In The Middle of Printers –
The (In)Security of Pull Printing Solutions

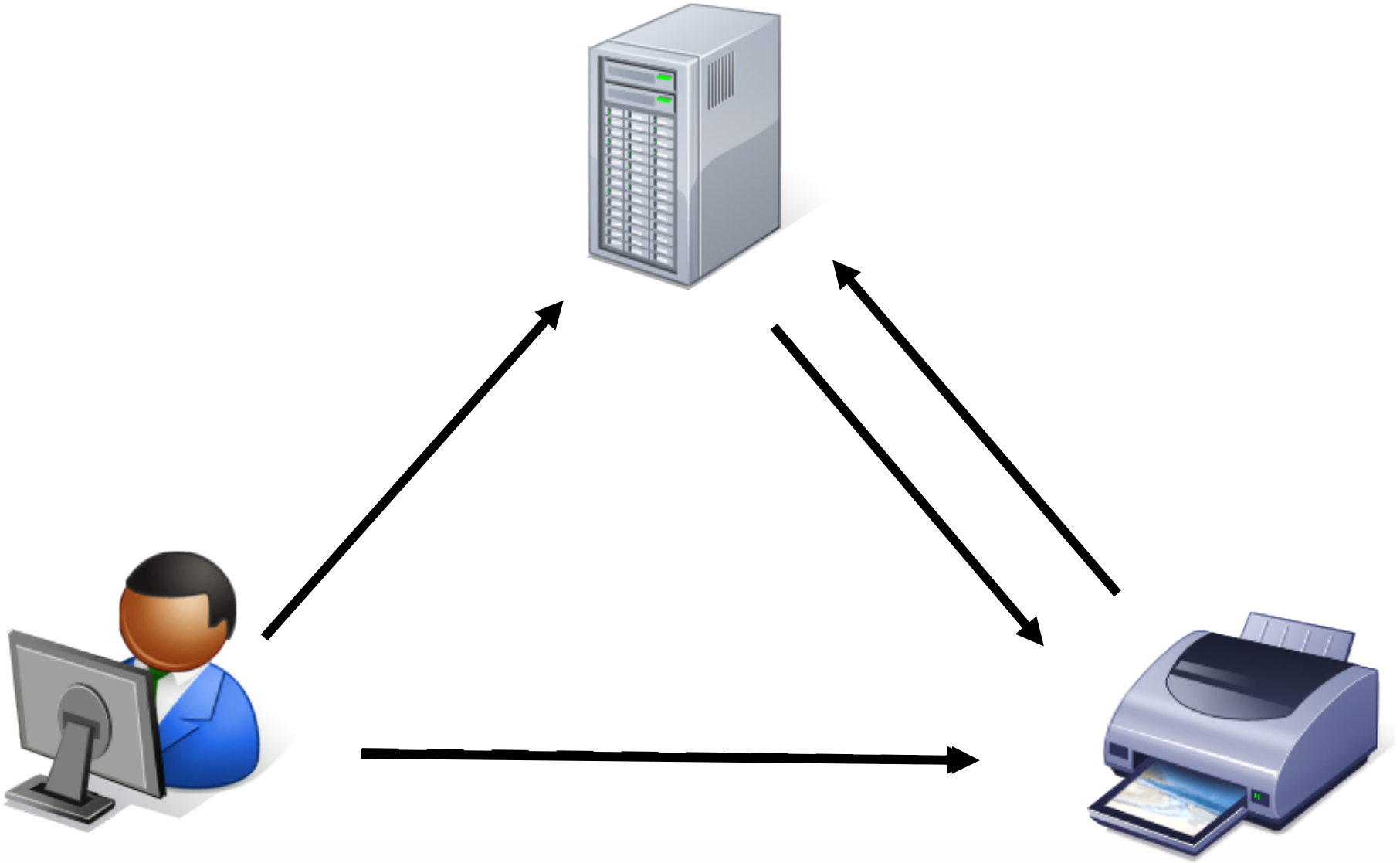
Jakub Kałużny

SecuRing

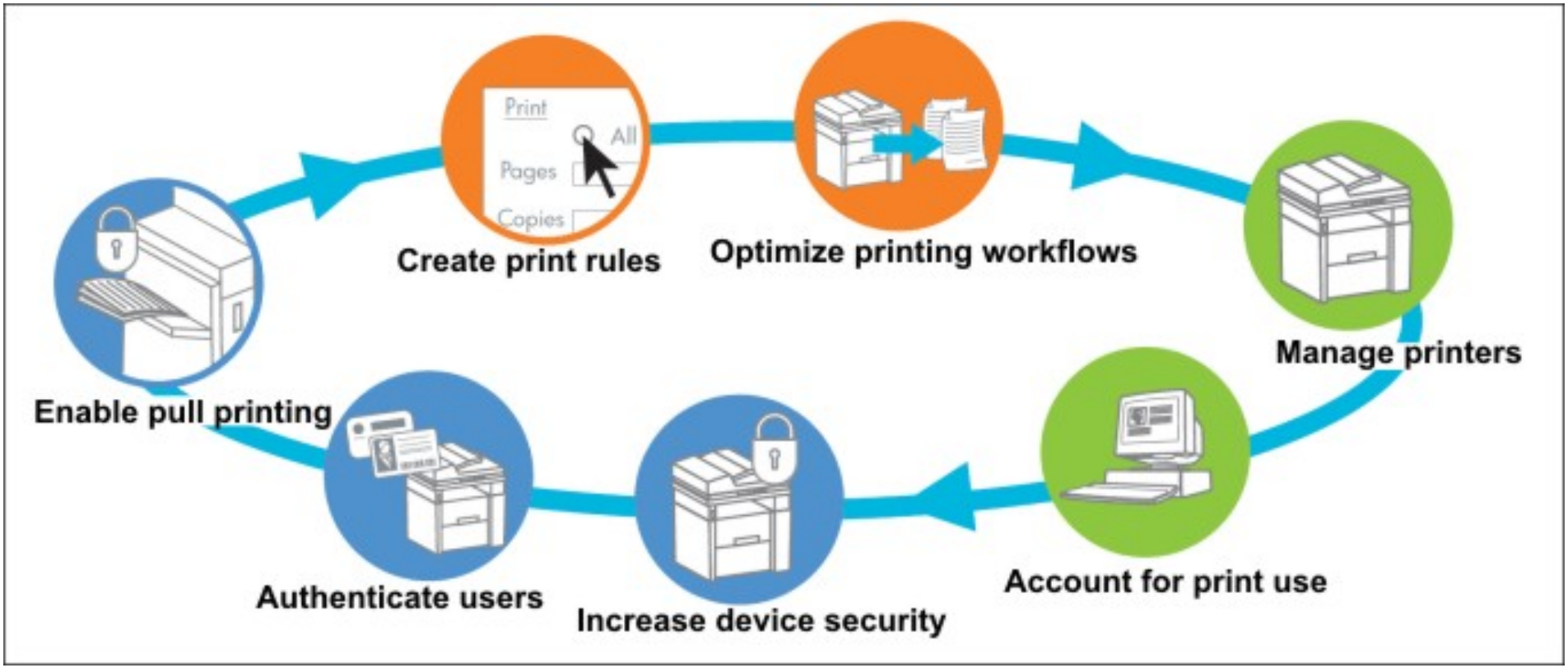
#whoami

- IT Security Consultant at SecuRing
- Consulting all phases of SDLC
- Previously worked for ESA and online money transfers company
- Bug bounty hunter

Pull Printing Solutions



Pull Printing Solutions



https://www.laservalley.com/images/hp_AccessControl.jpg

Why hack pull printing?

- It is cool
- Widely used
- Confidential data
- Getting popular
- Legal conditions

