How to Secure Network Printers?

IT Security Office
June 7, 2006

Agenda

- Printer History & Statistics
- The problem with Network Printers
- Tools for managing network printers
- How to secure your printers
- What can the Security Office do to help you secure your printers?
- Questions?

Printer History & Statistics

- What are printers suppose to do?
  - Dumb printers
- Serial/Parallel Printer
  - Locally attached printers
  - Local printer sharing
  - Printer Programming Languages (PostScript, Printer Command Line and Printer Job Language)

Printer History & Statistics

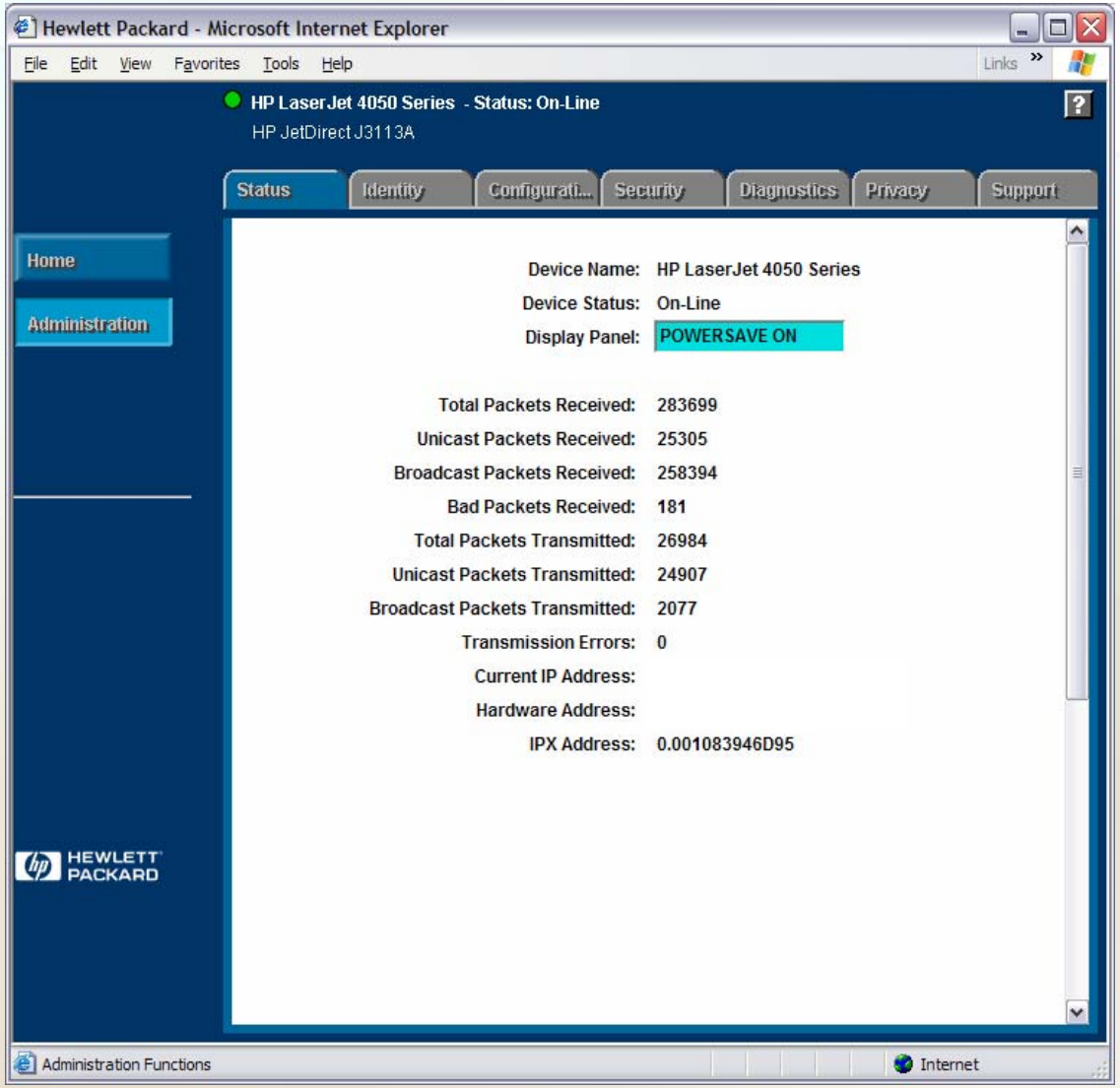
- Network Printers
  - Printing through Print Servers
  - Direct Printing
- Network Printers @ UI
  - 1484 Network Printers
  - 1184 HP Printers
  - 71 low toner cartridge
  - 20 order new cartridge
  - 10 empty tray
  - 3 paper jams
  - Longest Uptime: 285 days, 06:46:36.60
  - 112 printers with ACLs
  - 33 printers with syslog servers

The Problem with Network Printers

- Physical Security
- Embedded Devices
- Unauthenticated Remote Access
- Print Job Forwarding
- Print Job Notification & Printer Logs
- RAM Disks and Filesystems

Tools for managing Network Printers

- Front Panel
- Web browser
- CLI
- SNMP
- HP Jet Direct
- HP Web Admin
- HP DownLoad Manager



