Global Information Assurance Certification Paper

Mir Moosa Khan
SANS GSEC Practical Assignment Version 1.4 (b)
21 September 2003

Jetdirect Network Printers Security

ABSTRACT: In this paper I will describe Jetdirect Network Printer Security including various protocols used for printing. The main focus is on Jetdirect cards used by various models Hewlett Packard (HP) printers. The Jetdirect printers come embedded with print servers and web servers with administration capabilities. We will further explore the details of the protocols used, their potential exploits, and the configuration options used to tighten security for the Jetdirect printers.
In this paper I investigated three different Jetdirect cards with different firmware versions checking their features, default configuration and the various services. I examined the vulnerability of various services, the configuration options and the related security issues.

Overview

Printers are extensively used in many organizations. Until recently printers used to be connected using serial cables on standalone computers and with the advent of networking printers were connected to computer acting as print servers using serial connections to connect to printers. These days the print servers are embedded in the printers or are available as add on feature using a print server card and can be connected directly to the network. With the popularity of the TCP/IP protocol and the Internet, printers are available with TCP/IP support using embedded web servers and other protocols like FTP, telnet, LDP and IPP. The computer print server, using operating systems like Windows 2000, Linux and Unix connects to the printers typically using TCP/IP over Ethernet.

The internet enabled printers have the advantage that they can be managed from any location using a web browser and it also means that people can print from anywhere in the Wide Area Network using the Internet printing protocol (IPP) and other routable protocols like IPX/SPX. In this paper the security implication, of the Jetdirect line of cards from HP, for the enterprise is evaluated in detail.

The Jetdirect cards are used in various printer models of HP. I have investigated the three different Jetdirect cards J3113A used in HP LaserJet printer 4500 using Firmware: G.08.32, HP J4169A using Firmware Version: L.21.11 for HP LaserJet printer 9100 and HP J6057A for HP LaserJet 4600 using Firmware Version: R.22.09**.** The Jetdirect cards have different features based on Jetdirect model number and firmware version.

Active Ports and services that can be used by the Jetdirect print servers for various printing and management services

I performed port scanning on the printers (1) and used NetLab 1.4 for scanning the printers. The result of a ports scan revealed the following ports as active. I tested various methods for evaluating the ports and services

FTP: Port 21. FTP is a basic TCP/IP utility used to transfer files. FTP is used to send print files from clients to Jetdirect printers. The printers come with ftp server running on by default. I logged in the ftp server using a command line ftp client in Solaris. It asked for a username, but accepted anonymous login. It recommended an email address as password. It even gave the instructions on how to print files. I tested this on the three printers and it allowed me to enter all of them. The directory listing command showed me a public directory and the printers had only one port port1. Using Internet Explorer 6.0 I could log in to the print servers using FTP://IP address of printer print files. The files can be printed in TEXT or RAW mode. Files using ASCII text will print out fine, but a wrong type of file like Microsoft Word document will lead the printer to print many papers with garbage output.

The FTP server in the printers is a stripped down version of FTP and does not let the users create folders. Also it does not allow users to make use of some commands like “rename”, even though the commands are listed when you type help. If a user tries to use such a command, an error message of “command unrecognized or unimplemented” shows up.

Telnet: Port 23. Telnet is a TCP/IP based protocol and is widely used to connect to remote devices using the concept of “Network Virtual Terminal” (2). In Jetdirect printers telnet is used to view or change the printer configuration and other relevant information.

HTTP: Port 80. Hyper Text Transfer Protocol (HTTP) uses TCP/IP to connect to web servers. The Jetdirect cards I tested came with embedded web servers. The web servers can be used to configure and view the printer status. The other convenient features were the viewing of printer supplies status like the amount of INK in the printer cartridges and the message being displayed on the printer screen like paper jams etc. Printer logs can also be viewed from a web browser.

HTTP-MGMT: Port 280 this port is used by HTTP Management Transport Control Protocol (3). This port is used for HTTP management and can be used by programs to find out HTTP managed devices. This port is used to access the same content as on the default port 80 for HTTP and does not use managed and unmanaged content separately on different ports.

