

Practical considerations for imaging and printing security



Overview.....	3
Imaging and printing security	3
Common Criteria Certification.....	3
IEEE p2600.....	4
Security checklists	4
Conclusion: look beyond Common Criteria Certification	4
HP's imaging and printing security framework.....	4
Secure the Imaging and Printing Device.....	5
MFP walk-up authentication	5
Network printing authentication	5
Physical document access control	5
HP Secure Erase.....	6
Vulnerabilities, viruses, and worms	6
Protect Information on the Network	6
Network connectivity with HP Jetdirect devices.....	6
HP Digital Sending Software (DSS).....	7
Fax/LAN bridging.....	7
Effectively Monitor and Manage	7
HP Web Jetadmin for fleet management.....	7
Device and service control.....	7
Firmware updates.....	7
Logging device activity.....	8
Common Criteria Certification	8
The future of imaging and printing security	8
Document security and Digital Rights Management	8
Trusted Computing Group	8
Conclusion.....	9
Appendix A—Access controls	10
HP Digital Sending Software 4.0	10
HP Job Retention and PIN Printing.....	10
Capella Technologies VeriUser Authentication	10

Jetmobile SecureJet-PS Secure Print Product	10
Jetmobile Technologies SecureJet Authenticator Products	10
SafeCom	11
Ringdale FollowMe printing	11
Appendix B—HP Secure Erase	12
For more information	13

Overview

The IT security climate has changed. While in the past the challenge has been to convince customers of the need for security, the current need is to show how a product's security capabilities complement a customer's existing security environment.

Security measures have evolved through the years, from firewalls that kept intruders out, to sophisticated virus throttling systems that detect viruses before they take hold and prevent them from spreading. Attacks now often originate from inside the network, for example: employees take advantage of access, wireless networks are improperly secured, and unaware users introduce viruses or worms to the secure network.

As attacks increase in sophistication, hardening the internal network's security—from clients and servers to the imaging and printing infrastructure—becomes critical. Further, regulatory requirements, including Sarbanes-Oxley and the Health Insurance Portability Protection Act, are mandating protection accountability.

Imaging and printing security

Security of the imaging and printing environment has long been ignored by IT administrators. Printers and scanners have been considered little more than network appliances, posing none of the risks of client and server PCs. 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.

This whitepaper explains the threats and risks unique to imaging and printing environments and provides recommendations and strategies to prevent their effects. Parallels to common security capabilities are drawn to aid in explaining hardcopy-specific needs. Imaging and printing devices are put into the context of regulatory requirements, although—as will be seen—there is no simple solution.

Common Criteria Certification

While Common Criteria Certification provides a valuable means for assessing the security capabilities of a product, it is important to understand the true significance of Certification, what Common Criteria is and is not, and the role Common Criteria Certification plays in imaging and printing manufacturer's marketing differentiation claims.

Common Criteria Certification provides no credible means for assessing the true security capabilities of hardcopy products today, and should not be used as a measure for purchasing requirements. Common Criteria does not dictate necessary security functionality, it merely provides a means to assess the correctness of a manufacturer's implementation claims.

The varying levels of EAL (Evaluation Assurance Level) certification foster further confusion. Higher certification levels are assumed to provide greater levels of security. However, as certification reflects only the manufacturer's functional claims, the higher levels of certification are frequently meaningless.

The majority of the hardcopy industry currently certifies Disk Erase and Analog Fax functions, but this certification does not accurately portray a product's security capabilities or vulnerabilities. A product may advertise certification of these capabilities while providing no, or rudimentary, protection for the remaining system.

To ensure Common Criteria Certification provides value, it is important to understand the product's complete range of capabilities versus those for which certification is claimed. While certification can prove what a product does properly, it says nothing of what a product does not do, and to what degree that omission represents a security risk.

IEEE p2600

The IEEE p2600 working group is defining a security standard for hardcopy devices, as well as recommendations for the security capabilities of devices when deployed in various environments, including enterprise, high-security, small office/home office, and public spaces.