https://www.flickr.com/photos/girlgeek/1877517607

Threat modelling – key risks

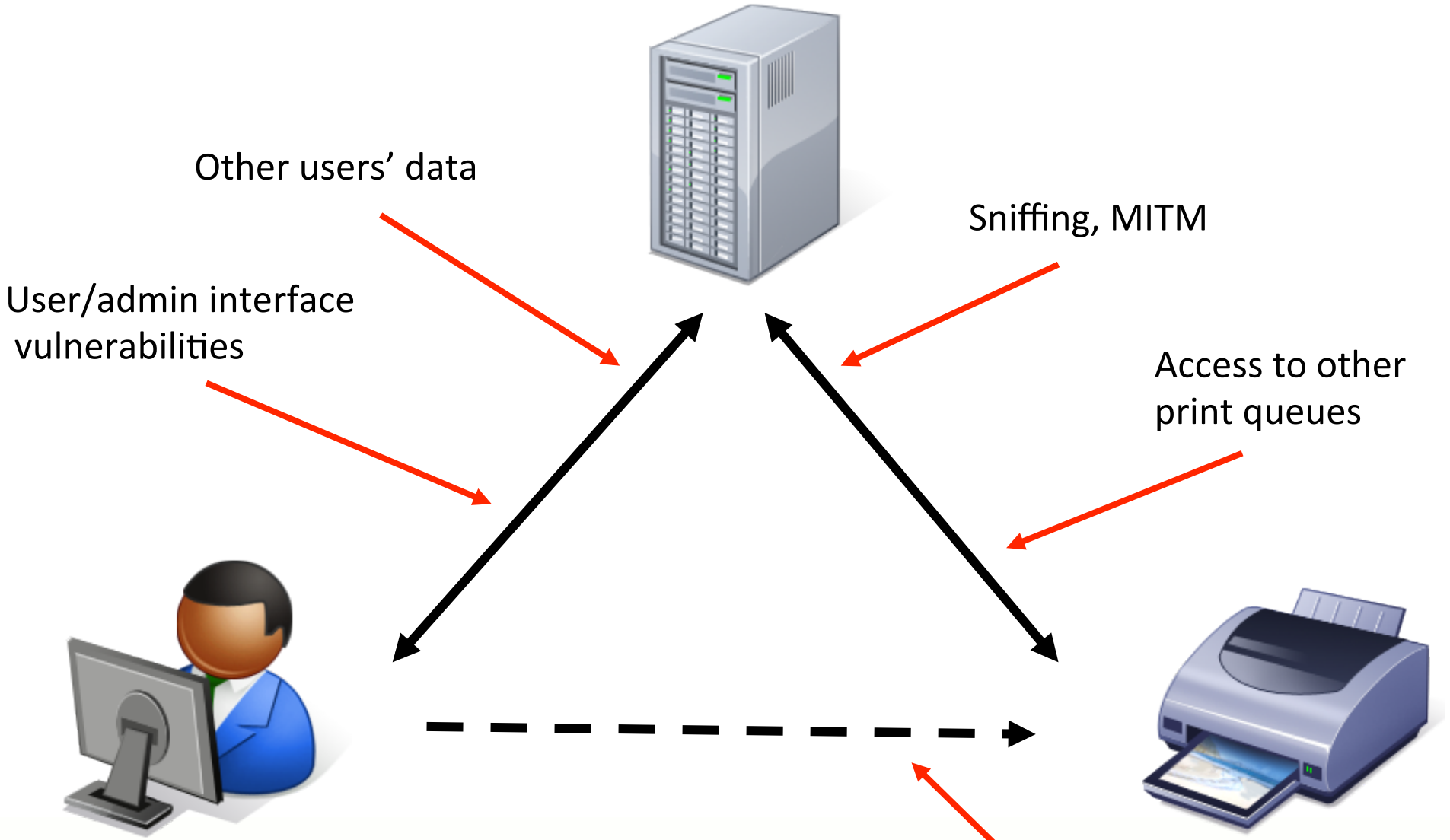
sniffing

print queues

accountability

users' data

Attack vectors

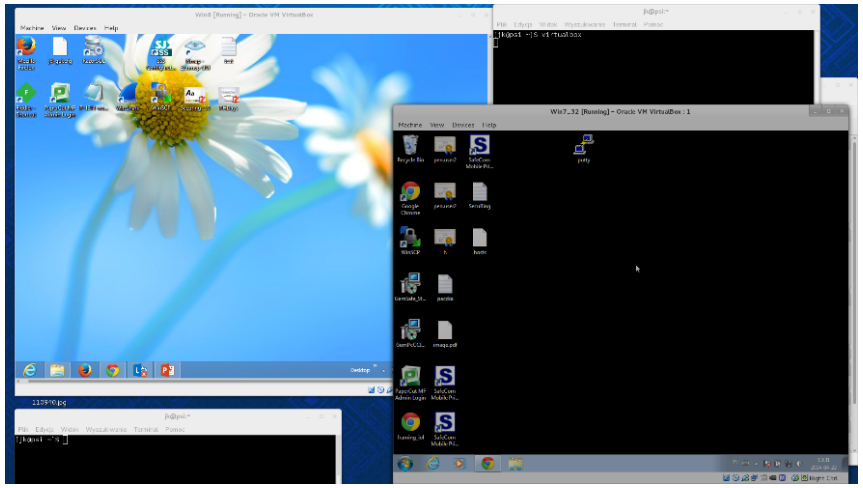


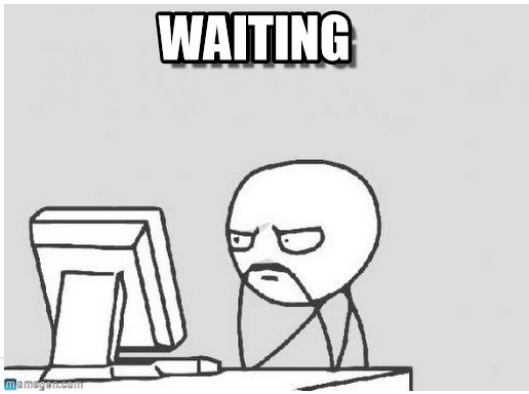
Proprietary network protocols

- You will encounter one
- No docs, specs, tools
- What to do ?
  - decompile the client?
  - search for some tools?
  - watch the raw packets?
- Let’s try!

https://www.flickr.com/photos/canonsnapper/2566562866

What is needed ?





http://www.memegen.com/meme/e4tvwy

Ex 1: Secure Pull Printing

