Interested in learning more about security?

SANS Institute InfoSec Reading Room

An Overview of Hardware Security Modules

This paper intends to introduce the concept of a cryptographic hardware device. It will describe its functions, uses and implementations. It will explain some of the desirable features offered by hardware vendors, as well as examine some of the pitfalls, weaknesses, and disadvantages associated with these types of devices. It will summarize the FIPS 140 standard and explain how it pertains to these devices.

Version 1.2f of GSEC Practical Assignment for GIAC Certification for Jim Attridge

An Overview of Hardware Security Modules

Jim Attridge
January 14, 2002

Summary

This paper intends to introduce the concept of a cryptographic hardware device. It will describe its functions, uses and implementations. It will explain some of the desirable features offered by hardware vendors, as well as examine some of the pitfalls, weaknesses, and disadvantages associated with these types of devices. It will summarize the FIPS 140 standard and explain how it pertains to these devices.

It is assumed that the reader of this paper is already familiar with the basics of cryptography, Public Key Infrastructure (PKI) and the use of smart cards. Microsoft offers an online document that is a very good overview of these subjects at http://www.microsoft.com/windows2000/docs/CryptPKI.doc.

The Definition of an HSM

Within the context of this document, an HSM (or Hardware Security Module) is defined as a piece of hardware and associated software/firmware that usually attaches to the inside of a PC or server and provides at least the minimum of cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing. The physical device offers some level of physical tamper-resistance and has a user interface and a programmable interface

Other names for an HSM include Personal Computer Security Module (PCSM), Secure Application Module (SAM), Hardware Cryptographic Device or Cryptographic Module. For the sake of consistency and brevity, this paper will refer to these devices by the acronym HSM. To avoid confusion, it should be stated here that it is beyond the scope of this document to cover hardware firewall solutions.

HSM Functionality

An HSM can perform a number of important security-related functions. It provides accelerated cryptographic operations such as encryption, digital signatures, hashing, and Message Authentication Codes. A Message Authentication Code (or MAC) is an algorithm that mathematically combines a key with a hash to provide a “code” that can be appended with a given piece of data to ensure its integrity.

For example, suppose a database contains a list of account balances. It is very desirable from a security perspective to be able to prevent an unauthorized person from manually changing these values. Therefore, when an authorized entry is made, the HSM would provide an interface to MAC the input value that would be contained within the record itself. Because the HSM maintains the key that formulates the MAC, nobody else can theoretically reproduce a valid MAC for a given account balance. So when an authorized program retrieves the database value, the data provider would automatically ask the HSM to verify that the MAC for the value is correct. If the MAC verification fails, the program would know that the data has been tampered with and can perform the appropriate action such as auditing, logging, generating alarms, etc.

Another important function of an HSM is key management. With any type of system that uses cryptographic keys, it is imperative that the tools that generate, backup and hold these keys do so in a secure manner. To be optimally secure, the HSM should store all of the keys on the physical device itself. The key backups should be done using a secure connection to another HSM or to one or more smart cards (preferably more than one). The card reader should attach directly to the HSM to prevent the data from intercepted.

Some Common Implementations of an HSM

An HSM has a number of different uses. The functionality and security vary with price. Generally HSMs are implemented for the following uses:

- The key generator and safe key storage facility for a certificate authority [CHR98].
- A tool to aid in authentication by verifying digital signatures.
- An accelerator for SSL connections. (When the new IPSec standard begins replacing IP, the demand for server-side cryptographic acceleration will likely increase further)
- A tool for securely encrypting sensitive data for storage in a relatively non-secure location such as a database.
- A tool for verifying the integrity of data stored in a database.
- A secure key generator for smartcard production.

Typically, an HSM is installed inside a server box or within an Ethernet cluster within your architecture [FRA00]. The HSM is “wrapped” by your company’s software, the vendor’s software, a third party’s software, or a combination of the three. It is this software that provides access to the cryptographic functionality provided within the HSM. Ideally, the HSM will conform to PKCS #11, a standard that outlines the programmatic interface that the HSM supports. This standard is available online from RSA’s web site at http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html.

