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
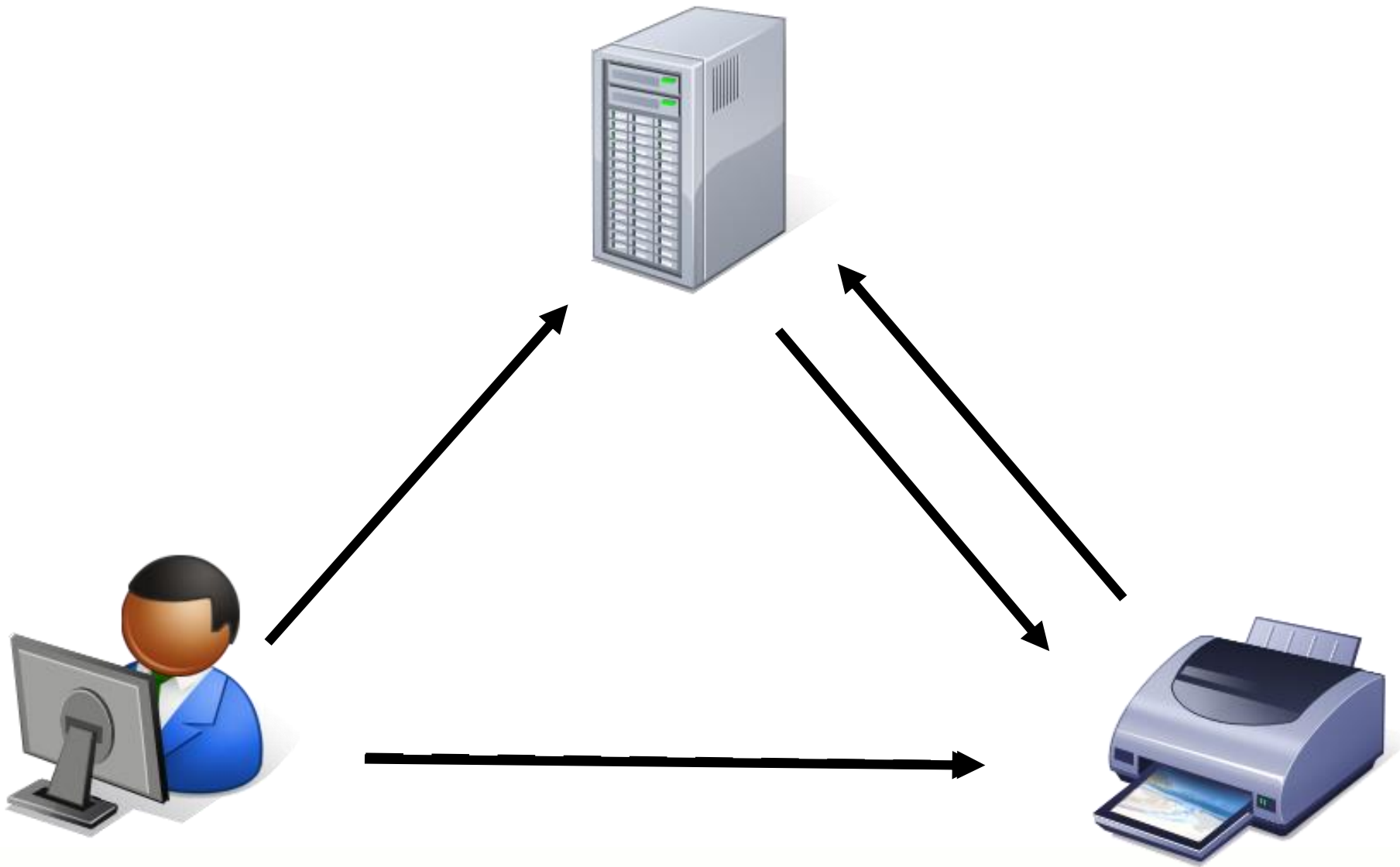
Pull Printing Solutions
