Analysis of best practices for Information Security Evaluation and Management

Pradnya S. Gotmare and Satish R.. Devane

***Abstract*—Information security is the important aspect because of the major use of electronic devices and systems. Information security deals with several different "Trust" aspects of information. Another common term is information assurance. Information security is not confined to computer systems. It applies to all aspects of safeguarding or protecting information or data. Today, Lack of computer security is a multi-pronged menace to which a multi-faceted defense is the only solution. It is essential to have well implemented and comprehensive security mechanism in IT products and IT systems. security evaluation play a critical role in establishing the assurance of a product's security-worthiness. Security evaluations provide a formal yardstick against which a product or system can be certified having internationally developed and recognized security standards by independent but authorized and accredited organizations. Appropriate security standards like BS-7799, CC, and FIPS can be used together for effective and efficient security evaluation and management.**

***Index Terms* — Evaluation Assurance Level, Information Security, Information Security Management System, Security evaluation, Security Functional Requirements, Target of Evaluation.**

I. INTRODUCTION

Information held by IT products or systems is a critical resource that enables organizations to succeed in their mission. The information used for business transactions is more valuable than any infrastructure or asset in that organization. The first step to security is "identifying the assets" and then working towards protecting them. At the same time, individuals need to keep their personal information contained in IT products or IT systems remain private, and should be available to them as needed, and should not be subject to unauthorized modification. IT products or IT systems should perform their functions while exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. The term IT security is used to cover prevention and mitigation of these and similar hazards. Many consumers of IT lack the knowledge, expertise or resources necessary to judge whether their confidence in the security of their IT products or IT systems is appropriate, and they may not wish to rely solely on the assertions of the Developers. Consumers may therefore choose to increase their confidence in the security measures of an IT product or IT system by ordering an analysis of its security. This is termed as security evaluation.

The Common Criteria is an international standard for computer security evaluation. It contains criteria for evaluation of security requirements. It describes the framework in which computer system users can specify their security requirements, vendors can then implement and/or make claims about security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. 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.

The Federal Information Processing Standard 140 (FIPS) is the the standard that specify requirements for cryptography modules. FIPS provides assurance that a module conforming to its requirements is secure.

BS-7799 is one of the international standard for managing information security. It is developed to provide a model for setting up and managing an effective Information Security Management System (ISMS).

II. SECURITY CONTEXT

A. General Security Context

Security is concerned with the protection of assets from threats, where threats are categorized as the potential for abuse of protected assets. All categories of threats should be considered. Safeguarding assets of interest is the responsibility of owners, who place value on those assets. Threat agents may seek to abuse or may damage assets. Security specific impairment commonly includes disclosure of the asset to unauthorized recipients (loss of confidentiality) , damage to the asset through unauthorized modification (loss of integrity), or unauthorized deprivation of the asset (loss of

[1] Pradnya S Gotmare is pursuing M.E. in Computer science at Ramrao Adik Institute of Technology (RAIT)***, Nerul, Navi Mumbai.***

[2] .Dr. ***Satish R*** Devane is working as a professor and Head, Department of Computer Engineering at Ramrao Adik Institute of Technology (RAIT), Nerul, Navi Mumbai.

availability).The owner of the asset will analyze the possible threats to determine which one apply to their environment. The results are known as risks. This analysis can aim in the selection of countermeasures to counter the risks and reduce it to an acceptable level. Countermeasures are imposed to reduce vulnerabilities and to meet security policies of the owners of the assets (either directly or indirectly by providing direction to other parties).