HTTPS: Port 443 Hypertext Transfer Protocol Secure. HTTPS is a used to communicate information over the World Wide Web using secure communications. HTTPS uses HTTP with secure socket layer (SSL). The latest

models of Jetdirect can use HTTPS for transfer of information from the embedded print server to the client. It allows for the self-generation of a SSL certificate and even gives the option of selecting the security key size for the Secure Socket Layer certificate. The embedded web server becomes secure server.

LPD: Port 515. Line Printer (4) Daemon Protocol commonly known as LPD and thoroughly defined in RFC1179 runs on port 515. LPR is commonly used by many operation systems to print through the network including Unix and Linux.

IPP: Port 631. The Internet Printing Protocol IPP uses this port. IPP is defined many rfc's including rfc2567 (5). IPP uses TCP/IP stack of protocols and allows people to print from anywhere to the printer using port 631. The newer versions of operating systems like windows 2000, Windows XP and Linux support IPP. Linux uses a software CUPS for connecting to printers using IPP.

Port 9100: The Jetdirect printer uses port 9100 for printing. Users can send RAW postscript files and have their contents printed on the printers. As 9100 is an unprivileged port (above port number 1024) it allows any user to connect and print bypassing the accounting methods if any have been set up. In the version J6057 the user has the option of setting up other raw ports.

SLP Service Location Protocol is can be used by the Jetdirect printers. It can be used to discover printer devices on the network. SLP advertises its presence and can be used for printer discovery.

Simple Network Management Protocol (SNMP). SNMP is used to manage networks. SNMP uses community names (passwords)to read anmd write information to devices. SNMP set community name is the password able to write information and gets community name is used to read information on the HP Jetdirect Print Server. A community name can be up to 255 characters long. Different card use different version of SNMP

DHCP/TFTP Jetdirect J6057A allows for the configuration of the print server using a Dynamic host configuration protocol (DHCP) and Trivial File Transfer Protocol (TFTP). DHCP allows for the dynamic setting of the IP address. This is the default behavior which means that the Jetdirect server when it is not manually configured with an IP address comes up on the network ad starts sending Address resolution protocol requests looking for a DHCP server to assign it an IP address. The Jetdirect card can also be configured using a TFTP server. The TFTP server serves a configuration file with all the required parameters to the Jetdirect print server.

Vulnerabilities and limitations of various protocols and services used by Jetdirect cards

FTP: FTP is widely used on the Internet. There are limitations to this. One such limitation is that FTP is enabled by default and can be used from anywhere to

print. The down side is that there is no password protection for FTP connectivity, which means it allows every user to connect. Users may mistakenly or maliciously print large files on the printer. They may also be able to bypass any printer logging which has been enabled or have the printer print large amount of garbage. In my test, using Internet Explorer 6 on Windows, I connected using FTP to a printer and printed a small PDF file of 6 pages. It printed out more than a hundred pages of garbage characters using only the first few lines of the pages.

Sample FTP connection to a Jetdirect printer called white
FTP white
Connected to white
220 JD FTP Server Ready
User :(none)): m
331 Username Ok, send identity (email address) as password.
Password:
230-Hewlett-Packard FTP Print Server Version 2.0
Directory: Description:

PORT1 Print to port 1 HP LaserJet 9000 Series

To print a file, use the command: put <filename> [portx]
or 'cd' to a desired port and use: put <filename>.

Ready to print to PORT1
230 User logged in.

Telnet: By default the printers have telnet enabled and did not have any password set but had a configuration option to have password enabled. Telnet protocol uses clear text to communicate with the server, which means anyone using tools like sniffer can sniff the passwords. It is an insecure way of communicating. This vulnerability is not specific to printers but the weakness of the telnet protocol

HTTP: HTTP transmits information in clear text. In HTTP, the passwords can easily be sniffed as there is no encryption. The embedded web server provides useful features for configuring the printers, but on the previous model J3113A there is no username and password required to view the printer configuration. This vulnerability allows anyone to access the printer configuration administration console. The password or SNMP community string is required to change the information. The configuration setting provides important information about the network like gateway, subnet mask, total packets received and broadcast packets received etc. This information should be only available to authorized users, and not to everyone. This is especially important when the printer is connected to the internet without a firewall. Another potential risk is that the information from the embedded web server may be cached on search engines as

they crawl the web and may continue giving away valuable network information even after the printer has been decommissioned.

