hp

Protect your multifunction products, output, network communications, and management with HP.

Despite the critical roles networked imaging and printing resources play in the processes and workflows of large and small organizations alike, IT professionals frequently ignore security threats to the imaging and printing infrastructure and often leave it entirely unsecured. Imaging and printing environments aren't currently a primary target for network attacks, but this will likely change as hackers find traditional servers more difficult to exploit and look for other targets.

If IT fails to safeguard these valuable resources beforehand, attacks against unsecured network communications can endanger data confidentiality, which can increase litigation exposure and compromise compliance with government and industry regulations like the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act of 2002, the Patriot Act, the California Database Protection Act of 2001, the Gramm-Leach-Bliley Act (GLB), the Basel II Accord, the IPv6 Mandate, and SEC rules.[1] For example, print and digital-send jobs sent via traditional 802.11x networking can be intercepted, compromising the confidentiality and integrity of the information.

Imaging and printing security threats will undoubtedly increase. For instance, the Computer Security Institute reported in its 2005 CSI/FBI Computer Crime and Security Survey that unauthorized access rose dramatically in the last year and replaced denial of service as the second most significant contributor to computer crime losses. And recent publications by hacker groups have raised the awareness that imaging and printing devices are more than simple appliances and that these devices have capabilities beyond printing and scanning. Unauthorized data access isn't the only problem, either — denial-of-service strikes against networked MFPs and printers can diminish productivity, and unauthorized device usage can deplete consumables stocks and increase supplies costs.

HP has made security an integral component of its imaging and printing devices and solutions. In addition to supporting a wide range of standard, trusted security protocols, HP digital senders and HP LaserJet MFPs and printers offer industry-leading security capabilities and solutions that are designed to enable secure management, network communications, output, access, and device integrity. Moreover, HP has reduced complexity — the biggest obstacle to ensuring end-to-end security. Impressive security features are frequently ignored because IT can find them difficult to implement, so HP focuses not only on delivering state-of-the-art security capabilities, but creating seamlessly integrated, easy-to-use solutions, as well.

Protect your devices with HP.

- **Disk drive lockout** — The hard disk drive on many HP LaserJet MFPs and printers can be physically secured from theft and tampering using an accessory lock that requires a physical key for removal. Today most disk drives in MFPs and printers are insecure because they can be quickly removed — potentially leaving valuable data at risk.

- **Encryption** — Encryption of network-transmitted data stored on HP MFP hard disk drives is available via Capella Technologies' SecureDIMM II and other solutions. These accessory modules help secure the print job from the printing client to the MFP's or printer's internal printing engine, plus it keeps the print job encrypted while it is retained on the hard disk drive.

- **Hard disk overwrite** — HP MFPs and printers provide built-in capability for overwriting data stored on them, allowing sensitive data to be safely removed. HP offers multiple mechanisms to erase stored data, including sanitized erase functionality that conforms to U.S. DoD (Department of Defense) overwrite algorithm specifications.

- **Server-based access control** — All HP MFPs and digital senders offer server-based Windows NTLM, LDAP, Kerberos, and Novell authentication and authorization that integrates with your existing infrastructure to help your organization manage user access, prevent unwanted printing and digital sending, and help secure access to the management utility to prevent unwanted device configurations. With the exception of the HP 9085mfp and HP Color 9850mfp, all HP MFPs have device-based LDAP authentication (embedded from HP or installable from Capella Technologies). In addition, most HP MFPs have device-based Kerberos available. The HP Officejet 9130 All-in-One supports authentication, as well, via the optional C8267A Secure Digital Sending Solution DIMM. A wide variety of numeric keypad, proximity, and swipe-card solutions are also available, providing a very rich set of capabilities to meet your particular needs.

- **Color access control** — HP's suite of color access control features, available on some HP LaserJet MFPs and printers, lets you closely monitor color use, enable or disable color by individual users or groups or even applications, disable color printing and copying entirely until it's needed for special projects, and report costs back to specific clients, projects, workgroups, or departments.[2]

- **Control panel lock** — This feature within HP Web Jetadmin allows network administrators to deter unauthorized users from changing certain device configurations and control-panel settings by establishing a password and locking the control panel. You can choose from multiple levels of security, locking out specific control panel menus and allowing users to change the rest of the menus, or locking out all of the menus. It is even possible to lock the STOP button.

- **Private PIN printing** — HP MFPs allow a personal identification number to be associated with the print job, which will only be released after that PIN has been entered at the MFP's control panel. Enhanced capabilities, such as retrieval of print jobs at any HP MFP or printer and the use of proximity and swipe cards, can be applied using Ringdale's FollowMe or Capella Technologies' pull printing solutions.

- **Remote printing security** — Secure Document Express provides advanced document-encryption/decryption technology for HP devices equipped with embedded virtual machines. This third-party solution by Capella Technologies provides a fast and economical alternative to certified mail, courier services, and other secure document-delivery methods by allowing users to safely print to any SD-Express-equipped MFP or printer from anywhere on the Web.

