

A Study on Security Policy Making Adaptable to Users' Environments Based on International Standards

Guillermo Horacio RAMIREZ CACERES
Yoshimi TESIGAWARA

Graduate School of Engineering, Soka University
1-236 Tangi-cho, Hachioji, Tokyo 192-8577, Japan
E-mail: {guillerm,teshiga}@soka.ac.jp

Abstract. The security information can be understood like the capability of the information system to resist all the accidents or deliberate actions, with Evaluation Assurance Levels (EAL)[1] as defined in international standards ISO/IEC 15408. These put in danger of the availability, integrity, and confidentiality of stored or transmitted data and the corresponding services that these networks and systems offer or make accessible. In this paper, we propose a security policy making flexibly adaptable to users' environments to defend them against the information system environment threats. This proposed model allows a user to select the appropriate policy agile and effectively according to the user's environment. This threats-policy relationship is based on ISO/IEC TR 15446. At the same time, this model allows the user to select the appropriate systems or products evaluated by Common Criteria (CC) or ISO/IEC 15408.

1 Introduction

The security information can be understood like the capability of the information system to resist, with Evaluation Assurance Levels (EAL) as defined in international standards ISO/IEC 15408, all the accidents or deliberate actions. These put in danger of the availability, integrity and, confidentiality of stored or transmitted data and the corresponding services that these networks and systems offer or make accessible. In this paper, we propose a security policy making flexibly adaptable to users' environments to defend them against the information system environment threats.

2 Research Background

We have been working to create a set of security policies for systems of home users based on ISO/IEC 15408[2]. As shown in Fig.1, we construct a knowledge base to be used for an audit system based on a Protection Profile (PP) for systems of home users. This knowledge base works on Web base. This allows home users

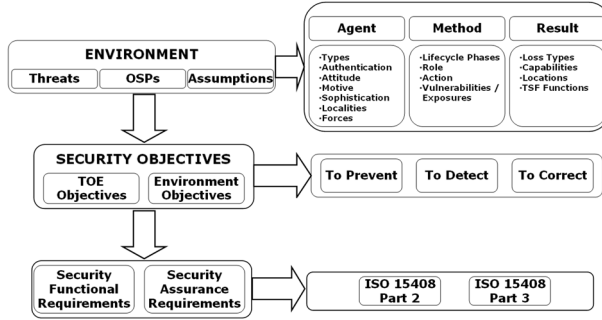


Fig. 1. Knowledge Base

to access to information of the threats that affect the home user environment. The home user can search about some threats and also can know about his or her appropriate security policy. Moreover, this system shows how to implement these policies with IT components enunciated in the ISO/IEC 15408[1].

2.1 Protection Profile for systems of home users

In order to describe a protection profile for system of home users, we made a survey for home user security by asking questionnaires to 100 home users in Japan and Argentina, respectively, in May 2003. The Protection Profile for systems of home users was constructed to be use like a reference for any home users, to create a safe IT environment at home. Operating systems evaluated against this PP can operate in EAL 4. This level permits a developer to maximize assurance gained from positive security engineering based on good commercial development practices. Although these practices are rigorous, they do not require substantial specialist knowledge, skills or other resources. EAL4 is the highest level at which it is likely to be economically feasible for home users to retrofit to existing product lines. It is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodities, and there is willingness to incur some additional specific engineering costs.

The security environment for the functions addressed by this specification includes threats, organizational security policies, and usage assumptions. For EAL 4, the Target of Evaluation (TOE) for system of home users includes 30 threats, 10 organizational security policies and 36 assumptions. Each of the identified threats to security is addressed by one or more security objectives. These objectives are suitable to counter all identified threats and cover all identified organizational security policies and assumptions. For EAL 4, the TOE for system of home users includes about 150 security objectives. Each of the identified security objective implies a set of threats, assumptions and security policy to be met. And, each of the security objectives is met by a set of security requirements. Functional requirements in this PP were drawn from Part 2 of the ISO/IEC

15408. These requirements are relevant to supporting the secure operation of the TOE.

3 Purpose of Research and Expected Effects

A security policy will be defined as clear instruction that provides the guidelines to users' behaviors for safeguarding information, and it is a fundamental building block in developing effective control to counter potential security threats.

In this paper, we propose security policy making flexibly adaptable to users' environments so they can defend themselves against the information system environment threats. The users' environments may change but these security policies are flexible and change according to the new environment. In addition we propose a new security level according to the users' environments.

4 Fundamental Research Target

Our fundamental research target is the construction of security policy based on PP structure. The policy making architecture is shown in Fig 2, each of the identified threats to security is addressed by one or more security objectives. These objectives are suitable to counter all identified threats and cover all identified organizational security policies and assumptions. Each of the identified security objective implies a set of threats, assumptions and security policies to be met.

In addition, each of the security objectives is met by a set of Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) which are drawn from part 2 and part 3 of the ISO/IEC 15408[1]. These requirements are relevant to supporting the security objective.

Dependencies may exist between components. Dependencies arise when a component is not self sufficient and relies upon the presence of another component. Dependencies may exist between functional components, between assurance components, between functional and assurance components, and more complicated dependencies may also exist.

4.1 Users' Environments

The users' environments are defined by assumption, threats and organizational security policy (OSPs).

– Assumptions

To identify and specify the assumptions we must respond the next question: What assumptions am I making about the IT security environment and the scope of the security needs?

For example: *Users of the system are assumed to possess the necessary privileges to access the information.*

For easy interpretation the assumptions are displayed in 6 category like Administrator, User, Assumed Protection, Procedural Security, Physical Security, and Communications.

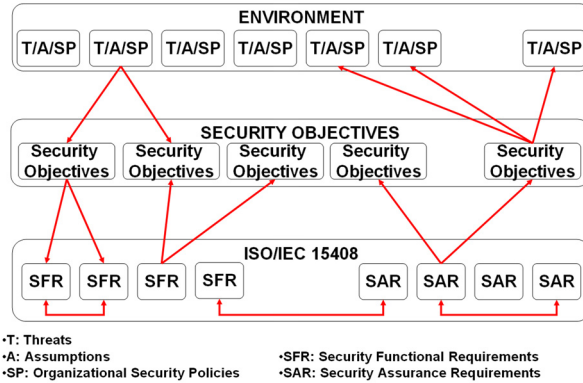


Fig. 2. Policy Making Architecture

– **Threats**

Next, to identify and specify the threats is necessary to know “WHO” is the threat agent, “HOW” the agent or malicious attackers can gain access or deny services, and finally “WHAT” kinds of security issues could occur.

For example: *An attacker or an authorized user may gain unauthorized access to information or resources by impersonating an authorized user.*

How should threats be specified?

WHO: An attacker or an authorized user

HOW: Impersonation of an authorized user

WHAT: Confidential or sensitive data

The threats are also displayed in categories like Administrator, Authorized User, Physical Environment, System, Hardware, Software, and Malicious User.

– **Organizational Security Policies**

Sometimes it is necessary to restate the threat in a different form; in this case we use the OPS. These OSP could be used like a pre-security objective.

For example: *If we have a threats like “An unauthorized person may gain logical access to the system.” the OSP would be “Users must be identified before accessing the system”.*

4.2 Security Objectives

The security objectives provide a concise statement of the intended response to the environment threats. Usually the security objective can not be satisfied only by technical countermeasures. For example, an administrator creates a great password, but the user may not be able to remember and may write the password in a memo. In this case, it is necessary to re-educate the user about the security issues.

Table 1. Example of Security Objectives

Preventive Ensure that each user is uniquely identified, and authenticated, before the user is granted to access to the system.
Detective Generate evidence which can be used as proof of the origin of that information.
Corrective Detection of events that are indicative of an imminent security violation, take appropriate steps to curtail the attack.

In some cases, security objectives would be identified or sub-classified in three categories.

- Preventative objectives, to prevent a threat from being carried.
- Detective objectives, to detect and monitor the occurrence of events relevant to the secure operation.
- Corrective objectives, to take actions in response to potential security violations.

Table 1 shows the possible security objectives to protect the system against the threats “*An unauthorized person may gain logical access to the system.*”

4.3 Security Requirements

The IT Security Requirements define the security functional requirements on the TOE, the security assurance requirements, and any security requirements on software, firmware and/or hardware in the IT environment for the TOE. The IT security requirements are to be defined using, where applicable, functional and assurance components from ISO/IEC 15408.

In addition, each of the security objectives is met by a set of SFRs and SARs. There are 135 SFR components and 93 SAR components. As described before, dependences may exist between components. Each security requirement component is assigned to a unique reference in ISO/IEC 15408, based on a defined taxonomy. Using this Knowledge Base can help users to understand security requirements.

Table 2 shows possible requirements for *user’s identification and authentication* security policy.

5 Conclusion and Future Work

This proposed model allows the user to select the appropriate policy agile and effectively according to the user’s environment, because the user works only for

Table 2. SFRs Example

Identification and authentication		
Security Requirement		Component
Login	Identification of user	FIA_UID.1-2
	Authentication of users	FIA_UAU.1-2
Controls	Limits on repeated login failures	FIA_AFL.1
	Trusted path for login	FTP_TRP.1-2
	Time of day restriction of access to TOE	FTA_TSE.1

a minimal set of security policies. In addition, all security policies in this model are created for respective environment threats.

All security policies created by this architecture are supported by SFRs and SARs. This threats-policy relationship is based on ISO/IEC TR 15446[3]. At the same time, this model allows the user to know the necessary SFRs for his or her environment and to select the appropriate systems or products evaluated by Common Criteria (CC) or ISO/IEC 15408.

The present research was destined to home user or small networks. In the future we want to implement this policy making architecture in a large scale networks like universities, hospitals or small/medium size companies.

In order to create this new system, it is necessary to work on threats modeling to simplify the study of the new large-scale environment. We are working on a new threat architecture to create an interactive application to select the policy according to change of environments. This threats model architecture is based on ISO/IEC 15446 and ISO/IEC TR 13335[4]. Safeguarding assets of interest is responsibility of owners or user who place value on those assets. The value of these assets can vary according to the company or the network environments. We want to include an asset value modeling and risk management.

Finally, we are working on a new security policy model based on ISO/IEC 15408. On the other hand, we are also working on a new security policy making model based on ISO/IEC 17799[5]. The purpose of this research is to fuse ISO/IEC 15408 with ISO/IEC 17799 to create more effective security policies.

References

1. ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation Part 1-3. Version 2.1 CCIMB-99-031, August 1999
2. Ramirez Guillermo and Yoshimi Teshigawara, "A proposal of a security audit system for home users based on international standards." IPSJ SIG Technical Reports 2003-CSEC-22, pp. 265-272, July 2003
3. ISO/IEC TR 15446. Information technology - Security techniques - Guide for the production of protection profiles and security targets, 1999
4. ISO/IEC TR 13335-1-5, Information technology - Guidelines for the management of IT Security
5. ISO/IEC 17799. Information technology - Code of practice for information security management, 2000