White Paper

March 2004

Document Version: 1.0

Imaging and Printing Group
Hewlett-Packard Company

Multifunction Peripheral (MFP) Security for Enterprise Environments

Contents

Abstract:

Networked imaging and printing infrastructure has the potential for abuse just as any other networked system. Imaging and printing devices have gained levels of sophistication comparable to network servers and workstations, and should be managed as such. Understanding, and effectively using, the security features of HP imaging and printing devices is crucial for the maintenance of a secure network.

Notice:

©2004 Hewlett-Packard Company

Microsoft®, Windows®, and Windows NT® are trademarks of Microsoft Corporation in the U.S. and/or other countries. UNIX® is a trademark of The Open Group in the U.S. and/or other countries. Intel® and Itanium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the U.S. and other countries. Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California. All other product names mentioned herein may be the trademarks of their respective companies.

Neither HP, nor any of its subsidiaries, shall be liable for technical or editorial errors or omissions contained herein. The information in this publication is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

1 Introduction

The networked imaging and printing infrastructure has become increasingly sophisticated, becoming a critical component of the office infrastructure. Despite its importance, network administrators have largely ignored the security risks of their imaging and printing infrastructure, oftentimes leaving the infrastructure entirely unsecured.

While attacks against imaging and printing devices have been rare, administrators should safeguard their resources before becoming affected; attacks against unsecured network communications can result in loss of confidential data, denial of service attacks against networked printers may result in lost productivity, and unauthorized use of imaging and printing devices may result in the loss of consumables.

HP has made security an integral component of its imaging and printing devices and solutions. HP devices support a wide-range of industry standard and trusted security protocols, as well as class-differentiating functions and solutions, allowing for secure management, device integrity, privacy, and access control:

- SNMPv3 for standards-based secure enterprise management
- SSL/TLS (Secure Sockets Layer/Transport Layer Security) and HTTPS (Hypertext Transmission Protocol, Secure) for standards-based secure web management
- 802.1X authentication for Wireless security, including EAP-TLS, EAP-MD5, LEAP, and PEAP for access control and dynamic key encryption (WEP and WPA are supported wireless security feautres)
- AES (Advanced Encryption Standard) for print encryption and integrity
- DoD (Department of Defense) 5520-22m conforming Disk Erase
- Microsoft Windows and Novell Authentication for Digital Sending
- X.509 Certificates for server/device authentication
- IP (Internet Protocol) Access Control Lists for secured printing and management
- Control Panel Lock

Section 2, Imaging and Printing Infrastructure, describes the security capabilities of the components that form the imaging and printing infrastructure.

Section 3, Recommendations, provides guidance on the configuration of the Imaging and Printing infrastructure for secure operation.

Section 4, Acronyms, defines acronyms used throughout this paper.

Section 5, References, provides web-based references to the components of the system.

2 Imaging and Printing Infrastructure

Today's imaging and printing infrastructure consists of a sophisticated system of components, including print users, print spoolers, management platforms (for example, Web Jetadmin or Digital Sending software), and imaging and printing devices (for example, multifunction peripherals and printers).

A variety of network protocols are used to interconnect these components: the SMB/CIFS printing protocol for print users, Port 9100 and LPR protocols for printing from spoolers, and the SNMP protocol for management.

Ease of Use

Frequently, security features are ignored because of their complexity. A device may offer credible security features, however because of the complexity of their use, they may go unused.

HP has concentrated on reducing the complexities of security, while continuing to lead with state-of-the-art capabilities. By making security seamless in the operation of the device, administrators of all abilities can ensure the security of their imaging and printing infrastructure (Figure 1).

