Global Information Assurance Certification Paper

A Security Assessment of the Minolta Di251 Network Printer Copier
Version 1.1 28th January 2004
SANS GSEC Practical Version 1.4b Option 1
Russell Owsianski

Introduction/Abstract

The use of networked printers is increasing in many businesses. Networked printing is more easily monitored and controlled than desktop printing, reducing waste and discouraging non-business use. As well, the cost of ink jet printers for each worker's desk (and more significantly, the cost of ink cartridges) is thought to be much higher than a smaller number of work group laser printers. Individual printers, copiers, scanners and faxes can be replaced by a single feature rich network device.

Although security vulnerabilities can happen in any printer, for the purposes of this essay I will examine the security concerns surrounding the Minolta Di251 printer/copier when it is installed on a typical corporate LAN. In addition to my research, I have scanned the printer with various security tools to discover available network services and search for vulnerabilities in them. After investigating the vulnerabilities, I will suggest policy and technical methods of mitigating or preventing these weaknesses. My investigations show that the Di251 has a number of serious security vulnerabilities. Many of these vulnerabilities are likely to be present in other manufacturer's multifunction printers as well, and demonstrate that these devices must be protected with the same defense in depth approach that is applied to servers.

About the Minolta Di251

The network at my workplace includes a number of manufacturers' networked printers: Ricoh, Minolta and HP. I have chosen to examine the Minolta printers because the others have been featured in previous studies. The Ricoh Aficio 450E by David Garrard (Garrard) and HPs (specifically Jetdirect cards) by Mir Moosa Khan (Moosa Khan).

The Minolta Di251 is a network capable digital printer copier for business use. It has up to 256MB of memory, prints postscript and PCL, and has a number of optional attachments to provide duplex printing, sorting, stapling and collating. It includes Minolta's Pi3502 network controller with a 10/100 baseT network card and optional hard drive. Strictly speaking, it is this combination of a Di251 printer/copier plus a Pi3502 network controller that I will be investigating, though I will sometimes refer to 'the printer' as a whole for simplicity. The Pi3502 is also used in other Minolta network printer models, the Di200 and Di351.

The printer's networking capabilities include: Appletalk; peer to peer TCP/IP and IPX/SPX; Novell Bindery and NDS support; lpr/lpd under TCP/IP; SNMP (MIB-II and a Minolta enterprise MIB); on board HTTP and telnet servers for configuration; direct printing from a web browser or other ftp client; direct printing from an IPP client and SLP (Service Location Protocol) support.

Vulnerability Assessment

The first step in examining a device's security is to perform an analysis of the potential threats it may face. Printers and copiers are often used to produce or duplicate sensitive documents, so the confidentiality of this networked information must be protected. While unlikely, it may be possible to alter printed/copied documents, damaging their integrity. Finally, exposed network services and weakly authenticated configuration interfaces can make these devices ripe targets for denial of service attacks which reduce their availability to legitimate users.

The risk that a computer system faces is directly related to the threats arrayed against it, and the vulnerabilities present on the system. Any system connected to a network is threatened with scans and possible attacks. This threat is much greater if the system is visible from the outside internet. Using research and scanning tools, I will make a detailed investigation of the vulnerabilities present on the Minolta Di251 printer and its Pi3502 network controller.

For the purposes of this essay I will be concentrating on remote attacks over the network, but in a real life situation, the physical security of the printer copier must also be considered. Confidential documents could easily be taken from a busy, insecure area. The device may be disabled by unplugging it, changing its configuration from the front panel controls, or causing physical damage. Most networked printers can be purchased with an optional hard drive for storing print jobs. The hard drive might be physically removed from the machine for later examination of the documents stored on it. This consideration is especially important when the printer reaches the end of its life and is sold or otherwise discarded. I could not find any procedure in the Minolta documentation for ensuring that files were erased, though it is possible to format the hard drive. However, if the data were sufficiently valuable, even this method wouldn't ensure that it could not be recovered. While the Di251's hard drive is only used for storing postscript fonts, the hard drive of higher end models like the Di551 and Di850 can be used to store print jobs.

There are a number of ways that printer copiers might be compromised; attacks could be made via vulnerable network services to compromise or create a denial of service on the device, or changes made to the printer's network configuration which could render it unusable or create wider network outages. An attacker could glean information from the printer about the organization of the network to which the printer is attached as reconnaissance for later attacks. This

information may suggest promising vulnerabilities or weak points ripe for exploitation. It might be possible to use the printer as an intermediate host from which to attack other network resources. Also, the printer may be vulnerable to attack by malware such as worms or virii. For practical reasons, I was not able to investigate this last possibility directly.

