GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Auditing and Securing Multifunction Devices

GSEC Gold Certification

Author: Charles H. Scott, Jr.

cscott@infosec.utexas.edu

Adviser: Richard Wanner

Accepted: January 25, 2007

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, Author retains full rights.

Outline

1 Introduction 5

2 Multifunction Printer Risks 6

Network Services 6

Management Protocols 7

Services Protocols 10

Information Disclosure 15

Print, Fax, and Copy/Scan Logs 15

Address Books 18

Mailboxes 20

Denial of Service 21

Physical Security 22

3 Detecting MFDs on Your Network 24

© SANS Institute 2007, Author retains full rights.

Port Scanning 24

Service Scanning 25

OS Fingerprinting 28

SNMP Scanning 29

4 Securing MFDs 29

Locking Down Network Services 30

Using Secure Communications Protocols 31

Preventing Information Leakage 31

Preventing Denial of Service Attacks 32

Physically Securing the Device 32

5 Conclusion 34

6 References 35

7 Appendix: Multifunction Device Hardening Checklist 40

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, Author retains full rights.

1 Introduction

It used to be that a printer was connected directly to a computer via a serial or parallel interface, while fax machines and copiers did not connect to a computer at all. You knew where these devices were in your buildings and securing their physical output was your primary concern. In today's all-in-one world, you can now obtain single devices that are not only printers, but also copiers, scanners, and fax machines. These networked multifunction devices (MFDs) are increasingly common in enterprise environments and are manufactured by vendors such as Canon, HP, Kyocera, Xerox, and many others.

While time and money is spent on securing computer systems, MFDs (also called multifunction printers or all-in-one devices) are often overlooked. Unfortunately, they are computers in-and-of themselves, running an embedded operating system, advertising a variety of network services, and sporting gigabytes of hard drive space. Possible risks include information leakage from logs (e.g. fax numbers, long distance telephone codes, and filenames), SNMP attacks, poorly configured network services, and buffer overflows. Beyond the network attacks, there is the potential for data recovery from an MFD's internal hard drive. While it might be a standard practice to secure wipe or destroy the hard drives from

© SANS Institute 2007, Author retains full rights.

decommissioned laptops, workstations, and servers, what about MFDs that go in for maintenance or back to a leasing company after an upgrade?

This paper covers how to audit and secure your multifunction devices. It starts by giving an overview of the risks. Then it delves into how to discover MFDs on your network. Finally, it presents a checklist for securing these devices.

Note that the administration and configuration of MFDs varies widely depending on manufacturer, model, and firmware revision. This paper is intended as a starting point for securing MFDs; for specifics on how to implement its recommendations, consult your device's manual or manufacturer's website.

2 Multifunction Printer Risks

Network Services

MFDs often come with a wide variety of services enabled (Bullock, 2007). Chances are that many of these services are not required in all environments and should be turned off to decrease the attack footprint. Services that these devices support can be broken down into management protocols and services protocols. Management protocols are used for configuring, managing, and monitoring the device, while services protocols are used for printing, faxing, and scanning.

© SANS Institute 2007, Author retains full rights.

Management Protocols

- HTTP/HTTPS (TCP ports 80/443, sometimes 8080): Modern MFDs often include an embedded web server for management (Crenshaw, 2007). While this web server provides an easy-to-use, consolidated interface for managing the device, it is also the Holy Grail for anyone attacking to the device. Among the functions these interfaces typically provide (Bullock, 2007):
  - Log viewing.
  - Fax and scan mailbox viewing.
  - Direct print of Postscript or PDF files.
  - User management, access control list management, network configuration, and other administrative functions.

  Risks posed by the web interface:

  1. One-stop access for a cornucopia of information about the MFD (Bullock, 2007).
  2. HTTP is sent in the clear, meaning that authentication and configuration information might be sniffed from the network (Defense Information Systems

© SANS Institute 2007, Author retains full rights.

Agency, 2005).

- Telnet (TCP port 23): Some MFDs provide telnet configuration interfaces, which are also used by some older management tools (Hewlett-Packard, 2007). Telnet access gives a printer administrator a text-based (usually menu-driven) configuration and management interface to the printer.

  Risks posed by Telnet:

  1. Although telnet functionality is sometimes limited, compared to the web interface, it can still be used to modify network, password, and access list information, as well as monitor and manage print queues.

  2. Telnet is unencrypted and is considered an insecure protocol. Authentication and configuration information is sent in the clear, where it can be sniffed off the network (Homsher, 2006).

- SNMP (TCP port 161): SNMP is a network management protocol used for centralized monitoring and configuration of network-based devices (CERT, 2002). In general, it is used to gather information on the configuration of devices, and also allows for "traps" to be sent to a management console whenever an event occurs that warrants it (in the

© SANS Institute 2007, Author retains full rights.

case of MFDs, this could be an “out of paper” error). What follows is a samplelisting of SNMP information gathered by the *snmpwalk* program against a Canon MFP, which includes system and IP address information. Much of the output was omitted for space considerations.

```
sysDescr.0 = STRING: Canon iR3570 /P
sysObjectID.0 = OID: enterprises.1602.4.7
sysUpTime.0 = Timeticks: (118508900) 13 days, 17:11:29.00
sysContact.0 = STRING:
sysName.0 = STRING: iR3570
sysLocation.0 = STRING:
sysServices.0 = INTEGER: 72
.. omitted ..
ipAdEntAddr.127.0.0.1 = IpAddress: 127.0.0.1
ipAdEntAddr.10.16.42.188 = IpAddress: 10.16.42.188
ipAdEntIfIndex.127.0.0.1 = INTEGER: 2
ipAdEntIfIndex.10.16.42.188 = INTEGER: 1
ipAdEntNetMask.127.0.0.1 = IpAddress: 255.0.0.0
ipAdEntNetMask.10.16.42.188 = IpAddress: 255.255.255.0
ipAdEntBcastAddr.127.0.0.1 = INTEGER: 1
ipAdEntBcastAddr.10.16.42.188 = INTEGER: 1
ipAdEntReasmMaxSize.127.0.0.1 = INTEGER: 65535
ipAdEntReasmMaxSize.10.16.42.188 = INTEGER: 65535
ipRouteDest.0.0.0.0 = IpAddress: 0.0.0.0
ipRouteNextHop.0.0.0.0 = IpAddress: 10.16.42.250
.. remaining omitted ..
```


© SANS Institute 2007, Author retains full rights.

Risks posed by SNMP:

1. SNMP community strings (similar to passwords) are often set by default to "public" for read-only access and "private" for read-write access (Reavis, 1999). Many organizations do not change these.

2. An attacker could use SNMP to gather configuration information about the MFDs or possibly modify the configuration (Crenshaw, 2007).

