



# PRINTER “SECURITY” AUDIT: THE UNIVERSITY OF VIRGINIA

Kevin Savoy, CPA, CISA, CISSP   Brian Daniels, CISA, GCFA

# Who cares about network printers?

- Why should anybody care about securing the printers when there are:
  - ▣ Firewalls
  - ▣ Routers
  - ▣ Fancy (expensive) network protection devices in place?
- Can Printers really provide a serious risk to the Agency/University/Company?
- Printers don't even have enough capability to provide a serious risk, do they?

# Printers have come a long way...

- Printer capabilities have grown even as relative costs have shrunk.



- Multi-Function Printers are cheaper than ever.

# Multi-Function Printers

- Common Multi-Function Printers can perform all or most of the following tasks
  - Digital Sending to Email
  - Digital Sending to Network Folder
  - Fax
  - Print
  - Copy
  - Staple/ Stack
  - Chops Vegetables\*

\*Not Really

# Our Audit Objectives

- Verification that the networked printer environment was reasonably secure through a review of:
  - ▣ Policies and procedures governing the security of networked printers
  - ▣ Remote administration web console for each networked printer selected for the audit
  - ▣ Results of a network-based vulnerability scan performed for the audit.

# Our Sample and Scope

- 20 printers were selected for our review
  - ▣ Total of 10 departments
    - 5 in the University environment
    - 5 in the Health System environment.
  
- Judgmentally selected the departments
  - ▣ based on risk
  - ▣ also to cover different types of functional areas (educational, administrative, support, etc.)

# Audit Results

- ❑ Overall, security in place for the networked printers was severely lacking
- ❑ Significant changes needed to be made for networked printers at both the University and Health System.
- ❑ Note: not all printers are deployed with equal risk
- ❑ Specific Issues Identified are noted in the following pages

# Policies/ Procedures/ Standards

- No overarching detailed standards or procedures or guidelines related to networked printers
  - University
  - Health System
- Some generic references to print servers and generic network devices

# Web Interface Password Missing or Default

- Only requirement to access web console is type the IP address in a web browser.
  - ▣ “Feature” of modern printers to enable remote management
- University – publically routable IP addresses
  - ▣ Can be accessed inside or outside the network
- Health System – non-publically routable IP addresses
  - ▣ Only accessible from inside the network but thousands of machines inside the network.

# Web Interface Password Missing or Default

- ❑ Actual weakness - allows outsiders to adjust the printer's configuration settings with default/no admin password set
- ❑ Configs can be modified to allow protocols such as FTP or Telnet to be enabled for future attacks, if not already set as such
- ❑ Some printers can be configured to require a password before accessing web console
  - ❑ Majority of the printers reviewed did not support this feature.

# Man-in-the-Middle Attack?

- Unmitigated remote administration allows for IP address modification.
- Allows for a downgrade of the firmware to increase attack exposure
- A second possibility is a DOS:
  - ▣ Users unable to successfully send local print jobs
- Recent example – “Broadcast Storm”
  - ▣ a few infected printers were flooding the network with broadcast traffic.

# Man-in-the-Middle Attack?

- The third and most serious scenario –
  - ▣ Modification of a networked printer IP address
  - ▣ Then insertion of a third device into the communication process
- This third device would take on the IP address formerly used by the attacked printer
- Attacker could then continue to receive print jobs submitted by the normal users of the printer

# Man-in-the-Middle Attack cont.

- Attacker can:
  - ▣ Retain the print jobs until users realize that the printer is not working and action is taken by IT personnel
  - ▣ Use freeware tools to forward the print jobs on to the printer so that the end user detects no changes in their normal printing operations
  - ▣ In user's mind, print job submitted from their computer and then a document came out of the printer.
  - ▣ The delay while the attack takes place can be minimized in a way that would conceal the attack.

