INTERNATIONAL STANDARD

ISO/IEC 21827

First edition
2002-10-01

Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)

Technologies de l'information — Ingénierie de sécurité système — Modèle de maturité de capacité (SSE-CMM®)

Reference number
ISO/IEC 21827:2002(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Background 5
4.1 Reason for Development 5
4.2 The Importance of Security Engineering 6
4.3 Consensus 6

5 Structure of the Document 7

6 Model Architecture 7
6.1 Security Engineering 7
6.2 Security Engineering Process Overview 9
6.3 SSE-CMM® Architecture Description 12
6.4 Summary Chart 20

7. Security Base Practices 20
7.1 PA01 - Administer Security Controls 21
7.2 PA02 - Assess Impact 24
7.3 PA03 - Assess Security Risk 28
7.4 PA04 - Assess Threat 31
7.5 PA05 - Assess Vulnerability 34
7.6 PA06 - Build Assurance Argument 37
7.7 PA07 - Coordinate Security 40
7.8 PA08 - Monitor Security Posture 42
7.9 PA09 - Provide Security Input 47
7.10 PA10 - Specify Security Needs 50
7.11 PA11 - Verify and Validate Security 54

Annex A(normative)Generic Practices 57
A.1 General 57
A.2 Capability Level 1 - Performed Informally 57
A.3 Capability Level 2 - Planned and Tracked 58
A.4 Capability Level 3 - Well Defined 63
A.5 Capability Level 4 - Quantitatively Controlled 68
A.6 Capability Level 5 - Continuously Improving 70

Annex B(normative)Project and Organizational Base Practices 73
B.1 General 73
B.2 General Security Considerations 73
B.3 PA12 - Ensure Quality 73
B.4 PA13 - Manage Configurations 78
B.5 PA14 - Manage Project Risks 81
B.6 PA15 - Monitor and Control Technical Effort 85
B.7 PA16 - Plan Technical Effort 88
B.8 PA17 - Define Organization's Systems Engineering Process 93
B.9 PA18 - Improve Organization's Systems Engineering Processes 96
B.10 PA19 - Manage Product Line Evolution 99
B.11 PA20 - Manage Systems Engineering Support Environment 101
B.12 PA21 - Provide Ongoing Skills and Knowledge 105
B.13 PA22 - Coordinate with Suppliers 110

Annex C(informative)Capability Maturity Model Concepts 114
C.1 General 114
C.2 Process Improvement 114
C.3 Expected Results 115
C.4 Common Misunderstandings 115
C.5 Key Concepts 116

Bibliography 120

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an Internationa Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 21827 was prepared by the International Systems Security Engineering Association (ISSEA) (formerly the Systems Security Engineering Capability Maturity Model®[1] Project) and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Annexes A and B form a normative part of this International Standard. Annex C is for information only.

1) ®CMM and Capability Maturity Model are Service Marks of Carnegie Mellon University

Not-for-profit corporation

5000 Forbes Avenue, Pittsburgh, PA 15213

Introduction

A wide variety of organizations practice security engineering in the development of computer programs, whether as operating systems software, security managing and enforcing functions, software, middleware of applications programs. Appropriate methods and practices are therefore required by product developers, service providers, system integrators, system administrators, and even security specialists. Some of these organizations deal with high-level issues (e.g., ones dealing with operational use or system architecture), others focus on low-level issues (e.g., mechanism selection or design), and some do both. Organizations may specialize in a particular type of technology, or a specialized context (e.g. at sea).

The SSE-CMM® is designed for all these organizations. Use of the SSE-CMM should not imply that one focus is better than another is or that any of these uses are required. An organization's business focus need not be biassed by use of the SSE-CMM®.

Based on the focus of the organization, some, but not all, of the security engineering practices defined will apply. In addition, the organization may need to look at relationships between different practices within the model to determine their applicability. The examples below illustrate ways in which the SSE-CMM® may be applied to software, systems, facilities development and operation by a variety of different organizations.