HTTPS: The Jetdirect embedded web server on the latest model J6057A allows the administrator to enable secure transactions.

SNMP (6) The default SNMP get setting is public which allows everyone to view it. However, Jetdirect card J6057A allows for the use of SNMP version 3, which is more secure.

IPP Print jobs can be dumped on the IPP port and clients can connect remotely without any accounting. IPP has been in production since the past few years and many vulnerabilities are being discovered in the many implementation of IPP (11).

9100 The Jetdirect printers use a non-privileged port of 9100 as default and it can be used by anyone to dump print jobs. This port number can be changed with the later cards.

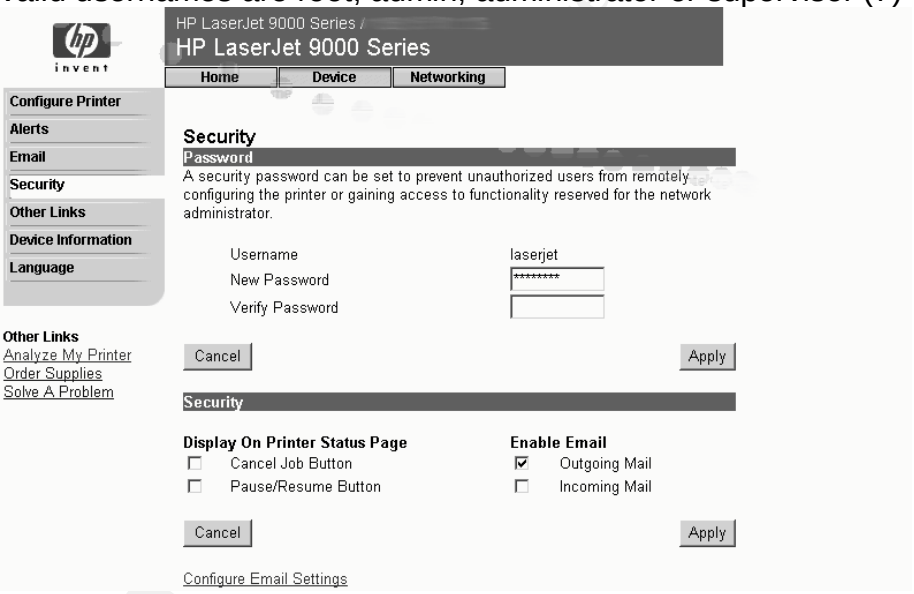
DHCP Jetdirect print servers act as DHCP clients out of the box. A DHCP server can assign the Jetdirect print server an IP address. As soon as an IP address is assigned the printer is on the network. In networks without proper firewall protection, it will lead the out of the box printer to be connected on the network with many services open like FTP with anonymous login, telnet without a password and the embedded web server being accessible.

Configuration Options

The following are the steps to configure and secure a Jetdirect J4169A printer card using a web browser.

- IP configuration should be manual and a printer should be given a static address rather than getting it from DHCP.
- Set Hostname: It should be assigned using uppercase. It is also known as printer name
- Set IP address subnet mask and default gateway
- Domain Name
- Primary and Secondary WINS server. IP address of Primary and secondary WINS servers this is useful when printers communicate with Microsoft Windows network over the network. This allows the printer to be registered in the WINS database
- SYSLOG server. IP address of the SYSLOG server. It will allow the printer messages to be logged at a centralized syslog server. The logged messages should be periodically checked
- SET banner to be disabled or enabled according to your preference
- IPX, APPLETALK and DLC/LLC should be disabled if not being used
- Disable FTP through telnet, using the command sequence: ftp-config: 0