"is a modern printing solution that **safeguards document confidentiality** and unauthorized access to print, scan, copy and e-mail functions. Its user-authentication **provides air-tight security** on your shared MFPs that function as personal printers."

Vendor ensures

„Documents are delivered **only** into the right hands”

„Information is kept **confidential**. **No risk** of being left unattended at the printer”

„Document collection is **safe anytime and anywhere** — no “print and sprint”.”

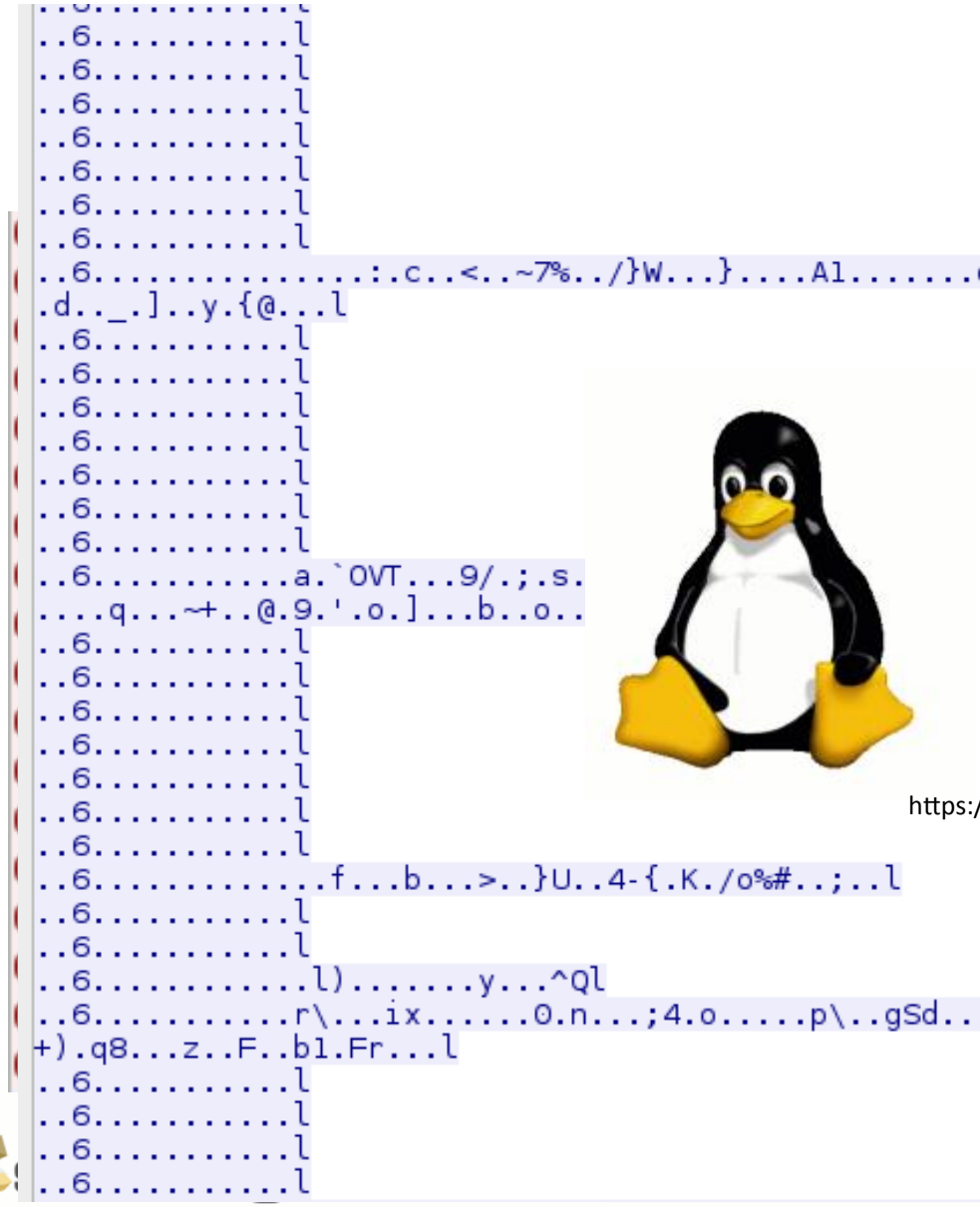
„Integration with other enterprise applications and workflows **is kept secure** through single sign-on”

