PP と ST 情報を再利用可能にするセキュリティ仕様モデルの提案

ラミレス　カセレス　ギジェルモ　オラシオ　　　勅使河原 可海

創価大学大学院工学研究科
〒192-8755 東京都八王子市丹木町 1-236
ramirez_caceres@soka.gr.jp　teshiga@soka.ac.jp

あらまし　本稿では、国際標準および評価されたセキュリティターゲット(ST)情報に基づいた脅威モデルを提案する．評価標準（CC）に基づいてSTを評価し認証を得るためには，開発者はこのモデルを利用して、評価対象(TOE）のセキュリティ要件及び仕様書(仕様のセット：ST）を作成することができる．CCでは一つのプロファイル(PP)にいくつかのPPを追加することができるように、他のPPに適合することができる．さらに、評価するためのSTに評価されたPPを含めることができる．しかし、毎年評価STsの数は急激に増加しており、ウェブ上で関連するSTs およびPPsを検索するのは、非常に面倒でうまく行かない場合も多い．そのために、提案するモデルでは、今までCCに基づいて評価されたPPおよびSTを機能別や認証国別に参照できるようにする．さらに、このモデルを使用して、適合宣言プロセスで開発者を支援することも可能になる．

A Proposal of a Security Specification Model

to Support Reuse of PP and ST Information

Ramirez Caceres Guillermo Horacio　　　TeshigawaraYoshimi

Graduate School of Engineering, Soka University
1-236 Tangi-cho, Hachioji, Tokyo, 192-8577, JAPAN
ramirez_caceres@soka.gr.jp　teshiga@soka.ac.jp

Abstract In this paper, we propose a threat model based on multiple international standards and evaluated Security Target (ST) information, to be used for security specifications for production of a ST, to be evaluated by CC. The CC allows Protection Profile (PP) to conform to other PP, allowing chains of PP to be constructed, each based on the previous one. In addition, an evaluated PP can be included in a new ST for evaluation. However, the rapid increase in the number of evaluated STs every year makes the search for relevant STs and PPs on the Web very tedious and often fruitless. We propose threats specification and definition which allow ST developers to referring evaluated PP and ST information classified by product types and countries. In addition, by using this model, it is possible to help developers in the Conformance Claims process.

1 Introduction

ISO/IEC 15408, known as Common Criteria (CC) for Information Technology Security Evaluation, is an international standard that has been used as the basis for the evaluation of the security properties of IT products [1]. As shown in Figure 1, the number of IT products evaluated according to CC is growing rapidly.

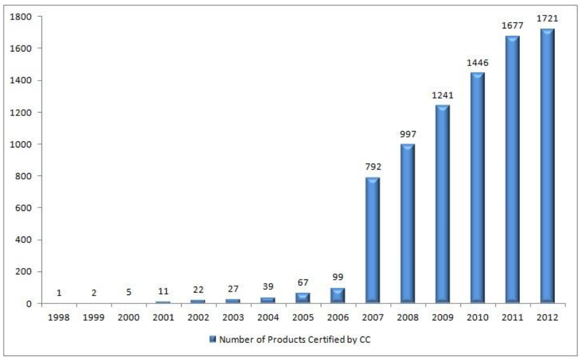


Figure 1 Number of Products Certified by CC

In order to evaluate an IT product or system based on CC, developers must create a Security Target (ST). However, a problem encountered in creating an ST is the determination of the Security Problem Definitions (SPDs), because the SPDs fall outside of the scope of CC. ISO/IEC 15408 nor provide a framework for risk analysis or the specification of threats. Usually, ST developers must refer to ISO/IEC 27005 for more detailed information [2].

In this paper, we propose a threat model based on multiple international standards and evaluated ST information, to be used for security specifications in the production of STs which are to be evaluated by ISO/IEC 15408. In addition, this model allows ST developers to referring evaluated Protection Profile (PP) and ST information.

This paper is organized as follows. In chapter 2, we briefly review the international standards used in this research. In chapter 3 and 4, we describe the issues motivating this research and the objectives to achieve. In chapter 5, 6 and 7, we describe our approach. In chapter 8 we briefly describe a Web application that has been developed using our model. Finally, in chapter 9, we present our conclusions and discuss future works.

2 Research Background

In this chapter we present a brief review of CC. As described above, CC is an international standard used as the basis for evaluating the security properties of IT products. CC Part 3 describes seven security requirements, called Evaluation Assurance Levels (EALs).

A Security Target, as defined in ISO/IEC 15408 Part 1, is a set of IT security objectives and requirements of a specifically identified Target of Evaluation (TOE) that defines the functional and assurance requirements.