- Set SNMP set community name and get community name. These to be used like passwords. The set community name allows programs like Jetadmin to make changes to the printer configuration and the get community name allows the printer configuration to be viewed
- Set Access control to the print servers (based on your configurations). This allows only the listed IP address to communicate with the printers. There is a option to bypass access control list for http. Using telnet to allow networks use the command allow: <IP address> <subnet mask> to allow individual IP addresses allow: <individual IP address>. You can check your entries using allow: List. If you made a mistake use the command allow:0
- Set DNS server IP address
- Set location and contact information. This information should be set if needed and with web based interfaces with no access restriction it gives out information like physical location and administrator name if used.
- Set and confirm Admin password it can be up to 16 characters long. The newer releases of Jetdirect ask for a username when using telnet and the valid usernames are root, admin, administrator or supervisor (7)



- Set Other Setings and check the protocols used for printing from SLP config 9100 printing, LPD printing, Telnet Config, FTP printing, IPP printing and disable what will not be used.
- Dynamic Raw Port setting can be used to open up another port from 3000 to 9000 for printing (7)
- Outgoing Mail This can be set to send alerts to an email address. The various alerts that can be set are for supplies and service related alerts
- Incoming email. This feature can be enabled to send printer commands to the printer.

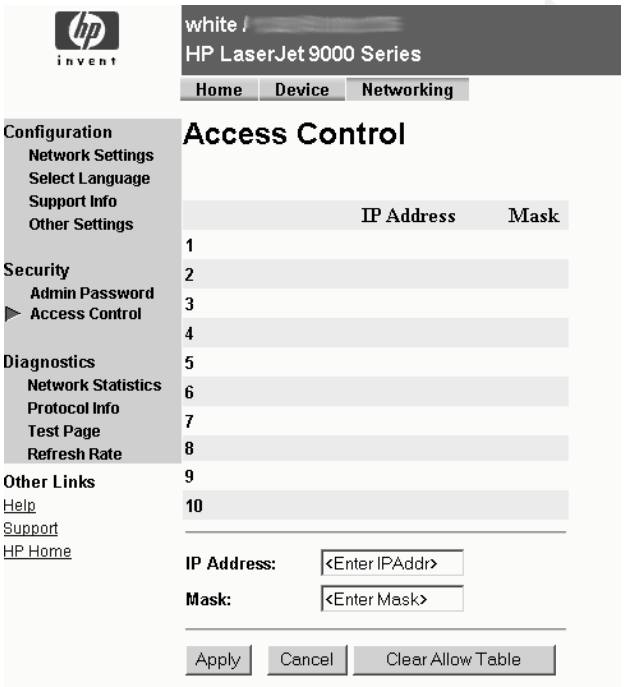
LaserJet Printers can also be configured using telnet Jetadmin and Web Jetadmin. When you telnet to the machine question mark (?) Can be used for help and slash (/)can be used for viewing the current configuration.

Sample Telnet Configeration options
===JetDirect Telnet Configuration===
HP JetDirect : J4169A
Firmware Version : L.21.11
Manufacturing ID : 41164116902007
Hardware Address : 00:01:E6:3F:CA:FD
System Up Time : 418:47:40

MAIN MENU
---
1. General Settings
2. TCP/IP Menu
3. SNMP Menu
4. IPX/SPX Settings
5. AppleTalk Settings
6. DLC/LLC Settings
7. Other Settings
8. Support Settings
9. Help
0. Exit

Default security on Jetdirect
The default settings on Jetdirect printers have been to keep all the features least restrictive by default. The full set of open default features allows the printers to be easily connected to all possible devices without requiring to enable any services but allows no security for a printer.
TCP/IP. The printer has no IP address. By default the printer tries to get an IP address using BOOTP or DHCP. Once and IP is assigned the printer is on the network. For the J3113A there is no default password.
The telnet prompt does not even ask for a password and the telnet connection just lets a user log in and change the configuration.
FTP is enabled by default, which means anyone can FTP to the machine without a password
SNMP setting for get is set to Public which is a very well known SNMP community name and will allow anyone access. It is like using password that everyone knows for securing a device.
The web Interface of J3113A allows everyone to who can access the printers to view the printer configuration. Jetdirect printers can be paused and jobs deleted from a web interface and allowing everyone access without any restrictions to this interface will lead to potential problems. IPX/SPX, AppleTalk, and IPP printing is enabled by default.