3. The most widely used versions of SNMP, v1 and v2c, send community strings and data in the clear, which can be sniffed off the network (Reavis, 1999).

4. If the device is capable of SNMP write, then configuration information may be modified (Reavis, 1999)

Services Protocols

- TCP Port 9100 (a.k.a. HP JetDirect or *socket*): This is the service over which most printing takes place, especially for Windows computers (Crenshaw, 2007). It is also a control port for many printers, primarily those made by HP. Using this port and the

© SANS Institute 2007, Author retains full rights.

right utility you can, among other things, change what shows up on the LCD display (Phenoelit, 2007).

Risks posed by TCP port 9100:

1. Unauthorized remote printing.

2. Capture of spool files.

3. Modification of the LCD panel, either causing confusion ("Out of Service") or opening the door for social engineering purposes ("Error. Call 555-5151."). This can be done with tools such as HiJetter (Bullock, 2007).

- LPD (TCP port 515): LPD (Line Printer Daemon) is the printing system commonly used by Unix and Linux systems (Brooks, 2007). Most Unix systems now support CUPS (the Common Unix Printing System), which allows for printing over a number of protocols, including port 9100 and IPP.

Risks posed by LPD:

1. Unauthorized remote printing.

2. Jobs sent in clear-text, which can be sniffed off of the network.

© SANS Institute 2007, Author retains full rights.

- IPP (TCP port 631): The Internet Printing Protocol allows for printing either over a LAN or the Internet. It is used by the CUPS printing system in Linux and is also supported in Windows and Mac OS X. It is based off of HTTP and can require authentication and authorization, and can be TLS-enabled for encryption (Herriot, 2000).

  Risks posed by IPP:

  1. Unauthorized remote printing, if misconfigured.

  2. Interception of jobs via network sniffing, if not configured to use TLS.

- FTP (TCP port 21): Some MFDs support connections via the file transfer protocol, allowing you to upload files to print (Xerox, 2003). Another function that might be available is the ability to have the MFP upload files (e.g. scanned documents) to a file server.

  Risks posed by FTP:

  1. FTP authentication and transfer is unencrypted, so login credentials and data can be sniffed across the network (Cole, 2006).

  2. The MFP might be vulnerable to an FTP bounce attack. An FTP bounce attack

© SANS Institute 2007, Author retains full rights.

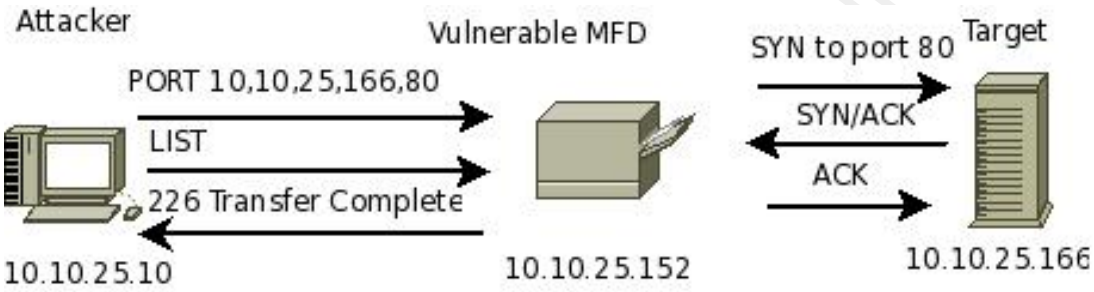
uses a proxy feature of FTP that allows a user to request that one FTP server copy files to another. Although this is not possible on many FTP servers today, it is still possible on some MFDs. FTP bounce scans allow an attacker to bypass firewalls, because the MFD might be behind the same firewall as the target of the scans, or the MFD's subnet might be allowed through the target's firewall (Cole, 2006). It has the added advantage of making the attack look like it is coming from the MFD, making the attacker harder to trace. Tools such as Nmap are capable of initiating FTP bounce scans (Fyodor, 2007). What follows is an example of what this looks like (it shows an MFD acting as an FTP bounce scanner scanning another MFD).

```
# nmap -P0 -b 10.10.25.152 10.10.25.166
Starting Nmap 4.20 ( http://insecure.org ) at 2007-09-20 14:30 CDT
Interesting ports on 10.10.25.166:
Not shown: 1690 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
280/tcp  open  http-mgmt
515/tcp  open  printer
631/tcp  open  ipp
9100/tcp open  jetdirect
```

Figure 1 shows an illustration of this scan. Note that if the scan hit a port that is not open (that is, it got a RST instead of SYN/ACK), it would return the FTP message of “425 Can’t Build Connection” (Messer, 2007).

© SANS Institute 2007, Author retains full rights.

Figure 1: An illustration of the FTP bounce attack (adapted from Messer, 2007).



- SMTP (TCP port 25): Some MFPs support inbound SMTP to allow an SMTP-to-fax service to work, and outbound SMTP is used to send scanned documents to their owners (Defense Information Systems Agency, 2005).

  Risks posed by SMTP:

  1. SMTP is unencrypted, meaning that data can be sniffed across the network.
  2. An inbound SMTP server might be used as an SMTP relay, allowing for spamming.

- SMB (TCP port 139): A few MFDs allow inbound SMB for Windows print services (Defense Information Systems Agency, 2005). Some MFDs can also attach to Windows network drives to upload information.

© SANS Institute 2007, Author retains full rights.

Risks posed by SMB:

1. SMB is an unencrypted protocol. Authentication hashes and data can be sniffed from the network.

2. Unauthorized printing, if not configured with authentication.

Information Disclosure

A risk often overlooked with MFDs is the potential for information disclosure. Read-only access to an MFDs web-based management interface or SNMP information is sometimes all that is needed for a social engineer to gather valuable information about an organization and its business practices (Bullock, 2007).