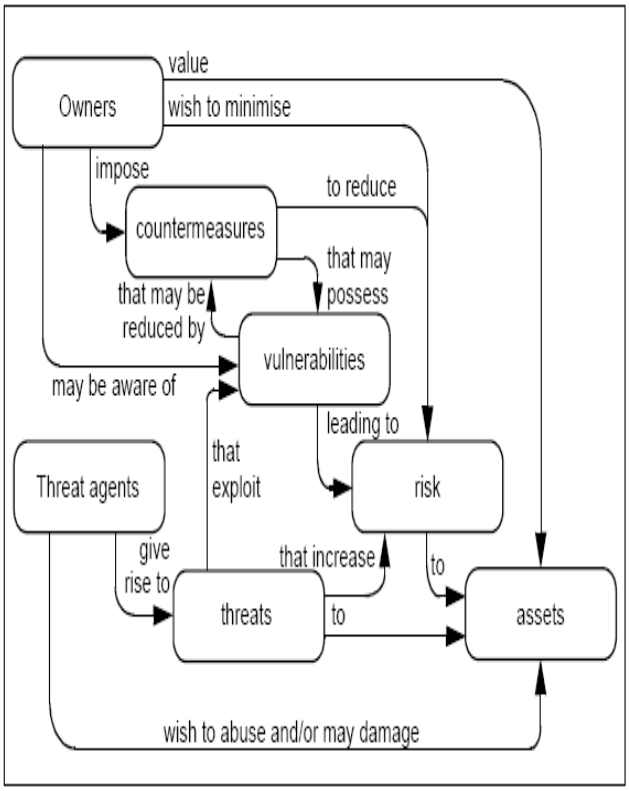

Fig. 1 Security concepts and relationships

Residual vulnerabilities may remain after the imposition of countermeasures. Such vulnerabilities may be exploited by threat agents. Owners will seek to minimize that risk given other constraints. Owners will need to be confident that the countermeasures are adequate to counter the threats to assets before they will allow exposure of their assets to the specified threats. Owners may not themselves possess the capability to judge all aspects of the countermeasures, and may therefore seek evaluation of the countermeasures. This relationship is shown in Fig. 1.

The outcome of evaluation is a statement about the extent to which assurance is gained that the countermeasures can be trusted to reduce the risks to the protected assets. The statement assigns an assurance rating of the countermeasures, that gives grounds for confidence in their proper operation. This statement can be used by the owner of the assets in deciding whether to accept the risk of exposing the assets to the threats. Fig. 2 illustrates these relationships.

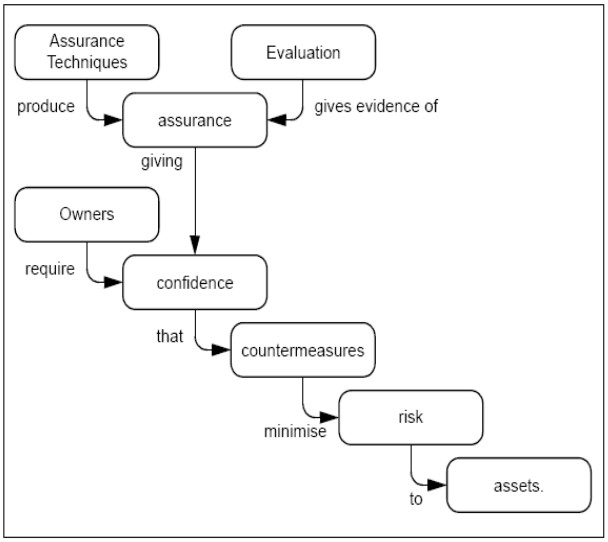

Figure 2 – Evaluation concepts and relationships.

B. Information technology security context

Many assets are in the form of information that is stored, processed and transmitted by IT products or systems. Information owner may require that the IT product or system implement IT specific security controls as part of the overall set of security countermeasures.

IT systems are procured and constructed to meet specific requirements and may, for economic reasons, make maximum use of existing commodity IT products such as operating systems, general purpose application components, and hardware platforms. IT security countermeasures implemented by a system may use functions of the underlying IT products and depend upon the correct operation of IT product security functions. The IT products may, therefore, be subject to evaluation as part of the IT system security evaluation.