How to Secure your printers

- HPs Recommendation for securing network printers

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj05999

  - Security Step 1 - Upgrade the HP Jetdirect firmware
  - Security Step 2 - Specify a telnet password
  - Security Step 3 - Disable all unused protocols
  - Security Step 4 - Disable all unused print and management services
  - Security Step 5 - Specify an SNMP set community name
  - Security Step 6 - Specify an access control list

How to Secure your printers

- Obtain information about your printer

  >telnet 128.255.x.x or http://128.255.x.x

HP JetDirect
Please type "?" for HELP, or "/" for current settings
>
  ===JetDirect Telnet Configuration===
      Firmware Rev.   : G.08.49
      MAC Address   : 00:10:83:xx:xx:xx
      Config By   : USER SPECIFIED

      IP Address   : 128.255.x.x
      Subnet Mask   : 255.255.255.0
      Default Gateway : 128.255.x.x
      Syslog Server   : Not Specified
      Idle Timeout   : 90 Seconds
      Set Cmnty Name : public

Host Name   : Printer1
Default Get Cmnty : Enabled
DHCP Config   : Disabled
Passwd   : Disabled
IPX/SPX   : Enabled
DLC/LLC   : Enabled
Ethertalk   : Enabled
Banner page   : Enabled

How to Secure your printers

- Set a password

  >passwd

  Enter Password [16 character max.; 0 to disable]:

  >

- Set a static IP address

  >dhcp-config: 0

  >ip: 128.255.x.x

  >subnet-mask: 255.255.255.0

  >default-gw: 128.255.x.x

- Set hostname

  >host-name: PRINTER1

How to Secure your printers

- Disable unused protocols
  - IPX, DLC/LLC, LPR, AppleTalk, JetDirect, etc.

```
>ipp-printing:      0 to disable, 1 to enable (TCP port 631)
>ftp-printing:      0 to disable, 1 to enable (TCP port 20, 21)
>ftp-config:        0 to disable, 1 to enable (TCP port 20, 21)
>lpd-printing:      0 to disable, 1 to enable (TCP port 515)
>9100-printing:     0 to disable, 1 to enable (TCP port 9100)
>slp-config:        0 to disable, 1 to enable (UDP port 427)
>ipx/spx:           0 to disable, 1 to enable
>dlc/llc:           0 to disable, 1 to enable
>ethertalk:         0 to disable, 1 to enable
```

How to Secure your printers

- Disable unused services
  - HTTP management
    - >ews-config:0 to disable, 1 to enable
- Enable SSL State for Web Management

  >ssl-state: 1 to enable redirection, 2 to disable redirection

How to Secure your printers

- Change the default community string

  >set-cmnty-name: secure-string

  (32 characters max)

  >default-get-cmnty: 0 to disable, 1 to enable

- Disable SNMP

  >snmp-config: 0 to disable, 1 to enable

Note: JetDirect will not respond to any remote access via the network requiring community strings for communication (ex. JetAdmin, WebJet, HP DownLoad Manager)

How to Secure your printers

- Configure Syslog
  - Enable Syslog Server

    >syslog-svr: 128.255.x.x
  - Configure Maximum messages per min.

    >syslog-max: integer 1..1000, 0 to disable
  - Configure Syslog Priority

    >syslog-priority: integer (0 .. 7), 8 to disable

How to Secure your printers

- Configure Access Control List (ACL)
  - Restricts access to telnet/www/ftp/printing
  - Single host or maskable network range
  - Maximum of 10 ACLs
  - Examples

    >allow: list (displays current ACLs)

    >allow: 128.255.1.1

    >allow: 128.255.1.0 255.255.255.0

    >allow: 0 (clears all ACLs)

How to Secure your printers

HP JetDirect

Please type "?" for HELP, or "/" for current settings
>

To Change/Configure Parameters Enter:
Parameter-name: value <Carriage Return>

Parameter-name Type of value
ip: IP-address in dotted notation
subnet-mask: address in dotted notation (enter 0 for default)
default-gw: address in dotted notation (enter 0 for default)
syslog-svr: address in dotted notation (enter 0 for default)
idle-timeout: seconds in integers
set-cmnty-name: alpha-numeric string (32 chars max)
default-get-cmnty: 0 to disable, 1 to enable
host-name: alpha-numeric string (upper case only, 32 chars max)
dhcp-config: 0 to disable, 1 to enable
allow: <ip> [mask] (0 to clear, list to display, 10 max)

addrawport: <TCP port num> (<TCP port num> 3000-9000)
deleterawport: <TCP port num>
listrawport: (No parameter required)

addstring: <name> <contents>
contents - For non-printable characters use \xx for two digit hex number
deletestring: <name>
liststring: (No parameter required)
addq: <name> [prepend] [append] [processing]
prepend - The prepend string name
append - The append string name
Use NULL for no string
processing - RAW, TEXT, or AUTO
deleteq: <name>
listq: (No parameter required)
defaultq: <name>

ipx/spx: 0 to disable, 1 to enable
dlc/llc: 0 to disable, 1 to enable
ethertalk: 0 to disable, 1 to enable
banner: 0 to disable, 1 to enable

Type passwd to change the password.

Type "?" for HELP, "/" for current settings or "quit" to save-and-exit.
Or type "exit" to exit without saving configuration parameter entries
>

What can the Security Office do to help you secure your printers?

- Scan for printers in your domain
- Test the security of the printers
- Help with ACL configuration

Questions?

Thank You!