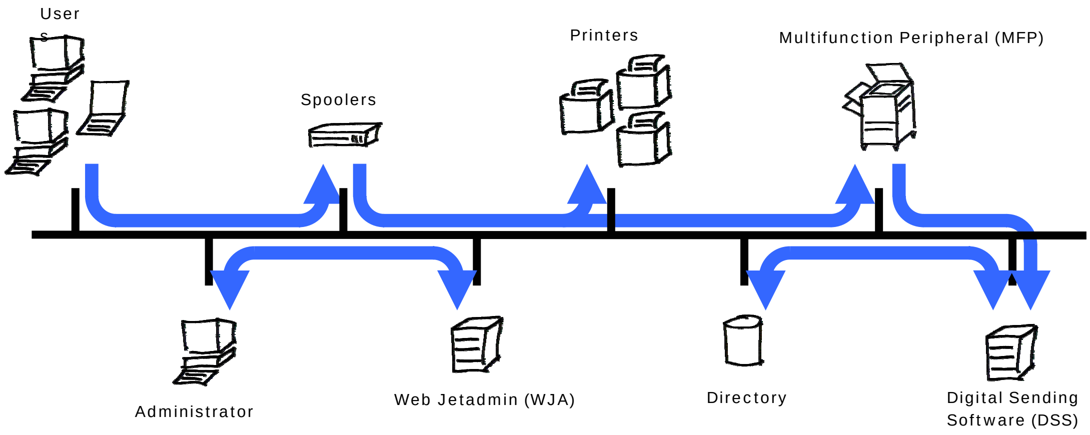

Figure 1: Imaging and Printing Infrastructure

The following describes the major components of the infrastructure, including their interrelationships, and security capabilities.

Multifunction Peripheral (MFP) Hardware

HP MFPs allow fast, high-quality printing and copying, as well as advanced finishing capabilities. Security has been integral to the MFPs design, including mechanisms to limit usage to authorized users, provide privacy and integrity of printed data, and ensure only authorized management use.

The HP MFP is composed of several subsystems, including major components for scanning and printing. A network interface provides connectivity allowing remote printing, as well as scanning to email, network folders, and LAN FAX. An analog FAX accessory allows the transmission and reception of FAXs over analog telephone lines. Internal to the system are processors, memory (RAM, ROM), firmware, and hard disk storage.

Embedded Operating System and Firmware

At the core of all HP multifunction peripherals (MFPs) are computer processors and firmware. The firmware consists of an "embedded" operating system and the instructions the processor is to execute to function. The processors and embedded operating systems contained in the MFP are not based on typical PC platforms such as Windows and MacOS, and as such have been largely unaffected by devastating network worms and viruses. While HP MFPs have been affected by denial of service attacks, resulting in slowed operation, there have been no known cases of viruses infecting these devices, or propagating from them.

Firmware Updates

To facilitate future upgrades and bug fixes, HP MFPs allow remote firmware updates. Using Web Jetadmin, batch updates of printers may be accomplished easily and quickly. To protect the system from unauthorized firmware updates, access controls integral to device management are supported. Mechanisms are used to check the authenticity of the firmware image; however it is still recommended that only firmware images provided directly from HP be applied.

Vulnerabilities, buffer overflows, et al.

HP MFPs have been extensively tested to ensure that they may not be compromised by buffer overflows, malformed data requests, and malformed data submissions.

The embedded web server and SNMP MIB have been rigorously tested to ensure HTML management pages and SNMP OIDs are only accessible to authorized users when access controls are enabled.

Chai Platform

The Chai Platform is a powerful mechanism for device extensibility. The Chai platform allows specialized applications known as "Chailets" to be installed on the MFP, extending its capabilities. A wide range of Chailets have been developed, enabling job accounting, custom management interfaces, and web services functionality.

While the Chai platform provides an excellent means of extending the device's capabilities, administrators should be careful to only allow Chailets from known and trusted sources to be installed. As is the case for PC servers and workstations, it is important for the administrator to enable security to prevent the unauthorized installation of potentially malicious applications.

Network Interface, EIO bus

Network connectivity is provided by Jetdirect network adapters using the MFP's EIO expansion bus. Jetdirect adapters support a variety of network types using the EIO bus:

Network Medium	Model
10/100T Ethernet	Jetdirect 615n and 620n
802.11b Wireless Ethernet	Jetdirect 680n

Wireless Ethernet

The 802.11b Wireless Ethernet adapter supports the leading industry standard security protocols, including WPA, WEP 64bit and 128bit encryption, as well as 802.1x-based protocols (EAP-TLS, EAP-MD5, PEAP, and RADIUS integration) for authentication and dynamic key distribution.

