Technology Paper

DriveTrust™ Technology: A Technical Overview

Introduction

As the importance of digital information increases, so does the need to secure that information. Through DriveTrust™ technology, Seagate® is ushering in a new era of secure computing.

Data security can be managed at the network and local computing levels with firewalls, antivirus software and smart cards, but data remains vulnerable to theft or loss. The hard drive is a critical element in the computing chain because it is where sensitive data is stored.

DriveTrust technology implements security on the hard drive itself, to provide a foundation for trusted computing.

What is DriveTrust Technology?

DriveTrust technology is a drive-level platform for hardware-based security that takes advantage of the hard drive's closed computing environment. While operating system environments are designed to enable widespread application support, hard drives are closed computing environments running specialized code (firmware) to manage drive functions. The hard drive is an ideal place to implement data security, because its internal operations are sealed from other elements of the computing system.

The DriveTrust platform does more than protect data stored on the disk. It establishes trust for data sent between the host and drive and allows the drive to authenticate applications, assign secure storage partitions, handle digital signatures and deliver many other security functions.

DriveTrust technology provides developers and IT administrators the tools they need to easily and cost-effectively secure the computing environment. DriveTrust resources are like a toolbox of hardware-based security functions that secure digital information.

Elements of DriveTrust Technology

DriveTrust technology comprises four elements, as illustrated in Figure 1.

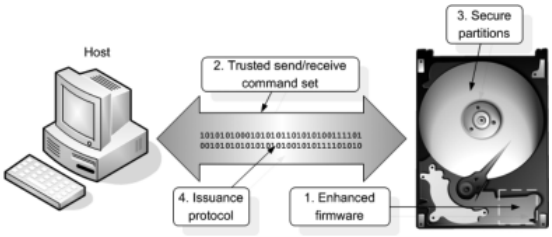

Figure 1: The DriveTrust framework includes enhanced firmware and hardware, the trusted send/receive command set, secure partitions on the drive and the issuance protocol.

1. Enhanced firmware and hardware

Firmware is the software that runs on the drive's internal computer. It is normally used to manage extremely complex drive functions, such as moving the read/write heads, tracking bad sectors on the disk and storing bitmaps of where data is located. DriveTrust technology extends a drive's capabilities with additional security code optimized on the drive's computing resources. DriveTrust technology implements on the drive a cryptographic service provider that provides encryption, hashing, secure storage, decryption, digital signature and random-number generating functions.

2. Trusted send/receive command set

Trusted storage requires a secure communication infrastructure. DriveTrust communications are sent through the trusted send/receive (in/out) command set, designed in collaboration with the standards bodies that define ATA and SCSI interfaces. Secure messaging has been designed into the ATA and SCSI interface protocol to enable support for security technologies, including DriveTrust technology.

3. Secure partitions

A 200-GB hard drive reserves roughly 200 MB of unaddressable disk space for internal system storage. DriveTrust technology uses this space to create secure partitions that are both logically and physically separated from the rest of the drive storage, with strong conditional access controls—providing an excellent place to store cryptographic keys and other sensitive information.

DriveTrust-equipped drives can make these secure partitions exclusively available to applications that present the proper credentials to store application code, additional content or data. ISVs can make use of this capability to build applications with additional features including stronger authentication, time stamping, forensic logging or transaction data.

4. Issuance protocol

Software applications, basic input/output systems and other programs interoperate with the DriveTrust-equipped drive through strictly controlled communication channels. ISVs and other developers can write applications and have them assigned to a secure partition in the drive through the issuance protocol. Anytime the application attempts to access those secure resources, it must present its credentials—given under the issuance protocol—to the administrator function in the drive. The administrator function authenticates the application, activates the appropriate secure partition, and allows the application to interact with the secure partition through the trusted send/receive command set.

DriveTrust Technology in Action

By facilitating the security of digital data where it is stored, DriveTrust technology becomes a solid foundation for a secure IT environment. DriveTrust capabilities can be applied to solve data security issues within most organizations. These applications include:

- **Full disk encryption.** A combination of strong authentication and encryption protects data against theft or loss. This solution automatically encrypts and decrypts all the data that travels in and out of the drive. Unlike other data encryption applications, DriveTrust encryption keys are password-protected and never appear in the clear or in any readable format on the drive.
- **Secure erase for repurposing or end-of-life disposal.** Government entities and large corporations spend millions of dollars to ensure that sensitive data is not recovered from discarded or repurposed hard drives. Simply changing the encryption key on a DriveTrust drive instantaneously and securely renders all stored data unreadable and unusable. It can be done in seconds and eliminates the time

and potential for human error associated with standard disk erase techniques.