Based on CC version 3, each ST consists of seven chapters as shown in Figure 2.

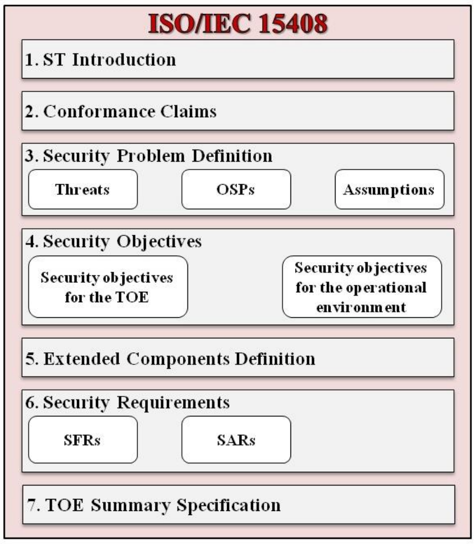

ISO/IEC 15408
1. ST Introduction
2. Conformance Claims
3. Security Problem Definition
Threats
OSPs
Assumptions
4. Security Objectives
Security objectives for the TOE
Security objectives for the operational environment
5. Extended Components Definition
6. Security Requirements
SFRs
SARs
7. TOE Summary Specification

Figure 2 ST Contents

2.1 ST Introduction

In this section, the ST developers must describe the TOE in a narrative way. An ST must provide clear and sufficient information, such as version, authors, and publication date to uniquely identify that particular ST. An ST also must contain a TOE reference. This information is consists of developer name, TOE name, and TOE version number. The ST reference and TOE reference can be used for the purposes of registration and inclusion in list of PP and ST evaluated.

2.2 Conformance Claims

In this section of the ST, the ST developers must describe how the TOE conforms with:

- The Common Criteria(CC)
- Protection Profiles (Optional)
- Packages (Optional)

The CC conformance describes which version of the CC the TOE is conformed with. This section also includes the conformance with SFR and SAR components. Figure 3 shows how a ST implement evaluated PPs or Security requirements.

The PP conformance claims must be included if the ST is referring to one or more PPs. CC allows two types of conformance: strict, and demonstrable. An intermediate combination of components is termed as a package.

The package permits the expression of a set of functional or assurance requirements that meet an identifiable subset of security objectives. A package is intended to be reusable and to define requirements that are known to be useful and effective in meeting the identified objectives.

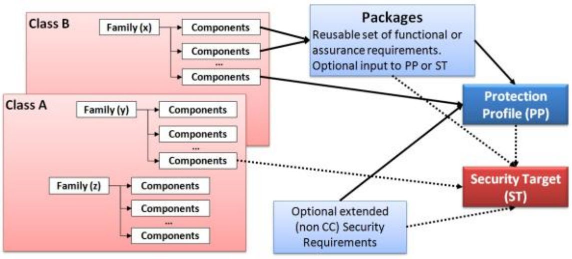


Figure 3 ST and Security Requirements Relationship

2.3 Security Problem Definition

In this section, the ST developer must describe the security problems to be addressed by the TOE, the operational environment of the TOE, and the development environment of the TOE. The security problem definition must have Threats (T), Organisational security policies (OPS), and Assumptions (A). However, it is not mandatory to have statements in all section.

2.4 Security Objectives

This section must provide a concise and abstract statement that intends to respond to the security problem definition. The security objective must be written in common language.

The evaluation of security objectives must demonstrate that each part meets the security problem defined in the previous section. In this section, ST developers can search inside the knowledge-based tools to know how previous evaluated STs resolve this problem.

2.5 Extended Components Definition

This section is optional. In this section ST developers must include all security requirements that are not based or included in ISO/IEC 15408 Part 2 or Part 3.

2.6 Security Requirements

The security requirements must be a well-defined translation of the security objectives.

There are two kinds of security requirements, Security Functional Requirements (SFR) and Security Assurance Requirements (SAR).

SFR provide information about what is to be evaluated, and SAR provides information about how the TOE is to be evaluated. Each security objectives described earlier must be met by a set of SFR and SAR which are drawn from Part 2 and Part 3 of the ISO/IEC 15408. These requirements are relevant to supporting the security objectives.

2.7 TOE Summary Specification

The objective of this section is to provide to potential consumers of the TOE with descriptions about how the TOE satisfies the security functional requirements.

