



Storage Work Group

Use Case White Paper – v 1.0

Abstract

This white paper describes use cases for the application of Trusted Computing Group (TCG) techniques and specifications to storage devices. The use cases fall into three broad categories: the trusted attachment of storage devices to their hosts, more general policy driven secure control over features of storage devices such as storage locations and storage encryption, and secure, session-oriented, messaging of such controls to storage devices. This document also describes the proposed T10 SCSI and T13 ATA commands that support these security communications to storage devices.

The Use Cases provided in this document are a subset of the use cases developed by the Storage Workgroup that have been entirely re-written for this exposition for the sake of clarity. The specific terms used in this Use Case exposition may change in the actual specification as the terminology is vetted for consistency with other TCG Workgroups later in the specifications process.

Terms and conditions for use of TCG documents can be downloaded from <https://www.trustedcomputinggroup.org/about/legal/>

Contents

1	INTRODUCTION	3
1.1	Background and Problem.....	3
1.2	Architectural Framework	3
1.3	Use Cases.....	4
1.3.1	Enrollment and Connection	4
1.3.2	Protected Storage	5
1.3.3	Locking and Encryption	5
1.3.4	Logging	5
1.3.5	Cryptographic Services	6
1.3.6	Authorizing SD Feature Sets to Hosts	6
1.3.7	Secure Download of Firmware.....	6
1.4	ATA and SCSI Commands	6

2 TERMS AND ABBREVIATIONS7

1 INTRODUCTION

1.1 Background and Problem

Permanent storage devices (SDs) such as hard disk drives, flash memory drives, optical drives, and digital tape drives, play a central role in computing. The Trusted Computing Group (TCG) has focussed to date on assuring the predictable operation of computing hosts that may or may not incorporate permanent storage devices. But most hosts do incorporate non-volatile storage devices. So it is natural to extend the trust boundary into the storage device as opposed to just viewing storage devices as perfectly trustable elements within the computing infrastructure.

A well-known example of the trust boundary breakdown is SD end-of-life or repurposing. It should be possible to know with certainty, and with ease, that a SD that is repurposed is not also providing a means for transmitting private data to the next, legal or illegal, physical possessor of the SD. This is particularly salient and obvious as SDs become smaller and more portable, but it is also true in large data centers that may use thousands of SDs containing data and programs of high monetary value or high needs for the protection of individual privacy.

Contrary to many conceptions about 'dumb storage devices,' storage devices are not dumb. They incorporate modern, high-speed processors, often large amounts of high-speed dynamic memory, and multiple data ports. TCG Trusted Platform Modules (TPMs) that are shipping in hosts today are, in this sense, small, special-purpose, dedicated-processor flash-storage devices that provide a root of trust for their hosts. However, the TPM's main function is providing roots of trust, while the SD's main function is providing digital storage.

Like TPMs, most all SDs are not re-programmed in the field except in exceptional circumstances. The TPM was designed extending trust, or predictable operation, to hosts, where applications written by an open global community of commercial and non-commercial interests are commonly downloaded and executed on the host. SDs are also programmable by this same community but in much more limited ways. It is anticipated they will become more programmable in the future, and therefore there is a need to extend host TPM trust into the computing environment within all SDs.

1.2 Architectural Framework

The Storage Workgroup is extending the trust boundary into the SD by proposing a standard system for access control over features and properties of the internal SD computing environment. In this sense, the TPM is a root of trust that extends to trusted applications running on the host that may then securely manage such resources in the internal SD computing environment. Since such host applications are written by the open community, it is essential that one application cannot affect SD resources that another application depends upon, except in predictable ways. Therefore the system of access controls may be divided among applications that may run on the host.

It is precisely this strong notion of SD-enforced host application rights that allows trust to be extended from the TPM-grounded host to the SD. A natural consequence of this is to provide greater opportunities in storage, such as permanent storage areas that are restricted to particular host applications, and exclusive control over the data-at-rest encryption capabilities of the SD.

So, unlike solutions developed for the PC-Client Workgroup, the Mobile Device Workgroup, and the Server Workgroup, the Storage Workgroup assumes there is no TPM necessarily internal to the storage device, but rather the Storage Workgroup is focussed on defining controllable features and properties of the internal SD computing environment, and providing for strong, policy driven, securely authenticated and messaged, access controls over those features and properties of the internal SD computing environment.

Since nearly all communications with SDs is through the SCSI (ANSI/INCITS T10) or ATA (ANSI/INCITS T13) command sets, the architecture also includes proposed additional SCSI and ATA commands that support the above trusted messaging from the host applications to the access control systems of the SD. This is deemed a necessary component of any solution that attempts to ubiquitously extend the trust boundary to the internal features and properties of the SD.