Positive Attributes of an HSM

There are many attributes vendors will accentuate to attempt to make their product look superior to others. The following attributes are actually desirable from a security perspective:

- FIPS 140-1 or 140-2 validation. This widely known standard provides four well-defined levels for validating HSMs. This validation does not mean that the product is perfect. However, if it is validated then there is at least a reasonable baseline of security tests performed on the HSM by qualified professionals at FIPS accredited testing facilities. Therefore, an important aspect of choosing an HSM is understanding the FIPS certification levels and weighing the costs of these levels versus the value of what is being secured. It is important to distinguish between vendors that claim FIPS 140 "compliance" versus "validation" since any vendor can claim that their product is compliant [SMI99].

- Widely accepted and open secure cryptographic algorithms. Many vendors' products will offer secret proprietary algorithms. It is preferable to stay away from these [SCH99]. For digital signatures, look for RSA or DSA based algorithms. For encryption, look for 3-DES or another well known and secure algorithm. For hashing, look for SHA-1 or MD5 [REE00, NISa01]. Some offer proprietary algorithms in addition to these open standard ones. It is important that the HSM is properly configured not to use the proprietary algorithms in this case.

- Strong random number generation. Random number generation (RNG) or pseudo-random number generation is critical to many cryptographic functions including key generation [AND98]. If the RNG is weak, the entire product is cryptographically unsound [SCH99].

- A secure time source. Secure auditing and non-repudiation require logged messages that include a time and date that comes from a protected source. A server's system clock can be easily changed. If a digitally signed message is constructed using an insecure time source, the time and date of the message (and the entire transaction) can be more easily disputed. An HSM should only allow an authenticated administrator to change the time and should securely log this event.

- A standardized interface for developers. A company looking to purchase an HSM needs to consider the complexity of their cryptographic needs. If they have more than basic needs then products that conform to PKCS #11 will offer a good industry-accepted standard. This is the "Cryptographic Token Interface Standard", which defines how software will interface with the cryptographic functions specified by the device.

- A user interface that provides simplicity and security. The installation of the physical hardware will be followed by the installation of software on the same machine to administer the HSM. Ideally, access to this interface should require at least one smart card (to be kept in the possession of a trained Security Officer). The user interface should be intuitive, user friendly, and have good 'Help' facilities. Administration duties from this interface can be critical to the very operation of an organization. If the interface is not easy to understand, very costly mistakes can be made.

- The physical device installation should be well documented. Physical switches on the device, machine compatibility, battery replacement and known hardware conflicts are among the issues that should be clearly documented.

- Key backup. If the HSM is to be used within a certificate authority, or for encrypting or verifying data in a database, it is imperative that the HSM have a secure mechanism for backing up the key(s) in the event of the device failing [CHR98]. Ideally, the key backup should be done to three or more smart cards [WAK01]. Each card contains a piece of the key being backed up and is stored in a separate location.

- Key protection. The device should never allow a plaintext private or secret key to be stored or transmitted outside its physical boundary. Any key that is exported should be encrypted. [AND98, CHR98].

- Tamper-resistance. The HSM should "zeroize" itself (erase all sensitive data), in the event it detects physical tampering, for example, by means of physical penetration, anomalous electrical activity or anomalous temperature. This is to prevent an adversary who has gained physical access to the card from retrieving the keys protected within.

- Scalability. If your network architecture needs to be scaled, it is essential that your HSM architecture be able to grow with it. HSMs that support clustering and load balancing are beneficial in this case. You can always buy another piece of hardware but it is important to consider if your architecture will support it.

- HMAC. As previously described in this document, one of the important functions of an HSM is the ability to verify the integrity of data stored in a database using a MAC. There are many implementations of MAC. The HMAC implementation is regarded as being one the most secure against cryptanalysis when implemented using a strong hashing algorithm such as SHA-1 or MD5 [WAD97].

Drawbacks to Using HSMs

The biggest drawback to using an HSM is cost. These devices can range in price from under a thousand dollars each to many thousands, depending on the level of functionality and security that is required.

Vendors typically withhold a lot of information about how their security products work. HSMs are no exception to this. While there are guidelines available for implementing and testing random number generators (RNGs), most vendors simply specify their RNG capability as “true”, “strong”, or “hardware-based”. Part of the problem is that there is currently no sufficient standard for randomness [SCH99].

Another disadvantage of HSMs over software is the difficulty in upgrading. If, for example, a weakness is exposed in a cryptographic algorithm, a new cryptographic software module can be plugged into a well-designed architecture with relative ease. This is typically not so with HSMs [LEE99].

