Global Information Assurance Certification Paper

Securing Embedded Network Devices
Doug Felteau
GSEC v1.4b Option 1
February 23, 2003

1 Abstract

Systems administrators should approach security for embedded network devices (ENDs) with the same mindset as they approach security for a network server; after all, these devices contain embedded operating systems, network connectivity and embedded servers.

Manufacturers of these ENDs do not always design the products with security in mind, which leads to design failures.[1] Also, people or organizations deploying these devices often overlook security because of misconceptions about the devices, lack of time or money to configure them correctly and/or lack of knowledge on how to properly secure them. This paper will describe the problems related to unprotected ENDs and will reveal the steps to secure them. HP holds the number one spot in printing and imaging in the world and enjoys over fifty percent of the market share in networked printers; therefore, this paper will apply the universal steps of securing ENDs to HP networked printers. [2]

2 What is an Embedded Network Device?

ENDs are systems with network connectivity that feature a processor with memory and/or disk space and an operating system which often features a web server. These special purpose devices are usually limited to specific functionality. Some common examples of embedded network systems include switches and routers. Other examples often overlooked are networked printers and copiers. Internet-enabled coffee machines and refrigerators, Sony Playstation 2's with Network Adaptors and MP3 networked receivers are examples of some uncommon ENDs.[3] In a press release Hewlett Packard (HP) referred to a research report titled "IDC Internet Commerce Market Model Version 6.3" which stated that an estimated thirty-five percent of devices on the Internet will be non-PC based by the year 2004.[4] As more of these devices are deployed on networks, additional vulnerabilities and exploits will be discovered which will require protection.

3 Why do embedded network devices need to be secured?

There are many misconceptions related to securing ENDs. For instance, in speaking with a colleague about the subject of this paper, he inquired if there was anything worse a hacker could do than reboot the device. His statement

indicates his lack of knowledge regarding the security threat to these devices. One mistaken belief is that ENDs are harder to exploit than regular computers with multipurpose operating systems. Also, a fallacy exists that since these devices do not have shells, useful shell code cannot be created to exploit them. Another false impression involves the concept of defense by obscurity. People erroneously believe that since these devices contain undocumented addressing and elements, creating exploits is nearly impossible.[1] Network administrators that believe these common misconceptions continue to deploy millions of these devices every year without properly securing them.

ENDs share design and software vulnerabilities with common desktop systems. Many devices contain backdoors or automatically turn on insecure protocols and services. Also, standards are sometimes ignored or altered. These systems can contain several different administrative access methods as well as inconsistent access restrictions. Due to the various access restrictions and methods, sometimes a new feature accidentally circumvents the security checks the device employs.[1] In fact, as a result of the devices containing network services such as embedded FTP servers, telnet servers and web servers, they are more similar to servers than common desktop systems.

As of the writing of this paper, there are ten known vulnerabilities noted in the Common Vulnerabilities and Exposures dictionary for HP networked printers.[5] Using one of these vulnerabilities, any deployed unsecured HP networked printer can be compromised and turned into a reconnaissance or attack platform.

Security relies on three principles: confidentiality, integrity, and availability. Confidentiality ensures that information is not disclosed to unauthorized individuals, programs or processes. Integrity ensures that data has been protected against modification and is complete. Availability guarantees that a resource is available to users when needed.[6]

HP networked printers store print jobs in a spool area located in memory. There is a tool that allows a user access to this spool area which could compromise the confidentiality of that data. Integrity would be breached if a user accessed that spool area, downloaded the document to be printed, modified, and uploaded that file back to the spool directory of the printer. The hacked version of the document would print instead of the original.

ENDs tend to have limited resources and do not always perform full sanity checks. Sanity checks validate input and make sure the data is consistent with what the program is expecting. For instance on HP printers, too many open threads could stop incoming connections, in effect denying service to legitimate users. These devices also need to be protected from other types of Denial of Service (DoS) attacks.

To assure confidentiality, integrity and availability of a network and all networked resources, ENDs must be secured. One cannot "assume that an embedded device is too dumb or too obscure to be compromised!"[7]

4 Universal Steps to Securing Embedded Network Devices

As with any network accessible computer, ENDs have security vulnerabilities; therefore, until the END has been secured, the device should either be configured off-line or on a secure network. If a networked device is inserted into an insecure network before the device has been secured, an administrator should not assume that it has not been compromised.

Below are several universal solutions that companies can take to secure ENDs. Not all devices have the ability to perform all the universal steps; however, it is necessary to execute as many as possible. Also, a detailed step-by-step procedure guide based on these universal tenets for securing HP 4100 networked printers are available in the appendix. (Appendix B)

4.1 Keep device up to date

As with most well-maintained secure networked systems, ENDs need to be patched regularly. Updating ENDs requires upgrading the firmware to the latest available stable revision. Not only does patching fix bugs that were present when the device shipped, but it also corrects security holes that are discovered over time.

