Regular Paper

A Threat Model for Security Specification in Security Evaluation by ISO/IEC 19791

Guillermo Horacio Ramirez Caceres[1,†1,a) Yoshimi Teshigawara[1,†2,b)

Received: November 29, 2012, Accepted: June 14, 2013

Abstract: ISO/IEC TR 19791 is an international standard that must be used as the basis for the security evaluation of operational systems. This standard has been recently developed, and the first version was made available in May 2006. ISO/IEC TR 19791 is intended to be an extension of ISO/IEC 15408, known as "Common Criteria" (CC). In order to evaluate an IT product or system using CC or ISO/IEC TR 19791, developers must create a Security Target (ST), or a System Security Target (SST). However, a problem encountered in creating these is the determination of the Security Problem Definitions (SPDs), because the SPDs fall outside of the scope of CC. Neither ISO/IEC 15408 nor ISO/IEC TR 19791 provides a framework for risk analysis or the specification of threats. In this paper, we propose a threat model based on multiple international standards and evaluated ST information, and describe a Web application that can be used for security specifications in the production of STs and SSTs which are to be evaluated by CC and ISO/IEC TR 19791, respectively.

Keywords: international standards, threat modeling, risk management

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], [2], [3]. IT products that have been evaluated and authenticated based on CC will be approved by 16 certificate authorizing countries members of the Common Criteria Recognition Arrangement (CCRA) [4]. These IT products will also have certifications that are accepted by 26 certificate consuming countries. As shown in **Fig. 1**, the number of IT products evaluated according to CC is growing rapidly.

Unlike Common Criteria, ISO/IEC TR 19791 is used for the security evaluation of operational systems [5]. The first version of this standard was made available in May 2006. This standard is intended to be compatible with and providing additional security evaluation criteria to address those aspects of operational systems not covered by the ISO/IEC 15408 evaluation criteria.

Common Criteria provides support for specifying the IT security functional requirement in products and systems. ISO/IEC TR 19791 extends this support to the environment of operational systems.

In order to evaluate an IT product or system based on CC or ISO/IEC TR 19791, developers must create a Security Target (ST), or a System Security Target (SST). However, a problem encountered in creating an ST or SST is the determination of the Security Problem Definitions (SPDs), because the SPDs fall outside of the scope of CC. Neither ISO/IEC 15408 nor ISO/IEC TR 19791 provides a framework for risk analysis or the specification of threats. Usually, ST developers must refer to ISO/IEC 13335 for more detailed information [6], [7], [8], [9], [10].

Common Criteria provides a definition of the context in which the Target of Evaluation (TOE) resides. In particular, it defines the "Security Environment" which the TOE is designed to address. This description details any assumptions defining the scope of the security needs, the identified threats to the assets requiring protection, and any organizational security policies with which the TOE must comply.

Based on ISO/IEC TR 19791, the SST security problem definition (SPD) needs to provide a coherent, consistent and sufficiently complete definition of the security problems that the operational system is intended to address. The security problems are stated

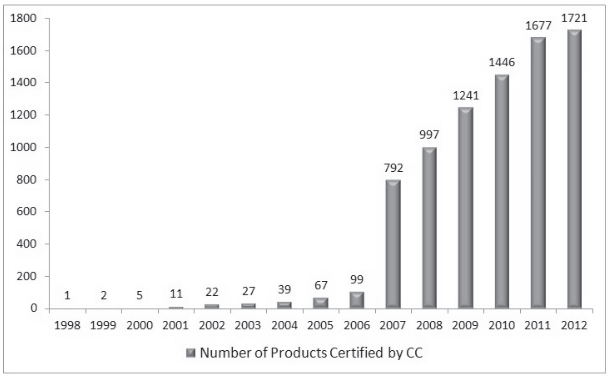


Fig. 1 Number of products certified by CC.

[1] Graduate School of Engineering, Soka University, Hachioji, Tokyo 192–8577, Japan

[†1] Presently with Universal Communication Research Institute, National Institute of Information and Communications Technology (NICT), Soraku, Kyoto 619–0289, Japan

[†2] Presently with School of Science and Technology for Future Life, Tokyo Denki University, Adachi, Tokyo 120–8551, Japan

[a)] ramirez.caceres@nict.go.jp

[b)] 13kz002@ms.dendai.ac.jp

in terms of the risks that will be countered by the operational system and the organizational security policies that support and govern the use of the operational system to reduce operational system risk to an acceptable level.