Print, Fax, and Copy/Scan Logs

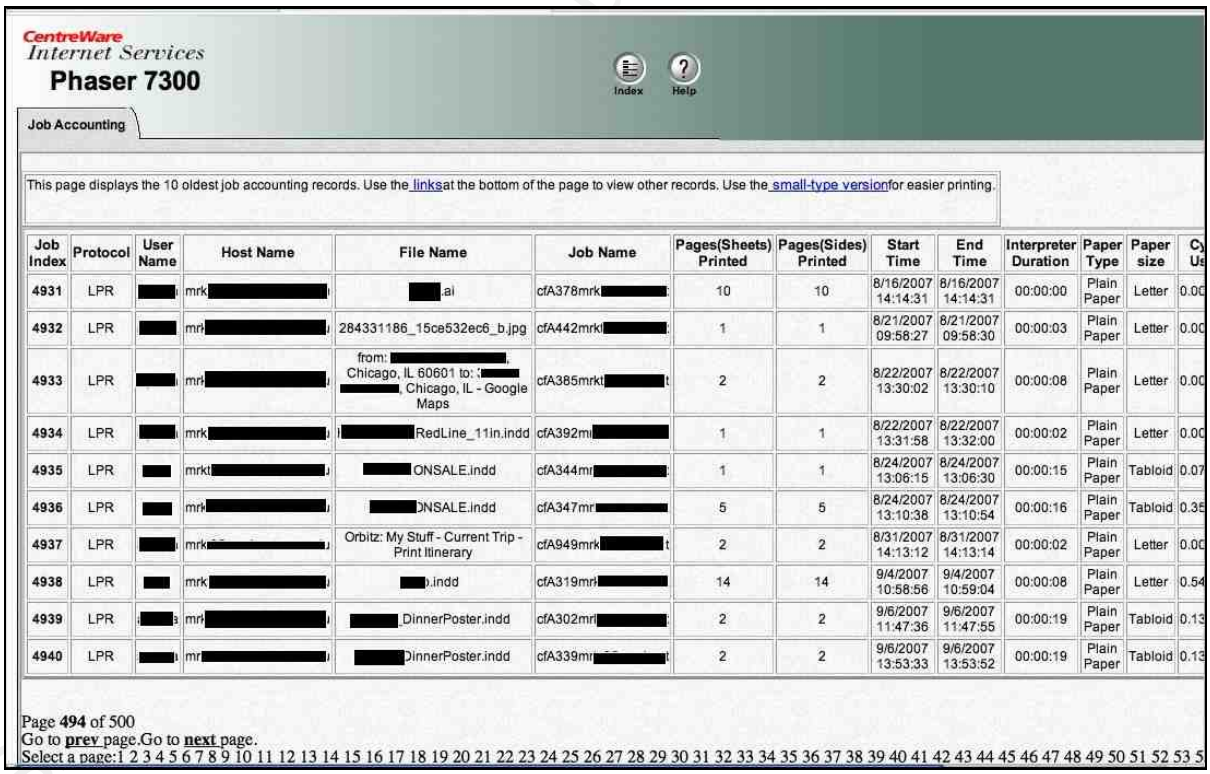
Print, fax, and copy/scan logs can reveal an abundance of information. On some MFDs, administrator access is not required to view these logs, obviating the need for an attacker to "dumpster dive" to get this information. This is just a small sample of the types of data that might be revealed:

Print Logs (also see **Figure 2**):

© SANS Institute 2007, Author retains full rights.

- Sensitive document names (e.g. Doe_Hepatitis_Results.xls).
- Network usernames (e.g. DoeJane).
- URLs of web sites users have printed from (e.g. https://www.myhealthinsurance.com)

Figure 2: A redacted screen shot of a print log from a Xerox MFP showing usernames, hostnames, filenames, and URLs.



CentreWare Internet Services
Phaser 7300

Index Help

Job Accounting

This page displays the 10 oldest job accounting records. Use the links at the bottom of the page to view other records. Use the small-type version for easier printing.

Job Index	Protocol	User Name	Host Name	File Name	Job Name	Pages(Sheets) Printed	Pages(Sides) Printed	Start Time	End Time	Interpreter Duration	Paper Type	Paper size	Cy Us
4931	LPR	[redacted]	mrk[redacted]	[redacted].ai	cfA378mrk[redacted]	10	10	8/16/2007 14:14:31	8/16/2007 14:14:31	00:00:00	Plain Paper	Letter	0.00
4932	LPR	[redacted]	mrk[redacted]	284331186_15ce532ec6_b.jpg	cfA442mrk[redacted]	1	1	8/21/2007 09:58:27	8/21/2007 09:58:30	00:00:03	Plain Paper	Letter	0.00
4933	LPR	[redacted]	mrk[redacted]	from: [redacted], Chicago, IL 60601 to: [redacted], Chicago, IL - Google Maps	cfA385mrkt[redacted]	2	2	8/22/2007 13:30:02	8/22/2007 13:30:10	00:00:08	Plain Paper	Letter	0.00
4934	LPR	[redacted]	mrk[redacted]	[redacted]RedLine_11in.indd	cfA392mr[redacted]	1	1	8/22/2007 13:31:58	8/22/2007 13:32:00	00:00:02	Plain Paper	Letter	0.00
4935	LPR	[redacted]	mrkt[redacted]	[redacted]ONSALE.indd	cfA344mr[redacted]	1	1	8/24/2007 13:06:15	8/24/2007 13:06:30	00:00:15	Plain Paper	Tabloid	0.07
4936	LPR	[redacted]	mrk[redacted]	[redacted]ONSALE.indd	cfA347mr[redacted]	5	5	8/24/2007 13:10:38	8/24/2007 13:10:54	00:00:16	Plain Paper	Tabloid	0.35
4937	LPR	[redacted]	mrk[redacted]	Orbitz: My Stuff - Current Trip - Print Itinerary	cfA949mrk[redacted]	2	2	8/31/2007 14:13:12	8/31/2007 14:13:14	00:00:02	Plain Paper	Letter	0.00
4938	LPR	[redacted]	mrk[redacted]	[redacted].indd	cfA319mrk[redacted]	14	14	9/4/2007 10:58:56	9/4/2007 10:59:04	00:00:08	Plain Paper	Letter	0.54
4939	LPR	[redacted]	mrk[redacted]	[redacted]_DinnerPoster.indd	cfA302mr[redacted]	2	2	9/6/2007 11:47:36	9/6/2007 11:47:55	00:00:19	Plain Paper	Tabloid	0.13
4940	LPR	[redacted]	mr[redacted]	[redacted]DinnerPoster.indd	cfA339mr[redacted]	2	2	9/6/2007 13:53:33	9/6/2007 13:53:52	00:00:19	Plain Paper	Tabloid	0.13