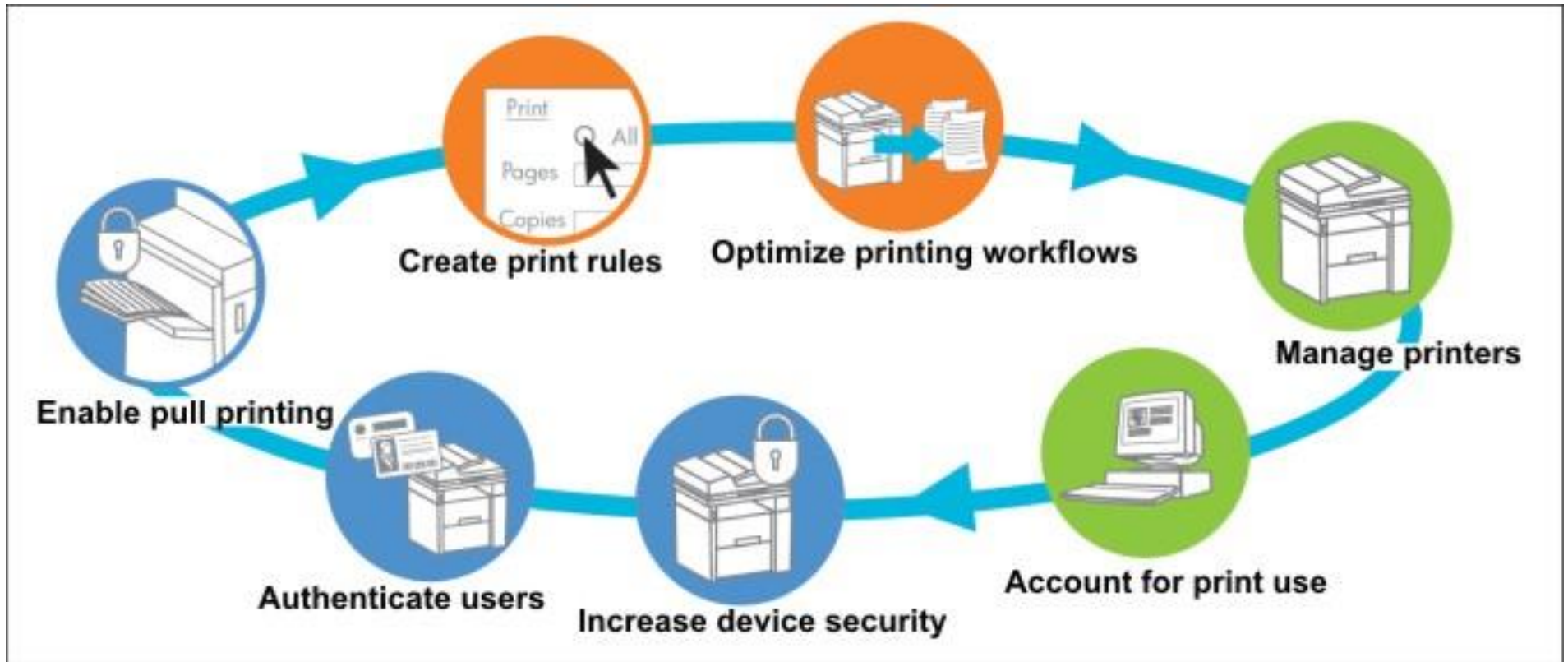
https://www.laservalley.com/images/hp_AccessControl.jpg