III. STANDARDS FOR INFORMATION SECURITY

A. Common Criteria (CC).

Common Criteria is an ISO/IEC 15408 standard used as the basis for evaluation of security properties of IT products and systems. The evaluation serves to validate claims made about the target. The evaluation must verify the target's security features. Protection Profile(PP) and Security Target(ST) has to consider physical/operating environment relevant to TOE(Target of Evaluation)security. PP is a technical document, typically created by a user or user community, which identifies security requirements relevant to that user for a particular purpose. A PP effectively defines a class of security devices (for example, smart cards used to provide digital signatures, or network firewalls). Product vendors can choose to implement products those comply with one or more PPs. 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 certified products PPs that meets their requirements.

Security Functional Requirements (SFRs) – It specifies individual security functions which may be provided by a product. The Common Criteria presents a standard catalogue of such functions.

Security Target (ST) – It is the technical document that identifies the security properties of the Target of Evaluation. Each target is evaluated against the SFRs established in its ST. 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 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. 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 (SAR) - Descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. 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) – It is the numerical rating assigned to the target to reflect the assurance requirements fulfilled during the evaluation. Each EAL corresponds to a package of assurance requirements which covers the complete development of a product, with a given level of strictness.

B. CC Evaluation Levels

Common Criteria lists seven levels, from EAL1 through EAL7 representing the degree of confidence in the correctness of the product or system. Level EAL1 mandates a minimum of functional testing. Level EAL4 requires the specification of a security target, an informal description of detailed design, functional testing, source code analysis, testing of security mechanisms, configuration control systems and approved product distribution procedures. Level EAL7 represents the highest level of confidence and requires very stringent formal development, verification and distribution methods significantly beyond the scope of commercially-available products or systems. Higher EAL levels do not necessarily imply "better security", they only mean that the claimed security assurance of the TOE has been validated more extensively .

C. CC Evaluation Process.

In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations and administers the regulations. The TOE evaluation process as described in Fig. 3 may be carried out in parallel with development. The principal inputs to TOE evaluation are

the set of TOE evidences, which includes the evaluated ST as the basis for TOE evaluation.

the TOE for which the evaluation is required.

the evaluation criteria, methodology and scheme.

In addition, the IT security expertise of the evaluator and the evaluation community are likely to be used as inputs to the evaluation. The expected result of the evaluation process is a confirmation that the TOE satisfies its security requirements as stated in the ST with one or more reports documenting the evaluator findings about the TOE .

In order to maintain consistency of the evaluation findings, the final evaluation results could be submitted to a certification process. The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval. The certificate is normally publicly available.

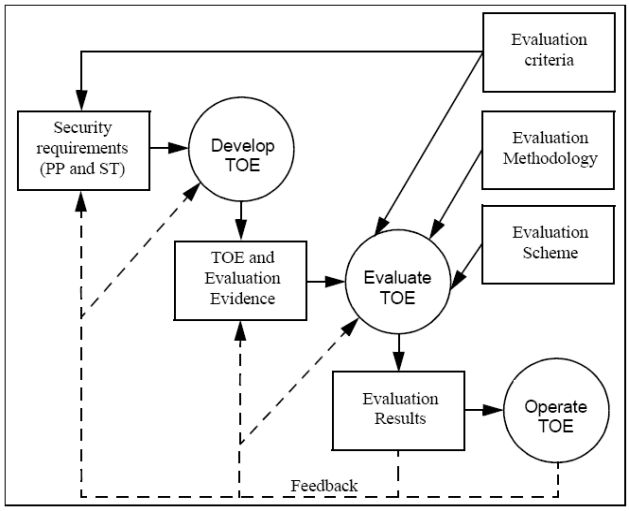

Fig. 3 Evaluation process.

These reports will be useful to actual and potential consumers of the product or system as well as to the developer. The degree of confidence gained through an evaluation depends on the assurance requirements (e.g. Evaluation Assurance Level) met.

D. FIPS (Federal Information Processing Standard 140-2).

The NIST (National Institute of Standards and Technology) has issued the 140 publication series to coordinate the requirements and standards for cryptographic

modules It include both hardware and software components that encrypts and decrypts data or performs other cryptographic operations. FIPS 140-2 is the ISO/IEC 19790 standard for security requirements for cryptographic modules.Additional FIPS standards govern cryptographic algorithms.