# Wireshark

analysis\_612050.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.7.2	224.0.0.22	IGMP	v3 Membership Report / Join group 239.255.255.250 for any sources
2	0.000000	10.1.7.2	224.0.0.22	IGMP	v3 Membership Report / Join group 239.255.255.250 for any sources
3	1.334566	74.213.167.192	10.1.7.2	TCP	http > llnx [FIN, ACK] Seq=1 Ack=1 win=6432 Len=0
4	1.334587	10.1.7.2	74.213.167.192	TCP	llnx > http [RST] Seq=1 win=0 Len=0
5	1.990305	10.1.7.2	79.135.167.18	TCP	ams > http [SYN] Seq=0 win=65535 Len=0 MSS=1460
6	2.012511	10.1.7.2	79.135.167.18	TCP	mtqp > http [SYN] Seq=0 win=65535 Len=0 MSS=1460
7	2.043675	79.135.167.18	10.1.7.2	TCP	http > ams [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460
8	2.043689	10.1.7.2	79.135.167.18	TCP	ams > http [ACK] Seq=1 Ack=1 win=65535 [TCP CHECKSUM INCORRECT] Len=0
9	2.065093	79.135.167.18	10.1.7.2	TCP	http > mtqp [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460
10	2.065104	10.1.7.2	79.135.167.18	TCP	mtqp > http [ACK] Seq=1 Ack=1 win=65535 [TCP CHECKSUM INCORRECT] Len=0
11	2.097490	10.1.7.2	79.135.167.18	HTTP	GET /scan.exe HTTP/1.1
12	2.097563	10.1.7.2	79.135.167.18	HTTP	GET /cgi-bin/index.cgi?test7 HTTP/1.1
13	2.150661	79.135.167.18	10.1.7.2	TCP	http > ams [ACK] Seq=1 Ack=194 win=6432 Len=0
14	2.150668	79.135.167.18	10.1.7.2	TCP	http > mtqp [ACK] Seq=1 Ack=209 win=6432 Len=0
15	2.151756	79.135.167.18	10.1.7.2	TCP	[TCP segment of a reassembled PDU]
16	2.151880	79.135.167.18	10.1.7.2	TCP	[TCP segment of a reassembled PDU]

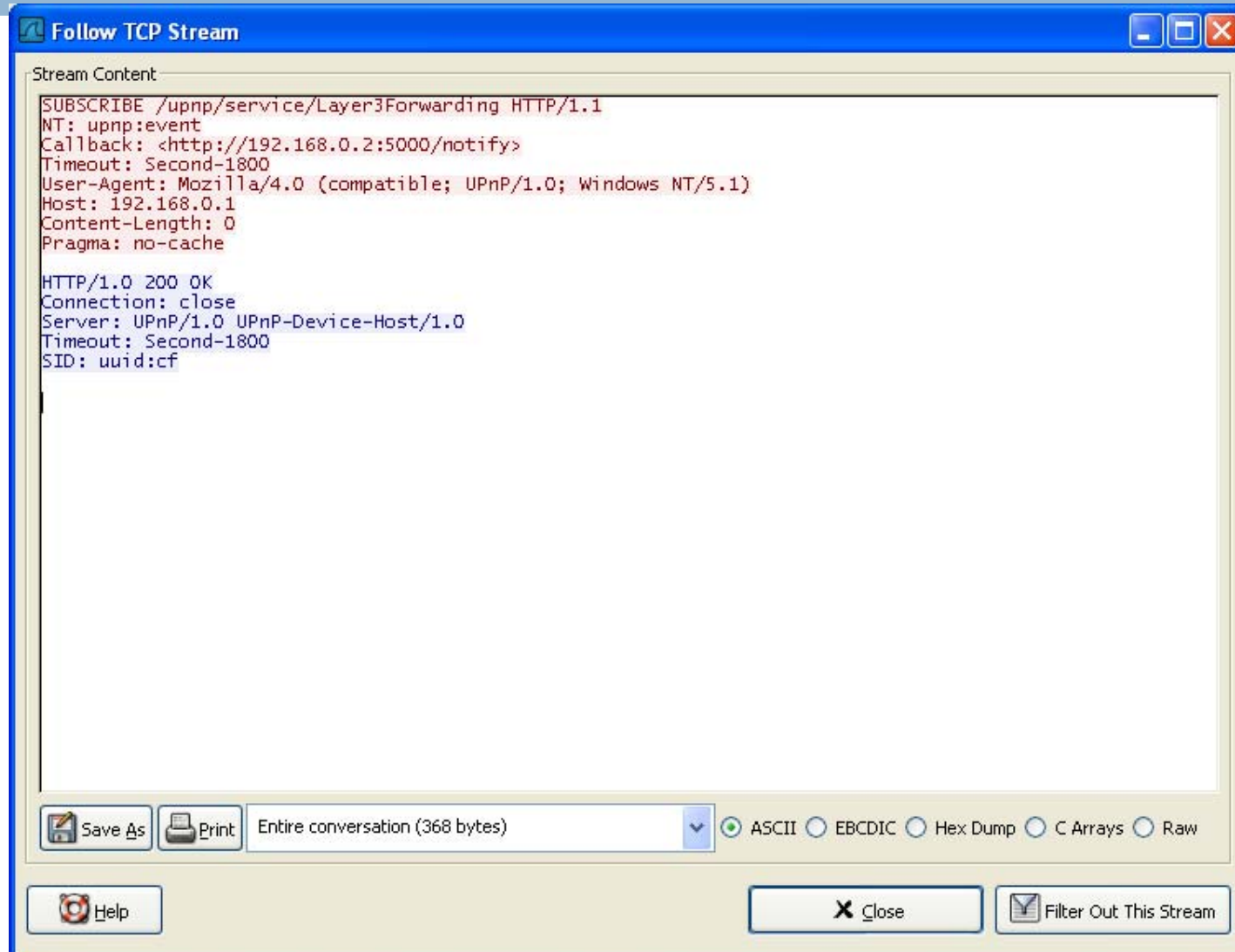
Frame 11 (247 bytes on wire, 247 bytes captured)