Security Issues

- Disable FTP or use access control lists to limit connections if used by a set of servers.
- Allow only the services used and disable the unused services. Users may disable FTP, IPP, SLP, and change the default port from 9100 to another port within range of 3000 to 9000 to be most secure
- Do not put a printer on the network before configuring all the options and disabling Telnet or Web access as planned. (8)
- Telnet Passwords should be long and complicated including numbers and special characters. Telnet access may be disabled through the embedded web server. Telnet password can be up to 16 characters long but the telnet protocol s not secure.
- The HP LaserJet Model J4169A was found vulnerable for DNS resolver (9) which makes the printers vulnerable to potential denial of service attacks and unauthorized access
- Limit the Access Control list to the print servers. Aces control allows up to 10 host systems or networks of host systems access to the HP Jetdirect print server.
- 

- Access lists do not check host systems that use HTTP (embedded web server or using IPP) by default. It can be disabled through the embedded web server
- SNMP get and set stings are to be treated like passwords and commonly used default names like public for get and private for set should be avoided. The default SNMP get community name is public. If public is disabled some utilities may not work properly (10). The SNMP protocol version 1 and 2 have been found to contain some vulnerabilities

- Treat your printer like a network device and keep them behind the firewall
- Some Jetdirect printers like J4169 allow the lock the printer control panel so that everyone cannot make changes
- Disable printer reset. Clearing the settings through cold reset of the printer will bring up the factory default settings and clear all the passwords and settings.

Conclusion

Individuals and organizations can benefit from this paper as it will lead them to a better understanding of printer security in general and Jetdirect printers in particular. With the latest printers having built in print servers that can communicate with all the clients directly. In today's network environment computer print servers using LINUX or Windows 2000 connect to Jetdirect as clients for printing control and accounting purposes.

Users view printers as limited capability hardware devices capable of just printing and communicating only with the print servers and are unaware of all the advanced capabilities which the printers have built into them and as new models are released more features are being built into them. Printer administrators should be checking all the features of a printer before deploying it in the network as the printer model may remain the same but a different firmware will mean a host of different features. With the increase in the awareness of your printers capabilities and settings will lead to better understanding of your network security

I was able to increase my own network security after running the port scan on my printers I disabled the FTP ports as they were open but were not used by anyone. I also disabled the protocols, which my organization was not using IPX/SPX and AppleTalk.. Therefore it is important to have a standard printer communication strategy based on the organizations network design and needs.

Sample Jetdirect printer configuration viewed through telnet

```
Enter username: admin
Enter password:

Please type "menu" for the MENU system,
or "?" for help, or "/" for current settings.
> /
  ===JetDirect Telnet Configuration===
  HP JetDirect     : J4169A
  Firmware Version : L.21.11
  Manufacturing ID : 41164116902007
  Hardware Address : 00:01:E6:3F:CA:FD
  System Up Time   : 418:35:09

    GENERAL_____________________________________
    Admin Password   : Specified
    System Location  : Not Specified
    System Contact   : Moosa Khan

    TCP/IP MAIN_________________________________
    Host Name        : white
    IP Config Method : USER SPECIFIED
    IP Address       : 10.1.101.126
    Subnet Mask      : 255.255.255.0
    Default Gateway  : 10.1.101.254
    Config Server    : Not Specified      (Read-Only)
    TFTP Server      : Not Specified      (Read-Only)
    TFTP Filename    : Not Specified      (Read-Only)
    Domain Name      :                    DNS Server       :
10.1.100.4
    Pri WINS Server  : 10.1.108.11
    Sec WINS Server  : 10.1.109.99

    TCP/IP PRINT OPTIONS________________________
    9100 Printing    : Enabled
    FTP Printing     : Disabled
    IPP Printing     : Disabled
    LPD Printing     : Enabled
    LPD Banner Page  : Enabled

    TCP/IP RAW PRINT PORTS______________________
    Raw print port   :
    Raw print port[1]: 9000

    TCP/IP ACCESS CONTROL_______________________
```

Allow :