One easy way for an administrator to secure a particular vendor's END is to use a firmware monitoring tool, which many vendors provide free of charge. These applications can report the currently installed firmware on all same-vendor ENDs on the network and can then patch them. This is much easier to do than manually updating each individual device. One example of a firmware monitoring tool is the HP Jetdirect Download Manager (DLM 3.X) available through a free download from HP's website.[8] The DLM uses discovery to find all of your HP networked printers and then gathers their firmware versions. Using either the Internet or a local source, an administrator can then apply the latest firmware to all the printers network-wide.

In addition to regular patching, administrators should subscribe to several mail lists that issue advisories for vulnerable systems, including any lists the vendor of the device maintains to check for updates. Several mail lists with the website URL to subscribe to them are provided in the appendix. (Appendix A)

4.2 Change defaults on device

Defaults for ENDs are well known and published on the Internet and should be changed before deploying the device. They are one of the simplest mechanisms hackers use to compromise a system. Defaults not only include passwords, but also include Simple Network Management Protocol (SNMP) community strings.

By using OS fingerprinting with an application like Nmap or Saint, the END's fingerprint can reveal the manufacturer and model of the device. Using this information, a hacker can look up the default passwords in a publicly accessible repository such as the one maintained by Phenoelit at http://www.phenoelit.de/dpl/dpl.html.

Phenoelit's list, for example, includes the telnet, http and ftp port administration access default passwords for HP networked printers. To gain administrative access on a newly set up HP printer, a hacker simply needs to enter nothing as the password. Passwords not created on an HP printer can easily compromise these ENDs.

ENDs often have multiple access restrictions, which mean there are several different ways to gain administration access on the device. For example, HP networked printers using HP Jetdirect have an administration password that is the same for telnet and web access, a Printer Job Language (PJL) administration password and the SNMP read and write community strings.

Once an administrator changes any default passwords for an END, they should also change the set community name for SNMP or simply turn off SNMP altogether if he/she does not use this protocol.

Network management applications use SNMP to control and monitor devices. Therefore, if an organization uses SNMP to monitor (for example with HP OpenView), do not disable it. However, according to the HP Company Security Bulletin: #0184, SNMP vulnerabilities put HP networked printers at risk for denial-of-service, service interruptions and possible unauthorized access.[9] In addition to availability concerns with SNMP turned on, confidentiality can also be compromised on HP networked printers. According to a Phenoelit Advisory and CERT Vulnerability Note VU#37703, HP Jetdirect stores the administrative password in the SNMP Object ID of .iso.3.6.1.4.1.11.2.3.9.4.2.1.3.9.1.1.0.[10]

Again, make sure all defaults are changed on the END since defaults for all devices are well known and published on the Internet.

4.3 Know the device

As with any workstation or server deployed on the network, all ports, services and software available on ENDs must be known. A port scanner, or even better,

a security scanner should be run against the device to see what ports and services are running. Also, a systems administrator should regularly visit the vendor's website and read through the documentation to learn more about the device before installing it on the network. In general, if a port, service or software is unused, it should be disabled.

In figure 1, a Nessus scan shows a brand new HP 4100 network printer. Nessus is a powerful freeware security scanner available from http://www.nessus.org/.