Security Research About the Minolta Di251

I began my investigation by searching the web. I checked Mitre CVE (Mitre), Packetstorm (Packetstorm), X-Force (X-Force), Bugtraq archives (Bugtraq) and Google (Google) for various combinations of the terms Minolta, network, security, printer and Di251. I used boolean operators in searches such as '"network printer" Di251 OR Pi3502 NOT HP' to reduce the number of extraneous results. There were very few results. Packetstorm had nothing specific about Minolta devices, but there was a result about sniffing network print jobs, and a discussion about vulnerabilities/exploits for other printers via httpd, ftp bounce and denial of service attacks. The SANS reading room contains a paper by David Garrard about the Ricoh 450e multifunction device (Garrard), and that paper refers to some older work on the topic of network printer security (Smith, Daniels, Orvis).

Next, I examined the manufacturer's documentation for the device and checked the manufacturer website for any information about the Di251 and its Pi3502 controller. The Di251 User Manual (Minolta 1) had little information of interest. The Pi3502 Service Manual (Minolta 2) is mainly concerned with physical installation/connection of the controller (the Pi3502). This includes dismounting the hard drive, memory and 'smartmedia' which stores the controller's programming (looks like a PCMCIA card). The section describing error codes mentions SMTP and FTP server errors. The Pi3502 Network Interface Card Operators Manual (Minolta 3) describes how to configure the many protocols available. This and other information included in this manual would be very valuable to an attacker seeking to compromise the security of the printer.

The default authentication for changing configuration via telnet is username 'sysadm' and password 'sysadm' (Minolta 3, pg. 9-2). This password is also used for authenticating to the configuration web page on the printer. The password can be changed, but has a maximum of eight characters. The printer can be reset to default configuration with the telnet or web interface, or via a jumper on the network card. For ftp access, the default username is 'port1' and the password is also 'port1'. Any file which is 'put' to the ftp server will be printed.

I was able to find a wide selection of Minolta manuals (as CDs full of pdf files) for sale on Ebay (Ebay) for between $12 and $40. With a bit more searching I was able to find these files available for download on Minolta's website including the Network Interface Card Operators Manual which details the network protocol and service configuration options and includes the default 'full access' passwords.

Searching for Vulnerabilities

Next, I tried using various security tools on the device. I obtained explicit permission from my employer for these steps, and did all my testing outside of normal business hours, when the devices were not in use.

I began with Nmap. Nmap is an open source port scanner with many features and options. I tried both a 'traditional' SYN scan and a more stealthy FIN scan. The results for both types of scan were the same.

Nmap showed a number of open ports that could be investigated:
21 ftp
23 telnet
80 HTTP
161 SNMP
515 lpr
631 ipp
8080 HTTP proxy
10000 snet-sensor-mgmt (actually used by Minolta's proprietary MAP software)

It is also possible for port 25 SMTP to be listening on Di251 units which are equipped with a scanner option. The local email system is used to send scanned documents to users.

I used telnet to connect to each of the listening ports to check for banners or other information.

Port 23 - Telnet

Telneting to port 23 gave me a bannerless login prompt. The printer accepted the default username and password from the operator's manual. I logged the conversation and included it here. I have replaced the real IP address information with private RFC 1918 (Rekhter) addresses.

```
login: sysadm
Password:

        The Configuration Utility
        Unit Serial no. 055230  v6.20

        Main Menu

        1.  IP Parameters
        2.  LPD Printers
        3.  Protocols
        4.  Reset Unit
        5.  Restore Factory Defaults
        6.  Change Password
        E.  Exit

        Please Enter Selection (? for Help) : 1
```

```
The Configuration Utility
Unit Serial no. 055230  v6.20

IP Parameters

1.  IP Address                              192.168.0.17
2.  Subnet Mask                             255.255.255.0
3.  Default Gateway                         192.168.0.254
4.  Base Port Number                        10000

Please Enter Selection (? for Help) :

The Configuration Utility
Unit Serial no. 055230  v6.20

Main Menu

1.  IP Parameters
2.  LPD Printers
3.  Protocols
4.  Reset Unit
5.  Restore Factory Defaults
6.  Change Password
E.  Exit

Please Enter Selection (? for Help) : 2

The Configuration Utility
Unit Serial no. 055230  v6.20

LPD Printers

1.  Printer 1                               ASCII
2.  Banners                                 DISABLED

Please Enter Selection (? for Help) :

The Configuration Utility
Unit Serial no. 055230  v6.20

Main Menu

1.  IP Parameters
2.  LPD Printers
3.  Protocols
4.  Reset Unit
5.  Restore Factory Defaults
6.  Change Password
E.  Exit

Please Enter Selection (? for Help) : 3

The Configuration Utility
Unit Serial no. 055230  v6.20

Protocols

1.  NetWare                                 DISABLED
2.  AppleTalk                               DISABLED

Please Enter Selection (? for Help) : 1

The Configuration Utility
```

```
Unit Serial no. 055230  v6.20

Protocols

1.  NetWare                                  ENABLED
2.  AppleTalk                                DISABLED

Please Enter Selection (? for Help) : 1

The Configuration Utility
Unit Serial no. 055230  v6.20

Protocols

1.  NetWare                                  DISABLED
2.  AppleTalk                                DISABLED

Please Enter Selection (? for Help) :

The Configuration Utility
Unit Serial no. 055230  v6.20

Main Menu

1.  IP Parameters
2.  LPD Printers
3.  Protocols
4.  Reset Unit
5.  Restore Factory Defaults
6.  Change Password
E.  Exit

Please Enter Selection (? for Help) : e
```