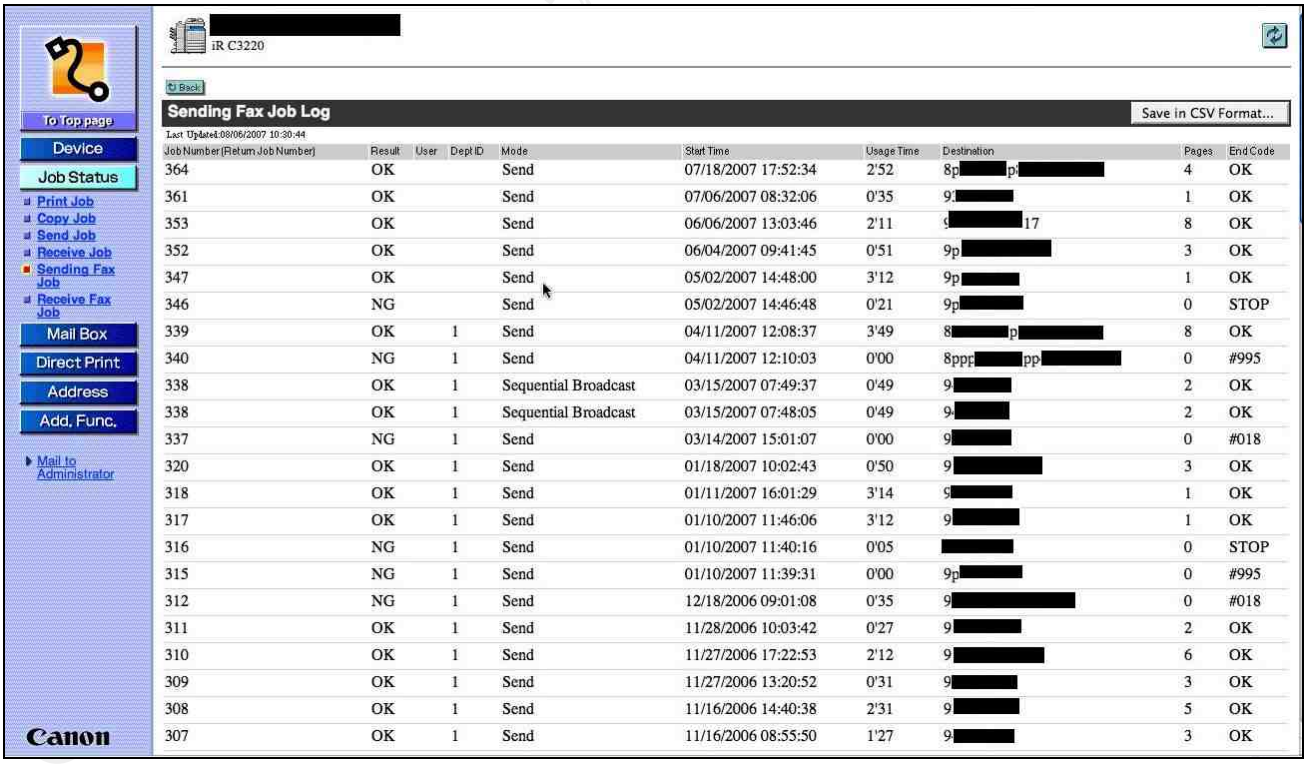
Page **494** of 500
Go to **prev** page.Go to **next** page.
Select a page:1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 5

- Fax Logs (also see **Figure 3**):

© SANS Institute 2007, Author retains full rights.

- Incoming fax numbers (tells an attacker with whom you are doing business).
- Outgoing fax numbers (again, with whom you are doing business).
- Long distance codes / long distance credit-card numbers (may show up with dialed numbers).

Figure 3: Redacted sent fax log from a Canon MFP, showing destination numbers and long distance codes.



Job Number (Return Job Number)	Result	User	Dept ID	Mode	Start Time	Usage Time	Destination	Pages	End Code
364	OK			Send	07/18/2007 17:52:34	2'52	8p[redacted]p[redacted]	4	OK
361	OK			Send	07/06/2007 08:32:06	0'35	9[redacted]	1	OK
353	OK			Send	06/06/2007 13:03:46	2'11	[redacted]17	8	OK
352	OK			Send	06/04/2007 09:41:45	0'51	9p[redacted]	3	OK
347	OK			Send	05/02/2007 14:48:00	3'12	9p[redacted]	1	OK
346	NG			Send	05/02/2007 14:46:48	0'21	9p[redacted]	0	STOP
339	OK	1		Send	04/11/2007 12:08:37	3'49	8[redacted]p[redacted]	8	OK
340	NG	1		Send	04/11/2007 12:10:03	0'00	8ppp[redacted]pp[redacted]	0	#995
338	OK	1		Sequential Broadcast	03/15/2007 07:49:37	0'49	9[redacted]	2	OK
338	OK	1		Sequential Broadcast	03/15/2007 07:48:05	0'49	9[redacted]	2	OK
337	NG	1		Send	03/14/2007 15:01:07	0'00	9[redacted]	0	#018
320	OK	1		Send	01/18/2007 10:02:43	0'50	9[redacted]	3	OK
318	OK	1		Send	01/11/2007 16:01:29	3'14	9[redacted]	1	OK
317	OK	1		Send	01/10/2007 11:46:06	3'12	9[redacted]	1	OK
316	NG	1		Send	01/10/2007 11:40:16	0'05	[redacted]	0	STOP
315	NG	1		Send	01/10/2007 11:39:31	0'00	9p[redacted]	0	#995
312	NG	1		Send	12/18/2006 09:01:08	0'35	9[redacted]	0	#018
311	OK	1		Send	11/28/2006 10:03:42	0'27	9[redacted]	2	OK
310	OK	1		Send	11/27/2006 17:22:53	2'12	9[redacted]	6	OK
309	OK	1		Send	11/27/2006 13:20:52	0'31	9[redacted]	3	OK
308	OK	1		Send	11/16/2006 14:40:38	2'31	9[redacted]	5	OK
307	OK	1		Send	11/16/2006 08:55:50	1'27	9[redacted]	3	OK

© SANS Institute 2007, Author retains full rights.

Copy/Scan Logs

- E-mail addresses of recipients.
- Host, username, and password information for FTP or SMB file uploads.

Risks posed by logs:

1. Combining information from these logs gives an attacker a very good picture of what an individual does in their day-to-day job, with whom they communicate, and how to get in touch with them.
2. Almost any of the gathered information can be used for social engineering purposes.
3. The unauthorized use of long distance codes or long distance credit cards.

Address Books

Address books (sometimes called distribution lists or destination lists) are used as shortcuts to tie names to contact information. Among the types of data that can be leaked by address books (also see **Figure 4**):

- Internal e-mail addresses, customer e-mail addresses.

