JULY 22-27, 2017

MANDALAY BAY / LAS VEGAS

#BHUSA / @BLACKHATEVENTS

black hat USA 2017

Exploiting Network Printers

Jens Müller, Vladislav Mladenov,
Juraj Somorovsky, Jörg Schwenk

hgi NDS

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

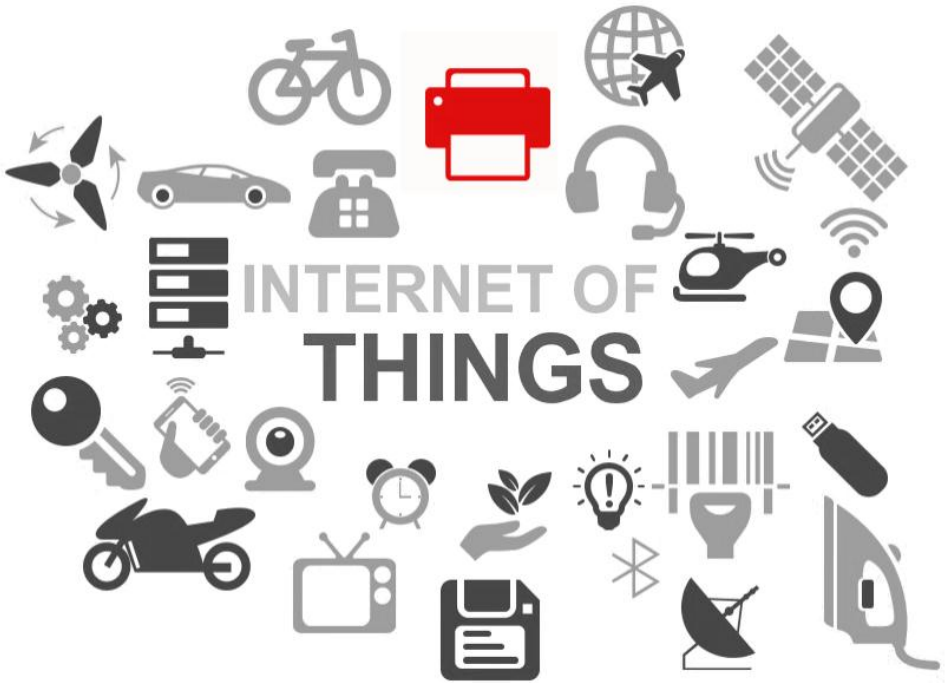
Why printers?

Evolution

1987

2017

Yet another T in the IoT?



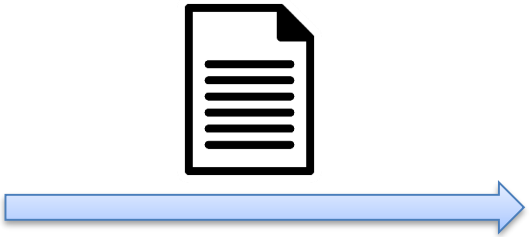
Contributions

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

Overview

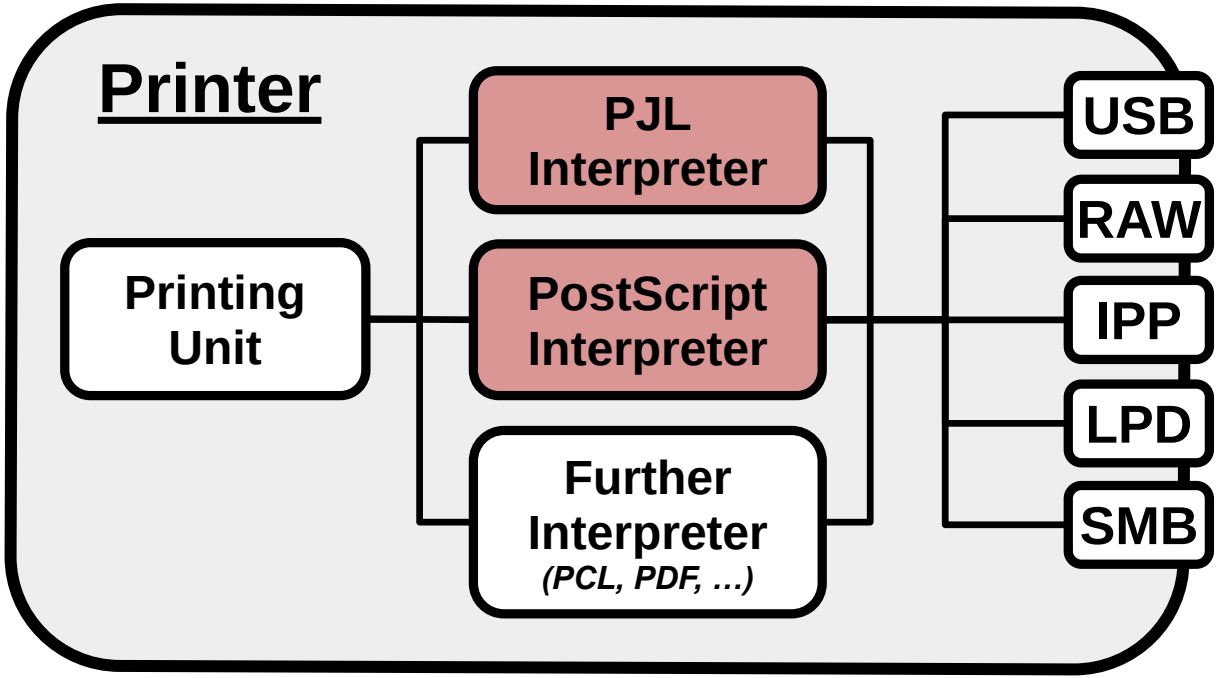
1. **Background**
2. **Attacks**
3. **Evaluation**
4. **PRET**
5. **Beyond printers**
6. **Countermeasures**