Security Service Providers

To measure the process capability of an organization that performs risk assessments, several groups of practices come into play. During system development or integration, one would need to assess the organization with regard to its ability to determine and analyze security vulnerabilities and assess the operational impacts. In the operational case, one would need to assess the organization with regard to its ability to monitor the security posture of the system, identify and analyze security vulnerabilities, and assess the operational impacts.

Countermeasure Developers

In the case of a group that focuses on the development of countermeasures, the process capability of an organization would be characterized by a combination of SSE-CMM® practices. The model contains practices to address determining and analyzing security vulnerabilities, assessing operational impacts, and providing input and guidance to other groups involved (such as a software group). The group that provides the service of developing countermeasures needs to understand the relationships between these practices.

Product Developers

The SSE-CMM® includes practices that focus on gaining an understanding of the customer's security needs. Interaction with the customer is required to ascertain them. In the case of a product, the customer is generic as the product is developed a priori independent of a specific customer. When this is the case, the product marketing group or another group can be used as the hypothetical customer, if one is required.

Practitioners in security engineering recognize that the product contexts and the methods used to accomplish product development are as varied as the products themselves. However, there are some issues related to product and project context that are known to have an impact on the way products are conceived, produced, delivered, and maintained. The following issues in particular have significance for the SSE-CMM®:

- Type of customer base (products, systems, or services);
- Assurance requirements (high vs. low);
- Support for both development and operational organizations.

The differences between two diverse customer bases, differing degrees of assurance requirements, and the impacts of each of these differences in the SSE-CMM® are discussed below. These are provided as an example of how an organization or industry segment might determine appropriate use of the SSE-CMM® in their environment.

Specific Industry Segments

Every industry reflects its own particular culture, terminology, and communication style. By minimizing the role dependencies and organization structure implications, it is anticipated that the SSE-CMM® concepts can be easily translated by all industry segments into their own language and culture.

How Should the SSE-CMM® Be Used?

The SSE-CMM® and the method for applying the model (i.e., appraisal method) are intended to be used as a:
- Tool for engineering organizations to evaluate their security engineering practices and define improvements;
- Method by which security engineering evaluation organizations such as certifiers and evaluators can establish confidence in the organizational capability as one input to system or product security assurance;
- Standard mechanism for customers to evaluate a provider's security engineering capability.

The appraisal techniques can be used in applying the model for self improvement and in selecting suppliers, if the users of the model and appraisal methods thoroughly understand the proper application of the model and its inherent limitations. Additional information on using process assessment can be found in ISO/IEC CD 15504-4 Software Engineering — Process Assessment — Part 4: Guidance on use for Process Improvement and Process Capability Determination.

Benefits of Using the SSE-CMM®

The trend for security is a shift from protecting classified government data to a broader spectrum of concerns including financial transactions, contractual agreements, personal information, and the Internet. A corresponding proliferation of products, systems, and services that maintain and protect information has emerged. These security products and systems typically come to market in one of two ways: through lengthy and expensive evaluation or without evaluation. In the former case, trusted products often reach the market long after their features are needed and secure systems are being deployed that no longer address current threats. In the latter, acquirers and users must rely solely on the security claims of the product or system developer or operator. Further, security engineering services traditionally were often marketed on this caveat emptor basis.

This situation calls for organizations to practice security engineering in a more mature manner. Specifically, the following qualities are needed in the production and operation of secure systems and trusted products:
- Continuity - knowledge acquired in previous efforts is used in future efforts;
- Repeatability - a way to ensure that projects can repeat a successful effort;
- Efficiency - a way to help both developers and evaluators work more efficiently;
- Assurance - confidence that security needs are being addressed.

To provide for these requirements, a mechanism is needed to guide organizations in understanding and improving their security engineering practices. To address these needs, the SSE-CMM® is being developed to advance the state of the practice of security engineering with the goal of improving the quality and availability of and reducing the cost of delivering secure systems, trusted products, and security engineering services. In particular, the following benefits are envisioned:

To Engineering Organizations:

Engineering organizations include System Integrators, Application Developers, Product Vendors, and Service Providers. Benefits of the SSE-CMM® to these organizations include:
- Savings with less rework from repeatable, predictable processes and practices;
- Credit for true capability to perform, particularly in source selections;
- Focus on measured organizational competency (maturity) and improvements.