FIPS 140-1 (or 140-2)

FIPS 140-1, released in January, 1994, is the original standard for certifying HSMs. A newer standard, FIPS 140-2 was released in June, 2001. Their certification levels range from one to four, with four being the strongest level of security. FIPS 140 sets out eleven specific areas and criteria that a module must meet for a given level of certification. These categories are [NISa01]:

1. The specification of the cryptographic module and its boundary as well as its security policy.
2. The interface to the device (ports, etc.)
3. The definition and separation of roles for operation and administration of the device
4. The finite state model for the device
5. The physical security of the device
6. The security of the embedded software/firmware on the device
7. Key management methods
8. Compliance with electromagnetic standards
9. Ability to perform self-tests such as power-up algorithmic tests and RNG tests
10. Design assurance
11. A specification of mitigated non-testable attacks.

The FIPS standard is certainly the easiest way to verify the security of a given HSM. A program affiliated with FIPS, called the Cryptographic Module Validation Program (CMVP), is responsible for verifying and validating a given HSM to a certification level. However, the validation program does not guarantee anything absolutely. The first ever HSM to receive a level 4 validation (the highest standard) was the IBM 4758. However, two researchers from the University of Cambridge demonstrated that when implemented with the “Common Cryptographic Architecture” (CCA), an optional architectural solution provided by

IBM with the hardware device, the device's 3-DES keys might become vulnerable to attack [BON01].

While this weakness in the CCA does not explicitly break the validity of FIPS 140 standard, it raises questions as to whether or not its scope is comprehensive enough [REE00]. The bottom line is that when selecting any tool or methodology to assist a security process, there are no shortcuts. It is essential that any solution be thoroughly researched and reviewed by well-trained security professionals [AND98].

Considerations in Purchasing an HSM

An HSM provides cryptographic functionality. So does software. There are even free, downloadable cryptographic components that functionally do just about anything that an HSM would do. So why pay $500 to over $10,000 for an HSM [BRA00]?

Basically, there are three main reasons: Increased security, accelerated cryptographic performance [BRA00, CRO01, CAR01] and an industry standardized certification and validation program (CMVP) [SMI99, CHR01]. If selected carefully and implemented properly, an HSM provides roughly one or two orders of magnitude increase in speed over software [CAR01]. It does this within an operating environment where keys are generated, used, and stored within what should be a tamper-resistant hardware device. It is this ability to securely create, store, and use cryptographic keys that is the greatest benefit of the HSM. The CMVP provides a baseline for security and quality assurance [CHR01].

The cost of the device can be partially offset by reducing the need for more servers to support the increased need for cryptography [CAR01]. It should be noted, however, that an HSM is often sold by a security vendor as part of a broader PKI security package or solution, the cost of which can be formidable (hundreds of thousands to several million dollars) [FRA00]. Still, if a purchaser is diligent, it is possible to implement an HSM without the vendor's supporting security package or solution.

Sources for Locating HSM Vendors

There are multitudes of vendors that sell HSMs. The individual vendor's web sites will, naturally, offer their product as being superior. As such, there are no shortcuts to selecting an appropriate vendor and careful scrutiny must be taken. To assist in the selection, the CMVP (Cryptographic Module Validation Program) supplies a current list of products, vendors, and what level of FIPS certification their modules have obtained [NISb01]. This list is at least a good start to the process of selecting a vendor.

The CMVP is accessible on the Internet at http://csrc.nist.gov/cryptval/vallists.htm.

Conclusion

An HSM can be an invaluable part of an overall security solution. However, it alone is worthless without proper consideration given to the foundations of proper security process, such as careful risk analysis, design, implementation, security testing, user education, security policy, and careful installation and administration of the product.

The overall benefits that an HSM can bring to a security solution are increased security for the creation, storage and use of cryptographic keys, accelerated cryptographic performance, and an industry standardized hardware platform from which to architect a suitable security solution for your organization.