How to print?



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

What to attack?



PJL

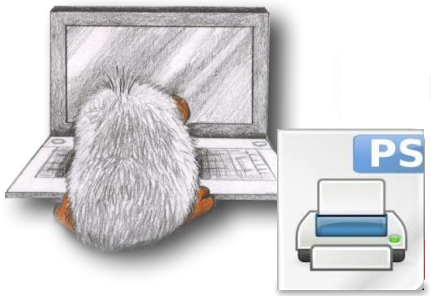
- Printer Job Language
- Manages settings like output tray or paper size

```
@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**

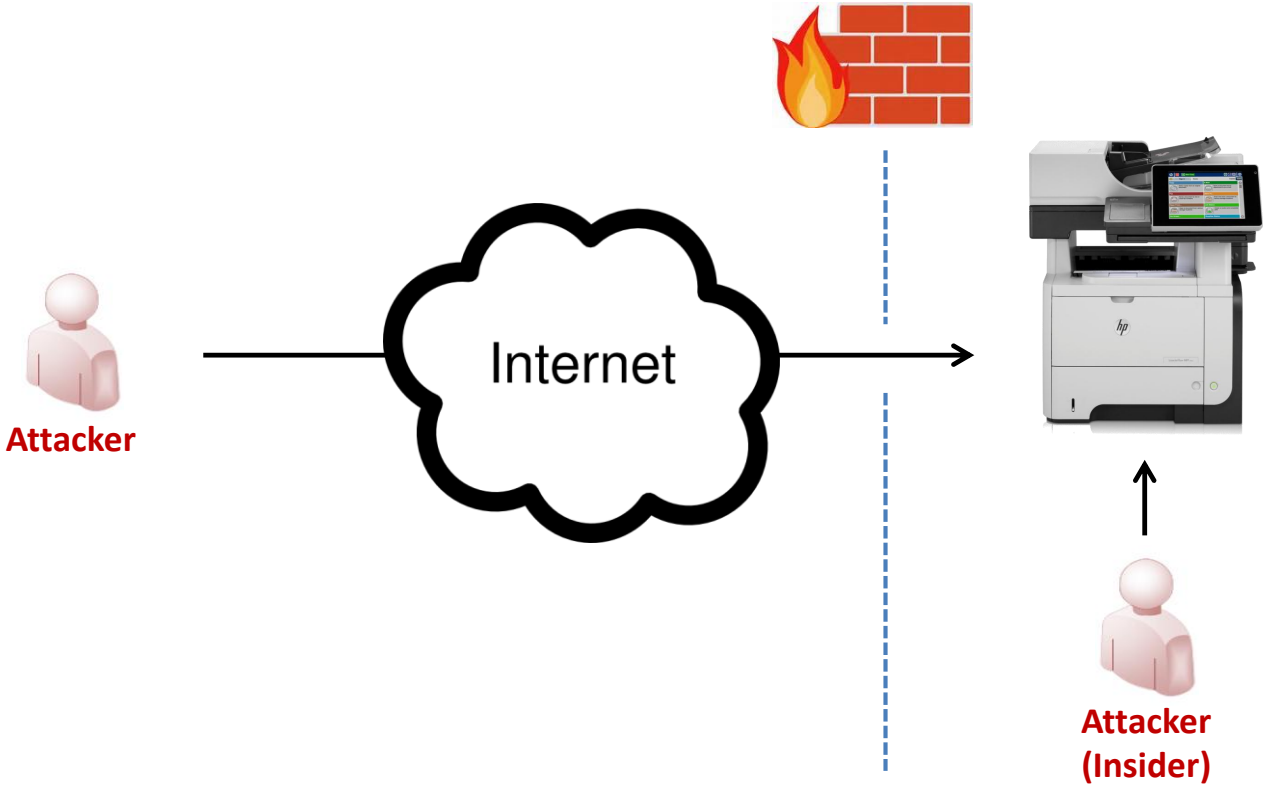
Attacker model: Physical access

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

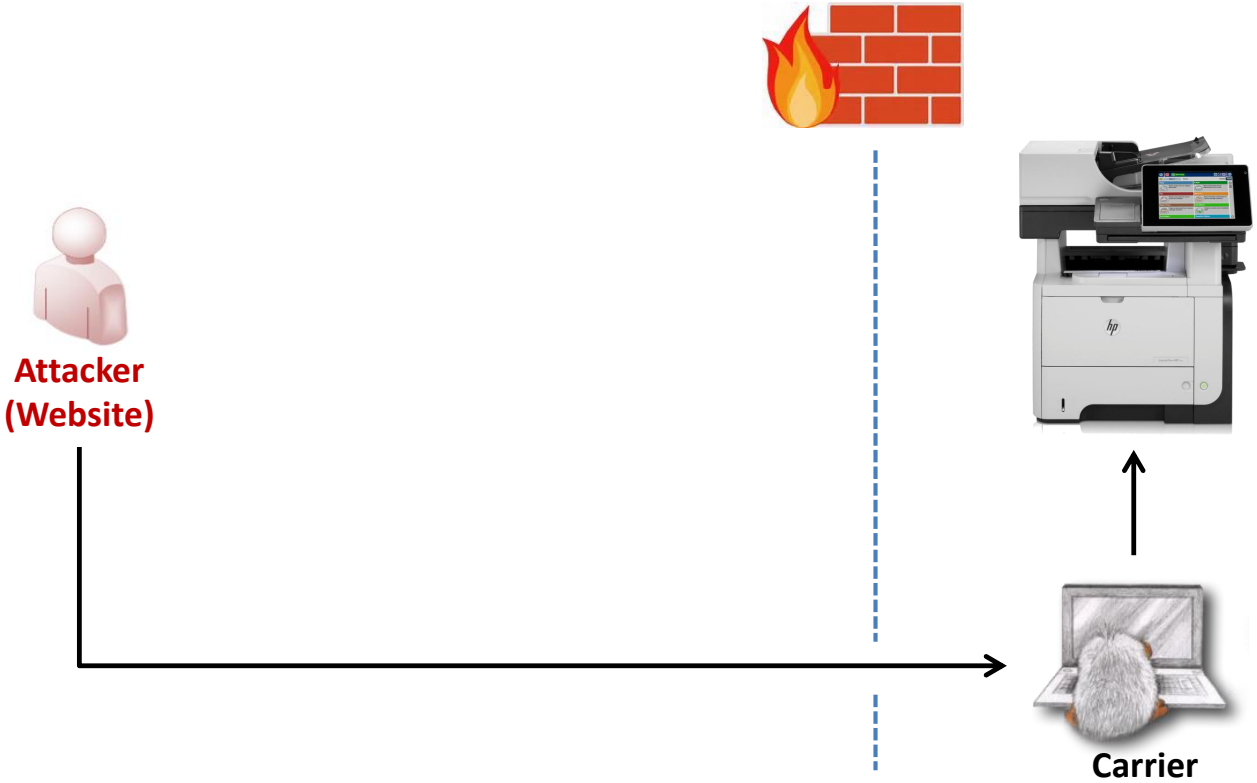
Attacker model: Network access

- Who would connect a printer to the Internet?

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
```