One of the problems in creating an ST is to determine the SPDs, because they fall outside of the scope of CC. When evaluating a system against ISO/IEC 19791, this problem becomes more complex because, to determine the SPDs in this case, the SST must also address the establishment of acceptable risk and the determination of actual residual risk. However, ISO/IEC 15408 and ISO/IEC TR 19791 do not provide a framework for risk analysis or the specification of threats. The ST developer must, therefore, refer to other standards [1], [5].

Another problem is in the area of knowledge required in creating an ST or SST. There is a large amount of information to digest. 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 [11].

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

Following on from a previous study [12], 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. The objective is to support developers to describe the SPDs. In addition, this threat model will allow developers to determine the level of risk which the organization is willing to accept [13].

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 and SSTs which are to be evaluated by ISO/IEC 15408 and ISO/IEC TR 19791, respectively.

This paper is organized as follows. In Section 2, we briefly review the International Standards used in this research and related works to describe the issues motivating this research and the objectives we will achieve. In Section 3, we describe the threat model proposed in this research. In Section 4 we describe a knowledge base and Web application that have been developed in this research. Finally, in Section 5, we present our conclusions and discuss a future work.

2. Research Background

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 [1]. Based on CC version 3, each ST consists of seven chapters as shown on the left hand side of **Fig. 2**.

A System Security Target, as defined in ISO/IEC TR 19791, provides a specification for the implemented security capabilities of an operational system as it is employed in a specific operational context to counter assessed risk and enforce stated organizational security policies to achieve an acceptable level of residual risk [5].

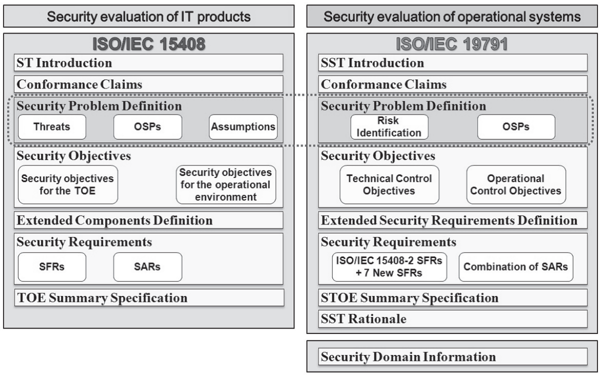

Security evaluation of IT products
Security evaluation of operational systems
ISO/IEC 15408
ST Introduction
Conformance Claims
Security Problem Definition
Threats
OSPs
Assumptions
Security Objectives
Security objectives for the TOE
Security objectives for the operational environment
Extended Components Definition
Security Requirements
SFRs
SARs
TOE Summary Specification
ISO/IEC 19791
SST Introduction
Conformance Claims
Security Problem Definition
Risk Identification
OSPs
Security Objectives
Technical Control Objectives
Operational Control Objectives
Extended Security Requirements Definition
Security Requirements
ISO/IEC 15408-2 SFRs + 7 New SFRs
Combination of SARs
STOE Summary Specification
SST Rationale
Security Domain Information

Fig. 2 ST and SST contents.

The operational system is composed of an integrated combination of technical and operational control functions. The SST describes the requirements and behavior of the functions that implement the security objectives through a combination of technology-based and operation-based mechanisms [5].

An SST differs from an ST in that an SST focuses on the technical and operational controls of the operational systems. Each SST includes two parts: a common part applicable to the whole System Target of Evaluation (STOE) and a domain part, dealing with each security domain included in the STOE. The common part is made up of eight chapters as shown on the right hand side of Fig. 2.

These international standards provide a catalog of security requirements to support only one chapter of the security target. As explained in the previous section, describing the Security problem definition is one of the most complicated parts of the ST, because the risk assessment necessary to describe the SPD is outside the scope of these standards [1], [5].