It is within this architectural context that the Storage Workgroup use cases apply.

1.3 Use Cases

Use cases serve the purpose of highlighting desired functionality that should interoperate among all SDs. Use cases are excellent in describing the scope of a technical specification that unambiguously implements interoperability, but the technical specification itself is the sole authoritative definition of interoperability constraints. In the current case, this is the specification of the SCSI and ATA commands and the payloads of those commands. The current specification effort is within the TCG and the specification effort is open to all TCG members of contributor status and above. The TCG itself is an open organization available to any corporation. The TCG also maintains a Liaison program for non-commercial organizations and individuals, and a Mentor program that provides outreach to the scientific and educational communities on a global basis. The Storage Workgroup specification, as with all other TCG specifications, will be publicly available once it is completed and accepted by the TCG.

The Storage Workgroup recognizes that there are different types of SDs, such as disk drives, optical drives, and tape drives, and that these must be differentiated in the specifications. However, in these Use Cases we do not discriminate among device types precisely because the Use Cases describe abstract functional requirements. One purpose of this public disclosure of use cases is to alert other standards creating bodies as to the specifications efforts underway in the TCG Storage Workgroup.

In all cases below, whenever the term “host” is used, it should be taken to mean “host or host application”, and whenever the term “SD” (Storage Device) is used, it should be taken to mean “SD or SD feature”.

1.3.1 Enrollment and Connection

It is often desirable to mate particular SDs to particular hosts. The mating can have two manifestations.

In one case, the SD can refuse to perform its storage (or other) operations unless SD recognizes the host as authorized to have access to those operations.

In the other case, the host can refuse to employ the SD in any operation unless the host can authenticate that the SD is authorized.

TCG is providing specifications for both SD-to-Host and Host-to-SD mating.

In order that this dual mating be easy, it is desirable to separate the mating process into parts that we have termed **enrollment** and **connection**. Enrollment refers to a process by which an SD and host are set up for connection. Ideally, a person may be involved in enrollment, but afterwards, secrets exchanged between the host and SD automatically gate the connection. So a person may freely connect and disconnect authorized SDs from authorized hosts without having to type in passwords or providing other authentication credentials on each connection.

The setup SD-to-Host mating involves several steps. These include the authorization of the right to set up the connection, and setting up the authorization sequence needed by the SD on each connection. Typically the enrollment is enabled or disabled. If it is enabled, then connection must be authenticated. The authorization needed to enroll is different than the authorization to connect.

The setup for Host-to-SD mating also involves several steps. These include fetching authentication credentials from the SD that may be employed or later used in connection, or for immediate use in transferring a secret to the SD that may be employed for later use in connection, as defined by the security policy of the host. Since, in this case, the host is making the decision to connect to the SD, the

authorization to enroll is equivalent to fetching a credential and optionally setting up the SD to use a host defined secret for connection or the secret the SD has declared directly in the credential.

The use cases also require that the secrets needed for connection, either SD-to-Host or Host-to-SD, may need to be unavailable to any other host process or unavailable to a simple physical attack across the interface. Since ATA and SCSI commands may be transmitted across both wired and wireless interfaces, it is important that the communications of the enrollment and connection secrets be confidential. Also, since challenge-response authentication takes more than one command, the confidential communication needs to be in a secure session that is established between the host and the SD. Establishing such confidential communications extends the TPM-rooted trust in the host to the SD.

1.3.2 Protected Storage

Optical disks have offered protected storage for many applications, such as DVD, for several years, and all SDs (that employ embedded processors) have protected storage locations for system data. This protected storage is outside of the normally addressable user space. An attribute of this protected storage is that it survives intact even after the SD user space is repartitioned or reformatted.

In this use case, the Storage Workgroup has called out protected storage that extends the trust boundary from the TPM and trusted host. The process is almost identical to the two-step enrollment-connection process in mating, and may be thought of as mating a host to an SD feature. In this way a host application can gain exclusive access to an area of protected storage. There are many applications for secure protected storage, including the protection of private data, the protection of software licenses that can survive a change of operating systems, and the like. Since many different applications may each desire their own protected-storage space, the Storage Workgroup use cases call out the need for the creation and deletion of such protected storage locations under separate authorization than the authorization of the use of the protected storage locations.