MFP Analog FAX Accessory

The Analog FAX accessory allows the MFP to act as a stand-alone FAX machine, able to transmit and receive analog faxes. The analog FAX accessory operates through a parallel port connection with the MFP. Neither the MFP nor Jetdirect network adapter nor FAX accessory firmware provides mechanisms for the bridging of network to analog interfaces.

Disk Drive

The HP MFP uses a hard disk drive (HDD) for a variety of spooling, job retention, and private printing (see MFP Scanning/Copying) tasks. The HDD uses the MFP's EIO bus for connectivity. The HDD may be physically secured from theft and tampering using an accessory lock. The accessory lock requires a physical key for hard disk drive removal.

Encryption of network transmitted data stored on the disk is available using the JetCAP SecureDIMM II accessory module. The SecureDIMM II module secures the print job from the printing client to the MFP's internal printing engine. While the print job is retained on the hard disk, it remains encrypted.

Unless otherwise specified, print job data is deleted from the disk at the completion of the print job. Multiple mechanisms are supported for the erasure of disk drive data:

- Sanitized Erase: Conforms to the DoD 5220-22m specification for deletion of magnetically stored data. Using multiple data writes to eliminate trace magnetic data, Sanitized Erase prevents subsequent analysis of the HDD's physical platters for the retrieval of data.
- Secure Erase: Provides greater performance, overwriting the existing data once, and preventing software-based "undelete" operations to the data.
- Fast Erase: Provides the greatest performance, flagging the print job as deleted, and allowing the MFP's operating system to reclaim and subsequently overwrite the data when needed.

MFP Management Security

Management Interfaces and Protocols

HP MFP's support a variety of management interfaces, including Web Jetadmin, SNMP, the Embedded Web Server (EWS) Management Interface (HTTP), Telnet, FTP, DHCP, and BOOTP.

The choice of which management interface used is normally based on the complexity of the deployed environment. For environments with many devices, Web Jetadmin allows the centralized management of all of the devices. In environments where few devices are deployed, an administrator may choose to manage each device individually through the device's Embedded Web Server Management Interface.

The management interfaces may be separated into three categories, based on the security capabilities of their underlying protocols. Web Jetadmin using SNMPv3 and the Embedded Web Server using HTTPS (TLS/SSL) provide the highest level of security, supporting encryption and access controls, and are the recommended interfaces. Interfaces using SNMPv2, HTTP, Telnet, and FTP, provide access control, however do not provide encryption. DHCP and BOOTP provide neither access control nor encryption.

Interface	Protocol
High Security [access control and encryption]	
Web Jetadmin	SNMPv3
Embedded Web Server	HTTPS - TLS/SSL
Medium Security [access control only]	
Web Jetadmin	SNMPv2
Embedded Web Server	HTTP
Telnet	
No Security	
BOOTP, DHCP	

Out-of-Box Security

Enabling security out of the box, and as an integral part of the MFP installation and configuration, ensures subsequent secure operation. Providing privacy of communications for the initial configuration also ensures that security credentials are not "leaked" and captured by network sniffers.

> ! Default Passwords
> Default passwords provide no practical security, yet they are one of the most commonly used mechanisms for securing systems. Default passwords do nothing more than provide the administrator with a false sense of security. Default passwords are readily available from product user manuals, and hackers have created web sites to catalog and distribute default passwords for a variety of products.

To enable HP products to have a high level of initial security, two mechanisms are used together:

- Make security configuration integral with the installation process
- Encrypt the communications for privacy

By making the security configuration integral with the system installation, administrators may be assured that subsequent system management may only be performed by authorized users. Using the Security Wizard of the Embedded Web Server Management Interface, administrators are able to select all security-related configuration settings during installation.

By encrypting the communications for security configuration, the administrator is assured that the credentials, passwords, and keys, cannot be intercepted by network hackers and reused.

Encryption

To secure network communications, providing both integrity as well as privacy, encrypted protocols are used.