To Acquiring Organizations:

Acquirers include organizations acquiring systems, products, and services from external/internal sources and end users. Benefits of the SSE-CMM® to these organizations include:
- Reusable standard Request for Proposal language and evaluation means;
- Reduced risks (performance, cost, schedule) of choosing an unqualified bidder;
- Fewer protests due to uniform assessments based on industry standard;
- Predictable, repeatable level of confidence in product or service.

To Evaluation Organizations:

Evaluation organizations include System Certifies, System Accreditors, Product Evaluators, and Product Assessors. Benefits of the SSE-CMM® to these organizations include:

- Reusable process appraisal results, independent of system or product changes;
- Confidence in security engineering and its integration with other disciplines;
- Capability-based confidence in evidence, reducing security evaluation workload.

Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)

1 Scope

The SSE-CMM® is a process reference model. It is focussed upon the requirements for implementing security in a system or series of related systems that are the ITS domain. Within the ITS domain the SSE-CMM® Model is focussed on the processes used to achieve ITS, most specifically on the maturity of those processes. There is no intent within the SSE-CMM® Model to dictate a specific process to be used by an organization, let alone a specific methodology. Rather the intent is that the organization making use of the SSE-CMM® Model should use its existing processes, be those processes based upon any other ITS guidance document. The scope encompasses:

- the system security engineering activities for a secure product or a trusted system addressing the complete lifecycle of: concept definition, requirements analysis, design, development, integration, installation, operation, maintenance end de-commissioning;
- requirements for product developers, secure systems developers and integrators, organizations that provide computer security services and computer security engineering;
- applies to all types and sizes of security engineering organizations from commercial to government and the academe.

While the SSE-CMM® is a distinct model to improve and assess security engineering capability, this should not imply that security engineering should be practised in isolation from other engineering disciplines. On the contrary, the SSE-CMM® promotes such integration, taking the view that security is pervasive across all engineering disciplines (e.g., systems, software and hardware) and defining components of the model to address such concerns. The Common Feature "Coordinate Security Practices" recognizes the need to integrate security with all disciplines and groups involved on a project or within an organization. Similarly, the Process Area "Coordinate Security" defines the objectives and mechanisms to be used in coordinating the security engineering activities.

This International Standard has a relationship to TR 15504, particularly part 2, as both are concerned with process improvement and capability maturity assessment. However, TR 15504 is specifically focussed on software processes, whereas the SSE-CMM is focussed on security.

This International Standard has a closer relationship with the new versions of 15504, particularly CD 15504-2, and is compatible with its approaches and requirements.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 12207, *Information technology — Software life cycle processes*

ISO/IEC TR 13335-1, *Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security*

ISO/IEC 15288, *Systems engineering — System life cycle processes*

ISO/IEC TR 15504-2, *Information technology — Software process assessment — Part 2: A reference model for processes and process capability*

ISO/IEC TR 15504-4, *Information technology — Software process assessment — Part 4: Guide to performing assessments*

ISO/IEC 17799: 2000, *Information technology — Code of practice for information security management*

3 Terms and definitions

For the purposes of this International Standard, the following terms and definitions apply.

3.1 Accountability
The property that ensures that the actions of an entity can be traced uniquely to the entity. [ISO 7498-2:1988]

3.2 Accreditation
In the context of this document: formal declaration by a designated approving authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards.

Note: This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks. [ISO/IEC Guide 2].

3.3 Assessment
Verification of a product, system, or service against a standard using the corresponding assessment method to establish compliance and determine the assurance. [ISO/IEC 15443-1].

3.4 Asset
Anything that has value to the organization [ISO 13335-1:1996].

3.5 Assurance
In the context of this document: Grounds for confidence that a deliverable meets its security objectives. [ISO/IEC 15408–1] .

