Your Printer – An Open Door for Hackers?

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

On August 7, 2003, a staff member at the Public Health Laboratory of the Ministry of Health and Long Term Care of the Province of Ontario in Canada tried to send a fax to a doctor’s office. (By the way, for US readers, Canada is the large blank pink region north of the border on your maps and which, contrary to popular belief, actually includes people as well as moose and beavers.) Alas, the clerk mistyped a 5 as an 8 in the fax number and inadvertently sent medical records to a local gasoline station. The owner very kindly gave the fax to a doctor who was a regular customer and the doctor reported the breach of the _Freedom of Information and Protection of Privacy Act_.<http://www.accessandprivacy.gov.on.ca/english/pir/prov/pc030034.htm>

Everyone knows that fax misdirection is a problem; even properly directed faxes pose a security risk when confidential documents are sent, unprotected, to a nonsecure fax machine that prints everything out whether the proper recipient is ready to receive them or not. Now hold those ideas for a moment and let’s go back to when I was a young man, oh so long ago.

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. It turns out that the old problem of misdirected faxes has a new twist: networked printers are posing the potential for misdirected printouts – including printer hacking.

The remainder of today’s contribution is from Dale and his colleague Gary Lefkowitz 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.

The story continues in our next column.

* * *

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.