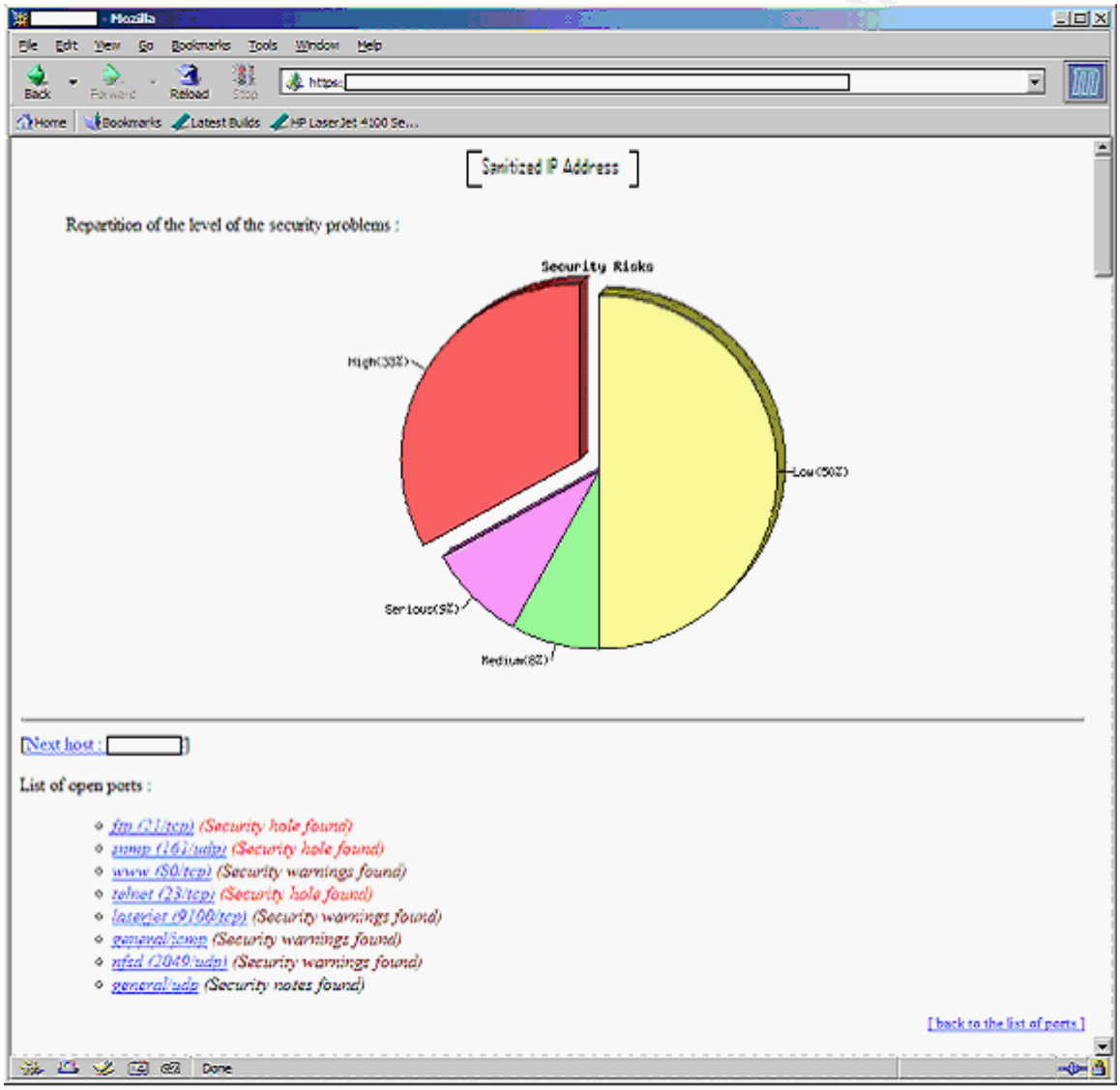

Figure 1

Figure 2 shows a Nessus scan of a HP printer after implementing the step-by-step security measures listed in the Appendix. (Appendix B)

