Auditing and Securing Multifunction Devices

Multifunction devices (MFDs) are manufactured by vendors such as Canon, HP, Kyocera, Xerox, and many others....
Auditing and Securing Multifunction Devices

GSEC Gold Certification

Author: Charles H. Scott, Jr.

cscott@infosec.utexas.edu

Adviser: Richard Wanner

Accepted: January 25, 2007
Auditing and Securing Multifunction Devices

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

Charles H. Scott, Jr.  2
Auditing and Securing Multifunction Devices

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

Charles H. Scott, Jr.
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

Charles H. Scott, Jr.
Auditing and Securing Multifunction Devices

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.

Charles H. Scott, Jr.
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):

  o Log viewing.

  o Fax and scan mailbox viewing.

  o Direct print of Postscript or PDF files.

  o 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...
Auditing and Securing Multifunction Devices

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

Charles H. Scott, Jr.
case of MFDs, this could be an “out of paper” error). What follows is a sample listing 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..
```
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
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.
Auditing and Securing Multifunction Devices

- **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
Auditing and Securing Multifunction Devices

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).
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.
Auditing and Securing Multifunction Devices

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):

Charles H. Scott, Jr.
Auditing and Securing Multifunction Devices

- 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.

Fax Logs (also see Figure 3):

Charles H. Scott, Jr.
- 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.

<table>
<thead>
<tr>
<th>Job Status</th>
<th>Job Type</th>
<th>Start Time</th>
<th>Destination</th>
<th>Status</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>07/18/2007 17:52:34</td>
<td>12345678901234567890</td>
<td>035</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>07/18/2007 20:32:06</td>
<td>012345678901234567890</td>
<td>035</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>06/06/2007 13:03:46</td>
<td>12345678901234567890</td>
<td>114</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>06/06/2007 09:41:45</td>
<td>12345678901234567890</td>
<td>051</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>05/02/2007 14:48:00</td>
<td>12345678901234567890</td>
<td>112</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>05/02/2007 14:46:48</td>
<td>12345678901234567890</td>
<td>021</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>04/11/2007 12:08:37</td>
<td>12345678901234567890</td>
<td>349</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>04/11/2007 12:05:03</td>
<td>12345678901234567890</td>
<td>9995</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>03/15/2007 07:49:37</td>
<td>12345678901234567890</td>
<td>049</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>03/15/2007 07:48:05</td>
<td>12345678901234567890</td>
<td>049</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>03/14/2007 15:01:07</td>
<td>12345678901234567890</td>
<td>900</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>03/14/2007 16:19:29</td>
<td>12345678901234567890</td>
<td>314</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>03/10/2007 11:41:06</td>
<td>12345678901234567890</td>
<td>312</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>03/10/2007 11:40:16</td>
<td>12345678901234567890</td>
<td>005</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>03/10/2007 11:39:31</td>
<td>12345678901234567890</td>
<td>0995</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>12/18/2006 09:01:08</td>
<td>12345678901234567890</td>
<td>035</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>11/28/2006 10:33:42</td>
<td>12345678901234567890</td>
<td>027</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>11/16/2006 14:40:38</td>
<td>12345678901234567890</td>
<td>731</td>
<td>OK</td>
</tr>
<tr>
<td>Send Job</td>
<td>Send</td>
<td>11/16/2006 08:55:50</td>
<td>127</td>
<td>3 OK</td>
<td></td>
</tr>
</tbody>
</table>
Auditing and Securing Multifunction Devices

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.
Auditing and Securing Multifunction Devices

- 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.
Auditing and Securing Multifunction Devices

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).

Charles H. Scott, Jr.
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
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
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.
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

Charles H. Scott, Jr.
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...
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)
```
### TABLE 1: HTTP Server Banners for Several MFDs and Printers