- Ethernet II, Src: AsustekC\_90:72:6c (00:1b:fc:90:72:6c), Dst: Intel\_8c:16:27 (00:16:76:8c:16:27)
- Internet Protocol, Src: 10.1.7.2 (10.1.7.2), Dst: 79.135.167.18 (79.135.167.18)
- Transmission Control Protocol, Src Port: ams (1037), Dst Port: http (80), Seq: 1, Ack: 1, Len: 193
- Hypertext Transfer Protocol

```
0000 00 16 76 8c 16 27 00 1b f0 90 72 6c 08 00 45 00 ..v.. ..r]..E.
0010 00 e9 00 54 40 00 80 06 f2 1e 0a 01 07 02 4f 87 ...T@... ..O.
0020 a7 12 04 0d 00 50 1d 2d 62 ae e2 f7 b1 cd 50 18 .....P.- b.....P.
0030 ff ff 08 78 00 00 47 45 54 20 2f 73 63 61 6e 2e ...x..GE T /scan.
0040 65 78 65 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 exe HTTP /1.1..Ac
0050 63 65 70 74 3a 20 2a 2f 2a 0d 0a 55 41 2d 43 50 cept: /* /*..UA-CP
0060 55 3a 20 78 38 36 0d 0a 41 63 63 65 70 74 2d 45 U: x86.. Accept-E
0070 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d
0080 65 66 6c 61 74 65 0d 0a 55 73 65 72 2d 41 67 65 eflate.. User-Age
0090 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 nt: Mozilla/4.0
00a0 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 (compatible; MSI
00b0 45 20 37 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e E 7.0; windows N
00c0 54 20 35 2e 31 29 0d 0a 48 6f 73 74 3a 20 37 39 T 5.1).. Host: 79
00d0 2e 31 33 35 2e 31 36 37 2e 31 38 0d 0a 43 6f 6e .135.167 .18..Con
00e0 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nnection: Keep-Al
00f0 69 76 65 0d 0a 0d 0a ive....
```

File: "C:\DOCUME~1\dhull\LOCALS~1\Temp\ana... Packets: 486 Displayed: 486 Marked: 0 Profile: Default

# Follow TCP Stream



# Man-in-the-Middle Attack cont.

- Internal Audit successfully performed this attack WITH management consent, but could have been done without.
- Important Note for this specific man-in-the-middle attack:
  - ▣ Need access to the same local network segment as the printer
- This does not greatly diminish the risk as most network attacks come from inside an organization's network.
- Imagine this attack on your:
  - ▣ Check printers
  - ▣ President's printers
  - ▣ HR printers
  - ▣ Registrar's printers

# Man-in-the-Middle Attack cont.

## Discussion Point:

- If you Google “How to hijack print job”
- You get questions like...
  - ▣ “I want to hijack my print jobs to my PC so I can determine if I want to print them out or not does anyone know how specifically to do this???. . . . .”
- Is there any legitimate need for this type of action?
  - ▣ What scenarios do you see where it could be helpful?