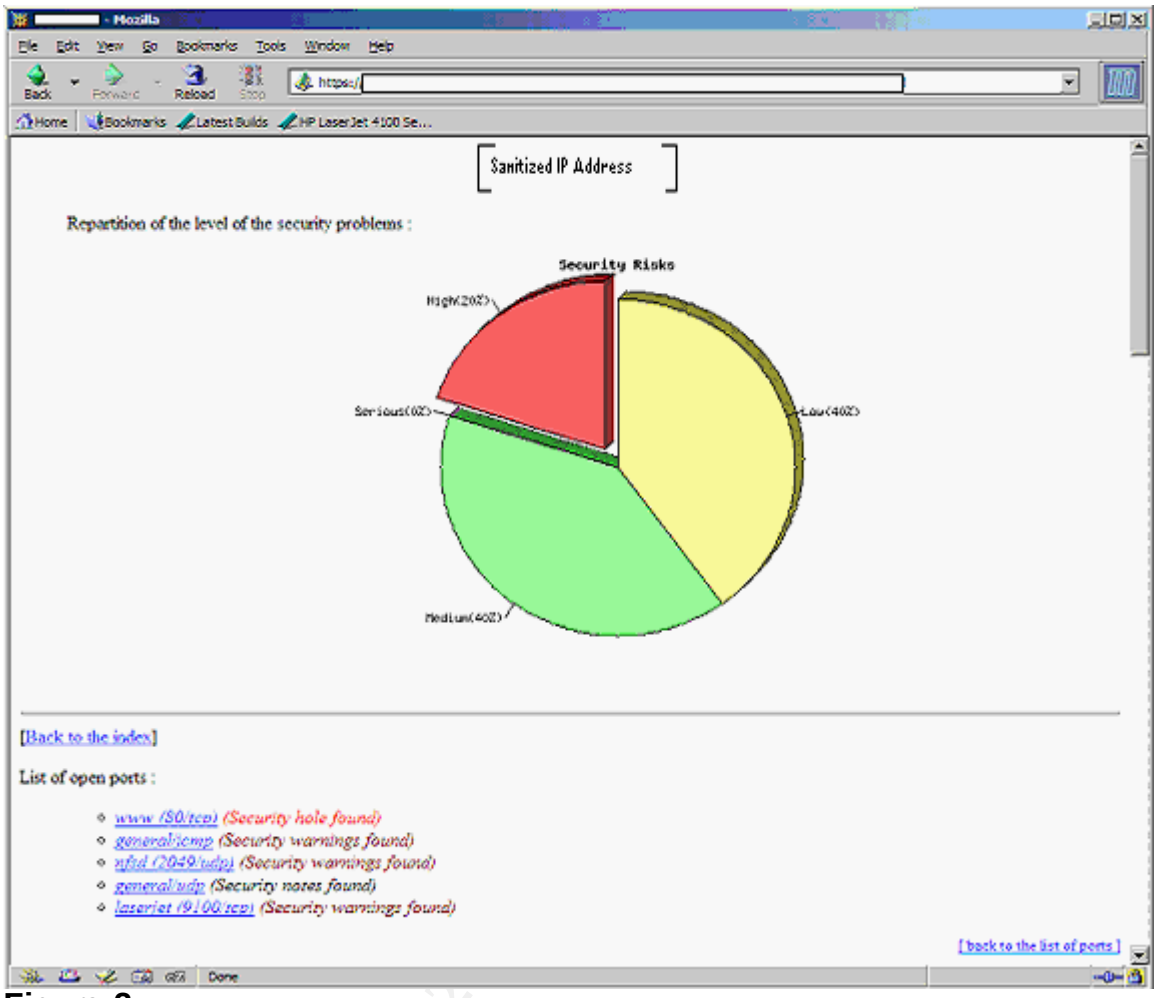

Figure 2

As you can see, the FTP, SNMP and telnet ports are no longer active. Even though the Nessus scan shows a security hole for www (80/tcp), there is no hole as all web traffic is encrypted. When you go to port 80, you are automatically redirected to port 443 (https) and encrypted from the web browser to the web server or HP 4100 in this case.

On HP networked printers, HP Jetdirect turns on the following ports and services by default: Novell or IPX/SPX protocol, Data Link (DLC) protocol, EtherTalk protocol, Internet Printing Protocol (IPP), File Transfer Protocol (FTP), HP Jetdirect's Embedded Web server (EWS), Service Location Protocol (SLP), and Simple Network Management Protocol (SNMP).[11]

One particularly powerful port is the Printer Job Language (PJL) port. The PJL port, ports 9100-9102, allows access to the printer configuration, which can display the number of copies the printer has printed, provides the ability to lock the panel, can determine which input and output trays are installed and can enable or disable economy mode and power save.

Unfortunately, security for this powerful service relies on a PJL password that is a number between 1 and 65,535 (0 disables password protection and is set by default) -- by today's standards this is quite weak; it takes less than six hours to crack by brute force. [1] Regardless, the PJL password should be set as the DEFAULT and INITALIZE commands are disabled unless the correct password is specified in the PJL command. The commands allow the ability to set the value of PASSWORD, CPLOCK and DISKLOCK until the next End Of Job (EOJ) command is received.

Besides setting the PJL password, DISKLOCK and CPLOCK security mechanisms should be employed. The disk on the printer can be locked using the DISKLOCK PJL command. When this is set, volume 0 on the file system cannot be written to. In addition to locking the disk, the CPLOCK command locks the control panel on the printer. There are several different levels including:

- MINIMUM – locks RESET, CONFIGURATION and I/O menus;
- MODERATE – locks everything MINIMUM locks and print quality and paper handling;
- MAXIMUM or ON – locks everything MODERATE locks plus printing information and the job cancel button.[12]

Also, PJL allows access to printer file systems on DRAM and FLASH including the spool directory which could contain spooled jobs, PCL macros which could contain information such as letterhead and more file system content such as the firmware, web server content and subsystem configuration. If the printer's PJL password is compromised, the printer could be turned into a PJL-based file server. [1]

A hacker tool called "Hijetter" was created by FtR. This tool provides direct PJL communication including reading, modifying and writing environment variables, full filesystem access, changing of display messages and PJL "security" removal. To secure against the vulnerabilities that "Hijetter" exploits, PJL administration access should be assigned a password and blocked from external sources. [13]

In addition to disabling ports on ENDs, software not used should be deleted from the device. HP printer model numbers 9000, 4100, 4550, and 8150 run ChaiVM which is a Java Virtual Machine for embedded systems. [14] ChaiVM on these HP networked printers comes complete with a web server, static files and objects. The printer's filesystem contains everything needed to run ChaiVM.