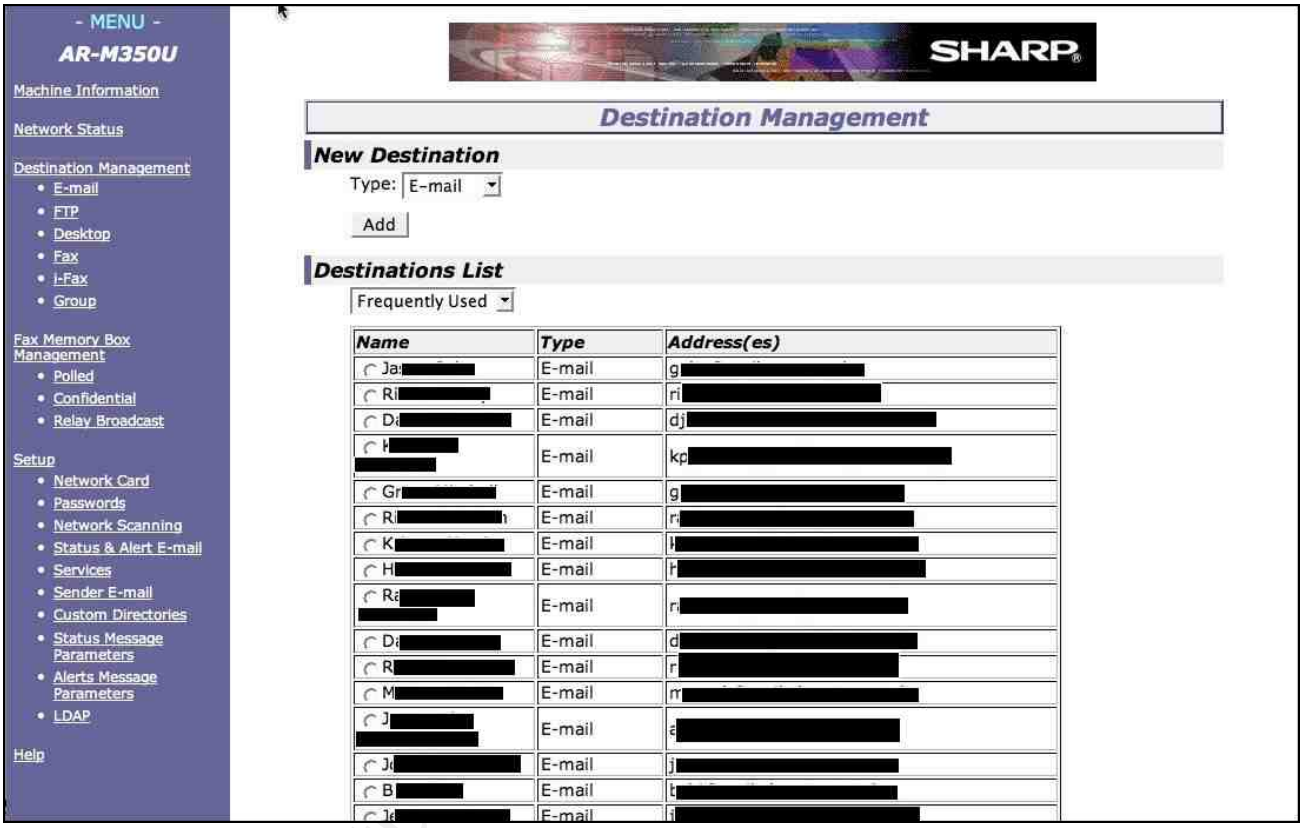
© SANS Institute 2007, Author retains full rights.

- Confidential internal or customer fax numbers.
- Long distance codes and long distance credit card numbers.
- Server addresses and usernames for FTP sites or SMB shares.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, Author retains full rights.

Figure 4: A redacted screen shot of the destination list on a Sharp MFP, showing names and e-mail addresses.

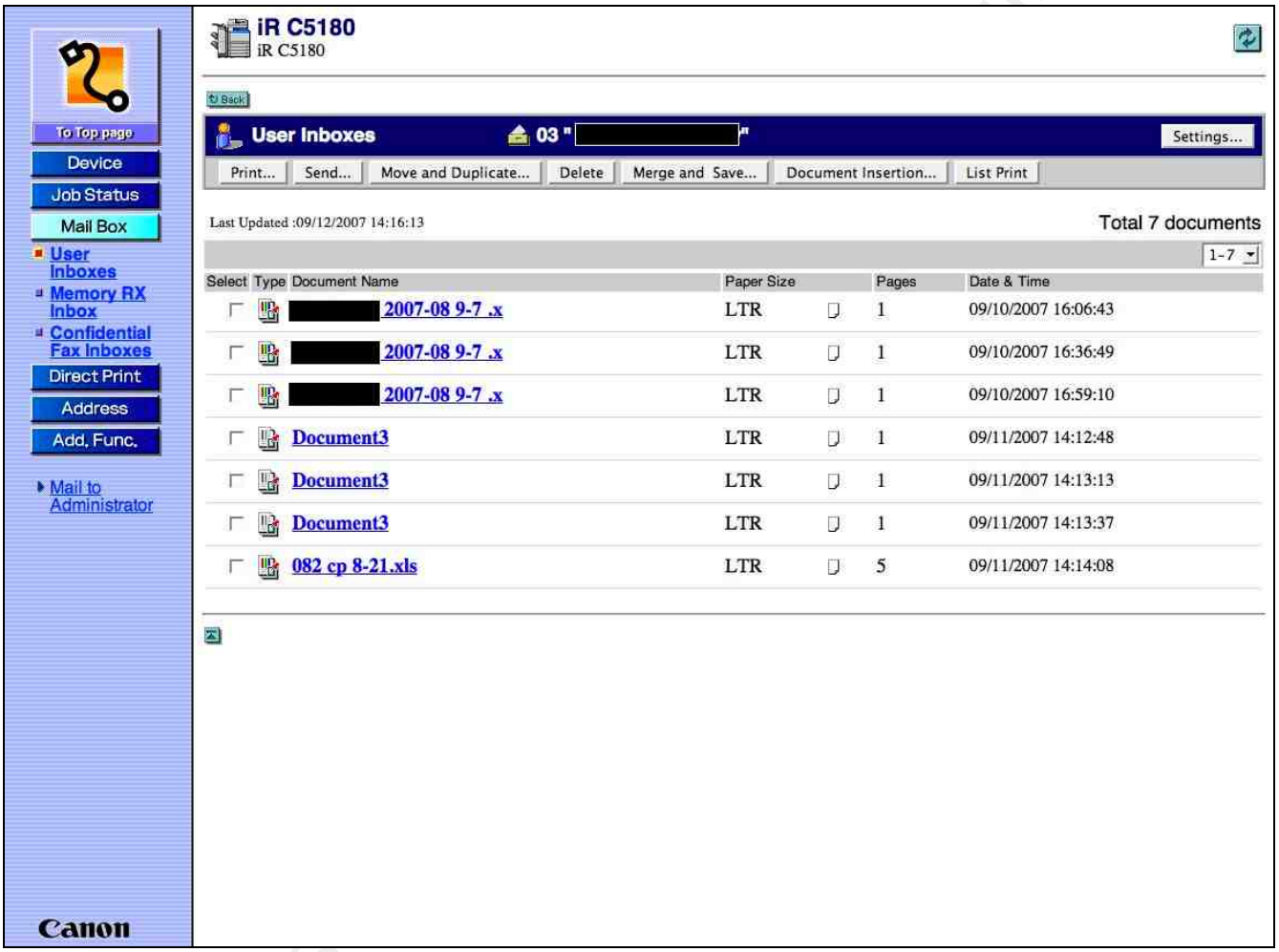


Mailboxes

Mailboxes are used to store scans, faxes, or templates on an MFD. Unless it is password protected, a mailbox could be a treasure trove of information for a potential attacker. Here they might find entire faxes or scanned documents containing sensitive information (also see Figure 5).

