Study on a Threat-Countermeasure Model Based on International Standard Information

Guillermo Horacio RAMIREZ CACERES and Yoshimi TESHIGAWARA
Graduate School of Engineering, Soka University
Tokyo, Japan
{guillerm,teshiga}@soka.ac.jp

ABSTRACT

Many international standards exist in the field of IT security. This research is based on the ISO/IEC 15408, 15446, 19791, 13335 and 17799 standards. In this paper, we propose a knowledge base comprising a threat countermeasure model based on international standards for identifying and specifying threats which affect IT environments. In addition, the proposed knowledge base system aims at fusing similar security control policies and objectives in order to create effective security guidelines for specific IT environments. As a result, a knowledge base of security objectives was developed on the basis of the relationships inside the standards as well as the relationships between different standards. In addition, a web application was developed which displays details about the most common threats to information systems, and for each threat presents a set of related security control policies from different international standards, including ISO/IEC 27002.

Keywords: Knowledge-base, Web Application, International Standards, Threat Model, Security Control.

1. INTRODUCTION

At present, owing to the advance of broadband mobile communications and the Internet, many home users enjoy the services brought by the IT revolution. Nevertheless, regarding security policies, only a limited number of people are aware of the dangers of information eavesdropping and privacy invasion. The path to true security for any system goes beyond the installation of the most recent OS updates, the configuration of certain files, or the careful administration of the access of users to system resources; it consists of recognizing different threats which can potentially affect the system and the security policies which have been arranged to avoid them.

Many international standards exist in the field of IT security. This research is based on the ISO/IEC 15408, 15446, 19791, 13335 and 27002 standards [1]~[5], and proposes a threat countermeasure model as a knowledge base for identifying and specifying the threats which affect IT environments. This study presents a system which demonstrates in detail the most common threats with respect to information systems, creates a knowledge base for identifying those threats, and is capable of selecting an appropriate security policy in accordance with the IT environment on the basis of international standards, including ISO/IEC 27002. In this research, the authors propose a security guideline tool based on such knowledge base.

This paper is organized as follows. In Section 2, we briefly review the background of the present research. Furthermore, we explain the purpose and the expected outcome of the research in Section 3, and the main objectives in Section 4. In Sections 5 and 6, we explain the threat model and the security control knowledge base respectively. Finally, we present the web application in Section 7, and conclude the paper and present the future line of work in Section 8.

2. RESEARCH BACKGROUND

Security information can be regarded as the ability of an information system which uses the Evaluation Assurance Levels (EAL) as defined in the ISO/IEC 15408 international standard to avoid all accidents or deliberate malicious actions. In other words, those are accidents and actions which can potentially endanger the availability, the integrity and/or the confidentiality of stored or transmitted data or of the corresponding services offered or made accessible by any related networks and systems.

ISO/IEC 27001, also known as the Information Security Management System (ISMS), is an international standard intended as a guideline for initiating, implementing, maintaining, and improving the information security management in organizations [6].

These standards are used by a broad range of organizations in most commercial and industrial market sectors: finance and insurance, telecommunications, utilities, retail and manufacturing sectors, various service industries, transportation sector, governments, etc. Furthermore, ISO/IEC 27002 provides guidance with respect to the implementation of security control policies. However, the risk analysis and risk assessment necessary for describing the environment where the security control policies are outside the scope of ISMS.

Different methodologies for risk assessment exist, some of which are discussed in ISO/IEC 13335. Therefore, the implementation of a secure system generally consumes large amounts of time and resources, and requires sufficient knowledge.

Security Concepts

As shown in Fig. 1, security concerns the protection of assets from threats, where threats are categorized in accordance with their potential to abuse the protected assets. Although all categories of threats should be considered, in the domain of security greater attention is given to threats which are related to human activities, regardless of whether or not they are malicious.