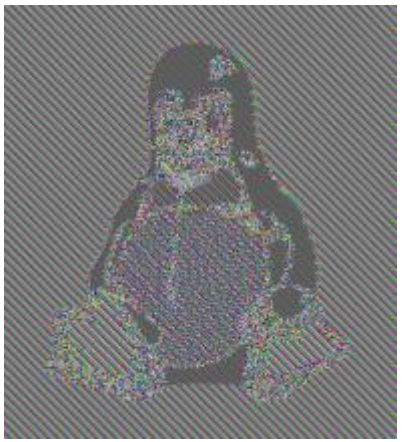
Ex 1: Proprietary protocol

First look on communication

- TCP, 2 ports
- No cleartext, no SSL
- Seems to follow some scheme…

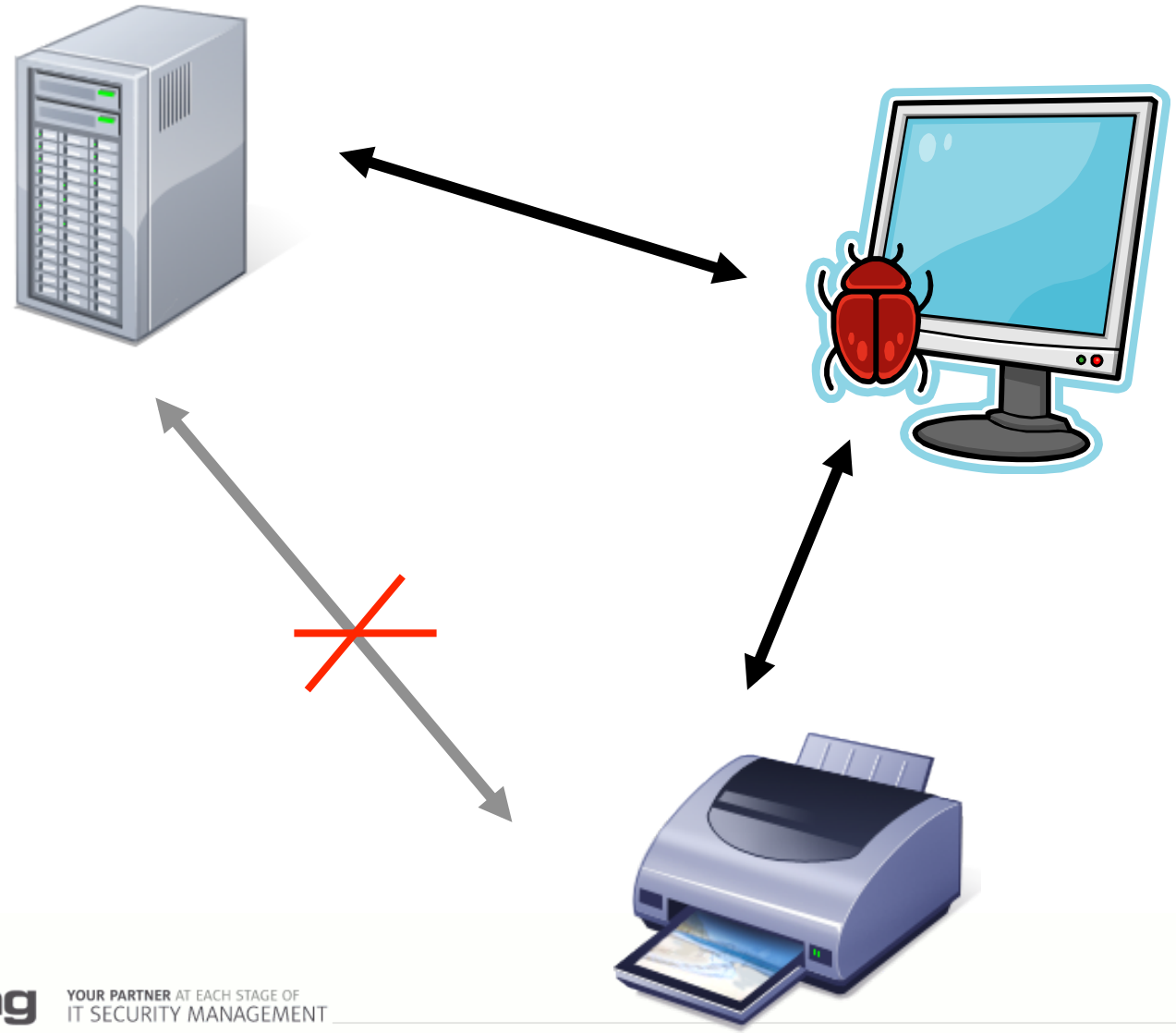
Ex1: Deeper sight on traffic





https://en.wikipedia.org/wiki/ECB_mode

PoC script for MITM



Ex 1: Reverse-engineered

- Hardcoded RSA certificate in printer embedded software
- No trust store!
- AES-128 ECB for symmetric cryptography
- More vulnerabilities inside
- Same protocol in admin interface

