NEW TRENDS IN IT&C SECURITY EVALUATION

Cristian Teodor PĂUN*
Emil SIMION**

Abstract

This paper focuses on the link between information security and cryptography represented by National Institute of Standards and Technology (NIST) cryptographic standards, Federal Information Processing Standard FIPS 140-2 (Security requirements for cryptographic modules) standard and Common Criteria for Information Technologies Security Evaluation (ISO 15408) standard. Information security is the science of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Cryptography deals with design, implementation and evaluating cryptographic algorithms (e.g. NIST AES selection process, SHA-3 completion etc.) in order to be used by products (software and/or hardware) which are intended to protect information or information systems. Before using in information systems those cryptographic products need to be tested and evaluated also. One evaluation standard is FIPS 140-2. After this evaluation is obtained, from an accredited Laboratory, the system itself needs to be evaluated in order to have a image of the assurance level obtained. Usually these evaluation is made using ISO 15408 (Common Criteria for Information Technology Systems) standard.

Keywords: cryptographic algorithms, FIPS 140-2, ISO 15408, crypto modules, security evaluation.

1. INFOSEC

INFOSEC domain covers the following areas:

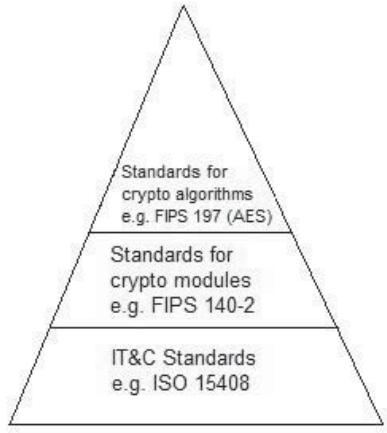

Figure 1: INFOSEC standards stratification

Physical security describes both measures that prevent or deter attackers from accessing a facility, resource, or information stored on a physical media and guidance on how to design structures to resist various hostile acts.

Personnel security describes the restriction of data which is considered very sensitive. Under need-to-know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information unless one has a specific need to know; that is, access to the information must be necessary for the conduct of one's official duties. As with most security mechanisms, the aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access. Need-to-know also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people.

Procedural security deals with the establishment and enforcement of security procedures. Some of these procedures may be independent of the type or types of computers involved. Others may not. For example, perimeter security controls are usually similar for all type of systems. But desktop computers may require forms of antitheft protection not required by mainframes. Procedural security regulates the performance of duties associated with system operation and use, and with the physical storage of system information. Common security practices include partitioning computer operating duties, using several operators, and storing backup tapes at bonded, offsite depositories. Procedural security also encompasses and may regulate company policies that deal with information security, such as policies that regulate the way individuals manage their own passwords.

Communications security (COMSEC) describes the measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, traffic-flow security and physical security of COMSEC equipment.

Computer security is a branch of technology known as information security applied to computers. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

TEMPEST is a codename referring to investigations and studies of compromising emanations (CE). Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment. Compromising emanations consist of electrical, mechanical, or acoustical energy intentionally or by mishap emitted by any number of sources within equipment/systems which process national security information. This energy may relate to the original encrypted message, or information being processed, in such a way that it can lead to recovery of the plaintext. Laboratory and field tests have established that such CE can be propagated through space and along nearby conductors. The interception/propagation ranges and analysis of such emanations are affected by a variety of factors, e.g., the functional design of the information processing equipment, system/equipment installation, and, environmental conditions related to physical security and ambient noise. The term "compromising emanations" rather than "radiation" is used because the compromising signals can, and do, exist in several forms such as magnetic-and/or electric-field radiation, line conduction, or acoustic emissions.

Information assurance (IA) is the practice of managing information-related risks. More specifically, IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These goals are relevant whether the information are in storage, processing, or transit, and whether threatened by malice or accident. In other words, IA is the process of ensuring that authorized users have access to authorized information at the authorized time.