There are some related works on risk assessment and threats identification. For example, OCTAVE presents a set of generic threats profiles that organizations can use to identify and analyze threats to their assets [14]. Microsoft also has developed a threats modeling based on commons attack STRIDE [15]. This threat model is widely used by organizations. However, it is difficult to implement in the evaluation scheme of Common Criteria or ISO/IEC 19791, because the identified threats are not linked to the target of evaluation.

In this paper, we present a threat modeling that we developed for use in the evaluation process of products and systems. By using this model, developers are able to identify the threats that affect the TOE for evaluation and select the necessary security requirements to address the security needs.

3. Threat Model for Security Specification

ISO/IEC 19791, describes a three-step approach to establishing the necessary level of security for an operational system:

- Step 1: Risk assessment
- Step 2: Risk reduction
- Step 3: Accreditation

The threat model proposed in this research is to support the developer to implement a risk assessment for security evaluation by ISO/IEC 19791. In addition, we propose a knowledge base of security control based on international standards, to support developers to select the necessary security controls in the step 2 risk reduction and step 3 accreditation. These three steps are shown in the next three subsections.

3.1 Step 1: Risk Assessment

To implement the risk assessment, it is necessary to determine the assets that need protection. In this research we implement the asset classification of ISO/IEC 27001.

The risk assessment is also necessary to identify a proposed course of action to reduce the risk to an acceptable level by implementing the security controls from ISO/IEC 19791.

Each risk is categorized as tolerated, accepted, avoided, transferred, or unacceptable, that is, requiring reduction or elimination through technical or operational controls within the STOE.

The list of risks includes risks relating to the development of the operational system. 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 threats are classified in terms of WHO, HOW and WHAT [12]. As shown in **Fig. 3**, 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 19791 [5]. It also includes asset value modeling and risk management based on international standards [16], [17].

To create this new model, we have been working with 170 SPD for STs evaluated by Common Criteria [4]. We classified the threats information 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 happen? (WHY)

WHO: Threat agents can be classified by two parameters: the type of agent and the agent's level of authentication [18]. 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. The first parameter has 2 values: human and the other. Human threats subsequently can be broken down according to authentication level, such as system administrator, authorized user or unauthorized user. This second parameter defines the agent as authenticated, unauthenticated or undefined.

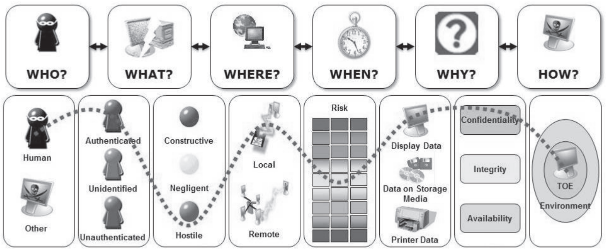


Fig. 3 Threat classification.

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 the vulnerabilities of the system. Some frequently used techniques for acquiring information are listed below.

- Eavesdropping and packet sniffing
- Snooping and downloading
- Tampering and data diddling
- Spoofing
- Trojans
- Social engineering
- Viruses
- Obtaining passwords, codes and keys

WHAT: Common Criteria defines an asset as information or a resource that may be protected by the security policy [1]. In this research, to define WHAT we classified the results of attacks in terms of loss types: availability, confidentiality, and integrity. The first parameter classifies the results of attacks in terms of loss types: availability, confidentiality, and integrity.

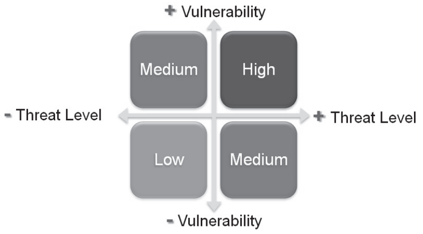
- Confidentiality: Confidentiality is the protection of communications or the data stored against interception and unauthorized reading by people.
- Integrity: Integrity is confirmation that the data has been sent, received or stored completely, and that the information has not been modified.
- Availability: This means that the data is accessible, even when alterations, natural power failures, catastrophes, accidents or attacks happen.

In addition, it is necessary to specify the assets that we must protect, because the attack may affect IT capabilities, as in a system or a user process. Then the second parameter shows the assets that we must protect, such as a hard disk, display data or printed data.

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.

