Taking a Hard-Line Approach to Encryption

Cameron Laird

Information security during the past few years has concentrated largely on data in motion—information communicated via networks. However, the focus has been shifting recently to protecting data at rest, which includes information on hard drives, flash memory devices, and magnetic tape.

This shift has been fueled in part by almost weekly reports of security breaches involving the theft or loss of laptops containing corporate or government secrets or sensitive personal data—including Social Security, credit card, and bank account numbers; passwords; and even medical information—that government agencies, insurance companies, healthcare facilities, financial institutions, and other organizations have collected.

To help address these concerns, companies are increasingly adopting hard drives that encrypt data as it is written, which vendors such as LaCie, Seagate, and Stonewood Electronics manufacture.

These types of hard drives have been around for several years but only as niche products, primarily for government agencies, banks, and other organizations with particularly strict privacy or secrecy requirements. Thus, as of mid-2006, only 15 percent of organizations encrypted data on laptops, noted Paul Stamp, senior security and risk analyst for Forrester Research.

Hardware-based encryption differs from the traditional approach to encrypting data on hard drives, in which computer CPUs run cryptographic software.

The hardware-based technique offers several advantages, including faster performance and less strain on a host system’s processing resources. However, the approach also has disadvantages, such as additional cost and the inability to patch or upgrade products.

**DRIVING THE SWITCH TO HARDWARE**

The ongoing loss of sensitive or other important information stored on computers is a major driving force behind the move to hard-drive-based encryption.

Most of the lost information has come from misplaced, stolen, loaned, improperly reassigned, or discarded laptops, although desktop computers also present a risk. Many organizations have experienced potentially troublesome problems. For example, a recent audit by the US Department of Justice’s Office of the Inspector General revealed that the FBI has lost 160 laptops over a 44-month period.

Organizations are thus looking for new ways to protect information.

“Companies choosing not to protect their data in spite of the recent prevalence of data theft will find it almost impossible to defend their position to the public,” said Stonewood IT security advisor Andrew Donaghue.

Many Asian, European, and North American governments mandate that companies in various fields—such as healthcare, finance, and education—protect data.

Regulations include the US government’s Health Insurance Portability and Accountability Act, the European Community’s Directive on Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and South Korea’s Act on the Protection of Personal Information Maintained by Public Agencies.

Numerous government agencies throughout the world also mandate that the computer equipment they buy include encryption capabilities.

Meanwhile, many individuals who keep private or personally important material on their computers also want better protection.

Proponents say the hard drive is a good place to implement data security because it is a closed environment in which the internal operations are sealed off from other computing-system elements.

“Nothing goes on the disk unless it’s encrypted. Whatever else happens [in the host system], the data will still be unreadable,” said security expert and Purdue University Professor Eugene Spafford.

Hardware-based encryption is more dependable because it is built into the drive and cannot be tampered with, unlike software-based encryption, which users can update or modify via potentially unreliable downloads, added Michael Willett, senior director of security at hard-disk vendor Seagate.

Moreover, he said, the software-based approach—offered by vendors such as PGP and WinMagic—
Computer

LaCie’s d2 SAFE external shows HDD’s SecureD technology

As

enables numerous users to work with

can accommodate multiple keys to

and various combinations of these

sequences, biometric identifiers such

combinations, designated character

conventional user name-password

pendent module.

be either part of the drive or an inde-

while the encryption hardware could

could be either external or internal,

data it contains.

unauthorized people can’t view the

presumably without an access key,

dentally assigned to a different user,

if the device is lost, stolen, or even acci-

functioning as removable access keys.

SecureD Desktop and SecureD

Laptop are packaged with internal

drives. HDD also bundles its smart-

card reader with a standard 120-

drives. HDD also bundles its smart-

information temporarily if desired.

either to lock all data cryptographi-

cally as soon as the key is removed

or to continue decrypting for a des-

ignated period of time after removal,

thereby allowing others to access the

information temporarily if desired.