Note that it was possible to enable and then disable the NetWare protocol. When I used the non-administrator username and password, 'guest' and 'guest' I was able to see all the settings, but not make changes.

Port 21 - FTP

Ftping to the printer gave me a standard looking ftp login prompt for a user name. I was able to login with the default username and password 'port1' and 'port1'. This password cannot be changed.

```
ftp> dir
200 PORT command OK.
550 Requested action not taken. Access not allowed.
ftp> pwd
202 Command not implemented, superfluous at this site.
ftp> status
Connected to 192.168.0.17.
Type: ascii; Verbose: On ; Bell: Off ; Prompting: On ; Globbing: On
Debugging: Off ; Hash mark printing: Off .
ftp> ls
200 PORT command OK.
202 Command not implemented, superfluous at this site.
ftp>
```

When I used ftp 'put' to send a file to the printer, it was accepted and printed

without any further authentication.

While searching the web I found a bugtraq reference to an 'ftp bounce attack' which is possible against the ftp server on a different manufacturer's networked printer.

> Nashuatec printer, 3 vulnerabilites found
>
> other flaw is present in the ftp daemon that permit the infamous "bounce attack".
> ftp printer.victim.com
> user xxxxx
> pass xxxxx
> quote port a1,a2,a3,a4,0,25
>
> a1.a2.a3.a4 is every other ip adress.
>
> the ftp server doesn't check neither the type of port in the request (< 1024 = administrative port) nor the ip adress used.
> So an intruder may use the service to attack some ohter boxes anonymously. (Duchemin)

I decided to try this technique on the Minolta Di251. The command was accepted, but when I used Ethereal to sniff the traffic leaving the printer I did not see anything destined for the IP I had specified in the bounce attack. This vulnerability is old, so it is likely that Minolta has patched their ftp server to prevent ftp bounce attacks.

Port 80 - HTTP

Browsing to the Di251 with Mozilla produced the printer's web page. This page should raise a number of security concerns for any network administrator.