WHEN: To specify this parameter it is necessary to know when the attack took place. For example, the time and the day need to be known. According to 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 life-cycle phase. The life-cycle of an operational system is considered to have four phases: development/integration, installation, system operation and maintenance.

WHY: Attacks can have several objectives, including fraud, extortion, theft of information, revenge or simply the challenge of penetrating a system. Attacks can be performed by internal employees who abuse their permissions of access, or by external attackers who break in remotely or intercept network traffic. The



		Levels of Vulnerability		
		Low	Medium	High
Levels of Threat	Low	1	2	3
	Medium	2	3	4
	High	3	4	5

Fig. 4 Threat – Vulnerability matrix.

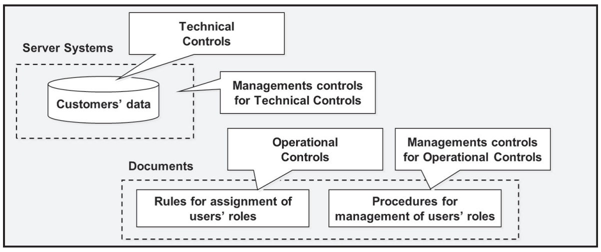

Server Systems
Technical Controls
Customers' data
Managements controls for Technical Controls
Operational Controls
Managements controls for Operational Controls
Documents
Rules for assignment of users' roles
Procedures for management of users' roles

Fig. 5 Risk reduction.

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

To determine the threats, we extracted and classified information based on these six elements.By combining these elements we can identify specific and detailed information concerning each threat. Finally, by including the asset values it is possible to know the impact of each threat. **Figure 4** shows the relationship between the level of threat and the vulnerability of the system.

3.2 Step 2: Risk Reduction

After identifying the risk, it is necessary to select security controls in order to reduce the risk [5]. Common Criteria specifies technical controls that are implemented by the IT systems. The operational system also needs to specify operational controls. As shown in **Fig. 5** technical and operational controls have related management controls and activities that are essential to ensure that they are implemented as specified and are effective in practice.

Risk reduction is the countering or elimination of security risks by the selection, application and assessment of security controls. Management, operational, and technical controls are prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. There are many security controls in different international standards. In this research, we have been developing a knowledge-base for security control that includes:

- ISO/IEC 15408
- ISO/IEC 19791
- ISO/IEC 27002
- ISO/IEC 13335
- FIPS 140-2

Table 1 Security functional requirements.

Security functional Class	Family	Components
Security Audit (FAU)	6	15
Communication (FCO)	2	4
Cryptographic Support (FCS)	2	5
User Data Protection (FDP)	13	31
Identification and Authentication (FIA)	6	14
Security Management (FMT)	7	14
Privacy (FPR)	4	10
Protection of the TSF (FPT)	14	23
Resource Utilization (FRU)	3	6
TOE Access (FTA)	6	10
Trusted Path/Channels (FTP)	2	2

3.2.1 Technical Controls

Security controls for an information system are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

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 classes are summarized in **Table 1**.

According to ISO/IEC 19791 security evaluation, the target of evaluation may employ cryptographic functionality to help to satisfy several high-levels of security objectives. However, cryptographic algorithms are not covered in the Common Criteria. Then ST developers must be able to refer to an external standard.

In order to support developers, in our knowledge base, we also include federal information processing standards publication FIPS PUB 140-2. This standard specifies the security requirements that are to be satisfied by cryptographic modules [11]. This standard also provides 4 levels of security. As shown in **Table 2**, the 11 security requirement areas are defined for the security of design and implementation of cryptographic modules.

There is a set of assertions for each security requirement. The number of assertions is increased according to the security level. In addition, following each assertion is a set of requirements levied on the vendor, and a set of requirements levied on the tester.

3.2.2 Operational Controls

Security controls for an information system primarily are im-

Table 2 FIPS 140-2 security requirements.