LaCie. LaCie’s d2 SAFE external

hard drives for desktop and laptop

computers use AES encryption and

fingerprint-based biometric keys, said

Marie Renouard, the company’s

product manager.

The system takes readings of

authorized users’ fingerprints, calcu-

lates hash values for them, and then

stores the information as well as each

person’s permitted level of system

access. People who want to work

14

industrial TRENDS

Figure 1. High Density Devices’ SecureD technology is a hardware module that

encrypts all data passing from a CPU to a hard drive or other storage device. To access
data, users must insert a smart card with the correct access key into a reader.

FIGURE 1

THE BIG PICTURE

Several companies, including IBM, experimented with crypto-

graphic coprocessors for hard-

drive-based encryption in the mid

1990s.

Under the hood

The central idea behind hardware-

based encryption is to encrypt all

data in real time as it is stored on a

computer’s hard disk. The technique

requires users to provide access keys
to retrieve the data. Thus, if the
device is lost, stolen, or even acci-
dentially assigned to a different user,
presumably without an access key,

unauthorized people can’t view the data it contains.

Encryption-enabled hard drives could be either external or internal,

while the encryption hardware could be either part of the drive or an inde-

pendent module.

The keys for these systems include conventional user name-password

combinations, designated character

sequences, biometric identifiers such

as fingerprints, hardware tokens,

and various combinations of these

elements.

Encryption-enabled hard drives can accommodate multiple keys to

enable numerous users to work with

a single protected computer or data set. The systems also come with key-

management tools.

All of the products work with a standard hard drive; a cryptographic

applications-specific integrated cir-

cuit (ASIC), usually proprietary, for

encoding and decoding; a small amount of memory to preserve ses-

tion information such as the current

key; and hardwired interconnects

that ensure that only encrypted informa-

tion reaches the disk.

The ASICs and other related tech-
nologies are designed to be fast

enough to avoid slowing the hard

drive’s read and write activities.

The ASICs also process informa-

tion independently of the host OS

and thus function across multiple

operating systems and aren’t vulner-
able to attacks from host processes.

Vendors working with the Trusted Computing Group (TCG) industry

collectors (www.trustedcomputing

group.org) will be able to include a

Trusted Platform Module crypto-

graphic chip in their hard-drive elec-

tronics.

Encryption-enabled hard-drive sys-

tems use established schemes such as

the Advanced Encryption Standard,

a symmetrical (the same crypto-

graphic key encrypts and decrypts
data) technique that employs 128-bit

blocks and 128-, 192-, or 256-bit

encryption keys. The US government

adopted AES as one of its official

cryptographic systems in 2000.

All encryption and decryption

occurs on the hard drive, so the sys-

tem doesn’t consume any of the host

computer’s processing or memory

resources.

Destroying the access key or keys

makes protected data inaccessible.

Thus, this process can make hard

drives safe to dispose of or reassign

without undertaking the time-con-

suming disk-wiping process, noted

Aage Kalsaeg, High Density Devices’

chief marketing officer.

Variations on a theme

Several vendors are selling differ-

ent types of hard drives with encryp-

tion capabilities. More products are

scheduled for the near future.

High-Density Devices. As Figure

1 shows, HDD’s SecureD technology

is a hardware module that works

with any standard off-the-shelf hard

drive. SecureD sits in what tradi-

tionally has been a direct connection

between the CPU and hard drive.

The module includes a reader that

works with smart cards functioning

as removable access keys.

SecureD Desktop and SecureD

Laptop are packaged with internal

drives. HDD also bundles its smart-
card reader with a standard 120-

gigabyte external hard drive and

controller that connect to systems

via FireWire or Universal Serial Bus

technology.

