

Commentary

June 4, 2007

Storage Needs To Be Trusted Everywhere

Previously, a storage device could reveal its confidential information to anyone who had network access to or possession of the device, allowing unauthorized users to gain access to and otherwise misuse (such as alter or delete) confidential data. Now thanks to the Trusted Computing Group's (TCG) Trusted Storage Specification, open specifications are in place that define security controls that enable conforming permanent storage devices to be trusted not to give away secrets. Hardware storage devices that conform to the TCG's specification will help lead the way to eliminating the unacceptable misuse of information on mobile, server, and data center storage devices.

Today's Storage Cannot Be Trusted

If storage device access controls fail, confidential information will be at the mercy of unauthorized users. A key example is mobile storage devices, particularly laptop computers. Headlines regularly trumpet the confessions of companies that have lost or had stolen laptops that contain confidential personal information including social security numbers and/or credit card numbers.

But that is only the tip of the data confidentiality breach iceberg, the errors that have to be reported according to law. What about all those cases where confidential information is lost, stolen, or compromised and not reported? Those constitute the vast majority of data breach instances and occur not only at the mobile storage device level, but also at server and data center levels as well.

Now the potential or actual loss of confidentiality may be on a scale from very serious (such as confidential merger and acquisition information) to the merely unacceptable (such as employee salary information). And while an enterprise needs to protect the most sensitive information today, as soon as possible, organizations will also want to make all storage devices trusted not to reveal confidential information to or become exposed to change by unauthorized parties. Eliminating any exposure of private information is simply sound business practice and standard operating procedure.

But in order to reach a state where storage can be trusted everywhere, open specifications have to be put in place. That is where the Trusted Computing Group (TCG) comes in.

The Role of the TCG Storage Work Group

The Trusted Computing Group is a not-for-profit industry standards organization

that focuses on developing, defining, and promoting open specifications for IT-benefiting trusted computing. TCG defines trust as “the expectation that a device will behave in a particular manner for a specific purpose.”

Trusted computing is about securing information assets, such as data, from being compromised by factors or events such as alteration due to an external software attack or loss of confidentiality due to physical theft.

The Storage Work Group within TCG focuses on specifications for security services on permanent storage devices, including hard disk drives, flash memory drives, optical drives, and digital tape drives.

The TCG Trusted Storage Specification defines a standard access control system over security features within the internal environment of storage devices, and also provides a general programming environment for platform-based applications to enable enterprises to exploit the trust and security functions on storage devices.

The Specification is not just for the mobile (client) world, but also for the server and data center side. Laptop full disk encryption is simply the appealing first application that illustrates the power of the Specification.

Although all enterprises can benefit from improving the security of storage devices, selected industries, such as banking and medical, may be early adopters as applications in those industries can draw upon cryptographic and secure storage functionality for high-security support.

Storage Devices as a Root of Trust

Hardware that cannot be changed and that can perform digital signatures is necessary to form what is called a root of trust. A disk drive can be a root of trust since no end user or IT administrator can change the drive’s firmware. A root of trust initiates a chain of trust that is essential for strong hardware security.

A hard drive is an ideal target for strong security because it is a closed, controlled, and intelligent environment. Disk drives are intelligent because they have custom controllers, which contain a processor and hidden system memory. Hidden memory is non-user-addressable memory that can be partitioned into segments that provide exclusive security system functions, called Security Provider (SP) segments.

As a result, firmware and chip hardware on the storage device can have security functions, including cryptography, built into them. These security functions can be made available exclusively to applications that run in the storage device’s host platform.

Moreover, communication between the host and storage device can use what are called Trusted Send/Trusted Receive commands. These commands support trusted messaging from the host applications to the device’s access control systems which is necessary for any authentication process.

All in all, a hard disk provides a strong security platform because it delivers:

- Strong access control
- Unobservable cryptographic processing of information
- Custom logic that enables inexpensive cryptographic function implementation and complex security operations.

Commentary

Full Disk Encryption Illustrates the Power of the Trusted Storage Specification

Let's consider an example that carries popular appeal and public interest and is likely to be the first application where the Trusted Storage Specification will come into play; that is full disk encryption (FDE) for mobile devices, particularly laptops.

FDE answers the problem of how to prevent confidential information being revealed when laptops are lost or stolen. FDE encrypts all the data at rest on a mobile storage device, say a hard disk, including the boot partition and system files. An unauthorized user who does not have the proper FDE password would find the device unbootable (through locking). Even if the data could somehow be accessed, it would be unreadable because it is encrypted.

Full disk encryption is far more effective than simple file and folder encryption methods. The user does not have the option of not encrypting data so there is no chance that any confidential data can slip between the cracks. Moreover, all the user has to do is enter a password at a pre-boot stage when powering up. Once the operating system has launched, the encryption process is transparent to the user.

The Lifecycle of a Storage Device

How does FDE figure in the lifecycle of a permanent storage device? Key stages in that lifecycle are manufacturing, initialization (typically referred to as enrollment), ongoing use, and disposal.