INFOSEC Standards

INFOSEC standards can be stratified like in Figure 1: standards for cryptographic algorithms, cryptographic modules and for IT&C security. In this chapter we focus on standards for cryptographic algorithms, crypto-modules (FIPS 140-2) and IT&C standards (e.g. ISO 15408).

2. CRYPTOGRAPHIC STANDARDS

Our discussion is based on National Institute of Standards and Technologies (NIST) cryptographic standards. These standards can be divided in four classes: symmetric key, public key, secure hash and random number generation.

In symmetric key we can found for example AES (FIPS 197), DES (FIPS 46-3) for block ciphers standards or HMAC (FIPS 198) for hashing and message authentication code. We remained that simple DES was replaced by AES, 3-DES being in use. In public key standards we can found Digital Signature Standard (FIPS 186-3), Key Establishing Schemes (DH&MQV, FFC&ECC SP 800-56A) and Key Management Guideline. Secure hash is referring to SHA-1, SHA-224, SHA-384, SHA-512 (FIPS 180-2). At this time there exists a draft for SHA-3 which will replace SHA-2.

One standard for random number generation standards is SP 800-90.

The following table gives the theoretical comparable strengths of symmetric and asymmetric cryptographic algorithms.

Sym Key	80	112	128	192	256
Hash functions (for signatures)	160	224	256	384	512
FFC and IFC	1K	2K	3K	7.5K	15K
ECC	160	224	256	384	512

NIST approved standards are referred by NIST Cryptographic Toolkit. Some of these standards are allowed to process classified information. For example, AES with 128 bit key can be used to protect SECRET classified information and AES with 192 or 256 bit key can be used to protect TOP SECRET classified information.

FIPS 140-2

Cryptographic controls are provided using cryptographic modules, which may include capabilities such as signature generation and verification, encryption and decryption, key generation, and key establishment.

An undetected error in a cryptographic module design could affect every user in the system for which it is supposed to provide protection. For example, the verification of a chain of public key certificates might not function correctly.

Verifying a chain of public key certificates helps a signature verifier determine if a signature was generated with a particular key. If the function is implemented incorrectly in a cryptographic module, the potential for the dissemination of weak cryptography could be introduced into the system, possibly allowing for signature forgery or the verification of invalid signatures. Therefore, it is important to have cryptographic modules tested before distributing them throughout a system.

The security requirements in FIPS 140-2 cover 11 areas related to the design and implementation of a cryptographic module:

• Cryptographic module specification includes definition of cryptographic boundary, approved algorithms and approved modes of operations;
• Cryptographic module ports and interfaces are referred to the specification of all interfaces and all input data paths. For security level 3 and 4 data ports for unprotected critical security parameters logically or physically separated from others data ports;
• Roles, services and authentication requires, for all security levels, logical separation of required and optional roles and services. For level 2 operators authentication must be role–based or identity–based. To achieve security level 3 and 4 operator authentication must be identity-based;
• Finite state model requires the specification of finite state model, required and optional states, state transition and specification of these transitions;
• Physical security is focusing to tamper evidence, detection and response (e.g. erasing critical security parameters);
• Operational environment is referring to evaluation, for example, of Protection Profile (PP) at (Evaluation Assurance Level) EAL 4;
• Cryptographic Key Management is referring to the key (secret, private and public) manipulation during its life time: generation, pre -activation, activation, usage, storage and deletion;
• EMI/EMC – electromagnetic compliance with Federal standards;
• Self – Tests includes power-up tests and conditional tests;
• Design assurance is referring to configuration management, secure installation, design policy and guidance documents;
• Mitigations of others attacks are referred to specification of mitigation of attacks for which no testable requirements are currently available.

Within most areas, a cryptographic module receives a security level rating of 1 to 4, from lowest to highest, depending on what requirements are met. For other areas that do not provide for different levels of security, a cryptographic module receives a rating that reflects the fulfillment of all of the requirements for that area.

