

SPOTLIGHT ON SECURITY

1 in a series of 4



What you should know to get the most from built-in security protection

According to an article published in the online journal *ComputerWeekly.com*, more than 70 percent of Fortune 1,000 companies in the US are increasing their security budgets to meet regulatory and audit compliance requirements such as Sarbanes-Oxley and the Payment Card Industry (PCI) data security standard.¹ Not a bad idea, considering that the Privacy Rights Clearinghouse reported more than 100 million personal records to have been improperly exposed from 2005 through 2006.²

As technology improves in response to such threats, malicious forces (both internal and external) have begun to search for new ways to exploit networks. Because today's printing and imaging technology is networked and provides much the same functionality of a computer or server, it is being increasingly targeted for attack. HP printing and imaging devices and network management tools are designed to support a wide range of industry-standard security protocols, as well as class-differentiating functions and solutions allowing for secure management, device integrity, privacy and access control (see sidebar below). Here are some important things you should know to get the most from HP's industry-leading technology.

Don't assume your firewall has got it covered.

To ensure out-of-the box plug-and-play availability, HP printing and imaging devices are shipped with open security settings. HP highly recommends that an organization subsequently configure these settings based on its unique IT environment and security concerns. Yet many organizations may never take this step, falsely believing that their network firewall provides all of the protection required to protect these valuable assets. Nothing could be further from the truth. In fact, a recent insider-threat study sponsored the US Department of Defense reveals that the majority of security incidents take place from within the organization.³ Whether they are caused intentionally (by a disgruntled ex-employee, for example) or unintentionally, an internal security breach can be every bit as damaging as the external variety in terms of its effect on things like consumer confidence and the integrity of sensitive or proprietary business intelligence.

Security settings must be turned on to ensure maximum protection.

HP has made security an integral component of its imaging and printing devices and solutions as evidenced by the large number of security settings built in to many HP printing and imaging devices. As previously mentioned, however, these safeguards cannot be effective if they are not enabled. HP Web Jetadmin is a simple software tool for managing printing and imaging peripherals, and it can be used to enable these safeguards in multiple HP devices simultaneously (via configuration or by creating a security profile which can then be downloaded to networked devices). HP Web Jetadmin is available as a free download at <http://www.hp.com/go/webjetadmin>. HP Web Jetadmin consulting services are available on a contractual basis. In addition, HP has prepared a comprehensive step-by-step guide to configuration best practices entitled "Configuring Security for Multiple LaserJet MFPs and Color LaserJet MFPs." This document was written by HP and approved by the National Institute of Standards and Technology (NIST). You'll find it at the NIST website at <http://checklists.nist.gov/repository>.

HP is the first printer vendor to have:

- » A security checklist approved by the National Institute of Standards and Technology.⁴
- » A US Department of Defense (DoD) approved IPsec solution.

Pick your passwords with care.

As part of the device configuration process, you will be asked to create several passwords. Here are some widely accepted password best practices to keep in mind as you complete this task:

- » Use the maximum number of possible characters. Many of these password settings will accept as few as one character, but one character is easy to guess. Data shows that it is extremely difficult to guess a password that has seven characters or more using current password-cracking tools.
- » Use complicated passwords with a variety of character types. Some passwords allow only numeric digits, but others can accept 96 or more different characters (upper case, lower case, numeric, special characters and punctuation marks).
- » Use meaningless random passwords. Passwords that are real words or phrases are easier to guess.
- » Use a different password for every password setting. Many password-cracking tools can pick up on patterns, which makes guessing easier.
- » Record your passwords in a safe but hidden place. These passwords are designed to restrict access to management options. Losing a password can eliminate your access to settings.

Printer Security Risks

Risk: Network printers have more vulnerable services running on them than networked PCs do.

Possible attacks	Solutions
Remote code execution	Disable services you don't need.
Sniffing (for passwords and network information)	Use vendor-provided document protection features.
Capture of intellectual property from documents in queue or in local memory	Change default passwords and encrypt them.
» Root control of printer services	

Risk: Network printer applications have a growing number of vulnerabilities.

Possible attacks	Solutions
Buffer overflows	Perform better code review.
Cross-site scripting and other common attack methods that disable an application and gain root control	Adopt more secure application development processes.

Risk: Web interfaces, Web servers, Web pages and e-mail are opening printers directly to the Worldwide Web.

Possible attacks	Solutions
Hijacking or impersonating a remote administrator or user session	Turn off Web connections unless absolutely needed.
Malicious code injection	Use strong authentication for remote administration.
Remote control of printer	Change default passwords.

Source: ComputerWorld[®]

How secure is secure enough?

There is no such thing as a one-size-fits-all solution when it comes to securing your printing and imaging devices and infrastructure. HP provides a wide array of products, tools, expertise and services to help you elevate the status of your printing and imaging devices to your overall security plan. Visit HP's secure printing website at www.hp.com/go/secureprinting for more information.

Why HP for printing and imaging security?

HP has been an industry leader in printing and imaging innovation and reliability for more than 20 years. Whether you need to buy one printer, enhance the security of your entire fleet or you want to improve and transform the way you manage your printing environment, HP has the expertise, experience and technology to deliver the right solution, right now.

Looking for more accountability, security and a better return on your printing and imaging investments? HP Managed Print Services can:

- » Quantify the total costs of your existing printing and imaging infrastructure
- » Help you identify savings opportunities and reconfigure your environment to take advantage of them
- » Provide ongoing supplies, service and support designed to meet your company's unique business needs
- » Monitor performance to maintain cost-effective and secure operation over time
- » Manage your printing and imaging environment for improved business results

Your local HP representative can help you explore a variety of cost-effective strategies for securing and enhancing your printing and imaging environment today and into the future. They can even help you create a comprehensive security strategy that addresses your organization's specific printing and imaging security concerns.

Want to know more?

- » HP provides a wide array of secure printing and imaging solutions for HP LaserJet printers and HP MFPs. Visit www.hp.com/go/secureprinting for details.
- » To learn more about HP Managed Print Services visit us online at www.hp.com/go/mps and www.hp.com/go/printservices
- » For the remaining white papers in this series plus the latest research, tips and tools for lowering costs and improving IT, visit the HP Printing and Imaging Resource Center at www.hp.com/large/ipg

Want to know more?

See what other people in your industry are doing to manage their environments and keep their data safe. Visit www.hp.com/blogs/enterpriseprinting to see what is going on.

Notes

1. *ComputerWeekly.com*, March 26, 2007
2. www.privacyrights.org/ar/ChronDataBreaches.htm
3. "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," CERT Program, Software Engineering Institute, December 2006
4. <http://checklists.nist.gov/repository/vendor.html>
5. "The Surprising Security Threat: Your Printers," *ComputerWorld*, Deb Raddliff, January 2007

Visit us on the web at www.hp.com/large/ipg



© 2007 Hewlett-Packard Development Company, LP. 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 statement 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.

4AA1-5143ENUS, September 2007