Enrollment

Enrollment is the process of initially setting up the use of a storage device. The first person who has physical possession of a storage device is considered to be an administrator, who implements the security policies for the device.

Remote administration for the management and control of the device from a central server is critical not only for creating a unified trust network, but also to enable the realistic management of a large number of storage devices, a key issue for companies with hundreds or thousands of such devices.

Individual devices can then be assigned to a user. A user has simple powers such as the ability to change a password and unlock a drive. The administrator retains higher level powers, such as enabling recovery management in case an individual user loses or forgets a password.

Ongoing Operation

For laptops, a secure FDE device has to be a bootable disk. A pre-boot screen appears every time a user powers up a system, as the pre-boot software resides on the disk. The user then has to enter a proper password to unlock the disk before the operating system boots.

Once the drive is unlocked all the data is in the clear to any software that wants to access the data. For example, search software can easily index and search the drive, an impossible process if individual files and folders are encrypted. Moreover, backup software can easily interact with data on the drive without having to go through any apparent decryption process.

Commentary

Disposal

Often, the original user may decide to replace a laptop or other device that may still have economic value to and a productive life remaining for a different user. However, it would be a mistake to transfer or sell a storage device that contains confidential information that a new user can access. A sound end of life (EOL) strategy is therefore essential for such devices.

A FDE-based crypto-erase capability and a re-initialization capability solves this problem, destroying the original encryption key while clearing information from the drive so that a new user appears to have a fresh clean disk. Even if the user could find the physical file of a logically deleted file, the data would be unreadable.

Deployment Strategy

Even though the case to improve the security of storage devices is a strong one that does not mean that old storage devices will be replaced immediately. The challenge for deploying Trusted Storage Specification conformant products is timing. Enterprises are not going to throw away their existing storage devices for both investment protection and migration reasons. New devices have to become part of an ongoing replacement cycle.

And depending upon the planned replacement cycle at an enterprise that process could likely take three years or more. That is not necessarily a bad thing because an IT organization needs a considerable amount of time to make the transition in an orderly manner.

Trying to accelerate the process could put a strain on IT resources for

centralized management of such essential tasks as backing up existing data, initializing new systems, and migrating data from old storage devices.

Now retrofitting with software-based FDE solutions might seem to be an alternative. However, in the long run, built-in hardware-based solutions seem more likely to win out over bolted-on software. Besides being more effective, the overall total cost of ownership is likely to be less with the hardware-based solution — less install time for instance.

Using a Triage Strategy

But what if there is a mandate to impose tighter security at the storage device level immediately? Such a goal may be laudable, but a more realistic timeframe is likely to prevail for two reasons. The first is the high cost both in terms of money and people if a large number of storage devices are involved. The second is that the most critical confidentiality and data preservation requirements are subject to a triage strategy. That is to say that the most important data should be protected first. In many or even most organizations, a small percentage of storage devices may contain the most sensitive data.

In the long run, IT administrators and business units do not want to sit in judgment as to what is sensitive information or not. All non-public information will be considered confidential information and receive the strictest protection simply as a matter of course. However, in the short run, priorities need to be set. Setting priority by role is one strategy. For example, the laptops of the CEO, CFO, and other executives may be considered to contain confidential information by the role that the executive plays in the enterprise.

Commentary

A second way of setting priorities is by determining both the most confidential information and who has access to it, and begin by securing those devices.

The downside of applying triage is that it distorts the normal replacement cycle. For example, the CEO may have just gotten a new laptop and now needs a laptop with a secure storage device. IT should be able to work around these challenges since solving the problem of protecting the most critical information is well worth the effort.

Conclusion

Today the vast majority of storage devices cannot be trusted. That has to change, since IT users have access to trusted storage devices. Achieving that goal will take time but is preferable to an alternative where the security level of mobile storage devices remains much lower than is acceptable. As society becomes increasingly interconnected, we are becoming more dependent upon IT technology to provide the mobility and security necessary to support a growing range of business and life processes.

That is why the work of the Trusted Computing Group in general and the Storage Work Group with its Trusted Storage Specification in particular is important. Open specifications to which vendors can design conform-

ing products are a necessity. Deployment will take time, but eventually open specifications will be embedded silently and ubiquitously in storage products throughout an increasingly secure digital universe.

David Hill

Analyst Name: David Hill
Topic Area: Data Protection

Mesabi Group LLC
26 Country Lane
Westwood, MA 02090
www.mesabigroup.com

Mesabi Group LLC is an affiliate of Valley View Ventures that aims to provide thought leadership and sound advice to both vendors and users of information technology. .

Phone: (781) 326-0038
email the author: davidhill@mesabigroup.com

The information contained in this publication has been obtained from sources Mesabi Group LLC believes to be reliable, but is not warranted by Mesabi Group LLC. Commentary opinions reflect the analyst's judgment at the time and are subject to change without notice. Unless otherwise noted, the entire contents of this publication are copyrighted by Mesabi Group LLC, and may not be reproduced, stored in a retrieval system, or transmitted in any form or by any means without prior written consent by Mesabi Group LLC