© SANS Institute 2007, Author retains full rights.

Figure 5: Redacted screen shot of a user's mailbox on a Canon MFP showing documents.



Denial of Service

MFDs are vulnerable to a number of remote denial-of-service attacks. The biggest threat is someone getting access to the configuration through HTTP or Telnet (Bullock, 2007) and making modifications that cause a denial of service. If a password is not set, default

© SANS Institute 2007, Author retains full rights.

passwords are used, or the password is brute-forced or guessed, then this could easily take place. An attacker could stop or delete print jobs, set the MFD back to factory defaults, or simply modify the administrator passwords and wreak havoc, requiring the IT staff to physically go to the device to make changes. Other ways to DoS MFDs include (Crenshaw, 2006):

1. Sending multiple bogus print jobs so that paper resources are exhausted.
2. Using *netcat* to send random data to port 9100 and exhaust resources.
3. Use HiJetter to modify settings, such as changing the language of the printer configuration or modifying the password.

Physical Security

Physical security is probably one of the greatest concerns when it comes to MFDs (Bullock, 2007). If someone has physical access to the device, they can perform any number of functions, including:

1. Make modifications to the global configuration via the console interface. While this can happen maliciously, it can also happen unintentionally when a user, IT staff person, or vendor troubleshoots the device. They might do is set the

© SANS Institute 2007, Author retains full rights.

device back to factory defaults to clear up a problem, and then only enter the bare minimum configuration, thus erasing any security hardening you may have done.

2. Send unauthorized faxes.

3. Obtain printouts or faxes that do not belong to them.

4. Physically remove the hard disk, which might contain print spool files and other information.

Besides these risks, there is a major one if the device (or its hard drive) ever leaves your physical premises. What happens if your MFD requires maintenance? Either you return it to the manufacturer or a vendor technician comes out to fix it. Either way, there is the risk that you might not get the same device or hard drive back, potentially exposing job spool files and other sensitive data. The same thing applies when the MFD reaches its end of use and is either sent back to a leasing company, disposed of, or sold. While it is fairly easy to use a utility such as Darik's Boot-and-Nuke to securely wipe the hard drive on a PC, MFDs present special challenges because they lack an external boot device. It may also be physically difficult to remove a hard drive from the MFD, or it may void your warranty if you do so.

© SANS Institute 2007, Author retains full rights.

3 Detecting MFDs on Your Network

Network scanning can help you locate the MFDs on your network. One way is with an active scanner, such as Nmap or Nessus, which generate network traffic on specified ports. When used against MFDs and printers, heavy active scanning can sometimes cause unpredictable results, such as a TCP/IP stack crash or garbage printouts. Passive scanners sniff network traffic and are much less intrusive than active scanners. In order to capture the relevant traffic, they must be placed in key network location, and the device you want to scan must actually be communicating (Bartlett, 2007). Passive scanners are available from companies such as Sourcefire and Tenable (Snyder, 2006). Primary methods for detecting MFDs are port scanning, service scanning, and OS fingerprinting, all of which can be done via active or passive scanning.

Port Scanning

One way to detect MFDs is to simply scan your network looking for hosts with TCP port 9100 (HP JetDirect) open, as most MFDs use this port for printing and not many other services utilize it (Bullock, 2007). You can also look for port 515 (LPD) and 631 (IPP) (Defense Information Systems Agency, 2006). If they also have port 80 or 443 open, they are likely an MFD, or at least a network-enabled printer. Scanning for port 80 or 443 individually

© SANS Institute 2007, Author retains full rights.

will also catch web servers that are not MFDs. The following is typical output from an Nmap SYN scan against a multifunction device:

```
# nmap -sS 10.52.146.28
Starting Nmap 4.20 ( http://insecure.org ) at 2007-09-23 17:15 CDT
Interesting ports on 10.52.146.28:
Not shown: 1691 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
515/tcp  open  printer
631/tcp  open  ipp
8000/tcp open  http-alt
9100/tcp open  jetdirect
```

Service Scanning

Although port scanning gives you a good idea of whether or not a system is an MFD, it does not tell you what brand of MFD it is. Service scanning uses application banners and other information to determine what is running on a specified port, giving you a better picture of the device's make. Because MFDs are commonly administered through web servers, HTTP server banners provide an excellent way to determine the manufacturer (Bullock, 2007). Table 1 presents a list of common MFD and printer manufacturers, along with the corresponding HTTP server banners used by the embedded web servers. Note that manufacturers often OEM the embedded web server, hence there are often different banners for each model and a banner may not contain the MFD manufacturer's name. What follows is

© SANS Institute 2007, Author retains full rights.

a sample service banner from a Xerox MFD, using Nmap's service detection:

```
# nmap -sV -p80 10.25.61.5

Starting Nmap 4.20 ( http://insecure.org ) at 2007-09-21 09:32 CDT
Interesting ports on 10.25.61.5:
PORT   STATE SERVICE VERSION
80/tcp open  http    Xerox MicroServer httpd Xerox11 (usually a
printer/copier)
```

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, Author retains full rights.

TABLE 1: HTTP Server Banners for Several MFDs and Printers

Manufacturer	HTTP Server Banner
Canon	Canon Http Server, CANON HTTP Server, Catwalk
HP	Virata-EmWeb, Agranat-EmWeb, HP-ChaiSOE, HP-ChaiServer, HTTP, Rapid Logic
Brother	debut, Debut
Xerox	Spyglass_MicroServer, Xerox_MicroServer
Sharp	RapidLogic
Epson	EPSON-HTTP
Dell	EWS-NIC3
Kyocera	NetworkScanner WebServer

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, Author retains full rights.

OS Fingerprinting

OS fingerprinting uses characteristics of a device's TCP/IP stack to determine what it is (Cole, 2006). Nmap (using the "-O" option) can perform an active OS fingerprint, while p0f is an example of a tool that performs a passive OS fingerprint (Skoudis, 2007). While OS fingerprinting works in some cases, there are countless different models of printers and MFDs and not all of them exist in OS fingerprint database (Cole, 2006). Indeed, for some it may be impossible to say with one hundred percent certainty that it is an MFD. In a test OS fingerprint scan performed by the author against 1855 known printers, Nmap was only able to discern the OS on 317 of them (or about 20%). In short, OS fingerprinting is not a reliable technique for detecting MFDs, and should only be used to support port scanning and service scanning. What follows is sample output from a successful Nmap OS detection:

```
# nmap -O 10.62.6.7
Starting Nmap 4.20 ( http://insecure.org ) at 2007-09-21 17:14 CDT
Interesting ports on 10.62.6.7:
Not shown: 1692 closed ports
PORT     STATE SERVICE
80/tcp   open  http
280/tcp  open  http-mgmt
515/tcp  open  printer
631/tcp  open  ipp
9100/tcp open  jetdirect
Device type: print server
Running: HP embedded
OS details: HP JetDirect J3110A print server
```


© SANS Institute 2007, Author retains full rights.