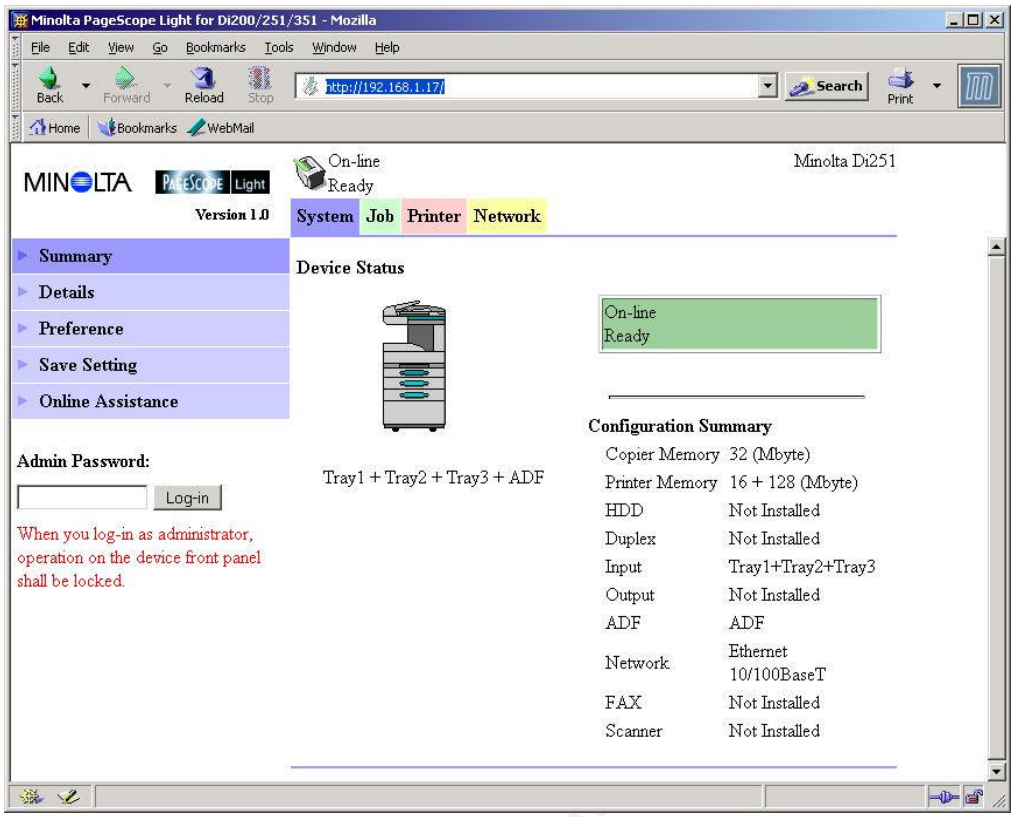

Figure 1 - Minolta Pi3502 main web page

The main page lists the model number of the printer and lists any installed options such as hard drive, network and scanner. A page labeled 'details' includes ROM version numbers of the software on the printer and the network controller. A page labeled 'printer' includes buttons for 'Format Hard Drive', 'Update Firmware' and 'Restore Factory Defaults'. For an attacker with the correct password, each of these would be an effective Denial of Service attack requiring a service call to return the printer to operation.

A 'Network' page lists the printer's IP address, MAC and serial number. The TCP/IP configuration page has IP address, net mask, subnet gateway, base port # (for Minolta administrative software, default is 10000) and whether or not the printer's IP is assigned by DHCP. The NetWare configuration page lists the print server name, preferred server, NDS context, and NDS tree. A NetWare Status subpage includes the name of the file server and print queue objects. The Appletalk configuration page lists the printer and zone names. The WINS configuration page has the NetBIOS name and WINS server IP.

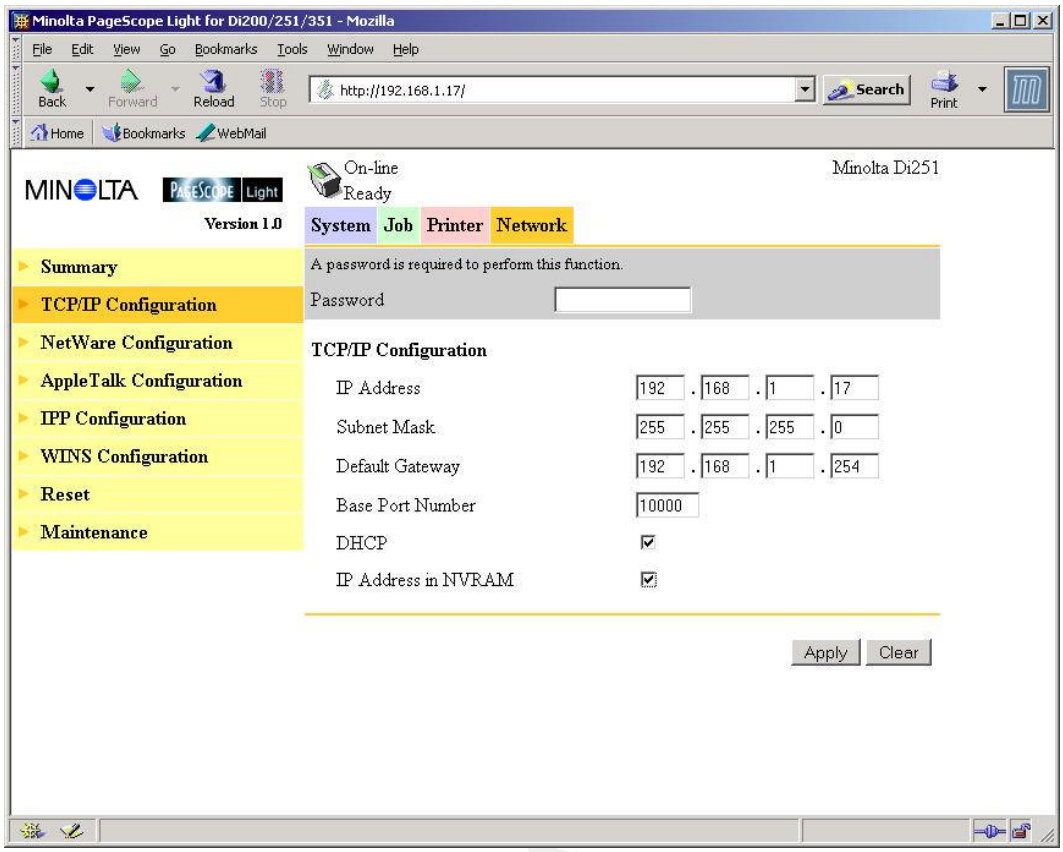

Figure 2 - Minolta Pi3502 TCP/IP Configuration web page

Finally, a 'Job' page includes information about documents being printed including document name, owner, total pages, number of copies, time submitted and printing status. It is possible to submit print jobs directly from the web page with no authentication. With a password, it is possible to delete or pause print jobs.