References

[AND98]
Anderson, R.; "Why Cryptosystems Fail"; March 1998; University of Cambridge Computer Laboratory web site URL: http://www.cl.cam.ac.uk/~rja14/wcf.html

[BON01]
Bond, M., Clayton, R.; "Extracting a 3DES key from an IBM 4758"; November 2001; University of Cambridge Computer Laboratory web site URL: http://www.cl.cam.ac.uk/~rnc1/descrack/index.html

[BRA00]
Bracco, T.; "Tales from the Crypto"; Network World Fusion Reviews; May 2000; Network World Fusion web site URL: http://www.nwfusion.com/reviews/2000/0522rev3.html

[CAR01]
Carter, S., Kilvington, S., Lockhart, H.W., Woollard, S., Nicolls, W.; "Ask The Experts – When and why should I chose hardware encryption rather than software encryption?";ITsecurity.com Security Clinic: May 2001; The Encyclopedia of Computer Security web site URL: http://www.itsecurity.com/asktecs/may501.htm

[CHR98]
Chrysalis-ITS Library Whitepaper; "It's 1:00 AM: Do you know where your root key is? A Security Assurance White Paper from Chrysalis-ITS"; Fall 1998; Chrysalis-ITS web site URL: http://www.chrysalis-its.com/news/library/white_papers/CAwhitepaper2.htm

[CHR01]

Chrysalis-ITS Library Whitepaper; "Evaluation, Validation, and Certification: FIPS 140-1 and Common Criteria"; June 2001; Chrysalis-ITS web site URL: http://www.chrysalis-its.com/news/library/white_papers/FIPS_CC_white_paper.pdf

[CRO01]
Cross, D., Franklin, W. A.; "Windows 2000 Server and PKI: Using the nCipher Hardware Security Module"; Microsoft Corporation; April 2001; Microsoft web site URL: http://www.microsoft.com/windows2000/docs/winpkihsm.doc

[DYE99]
Dyer, J., Perez, R., Smith, S., Lindemann, M.; "Application Support Architecture for a High-Performance, Programmable Secure Coprocessor"; 22nd National Information Systems Security Conference; October 1999; IBM Security Research web site URL: http://www.research.ibm.com/secure_systems/papers/nimp.pdf

[FRA00]
Franklin, B.; "Hardware Security Modules (HSM) and PKI"; September 2000; PKI Forum web site URL: http://www.pkiforum.org/meetings/icm/PKIF-ICM-Tech_files/slide0207.htm

[LEE99]
Lee, A.; "Guideline for Implementing Cryptography in the Federal Government"; National Institute of Standards and Technology (NIST), U.S. Department of Commerce; November 1999; NIST web site URL: http://csrc.ncsl.nist.gov/publications/nistpubs/800-21/800-21.pdf

[NISa01]
National Institute of Standards and Technology (NIST); "Security Requirements for Cryptographic Modules (FIPS PUB 140-2)"; U.S. Department of Commerce; May 2001; NIST web site URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[NISb01]
National Institute of Standards and Technology (NIST); "FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List"; U.S. Department of Commerce; December 2001; NIST web site URL: http://csrc.nist.gov/cryptval/140-1/1401val.htm

[REE00]
Reed, W.; "Cryptography Doesn't Protect Information Security Engineering Protects Information"; Cryptographic Centre of Excellence Quarterly Journal (Issue 1 2000); January 2000; pp. 24-29; PricewaterhouseCoopers web site URL:http://www.pwcglobal.com/Extweb/service.nsf/docid/076D2D5D726357E0852568AF00180975

[SCH99]
Schneier, B.; “Security in the Real World: How to Evaluate Security Technology”; Computer Security Journal (Volume XV, Number 4, 1999); June 1999; Counterpane web site URL: http://www.counterpane.com/real-world-security.pdf

[SMI99]
Smith, S.W., Perez, R., Weingart, S.H., Austel, V.; “Validating a High-Performance, Programmable Secure Coprocessor”; 22nd National Information Systems Security Conference; October, 1999; IBM Security Research web site URL: http://www.research.ibm.com/secure_systems/papers/nfips.pdf

[WAD97]
Wagner, D., Schneier, B.; “Analysis of the SSL 3.0 Protocol (revision)”; Counterpane Labs Publications; April 1997; Counterpane web site URL: http://www.counterpane.com/ssl-revised.pdf

[WAK01]
Wagner, K.; “Smartcards”; Cryptographic Centre of Excellence Quarterly Journal (Issue 5 2001); October 2001; pp. 5-13; PricewaterhouseCoopers web site URL: http://www.pwcglobal.com/Extweb/pwcpublications.nsf/docid/C185AF2B5E83A80685256B1B0054B2E1

Last Updated: June 28th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SEC564:Red Team Ops	OnlineCAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced