SNIA
Storage Security Industry Forum

Storage Security Standards: What Are They and What Do they Mean to Storage Consumers?

Andrew Nielsen
CISSP, CISA, ISSAP, ISSMP
SNIA Security TWG

Storage Security Standards: What Are They and What Do they Mean to Storage Consumers?

Table of Contents

Storage Security Standards: What Are They and What Do they Mean to Storage Consumers?

Introduction

It has long been said that storage is one of the "last frontiers" to be exposed to security. Post the 9/11 tragedy, there has been a flurry of activity around securing information as it moves, rests, and is archived for the long term. Several varieties of security technologies have been thrown at this goal with limited market adoption though some of it continues to survive post acquisition and integration into core infrastructure products.

Accompanying the proliferation of technology has been a variety of standards initiatives that are now driving security into the core functionality of the storage ecosystem. Since these standards activities are in various phases of development and completion, they operate in largely isolated environments. In the interim, the storage consumer will struggle with the reality of the famous quote "That's the nice thing about standards -- there being so many to choose from."

In order to make the various standards a bit more palatable they can be grouped into the following courses or domains: Storage Management and Services, Fabric Security, Encryption in Storage, and IP Services Retrofit. The following table outlines the current domains and their relevant activities.

Domain	Standards Body	Standards Activity
Storage Management and Services	Storage Networking Industry Association	Storage Management Initiative Specification (SMI-S) eXtensible Access Method (XAM)
Fabric Security	INCITS T10	SCSI Object-Based Storage Device Commands (OSD) SCSI Primary Command Set (SPC-4) SCSI Stream Commands (SSC-3)
	INCITS T11	Fibre Channel Security Protocol (FC-SP) Fibre Channel Security Protocol v2 (FC-SP-2)
Encryption In Storage	IEEE P1619	IEEE P1619-2007 IEEE P1619.1 IEEE P1619.2 IEEE P1619.3
	Trusted Computing Group	TCG Storage Architecture Core Specification
IP Services Retrofit	Internet Engineering Task Force	Simple Network Management Protocol (SNMPv3) Syslog Internet Protocol Version 6 (IPv6) Transport Layer Security (TLS)

Storage Management and Services

In the domain of Storage Management and Services, the Storage Networking Industry Association (SNIA) is actively developing open standards for uniform storage management and services. SNIA's mission is to lead the storage industry worldwide in developing and promoting standards, technologies, and educational services to empower organizations in the management of information. Two of their key standards initiatives with relevance to storage security are the Storage Management Initiative Specification (SMI-S) and eXtensible Access Method (XAM).

SMI-S defines a method for the interoperable management of a multi-vendor Storage Area Network (SAN). SMI-S version 1.1.1, which is almost an approved ANSI standard, employs a multi-level model, with specific Security Management Aspects regarding device-level security via basic authentication capabilities, connectivity-level security via basic device authentication, and access control management to storage volumes in the fabric.

Transitioning from managing storage to accessing archived information, the XAM (eXtensible Access Method) Interface specification defines a standard access method to support ILM-based practices, long term records retention, and information security. Via the XAM Application Programming Interface (API), the specifications seek to manage the relationship between applications, management software and storage systems to manage fixed content reference information storage services. XAM includes specific metadata definitions to accompany data XAM, whose version 1 architecture specification is still under development.

Fabric Security

While SNIA owns the standards around storage management and access methods, the International Committee for Information Technology Standards (INCITS) is where the action is when it comes to SCSI and Fibre Channel Security. Under the purview of INCITS, sits two committees that are squarely in charge of SCSI and Fibre Channel Security: T10 and T11.

INCITS Technical Committee T10

INCITS T10's principal work is the Small Computer System Interface (SCSI), including a variety of architecture, command set standards that are all modern I/O interfaces, including SCSI,SAS, Fibre Channel, SSA, IEEE 1394, USB, and ATAPI (ATA).

On the most recently approved list of SCSI standards with security implication is the *SCSI Object-Based Storage Device Commands (OSD).* The standard defines the command set extensions to control operation of Object-Based Storage devices. The objective of the standard is to permit an application client to communicate with a logical unit that declares itself to be a Object-Based Storage device; enable construction of a shared storage processor cluster with equipment and software from many different vendors; define commands unique to the type of SCSI Object-Based Storage devices; and define commands to manage the operation of SCSI Object-Based Storage devices. The standard defines the concept of a security manager, and credentials that enable the execution of specific commands on Object-based Storage class devices.

Currently under development in T10 are two efforts that seek to integrate security into the SCSI Primary Command Set (SPC-4), as well as SCSI Stream Commands (SSC-3).

SPC-4 defines a security model, and two commands named Security Protocol In &Security Protocol Out that enable a number of security protocols to be transported by a SCSI infrastructure. The Trusted Computing Group is one of the organizations taking advantage of this facility to create security protocols specifically for use by storage devices.

SSC-3 includes in the command set extensions new mode pages and protocols specifically created to support an encryption/decryption features contained within sequential-access devices. The protocols make use of the Security Protocol In & Security Protocol Out commands defined by the SPC-4 project.

INCITS Technical Committee T11

INCITS T11's principal work is Fibre Channel (FC) including interface, protocol, switch and service definitions. This includes a variety of standards for FC physical and signaling, FC interconnection scheme standards, FC Generic Services Standards, and the FC Security Protocol standards.

Published in December 2006, T10 is responsible for the creation of the Fibre Channel Security Protocol (FC-SP). The FC-SP project developed a set of methods that allow security techniques to be implemented in a Fibre Channel fabric. FC-SP includes Security Association (SA), Fabric Policy, and authentication services. These protocols provide means to guard against malicious attacks, accidental configuration changes, and to ensure tighter control of the deployment of fabric devices.
Following on the success of FC-SP, INCITS Project 1835 seeks to enhance Fibre Channel security in the form of FC-SP-2. Today, commonly deployed security techniques are centered about zoning and FC-SP techniques. FC-SP-2 will develop a set of additional and enhanced security services for the Fibre Channel fabric. Specifically this project will address Fabric Loop Security Issues, Authentication Material Distribution and Management, Fabric Credential Definition and Management, Security Associations Policy Management Interfaces, FC-IFR Security support, and SHA-256 support.

Encryption in Storage

As we move through the storage ecosystem from protecting data in the fabric to securing data on disk, there are a variety of activities underway in various states of approval and development. Activities around security data at rest are largely driven by two entities: IEEE 1619 and the Trusted Computing Group.

Institute of Electrical and Electronics Engineers (IEEE) 1619

IEEE 1619, which is also referred to at the Security In Storage Working Group (SISWG), is charged with developing standards for the protection of information on storage media. In this working group, there are four standards with status ranging from "approved" to "still under development

The first approved standard from IEEE 1619 is the *Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices (IEEE 1619-2007).* 1619-2007's primary purpose is to describe encryption methods for data stored in sector-based devices as well as specifying encryption methods and import/export methods of encryption keys for interoperability between different implementations.

The 1619-2007 standard also specifies the use of a tweakable block cipher (XTS-AES) and its use in sector-based storage. XTS-AES addresses a variety of threats, while allowing parallelization and pipelining of cipher implementations.

Another 1619 activity that is in an approved state is the *Standard for Authenticated Encryption with Length Expansion for Storage Devices (1619.1)*. 1619.1, which should be published in the very near future, seeks to provide methods for ensuring the privacy and integrity of stored data within high-assurance applications. Similar to IEEE 1619-2007, IEEE 1619.1 also prescribes the use of AES encryption using authenticated encryption modes (GCM and CCM) that allow for authentication and length expansion. While the standard is valuable to vendors in the creation and development of cryptographic modules, its true value is to the consumer. This standard really affords the consumer of encryption technology a measuring stick by which to evaluate the quality of cryptographic devices based on compliance with 1619.1.