HP MFPs allow encrypted communications immediately out of the box, without administrator configuration, using public key cryptography. During start-up, the MFP creates a unique asymmetric key pair, consisting of a "private key" that is known only to the MFP, and a "public key" that is exposed to the user's management interface. Data encrypted using the MFP's public key may only be decrypted by the MFP, allowing secure communications to the MFP, and data decrypted by the public key may only have been encrypted by the MFP, allowing authentication of the sending device.

For management interfaces' using the SNMP protocol, such as the Jetdirect Installer and Web Jetadmin, the public key is exposed as an SNMP object. For first time installation, the management application can retrieve the public key from the MFP, and then uses it to encrypt the credentials for subsequent SNMPv3 operation.

For management using the MFP's Embedded Web Server, the public/private key pair is bound to a self-signed X.509 server certificate. The server certificate facilitates the establishment of a secure connection using the SSL/TLS protocol. The administrator may subsequently add the certificate to their certificate store for future trust, or install an externally-signed X.509 certificate.

Access Control

Management access control is provided by a combination of administrator account (username and password), SNMP Community Names, SNMPv3 authentication keys, and IP Access Control Lists.

The administrator account utilizes a username and password for authentication, and is used by the EWS, Telnet, and FTP management interfaces. The SNMP Get/Set Community Names are used for the SNMPv2 protocol and emulate the functionality of a password. For added convenience and security, the EWS Security Wizard allows the Community Names to be set to match the administrator password. The SNMPv3 authentication key is an administrator-supplied key that allows for cryptographically strong authentication.

IP Access Control Lists allow the administrator to select a set of specific, or range of, IP addresses that are allowed TCP/IP access to the device. When using IP Access Control Lists for management security, the IP addresses of authorized management consoles (WJA) should be enabled, or the specific IP addresses of network administrator workstations.

Protocol/Service Configuration

Improperly configured systems are a common target for attack. Systems may have security settings improperly configured, or unused, unneeded, and unmonitored services installed. Oftentimes, services that are left unused are not secured, providing backdoors for exploitation. The following services and protocols may be selectively disabled:

- Management: Embedded Web Server (EWS), SNMPv2 and SNMPv3 protocols, Telnet, FTP, and RCFG.
- Network Protocols: IPX/SPX, AppleTalk, DLC/LLC.
- Print Services: Port 9100, LPD, IPP, and FTP
- Device Discovery: SLP, mDNS, and Multicast IPv4

MFP Copy/Scan/Print Security

HP MFP's provide a range of capabilities. The HP 4100 and 9000 series MFPs allow the capability to copy, scan, and print network documents. Scanned documents may be stored for subsequent reprinting, transferred to network folders, FTP sites, or remote printers, as well as transmitted electronically as email and LAN faxes.

Secured access to the MFP is provided by HP Digital Sending Software (DSS) components. Using HP DSS, access to the MFP as well as network and email functionality may be limited to authenticated NT and Novell users.

Private printing allows a personal identification number (PIN) to be associated with the print job. The print job will be released only after that PIN has been entered at the MFP's control panel.

Scan-to-email allows a document to be transmitted electronically. To ensure the integrity of scanned-to-email documents, as well as compliance to intellectual property policies, the administrator may configure the MFP email gateway to the trusted gateway (Figure 2).

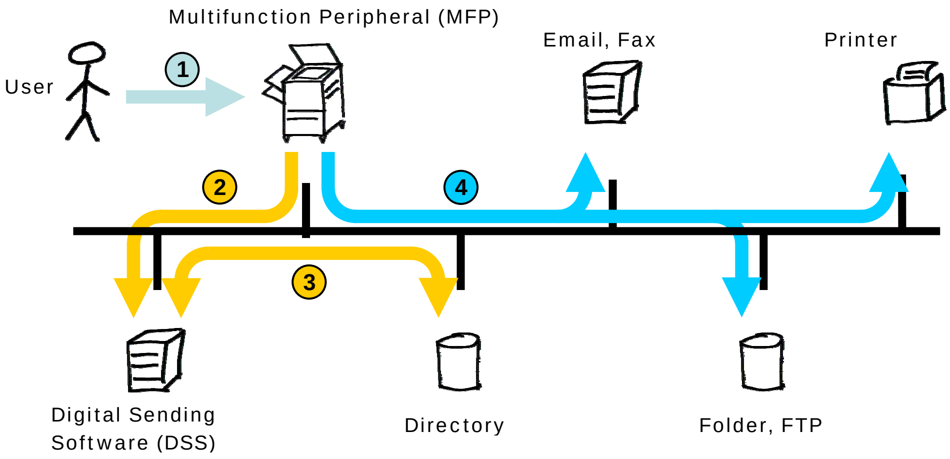
Multifunction Peripheral (MFP)
User
1
Email, Fax
Printer
2
4
3
Digital Sending Software (DSS)
Directory
Folder, FTP

Figure 2: The HP MFP Subsystems

Encrypted Scan to E-Mail and Network is provided by Authentica's content securing software. Additional information may be found in the reference section for Secure Document Delivery.

Networked Printing

MFPs use simple print protocols to receive print jobs from remote clients. The two common print protocols are LPR and "raw" Port 9100. Neither protocol provides encryption or access controls; however these features are typically integrated with other components of the system, including spoolers and encryption modules.

Spoolers and Access Control

Spoolers have evolved from simple services managing printer resource contentions between multiple users, to specialized servers able to provide sophisticated enterprise-integrated access controls, printer discovery, and client printer driver distribution.

The spooler acts as an intermediary between users and printers. All user print jobs are directed to the spooler, which may then prioritize their delivery to the appropriate printer. The print protocol used between user and spooler typically differs from that used between the spooler and the printer, allowing for increased capabilities such as access control. Microsoft spoolers use the CIFS protocol for both network printing and file sharing operations.

Access controls within the spooler may be integrated with the security policies used elsewhere in the IT environment. Users may be assigned access to specific printers or capabilities. Network administrators may audit usage through the spooler.

IP Access Control List

The IP Access Control List allows selected, or ranges of selected, IP addresses access to the MFP. The IP Access Control List may be used to limit printer accessibility to selected computers. IP ACLs do not provide "user" authentication however, and the ACLs are typically used to enforce the access restrictions provided by a print spooler.

Print Encryption

Encryption of print data is provided by the JetCAP SecureDIMM II accessory module. The SecureDIMM II uses AES encryption to secure the confidentiality and integrity of print jobs from originating clients, through all network transmissions and storage operations on print spoolers, to the MFP. While stored on the MFP's internal hard disk drive, the print job remains encrypted.

3 Recommendations

While the networked imaging and printing environment has to date not been a primary target for network attacks, this cannot always be assured. As hackers find traditional servers more difficult to exploit, they will look for other targets. It is important that administrators not wait until after they have been attacked before securing their environment. Tangible losses can be the result of an unsecured imaging and printing infrastructure; from loss of productivity due to denial of service attacks, to losses of consumables due to unauthorized use.

HP has enabled MFPs and networked hardcopy devices with extensive security capabilities, enabling the imaging and printing infrastructure to be integrated with the security policies of the existing infrastructure. HP has also done extensive testing on imaging and printing devices and solutions to ensure their robustness.

The following recommendations can be a starting point for securing your imaging and printing infrastructure:

- **Treat MFPs and networked printers as any other network server** – Networked MFPs and printers offer much of the same capabilities as general purpose servers. Integrate MFPs and printers into vulnerability scans, and into intrusion detection systems, and audit for compliance of policies.
- **Set Passwords** – The most overlooked element of hardcopy security is failing to secure the management interfaces via proper passwords. Setting the administrator password provides significant benefits with little effort.
- **Use Web Jetadmin for enterprise-wide hardcopy management** – Web Jetadmin allows the consistent management of large numbers of networked MFPs and printers. WJA simplifies the discovery and tracking of newly added devices.
- **Use "secure" protocols in lieu of insecure protocols** – HP has removed the complexity of enabling encryption. The use of SNMPv3 for Web Jetadmin or HTTPS and TLS/SSL for Embedded Web Management requires no extra effort, however provides encryption of network communications.
- **Disable unused protocols and services** – unused, and ignored, protocols and services are a common backdoor for attack.
- **Use printer spooler access controls** – common print spoolers are tightly integrated with the operating system, allowing for user-level access control for printing.
- **Use IP Access Control Lists** – used in conjunction with spooler and management console authentication, IP Access Control Lists can ensure only authorized users may print to, and manage, an MFP.
- **Physically lock the disk** – while it is possible to encrypt the content of the hard disk drive for network prints, ultimate security of the drive can only be provided if it cannot be removed.
- **Utilize JetCAPS partners for increased hardcopy security** – HP has developed partnerships through the JetCAPS program to provide leading security solutions for hardcopy environments.