Protection bypass

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

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

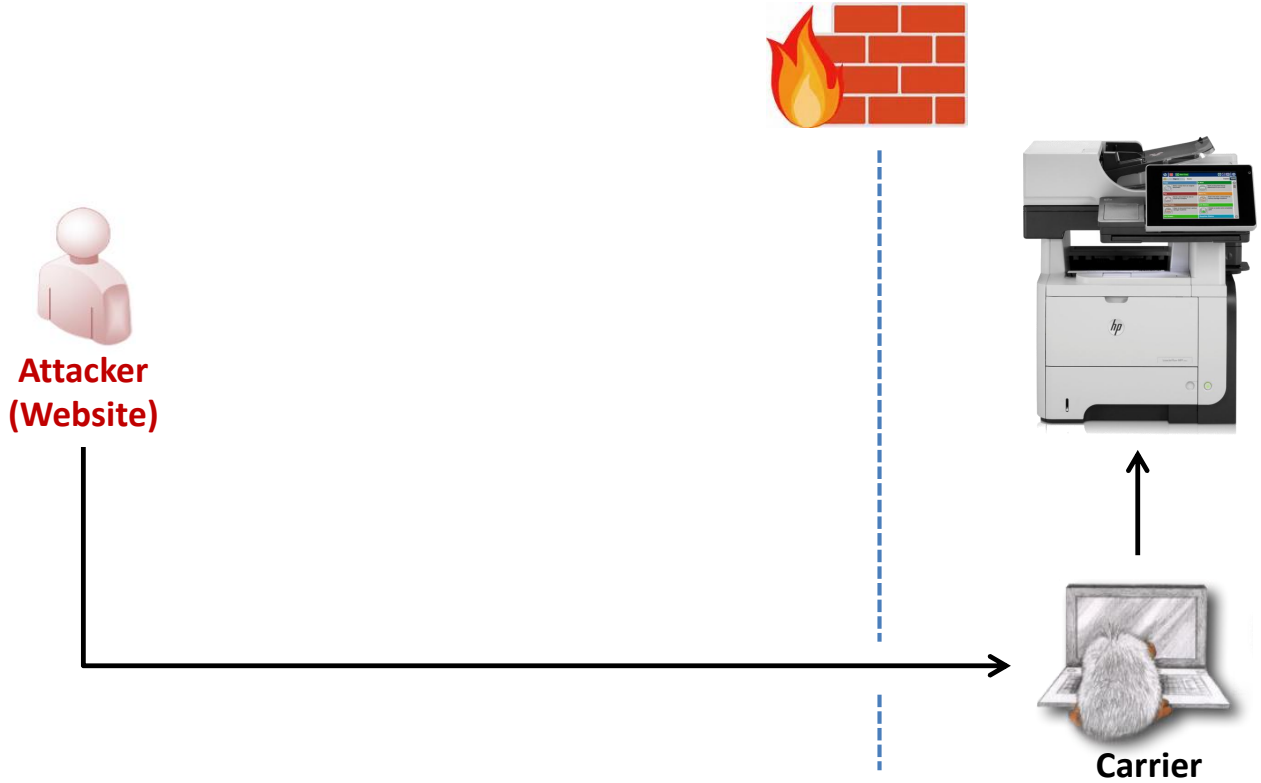
Print job manipulation

- Redefinition of Postscript *showpage* operator

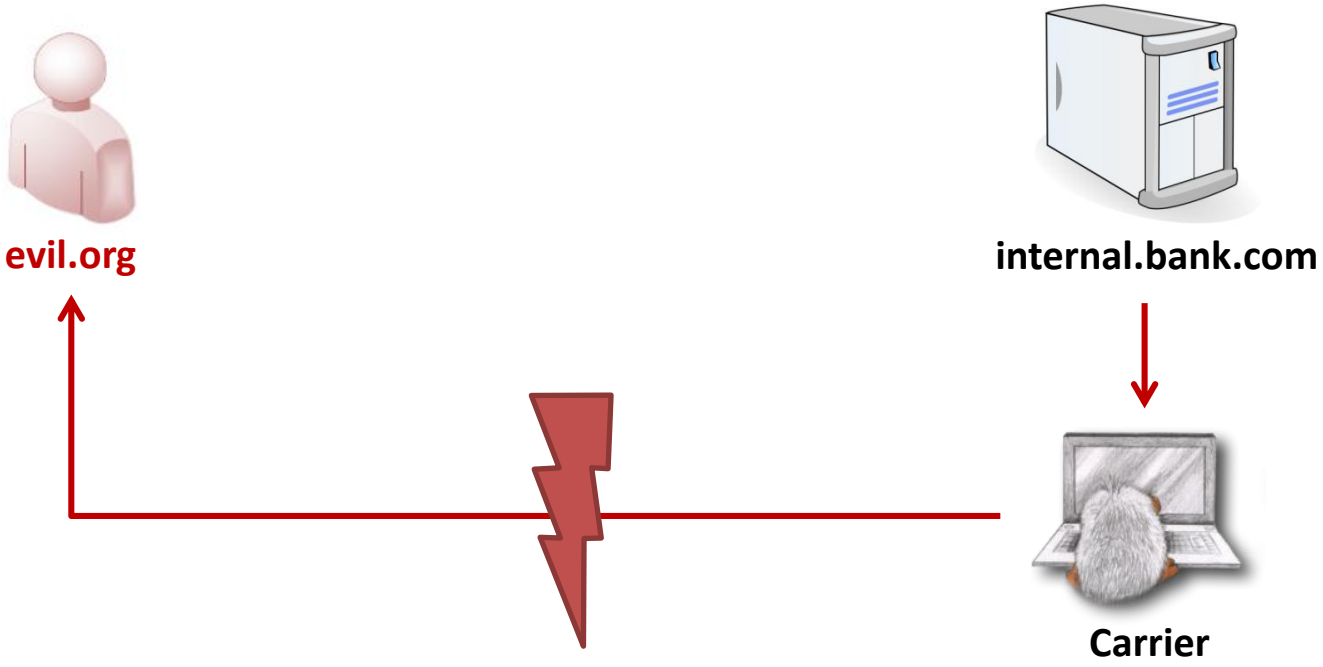
Information disclosure