The p2600 working group has broad industry participation, including Hewlett-Packard, Lexmark, Canon, Xerox, Sharp, Ricoh, IBM, Epson, Okidata, Equitrac, and Océ.

The p2600 standard will provide a means for credibly measuring the security capabilities of individual manufacturers. HP is actively participating within the working group, and will Common Criteria-certify products to the standard when complete. As of this time, HP devices support the majority of capabilities specified in the draft documents.

Security checklists

The National Institute of Standards and Technologies (NIST) has been tasked by U.S. legislation to develop checklists that facilitate security configuration of devices likely to be used by the U.S. Federal Government. NIST has requested IT equipment manufacturers to develop these security checklists for their products. Details of the checklist program are available at <http://csrc.nist.gov/checklists>.

NIST will review manufacturer's checklists for relevance and correctness and publish those checklists on a searchable NIST website.

HP considers security checklists as a means to significantly improve the security capabilities' ease of configuration for imaging and printing products. A security checklist for the HP LaserJet 4345mfp is available for public review at <http://checklists.nist.gov/repository/>, and is currently the only available hardcopy product checklist available from any manufacturer. HP plans to develop additional checklists for hardcopy devices in the future.

Conclusion: look beyond Common Criteria Certification

Ultimately, individuals must look carefully at their requirements and not be swayed by manufacturer advertising claims. Common Criteria Certification adds significant cost and development time to products, while providing limited assurance to the product's actual capabilities and potential vulnerabilities. Products that are not certified may actually provide more robust security capabilities than products that are certified. NIST security checklists simplify the complex process of enabling security functions, and better illustrate the product's capabilities

HP's imaging and printing security framework

To simplify the presentation of security concepts, HP developed an imaging and printing security framework with three categories of security functions:

Secure the Device	Includes elements that protect the function of the physical device, including access controls for management and use, secure deletion of files, and physical security.
Protect Information on the Network	Includes network communications, including media access protocols such as 802.1x and secure management, scanning, and printing protocols.
Effectively Monitor and Manage	Includes the capabilities to securely manage fleets of imaging and printing devices and audit devices for compliance to security policies and regulatory requirements

The categories within HP's imaging and printing security framework are built from traditional network security theory, which identifies the four elements that compose a secure system: confidentiality, access control, integrity, and non-repudiation.

In addition to directly implementing extensive security capabilities in the device, HP strategically partners with companies through the Global Solutions Catalog (www.hpgsc.com) to provide enhanced imaging and printing security, as well as solutions tailored to individual customers and environments. The breadth and depth of the capabilities provided by HP and its partners uniquely poises HP as the leader in imaging and printing security.

Secure the Imaging and Printing Device

Secure the Imaging and Printing Device includes capabilities that provide access controls to the functions of the device and ensure the integrity of its operations.

Access controls limit MFP and printer functions to authorized users and include:

- *Walk-up* capabilities such as copying and digital sending
- Network printing
- Physical access to printed documents

Authentication requirements vary by environment, as do integration requirements to existing authorization mechanisms.

MFP walk-up authentication

MFPs can require users to be authenticated before accessing MFP functions via the device control panel. MFPs can restrict access to digital sending functions and restrict digital sending email destinations based on user. MFPs can control access to installed functions and installed applications (e.g. HP Autostore) based on user. Device usage may also be tracked with associated users.

Integrating MFP access controls with existing enterprise access controls reduces complexity and minimizes administration requirements. HP and its partners support a wide variety of authentication mechanisms, including Windows® Domain accounts, proximity cards, and Smartcards.

HP's Digital Sending Software (DSS) enables Windows and Netware authentication using an intermediary server, while Capella Technologies' VeriUser provides Windows authentication embedded in the MFP. Jetmobile's SecureJet, Ringdale's FollowMe, and SafeCom external authentication each provide Smartcard, swipe card, and proximity card capabilities.