Note: This definition is generally accepted within the security community; within ISO the more generally used definition is: Activity resulting in a statement giving confidence that a product, process or service fulfills specified requirements. [ISO/IEC Guide 2]

3.6 Assurance Argument
A set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied.

3.7 Assurance Claim
An assertion or supporting assertion that a system meets a security need. Claims address both direct threats (e.g., system data are protected from attacks by outsiders) and indirect threats (e.g., system code has minimal flaws).

3.8 Assurance Evidence
Data on which a judgment or conclusion about an assurance claim may be based. The evidence may consist of observation, test results, analysis results and appraisals.

3.9 Authenticity
The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information. [ISO 13335-1:1996].

3.10 Availability
The property of being accessible and useable upon demand by an authorized entity. [ISO 7498-2: 1988].

3.11 Baseline
A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. [IEEE-STD-610].

3.12 Certification
In the context of this document, the process producing written results of performing a comprehensive evaluation of security features and other safeguards of a system to establish the extent to which the design and implementation meet a set of specified security requirements.

Note: This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements. [ISO/IEC Guide 2]

3.13 Confidentiality
The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO 7498-2:1988].

3.14 Consistency
The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component. [IEEE-STD-610].

3.15 Correctness
For specified security requirements, the representation of a product or system that shows the implementation of the requirement is correct.

3.16 Customer
Recipient of a product provided by the supplier.

NOTE 1: In a contractual situation, the customer is called the purchaser.
NOTE 2: The customer may be, for example, the ultimate consumer, user, beneficiary or purchaser.
NOTE 3: The customer can be either external or internal to the organization. [ISO 8402] [ISO/IEC TR 15504]

3.17 Effectiveness
A property of a system or product representing how well it provides security in the context of its proposed or actual operational use.

3.18 Engineering Group
A collection of individuals (both managers and technical staff) which is responsible for project or organizational activities related to a particular engineering discipline (e.g. hardware, software, software configuration management, software quality assurance, systems, system test, system security).

3.19 Evidence
Directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfies a specified requirement.

3.20 Integrity
Integrity is defined as safeguarding the accuracy and completeness of information and processing methods.

3.21 Maintenance
The process of modifying a system or component after delivery to correct flaws, improve performance or other attributes, or adapt to a changed environment. [IEEE-STD-610].

3.22 Methodology
A collection of standards, procedures and supporting methods that define the complete approach to the development of a product or system.

3.23 Penetration Profile
A definition of the activities required to effect a penetration.

3.24 Procedure
A written description of a course of action to be taken to perform a given task. [IEEE-STD-610].

3.25 Process
A set of interrelated activities, which transform inputs into outputs. [ISO/IEC 15288].

3.26 Reliability
The property of consistent behaviour and results. [ISO 13335-1:1996].

3.27 Residual Risk
The risk that remains after safeguards have been implemented [ISO 13335-1:1996].

3.28 Risk
The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets [ISO 13335-1:1996].

3.29 Risk Analysis
The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. [ISO 13335-1:1996].

3.30 Risk Management
Process of assessing and quantifying risk and establishing acceptable level of risk for the organization. [ISO 13335-1:1996].

3.31 Security Policy
Within the context of this document; rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems, particularly those which impact the systems and associated elements.

3.32 Security Related Requirements
Requirements which have a direct effect on the secure operation of a system or enforce conformance to a specified security policy.

3.33 System
A discrete, distinguishable entity with a physical existence and a defined purpose, completely composed of integrated, interacting components, each of which does not individually comply with the required overall purpose. [ISO/IEC 15288].

Note 1: In practice, a system is 'in the eye of the beholder' and the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. product system, aircraft system. Alternatively the word system may be substituted simply by a context dependent synonym, e.g. product, aircraft, though this may then obscure a system principles perspective.
Note 2: The system may need other systems during its life cycle to meet its requirements. Example - an operational system may need a system for conceptualization, development, production, operation, support or disposal.

