With the continuing decline in cost of flash drives (also known as “thumb drives”), your users are increasingly likely to be copying ever-more corporate data to these convenient, easily-lost devices. How are you ensuring that confidential data on these little drives are safe from prying eyes? And if you store critical information, how can you ensure that these data are not modified without authorization?

One solution I have been working with for several months now is an interesting combination of biometric authentication technology with electronic mass storage.

The ClipDrive Bio series from Memory Experts International (<http://www.memoryexpertsinc.com/en/index.html>) provides USB 2.0-equipped flash drives in capacities of 64MB, 128MB, 256MB, 512MB, 1GB, 2GB, 4GB; each has a fingerprint reader integrated into the case. The drives can be partitioned into secure (AES-encrypted) and public (unencrypted) sections in any proportion; the locking/unlocking software allows users to enroll up to five users with the recommended two fingers per user (in case a finger is damaged).

When you plug the ClipDrive into a USB socket, the public partition registers immediately. In my case, 100 MB suffices for the public partition, which also contains a copy of the locking/unlocking software so that I can install that program onto another computer if necessary to unlock the secured partition. I use the public section of my 1 GB drive to collect homework from my students in the database lab – much faster than asking for diskettes or CDs. I use the secured partition for everything else, including backups of student grade books, consulting reports, internal memoranda, e-mail repository and so on. I sometimes transfer all of the day’s work on my University-office computer by creating a backup of the modified files on the ClipDrive and then synchronizing from the backup onto my home-office computer at night. Then in the morning I reverse the process and bring changes back to the University on the ClipDrive. It’s mildly less nuisance than carrying the laptop computer back and forth (although in a later article I’ll be telling you about some interesting alternatives for securely synchronizing systems via the Internet).

The locking/unlocking software features an image of the fingerprint reader that shows what it is seeing – very useful in case the reader becomes dirty. The software usually recognizes my fingerprint right away even though I have terrible fingerprints due to ectodermal dysplasia that makes my skin very thin and the fingerprints extremely shallow (my friends joke that I should have become a bank robber). Sometimes I find that I need to move my finger slightly to register properly, but it rarely takes more than a few seconds to open access to the secured partition.

It is easy to add users and to adjust the balance between the public and secured partitions (with concomitant reformatting of both).

The ClipDrive family is widely available from a number of retailers, as any search engine will show.
I’m pleased with my secure ClipDrive and hope that it will be useful for others who are concerned about protecting the confidentiality and integrity of their portable data stores.

[Disclaimer: I have no financial interest whatever in Memory Experts or any other vendor. Norwich University Online Graduate Programs paid for my ClipDrive.]

* * *

For further reading:


ClipDrive Bio home page  

< http://www.pcmag.com/article2/0,1759,1551380,00.asp >

* * *

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.