An overall rating is issued for the cryptographic module, that indicates the:
1. Minimum of the independent ratings received in the areas with levels, and
2. Fulfillment of all the requirements in the other areas.

On a vendor's validation certificate, individual ratings are listed as well as the overall rating. It is important for vendors and users of cryptographic modules to realize that the overall rating of a cryptographic module is not necessarily the most important rating. The rating of an individual area may be more important than the overall rating, depending on the environment in which the cryptographic module will be used (this includes understanding what risks the cryptographic module is intended to address). Modules may meet different levels in different security requirement areas; for example, a module may implement identity-based authentication (level 3 or 4) and display tamper evidence (level 2).

At this time the draft for FIPS 140-3 where NIST has updated the standard to reflect changes in technology has a fifth security level. In this draft there is a special section dedicated to software security and specifying requirements to protect against non-invasive attacks. Also the reference to Common Criteria (ISO 15408) and requirements for the use of Common Criteria certified operating systems has been dropped. In this draft NIST improves the requirements for authentication for level 4 at two-factor authentication (at least two of three: something known, something possessed and some physical property). Also a greater importance is given to physical

security requirements to defeat non - invasive attacks/side channel attacks (protection to timing attacks (TA), differential power analysis (DFA) etc.)

3. CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP)

NIST and the Communications Security Esablishment (CSE) of the government of Canada established the CMVP. The goal of the CMVP is to provide Federal agencies with a security metric to use in procuring equipment containing cryptographic modules. The results of the independent testing by accredited laboratories provide this metric. Cryptographic module validation testing is performed using the Derived Test Requirements (DTRs) for FIPS 140-2. The DTRs list of all the vendor and tester requirements for validating a cryptographic module are the basis of testing done by the Cryptographic Module Testing (CMT) accredited laboratories. Figure 2 illustrates the CMV process.

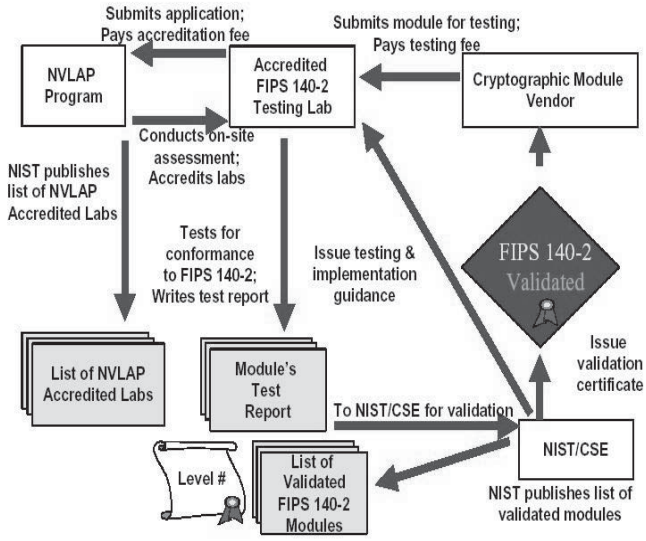

Figure 2: CMV process

4. IT&C ASSURANCE STANDARDS (COMMON CRITERIA)

Information Technology Security Evaluation Criteria (ITSEC), predecessor of Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC), is a structured set of criteria for evaluating computer security within products and systems. The ITSEC was first published in May 1990 in France, Germany, the Netherlands, and the United Kingdom based on existing work in their respective countries. Following extensive international review, Version 1.2 was subsequently published in June 1991 by the Commission of the European Communities for operational use within evaluation and certification schemes. Since the launch of the ITSEC in 1990, a number of other European countries have agreed to recognise the validity of ITSEC evaluations.

Thus Common Criteria is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1. Common Criteria is a framework in which computer system users can specify their security requirements, vendors can then implement and/or make

claims about the security attributes of their products and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. Common Criteria is performed on computer security products and systems and provides similarly-defined evaluation levels, implements the target of evaluation concept and the Security Target document.