3.34 Threat
Capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or a program or system or cause those to harm others.

3.35 Threat Agent
The originator and/or the initiator of deliberate or accidental man-made threats.

3.36 Validation
Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. [ISO/IEC 15288].

3.37 Verification
Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled. [ISO/IEC CD 15288].

3.38 Vulnerability
Includes a weakness of an asset or group of assets which can be exploited by a threat [ISO 13335-1:1996].

3.39 Work Product
An artefact associated with the execution of a process. [ISO/IEC TR 15504-9].

Note: A work product might be used, produced or changed by a process.

4 Background

The Systems Security Engineering Capability Maturity Model® (SSE-CMM®) describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The SSE-CMM® does not prescribe a particular process or sequence, but captures practices generally observed in industry. The model is a standard metric for security engineering practices covering:

- The entire life cycle, including development, operation, maintenance, and decommissioning activities;
- The whole organization, including management, organizational, and engineering activities;
- Concurrent interactions with other disciplines, such as system, software, hardware, human factors, and test engineering; system management, operation, and maintenance;
- Interactions with other organizations, including acquisition, system management, certification, accreditation, and evaluation.

The SSE-CMM® Model Description provides an overall description of the principles and architecture upon which the SSE-CMM® is based, an executive overview of the model, suggestions for appropriate use of the model, the practices included in the model, and a description of the attributes of the model. It also includes the requirements used to develop the model. The SSE-CMM® Appraisal Method describes the process and tools for evaluating an organization's security engineering capability against the SSE-CMM®.

4.1 Reason for Development

Both customers and suppliers are interested in improving the development of security products, systems, and services. The field of security engineering has several generally accepted principles, but it currently lacks a comprehensive framework for evaluating security engineering practices. The SSE-CMM®, by identifying such a framework, provides a way to measure and improve performance in the application of security engineering principles.

It must be stressed that security engineering is a unique discipline, requiring unique knowledge, skills, and processes which warrants the development of a distinct CMM® for security engineering. This does not conflict with the premise that security engineering is done in context with systems engineering. In fact, having well-defined and accepted systems engineering activities will allow security engineering to be practised effectively in all contexts.

Modern statistical process control suggests that higher quality products can be produced more cost-effectively by emphasizing the quality of the processes that produce them, and the maturity of the organizational practices inherent in those processes. More efficient processes are warranted, given the increasing cost and time required for the development of secure systems and trusted products. The operation and maintenance of secure systems relies on the processes that link the people and technologies. These interdependencies can be managed more cost effectively by emphasizing the quality of the processes being used, and the maturity of the organizational practices inherent in the processes.

The objective of the SSE-CMM® Project is to advance security engineering as a defined, mature, and measurable discipline. The SSE-CMM® model and appraisal methods are being developed to enable:

- Focussed investments in security engineering tools, training, process definition, management practices, and improvements by engineering groups;
- Capability-based assurance, that is, trustworthiness based on confidence in the maturity of an engineering group's security practices and processes;
- Selection of appropriately qualified providers of security engineering through differentiating bidders by capability levels and associated programmatic risks.

4.2 The Importance of Security Engineering

With the increasing reliance of society on information, the protection of that information is becoming increasingly important. Many products, systems, and services are needed to maintain and protect information. The focus of security engineering has expanded from one primarily concerned with safeguarding classified government data to broader applications including financial transactions, contractual agreements, personal information, and the Internet. These trends have elevated the importance of security engineering.

4.3 Consensus

The SSE-CMM® Model was developed by over 50 organization, many of them multi-national corporations. The Project had representatives from several Nations, notably Australia, Canada, Europe and the US. In addition, the SSE-CMM® project continually sought participation through various venues, including presentations and booths at conferences and through the public website www.sse-cmm.org.

The participants were organized into a Steering Group, and a number of Working Groups. The majority of the development was performed by the Working Groups, while the Steering Group was responsible for overall project progress and approval of Project deliverables.