A user can configure SecureD
either to lock all data cryptographi-

cally as soon as the key is removed

or to continue decrypting for a des-

ignated period of time after removal,

thereby allowing others to access the

information temporarily if desired.
with a system pass a fingertip over a sensor, and if their fingerprint’s hash value matches that of an authorized user, they gain access. Registered users can swipe a finger across the sensor to relock their systems.

**Seagate.** Seagate sells encryption-enabled hard drives for digital video recorders and plans to release other models for internal use in laptops and eventually servers soon.

The company targets big organizations ordering large numbers of high-end hard drives at one time. Thus, its DriveTrust products simplify the administration process. They include a standard API and a software developer’s kit to let companies write applications that, for example, manage and update keys, report on disk usage, and handle authentication.

The top DriveTrust models use two ASICs to achieve high throughput.

Current DriveTrust products rely on Triple DES (Data Encryption Standard). However, Willett said, the upcoming Momentus line of drives will offer the stronger AES. The disks use password-based keys and an optional thumbprint-based biometric approach.

**Stonewood Electronics.** Stonewood’s FlagStone technology integrates data storage, AES encryption, and authentication into internal and portable disk drives for desktop and laptop computers. The drives offer storage capacities between 30 and 120 gigabytes and operate across multiple operating systems and applications.

The products present authentication requests as the BIOS process begins. Each requires different types and levels of authentication, depending on the desired security level, to continue the bootup process and enable hard-drive access. For example, FlagStone Corporate requires a single password, FlagStone Baseline Plus requires two passwords, and FlagStone Enhanced requires a password and a token.

**BARRIERS**

Retail comparisons show that 200-gigabyte hard drives with encryption capabilities cost up to $150 more than those without them. The additional cost may be a barrier to some small firms but probably not to companies for whom data protection is a high priority.

Encryption-enabled hard drives add key management, maintenance, and other administrative tasks. However, companies such as Seagate include features designed to make this process easier.

At the same time, standardization of hardware-based encryption remains in its infancy, so management tools from one vendor do not work with products from a different vendor.

Most software-based encryption products, on the other hand, work across different hard-disk platforms and types, which makes management easier, according to John Dasher, PGP’s director for product management.

Software-based encryption is also flexible and scalable, which enables better key management, particularly when used across large numbers of drives, stated WinMagic founder, CEO, and president Thi Nguyen-Huu.

Purdue’s Spafford said software-based encryption might be better than hard-drive-based encryption at recovering data from disks with hardware-based defects.

Another issue is that security functionality is hardwired into most encryption-enabled hard drives, which thus can’t be patched or upgraded if problems arise or improvements are available later.

And if users who have access to data lose their password, smart card, or other key, the information that the key accesses cannot be retrieved.

For example, hard drives eventually could work with elliptic curve encryption, said Seagate’s Willett. ECC is a public-key encryption technique, not yet widely used, based on elliptic curve equations that can create faster, smaller, and more efficient cryptographic keys.

Currently, the encryption-enabled hard-drive market is fragmented, with most offerings from small vendors, noted Johannes Ulrich, chief research officer with the SANS Institute, a computer-security training and research organization.

Of course, this could change as the market grows. And, Ulrich said, growth appears to be in the offing because the technology is receiving considerable attention from industry observers.

In fact, because of ongoing cybercrime and data breaches and the expected adoption by many users of Microsoft Vista—which has two versions that offer a software-based hard-disc encryption utility called BitLocker—2007 could be a crucial year for hard-drive-based encryption.

Organizations’ specific security requirements and practices vary enormously, so there apparently will be a healthy demand for both software- and hardware-based hard-drive encryption.

“No one size fits all,” said Forrester’s Stamp.

“We’re seeing a trend in which the boundaries around our data are shrinking,” he concluded. “Security used to be about protecting the perimeter. We’re on a path to what we really need: an infrastructure that protects the data itself. A big part of that is encrypting the data as it appears on hard drives.”

Cameron Laird is a freelance technology writer based in Friendswood, Texas. Contact him at cameron@phaseit.net.