No authentication is required to browse the printer's web pages. An attacker may learn detailed network information, server names, protocols in use, and user names. This information could provide an attacker with a significant amount of data about the structure and organization of the network the printer is attached to and suggest possible avenues for farther attacks.

All of these options could be changed through the web interface. Although any changes require a password for authentication, the default password is the same as for telnet, and is available in the NIC Operators Manual. (Minolta 3).

Since nmap showed that port 80 was listening, I tried scanning the printer with Nikto. Nikto is an open source tool for locating vulnerabilities in web servers. It is a newer incarnation of the now defunct Whisker. Nikto tests for multiple items, including over 2600 potentially dangerous files/CGIs. Nikto's scan of a Di251 revealed little info, it identified the webserver as EMWHTTPD/1.0, but found no

other weaknesses. A quick search on google for EMWHTTPD found only a reference to it in a BlackHat paper about httpd fingerprinting (Shah).

Port 161 - SNMP

The Di251/Pi3502 listens for SNMP requests on port 161 tcp. I was surprised and dismayed to find that there is no way to change the default, well known SNMP community strings 'public' for read-only and 'private' for read-write access. There is also no way to disable the SNMP service. I sent SNMP queries to the device using the Net-SNMP tools (previously known as 'ucd-SNMP') and retrieved all of the printer's MIB-II information, including details of its TCP/IP networking configuration. I was unable to find a copy of Minolta's enterprise MIB for the Pi3502, but using SNMP 'get next' queries I got responses from a small number of non-MIB-II OIDs.
I was able to change the printer's network configuration with SNMP set commands.

```
>snmpset.exe 192.168.0.17 private .1.3.6.1.2.1.4.2.0 i 59
Changed ip.ipDefaultTTL.0 fm 60 to 59
```

In this example, the default IP TTL setting of the stack was changed from its default of 60 to 59. While this is an harmless change, it demonstrates that it would also be possible to change the printer's IP address or routing table.

Port 631 – ipp, and port 8080

An attempt to telnet to either of ports 631 or 8080 gave this result:

```
telnet 192.168.0.17 631
HTTP/1.1 405 Method Not Allowed
Allow: GET, HEAD, POST
Content-Length: 0
Server: Allegro-Software-RomPager/2.00

Connection to host lost.
```

A quick Google search for 'Allegro-Software-RomPager' found this;

> Allegro-Software-RomPager/2.10 vulnerable to Dos Attack
> Recently I was bashing up a D-Link DES-3224+ ethernet switch and after submitting a number of invalid authentication requests to the Allegro-Software-RomPager installed on it I managed to freeze the whole switch putting all the network down. (Netsec)

While the software version is slightly different, it is possible that the older version used on the Di251/Pi3502 is susceptible to the same DOS attack.

Ports 515 – lpd and port 10000

All attempts to telnet to ports 515 and 10000 gave no response. However even this meager result gives some information. It shows that some service is listening on those ports, since telnet to closed ports such as 175 and 715 gives the message;

```
Connecting to 192.168.0.17...Could not open a connection to host on
port 175 :
Connect failed
```

The various protocols that the printer understands: TCP/IP, IPX/SPX, NetBIOS and Appletalk, can be enabled or disabled from the web or telnet interfaces. As well, the SMTP service on scanner equipped printers can be effectively disabled by assigning an IP of 0.0.0.0 to that service. There is no way to add Access Control Lists to the printer's telnet, HTTP, ftp and SNMP services or otherwise limit access to those services from the network. If TCP/IP networking is enabled and configured, there is no way to disable individual services. There is no facility for logging accesses to the printer or its services.