FIPS 140 imposes requirements in 11 different areas:

Cryptographic module specification (what must be documented) .

Cryptographic module parts and interfaces. (What information flows in and out, and how it must be segregated).

Roles, services and authentication. (who can do what with the module and how this is checked).

Finite state model (documentation of the high-level states the module can be in, and how transitions occur) .

Physical security (tamper evidence and resistance, and robustness against extreme environmental conditions).

Operational environment (what sort of operating system the module uses and is used by).

Cryptographic key management (generation, entry, output, storage and destruction of keys).

EMI/EMC(electromagnetic interference/electromagnetic compatibility).

Self-tests (what must be tested and when, and what must be done if a test fails) .

Design assurance (what documentation must be provided to demonstrate that the module has been well designed and implemented).

Mitigation of other attacks (if a module is designed to mitigate against, say, TEMPEST attacks then its documentation must say how).

FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

Level 1 the lowest, imposes very limited requirements; loosely, all components must be "production-grade" and various egregious kinds of insecurity must be absent.

Level 2 adds requirements for physical tamper-evidence and role-based authentication.

Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication , and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.

Level 4 makes the physical security requirements more stringent, and requires robustness against environmental attacks.

E. BS-7799 (British Standard for information security management).

Organizations must treat information security as an ongoing process requiring a set of well-managed best practices. Best practices are a set of documents compiled for use as a guideline during the implementation of different information security aspects. Best practices are the combined experiences of several companies that have already had a great influence in the information security environment. The main aim of best practices in information security is to focus on the management of information security in an organization.

BS7799 is an information security standard developed to provide a model for setting up and managing an effective Information Security Management System (ISMS). The BS7799 Standard is based on a process approach to information security and adopts the “Plan-Do-Check-Act” model.

ISO/IEC 17799:2000 defines 127 security controls structured under 10 major headings to enable readers to identify the particular safeguards that are appropriate to their particular business or specific area of responsibility. These security controls contain further detailed controls and elements of best practice.

The 10 headings are listed below :

1. *Security Policy* To provide management direction and support for information security.
2. *Security Organization* To manage information security within the organization.
3. *Asset Control and Classification* To maintain appropriate protection of organizational assets.
4. *Personnel Security* To reduce the risks of human error, theft, fraud or misuse of facilities.
5. *Physical & Environmental Security* To prevent unauthorized access, damage and interference to business premises and information.
6. *Communications & Operations Management* To ensure the correct and secure operation of information processing facilities.
7. *Access Control* To control access to information.
8. *Systems Development & Maintenance* To ensure that security is built into information systems.
9. *Business Continuity Management* To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.
10. *Compliance* To avoid breaches of any criminal and civil law, statutory, regulatory or contractual.

Using a systematic management approach to information security, such as ISO 17799, a company is able to adopt best practice controls, quantify the level of acceptable risk and implement the mitigating measures which protect the confidentiality, integrity and availability of information. The standard is recognized globally and provides an excellent stage for introducing effective protection measures.

F. ANALYSIS OF THE CC, FIPS-140 , BS-7799.

1) Necessity of the standard.

Common Criteria is an ISO/IEC 15408 standard. It can be used to select the appropriate IT security measures and it

contains criteria for evaluation of security properties of IT products and systems.

FIPS 140-2 is the ISO/IEC 19790 standard for security requirements for cryptographic modules.

BS7799 is a standard specification for an Information Security Management Systems (ISMS).Current version of BS-7799 is ISO 27002.

2) Applicability.

CC evaluations are performed on computer security products and systems.

FIPS 140-2 only applies to the cryptographic modules of the products. It is limited to module level.

BS 7799 is one of the leading international best practices that can be implemented in an organization for the prevention of security risks.

3) Certification support.

The Standards Council of Canada (SCC), NIST, National Voluntary Laboratory Accreditation Program (NVLAP) United Kingdom Accreditation Service (UKAS) accredits Common Criteria Evaluation Facilities.