Ex 1: Consequences

sniffing

print queues

accountability

users' data

Ex 1: Vendor gets notified

"(…) system has been deployed at many high security customers and **has passed internal audits**."

Ex 2: Responsible vendor

"**Secure print release** (…) can integrate card-swipe user authentication at devices (…) ensuring jobs are **only** printed when the collecting user is present."

Ex2: binary protocol

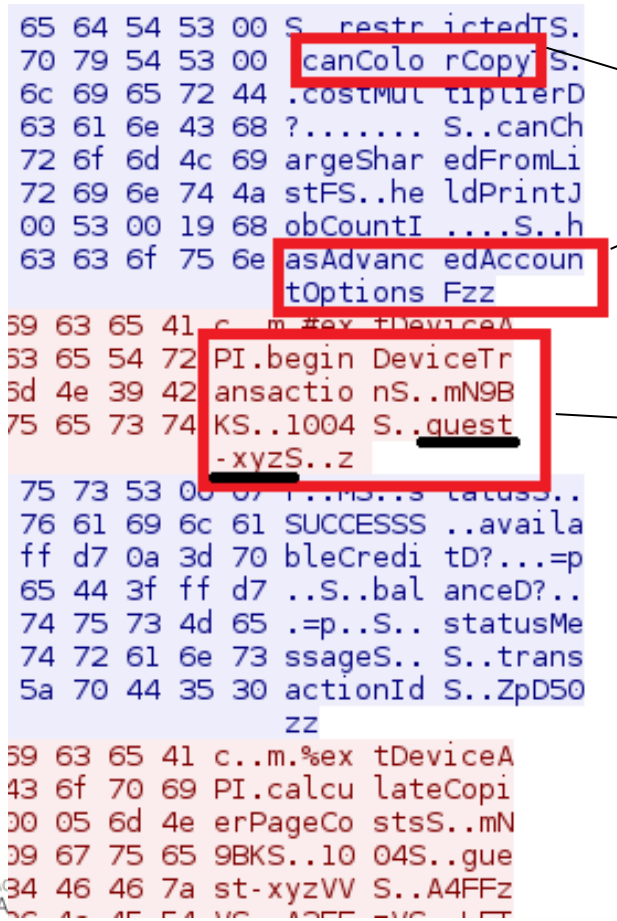
Ex 2: Closer look

SERVER

PRINTER

Release print queue for user "guest-xyz"