Network printing authentication

Printers and MFPs may enforce access controls for network printing to restrict usage of devices and the use of high-value consumables. Auditing systems may also use the access controls to log user activity, such as dates and times of documents printed.

The HP Output Server and the Microsoft® Print Spooler provide direct integration of Domain accounts with printing access controls, which allows control of individual users and groups, including access rights to network printers.

Physical document access control

Documents in the output bin of a network printer are at risk for unauthorized access. *PIN* and *Pull Printing* allow print jobs to be saved electronically in the device, or on an external server, until the authorized user is ready to print them. The user provides a simple PIN code, or uses an authentication method supported for other MFP walk-up operations, to release the print job. HP printers and MFPs provide native support for PIN printing, while Jetmobile, Capella Technologies, Ringdale, and SafeCom each provide solutions integral to their authentication products.

For more information on Access Controls, including HP and partner solutions, see Appendix A, "Access controls," on page 10.

HP Secure Erase

HP Secure Erase implements the Department of Defense (DoD) 5220-22m specification for the deletion of data from hard disk storage. DoD 5220-22m specifies an algorithm to repetitively overwrite hard disk data sectors to remove all trace magnetic information.

For more information on HP Secure Erase, see Appendix B, “HP Secure Erase,” on page 12.

Vulnerabilities, viruses, and worms

Vulnerability assessments are an integral step in HP’s imaging and printing product development, and as a result these devices have been affected little by the viruses and worms that afflict enterprise networks. While the ingenuity of hackers continues to evolve, HP ensures its products meet the threat posed by hostile network environments.

- **Chai**

HP’s Chai provides a means to extend an imaging and printing device’s functionality. For example, Capella Technologies’ VeriUser Authentication is implemented as a Chailet. Access controls restrict installation of Chailets to authorized administrators, however, as it is important to avoid installing malware on PCs, Chailets should only be installed from known and trusted sources, such as HP and its partners.

Protect Information on the Network

Protecting Information on the Network insures that network communications between users, administrators, the imaging and printing device, and the workflow are confidential and prevent unauthorized modification by maintaining their integrity.

Network connectivity with HP Jetdirect devices

Network connectivity for HP imaging and printing devices is provided by the HP Jetdirect family of products, including internal cards, external boxes, and embedded networking. HP Jetdirect provides many secure network protocols and services, including:

802.1x for Wired Networks	Provides access control to the Ethernet network. Network devices that are unable to authenticate to the 802.1x authorization server have all network access denied. 802.1x can prevent unauthorized users from attaching devices to the network as well as insure that only IT deployed and trusted devices, such as those with virus protection software, are allowed access.
IPsec	Allows for strong authentication, confidentiality, and integrity of communications, and can secure network printing and scanning protocols. The HP Jetdirect 635n IPv6/IPsec and Gigabit Ethernet internal print server, available November 2005, uses a cryptographic accelerator to provide <i>click-to-clunk</i> performance that rivals unsecured protocols, and supports the IPsec implementations available in all current major operating systems, including Windows, Unix®, and Linux®.
SNMPv3 and HTTPS	Provide secure management of the imaging and printing device. SNMPv3 provides strong authentication and encryption of management communications and is used by HP Web Jetadmin to provide fleet management of HP imaging and printing devices. HTTPS using SSL/TLS provides security of web protocols and is used for secure management using the device’s embedded web server, as well as security of web services such as consumable reordering.
Secure IPP (IPP-S)	The secure form of the IPP protocol using SSL/TLS, secure IPP requires no additional configuration and is primarily intended for small networks lacking sophisticated IT administration. While Secure IPP may be used in large enterprise environments, IPsec is the recommended protocol for securing printing and scanning functions.

