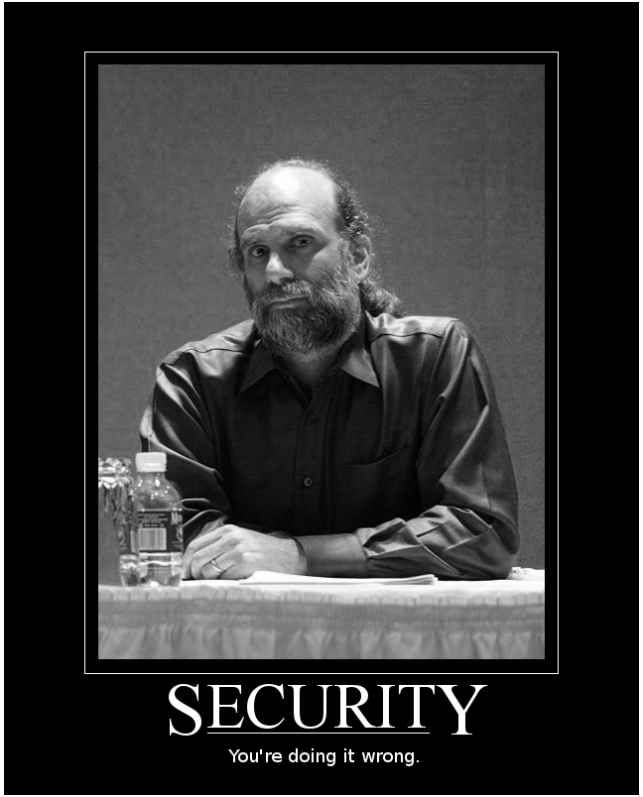
Conclusions

- Most scary: This isn't really new
- Missing awareness
- Think about MFDs as *aggregators of sensitive information*
  - … in your own environment!

ERNW
providing security.

Thank you!

Questions?



ERNW
providing security.

References

- http://www.konicaminolta.co.uk/fileadmin/CONTENT_local/Business_Solutions/Press-Office/White-Papers/Fundamentals-of-Security.pdf
- http://www.hp.com/united-states/business/catalog/nist_checklist.pdf