The SSE-CMM® model was developed by a consensus process. All member organizations could send representatives to the working group meetings, and the majority did. Contributions were sent electronically to all members of the working group in the intervening period between meetings. Meetings were held on a monthly basis where input suggestions were discussed, revised and agreed. The results of any votes that were necessary were recorded in the working group meeting minutes issued for each meeting. These records have been maintained.

Each version of the SSE-CMM® Model was first approved by the working group tasked with development. It was then reviewed and approved by the Steering Group. After the Steering Group had approved the version it was then sent to a group of “Key reviewers” drawn from the ITS community at large for their review and comment. Each version was then released for public review and feedback. Based on the feedback from the Key reviewers and the community at large, the Steering Group made a determination of the final release of that version of the SSE-CMM® Model.

The SSE-CMM® Model has been approved first at the working group level; second at the Steering Group level, third at the Key Reviewer level, and finally at the community level. Thus, in essence, four levels of approval have been obtained.

Additional approval and consensus has been achieved during the Pilot Appraisals through the impact of application of the Model to different application domains. The Alternative Assurance Working Group (AAWG) of the Common Criteria Project has reviewed the SSE-CMM® Model for applicability as an alternative to the generation of assurance by evaluation and provided IT systems security community consensus feedback to the project.

Each major release of the Model was reviewed by a set of independent reviewers who had not been involved in its development. Their comments were consolidated, reviewed and incorporated in the Model. Finally, each version of the document was subjected to public review, the CDR and the two public workshops, and the comments received, addressed.

5 Structure of the Document

Clause 4 discusses some of the background of the document and the reasons for it development. Clause 6 addresses the architecture of the SSE-CMM Model and the role of systems security engineering. Clause 7 describes the systems security engineering process areas and base practices in detail. Annex A describes the capability maturity levels and generic practices, while Annex B describes the project and organization process areas and base practices. Annex C discusses the concepts of capability maturity models. ISO/IEC TR 15504-4 can also be applied to the use of the SSE-CMM®.

6 Model Architecture

The SSE-CMM® is a compilation of the best-known security engineering practices. To understand this model, some background in security engineering is required. This section provides a high level description of security engineering, and then describes how the architecture of the model reflects this basic understanding.

6.1 Security Engineering

6.1.1 What Is Security Engineering?

The drive toward pervasive interconnectivity and interoperability of networks, computers, applications, and even enterprises is creating a more pivotal role for security in all systems and products. The focus of security has moved from safeguarding classified government data, to a wider application, including financial transactions, contractual agreements, personal information, and the Internet. As a result, it is necessary that potential security needs are considered and determined for any application. Examples of needs to consider include confidentiality, integrity, availability, accountability, privacy, and assurance.

The shift in focus of security issues elevates the importance of security engineering. Security engineering is becoming an increasingly critical discipline and should be a key component in multi-disciplinary, concurrent, engineering teams. This applies to the development, integration, operation, administration, maintenance, and evolution of systems and applications as well as to the development, delivery, and evolution of products. Security concerns must be addressed in the definition, management, and re-engineering of enterprises and business processes. Security engineering can then be delivered in a system, in a product, or as a service.

6.1.2 Description of Security Engineering

Security engineering is an evolving discipline. As such, a precise definition with community consensus does not exist today. However, some generalizations are possible. Some goals of security engineering are to:

- Gain understanding of the security risks associated with an enterprise;
- Establish a balanced set of security needs in accordance with identified risks;
- Transform security needs into security guidance to be integrated into the activities of other disciplines employed on a project and into descriptions of a system configuration or operation;
- Establish confidence or assurance in the correctness and effectiveness of security mechanisms;
- Determine that operational impacts due to residual security vulnerabilities in a system or its operation are tolerable (acceptable risks);
- Integrate the efforts of all engineering disciplines and specialties into a combined understanding of the trustworthiness of a system.

6.1.3 Security Engineering Organizations

Security engineering activities are practised by various types of organizations, such as:

- Developers;
- Product vendors;