The articles about proliferating USB data storage devices in a variety of shapes prompted a fair amount of e-mail, including a pointer from one reader who gave me the URL <http://www.dynamism.com/sushidisk/index.shtml> for a sampler of, ah, sushi-shaped USB disks. It is not entirely clear why anyone would want a sushi-shaped USB disk, but at least it is unlikely to be a serious threat to security.

The next time you see someone plugging a 128 MB Uzura Natto or Futomaki into one of your computers, you will know they are up to no good.

Now on to more serious matters.

There are three distinct approaches I’ve seen to protecting data against unauthorized copying to USB devices (or to any other storage device):

- Prevent the unauthorized devices from functioning at all;
- Prevent data from being copied to unauthorized devices;
- Encrypt all data so that unauthorized users can’t use the copied data.

The pointers below don’t claim to be exhaustive, and inclusion should not be interpreted as endorsement. I haven’t tried any of these products and I have no relationship with the vendors whatsoever.

- For corporate networks using Microsoft’s Active Directory, a company called FullArmor makes a product called IntelliPolicy; it was recently reviewed in the Network World Fusion Systems Management column by John Fontana <http://www.nwfusion.com/news/2004/1117armor.html>. That article specifically quotes a system administrator who said, “We like the ability to lock out devices like USB ports on our sensitive machines. It prevents users from downloading information and disappearing with it.”

- Another tool that blocks access to USB devices is SecureWave Sanctuary Device Control <http://www.securewave.com/sanctuary_DC.jsp>. By default, the system sets up restrictive access control lists (ACLs) blocking everyone from using all devices. Administrators then define changes in the ACLs to permit specific users or groups of users to access the devices and device types they justifiably need. The tool includes provisions for encrypting data moved to portable devices and a stand-alone decryption tool that can allow access to such data on a non-protected computer.

- Reflex Disknet Pro software <http://www.reflex-magnetics.com/products/disknetpro/> not only provides all kinds of device and port controls but also includes software for automatic encryption of all data transferred to any removable devices. Here too, the
encrypted data can be recovered offsite using a special reader tool.

- Liquid Machines <http://www.liquidmachines.com/> Enterprise Rights Management (ERM) software encrypts corporate data and manages decryption keys on a specialized server. Authorized users simply run their office applications as usual while decryption and encryption go on below their level of awareness. Unauthorized users simply cannot decrypt protected information.

On a slightly different note, it is not at all clear how any of these products can cope with the rather nasty characteristics of the KeyGhost USB Keylogger <http://www.keyghost.com/USB-Keylogger.htm>, which, as far as I can see from reading the Web pages, may be completely invisible to the operating system. This device can be stuck on to the end of the cable of any USB keyboard and will cheerfully record days of typing into its 128MB memory. Such keyloggers can provide a wealth of confidential data to an attacker, including userIDs and passwords as well as (no doubt tediously error-bespattered) text of original correspondence.

Hmm, time to check those keyboard cables, eh? And watch out for those high-capacity sushi.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see

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

Copyright © 2005 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.