The Chai standard loader service is located at the following URL: http://ip_of_printer/hp/device/this.loader. The loader service validates JAR signatures through HP to ensure integrity. Unfortunately, HP released a new EZloader which does not require signatures. In order to load ChaiJava applications without integrity signatures, all a hacker needs to do is upload EZloader on the filesystem. Once the standard loader service has been

replaced, a hacker can upload their application JAR file, class files and a new csconfig. The csconfig file (0:\default\csconfig) adds services to the HP networked printer. [1] There are already a couple of ChaiJava applications written by Phenoelit including a port scanner and a password cracker.

Availability could also become a concern with ChaiVM as well; there are several problems which could contribute to downtime for HP printers. First, ChaiVM is unstable. If too many threads are open, the printer hangs and needs to be reset. Also, if the connect() function is used to try to connect to unreachable hosts or closed ports, ChaiVM is killed. In either case, the printer must be reset and would result in downtime. Finally, ChaiVM does not always throw exceptions on a consistent basis. [1]

Other problems with ChaiJava include:

- ChaiServices fully trust each other,
- ChaiApnp (Chai Appliances Plug And Play) service support SLP which finds other devices using multicast,
- the notifier service can be setup to notify the hacker by http or email of interesting events such as when a specific user sends a print job,
- ChaiOpenview enables ChaiVM configuration via SNMP,
- ChaiMail service has been "designed to work across firewalls."[1]

In summary, a systems administrator should scan the device and read documentation to learn more about the END. He should also shut down any ports or services and delete any unused software.

4.4 Control device access

Most ENDs provide a mechanism for limiting access to the device by using Access Control Lists (ACLs). Unfortunately, most devices have various access controls and restrictions and can be confusing to set up. For example, HP printers have an administration password on http and telnet, IP address access restrictions, SNMP communities, and the PJL security password.

On HP networked printers, "the access control specifies a range of IP addresses that would be allowed TCP connections with the HP Jetdirect."[15] Not only does the ACL affect management of the device but printing as well.

To learn how to change the various passwords and setup ACLs on HP networked printers, please see the appendix which provides a step-by-step procedure for securing a HP 4100 printer. (Appendix B)

4.5 Encrypt data

If the END supports data encryption, the device should be configured to only use encryption. Encryption helps ensure data confidentiality.

Once the device is initially set up and encryption turned on, never administrate an END without using encryption. For example, if the most robust encryption settings are set on an END, but an administrator administrates the device though a clear-text Telnet session, information such as the administrative passwords are available to anyone eavesdropping on the network. Most business devices now support encryption for administration. For example, both Cisco routers and HP Jetdirect printers support encryption built into their latest firmware. Cisco router IOS' include support for Secure Shell (SSH). Please note that SSHv1 is no longer considered secure since vulnerabilities were found. Administrators should use SSHv2 instead.[16] Also, HP Jetdirect printer servers now provide support for Secure Socket Layer/Transport Layer Security (SSL/TLS) which is a protocol that encrypts traffic between a web browser and a web server or in this case the HP Jetdirect Embedded Web Server.

To provide data confidentiality through encryption from a user's application over the network to the printer, third party solutions are usually needed. "The JetCAPS SecureDIMM slots into your HP LaserJet printer to monitor and decrypt and check the integrity of data just as it is about to be printed, without interfering with standard or extended printer functionalities… A simple encryption utility captures and encrypts data before it leaves the computer. For increased security, encryption can also be directly incorporated into the required applications."[17] JetCAPS was developed by Capella Technologies and uses the Rijndael encryption algorithm.[18] Rijndael was selected as the new Advanced Encryption Standard (AES) by National Institute of Science and Technology (NIST).[19]

Using encryption between the administrator and the END is the only way a device's configuration should be altered after deploying it. The administration password and configuration changes could otherwise be sniffed off the wire, destroying confidentiality. Also, third party solutions can help ensure confidentiality by using encryption for clients connecting to the device.

4.6 Use SNMPv3 if SNMP must be used to monitor the Device

SNMP allows a company to monitor and even configure ENDs. Unfortunately, earlier versions of SNMP fail to provide integrity, authentication and confidentiality that SNMPv3 provides. If the device supports SNMPv3 and needs to be monitored or configured in this manner, disable earlier versions of SNMP and set up SNMPv3.

"SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network."[20] SNMPv1 and SNMPv2c allow a simple community string match for authentication. Considering most devices ship with the standard public and private defaults and this challenge is not encrypted, earlier versions of SNMP should not be used to monitor and configure the device as they can be lifted off the wire.

Using SNMPv3, devices can be monitored securely with the assurance of integrity of the data. Confidentiality is gained using encryption as the END's configuration changes can be encrypted to save its contents from being monitored. Also, SNMPv3 no longer simply uses community strings but uses encryption such as MD5, SHA, or at minimum a username for authentication.