3 Research Issues

One of the problems in creating an ST is to determine the SPDs, because they fall outside of the scope of CC. ISO/IEC 15408 do not provide a framework for risk analysis or the specification of threats. The ST developer must, therefore, refer to other standards. In addition, according to CC, the subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. However, the TOE may employ cryptographic functionality to help to satisfy several high-level security objectives. In this case, ST developers must be able to refer to external standards, such as particular cryptographic standards or protocols.

Another problem is in the area of knowledge required in creating an ST. There is a large amount of information to digest. The CC allows Protection Profile (PP) to conform to other PP, allowing chains of PP to be constructed, each based on the previous one. In addition, an evaluated PP can be included in a new ST for evaluation.

4 Research Objectives

This research was motivated by a desire to help ST developers to indentify and specify the threats that affect the TOE and its environment.

Following a previous study [3], this paper proposes a threat model based on international standards to be used for security specification of security evaluation by CC and ISO/IEC 19791 [4]. The objective is to support developers to describe the SPDs.

We propose threats specification and definition which allow ST developers to refer evaluated PP and ST information classified by product types and countries. In addition, by using this model, it is possible to help developers in the Conformance Claims process.

5 Security Problem Definition

To implement the risk assessment, it is necessary to determinate the assets that need protection. In this research we implement the asset classification of ISO/IEC 27002 [5].

The description of each risk needs to be sufficiently detailed to identify the assets that can be damaged or compromised, the threats and vulnerabilities applicable to each asset and the impact of a successful attack.

In the former model [3] threats are classified in terms of WHO, HOW and WHAT. As shown in Figure 4, this new model also includes WHY, WHEN and WHERE to simplify the study of the large-scale environment and to help developers to describe SPDs for security evaluation by ISO/IEC 15408. It also includes asset value modeling and risk management based on ISO/IEC 27005.

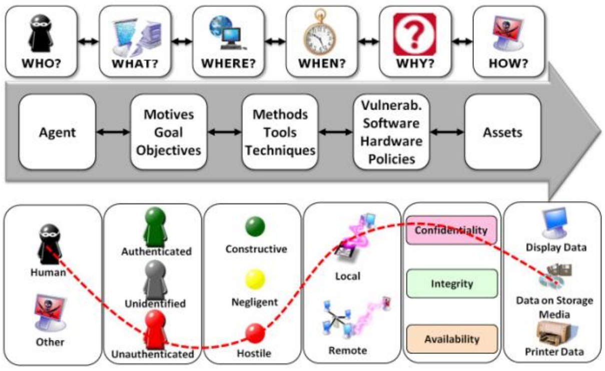


Figure 4 Threat Classification

To create this new model, we have been working with 170 SPD for STs evaluated by CC. We classified the threats included in evaluated STs, according to this new threat model.

To identify and specify an SPD, it is necessary to know the following:

- Who is the person posing a threat? (WHO)
- How is the attack implemented? (HOW)
- What is the object exposed to the threat? (WHAT)
- Where is the attacker located? (WHERE)
- When does the attack take place? (WHEN)
- Why did the attack happened? (WHY)

5.1 WHO

Based on ISO/IEC 15446 [6] we can classify threat agents which have the potential to access resources and to cause harm in terms of agent types, such as a person, a place, or a thing that.

Threat agents can be classified by two parameters: the type of agent and the agent's level of authentication.

5.2 WHAT

ISO/IEC 15408 defines an asset as information or a resource that may be protected by the security policy. In this research, to define WHAT we classified the results of attacks in terms of loss types: availability, confidentiality, and integrity. In addition, it is necessary to specify the assets that we must to protect, because the attack may affect IT capabilities, as in a system or a user process.

5.3 WHERE

To specify this parameter, it is necessary to know the location of the threat agent attacking the system. In addition, it is necessary to explain whether the attack affects the system directly or affects the system environment.

5.4 WHEN

To specify this parameter is necessary to know when the attack took place. For example, the time and the day need to known.

According ISO/IEC 19791 security evaluation, the security controls of an operational system must be assessed throughout the lifetime of the system. Therefore, it is also necessary to classify the attack according to the lifecycle phase.

5.5 WHY

This classification is used to evaluate the attitude of some agents. We can, for example, identify the motivation of the agent attacking the system as malicious or non-malicious. Malicious attacks usually come from external people or disgruntled current or ex-employees who have specific goals or objectives to achieve.

5.6 HOW

The methods of attack can be divided into general categories that are related to each other, since the use of a method in a category allows the use of other methods in other categories.

For example, after cracking one password, an intruder can log in like a legitimate user to view the archives and exploit vulnerabilities of the system.