Nessus

Next I tried scanning the device with nessus 2.0.9. I used nessus' 'safer' mode, which skips plugins likely to crash the scanned services. Despite this precaution I inadvertently caused the printer's webserver to stop responding. Power cycling the printer brought it back to normal operation. I have included nessus results below.

```
192.168.0.17|http (80/tcp)|10919|NOTE|This port was detected as being
open by a port scanner but is now closed.;This service might have been
crashed by a port scanner or by a plugin;;
192.168.0.17|ftp (21/tcp)|10092|NOTE|Remote FTP server banner :;220 FTP
Server ready.
;
192.168.0.17|http-proxy (8080/tcp)|10330|NOTE|An unknown service is
running on this port.;It is usually reserved for HTTP-Alt;
192.168.0.17|general/tcp|10201|INFO|;The remote host uses non-random IP
IDs, that is, it is;possible to predict the next value of the ip_id
field of;the ip packets sent by this host.;;An attacker may use this
feature to determine traffic patterns;within your network.   A few
examples (not at all exhaustive) are:; ;1. A remote attacker can
determine if the remote host sent a packet ;in reply to another
request.  Specifically, an attacker can use your ;server as an
unwilling participant in a blind portscan of another ;network.  ;;2. A
remote attacker can roughly determine server requests at certain ;times
of the day.  For instance, if the server is sending much more ;traffic
after business hours, the server may be a reverse proxy or ;other
remote access device.  An attacker can use this information
to;concentrate his/her efforts on the more critical machines.;;3. A
remote attacker can roughly estimate the number of requests that ;a web
server processes over a period of time.;;;Solution : Contact your
vendor for a patch;Risk factor : Low;
192.168.0.17|http (80/tcp)|10330|NOTE|A web server is running on this
port;
192.168.0.17|general/tcp|11834|INFO|;The remote host accepts loose
```

```
source routed IP packets.;The feature was designed for testing
purpose.;An attacker may use it to circumvent poorly designed IP
filtering ;and exploit another flaw. However, it is not dangerous by
itself.;;Solution : drop source routed packets on this host or on other
ingress ;routers or firewalls.  ;;;Risk factor : Low;
192.168.0.17|ftp (21/tcp)|10330|NOTE|An FTP server is running on this
port.;Here is its banner : ;220 FTP Server ready.
;
192.168.0.17|general/udp|10287|NOTE|For your information, here is the
traceroute to 192.168.0.17 :
;192.168.23.61;192.168.23.62;192.168.0.17;;
192.168.0.17|http-proxy (8080/tcp)
192.168.0.17|printer (515/tcp)
192.168.0.17|ipp (631/tcp)
192.168.0.17|snet-sensor-mgmt (10000/tcp)
192.168.0.17|ftp (21/tcp)
192.168.0.17|telnet (23/tcp)
192.168.0.17|http (80/tcp)
```

Nessus found only two minor vulnerabilities: there are non-random IP IDs and the remote host accepts loose source routed IP packets. Nonetheless, it reported a significant amount of information about the printer and its network services, which could provide a starting point for more concerted attacks.

Packet Sniffing

I used Ethereal to try to sniff the contents of a print job being sent to the device. Ethereal is an open source network packet analyzer for UNIX and Windows. I sent a test print job from my workstation to the device while sniffing from a laptop. Using Ethereal's 'follow TCP stream' and 'save file' tools, I was able to retrieve the data and reconstruct the document in a readable form. The workstation, printer and laptop were all attached to different switches on the network. Since I am a network administrator at my site, I was able to set up port mirroring, which made this test easier. As with my other tests, I made sure to inform my supervisor and obtain permission. However, using a tool such as Ettercap could make this possible without such privileges. Ettercap allows sniffing between normally isolated hosts on a switched LAN by using the technique of 'arp poisoning'. Also, had either the workstation or printer been connected to a hub rather than a switch, or if an attacker was able to place a small hub between the printer and its regular network connection, sniffing print jobs would be an easy way to compromise their confidentiality.

Vulnerabilities Discovered

My scans and probes convinced me that a malicious attacker would have little trouble changing the network configuration of the printer, effectively removing it from the network. I suspect that most installed Di251s have not had their default passwords changed. When I asked the system administrator responsible for the printers at our site, she said that Minolta's technicians had suggested leaving the passwords at their default values so that they would be able to service the machines without having to contact IT staff for the passwords each time. Even if

they have been changed, there is nothing to stop the attacker from endlessly guessing passwords, which are limited to eight characters. If the attacker was able to sniff the traffic to the printer, they could easily extract the plaintext http or telnet passwords. Another technique that could easily succeed is sniffing SNMP traffic, which would include the community strings in plaintext, or simply generating SNMP queries using the extremely well known default community strings 'public' and 'private'. More seriously, once an administrative password was discovered, it would be possible to change the printer's IP to match that of an important server or subnet gateway. This would create a more widespread Denial of Service, and might be tricky for network administrators to troubleshoot. It is unlikely that the first investigations into a network outage would include checking the IP addresses of photocopiers. An additional type of DOS would be to send bogus print jobs to the device's ftp server. This could prevent legitimate jobs from being printed and waste paper and ink.

The amount of information that is available on the printer's web page could greatly aid an attacker doing a reconnaissance of the network prior to a more serious incursion. The printer can reveal other server's names and services, protocols in use, valid usernames and router/gateway IP addresses. This network information is also easily available via SNMP. While 'security through obscurity' cannot be relied upon, it is bad practice to make such detailed information available to anyone with a web browser or SNMP tools.

Mitigating Di251 Vulnerabilities

Unfortunately, there are few controls on the Di251/Pi3502 itself that can mitigate its vulnerabilities. In this way, these printers are a good example of the importance of defense in depth.

As a first step, any unused protocols (Appletalk, NetBIOS, IPX/SPX) should be disabled. If the printer has a scanner installed, it will be SMPT capable, and this could also be disabled.

Next, the printer should be connected to a subnet or VLAN where it will not be exposed to the outside internet. In fact, given the amount of information available via http and SNMP, the printer should be isolated by internal firewalls or filtering routers from all other subnets except those that need to send print jobs to it. If possible, a separate, screened subnet populated only by printers could be created, with only those protocols and services essential to printing allowed to pass. As well, perimeter firewalls and routers should be configured to prevent unwanted access to the printer's services - these would include ports 21 tcp (telnet), 23 tcp (ftp) 25 tcp (SMTP), 80 tcp (HTTP),139 tcp (NetBIOS) 161 udp (SNMP), 427 tcp (NetWare Service Locater), 515 tcp (lpr), 631 tcp (ipp), 8080 tcp and 10000 tcp. In practice, there is no legitimate reason for any traffic from the outside to reach the printer, so all ports should be blocked in keeping with the principal of least privilege, or 'that which is not specifically permitted should be

denied.'

The Di251 and Pi3502's software should be regularly updated to the latest available versions.

Ensuring the security of network devices such as printers is especially challenging since traditional methods of protecting servers such as host-based IDS or logging are not available.

The inclusion of networked printer copiers in an organization's security policy is essential. Printers must be recognized as servers with many network services and be protected accordingly. This is especially critical in environments where copiers have traditionally been purchased, installed and operated by individual business units, or by a centralized purchasing department rather than by an IT department. The days when copiers could be considered 'stationary supplies' are long over.

A good security policy should clearly and concisely state what must be done to protect information on computers and networks. It should define, in writing, what is expected of users, what is to be protected, how it will be protected and who is responsible.

With regard to network printers, the policy should include guidelines about which staff may access the device over the network, and for what purposes. Procedures should designate which LAN segments printer copiers may be attached to, and which ports should be screened by firewalls and filtering routers. It is important to ensure that passwords are changed from their default values and that an IT system administrator is responsible for changing and distributing those passwords. The policy should include procedures for verifying the identity of outside service personnel to avoid social engineering or impersonation attacks. Updates to the printer's software should be scheduled on a regular basis.

Conclusion

Only a few years ago, printers were considered to be dumb peripherals, and photocopiers were not even within the realm of information technology departments. Today, however, these fully networked devices are common on corporate LANs and have many of the capabilities, and security vulnerabilities commonly found in servers.

My investigation of the Minolta Di251 network printer and its Pi3502 controller have shown a number of insecurities. The default administrative passwords are contained in easily available manuals. Using these passwords, the device can be reconfigured via telnet or the web. The printer's ftp port will always accept print jobs, and the default password cannot be changed. The printer's web page

reveals a wealth of information about the printer and the network it is connected to as well as details of print jobs. Even more detailed information is available via SNMP using the well known default community strings and network configuration can be altered. There is no means of changing these SNMP community strings. The printer is subject to a number of Denial of service attacks via http and ftp and could be used to cause a wider DOS on the network. Finally, the confidentiality of any print job sent over the network unencrypted can be compromised by common sniffing tools and techniques.

Mitigating these threats is no easy task. Not surprisingly, fully featured network printers must be defended using the same principals as fully fledged servers, that is, defense in depth. A security policy should clearly state who may access the printer and why. Unneeded services and protocols should be disabled. All software should be kept up to date. The printer must be screened by firewalls and routers.

While I've been looking specifically at the Minolta Di251, many of the aforementioned suggestions would also apply to other networked printers.
I hope that I have demonstrated the often overlooked security risks presented by network printers and shown that administrators responsible for network security must consider these devices as multifunction servers hosting many services rather than the mere office supplies they once were.

Glossary

DOS - Denial of Service
FIN scan - a stealthier port scanning technique, used because most firewalls will block SYN packets
ipp - internet printing protocol – allows print jobs to be directed to an ipp:// URL. Described in RFCs 2569 and 3510 et al.
lpr - standard unix line printer service
MIB-II - Management Information Base - a database of information accessible through SNMP - described in RFC 1213
OID - Object Identifier - a numeric string identifying one element in an SNMP MIB
Pi3502 - network controller card with NIC, used on Minolta Di251 printers
SMTP - Simple Mail Transfer Protocol - described in RFC 821
SNMP - Simple Network Management Protocol - described in RFC 1157
SRVLOC - NetWare Service Locater Protocol
SYN scan - A scan where SYN packets are sent to each port to try to elicit a response

References

Bugtraq Computer Security Mailing List. http://www.securityfocus.com/archive/1 (10 January 2004).