Safeguarding the assets of interest is a responsibility of users who places value on those assets. Threat agents could also regard the same assets as valuable, and could consequently attempt to abuse the assets in a manner contrary to the interests of the users. In this regard, the users perceive such threats as potential attempts to impair and subsequently reduce the value of the assets. More specifically, such impairment commonly includes loss of confidentiality, integrity, or availability.

The users of the assets need to analyze the possible threats in order to determine which apply to their environment. The results are commonly known as risks, and such analysis can aid the selection of the appropriate countermeasures needed to reduce the relevant risks to acceptable levels. The countermeasures are implemented for the purpose of reducing vulnerabilities and meeting security policy requirements.

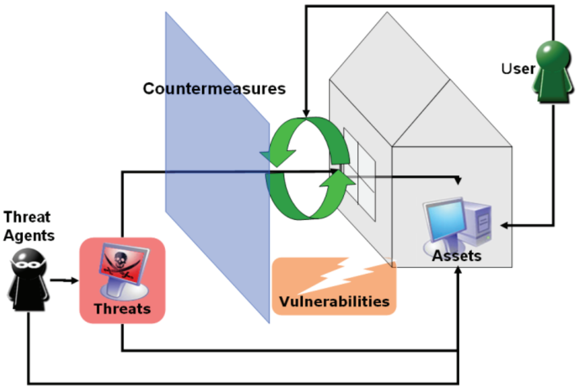
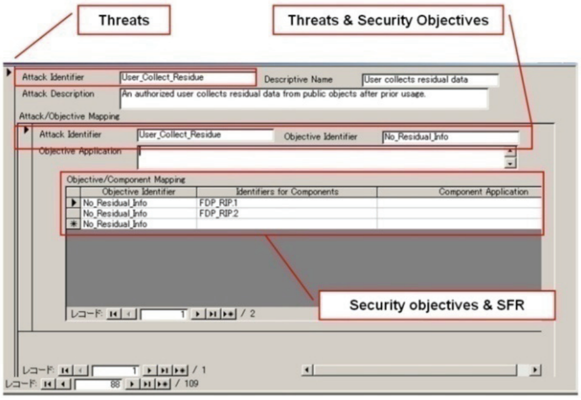


Fig. 1 Security concepts

Security Guideline for Home Users

We are working on creating a security guideline tool for home users based on ISO/IEC 15408. This application allows home users to access information about threats which affect home user environments and thereby select the security objectives based on this environment [7].

This previous model included 76 environment threats and 150 security objectives as countermeasures against all identified threats for home user environments [8]. As shown in Fig. 2, all security policies created by this architecture are supported by the Security Functional Requirements (SFRs) and the Security Assurances Requirements (SARs). This threat-policy relationship is based on ISO/IEC TR 15446.



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

Fig. 2 Threats, security policies, and SFR

3. RESEARCH OBJECTIVE

The issues described in Section 2 motivated us to develop this knowledge-based tool to help users to implement a security system. This research includes a simple application which can be easily understood by common users when evaluating potential threats to their system environment. The cost of the implementation of the corresponding security policy varies depending on the system environment.

The main objective of this research is to create a knowledge base for identifying and specifying the threats which can affect the IT environment. In addition, our proposed knowledge base system aims at fusing similar security controls or objectives to create effective security guidelines for specific IT environments. This security objective knowledge base is developed using the relationships inside the standards as well as the relationships between different standards.

These security guidelines allow users to access information about threats which affect IT environments. Users can search for threats and select the security objectives based on the relevant environment. The security objectives provide a concise statement regarding the intended response to the security problems.

4. MAIN RESEARCH TARGET

Our main research target is the construction of a knowledge base system for security policies for building secure and trustable IT environments based on multiple international standards. The threat countermeasure architecture is introduced in Fig. 3. Our proposed method has been divided into two steps. The first step identifies and specifies the threats which affect the IT environment. Each of the identified threats is addressed by at least one objective. The second step specifies the countermeasures, also called security objectives, which are suitable for implementation with regards to the identified threats.