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>HTTP Server Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canon</td>
<td>Canon HTTP Server, CANON HTTP Server, Catwalk</td>
</tr>
<tr>
<td>HP</td>
<td>Virata-EmWeb, Agranat-EmWeb, HP-ChaiSOE, HP-ChaiServer, HTTP, Rapid Logic</td>
</tr>
<tr>
<td>Brother</td>
<td>debut, Debut</td>
</tr>
<tr>
<td>Xerox</td>
<td>Spyglass_MicroServer, Xerox_MicroServer</td>
</tr>
<tr>
<td>Sharp</td>
<td>RapidLogic</td>
</tr>
<tr>
<td>Epson</td>
<td>EPSON-HTTP</td>
</tr>
<tr>
<td>Dell</td>
<td>EWS-NIC3</td>
</tr>
<tr>
<td>Kyocera</td>
<td>NetworkScanner WebServer</td>
</tr>
</tbody>
</table>
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
```

Charles H. Scott, Jr.
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.
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
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
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

Charles H. Scott, Jr.
Auditing and Securing Multifunction Devices

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

Charles H. Scott, Jr.
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.
6 References


http://www.cert.org/tech_tips/snmp_faq.html


Charles H. Scott, Jr. 36
Auditing and Securing Multifunction Devices

Information Assurance Support Environment Web site:


Charles H. Scott, Jr.
Auditing and Securing Multifunction Devices


Charles H. Scott, Jr.
Auditing and Securing Multifunction Devices


http://www.utexas.edu/its/policies/checklists/mfprinter.php

7 Appendix: Multifunction Device Hardening Checklist

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Place the device in an area with physical security controls consistent with the sensitivity data it processes.</td>
</tr>
<tr>
<td>13</td>
<td>Set an administrator password on the console.</td>
</tr>
<tr>
<td>14</td>
<td>Require that users authenticate to scan, fax, or copy from the console.</td>
</tr>
<tr>
<td>15</td>
<td>If the MFD has a removable hard drive, ensure that it is locked into the device.</td>
</tr>
<tr>
<td>16</td>
<td>If possible, implement measures to encrypt or secure-wipe print spool files.</td>
</tr>
<tr>
<td>17</td>
<td>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.).</td>
</tr>
</tbody>
</table>
### Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Riyadh July 2018</td>
<td>Riyadh, SA</td>
<td>Jul 28, 2018 - Aug 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pittsburgh 2018</td>
<td>Pittsburgh, PAUS</td>
<td>Jul 30, 2018 - Aug 04, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Summer 2018</td>
<td>Boston, MAUS</td>
<td>Aug 06, 2018 - Aug 11, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Hyderabad 2018</td>
<td>Hyderabad, IN</td>
<td>Aug 06, 2018 - Aug 11, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS August Sydney 2018</td>
<td>Sydney, AU</td>
<td>Aug 06, 2018 - Aug 25, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS New York City Summer 2018</td>
<td>New York City, NYUS</td>
<td>Aug 13, 2018 - Aug 18, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Prague 2018</td>
<td>Prague, CZ</td>
<td>Aug 20, 2018 - Aug 25, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2018</td>
<td>Virginia Beach, VAUS</td>
<td>Aug 20, 2018 - Aug 31, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Francisco Summer 2018</td>
<td>San Francisco, CAUS</td>
<td>Aug 26, 2018 - Aug 31, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Copenhagen August 2018</td>
<td>Copenhagen, DK</td>
<td>Aug 27, 2018 - Sep 01, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC504 @ Bangalore 2018</td>
<td>Bangalore, IN</td>
<td>Aug 27, 2018 - Sep 01, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam September 2018</td>
<td>Amsterdam, NL</td>
<td>Sep 03, 2018 - Sep 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Wellington 2018</td>
<td>Wellington, NZ</td>
<td>Sep 03, 2018 - Sep 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Tokyo Autumn 2018</td>
<td>Tokyo, JP</td>
<td>Sep 03, 2018 - Sep 15, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Tampa-Clearwater 2018</td>
<td>Tampa, FLUS</td>
<td>Sep 04, 2018 - Sep 09, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS MGT516 Beta One 2018</td>
<td>Arlington, VAUS</td>
<td>Sep 04, 2018 - Sep 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response Summit &amp; Training 2018</td>
<td>New Orleans, LAUS</td>
<td>Sep 06, 2018 - Sep 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2018</td>
<td>Baltimore, MDUS</td>
<td>Sep 08, 2018 - Sep 15, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Alaska Summit &amp; Training 2018</td>
<td>Anchorage, AKUS</td>
<td>Sep 10, 2018 - Sep 15, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich September 2018</td>
<td>Munich, DE</td>
<td>Sep 16, 2018 - Sep 22, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2018</td>
<td>London, GB</td>
<td>Sep 17, 2018 - Sep 22, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2018</td>
<td>Las Vegas, NVUS</td>
<td>Sep 23, 2018 - Sep 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Oil &amp; Gas Cybersecurity Summit &amp; Training 2018</td>
<td>Houston, TXUS</td>
<td>Oct 01, 2018 - Oct 06, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS DFIR Prague Summit &amp; Training 2018</td>
<td>Prague, CZ</td>
<td>Oct 01, 2018 - Oct 07, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Bangalore 2018</td>
<td>OnlineIN</td>
<td>Jul 16, 2018 - Jul 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>