Charge user "guest-xyz" for using 1000 pages



User permissions

beginDeviceTransaction

(…) guest-xyz

guest-abc

Ex 2: Consequences

sniffing

print queues

accountability

users' data

Ex 2: Vendor gets notified

- KB access and support service
- And all versions of software

- Responded in few hours and patched in few days
- Was happy to be pentested

Ex 3: Secure Print Solutions

"The Secure Print technology offers:

High Security - Jobs only print when released by the user"

Ex 3: Architecture design

- Network level protection
- IP whitelist
- Stateless HTTP service, no session token, no cookie

Ex 3: Authentication request

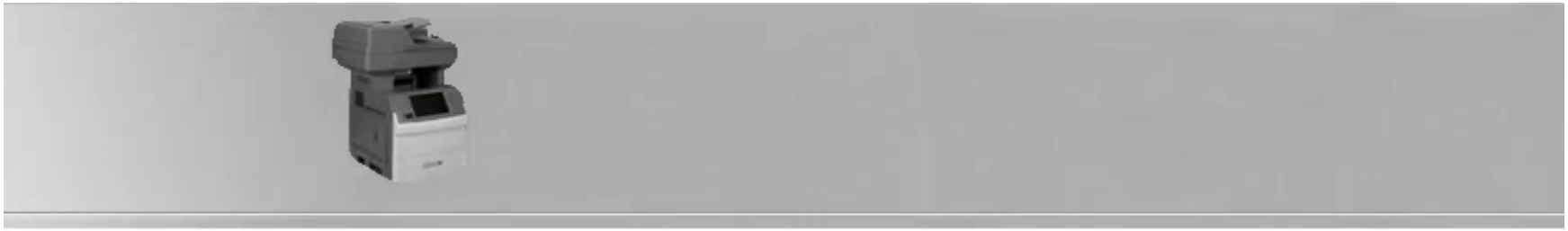
SERVER

```
POST /AuthenticateLogin2 HTTP/1.1
(...)

param1=username&param2=password
```

PRINTER

Ex 3: Hacking without any tools



Ex 3: Tampering accountability

SERVER

Just printed a job, note it and charge

PRINTER

```
POST /LogJob HTTP/1.1
(…)
data=<job><job-id>1073741847</job-
id><name>_Print_____1073741847</name><type>103</
type><type-string>Print</type-string><page-cnt>0</
page-cnt><color-page-cnt>0</color-page-cnt><color>0</
color><duplex>0</duplex><page-size>0</page-size><page-
size-string>Unknown_Size</page-size-
string><media>Unknown</media><dest>UNKNOWN</dest>
<user-name>USER1</user-name><email-
address>unknown@unknown.com</email-address></job>
```

Ex 3: Consequences

sniffing

print queues

accountability

users' data

Ex 3: Vendor gets notified

Received, and will look it over with engineers. I'll come back to you shortly.

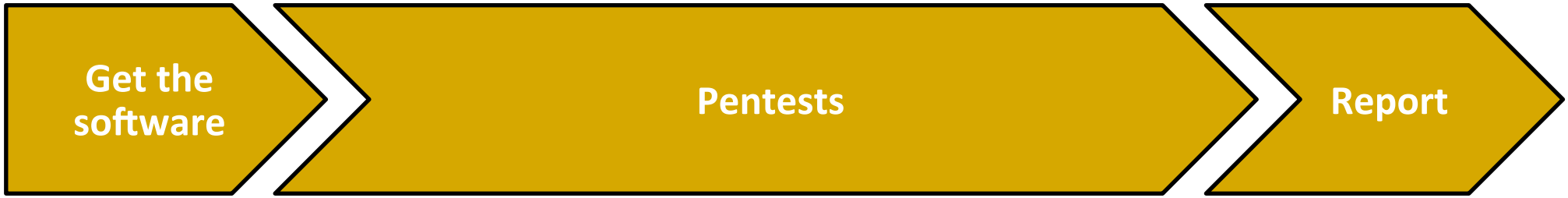
Discussed with engineers, and the reason why communication was non-SSL, was to support older Lexmark devices which cannot do SSL.