6 Security Requirements

The Security requirements define the security functional requirements regarding the TOE, the security assurance requirements, and any security requirements regarding software, firmware and/or hardware in the TOE IT environment. The IT security requirements need to be defined using, where applicable, functional and assurance components from ISO/IEC 15408 Part 2 and Part 3.

6.1 Security Functional Requirements

ISO/IEC 15408 Part 2 establishes a set of security functional components as a standard way of expressing the security functional requirements for TOEs. Security functional requirements are grouped into classes. Classes are the most general grouping of security requirements, and all members of a class share a common focus.

The members of a Class are called “Families”. They are a set of security requirements that share security objectives. Finally, the members of Families are called “Components”. These describe a specific set of security requirements and are the smallest selectable sets of security requirements for inclusion in the ST for evaluation.

Eleven functionality classes are contained within Part 2 of the CC. These are as follows.

- Security Audit (FAU)
- Communication (FCO)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Privacy (FPR)
- Protection of the TSF (FPT)
- Resource Utilization (FRU)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

6.2 Security Assurance Requirements

ISO/IEC 15408 Part 3 establishes a set of assurance components to be used as standard templates to meet security assurance requirements (SARs) for TOEs. These eight classes are summarized below.

- Protection Profile evaluation (APE)
- Security Target evaluation (ASE)
- Development (ADV)
- Guidance documents (AGD)
- Life-cycle support (ALC)
- Tests (ATE)
- Vulnerability assessment (AVA)
- Composition (ACO)

The security assurance requirements are catalogued and organized in Class and Families. In addition, this part also defines the evaluation criteria for protection profile (PP) and ST. Figure 5 show the security assurance requirement structure and the relation with EAL package. There are seven predefined assurance packages, usually called Evaluation Assurance Levels (EALs).

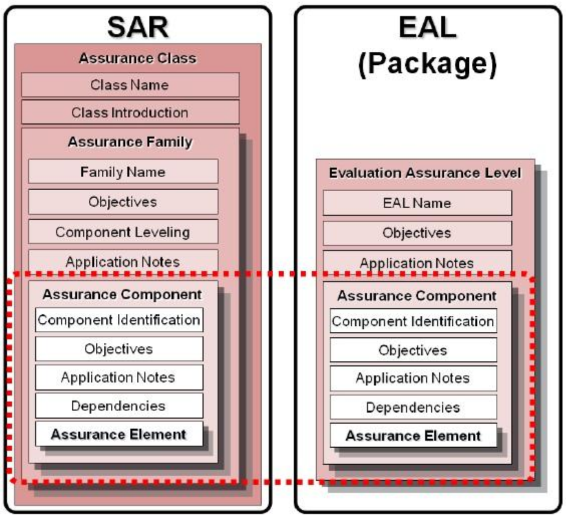


Figure 5 SAR and EALs relationship

7 Conformance Claims

As explained above, a Security Target is a set of IT security objectives and requirements of a specifically identified TOE that defines the functional and assurance requirements. And the PP intend to describe functional and assurance requirement for a type of TOE.

In other words, an ST describes requirements for a specific TOE, and is written by the developer of the TOE. A PP describes requirements for a type of TOE and will be written by a use community, a developer, or a government.

As mentioned above, the CC allows two types of conformance: strict, and demonstrable. However, the PP states what the allowed types of conformance for the ST are. In other words, an ST is only allowed to conform in a PP in a demonstrable manner, if the PP explicitly allows this.

7.1 Strict Conformance

For PP that specified strict conformances, then the following requirement are apply.

The SPD section of the ST shall contain the SPD of the PP, and occasionally, may include additional threats and OSPs, but not additional assumptions.

The security objective section of the ST shall include all security objectives for the TOE and operational environment of the PP. In addition, is possible to specify additional security objective for the TOE of the ST, but not security objective for the operational environment of the TOE.

The Security requirement section of the ST shall contain all SFRs and SARs in the PP, but may claim additional or hierarchically stronger SFRs and SARs.

7.2 Demonstrable Conformance

In the case of demonstrable conformance for PP the following requirements apply.

The ST shall contain a rationale on why the ST is considered to be equivalent or more restrictive than the PP.

Demonstrable conformance allows a PP to describe a common security problem to be solved and provide generic guidelines to the requirements necessary for its resolution.

8 Knowledge base Application

This section introduces our knowledge base application. This application was developed in ASP 2.0.

Using on the threat classification described in Section 5, the authors have been working to create an application to be used as a knowledge base for the identification and specification of the threats that affect an TOE under evaluation.

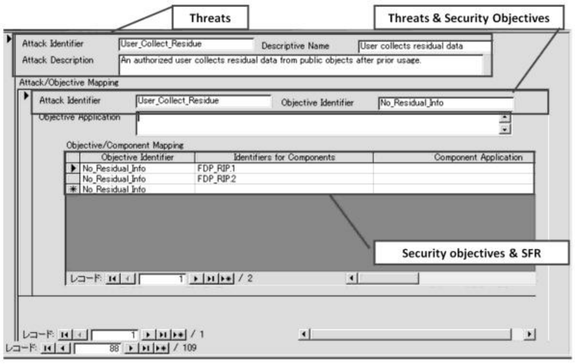
The knowledge-base application was created to support ST developers. This tool provides access to information about threats that affect an TOE. Developers can search and select the appropriate threat from the knowledge base. ST developers are also able to select WHO poses a threat, HOW the attack is implemented, WHAT object is exposed to the threat, WHERE the attacker is located, WHEN the attack takes place, and WHY the attack occurs.

Our knowledge base also includes a list of security policies based on international standards, including ISO/IEC 15408. After having defined the security objectives in response to the identified threats, it is necessary to elaborate on how these security objectives should be met. This is accomplished by selecting an appropriate set of Systems Functional Requirements (SFRs) and SARs.

8.1 Rationale

This section provides the rationale for the selection of the IT security requirements, objectives, assumption, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

As shown in Figure 6 the rationale demonstrates that the PP specifies a complete and cohesive set of IT security requirements, and that a conformant TOE will effectively address the defined security needs.



Attack Identifier: User_Collect_Residue
Descriptive Name: User collects residual data
Attack Description: An authorized user collects residual data from public objects after prior usage.

Attack/Objective Mapping

Attack Identifier: User_Collect_Residue
Objective Identifier: No_Residual_Info
Objective Application:

Objective/Component Mapping

Objective Identifier	Identifiers for Components	Component Application
No_Residual_Info	FDP_RIP.1	
No_Residual_Info	FDP_RIP.2	
No_Residual_Info		

レコード: 1 / 2

レコード: 1 / 1

レコード: 88 / 109

Figure 6 SAR and EALs relationship

In addition, as shown in Figure 7, there are many relationships between security controls described in CC. However, in this research, most of the information on CC and other standards are graphically displayed on the system. Furthermore, references in the same standards or other standards are graphically represented, to help users to read and understand these relationships effectively.

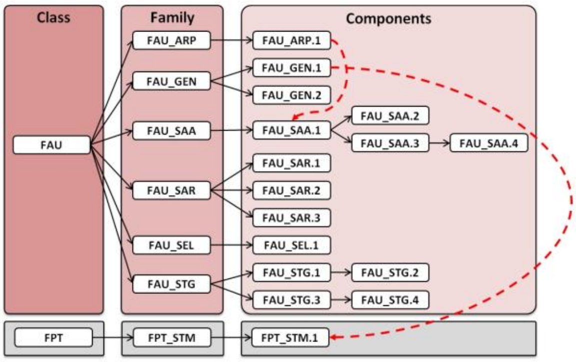


Figure 7 SFR relationship

9 Conclusion and Future Work

We have proposed a threat model based on international standards to be used as a knowledge base for the identification and specification of threats that affect TOEs. In addition, this model includes a risk methodology based on ISO/IEC 27005.

On the basis of this model, we have developed an application which an ST developer can use to access to the necessary information on security controls. Furthermore, references within standards or to other standards are graphically represented, to help the user to read and understand these relationships effectively.

We propose threats specification and definition which allow ST developers to refer evaluated PP and ST information classified by product types and countries. In addition, by using this model, it is possible to help developers in the Conformance Claims process.

We are working to create a model that combines security controls and security tests from different international standards, to reduce the time and cost of the security evaluation process.

Reference

[1] ISO/IEC 15408:2009, Common Criteria for Information Technology Security Evaluation. Part 1~3.

[2] ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management.

[3] Ramirez Guillermo and Yoshimi Teshigawara, “A Study of Threat Modeling Based on International Standards for Production of Security Targets” DICOMO 2005, pp.189-192. July, 2005

[4] ISO/IEC TR 19791:2005, Information technology - Security techniques - Security assessment of operational systems.

[5] ISO/IEC 27002:2005, Information technology - Security techniques - Information security management systems - Requirements

[6] ISO/IEC TR 15446:2004, Information technology - Security techniques - Guide for the production of protection profiles and security targets.