- **Hardware-based security for biometric authentication data.** Biometric authentication is the cutting-edge technology used to verify users, but what happens when the biometric credentials themselves are compromised? DriveTrust technology allows software applications to store biometric data in secure partitions on hidden portions of the hard drive for the strongest security.
- **Centralized authentication and credentialing for DriveTrust-equipped drives in multiple drive environments, such as storage area networks, network attached storage and redundant arrays of independent disks.** An open standard is being developed within the Trusted Computing Group that will allow enterprises to implement policy-driven authentication across their networked or array-based storage infrastructure, providing a security management infrastructure for DriveTrust technology drives in storage systems. This base-level protection provided by DriveTrust technology will complement other security measures implemented higher up the storage architecture.
- **Enterprise management of USB-attached external hard drives through drive pairing and encryption.** USB-attached external hard drives pose a serious risk to IT security because gigabytes of stored information can be copied and stolen in a matter of minutes. IT departments can use DriveTrust drive-pairing functionality so that department computers only work with authorized external hard drives.

Who Uses DriveTrust Technology?

DriveTrust technology gives both individuals and businesses a security foundation that protects sensitive data and enables additional application functions. Independent software vendors (ISVs) and computer makers can use the DriveTrust software development kit offered by Seagate to integrate or leverage security capabilities.

Seagate offers two product lines that feature DriveTrust technology: DB35 Series™ drives for digital video recorders and Momentus® 5400 FDE drives—the first hard drive with full disk encryption—for notebook computers. The 3.5-inch DB35 Series drives use DriveTrust technology to pair drives and set-top devices to protect content stored on the drives. DriveTrust technology allows DB35 Series drives to engage in a dual challenge-response authentication procedure upon startup, using cryptographically protected credentials securely stored on a hidden partition.

The 2.5-inch Momentus 5400 FDE.2 drive automatically encrypts all data, restricting access to those with the appropriate cryptographic keys. The drive uses a specialized chip to efficiently encrypt and decrypt all the data stored on the drive with no performance penalty. DriveTrust provides strong authentication and stores the encryption keys in a secure partition using a cryptographically derived format.

Leading the Industry Towards Open Standards

The Trusted Computing Group is a not-for-profit industry organization formed to develop, define and promote open standards for hardware-enabled trusted computing and security technologies. Seagate and other industry leaders involved in the Trusted Computing Group (TCG)—including AMD, Hewlett-Packard, IBM, Intel, Microsoft and Sun Microsystems—are working together to develop technology to ensure that elements in the computing environment behave in an expected manner for their intended purpose. These trusted elements, also called *roots of trust*, can be used to authenticate other elements and control access to the system.

Seagate introduced DriveTrust technology to the Trusted Computing Group as a framework for developing an open standard for extending trust and security to storage devices. Subsequently, the Storage Work Group was formed, comprised of all leading disk drive manufacturers as well as flash storage, storage management and storage integration vendors. Seagate chairs the Storage Work Group and actively contributes to the standardization effort.

The Storage Work Group is developing the Core Storage Specification that will enable secure storage solutions that protect data and interoperate with trusted systems. The primary goal is to help users protect information assets such as data, passwords, and encryption keys from attack and theft. DriveTrust-equipped drives

become a root of trust in the trusted computing chain, authenticating and protecting data stored on the drive.

In addition, the Storage Work Group has collaborated with the advanced technology attachment (ATA) and small computer system interface (SCSI) standards bodies to incorporate a security payload into ATA and SCSI trusted send/receive protocols. The Core Storage Specification defines the payload command set, and will ensure that all storage devices using ATA and SCSI interfaces—including USB-attached flash devices, tape drives and hard drives—will be able to recognize trusted send/receive commands.

The Core Storage Specification is currently being prepared for publication, and future DriveTrust products will comply with the open standard.

Seagate: The Leader in Drive-Based Security

DriveTrust technology provides the tools necessary to turn the hard drive into a root of trusted computing. Security provided by DriveTrust technology is essentially transparent to the user and is not burdensome to general computing resources.

Seagate continues to pioneer drive-based security and make the technology available to ISVs and technology vendors, with the goal of making the overall computing environment more secure for both business and home users.

To find out more about how DriveTrust technology can be used and how it addresses compliance issues, please see our DriveTrust technology general overview white paper and DriveTrust technology compliance white paper.

For more information on the Trusted Computing Group, including continuing work in the TCG's Storage Working Group, visit their Web site at www.trustedcomputinggroup.org.

AMERICAS Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
ASIA/PACIFIC Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 130–136, rue de Silly, 92773, Boulogne-Billancourt Cedex, France 33 1-4186 10 00