1.3.3 Locking and Encryption

Locking and Encryption refer to additional protections to the addressable user space, as opposed to the protected storage areas outside of the user space. Locking is actually identical to SD-to-Host connection but the locking and encryption use cases call out the separation of read-locking and write-locking. Encryption is simply an additional measure meant to prevent unauthorized reading. The enrollment and connection phases of mating are identical to the enrollment and connection phases of SD-to-Host connection (recalling that "SD" can mean "SD feature" and "Host" can mean "Host application").

However, the Locking and Encryption use cases also call out read/write locking and encryption for different logical partitions of the SD. In this way, the credentials needed to authorize writing or reading for one partition of user space may be different than the credentials needed to authorize writing or reading for another. Furthermore, the encryption keys for one partition may be different than the encryption keys for another. The use cases also require that the encryption keys be secured by separate authorization than that needed for reading or writing authorization, although the 'enrollment' phase for a particular partition may set, create, or fetch such encryption keys.

1.3.4 Logging

Many storage devices including nearly all hard disks maintain internal logs, called SMART logs, in order to provide early warning of possible hard disk failure. The Storage Workgroup use cases call out the offer of logging services to the host that make use of protected storage areas. Again, there is an enrollment and use or two-phase establishment so that the actual use is simplified. Also called out is a means for establishing clock time or at minimum a monotonic counter so that log entries can be automatically time stamped in a protected fashion. The workgroup believes that this logging is most useful for forensic logging. This is logging being done for later detecting security violations in the host, rather than for diagnostic logging, as with SMART. However, the use of the logging capability is not technically restricted to one or the other kind of logging.

1.3.5 Cryptographic Services

The access control mechanisms in the SD are required to be versatile in the sense that the SD can support different types of authentication algorithms. The TCG TPM, in the realm of authentication, is principally a passcode and public key (RSA cryptography) authentication device. In the storage industry, symmetric key and hash message authentication codes (HMAC) are also in common use. Therefore, the access control mechanisms, including all of the above-mentioned ones for protected access to read/write operations, key management, and storage, are assignable in enrollment to passcode, symmetric key, HMAC, or public key authentications.

In addition the requirement of secure messaging additionally imposes cryptographic services for key exchange.

A particular SD may support only a subset of the identified cryptographic operations. In all cases, other bodies, such as IETF, standardize the basic cryptographic operations. For symmetric ciphers, for example, the use cases call out AES 128. For hashing, they call out SHA-1 and SHA-256, and for public key ciphers RSA and Elliptic Curve (in various lengths and for various curves). Provision is made for the modular introduction of other ciphers.

Finally, the use cases call out uses of these standard cryptographic functions including the capability to verify signed hashes on material that has to be decrypted using a key only available on the storage device.

Since the cryptographic services may require hiding keys and keeping one set of keys secret from one host application to another, the cryptographic services must obey the same partitioning of authorizations available to the rest of the use cases.

1.3.6 Authorizing SD Feature Sets to Hosts

It should be clear from the above use cases that there is a need, associated with enrollment, to be able to assign to a particular host application (whether it be local on the local host or remote from the local host), exclusive access to SD feature sets. The use cases therefore calls out the notion of being able to define a feature set that can be claimed exclusively. The exclusivity of the claim is performed by setting access controls using the authentication operations supported by the SD.

1.3.7 Secure Download of Firmware

While typically rare, it is usually possible to download manufacturer-authorized firmware to SDs. The Storage Workgroup use cases call out the need to properly authorize such downloads using strong authentication methods built into the overall architecture. In particular, downloads are hashed and the hashes signed, and the SD confirms the signer and publishes to the trusted platform what entities are permitted to offer acceptable downloads. Typically, this is as simple as providing a pointer to a manufacturer certificate if the manufacturer retains exclusive control over firmware downloads (as is usually the case).

This requirement for signed downloads is fully consistent with the TCG TPM trust model and therefore with extending TCG trust from the TPM to the host and to the internal operations of the SD.

1.4 ATA and SCSI Commands

Because of the requirements for secure sessions and the ATA and SCSI commands proposed to T13 and T10 serve mainly to provide a transport for the TCG-defined message streams. These commands have a field for a "Trusted Protocol ID" which is one byte. Five of the ordinals, 1-6, are assigned to trusted protocols defined by TCG; the remainder are reserved to INCITS or made available for proprietary use. If the Trusted Protocol ID is set to 0, then the SD is to return a credential that identifies the SD and it is this credential that can be used in some of the enrollment processes identified in the previous use cases.

2 TERMS AND ABBREVIATIONS

This document uses the following terms and abbreviations.

Term	Description
ATA	Attached
SCSI	Small Computer Storage Interface
SD	Storage Device
TCG	Trusted Computing Group
TPM	Trusted Platform Module