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

Other users' data

User/admin interface vulnerabilities

Sniffing, MITM

Access to other print queues

Authorization bypass

SecuRing   YOUR PARTNER AT EACH STAGE OF IT SECURITY MANAGEMENT
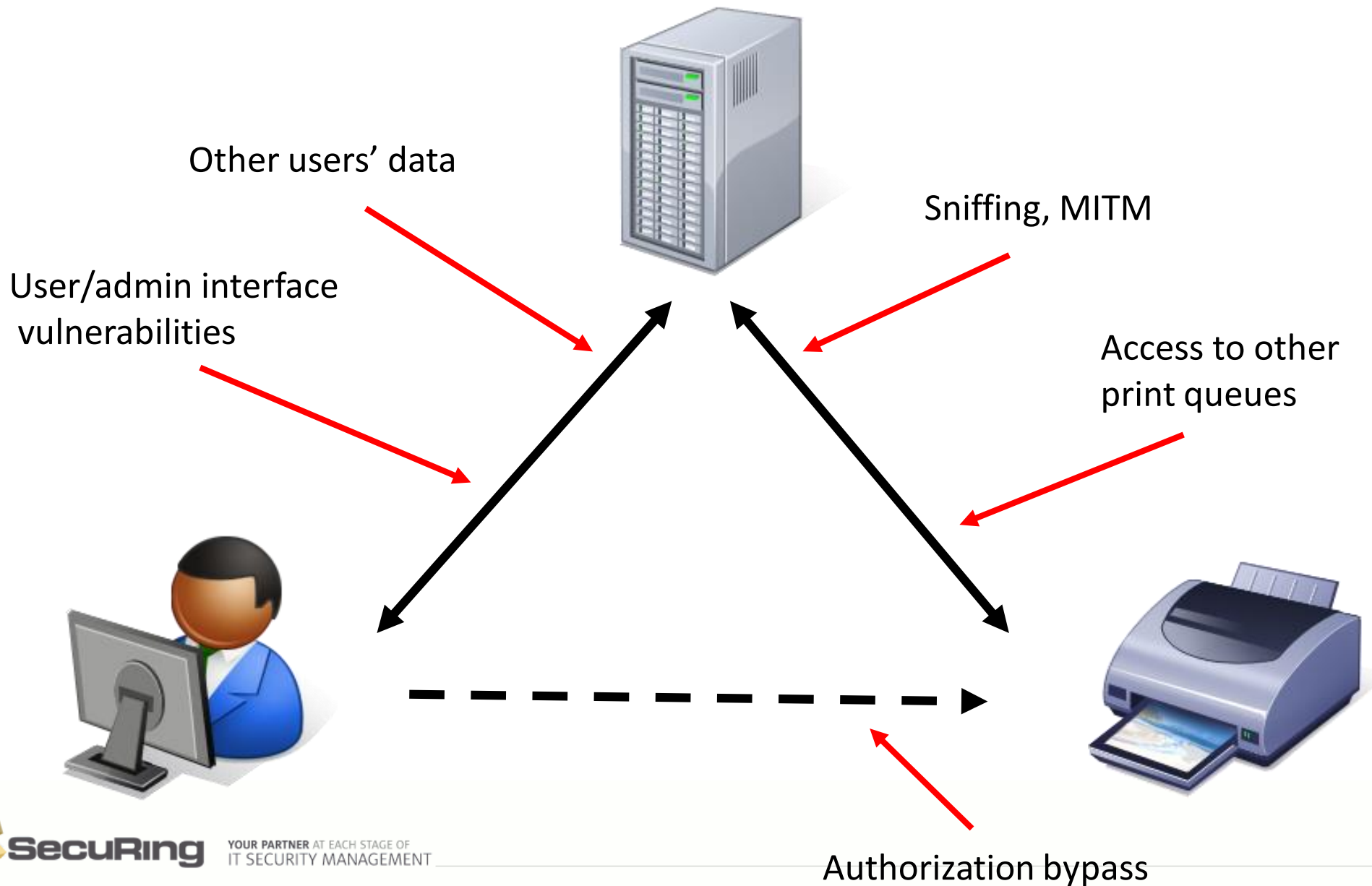
Proprietary network protocols

- 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!

SecuRing YOUR PARTNER AT EACH STAGE OF IT SECURITY MANAGEMENT

What is needed ?

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

```
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6.................:.c..<..~7%../}W...}....A1.......dh{hR9....
.d.._.]..y.{@...l
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6...........a.`OVT...9/.;.s.
....q...~+..@.9.'.o.]...b..o..
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6...........l
..6.............f...b...>..}U..4-{.K./o%#..;..l
..6...........l
..6...........l
..6..............l).......y...^Ql
..6............r\...ix......0.n...;4.o.....p\..gSd............qg........
+).q8...z..F..bl.Fr...l
..6...........l
..6...........l
..6...........l
..6...........l
```

https://en.wikipedia.org/wiki/ECB_mode
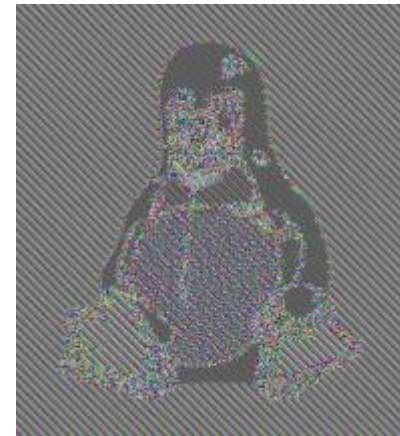
PoC script for MITM