The testing and validation of products against the FIPS 140-1 criteria is performed by NIST and CSE-approved and accredited certification laboratories.

There are a growing number of organizations accredited to grant certification against ISO27001. The following are amongst them: BSI, Certification Europe, DNV, JACO IS, KEMA, KPMG , SGS, STQC etc.

4) Certification Result.

The CC provides a collection of Evaluation Assurance Levels (EAL) ranging from EAL1 (lowest) through EAL7 (highest) to be awarded to products and systems upon successful completion of evaluation.

Products are validated against FIPS 140-2 at security levels, ranging from level 1 (lowest) through level 4 (highest).

Bs-7799 provides a certificate. It is a report with the positive finding and non-compliant areas.

5) Documentation Support.

CC presents requirements for functional and assurance aspects. CC defines three types of requirement constructs PP, ST, package. The package permit the expressions of a set of functional or assurance requirements that meet an identifiable subset of security objectives.

FIPS imposes requirements in different areas as cryptographic module specification , cryptographic module parts and interfaces, roles, physical security etc.

ISO 27000 provides Toolkit for documentation support. BSI has published a useful set of supporting documentation to help apply ISO/IEC 17799:2000 and BS7799-2:1999.

F. Assurance of accepted levels

In CC, Assurance level depends on requirement of the application.

In FIPS-140, Assurance level depends on requirement of the application.

In BS-7799, acceptable level depends upon size and requirements of the organization. All the controls are not applicable everywhere.

IV. CONCLUSION

Insights of the Security evaluation practices are yet not common to all IT professionals. We have attempted to bring various evaluation standards and procedures forward to the IT professionals. We have reviewed various approaches for information security standards and practices. Today, Security is not limited to only government and military institutions. With the ever increasing reliance on mass data storage in database servers, secure networking, more powerful operating systems and newer products and technologies to support modern business processes, the need for verification of products and systems has increased tremendously. No longer the purchasers of IT products and IT systems can rely on the word of vendor. Most of the organizations are demanding well known international standards but still all the IT professionals are not familiar with the insights of these standards/practices.

In the context of Security evaluation CC provides assurance based upon an evaluation of an IT product or system that is to be trusted. FIPS 140 helps to coordinate the requirements and standards for cryptographic modules. An ISMS framework, BS-7799 helps co-ordinate and maintain assurance in the community. An ISMS framework in development brings effectiveness to CC and FIPS-2 deployment by supporting effective and efficient provision of a correct environment .

V. REFERENCES

Technical Reports:

[1] The Common Criteria Sponsoring Organizations. "Common Criteria for Information Technology Security Evaluation Version 2.2" 2004.

[2] The Common Criteria Sponsoring Organizations,. "Common Criteria for Information Technology Security Evaluation Version 2.4" 2004.

[3] Federal Criteria for Information Technology Security, Draft Version 1.0, (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.

[4] The BS7799, ISO 27001 and ISO 17799 awareness site. available from www.induction.to/bs7799

[5] ISO 27001, ISO 27002 & ISO17799 User Group BS7799-2, the original specification for an information security from www.17799.com/

Papers from Conference Proceedings (Published):

[6] Brewer, David. "ISO/IEC 17799 Information Security Management Application to Smart Cards." Paper presented at the Smart Card Security Conference, Tokyo 2001.

Journals:

[7] ISMS Journal Issue 5, Nov 2004.

VI. BIOGRAPHIES

Pradnya S Gotmare is pursuing M.E. in Computer science at Ramrao Adik Institute of Technology (RAIT)***, Nerul, Navi Mumbai.*** She has received B.E. degree in computer science and Engineering from Govt. college of En***gineering, Amravati University.*** Her area of interests includes information security, web technology and web mining.

Dr. Satish R Devane received his PhD degree in Smartcard Security for E-commerce applications from IIT Bombay, India. He is currently working as a professor and Head, Department of Computer Engineering at Ramrao Adik Institute of Technology (RAIT), Nerul, Navi Mumbai. His main research interests are Network Security , E-commerce payment systems and Smartcard security.