On HP network printers, SNMPv3 is available on the HP Jetdirect print server models 610n, 615n, 250m, and 310x with firmware version x.22.09. [21]

4.7 Log device events and audit the logs

While log files cannot actually secure an END, logs can be useful if monitored correctly. Logs show trends in interesting traffic to your device, such as excessive amounts of incorrect password attempts or many connections to the web port from an unknown host. In addition to trending, logs are very useful in forensics and can help determine accountability.

To enable logging on HP network printers, simply set the syslog server entry to the company's syslog server. A syslog server waits for incoming traffic on UDP port 514 and logs that information into a log file using a syslog daemon. Generally, companies use an audit tool that scours the log files looking for uncharacteristic log messages. Using syslog servers allow centralization of log files for many devices and computers.

4.8 Defense in Depth

The concept of defense in depth "is a term used to describe a critical approach to information assurance in today's world of connectedness."[22] Companies should not rely on just the device for protection of itself, but should use multiple devices and layers to separate the END from other networks.

For example, to secure a HP network printer using the defense in depth concept, turn on all its security features. Also, place the networked printer behind a firewall. The firewall should not allow any access in or out of the printer. In addition to a firewall, place the printer on a switched network to help prevent packet sniffing. Physically securing the device adds yet another layer of defense.

Third-party solutions like JetCAPS can supplement the precautions listed above. "Too often the weakest link in the protection and control of your sensitive data is when it is on its way to the printer, or while it is in the printer's output-tray – particularly if you want to make the most of your network by printing remotely."[23]

Defense in depth is a security concept that should be employed when installing any device on a network including ENDs.

5 Conclusion

As with any server, the device should be configured either off-line or behind a protected network. Create a security checklist and check it off as items are accomplished. The universal security checklist is outlined below:

- Keep device up to date – perform patches or firmware updates as the vendor releases revisions;
- Change defaults on device – change default administrator passwords, SNMP community strings, and any other standard defaults;
- Know your device – inventory and understand all the ports, services, and software running off the embedded operating system. Disable any ports, services or software if you do not use them;
- Control device access – use the device's access control to limit access to functions and administration of the device as well as physically securing the device if required;
- Encrypt data – do not use weak encryption or clear-text protocols to administer the device, enable strong encryption when available to provide confidentiality instead;
- Use SNMPv3 if your company must use SNMP – enable SNMPv3 if the device allows it as SNMPv3 provides encryption for confidentiality and authentication whereas SNMPv1 and SNMPv2c do not;
- Log device events and audit those logs – while this will not secure the device, this will help with forensics after a break-in and by auditing the logs, trending of possible attempts at break-ins can be discovered.
- Defense in Depth – do not rely on just one device for protection, use router and firewall ACLs, switches and third-party solutions to add additional layers of defense.

The most important aspect of securing ENDs is not to underestimate their importance in the security of the network. By following this universal security checklist, systems administrators can improve security of ENDs.

6 Appendixes

A. Security mailing lists and how to subscribe to them:

- "SANS Security Alert Consensus weekly bulletin" and the "SANS Critical Vulnerability Analysis weekly bulletin"
  http://server2.sans.org/sansnews

- "HP's driver & support alerts/notifications"
  http://hp-newsletter.m0.net/m/p/hp1/drv/signup.asp

- "CERT® Advisory Mailing List"
  http://www.cert.org/contact_cert/certmaillist.html

- "BugTraq", "Vuln-Dev", and "SecurityFocus News"
  http://online.securityfocus.com/cgi-bin/sfonline/subscribe.pl

B. Step by Step Procedure for Securing a New HP 4100 Networked Printer

To secure a new HP 4100 networked printer, the universal steps to securing ENDs are applied and compiled into an example step-by-step procedure below.

To perform all the steps the following tools must be installed and used:

- HP Jetdirect Download Manager – DLM 3.x
  http://www.hp.com/cposupport/networking/support_doc/bpj06917.html

- Nessus Security Scanner
  http://www.nessus.org/

- Phenoelit Hijetter
  http://www.phenoelit.de/hp/download.html

Start by setting up the printer with a static IP address on a secure network that has no incoming access available from the outside. Once the printer's network is set up, follow the instructions below:

