Your Printer – An Open Door for Hackers?

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

In April 1981, I was sent to Hewlett-Packard (HP) headquarters in Cupertino, CA on a six-month assignment to be trained as an HP3000 operating systems internals and performance specialist and also to work on a pioneering computer-based training system I invented for the company. I brought my flute along and met a friendly lab engineer called Dale Morris who played excellent guitar. We had a good time playing duets that summer. I remember that he was working on a new series of HP3000 machines with a vastly increased memory space: 4 GB. I laughed and wondered why anyone could possibly need so much main memory – especially since a 1 MB memory board still cost $64,000 at that time (about $200,000 in today’s currency).

Today, I have 2 GB of RAM on my main tower PC and Dale Morris is a Distinguished Technologist at HP in Fort Collins, CO. Recently he told me about an interesting security issue involving printers and I invited him to tell us about it in this column. The remainder of today’s contribution is entirely Dale’s with minor edits.

* * *

In 1999, TechWeb reported an alleged printer-based attack on the Space and Naval Systems Warfare Center in San Diego, California (SSC San Diego). A network operations engineer noticed that a local print job took an unusually long time. After examining the problem, he concluded that a network intruder had hacked into the printer and reconfigured the routing tables – so that the print job shipped to Russia!

We’ve all thought about security as it applies to printing. Your organization probably has written policies governing who can print certain documents and where and when they can be printed. But such policies are difficult to enforce; for example, authorized users printing sensitive documents might find the documents missing from the tray of a shared network printer. Furthermore, informal policies aren’t the best support for audit requirements, and such approaches address only a subset of printer security issues. You might be surprised to learn that your database server could be attacked by a rogue printer.

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 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, 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 an 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 ____.

* * *

Dale Morris graduated with an MSEE from University of Missouri at Columbia in 1980. He is currently a processor architect 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>.