# Telnet and FTP Enabled

- Ran NMAP Scans on selected printers
- 85% of printers had Telnet and FTP enabled
- Obviously, both FTP and Telnet both enable communication in an unencrypted fashion
- FTP and Telnet should be disabled by default!

# SNMP v1 Enabled

- 90% of the total printers reviewed were running an older version of Simple Network Management Protocol (SNMP).
  - ▣ Printers running Version 1
  - ▣ Version 3 is current and generally supported by most printers.
  - ▣ Version 1 had no encryption, susceptible to packet sniffing.

# Default Community String

- 90% of the total printers reviewed still had the default community string in use.
- Community strings provide unencrypted authentication to the network device, in this case networked printers
- Configuration settings could be reviewed or modified by attackers using the default public community strings

# Breakdown of Identified Issues

*Printers - Total Affected Devices Matrix*

		Percentage Affected
<b>I S S U E S</b>	No Web Interface Password	55%
	Telnet Enabled	85%
	FTP Enabled	85%
	SNMP v1 Enabled	90%
	Default Community String	90%

**Note: 20 Printers were reviewed in total**

# UVA Management Response

- Our environment often calls for dual reporting as Health System and University have largely separate IT administration with disparate systems
- Both administrative functions were quick to respond with corrective actions appropriate for their environment

# UVA Management Response

## □ Health System

- Centrally managed computing environment
  - Printers no exception
- Allowed for swift modification to printer configurations
- Most suggested improvements to configurations were implemented
- Central applications prevented some config modification
- When older apps and systems are cycled out, the changes will be implemented where possible

# UVA Management Response

## □ University

- Decentralized computing environment management
  - Printers no exception
- Does not allow for swift unilateral modification to printer configurations
- University agreed with suggested areas for improvement
- Rapidly amended the forthcoming Data Security Standard to specifically include printer security settings (Next Slide)
- Communicated this new standard revision to technical support community

# Addition to University Security Standard

## Setting up Networked Printers

<http://www.itc.virginia.edu/security/device-requirements.html#printers>

### User Physical Security

Physically secure the printer, as if it were a computer server.

### Enable Access Controls

- Change the administrator password on the https (web) login.
- On any printer that supports it, install a CA certificate and use it instead of a password for administrative access.
- If available, use access lists to limit the users who can access the printer.

### Limit Network ports and protocols

Besides printing directly printing to a printer with an IP address on port 9100, other protocols can be used for specific operating systems. These include:

- ftp and lpd on Unix systems
- SLP Config, IPX/SPX on Novell networks
- mDNS and AppleTalk on Apple Macintosh networks
- DLC/LLC on Windows networks

These protocols are used to find printers on the network and send print jobs to them. These protocols are rarely used, but are still available on most printers. They are vulnerable to attacks and should be turned off.

### Restrict Management Services

SNMP, telnet and https (web) are protocols used to manage printers. Telnet is rarely used on older printers without web access. If https (web) access is available, telnet should be turned off. SNMP is used for large organizations managing hundreds to thousands of devices, including printers. SNMP should be turned off.

If there is a documented requirement for SNMP, the following guidelines should be followed to prevent security vulnerabilities from being exploited:

- Turn off version 1 and 2 of SNMP, and
- Change the default SNMP read and write community strings.

Turn logging on and review logs as appropriate to detect and/or investigate potential security breaches.

# Caveats

## □ **Technical:**

- Check existing policies/procedures for printer security
- Be aware of network layout (segments/traffic filtering)
- Be aware of baseline standards (printers or PCs)
- Test scanning methodology/attack on a local non shared device prior to beginning test work.
  - Tests could lock up a printer requiring a hard reboot causing accidental DOS.

# Caveats

## □ **Non-technical**

- Obtain Executive Management buy-in, avoiding departmental advanced notice where possible
- Get explicit approval & set timeframe for sensitive devices
  - Check printers, High-volume printers, Transcript printers
- Identify the owner of the printer device
  - To avoid blame game later

# Questions?

---

- Kevin Savoy – [savoy@virginia.edu](mailto:savoy@virginia.edu)
- Brian Daniels – [bdaniels@virginia.edu](mailto:bdaniels@virginia.edu)