1. Update the firmware using the HP Jetdirect Download Manager (DLM):
   a. While opening the DLM, it asks what operating mode the DLM should be run, choose Internet so the latest firmware will be loaded directly from the HP web site;
   b. Next, choose the discovery options. Either run an Automatic Discovery which searches all networks known to the PC the DLM is being run from or Custom Discovery where a network or a single IP address may be specified. If just one HP 4100 is being set up, use Custom Discovery to specify the IP address of the device;
   c. The Discovery Report should find the address, and if the firmware needs to be upgraded, a window will prompt to continue;

    d. An Upgrade Progress window will pop up showing status of percentage completed.
2. Use the HP Jetdirect Security Configuration Wizard to set up security:
    a. Using a web browser go to the IP address of the HP printer (ex. http://ip_of_printer/);
    b. Click on the networking tab;
    c. On the left side under the section of Security, click on Settings;
    d. Choose the Wizard tab and click the Start Wizard button;
    e. The next screen has radio buttons for different Security Levels including Basic, Enhanced, and Custom Security. Choose Custom Security and click Next;
    f. Administrator Account screen then appears. Enter the new Administrator account password in the areas provided and click Next;
    g. Next, the Web Mgmt. screen will appear. Choose an Encryption Strength of Medium, and check the Encrypt All Web Communication then click Next;
    h. A Management Tools screen appears. Uncheck both boxes to disable telnet and FTP Firmware updates and RCFG then click Next;
    i. SNMP Configuration screen then appears. Uncheck Enable SNMPv1/v2 to disable SNMP (if your company does not use SNMP management software). Also disable SNMPv3 if it is not needed. Otherwise, keep it checked and click Next;
    j. A second screen of SNMP Configuration inquires whether certain tools require SNMPv1/v2 to be enabled. Disable this by unchecking the choice and clicking Next;
    k. Access Control is the next screen. If the ACL is left empty, everything has access to the HP printer. To add addresses, click the Enable column on the correct row and enter an IP address and netmask on the same row. Complete for all addresses and networks needed to access the printer. Finally, clear the Allow Web Server (HTTP) access checkbox so ACLs are checked with HTTP connections and click Next;
    l. Next Print Protocols and Services screen appears. Uncheck any protocols and services not needed. For instance, uncheck IPX/SPX, AppleTalk, DLC/LLC, FTP, SLP, LPD, mDNS, and Multicast IPv4 then click Next;
    m. Finally, a Configuration Review screen will appear. Verify all the settings then click Finish. After clicking Finish a Configuration Result stating that the configuration settings have been set successfully appears.
3. Login to the newly secured HP printer and set the syslog server:
    a. Login to the HP printer using http://ip_of_printer/ and click on Networking. You will be redirected to port 443 (SSL). Accept the

certificate and then enter in the user of admin and the password entered earlier to get to the Networking screen;

b. Click on the Network Settings under the Configuration section and in the TCP/IP tab, locate and enter the IP address of the Syslog Server for the Syslog host and change the Syslog Priority if needed to.
c. To change the facility the logs are using (LPR is the default), click on Other Settings in the Network tab and change Syslog Facility to a Local facility. The default is recommended to group all the printer syslog entries together.

4. While the device is still connected to the secure network, use Nessus to scan the device for vulnerabilities and to determine which ports are open. Record the findings.
5. Finally, make sure that when the printer is deployed that it is protected from Internet access using a firewall. If the printer must be accessible to Internet addresses, make sure the ACLs allow only Internet addresses that are permissible and that the firewall provides similar ACL to block all but the few addresses that need access to the printer from outside the firewall. Instead of allowing external addresses to print to the printer, VPNs should be considered.
6. In addition to the basic steps above, there are a couple advanced options that will further secure the devices.
    a. Enable PJL Protection by setting a PJL password, locking the control panel and locking the disk.
        i. Load Hijetter and connect to the printer by inserting the IP address under Connection to, choosing the correct port (default of 9100), and clicking the connect icon next to the port;
        ii. Click on the $ENV icon. A window with all the environment variables should appear;
        iii. Click on CPLOCK and change the default to MINIMUM at the least. For a definition of what the different levels mean, please refer to section 4.3 above;
        iv. Click on the Enter icon to set the variable for modification. An M should appear next to CPLOCK;
        v. Next, click on DISKLOCK and change the default to ON;
        vi. Click on the Enter icon to set the M next to DISKLOCK;
        vii. Finally, locate PASSWORD and change to any number between 1 and 65535 and click the Enter icon;
        viii. To write the changes click the check mark. The steps just performed run the following PJL command script:

```
<Esc>%-12345X@PJL
@PJL DEFAULT PASSWORD = #
@PJL DINQUIRE PASSWORD
@PJL DEFAULT CPLOCK = MINIMUM
@PJL DINQUIRE CPLOCK
```

@PJL DEFAULT DISKLOCK = ON
@PJL DINQUIRE DISKLOCK
@PJL EOJ
<Esc>%-12345X

b. Disable the ability for the printer to send or receive email by logging into the device. Using a web browser, login as administrator to the printer by going to http://ip_of_printer/. Choose the Device tab then the Security choice on the left menu. Uncheck all boxes regarding Email Security.
c. Remove this.loader from the printer by editing 0:/default/csconfig and restarting the printer. This can be done using Hijetter. My company does not remove this.loader so we can continue to administrate the device via the web interface.