4 Acronyms

AES: Advanced Encryption Standard, chosen by IEEE 802.11i security task group and endorsed for secure government use; there is no known technique to break this code.

CIFS: Common Internet File System; defines a standard remote file-system access protocol for use over the Internet, enabling groups of users to work together and share documents across the Internet or within corporate intranets.

DoD: Department of Defense.

DSS: Digital Sending Software; enables users to distribute information securely via Novell and Windows authentication to Internet and LAN fax servers, network folders, and workflow applications.

EAP: Extensible Authentication Protocol, a Point-to-Point Protocol extension used by 802.1x; enhanced by TLS (Transport Layer Security) which provides mutual authentication and dynamic keying. Combined with AES, EAP-TLS is the holy grail of wireless LAN security.

EAP-MD5: Extensible Authentication Protocol-Message Digest 5. EAP-MD5; an EAP security algorithm developed by RSA Security that uses a 128-bit generated number string, or hash, to verify the authenticity of a data communication

EAP-TLS: EAP/Transport Layer Security. A high-security version of EAP that requires authentication from both the client and the server. If one of them fails to offer the appropriate authenticator, the connection is terminated

EWS: Embedded Web Server.

HTTP: Hypertext Transmission Protocol.

HTTPS:	Hypertext Transmission Protocol, Secure.
LEAP:	Lightweight EAP, officially called "EAP Cisco Wireless.
MFPs:	Multifunction peripherals.
MIB OID:	Management Information Base/Object Identifier;
PEAP:	Protected EAP.
RCFG:	Remote Configuration (SPX protocol)
mDNS:	Multicast DNS.
SMB/CIFS:	Server Message Block/Common Internet File System.
SNMP:	Simple Network Management Protocol.
SSL/TLS:	Secure Sockets Layer/Transport Layer Security.
WJA:	HP's Web Jetadmin, which is a simple peripheral management software application for remotely installing, configuring, and managing a wide variety of HP and non-HP network peripherals using only a standard Web browser. It can be used to proactively solve problems before they impact user productivity.

5 References

Multifunction Peripherals:

- Small & Medium Business Products:
  http://www.hp.com/sbso/product/mfp/index.html?jumpid=ex_R295_go/mfp
- Department Products:
  http://h10010.www1.hp.com/wwpc-JAVA/offweb/vac/us/en/sm/dept_prod_mfp/deptmfp_WF02.html
- Production Products:
  http://h10010.www1.hp.com/wwpc-JAVA/offweb/vac/us/en/sm/dept_prod_mfp/production_mfp_WF02.html

Multifunction Peripheral Accessories:

- HP MFP Analog Fax Accessory (Q1314A)
- HP High-Capacity Hard Disk (J6054B)

Secure Document Delivery:

- http://h71028.www7.hp.com/enterprise/cache/9128-0-0-225-121.aspx

JetCAPS Partner Solutions:

- Solutions Portfolio: http://h40041.www4.hp.com/uk/solutions/index.html
- Secure and Remote Printing: http://h40041.www4.hp.com/uk/solutions/category/secure.html
- Chai: http://h40041.www4.hp.com/uk/solutions/category/chai.html

Jetdirect Network Adapters:

- HP Jetdirect 680n 802.11b Wireless Print Server (J6058A)
- HP Jetdirect 620n Fast Ethernet Print Server (J7934A)
- HP Jetdirect 615n Fast Ethernet Print Server for Fast Ethernet (J6057A)

Hard Disk Drive Lock:

- PC Guardian HP LaserJet Printer Hard Drive Lock, Model 8300