HP Digital Sending Software (DSS)

HP Digital Sending Software 4.0 can encrypt scanned documents between the MFP and the DSS Server. The DSS Server may then use the “Secondary email” function to store the encrypted document in a location accessible to third-party applications, such as Omtool, that then securely retransmit the document to its final destination via email. In addition to the secondary email function, secure sending to email, fax, and network folders may be achieved by securing the network communications between the DSS Server and the remote server using IPsec.

To control email distribution, the SMTP server used by the DSS Server may be configured to enforce internal security policies. Such policies may prevent digital sending to email addresses outside of the internal network or analyzing the content of digitally sent documents to prevent breaches of confidentiality.

Fax/LAN bridging

The analog fax port of an HP imaging and printing device is isolated from the digital network connectivity of the device. Communications to the analog fax are routed directly to the device formatter and cannot be bridged to the digital network, preventing the threat of an attacker connecting to the analog fax through a telephone line and then gaining access to an internal network.

HP is currently in the process of receiving Common Criteria Certification to validate this behavior in the HP LaserJet 4345mfp and 4730mfp.

Effectively Monitor and Manage

Effectively Monitor and Manage allows for imaging and printing infrastructure maintenance and enables auditing to facilitate compliance with policy and regulatory requirements. Effectively managing network resources is critical to maintaining a secure network.

HP Web Jetadmin for fleet management

HP Web Jetadmin (WJA) is the backbone for the administration and maintenance of imaging and printing products, for both HP and its competitors, deployed on enterprise networks. *Fleet or batch* management enables consistent management and security policy enforcement across a large number of imaging and printing devices. WJA can manage any device that supports the SNMP Printer MIB and allow manufacturers to develop device-specific extensions using plug-ins.

WJA uses SNMPv3 to ensure authenticated and confidential management of networked devices. WJA allows devices to be manually administered and can automatically discover and configure newly installed devices.

Device and service control

Imaging and printing devices support many network protocols and services. Protocols and services that are unused often go ignored, resulting in unintended vulnerabilities, such as unsecured management interfaces or printing protocols that circumvent job accounting controls. HP imaging and printing devices allow individual control over these protocols and services and let administrators enable only the functionality required.

Firmware updates

Firmware updates can correct product defects and enhance product functionality, and they are an important means for preventing the exploitation of security vulnerabilities. It is important for IT and security administrators to monitor the availability of firmware updates and apply as necessary. HP releases firmware updates based on the severity of the defect and provides administrators the ability to receive automatic email notifications of releases.

HP Web Jetadmin allows an administrator to discover devices using out-of-date firmware and update those devices automatically over the network.

Logging device activity

Logging device activities ensures compliance to security and access policies. HP DSS, Capella, SafeCom, and Ringdale each allow device activity, including user, document, and destination, to be monitored. Logging functions can also include configuration and management actions.

Common Criteria Certification

HP is currently in process of receiving Common Criteria Certification for Disk Erase and analog fax capabilities for the HP LaserJet 4345mfp, 4730mfp.

HP supports the IEEE p2600's development of an imaging and printing security standard that will allow credible industry-wide Common Criteria Certification and expects to certify products to the standard when available.

The future of imaging and printing security

Document security and Digital Rights Management

Document security is evolving. Driven by Digital Rights Management, developers are focusing on the security of the content, rather than the security of the application that transports it. Current, rudimentary, examples include document password protection by application (e.g., Excel spreadsheets and Word documents). Passwords provide basic, limited capabilities.

Adobe® Systems (PDF) and Microsoft (Metro) have both introduced content protection capabilities in their respective document formats, allowing control over individual access to documents, limits on document redistribution, and automatic expiration of content after a defined date.

As content protection evolves, the enforcement of controls will move from PC-based applications that render documents for devices, to the devices themselves. Likewise, content originating at a device (e.g., scanned documents) will immediately receive content protections, rather than rely on attached PC-devices to provide it.

