Secure Print Advantage Protects Printers Against Hacking

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

This is the second of a two-part series by Dale Morris and Gary Lefkowitz of Hewlett-Packard looking at printer security.

* * *

Technology development has outstripped the earlier IT view of security in the imaging and printing environment. Printers and imaging devices were considered simple network appliances, with none of the risks of desktop PCs and servers. However, these devices have grown in sophistication – running full-capability operating systems like Linux, Windows and with features like built-in FTP services and Web servers.

Vulnerabilities exist in the network flow (client to print server, print server to printer) and the printer itself (printer memory awaiting print, output tray awaiting pickup). In addition, inadequate authentication and insufficient print activity records can compromise security. In general, there is little or no control over the IT infrastructure responsible for printing.

Traditional secure-printing initiatives have generally employed a heterogeneous mixture of four different types of point solutions:

- secure the device,
- protect the network,
- encrypt the document, or
- effectively monitor and manage printing and audit devices.

Although they do work, these solutions cannot guarantee security policy enforcement, and the task of integration is non-trivial.

Securing print and imaging devices requires creating access controls for management and use, securing file deletion, and even locking the doors to the printing station. However, securing the device alone does not create a secure print environment. For example, users can reset the device without the knowledge of the security administrator. To be secure, the devices must also work within a secure network which is overseen by security policy.

Forty years ago, banks thought that simply protecting networks would solve ATM security problems—but that didn’t work. Adding enforcement policies on the network, however, caused ATM abuses to decline. Printing and imaging security is similar. Protecting the network with simple link-layer security (such as IPSec or other point solutions) fails for many reasons. For example, IT departments and Intrusion Detection Systems (IDSs) do not typically check printing applications, even though they are subject to Trojan horses and viruses. Anyway, policy enforcement across a large number of imaging and printing devices can be circumvented and data integrity can be compromised. Securing the network, although important, is not enough to create a secure print environment.

Document encryption – another important component of secure printing – has its own
drawbacks, particularly manageability. For example, if the printer gets out of crypto-sync (i.e.,
the requirement that encryption and decryption keys must remain synchronized at all times), an
administrator must manually press a configuration button. This can cause printing of the crypto-
key, defeating its purpose. Improper key management ignores expected security standards and
creates a non-secure network environment.

Managing heterogeneous print devices and authentication systems also has challenges. Multiple,
competing security and authentication systems within the same environment are not easily
integrated. Ad-hoc and inconsistent security implementations leave users more vulnerable to
attack and administrators burdened with extra administrative tasks.

Truly secure printing must integrate device security, network security, encryption, and security
policy. Comprehensive, end-to-end solutions (such as HP’s Secure Print Advantage <
http://www.hp.com/go/spa >) do exist. Look for a solution that allows you to overlay your
existing network rather than completely reconfiguring it. Be certain that the solution provides
policy-based management with support for multiple roles (e.g., security administration vs. printer
support vs. audit) and that it has government certifications such as _FIPS 140-2 Federal
Information Processing Standards and Common Criteria._ <
http://csrc.nist.gov/publications/PubsFIPS.html >

[MK adds: my HP colleagues were too diffident to add more references, but I looked up the
Secure Print Advantage page and found pointers to an informative online demonstration <
http://h20223.www2.hp.com/NonStopComputing/cache/564666-0-0-0-121.html > and a white
paper elaborating on the approach.<
think it’s interesting – and I don’t work for HP any more!]

* * *

Dale Morris graduated with an MSEE from University of Missouri at Columbia in 1980. He is
currently a processor architect with HP in Colorado with experience in hardware
implementation, hardware/compiler partnership for optimal performance, OS functionality and
performance optimization. His focus is on constructing and leading technical teams within and
across companies. You may write to him at < mailto:dale.morris@hp.com >.

Gary Lefkowitz is Director of Marketing and Operations, Enterprise Storage and Server Security
at Hewlett-Packard in Palo Alto, Ca. He has a distinguished career spanning more than two
decades in marketing and management at Compaq, Tandem, Informix, Molecular Computing
and HP.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information
Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of
Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <
mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2007 Dale Morris, Gary Lefkowitz & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without
limit on any Web site, and to republish it in any way they see fit.