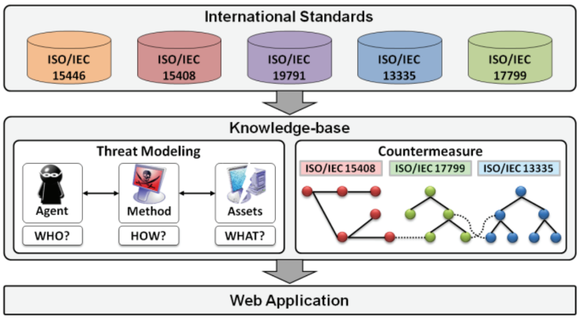


Fig. 3 The proposed knowledge-based model

5. THREAT MODEL

There are many types of attack models, including fraud, extortion, and robbery of information, revenge or simply the challenge to penetrate systems. These can be implemented by internal employees who abuse their access permissions, or by external attackers who break into the system remotely or intercept network traffic.

The majority of successful attacks on operating systems are linked to only a few pieces of vulnerable software. This can be attributed to the fact that attackers are opportunistic, taking the easiest and most convenient route, and exploiting the best-known flaws with the most effective and widely available attack tools. They often attack indiscriminately, scanning the Internet for vulnerable systems.

Based on the security concept described above, we developed a threat identification model based on multiple international standards. As shown in Fig. 4, our developed threat model is based on multiple international standards. In order to identify and specify a threat, it is necessary to know:

- Who is the person issuing the threat? (WHO)
- How is the attack implemented? (HOW)
- What are the objects exposed to the threat?(WHAT)

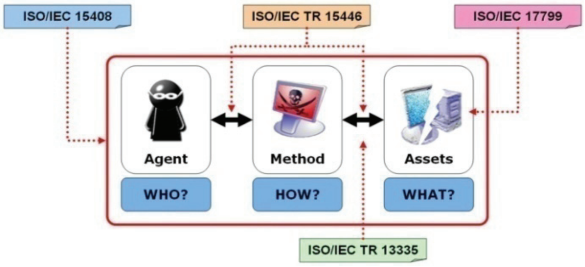


Fig. 4 Threat Model and ISO Relationship

The relationship among WHO, HOW, and WHAT are based on ISO/IEC 15446. The asset classification was based on the ISO/IEC 17799. Finally, the risk evaluation was based on ISO/IEC 13335.

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

WHO

Usually, attacks involve little technical sophistication. Insiders might use their permissions to alter archives or registries, and outsiders can acquire passwords in networks with simple validation.

Over time, more and more sophisticated forms of attacks have been developed to exploit "holes" in the design, the configuration, and the operation of systems. This allows new attackers to take exclusive control of the attacked systems, inflicting true disasters which can destroy organizations or companies with highest degree of technological dependency. Furthermore, these new attack methods have been automated, and this is why in many cases only basic technical skills are needed in order to implement them. Intruder apprentices now have access to numerous programs and scripts on "hacker" bulletin boards and websites, where there are additional instructions for executing attacks with the available tools.

As shown in Fig. 5, based on the ISO/IEC 15446 standard, we can classify “WHO” as the threat agents in terms of agent types, such as persons, places, or objects which have the potential to access resources and cause harm. In this research, the first parameter has 2 values, "human" and "other".

Next, human threats can subsequently be broken down according to the authentication level, such as system administrator or unauthorized user. Therefore, the second parameter categorizes the agent as "authenticated", "unauthenticated" or "unidentified".

Subsequently, the third parameter is related to the intentions of the agent, where the access to the system is categorized as "malicious" and "non-malicious". Malicious attacks are usually issued from external people or disgruntled current or former employees who have specific goals or objectives.

The last parameter is related to the identification of the location of the threat agent attacking the system.

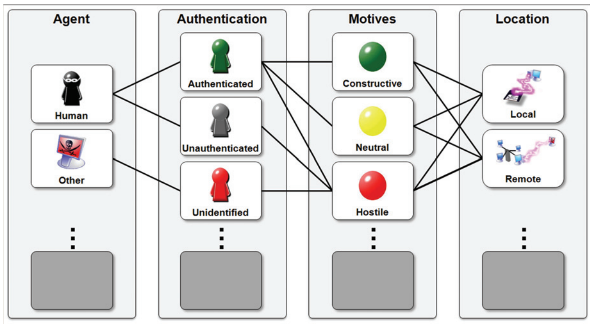


Fig. 5 WHO classification

HOW

The attack methods ("HOW") are divided into general categories which can be related to each other, since the use of one method from a given category allows the use of other methods from other categories. For example, after cracking one password, an intruder can log in as a legitimate user, which enables them to access archives and exploit other vulnerabilities of the system. The attacker can also acquire rights to places which allow virus or other logic bombs to be released, paralyzing the entire system.

Some of the frequently used techniques for attacking information systems are outlined below.

- Eavesdropping and packet sniffing
- Snooping and downloading
- Tampering and alteration of data
- Spoofing
- Jamming or flooding
- Trojan insertion
- Social engineering
- Virus infection
- Obtaining passwords, codes and keys

This chapter is to clarify that when we use the Internet, numerous threats exist and we must be conscientious about it, to be able to protect us. The methods used in terms of lifecycle phases, human roles, actions performed, and vulnerabilities and exposures exploited. An asset may be accessed through a threat that leverages vulnerability in home user's environment.

WHAT

ISO/IEC 15408 defines an "asset" as information or a resource which is subject to protection with security policies. In this research, as shown in Fig. 6, we use 3 parameters to define "WHAT" is the asset exposed to the threat.

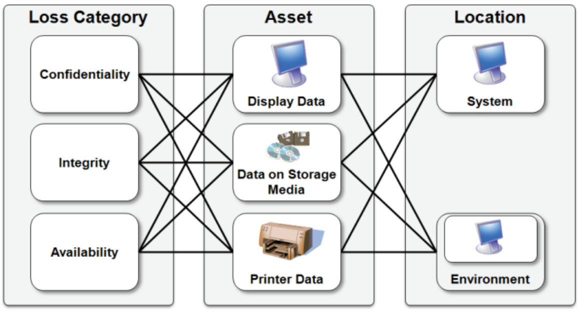


Fig. 6 WHAT Classification

The first parameter regards the results of the attacks in terms of loss types: availability, confidentiality, and integrity.

The second parameter represents the assets, for example, hard disks or other storage media, or displayed or printed data, which must be protected from attacks affecting different aspects of IT capabilities, such as system or user processing.

The third parameter is to explain if the attack affects directly the system or the system environment.

6. COUNTERMEASURES

Based on the threat information described in the previous section, users can recognize the threats which can affect specific environments. The next step is then to select countermeasures or security objectives to counter the risk of possible attacks. The security objectives provide a concise statement of the intended response to environment threats. Usually, security objectives cannot be realized only with technical countermeasures or functional requirements as described in ISO/IEC 15408. For example, even if an administrator creates a strong password, the user might write it down in a memo in case they forget it. In this case, it is necessary to re-educate the user about the security issues.

At present, there are too many security objectives in different international standards. In this regard, we have developed a knowledge base for security objectives which includes the following standards.

- ISO/IEC 15408
- ISO/IEC 17799
- ISO/IEC 13335 part 4 and 5

Security Objectives in ISO/IEC 15408

ISO/IEC 15408, also known as the Common Criteria (CC) for Information Technology Security Evaluation, is an international standard used as the basis to evaluate the security properties of IT products.

As explained in Chapter 2, the security guideline tools for home users are supported by SFRs and SARs from ISO/IEC 15408. In addition, we have designed and developed a knowledge base tool for ST developers based on CC [8].