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

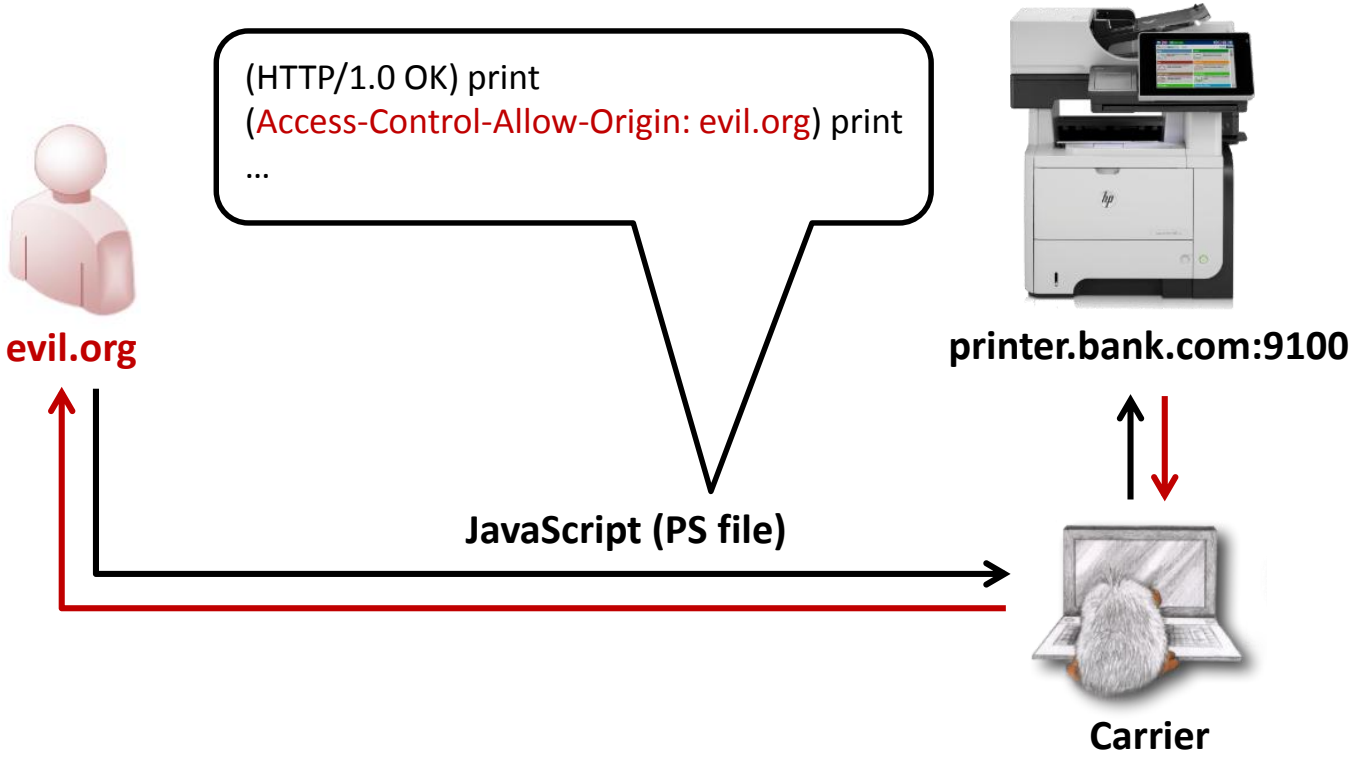
Attacker model: Web attacker



Same-origin policy



CORS spoofing



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 administraators

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	

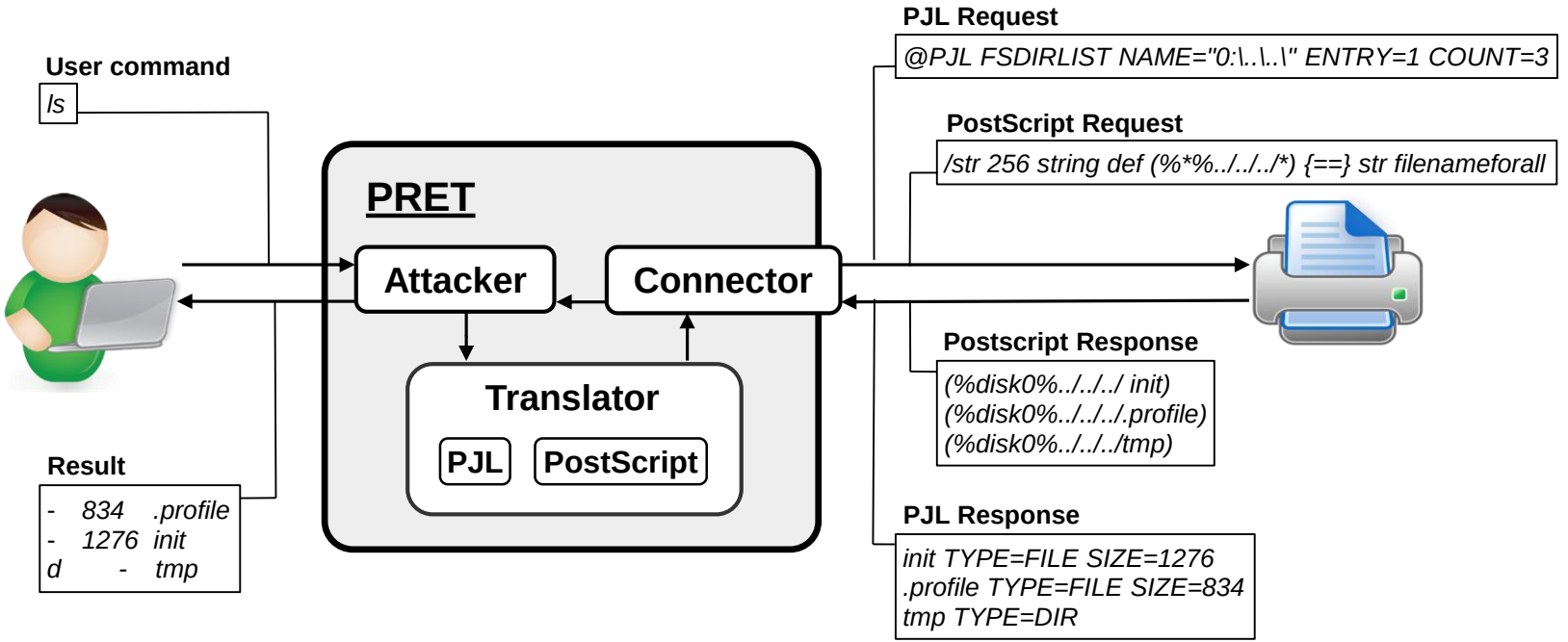
Legend:
- 1 — device vulnerable
- 1* — vulnerability is limited
- (empty) — not vulnerable/PostScript feedback not available
- ? — not tested – physically broken printing functionality
- n/a — no support for PostScript or PJL password protection

Overview

Overview

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

PRinter Exploitation Toolkit (PRET)