Exploring the "under development" realm of IEEE 1619, there are two activities that round out protection of data on disk. Those two activities are the *Standard for Wide-Block Encryption for Shared Media (IEEE P1619.2)* and the *Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data (IEEE P1619.3).*

1619.2 is an architecture specification for media security where an attacker has repeated access to encrypted data both in-flight and at rest. While 1619.2 is really geared to dealing with fixed-size encryption block, it is anticipated that future development of the standard will allow for data expansion, which will help prevent against data tampering.

While encryption of data on paper looks great, the market has been slow to adopt large scale encryption strategies as there has never been a uniform way to manage encryption keys that allows for vendor independence. IEEE 1619.3 seeks to address key management issues by specifying architecture for the infrastructure required to manage cryptographic protections for stored media. Additionally, this activity also manages the protections defined in the other 1619 standards.

Trusted Computing Group

Moving away from IEEE, the Trusted Computing Group (TCG) is also working on defining security protections for sector based devices. The TCG seeks to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, with their primary goal being to help users protect their information assets from compromise due to external software attack and physical theft.

The first version of the *TCG Storage Architecture Core Specification* is still currently under development. This TCG specification seeks to provide an architecture for applying policy-based access control to select storage features. This policy based control would allow storage devices to participate as part of a trusted platform. While the intended audience of the specification is storage device and peripheral device manufacturers, it is also useful for developers that may wish to integrate storage devices and peripherals into trusted platforms.

IP Services Retrofit (Courtesy of the IETF)

In recent history there has been a collision between the storage and networking worlds. With the advent of connected infrastructures, IT Compliance, executive dashboards, and single-pane of glass management interfaces, the storage world has been forced to integrate with a variety of internetwork services and protocols of varying security postures. Most of these protocols and services from a standards perspective are managed by the Internet Engineering Task Force (IETF).

The IETF formally under the purview of the Internet Society, develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standard bodies; and dealing in particular with standards of the TCP/IP and Internet protocol suite. Based on the broad scope of the work in the IETF, some of most relevant activity to storage security is SNMPv3, Syslog, IPv6, and TLS.

SNMPv3

The Simple Network Management Protocol (SNMP) is arguably the most commonly utilized network management Protocol (SNMP) on IP-based networks. The IETF recognizes SNMPv3 as defined by RFC 3411–RFC 3418 as the current standard version of SNMP as of 2004. Previous versions of SNMP lacked any security features mostly in the areas of authentication and confidentiality. SNMPv3 provides secure access to network based devices (including storage devices) using Message integrity, Authentication, and Encryption. As many network centric vendors have embraced SNMPv3, so are various storage vendors as this functionality is starting to appear in a variety of product offerings.

Syslog

While SNMP is the common for network management, Syslog is by far the most commonly utilized protocol for event logging of network based devices even though it was never a formal IETF standard. In the last few years, Syslog has become a standard feature on a variety of storage products as compliance and regulatory requirements continue to demand traceability of administrative actions. While many of the major storage vendors support the use of Syslog, the protocol has had its security challenges.

The Syslog Working Group under the purview of the IETF is charged with standardizing the Syslog protocol and its transport mechanism (currently UDP-based), and remediate the security issues around modification, disclosure, and masquerading. Based on this charter the Syslog Working Group has produced multiple draft standards to address these issues. The relevant draft standards for Syslog are:

- *Syslog Management Information Base (draft-ietf-syslog-device-mib-17)*
- *The Syslog Protocol (draft-ietf-syslog-protocol-23)*
- *Transmission of S9yslog messages over UDP (draft-ietf-syslog-transport-udp-12)*
- *TLS Transport Mapping for Syslog (draft-ietf-syslog-transport-tls-11)*

Internet Protocol v6

While it is well known that IPv6 was generally put in place to deal with IPv4 address exhaustion it also came with built-in transports security in the form of IPSec. The core IPv6 standards are widely implemented and are starting to see global deployment. While the IETF Editor has published three RFCs for IPv6 (RFC 4294, 4291, and 2460), even the US Federal Government has gotten in on the action publishing its own draft guidance in the form of NIST 500-267, which specifies the use of IPSec and cites specific cipher suites that must be supported.