In actual practice, government organizations in the US, Canada, France, Germany, Australia, New Zealand, Japan and UK are part of the recognition arrangement for CC-based IT security evaluations. IT products which have been evaluated and authenticated based on CC receive the mutual approval of 12 countries, including those mentioned above. Such IT products also receive certifications which are accepted by 25 other countries. Therefore, in this threat countermeasure model, we include the security objectives described in part 4 of the Security Target (ST) evaluated by CC.

Security Objectives in ISO/IEC 17799

ISO/IEC 17799 contains 11 security control clauses. Each clause contains a number of security categories, which in turn include a control objective and one or more controls. Table 1 presents the 11 clauses together with the number of main security categories and the number of security controls in each clause.

Table 1 ISO/IEC 17799: Security Control Clause

Security Control Clauses	Security Categories	Security Control
Security Policy	1	2
Organization Information Security	2	11
Asset Management	2	5
Human Resources Security	3	9
Physical and Environmental Security	2	13
Communications and Operations Management	10	32
Access Control	7	25
Information Systems Acquisition Development and Maintenance	6	16
Information Security Incident Management	2	5
Business Continuity Management	1	5
Compliance	3	10

Our proposed knowledge base includes all 11 clauses, 39 security categories and 133 security controls. However, there are too many relationships between these security controls. For example, some security controls include a reference, "see also x", where "x" is the numerical value of another security control to be included. As shown in Fig. 7, security control "7.1.1" includes 2 references to the other controls in the same clause. However, security controls "7.1.3" and "7.2.1" also include references to security controls in other security clauses. In this way, the ISO/IEC 17799 standard spans over approximately 200 pages. In order to address this issue, our knowledge base works as a Web application which relates security objectives inside ISO/IEC 17799 with other standards, allowing users to search easily and quickly the necessary security objectives.

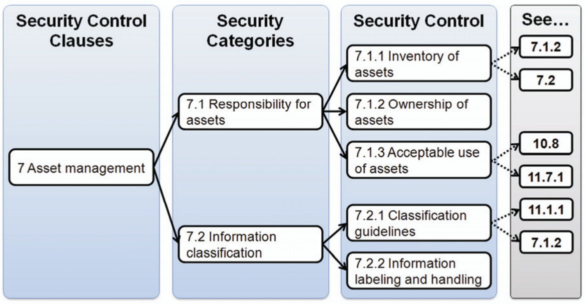

Security Control Clauses
Security Categories
Security Control
See…
7 Asset management
7.1 Responsibility for assets
7.2 Information classification
7.1.1 Inventory of assets
7.1.2 Ownership of assets
7.1.3 Acceptable use of assets
7.2.1 Classification guidelines
7.2.2 Information labeling and handling
7.1.2
7.2
10.8
11.7.1
11.1.1
7.1.2

Fig. 7 Clause 7 structure and reference

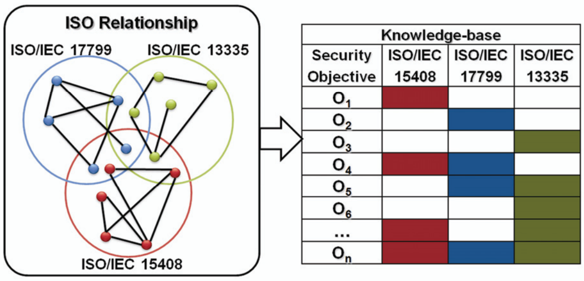
Security Objectives in ISO/IEC 13335

In order to be able to select countermeasures according to this threat classification, we also include information from ISO/IEC 13335, in particular, guidance information regarding the selection of safeguards from Part 4 of ISO/IEC 13335. Table 2 shows the safeguards for confidentiality.

As shown in Fig. 8, our proposed knowledge base intends to fuse similar security controls or objectives to create effective security guidelines for specific IT environments. In addition, it creates a ranking system of security objectives by using the relationships inside the standards as well as the relationships between different standards, as shown on the right side of Fig. 8.