PRET commands

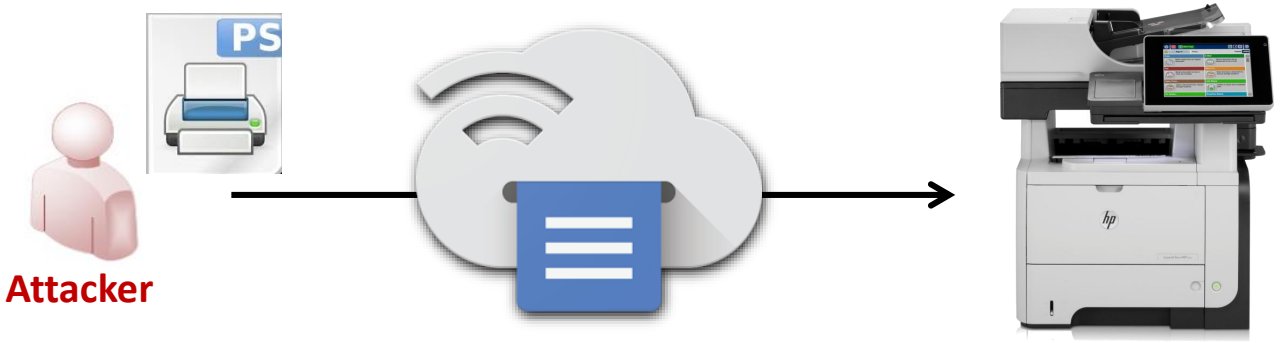
Command	PS	PJL	Description
`ls`	✓	✓	List contents of remote directory.
`get`	✓	✓	Receive file: get <file>
`put`	✓	✓	Send file: put <local file>
`append`	✓	✓	Append to file: append <file> <str>
`delete`	✓	✓	Delete remote file: delete <file>
`rename`	✓		Rename remote file: rename <old> <new>
`find`	✓	✓	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

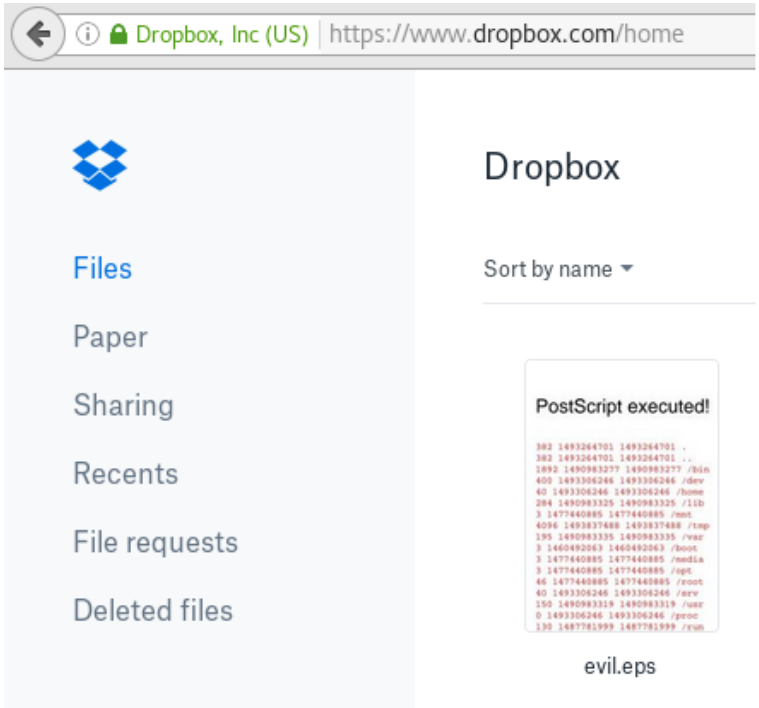
$ 3133.7



Converting PostScript = interpreting PostScript

PostScript in the web?