Network Distance: 3 hops

SNMP Scanning

As seen in the Management Protocols section, SNMP can provide you with a variety of information about an MFD. You can use this to your advantage as you scan for MFDs on your network. To pull this information, you need to either know the SNMP read community string for the device, or it needs to be set to a default (such as "public"). Once you have located a suspected MFD, you can use the Linux *snmpwalk* utility to scan it. Snmpwalk is the part of the Net-SNMP package, which is available for Windows, Linux, and Unix systems (Net-SNMP, 2002). Unfortunately, while this information might help you secure your MFDs, it is also useful to an attacker who wants to target your device. What follows is the output of *snmpwalk* scanning a Xerox MFD and pulling the "sysDescr" MIB object, which gives the system description (in this case, the manufacturer, model, and version).

```
# snmpwalk -Os -c public -v 1 10.26.9.20 sysDescr
sysDescr.0 = STRING: Xerox Document Centre Multi-function System, ESS 0.19.05.531.1, IOT
0.19.5.531, UI 0.19.5.527
```

4 Securing MFDs

In this section we will take each of the risks that an MFD presents and look at ways of preventing them.

© SANS Institute 2007, Author retains full rights.

Locking Down Network Services

Decreasing the attack footprint of the device can go a long way towards securing it (Cole, 2007). A good first step is to disable all protocols other than TCP/IP (Defense Information Systems Agency, 2006). Some MFDs support protocols such as AppleTalk and IPX/SPX, which are more difficult to monitor and secure than TCP/IP. If you are not using these in your environment, then disable them using your MFD's configuration interface.

Second, you should disable any network services that are not being used (Defense Information Systems Agency, 2006). As stated earlier, these generally fall into communications protocols (for print, fax, and scanning services) or protocols for management. Look at whether or not the protocol is used in your environment, the risk it presents if it is used, and decide whether or not the risk is acceptable. If the risk is not acceptable and the MFD allows for it, then disable them.

Third, consider assigning a static IP address to the MFD (Defense Information Systems Agency, 2006). Devices with static IPs are easier to locate and secure (say, with a firewall).

Finally, for the remaining protocols that must be available, lock them down to the minimum number of hosts or subnets that require access (Cole, 2006). Most MFDs offer the

© SANS Institute 2007, Author retains full rights.

ability to restrict who can connect to them via built-in TCP wrappers or ACLs (Defense Information Systems Agency, 2006). If only the marketing department needs to print from the device, then restrict access to ports 9100, 515, or 631 to that department; or, restrict printing to a single print server. Likewise, restrict the management services to a few IP addresses that actually need to manage the device (Hewlett-Packard, 2007). Also consider moving the MFDs to a VLAN specific to those devices and limiting access to particular ports and protocols using a firewall (Defense Information Systems Agency, 2005).

Using Secure Communications Protocols

To reduce the risk of your data being sniffed from the network on the protocols you left enabled, use secure communications wherever possible. Disable HTTP for management and use HTTPS instead. If at all possible, disable FTP and Telnet. If you are using SNMP to monitor or manage the printer, consider disabling SNMPv1 and v2c, and use SNMPv3 to take advantage of its authentication and encryption capabilities (Defense Information Systems Agency, 2005).

Preventing Information Leakage

Besides reducing protocols and services, the best way to prevent information leakage is to set a strong administrator password (Cole, 2006). This will prevent anyone from seeing

© SANS Institute 2007, Author retains full rights.

sensitive configuration information. Likewise, if you are using SNMP, change the community strings from the defaults to strong passwords. Also lock down log screens, mailboxes, and address books with passwords according to your password policy.

Preventing Denial of Service Attacks

As with information disclosure, locking down network services and setting passwords will help prevent denial of service attacks by ensuring that only legitimate users have access to the services. An addition to these measures, timely patching of the system's firmware is also prudent (Bullock, 2007). In order to do this, you need to know that security issues exist and that new firmware is available. Unfortunately, unlike many operating systems, MFDs do not typically have an "auto-update" capability. It is best to keep an eye out for CVEs for your devices (http://cve.mitre.org/) and monitor mailing lists such as Bugtraq. Likewise, your vendor may have ways of contacting you when there is an update available.

Physically Securing the Device

Restricting who has physical access to the device is the first step in physically securing it (Cole, 2006). Look at the type of data that is normally processed by the MFD and then decide how restrictive it should be. If the device regularly prints or faxes human resources, medical, legal, financial, or other sensitive information, consider limiting who has access to

© SANS Institute 2007, Author retains full rights.

the device by placing it in a locked room or a restricted office area. Personnel from shipping, for instance, should not be able to print to the HR printer nor get into the HR office area to get a printout.

Second, ensure that an administrator password is set on the MFD console and only given to authorized users. This will limit who can make changes (accidental or deliberate) to the global configuration.

Third, require authentication for people needing to fax, scan, copy, or print faxes, from the MFD. Require at least a password; however, some vendors can take this a step further and allow for two-factor authentication (a password and a card).

Fourth, if the MFD has an easily removable hard drive, ensure that the drive is locked into the device and only trusted people have the key.

Finally, look at ways the data that is on the hard drive can be secured. Some MFDs offer security features natively or through an add-on "security kit." One useful feature is the ability to secure-erase files in between jobs. This not only ensures that jobs are no longer there if someone remotely accesses the device's filesystem through FTP, HTTP, or a tool like HiJetter, but also keeps the jobs from being found if the MFD goes off-site. Likewise, encryption of the filesystem (usually only part of an add-on kit) can make sure the drive is

© SANS Institute 2007, Author retains full rights.

unreadable if removed from the MFD. Security kits can also implement a “secure wipe” of an entire drive to be used when the device is about to be sold or sent back to the manufacturer (Canon, 2007). If this is not possible on your device, then work with the manufacturer to see if you can remove and keep the hard drive so that you can wipe or destroy it yourself. In order to ensure this occurs, write it into your security policy for decommissioned devices.

5 Conclusion

Given the fact that they contain an embedded operating system, run popular services such as HTTP, FTP, and SMTP, and store gigabytes of data, multifunction devices should be treated like servers on your network. By following a hardening strategy similar to that which you use on your servers, many of the risks these devices present can be mitigated.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, Author retains full rights.