Cole, E. Fossen, J. Northcutt, S. Pomeranz, H. SANS Security Essentials with CISP CBK: Version 2.1. Bethesda, MD : SANS PRESS, 2003.

Daniels Thomas E, Kuperman Benjamin A, Spafford Eugene K. "Penetration Analysis of a XEROX Docucentre DC 230ST". October 2000. http://csrc.ncsl.nist.gov/nissc/2000/proceedings/papers/034.pdf (10 January 2004).

Duchemin, Gregory. "Nashuatec printer, 3 vulnerabilities found." 14 October 1999. http://seclists.org/lists/bugtraq/1999/Oct/0166.html (12 January 2004).

Ebay. http://www.ebay.com/ (9 January 2004).

Ethereal packet sniffer. Ver 0.96-1. http://www.ethereal.com/ (10 January 2004).

Ettercap packet sniffer. http://ettercap.sourceforge.net/ (11 January 2004).

Garrard, David. "A Security Assessment of the Ricoh Afcio 450E Multifunction Device." Version 1.0. 9th July 2003.

http://www.sans.org/rr/papers/index.php?id-1211 (9 January 2004).

Google search engine. http://www.google.ca/ (10 January 2004).

Khan, Mir Moosa. "Jetdirect Network Printers Security." 21 September 2003. http://www.giac.org/practical/GSEC/Mir_MoosaKhan_GSEC.pdf (12 January 2004).

Minolta Co. Ltd. 1 "Di200/Di251/Di351 Operator's Manual." 2000. http://bpg.minoltausa.com/eprise/main/minoltaUSA/MUSAbpg/support_center/Manuals/resultsmanual?ProductCat=b&w+printers/copiers&Product=Di251&x=17&y=6 (12 January 2004).

Minolta Co. Ltd. 2 Pi3502 for Di200/Di251/Di351/Di200f/Di251f/Di351f (Di200, Di200f: U.S.A. And Canada only) Service Manual. Osaka, Japan: Minolta, 2001.

Minolta Co. Ltd. 3 "Network Interface Card for Pi3502 Operator Manual." 2001. http://bpg.minoltausa.com/eprise/main/MinoltaUSA/MUSABPG/Showroom/ProductModels/4012-311?infotype=Software (10 January 2004).

Mitre Common Vulnerabilities and Exposure Database. http://www.cve.mitre.org/cve (10 January 2004).

Nessus vulnerability scanner. Version 2.0.9. http://www.nessus.org/ (10 January 2004).

Netsec [davidv]. "Hardware Exploit - Gets network Down." 01 June 2000. http://archives.neohapsis.com/archives/ntbugtraq/2000-q2/0223.html/ (10 January 2004).

Net-SNMP tools. http://www.net-snmp.org/ (12 January 2004).

Nikto vulnerability scanner. Ver 1.32. http://www.cirt.net/code/nikto.shtml/ (12 January 2004).

Nmap port scanner. Ver 3.00. http://www.insecure.org/nmap (9 January 2004).

Orvis William J, Van Lehm Allan L. "Data Security Vulnerabilities of Facsimile Machines and Digital Copiers". January 1995. http://www.ciac.org/ciac/documents/CIAC-2304_Vulnerabilities_of_Facsimilie_Machines_and_Digital_Copiers.pdf (12 January 2004).

Packetstorm. http://www.packetstormsecurity.nl/ (10 January 2004).

Rekhter, Y. Moskowitz, B. Karrenberg, D. deGroot, G. J. Lear, E. "RFC 1918 -

Address Allocation for Private Internets." February 1996. http://www.faqs.org/rfcs/rfc1918.html (19 January 2004).

Rose, Marshall. The simple book : an introduction to networking management. Upper Saddle River, NJ : Prentice Hall PTR, c1996.

Shah, Saumil. "An Introduction to HTTP Fingerprinting". 30th, November 2003. http://www.blackhat.com/presentations/bh-asia-03/bh-asia-03-shah/shah-httprint_paper.pdfhttp://www.blackhat.com/presentations/bh-asia-03/bh-asia-03-shah/shah-httprint_paper.pdf (12 January 2004).

Smith Kevin K. "Do you copy? Security issues with Digital copiers". 16 September 2000. http://www.giac.org/practical/Kevin_Smith_GSEC.DOC (12 January 2004).

X-Force Security Advisories. http://xforce.iss.net/xforce/search.php (10 January 2004).