- PS conversion websites
- Image conversion sites
- Thumbnail preview



Attacks on Cloud Storage

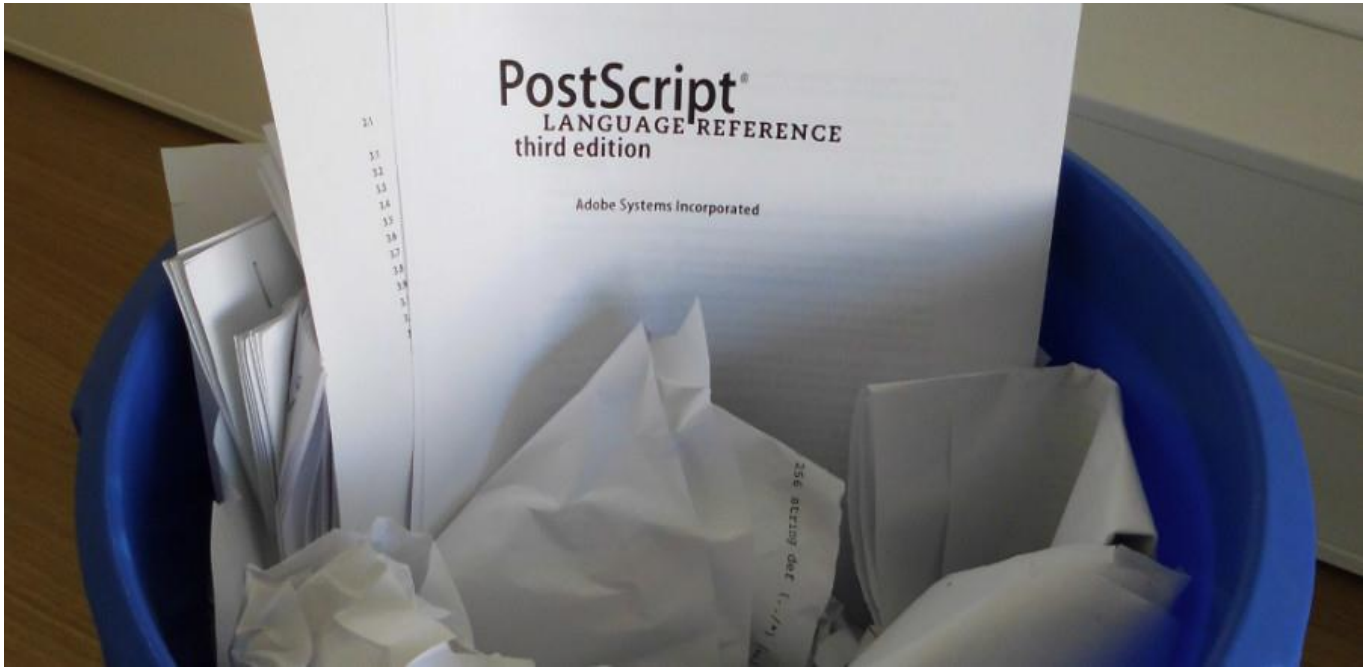
$ 5000

	File system					Environment variables	Command execution
[Dropbox]		read	list	stat		read	
Box.com		(read)	list	stat		read	
[Google Drive]		(read)	(list)	stat			
MS OneDrive		read	list	stat		read	
Yandex Disk		(read)	list	stat		read	
Jumpshare	write	read	list	stat		read	exec
CloudMe		(read)	list	stat			
[CloudConvert]	write	read	list	stat		read	exec

Overview

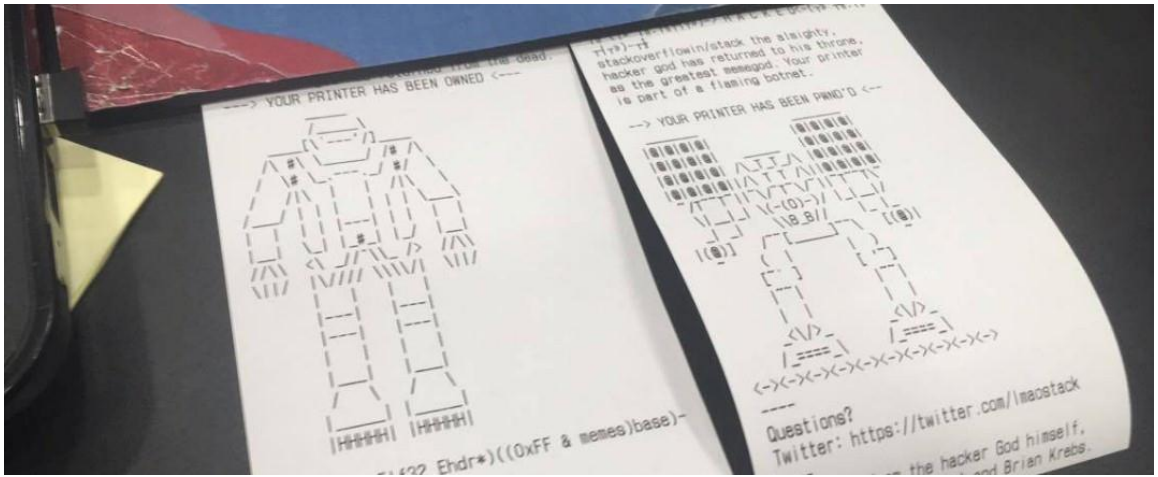
1. **Background**
2. **Attacks**
3. **Evaluation**
4. **PRET**
5. **Beyond printers**
6. **Countermeasures**

Countermeasures



Do not connect printers to the Internet

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



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

Conclusions and future work

- Systematic analysis of network printers and printing standards
- Insecurity of Postscript and PJL
- Attacks applied to different areas
- TODO:
  - Firmware Updates, Fax, 3D printing

Thanks for your attention...

PRET („**Pr**inter **E**xploitation **T**oolkit“)

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

Hacking Printers Wiki

- http://hacking-printers.net/

Questions?