# Information security standard research paper example

Business, Management

# Information security standard

Information security programs and policies are essential components of an organizations security. In formulation of these programs and policies certain relevant standards are used. A security program or policy determines the kind of standard to be used. For instance ITU-T and IEEE are bodies of standards that cover all fields in telecommunication and computer and electronic industry respectively. Fiba is a company that specializes in computer networking, storage and backup facilities and internet solutions. The company used the National Institute of Standards and Technology standards in formulation of its information security program and policy. Security of information systems for an organization is an important exercise that poses major implications on the operation of personnel and security of assets. Security controls are the fundamental parameters that define the managerial, operational and technical safeguards and counter measures deployed to an organizations information system. The fundamental aim of NIST standards is to aid in the development of policies that preserve and restore the confidentiality, integrity and availability of information within the system (Foreman, 2010).

NIST issued the FIPS 140 to coordinate the necessary standards for hardware and software cryptographic modules used in agencies and department in the US federal governments. The requirements stipulate the cryptographic modules, its documentation at the highest level and aspects of comments contained in the source code. FIPS 140-2 has definitions for four levels of security of which the first level imposes limited requirements while the fourth level has more stringent and robust requirements. The scope of the

requirements includes cryptographic modules, ports and interfaces, authentication, finite state model, physical security operational environment and cryptographic key management (Mun 2011).

ISO/IEC 19790 standard is a security requirement for cryptographic modules used within security systems with sensitive information in computer and telecommunication equipments. This standard provides four security levels for cryptographic modules for increased security of a larger spectrum of sensitive data.

## Points of analysis

Security

This is the level of security definitions defined by the standard. It defines the levels of security of information systems as well as the extra attacks and the mitigation strategies.

## Developing country

The countries that develop the standards are varied. For instance FIPS 140 is a standard for the US federal government. Algorithm requirements and module requirements are country dependent.

## Approval authority

Any cryptographic standards need an approval authority behind it. Also the algorithms should meet a certain standard with a universal or otherwise separate list.

## Requirement areas

Algorithm implementation

A standard has a set of algorithms for use when developing an information system. The algorithm might doffer according to the standard implemented.

## COMPARISON

Security

## The security requirements are arranged into 11 requirement areas. In ISO 19790, they include:

Cryptographic module specification

Cryptographic module interface

Roles, services and authentication

Software security

Operational environment

Physical security

Sensitive security parameter management

Mitigation of other attacks

Lifecycle assurance

Self-test

The difference between FIPS 140 and ISO 19790 is that most of these parameters have changed in FIPS 140.

Security

FIPS 140 has four levels of security but it does not describe in detail what measures of security are required by a particular application. FISP 140 is faulted as a standard that gives a false sense of security. For instance at

level 2, the standard implies that modules will be tamper-evident but the same modules are allowed to have side channels vulnerabilities that allow simple extraction of keys.

ISO/19790 specifies the cryptographic modules of a system having sensitive information in its computer networks. The four levels of security offer increasing level of security than the preceding one.

Developing country

As mentioned previously, FISP 140 is a US federal government standard that certifies cryptographic modules for the products in the US market. In contrast, reference to the US legislation and US algorithm site is removed in ISO 19790. The ISO/IEC JTC sub-committee 27 of 2003 was made up of experts from France, Japan and the US to produce the first edition of ISO 19790 which was subsequently published in 2006. FIPS 140 has long been recognized as a US government project and do not seem appropriate for cases beyond the US Government regulation (Nemati, 2008).

Approval authority

FISP 140 has numerous evaluating countries and labs. It is used by many nations and thus has a worldwide acceptance. In addition the standard has international collaboration as well as economic incentives of purchasing requirements. ISO 19790 has no defined approval authority as well as CCRA-like agreement to support it. It also has limited economic drivers. The limited number of nations using it and the few labs makes it less usable (Rausi, 2010).

# ALGORITHM IMPLEMENTATION

ISO-19790 provides for an individual definition of algorithms for each country. Therefore each country defines and tests the requirements according to its own mechanisms. In contrast, FIPS 140-2 is the defacto international cryptographic standard with a single algorithm definition for all nations.

NIST has the role of developing regulations and procedures that stipulates the operation of information systems run by federal agencies, contractors, enterprises and other sectors to ensure efficient detection and mitigation of national security threats. The standards explained above solve the security concerns through policies and programs. The solutions include:

- Authorization of information systems for processing
- Continuous monitoring and evaluation of the security controls for the purpose of ensuring adherence to the set goals
- Evaluation of the risks faced by the agency in respect to the business case and mission among others (NIST, 2013).

# References

Foreman, P. (2010). Vulnerability Management. London: Taylor & Francis.

Mun, G. J., Kou, K. S., & Ryu, D. J. (2011). The Development of SP Security Functional Requirements in CMVP. □□□□□□□□□ (Journal of Security Engineering), 8(6).

Nemati, H. R. (2008). Information security and ethics: concepts, methodologies, tools and applications, Volume 4. New York: Information Science Reference.

NIST. (2013). NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations. Washington: NIST .

Rauzy, P., & Guilley, S. (2010) Formally Proved Security of Assembly Code against Leakage.