Ex 1: Reverse-engineered

- Hardcoded RSA certificate in printer embedded software
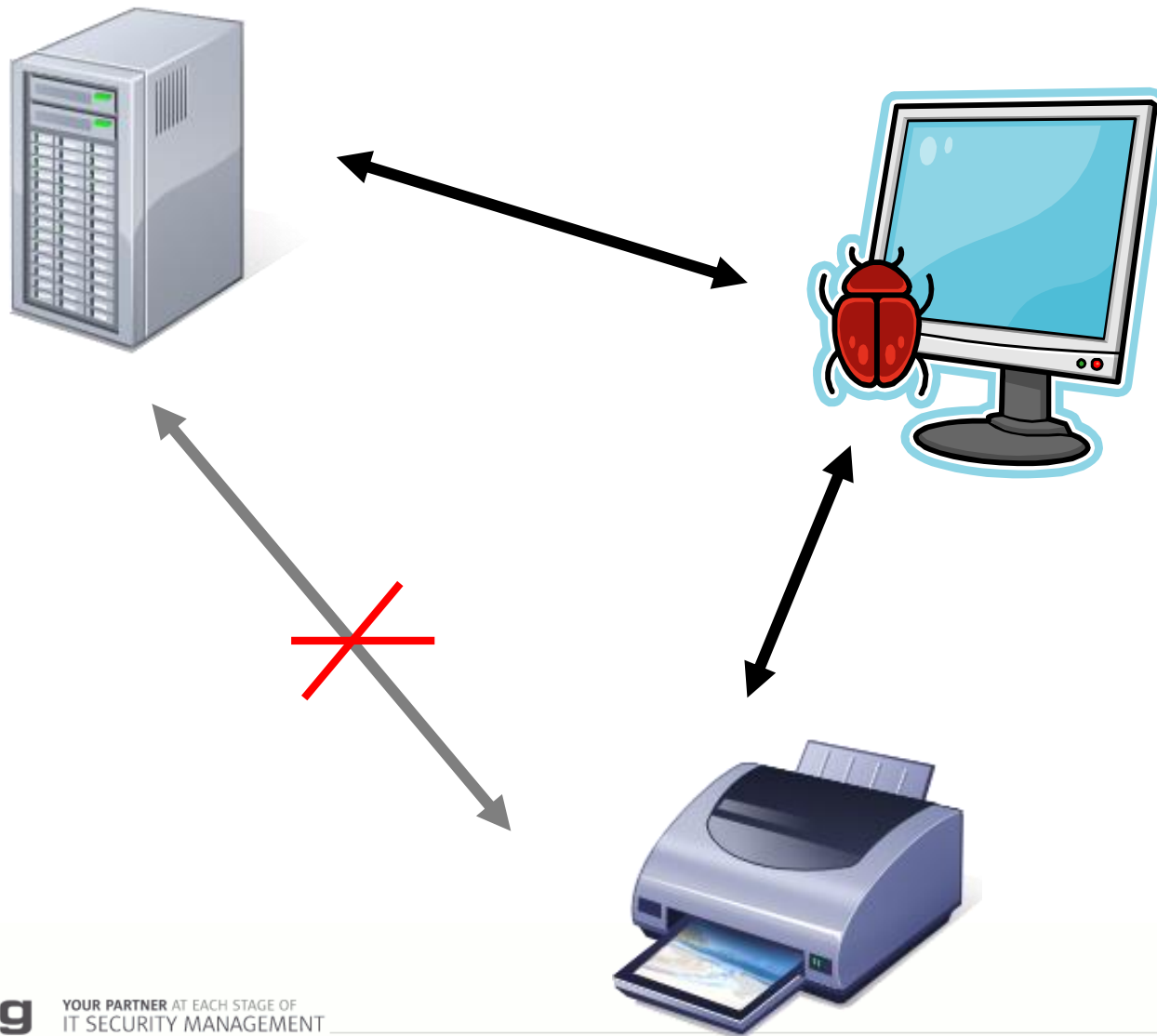
- No trust store!