Table 2 ISO/IEC 13335: Safeguards for confidentiality

10.2 Safeguards for Confidentiality
10.2.1 Eavesdropping
10.2.2 Electromagnetic radiation
10.2.3 Malicious code
10.2.4 Masquerading of user identity
10.2.5 Misrouting/re-routing of messages
10.2.6 Software failure
10.2.7 Theft
10.2.8 Unauthorized access to computers, data, services and applications
10.2.9 Unauthorized access to storage media

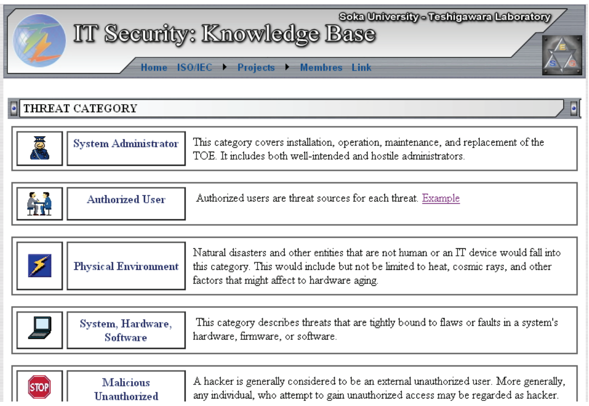


Knowledge-base			
Security Objective	ISO/IEC 15408	ISO/IEC 17799	ISO/IEC 13335
O_1	🟥		
O_2		🟦	
O_3			🟩
O_4	🟥	🟦	
O_5		🟦	🟩
O_6			🟩
...	🟥		🟩
O_n	🟥	🟦	🟩

Fig. 8 Knowledge base of security objectives

7. KNOWLEDGE-BASE APPLICATION

Our proposed knowledge base application targets home users who do not have special technical knowledge. This tool allows information about threats which affect IT environments to be accessed in a seamless manner, where users can search for threats by selecting a combination of parameters. In addition, as shown in Fig. 9, the threats have been classified into 5 categories: system administrator, authorized user, physical environment, system hardware and malicious unauthorized individual.


Soka University - Teshigawara Laboratory
IT Security: Knowledge Base
Home
ISO/IEC
Projects
Membres
Link

THREAT CATEGORY

System Administrator	This category covers installation, operation, maintenance, and replacement of the TOE. It includes both well-intended and hostile administrators.
Authorized User	Authorized users are threat sources for each threat. Example
Physical Environment	Natural disasters and other entities that are not human or an IT device would fall into this category. This would include but not be limited to heat, cosmic rays, and other factors that might affect to hardware aging.
System, Hardware, Software	This category describes threats that are tightly bound to flaws or faults in a system's hardware, firmware, or software.
Malicious Unauthorized	A hacker is generally considered to be an external unauthorized user. More generally, any individual, who attempt to gain unauthorized access may be regarded as hacker.

Fig. 9 Threats categories

In addition, each security threat is mapped to at least one security objective included in the abovementioned international standards.

After identifying the threats, users can read information about security control from multiple international standards.

For example:
Threats: An authorized user is the threat source. User abuses authorization to improperly collect sensitive or security-critical data. More specifically, user collects residual data from public objects after prior usage.

Objective:
ISO/IEC 15408: Eliminate residual information. Ensure there is no "object reuse;" i.e., ensure that there is no residual information in some information containers or system resources upon their reallocation to different users.

ISO/IEC 17799: 11.3.3 Clear desk and clear screen policy. The clear desk and clear screen policy should take into account the information classifications, legal and contractual requirements, and the corresponding risks and cultural aspects of the organization. The following guidelines should be considered:
a) Sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated;
b) Computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;
c) Incoming and outgoing mail points and unattended facsimile machines should be protected;
d) Unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented;
e) Documents containing sensitive or classified information should be removed from printers immediately.