Trusted Computing Group

The Trusted Computing Group (TCG, www.trustedcomputinggroup.org) is a standards organization with over 100 member companies developing standards to enhance the trustworthiness of computing equipment. HP chairs the Hardcopy Work Group, which is responsible for standards related to imaging and printing devices. Trusted Computing will ensure devices operate with a greater level of integrity. Trusted imaging and printing platforms will allow both IT administrators and users to validate the trustworthiness of a device prior to its use. Such trusted capabilities could ensure that only authorized MFPs are allowed access to the network, that designated MFPs are the actual originators of documents, and that printers cannot replicate print jobs without user permission.

Conclusion

HP imaging and printing has evolved with enterprise security needs. HP offers imaging and printing devices with a broad range of security capabilities, including high-security products that allow operations in the most demanding environments and the tools to effectively manage large-scale deployments of those devices.

While it would be impossible to prescribe all of the security requirements for an enterprise's imaging and printing environment, the following recommendations may be used as a starting point for enabling that security.

- 1. Assess Common Criteria Certification needs**

Today, features being certified by the hardcopy industry are not representative of the true risks that face imaging and printing devices. It is critical to scrutinize certification and assess the capabilities of the device against actual needs.
- 2. Fleet/batch manage using HP Web Jetadmin**

HP Web Jetadmin provides consistent management of enterprise-deployed imaging and printing devices and is critical for maintaining a secure environment. Fleet management aids in the consistency of policy enforcement and assists in audit and regulatory compliance.
- 3. Update firmware images**

Firmware updates protect against product defects and vulnerabilities. HP provides automated firmware update notification services, and HP Web Jetadmin aids in deploying updates across enterprise environments.
- 4. Disable unused ports and services**

Frequently, imaging and printing devices have unused capabilities that are enabled. In some cases, these capabilities may enable functionality counter to the intent of the administrator, such as leaving insecure management protocols accessible, when only encrypted management is desired.
- 5. Implement access controls**

HP printers and MFPs allow a variety of user-level authentication mechanisms, including passwords, proximity cards, and Smartcards. Access controls can ensure that only authorized users utilize the imaging and printing infrastructure, while authentication capabilities provide assurances of who is using the environment, and how they are using it, which aids in audit and regulatory compliance.
- 6. Implement secure protocols**

The sophistication necessary to *sniff* network traffic has been reduced by the distribution of hacking tools, as well as by legitimate network analyzers. IPsec secures existing printing and scanning applications with strong encryption, while SNMPv3 and HTTPS secures management functions.

Appendix A—Access controls

HP Digital Sending Software 4.0

HP Digital Sending Software allows MFPs to digitally send documents to a variety of destinations, including email, fax, and network folders.

DSS allows the MFP to authenticate a user prior to allowing access to MFP functions. DSS allows integration of authentication functions with Microsoft Windows (using NTLM or Kerberos) and Novell Netware (using Bindery or NDS) operating systems. If authentication is enabled, users are prompted for their username, password, and domain/tree by the MFP. The MFP then transmits these credentials to the DSS server, and the DSS server authenticates the user to the Windows or Novell system as appropriate.

If a remote network folder requires authentication for access, the user's previously provided credentials are used. If the user has not previously provided their user credentials, they are prompted to enter them to access the network folder.

HP Job Retention and PIN Printing

HP provides support for PIN printing on a variety of HP LaserJet platforms, including the HP LaserJet 2300, 2400, 4250, 4350, and LJ 5500 printers in conjunction with current PCL print drivers.

Capella Technologies VeriUser Authentication

Capella Technologies offers authenticated user access to MFP and digital sender functions in Windows environments through the VeriUser Authentication Solution. VeriUser consists of VuLDAP and VuNTLM, available as either a hardware module or software update, that can be installed on a wide range of existing MFP devices.

The printer administrator may specify which MFP and digital sender functions require authenticated access. As necessary, users are prompted for their user credentials, and the MFP authenticates access with the local Windows server using LDAP or NTLM.