7. Congratulations! The HP 4100 networked printer is now secured!
8. Periodically, you must maintain the HP 4100 to ensure security.
   a. Run the DLM at least once a month to verify that no new firmware has been released by HP.
   b. Run a Nessus scan every month and compare to the original Nessus scan to verify that no extra ports or services have been enabled.

7 References

[1] FX and kim0. "Attacking Networked Embedded Systems." Black Hat USA 2002 Briefings and Training.
URL: http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-phenoelit-network.pdf (23 Feb. 2003).

[2] No author. "Hewlett-Packard Annual Report 2001." (1 Feb. 2002).
URL: http://www.hp.com/hpinfo/investor/financials/annual/2001/text_only_10k.pdf (23 Feb. 2003).

[3] Zaborav, Dev. "Hack the Fridge, Man!" 29 Aug. 2002.
URL: http://www.itworld.com/nl/unix_sec/08292002/pf_index.html (23 Feb. 2003).

[4] No author. "Hewlett-Packard Brings the Power of the Internet to Printing." 20 Mar. 2001. URL: http://www.hp.com/hpinfo/newsroom.press/20mar01a.htm (23 Feb. 2003).

[5] No author. "Search Results." Common Vulnerabilities and Exposures.
URL: http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=jetdirect (23 Feb. 2003).

[6] Harris, Shon. All-in One CISSP Certification Exam Guide. New York: McGraw-Hill Osborne Media, 2001. 123.

[7] Weinberg, Bill. “Security checklist for embedded devices.” 22 Apr. 2002. URL: http://www.eetimes.com/printableArticle?doc_id=OEG20020419S0076 (23 Feb. 2003).

[8] No author. “Hewlett-Packard Jetdirect Download Manager – DLM 3.X, Upgrading Hewlett-Packard Jetdirect Firmware.” URL: http://www.hp.com/cposupport/networking/support_doc/bpj06917.html (23 Feb. 2003).

[9] No author. “Hewlett-Packard Company Security Bulletin: #0184.” 13 Feb. 2002. URL: http://www.attrition.org/security/advisory/hpalert/hp-0184 (23 Feb. 2003).

[10] FX and kim0. “Phenoelit Advisory.” 23 Jul. 2002. URL: http://www.phenoelit.de/stuff/HP_snmp.txt (23 Feb. 2003).

[11] No author. “HP Jetdirect Print Servers - HP Jetdirect Port Numbers for TCP and/or UDP Connections.” URL: http://www.hp.com/cposupport/networking/support_doc/bpj01014.html (23 Feb. 2003).

[12] No author. “Printer Job Language Technical Reference Manual.” October 1997. URL: http://www.lprng.com/DISTRIB/RESOURCES/DOCS/pjltkref.pdf (23 Feb. 2003).

[13] No author. “PFT and Hijetter: Printer Exploration.” URL: http://www.phenoelit.de/hp/docu.html (23 Feb. 2003).

[14] No author. “JetCAPS® Chai Applications.” URL: http://www.swedprint.se/pdf/ds_chai.pdf (23 Feb. 2003).

[15] No author. “HP Jetdirect Print Servers - Making HP Jetdirect Print Servers Secure on the Network.” URL: http://www.hp.com/cposupport/networking/support_doc/bpj05999.html (23 Feb. 2003).

[16] No author. “CERT® Advisory CA-2002-36 Multiple Vulnerabilities in SSH Implementations.” 20 Jan. 2003. URL: http://www.cert.org/advisories/CA-2002-36.html (23 Feb. 2003).

[17] No author. “JetCAPS SecureDIMM.” URL: http://h40041.www4.hp.com/jetcaps/solutions/securedimm.html (23 Feb. 2003).

[18] No author. “Print Security/Secure DIMM II.”
URL: http://www.capellatech.com/products/print_security/secure_dimm.php (23 Feb. 2003).

[19] Nechvatal, James et al. “Report on the Development of the Advanced Encryption Standard (AES).” 2 Oct. 2000.
URL: http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf (23 Feb. 2003).

[20] No author. “SNMPv3.” 7 Mar. 2000. URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.htm (23 Feb. 2003).

[21] No author. “HP Jetdirect Print Servers - Creating an Initial Account for Simple Network Management Protocol (SNMPv3) Using the Embedded Web Server (EWS).”
URL: http://www.hp.com/cposupport/networking/support_doc/bpj07131.html (23 Feb. 2003).

[22] VanMeter, Charlene. “Defense In Depth: A Primer.” 19 Feb. 2001.
URL: http://www.sans.org/rr/start/primer.php (23 Feb. 2003).

[23] No author. “JetCAPS secure and remote printing.”
URL: http://h40041.www4.hp.com/jetcaps/solutions/secure.html (23 Feb. 2003).