In the previous article in this series, I looked at some of the difficulties we face in preventing unauthorized copying of sensitive data. In this article, I review the problems caused by easy access to portable data storage media.

* * *

If there are no barriers to file copying onto removable media, data thieves have a wealth of options. The problem is made worse by the ubiquity of laptop computers, which are so common now as to be almost unnoticed by physical security personnel. Since today's laptops can be equipped with disk drives approaching 100 GB and most have high-speed LAN connections, the potential for data theft is enormous. In addition, inexpensive, pocket-sized ZIP diskettes can hold more than 100 or 250 MB of data; CD-ROMs, removable cartridges and DVDs can hold gigabytes. My wife just bought an external disk drive for her Mac; it fits in a roomy briefcase, costs $189 and holds 80 GB [a quick note to tickle younger readers: it's the same physical size as the 5 MB – yes, MB – external hard drive I bought in 1984 for $2,000). Some PC cards hold hundreds of MBs of data. Worse still, there are key-fob sized storage devices that fit on Universal Serial Bus (USB) ports and that have similar capacities. It would make sense for security guards protecting high-security areas to check for all such media and verify that anyone removing them has written authorization to do so. Realistically, though, there's no way that ordinary firms are going to demand that employees empty their pockets to prove they're not carrying electronic key fobs. In any case, regardless of thorough screening of media, the problem of dishonest authorized people comes up again: there's no practical way for security guards to be sure that the _data_ on the portable media are permitted off-premises.

Electronic loss of control over sensitive data is increasingly easy. Not only do many organizations fail to impose firewall filtering rules on _outbound_ transmissions (thus potentially permitting export of confidential data), but many users who carry sensitive data out of the office on their portable computers don't have any firewalls for these computers that they connect to cable modems and satellite systems. Without firewalls on those computers, Trojan Horse programs and e-mail enabled worms can easily send confidential data out onto the 'Net at odd moments.

In all of these cases, the easy availability of encryption is a mixed blessing; ciphertext protects data against unauthorized disclosure, but it also makes inspection a lot harder.

The best we can do to fight data leakage in the real world is to apply everything we know about defense in depth. In addition to all the technical defenses appropriate for a particular organization, we have to provide the additional but essential protection of sound personnel management policies and good facilities security personnel and procedures.

Unfortunately, the fact is that a determined attacker is almost certain to succeed no matter what we do. As a last resort, after all, a human being can simply _remember_ sensitive data. The
only attack against that covert channel is the one that has affecting me lately: getting older.

Now what was I saying?

***

In the next column in this occasional series on computer crime techniques, I'll look more closely at other covert channels that may unfortunately facilitate data leakage.

***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 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.