VuLDAP authenticates users via the LDAP protocol and supports:

- HP LaserJet 4100mfp, 9000mfp

VuNTLM authenticates users via Microsoft's NTLM protocol, which provides encryption of account credentials, and supports:

- HP LaserJet 4100mfp, 4345mfp, 9000mfp, 9040mfp 9050mfp
- HP Color LaserJet 9500mfp, 4730mfp
- HP Digital Sender 9200c

Jetmobile SecureJet-PS Secure Print Product

SecureJet PS supports a variety of authentication mechanisms for retrieving print jobs. A basic PIN may be used for job retrieval, using either the MFPs control panel or an add-on terminal, or a more advanced swipe card, proximity badge, or Smartcard can be used. Authentication provided by SecureJet may be integrated with Capella's MegaTrack software tool for job accounting.

Jetmobile Technologies SecureJet Authenticator Products

Jetmobile have a series of authentication products including user pin (SecureJet FP), Smart Card (SecureJet SC), Proximity Card (SecureJet PX), or Swipe Card (SecureJet SW). These authentication products can be used to authenticate MFP functions and supported applications. Authentication

provided by these SecureJet products may be integrated with Capella's MegaTrack software tool for job accounting.

SafeCom

SafeCom provides a suite of security capabilities, including Pull Printing and authenticated MFP device access. As with Jetmobile, SafeCom supports a variety of hardware authentication devices, including magnetic swipe cards and proximity badges. SafeCom provides optional encryption for communications and allows the authentication to be integrated with job tracking and billing tools. SafeCom is deployed using the DIMM module on HP LaserJet 4100, 4200, 4300, 9000, 9055, and 9065 devices, and HP Color LaserJet 4600, 5500, and 9500 devices. Other printers and MFPs are supported by external SafeCom equipment that attaches via a parallel or network port.

Ringdale FollowMe printing

Ringdale provides Pull Printing, as well as access controls to printing and scanning functionality. Jobs are stored on the FollowMe Q-Server and users may be authenticated using a variety of hardware authentication mechanisms, including proximity cards and Smartcards. FollowMe Hardware for job release is an external hardware component, allowing compatibility with a large range of printers and MFPs.

Appendix B—HP Secure Erase

HP Secure Erase implements the Department of Defense (DoD) specification 5220-22m algorithm for the deletion of data from hard disk storage. Typically when files are erased from a disk, they are simply *marked* as removed, however the data remains on the drive and can be recovered with *undelete* tools. The DoD 5220-22m algorithm specifies the repetitive overwriting of the disk data to ensure no trace magnetic data remains. Data erased using the DoD 5220-22m algorithm is considered unrecoverable.

Secure Erase can occur continuously as files are deleted, or erase the entire disk when triggered by an administrator or a regularly scheduled event configured by HP Web Jetadmin.

HP Secure Erase is available on the following devices:

- HP LaserJet 2400, 4250, 4350 printers
- HP LaserJet 4100mfp, 4345mfp, 4730mfp, 9000mfp, 9000Lmfp, 9040mfp, 9050, 9050mfp, 9055mfp, 9065mfp
- HP Color LaserJet 5550 printer
- HP Color LaserJet 9500mfp

For more information

- Please see the “HP Secure Erase for Imaging and Printing” whitepaper (www.hp.com/sbso/security/secure_disk_erase.pdf) for complete details of algorithms implemented and devices supported.
- Capella Technologies: www.capellatech.com
- Global Solutions Catalog: www.hpgsc.com
- Jetmobile: www.jetmobile.com
- National Institute of Standards and Technologies checklist: <http://csrc.nist.gov/checklists>
- Ringdale: www.ringdale.com
- SafeCom: www.safecom.dk
- Trusted Computer Group: www.trustedcomputinggroup.org

© 2003 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Linux is a U.S. registered trademark of Linus Torvalds. Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. UNIX is a registered trademark of the Open Group.

XXXX-XXXXEN, 09/2005