Protect communications with HP.

- **Send digital data safely** — HP devices support a wide range of industry standard and trusted security protocols, including:

  – IPsec secure networking for MFPs and printers can be utilized in either IPv4 or IPv6 networks to encrypt information on the network and help ensure data gets to the destination(s) for which it is intended[3]

  – Wireless networking via such 802.1x authentication protocols as EAP-TLS, EAP-MD5, LEAP, and PEAP for access control and dynamic key encryption (WEP and WPA are supported wireless security features); 802.1x is also available for wired environments

  – Secure-IPP for encryption of print jobs

  – X.509 certificates for server/device authentication

  – IP (Internet Protocol) Access Control Lists for protected printing and management

- **Bridge-free faxing** — HP's analog fax accessory allows MFPs to act as standalone fax machines that prevent bridging of network to analog interfaces.

- **Protected document transmission via your intranet** — The Capella Technologies SecureDIMM II allows network encryption and flexible user-authentication methods that help provide a secure path from scan to application.

- **Protected document transmission via the Internet** — Genidocs Secure Messaging from Omtool integrates with HP's digital-sending technologies to help you protect paper documents you send over the Internet without requiring expensive security infrastructure or proprietary software.

Monitor and manage fleet security with HP.

- **Fleet-based security management** — HP Web Jetadmin provides powerful capabilities that allow you to efficiently and effectively manage security in environments with many devices, remotely manage all of your

organization's imaging and printing resources, employ SNMPv3 to encrypt data and control access, and utilize checklists to assure proper configuration.

- **Device-based security management** — For environments where few devices are deployed, IT may choose to manage each device individually via its embedded Web server's management interface, which employs HTTPS for encryption and access control. In addition, HP provides security wizards to assist in proper security setup.

- **Usage reporting** — You can track usage for all models by job, user, device, or application via the HP Web Jetadmin Report Generation plug-in.

- **Content security management** — HP even lets you control document access, revision, and lifespan via a variety of offerings, including HP Information Lifecycle Management Solutions and HP Secure Printing Solutions. Visit www.hp.com/go/ilm or www.hp.com/go/secureprinting for details on each respective offering.

Getting started.

The following recommendations can help you protect your organization's 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 intrusion-detection systems, as well as audit them 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 or passphrase via HP Web Jetadmin provides

significant benefits with little effort. The use of strong passwords or passphrases is important, and you should avoid easily guessed or short passwords

- **Use HP Web Jetadmin for enterprise-wide hardcopy management** — HP Web Jetadmin allows the consistent management of large numbers of networked MFPs and printers, plus it simplifies the discovery and tracking of newly added devices.

- **Eliminate the chinks in your imaging and printing armor** — Identify and replace single-function devices and/or MFPs that leave your organization vulnerable to security risks. Older devices in particular may lack recent innovations that can help protect your imaging and printing environment.

- **Consider direct-connected scanners** — While networked devices need to have security measures built into or deployed in conjunction with them to help ensure the integrity of an organization's printing and imaging infrastructure, standalone scanners that connect directly to a PC have virtually no adverse impact to the inviolability of the environment. For starters, a direct-connected scanner is inherently more secure because it inherits all of the security and permissions that IT has bestowed on the PC to which it's attached. Furthermore, even if someone tried to gain unauthorized access to the device, there would be no data available for theft or misuse since HP single-function scanners do not store information locally. And since single-function scanners are not well suited for placement in high-traffic areas where MFPs are found, the resulting lack of physical access to the device further limits unauthorized use.

- **Use protected protocols** — HP has made enabling encryption of device control communication

straightforward. We recommend the use of SNMPv3 for HP Web Jetadmin or HTTPS and TLS/SSL for embedded Web management.

- **Implement available security checklists and white papers** — HP's detailed security checklists provide step-by-step instructions for protecting devices. In fact, HP is the first MFP vendor to provide checklists approved by the National Institute of Standards and Technology (NIST). The checklist for the HP LaserJet 4345mfp can be found at http://checklists.nist.gov/repository/category.html under the "Multi-Functional Peripherals" heading.

- **Disable unused protocols and services** — Unused and ignored protocols and services are a common backdoor for attacks.

- **Use print 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 help ensure only authorized users may print to, as well as 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. Many HP LaserJet MFPs and printers can be equipped with a standard Kensington lock to prevent unauthorized disk-drive removal.

- **Utilize HP partner solutions for increased hardcopy security** — HP has developed partner solutions that provide leading security capabilities for imaging and printing environments.

HP offers an array of offerings to help secure your imaging and printing environment. Visit www.hp.com/go/secureprinting for details about third-party data integrity, access control and authentication, and audit solutions available for HP LaserJet MFPs and printers. Visit www.hp.com/go/security to download The HP Security Handbook, a comprehensive guide for protecting your business, or for details about specific HP Security Solutions like HP Security Governance, HP Identity Management, HP Proactive Security Management, and HP Trusted Infrastructure offerings.

LTR version 1.5 • 1/27/06