6 References

Bartlett, G, Heidemann, J, and Papadopoulos, C (2007, May). *Understanding Passive and Active Service Discovery*. Retrieved on September 20, 2007 from the USC/Information Sciences Institute Web site: http://www.isi.edu/~johnh/PAPERS/Bartlett07b.html

Brooks Internet Software (2007). LPR-LPD Protocol. Retrieved September 25, 2007 from Brooks Internet Software Web site: http://www.brooksnet.com/lpr-lpd-protocol.html

Bullock, J (2007). MFDs: New Features Bring New Risks. Retrieved on September 21, 2007 from Dalhousie University Web site: http://ucis.dal.ca/depts/security/events/canheit2007/mfds.pdf

Canon U.S.A, Inc. (2007). Canon imageRUNNER Security Kit. Retrieved on September 20, 2007 from Canon USA Web site: http://www.usa.canon.com/opd/controller?act=OPDModelDetailAct&fcategoryid=2214&modelid=6607

© SANS Institute 2007, Author retains full rights.

CERT (2002, February 13). Simple Network Management Protocol (SNMP) Vulnerabilities. Retrieved September 25, 2007 from the CERT Web page: http://www.cert.org/tech_tips/snmp_faq.html

Cole, E (2006). *Security Essentials Bootcamp Style*. Bethesda, MD: The SANS Institute.

Crenshaw, A (2007, February 6). Hacking Network Printers. Retrieved on September 21, 2007 from Irongeek.com Web site: http://www.irongeek.com/i.php?page=security/networkprinterhacking

Defense Information Systems Agency (2005, July 28). Sharing Peripherals Across the Network, Security Technical Implementation Guide, Version 1, Release 1. Retrieved September 20, 2007, from Information Assurance Environment Web site: http://iase.disa.mil/stigs/stig/span-stig-v1r1.pdf

Defense Information Systems Agency (2006, April 14). Multi-Function Device (MFD) and Printer Checklist for Sharing Peripherals Across the Network, Security Technical Implementation Guide, Version 1, Release 1.2. Retrieved September 20, 2007, from

© SANS Institute 2007, Author retains full rights.

Information Assurance Support Environment Web site: http://iase.disa.mil/stigs/checklist/SPAN-MFD-ChecklistV1R1-2-14APR2006.pdf

Fyodor (2007). Nmap Reference Guide. Retrieved on September 20, 2007 from Insecure.org Web site: http://insecure.org/nmap/man/index.html

Herriot, R, Butler, S, Moore, P, Turner, R, Wann, J (2000, September). RFC: 2910: Internet Printing Protocol/1.1: Encoding and Transport. Retrieved September 25, 2007 from the Internet Engineering Task Force Web site: http://tools.ietf.org/html/rfc2910

Hewlett-Packard Development Company, L.P. (2006, March 29). HP LaserJet 4354 MFP Security Checklist. Retrieved September 20, 2007 from HP United States Web site: http://www.hp.com/united-states/business/catalog/nist_checklist.pdf

Hewlett-Packard Development Company, L.P. (2007). Making HP Jetdirect Print Servers Secure on a Network. Retrieved September 22, 2007 from HP Business Support Center Web site: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj05999

© SANS Institute 2007, Author retains full rights.

Homsher, L (2006, August 28). SANS Linux Security Checklist. Retrieved September 25, 2007 from the SANS Institute Web site: http://www.sans.org/score/linuxchecklist.php

Messer, J (2007). *Secrets of Network Cartography: A Comprehensive Guide to Nmap*. Retrieved September 30, 2007 from the Network Uptime web site: http://www.networkuptime.com/nmap/page3-20.shtml

Net-SNMP (2002, February 18). The snmpwalk man page. Retrieved September 30, 2007 from the Net-SNMP SourceForge Web site: http://net-snmp.sourceforge.net/docs/man/snmpwalk.html

Phenoelit (2007). PFT & HiJetter Printer Exploration. Retrieved on September 21, 2007 from the Phenoelit Web site: http://www.phenoelit-us.org/hp/docu.html

Reavis, J (1999, October 4). SNMP – simple management tool for hackers? Retrieved September 24, 2007 from Network World Web site: http://www.networkworld.com/newsletters/sec/1004sec1.html

© SANS Institute 2007, Author retains full rights.

Skoudis, E (2007). *Hacker Techniques, Exploits, & Incident Handling*. Bethesda, MD: The SANS Institute.

Snyder, J (2006, July 31). Sourcefire, Tenable seek vulnerabilities passively. Retrieved September 30, 2007 from the Network World Web site: http://www.networkworld.com/reviews/2006/073106-sourcefire-tenable-passive-test.html

The University of Texas at Austin Information Security Office (2007, September 13). Multifunction Printer Hardening Checklist. Retrieved September 20, 2007, from The University of Texas at Austin Web site: http://www.utexas.edu/its/policies/checklists/mfprinter.php

Xerox Corporation (2003, May 8). Xerox Product Implications When FTP is Disabled. Retrieved September 25, 2007 from the Xerox Corporation Web site: http://www.xerox.com/downloads/usa/en/h/HIPAA_fact_sheet_v1.pdf

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, Author retains full rights.

7 Appendix: Multifunction Device Hardening Checklist

#	√	Action
Network Protocols and Services		
1		Disable unused network protocols other than TCP/IP.
2		Disable unused network services (print/fax/scan and management).
3		Assign the MFD a static IP address.
4		Restrict access to MFD services (print/fax/scan and management) to the minimum number of hosts that require these functions.
5		Use encrypted communications protocols (e.g. HTTPS), where available, and disable insecure protocols.
Management		
6		Set a strong administrator password.
7		Change default SNMP community strings to strong passwords.
8		Ensure that logging is enabled on the MFD.
8		Ensure that logs are monitored on a regular basis.
9		Restrict access to address books, mailboxes, and logs using your current password policy.
Security Updates		
10		Monitor CVEs and vendor for security bulletins and patches.
11		Upgrade firmware in a timely manner, using your current change control process.

© SANS Institute 2007, Author retains full rights.

Physical Security		
12		Place the device in an area with physical security controls consistent with the sensitivity data it processes.
13		Set an administrator password on the console.
14		Require that users authenticate to scan, fax, or copy from the console.
15		If the MFD has a removable hard drive, ensure that it is locked into the device.
16		If possible, implement measures to encrypt or secure-wipe print spool files.
17		Ensure that your security policy specifies what to do with MFD drives that are decommissioned or sent back to the manufacturer or leasing company (e.g. retained, secure wiped, destroyed, etc.).

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, Author retains full rights.