Target of Evaluation

Target of Evaluation (TOE) - the product or system that is the subject of the evaluation. The evaluation serves to validate claims made about the target. To be of practical use, the evaluation must verify the target's security features. This is done through the following:

Protection Profile (PP) - a document, typically created by a user or user community, which identifies security requirements for a class of security devices (for example, smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose. Product vendors can choose to implement products that comply with one or more PPs, and have their products evaluated against those PPs. In such a case, a PP may serve as a template for the product's ST (Security Target, as defined below), or the authors of the ST will at least ensure that all requirements in relevant PPs also appear in the target's ST document. Customers looking for particular types of products can focus on those certified against the PP that meets their requirements.

Security Target (ST) - the document that identifies the security properties of the target of evaluation. It may refer to one or more PPs. The TOE is evaluated against the SFRs (see below) established in its ST, no more and no less. This allows vendors to tailor the evaluation to accurately match the intended capabilities of their product. This means that a network firewall does not have to meet the same functional requirements as a database management system, and that different firewalls may in fact be evaluated against completely different lists of requirements. The ST is usually published so that potential customers may determine the specific security features that have been certified by the evaluation.

Security Functional Requirements (SFRs) - specify individual security functions which may be provided by a product. The Common Criteria presents a standard catalogue of such functions. For example, an SFR may state how a user acting a particular role might be authenticated. The list of SFRs can vary from one evaluation to the next, even if two targets are the same type of product. Although Common Criteria does not prescribe any SFRs to be included in an ST, it identifies dependencies where the correct operation of one function (such as the ability to limit access according to roles) is dependent on another (such as the ability to identify individual roles).

5. EVALUATION PROCESS

The evaluation process also tries to establish the level of confidence that may be placed in the product's security features through quality assurance processes:

Security Assurance Requirements (SARs) - descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the ST and PP, respectively.

Evaluation Assurance Level (EAL) - the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) and EAL 7 being the most stringent (and most expensive). Normally, an ST or PP author will not select assurance requirements individually but choose one of these packages, possibly 'augmenting' requirements in a few areas with requirements from a higher level. Higher EALs do not necessarily imply "better security", they only mean that the claimed security assurance of the TOE has been more extensively validated.

So far, most PPs and most evaluated STs/certified products have been for IT components (e.g., firewalls, operating systems, smart cards). Common Criteria certification is sometimes specified for IT procurement. Other standards containing, e.g, interoperation, system management, user training, supplement CC and other product standards. Examples include the ISO 17799 (or more properly BS 7799-2, which is now ISO/IEC 27002) or the German IT-Grundschutzhandbuch.

Details of cryptographic implementation within the TOE are outside the scope of the CC. Instead, national standards, like FIPS 140-2, give the specifications for cryptographic modules, and various standards specify the cryptographic algorithms in use.

Conclusions

This paper presented the connections between ISO 15408 (Common Criteria for information Technologies Security Evaluation), FIPS 140-2 (Security requirements for cryptographic modules) and cryptographic algorithms.

References

Alexander W. D., Chris J. M. (2006). User's guide to Cryptography and Standards, Artech House.

Barker, E.B., Barker, W.C., & Lee, A.(2005). Guide line for implementing cryptography in the federal systems - Second Edition (SP 800-21), Gaithersburg, USA: National Institute of Standards and Technology (NIST).

Common Criteria for Information Technology Security Evaluation, ISO 15408.

Federal Information Processing Standards Publication (FIPS) 140-2 (2002). Security requirements for cryptographic requirements, Gaithersburg, USA: National Institute of Standards and Technology.

ISO standards available from World Wide Web: <http://www.iso.ch/>

Security requirements for cryptographic requirements, FIPS 140-2.

available from World Wide Web: <NIST standards: http://www.nist.gov/;

http://www.csrc.nist.gov/>