Other vulnerabilities

- Logs and printed files on a default web server
- Brute-force attack in admin/user interfaces, no logs
- XSS and CSRF in web interfaces
- Predictable session identifiers
- DoS attack vulnerability

Research process

What we thought

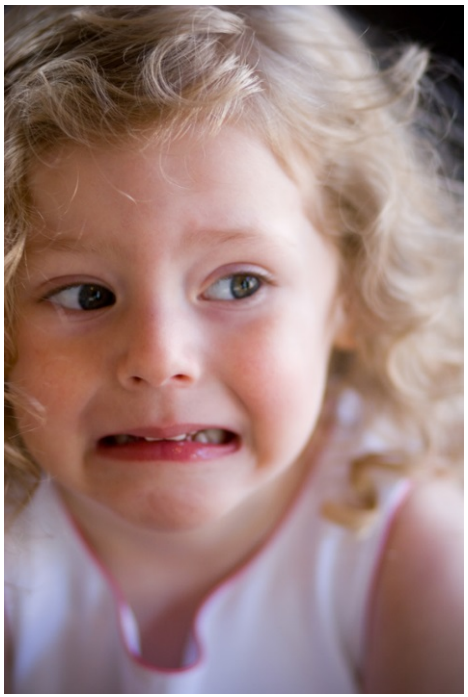


How does it really look like

Research problems

Why do vendors fear pentests?

- no direct profit
- risk of finding criticals
- implies a lot of patching



Cheat sheet - owners

While deploying a pull printing solution:

- Get it pentested
- Network layer security - IPsec, VLANs
- Verify vendor claims, ask for their SDLC, how do they handle vulnerabilities

Cheat sheet - developers

Encryption between server and printer/user:

- Avoid writing your own crypto
- Use known standards
- Authenticate both side

Cheat sheet - developers

Behind the proprietary protocol:

- Access control
- Separate interfaces
- MITM protection is not enough

Cheat sheet - testers

Look for vulnerabilities in:

- Encryption, trust stores, cipher suites
- Access control in proprietary protocols
- Infrastructure design

What's next ?

- CVEs disclosure
- A follow-up paper
- Ready to fight new proprietary protocols

Q & A

http://www.securing.pl
e-mail: info@securing.pl
tel. +48 (12) 4252575

Jakub Kałużny
jakub.kaluzny@securing.pl

CC license credits

https://www.flickr.com/photos/bru/2967030367
https://www.flickr.com/photos/calliope/1816120150
https://www.flickr.com/photos/liewcf/449611278
https://www.flickr.com/photos/mava/3111719841
https://www.flickr.com/photos/siradavis/2148761728
https://www.flickr.com/photos/acaben/18403502
https://www.flickr.com/photos/elevateprinting/3123470876
https://www.flickr.com/photos/wmjas/2378330389
https://www.flickr.com/photos/oskay/472097903
https://www.flickr.com/photos/fsse-info/3093021726/in/photolist-aFngAa-9PUjEk-fUJCjP-cwh2TC-cwh2oU-9Lag1z-9RByGf-8FDcLH-dvodj3-aWRC4R-dvoaPG-dvhyKF-bjzH5u-65zwkN-aWRDGc-5JYnU6-dnDDuL-bueg2C-DCHxv-5WapqT-fcuDBM-5T7QW3-7Pbpsw-6LFtWE-dj1hmz-iZBc-97WJJo-4VUGyN-dj1g2A-eazhzq-mXsEkZ-dnDyEB-8T3kyS-6tT6Na-orB7V-6mMWku-dvhC7a-4CayLn-5HjxKd-HHCg2-FJkDk-5HjxAN-kcAVp4-k5nj3Z-7JgVcV-kvhRaR-fRYLeC-ex2mmw-ewYafe-ewYa6M