- 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

SERVER → HELLO → PRINTER

PRINTER → USER: user1 → SERVER

SERVER → token → PRINTER

PRINTER → HASH(password + token) → SERVER

SERVER → Password ok → PRINTER

PRINTER → Release my print queue → SERVER

PRINTER → Just copied 100 pages → SERVER

SERVER → OK → PRINTER

Ex 2: Closer look

SERVER

PRINTER

Release print queue for user "guest-xyz"

Charge user "guest-xyz" for copying 100 pages

```
65 64 54 53 00   S_ restr ictedTS.
70 79 54 53 00   canColo rCopyTS.
6c 69 65 72 44   .costMul tiplierD
63 61 6e 43 68   ?....... S..canCh
72 6f 6d 4c 69   argeShar edFromLi
72 69 6e 74 4a   stFS..he ldPrintJ
00 53 00 19 68   obCountI ....S..h
63 63 6f 75 6e   asAdvanc edAccoun
                 tOptions Fzz
69 63 65 41      c..m.#ex tDeviceA
63 65 54 72      PI.begin DeviceTr
6d 4e 39 42      ansactio nS..mN9B
75 65 73 74      KS..1004 S..guest
                 -xyzS..z
75 73 53 00 07   T..MS..s tatusS..
76 61 69 6c 61   SUCCESSS ..availa
ff d7 0a 3d 70   bleCredi tD?...=p
65 44 3f ff d7   ..S..bal anceD?..
74 75 73 4d 65   .=p..S.. statusMe
74 72 61 6e 73   ssageS.. S..trans
5a 70 44 35 30   actionId S..ZpD50
                 zz
69 63 65 41      c..m.%ex tDeviceA
43 6f 70 69      PI.calcu lateCopi
00 05 6d 4e      erPageCo stsS..mN
09 67 75 65      9BKS..10 04S..gue
34 46 46 7a      st-xyzVV S..A4FFz
```

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

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

`param1=username&param2=`**password**

SERVER

PRINTER

Ex 3: Hacking without any tools

Ex 3: Tampering accountability

Just printed a job, note it and charge

SERVER

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.
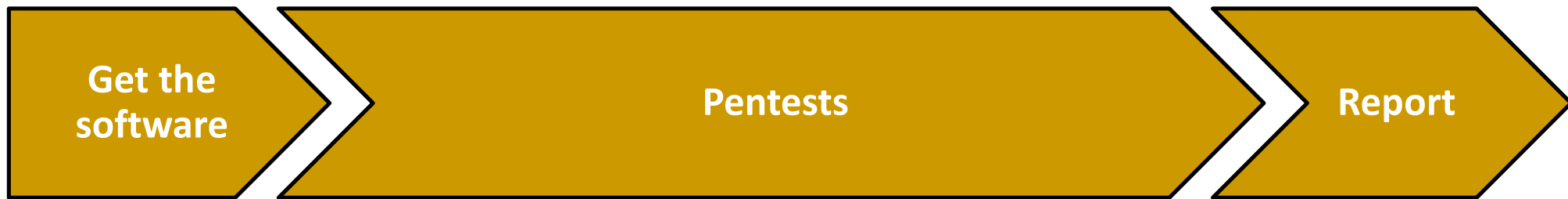
Other vulnerabilities

- 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

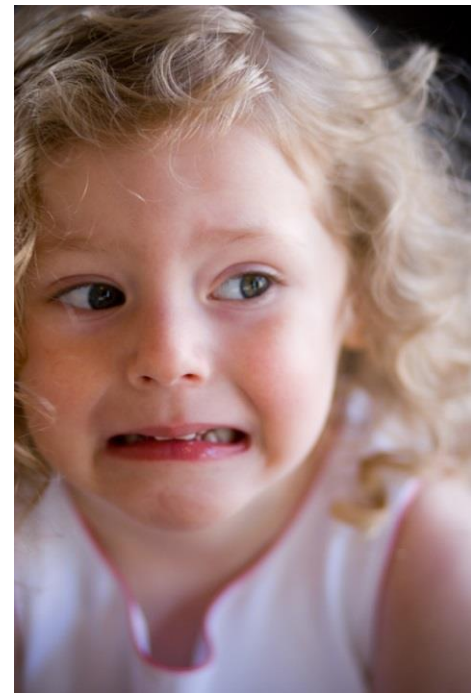- DoS attack vulnerability

Research process

What we thought

Get the software	Pentests	Report

How does it really look like

Get the software	Pentests	Report vulnerabilities

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

SecuRing

SecuRing YOUR PARTNER AT EACH STAGE OF
IT SECURITY MANAGEMENT

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