TCP/IP OTHER_____
Syslog Config : Enabled
Syslog Server : 10.1.100.94
Syslog MaxMsg/Min: 10
Syslog Priority : 7 SLP Config :
Disabled
TTL/SLP : 4 Hops
Idle Timeout : 3600 Seconds
Telnet Timeout : 900 Seconds
Cold Reset : Disabled
EWS Config : Enabled
TCP MSS : 0
Local Subnets : 0

SNMP_____
SNMP Config : Enabled
Get Cmnty Name : Specified
Set Cmnty Name : Specified

SNMP TRAPS_____
Authenticatn Trap: Enabled
Trap Destination :

IPX/SPX_____
IPX/SPX Config : Disabled
Print Server Name: NPI3FCAFD
Address : 0.0001E63FCAFD (Read-Only)
Frame Type : AUTO SAP Interval
: 60 Seconds
Mode : NONE (Read-Only)

NDS Tree Name : Not Specified
NDS Context : Not Specified
Job Poll Interval: 2 Seconds
PJL Banner Pages : Disabled
PJL End-Of-Job No: Disabled
PJL Toner Low : Disabled

APPLETALK_____
AppleTalk Config : Enabled
Device Name : HP LaserJet 9000 Series (Read-Only)
Zone : * (Read-Only)
Print Type 1 : HP LaserJet (Read-Only)
Print Type 2 : LaserWriter (Read-Only)

Print Type 3 : Not Specified (Read-Only)
Phase : 2 (Read-Only)
Status : Ready (Read-Only)

DLC/LLC_____
DLC/LLC Config : Enabled

OTHER_____
Panic Behavior : DUMP_AND_HALT

SUPPORT_____
Support Name : Not Specified
Support Number : Not Specified
Support URL : http://www.hp.com/go/jetdirect
Tech Support URL : http://www.hp.com/go/support

Refrences

(1)Cole Eric, Fossen Jason, Northcut Stepehen, Pomeranz Hal, “Sans Security Essentials” Sans Press Page 680

(2) Postel J, Reynolds J, "Request for Comments: 854" TELNET PROTOCOL SPECIFICATION May 1983
http://www.scit.wlv.ac.uk/rfc/rfc8xx/RFC854.html
(21 September 2003)

(3) Harrison Brian, Mellquist Peter E., Pell Adrian. "Web Based System and Network Management (Internet Draft)" November 18, 1996 URL:
http://www.watersprings.org/pub/id/draft-mellquist-web-sys-01.txt
(21 September 2003)

(4) McLaughlin III, Leo J. "Request for Comments: 1179" Line Printer Daemon Protocol August 1990 URL:
http://www.ietf.org/rfc/rfc1179.txt
(21 September 2003)

(5) Wright F.D. "Request for Comments: 2567" Design Goals for an Internet Printing Protocol, April 1999 URL:
http://ietf.org/rfc/rfc2567.txt?number=2567
(21 September 2003)

(6) Pechler Sven "HP Jetdirect SNMP password vulnerability when using Web JetAdmin" 4th Mar 2003 URL:
http://www.securitybugware.org/Other/6036.html
(21 September 2003)

(7) HP Jetdirect Administrators Guide Edition 2, August 2003 URL:
http://h20000.www2.hp.com/bc/docs/support/SupportManual/bpj07646/bpj07646.pdf
(21 September 2003)

(8) HP support Document “Making HP Jetdirect Print Servers Secure on a Network“ URL:
http://www.hp.com/cposupport/networking/support_doc/bpj05999.html
(21 September 2003)

(9) HEWLETT-PACKARD COMPANY "SECURITY BULLETIN: HPSBUX0209-218" SSRT2345 Security Vulnerability in DNS Resolvers for HP Peripherals (rev.1) 14 April 2003 URL:
https://www.auscert.org.au/render.html?it=2981&cid=1
(21 September 2003)

(10) Middleton, James. "SNMP exploit bugs HP printers" 20 February 002 URL: http://www.infomaticsonline.co.uk/News/1129369
(21 September 2003)

(11) Amore, Phil. "CUPS: vulnerability in the CUPS IPP implementation" May 27, 2003
http://lwn.net/Articles/33772/
(21 September 2003)