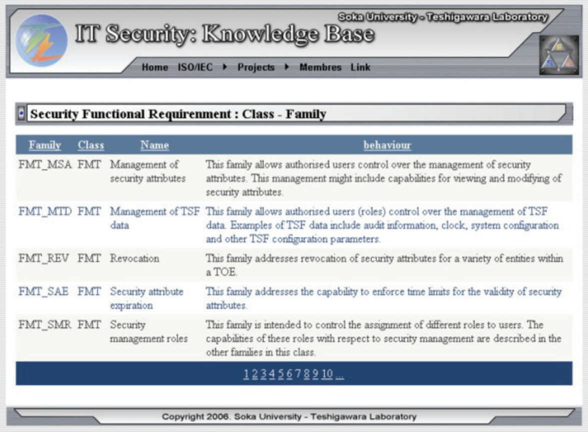
ISO/IEC 13335: 10.2.8 Unauthorized access to computers, data, services and applications. Unauthorized access to computers, data, services and applications can be a threat if access to any sensitive material is possible. Safeguards to protect against unauthorized access include appropriate identification and authentication, logical access control, audit at the IT system level, and network segregation at the network level.

8. CONCLUSION AND FUTURE WORK

Security policies represent organizational tools for informing users about the importance and sensibility of the information and the critical services which allow the company to grow and remain competitive.

This threat model architecture is based on ISO/IEC 15446 and ISO/IEC TR 13335. In addition, our proposed model aids users in the process of creating security policies by selecting the appropriate security controls agilely and effectively, in accordance with the IT environment, since the user operates only with a minimal set of security objectives. Moreover, all security policies in this model are created for the respective threats. At the same time, this model allows users to learn the necessary SFRs for their environment and to select the appropriate systems or products evaluated by the CC or ISO/IEC 15408.

We are working on a web application tool based on this knowledge base. Fig. 10 shows the user interface of our proposed model.


Soka University - Teshigawara Laboratory
IT Security: Knowledge Base
Home
ISO/IEC
Projects
Membres
Link

Security Functional Requirenment : Class - Family

Family	Class	Name	behaviour
FMT_MSA	FMT	Management of security attributes	This family allows authorised users control over the management of security attributes. This management might include capabilities for viewing and modifying of security attributes.
FMT_MTD	FMT	Management of TSF data	This family allows authorised users (roles) control over the management of TSF data. Examples of TSF data include audit information, clock, system configuration and other TSF configuration parameters.
FMT_REV	FMT	Revocation	This family addresses revocation of security attributes for a variety of entities within a TOE.
FMT_SAE	FMT	Security attribute expiration	This family addresses the capability to enforce time limits for the validity of security attributes.
FMT_SMR	FMT	Security management roles	This family is intended to control the assignment of different roles to users. The capabilities of these roles with respect to security management are described in the other families in this class.

1 2 3 4 5 6 7 8 9 10 ...

Copyright 2006. Soka University - Teshigawara Laboratory

Fig. 10 Web Application

Safeguarding assets of interest is a responsibility of the owners who place value on those assets. The value of the assets can vary according to the company or the network environment. In this regard, we aim at incorporating asset value modeling and risk management into the knowledge base in future work.

9. REFERENCES

[1] ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation Part 1~3 Version 3.0, June 2005

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

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

[4] ISO/IEC TR 13335-1-5, Information technology - Guidelines for the management of IT Security, 2000

[5] ISO/IEC 17799. Information technology - Code of practice for information security management, 2005

[6] ISO/IEC 27001. Information technology - Security techniques - Information security management systems - Requirements, 2005.

[7] Guillermo Horacio Ramirez Caceres 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.

[8] Guillermo Horacio RAMIREZ CACERES, Yoshimi TESHIGAWARA, “Design and Development of a Knowledge-based Tool for ST Developers Based on CC v3”, The 7th International Common Criteria Conference. Lanzarote, Spain. September, 2006. (http://www.7iccc.es/index_en.html)