As far as relevance to storage, there has been much discussion in the last year around the lack of security associated with various storage protocols such as CIFS, NFSv3, iSCSI, and iSNS. With customers slow to demand and deploy updated versions of these protocols, IPv6 with its native transport security in the form of IPSec may breathe new life into aging access methods.

Transport Layer Security (TLS)

The TLS protocol allows applications to communicate across a network in order to prevent eavesdropping, tampering, and message forgery. TLS is specified for transport security in SMI-S, Syslog, SNMP, and IEEE 1619 activities.

Established in 1996 The TLS Working Group was charged with standardizing a transport layer security protocol. Starting with SSL version 3.0, the working group has completed a series of specifications that describe the Transport Layer Security (TLS) protocol versions 1.0 (RFC 2246) and 1.1 (RFC 4346), extensions to the protocol, and new cipher suites to be used with TLS. Future work will include publishing a revision of TLS, version 1.2 *(draft-ietf-tls-rfc4346-bis-10)* that removes the protocol's dependency on the MD5 and SHA-1 digest algorithms. Version 1.2 will also provide new authenticated encryption modes and cipher suites for TLS.

Conclusions

While storage may be the next frontier for the integration of security, there is definitely no lack of activity to define standards in this space. While it is clear that all the major parts of the storage ecosystem have some amount of security activities underway or recently approved, what is not clear is how well all these standards will converge in the larger sandbox of the storage ecosystem as deployed by storage customers. Lack of integration at the standards level can lead to customer confusion, slow adoption rates, and vendors devising proprietary implementations as they push to get products to market to address customer needs. Such proprietary solutions limit customer flexibility and promote technology dependence, which can ultimately limit business agility.

Other than a few limited examples, most of these activities operate in fairly isolated environments with limited or non-existent communication between the activities. Most of the cross-talk between these security activities takes place in the SNIA Security Technical Working Group and the SNIA Storage Security Industry Forum. Going forward, SNIA will continue to be the nexus for monitoring these storage security standards.

What is a customer to do as they wait for storage security standards to be approved and vendors to implement? First and foremost, understand your storage infrastructure, the threats you face, your regulatory requirements, and the standards that are most applicable to help manage and protect your environment. Educated customers can help drive vendors to remain committed to supporting and implementing open standards with appropriate security as part of the core design. Continued customer and vendor support of storage security standards allows for all environments to be able to deploy a common set of security capabilities to protect information as it moves, as it sits, and as it migrates to new technologies.

About the SNIA

The Storage Networking Industry Association (SNIA) is a not-for-profit global organization, made up of some 400 member companies and 7,000 individuals spanning virtually the entire storage industry. SNIA's mission is to lead the storage industry worldwide in developing and promoting standards, technologies, and educational services to empower organizations in the management of information. To this end, the SNIA is uniquely committed to delivering standards, education, and services that will propel open storage networking solutions into the broader market. For additional information, visit the SNIA web site at www.snia.org.

About the SNIA Storage Security Industry Forum

The SNIA Storage Security Industry Forum (SSIF) is a consortium of storage professionals, security professionals, security practitioners, and academics dedicated to increasing the overall knowledge and availability of robust security solutions in today's storage ecosystems. The SSIF applies their deep body of knowledge and practical experiences in security and storage to produce best practices on building secure storage networks, provide education on storage security topics, and participate in standards development. SSIF educational, technical, and engineering activities influence the design, use, and management of storage technology to better protect and secure information. For more information, and to join, visit www.snia.org/forums/ssif.