Security Requirement	Assertions	Security Level			
		1	2	3	4
1. Cryptographic module specification	15	14	14	15	15
2. cryptographic module ports and interfaces	18	15	15	18	18
3. Roles, Services, and authentication	32	19	28	28	28
4. Finite State Model	5	5	5	5	5
5. Physical Security	69	18	28	41	68
6. Operational Environment	27	8	16	20	20
7. Cryptographic key management	42	35	35	42	42
8. EMI/EMC	5	4	4	4	4
9. Self Tests	48	48	48	48	48
10. Design Assurance	25	12	15	18	25
11. Mitigation of other attacks	1	1	1	1	1

Table 4 ISO/IEC 27002: Security control & SPD matrix.

Security Control	WHO	HOW	WHAT	WHERE	WHEN	WHY
Information security policy document	X		X	X		X
Review of the information security policy			X		X	X
Management commitment to information security	X					X
Information security co-ordination	X			X		X
Allocation of information security responsibilities				X		X
Authorization process for information processing facilities	X		X		X	X
Confidentiality agreements			X			X
Contact with authorities						X
Contact with special interest groups						X
Independent review of information security	X		X		X	X
Identification of risks related to external parties	X		X	X	X	X
Addressing security when dealing with customers	X		X	X	X	X
Addressing security in third party agreements	X	X	X	X		X

Table 3 Operational security control.

Operational security controls	Family	Components
Administration control (FOD)	6	10
IT System control (FOS)	7	18
User Assets control (FOA)	2	2
Business control (FOB)	2	2
Facility and Equipment control (FOP)	5	7
Third Parties control (FOT)	2	2
Management (FOM)	5	9

plemented and executed by people. Because most of these controls depend on human actions which are not necessarily predictable or repeatable, management and monitoring are even more important than for technical controls [5].

In ISO/IEC 15408, the evaluation of security functionality deals only with the provision of IT security functions. However, for ISO/IEC 19791, an operational system is generalized into an STOE that includes both the technical and operational control functions. Technical security controls are selected from the functional classes defined within ISO/IEC 15408-2 but ISO/IEC 19791 defines extensions to ISO/IEC 15408 to enable the security assessment of operational systems. 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. These classes are summarized in **Table 3**.

3.2.3 Management Controls

Security controls for an information system focus on the management of risk and the management of information system security.

ISO/IEC 27002 contains eleven security control clauses. Each clause contains a number of security categories. Finally, these security categories include a control objective and one or more controls. **Table 4** shows an example of how the security control on ISO/IEC 27002 meets the security problem definition (SPD) by using this knowledge base.

Table 5 Confidentiality – Risk matrix.

Types of risk	Trust Relationship References (Public)		
	LOW	MEDIUM	HIGH
Loss of Confidentiality	13.2.2	13.2.2	13.2.2
	13.2.3	13.2.3	13.2.3
	13.2.6	13.2.4	13.2.5
	13.4	13.2.6	13.2.6
	13.5	13.3.2	13.3.2
	13.7	13.3.3	13.3.3
	13.8	13.3.4	13.3.4
	13.9	13.4	13.3.5
	13.12	13.5	13.4
		13.7	13.5
		13.8	13.7
		13.9	13.8
		13.12	13.9
			13.12

Our proposed knowledge-base includes these 11 clauses, 39 security categories, and 133 security controls. However, there are many relationships between these security controls and it may be necessary to ignore some of these in practice.

To select countermeasures according to this threat classification, we also include in our knowledge-base information from ISO/IEC 13335, in particular guidance on the selection of safeguards from Part 4. **Table 5** shows the references to possible security controls for losses of confidentiality given in ISO/IEC 13335.

3.3 Step 3: Accreditation

This is the last step to establishing operational system security. In this step it is necessary to confirm the residual risks remaining within the system after the controls are applied and checked if

Table 6 Comparison of assurance classes.

ISO/IEC 15408	Operational system	Applicability
Protection Profile evaluation (APE)	System Protection Profile evaluation (ASP)	Specification of SPP
Security Target evaluation (ASE)	System Security Target evaluation (ASS)	Specification of SST
Development (ADV)	Operational system architecture, design and configuration document (ASD)	Interfaces and configuration of components External interfaces Architecture, information flow, access to STOE Mode of operation/transition condition
Guidance documents (AGD)	Operational system guidance document (AOD)	Rules and procedures for User and Administrator guidance Confirmation and verification (operation time)
Life-cycle support (ALC)	Operational system configuration management (AOC)	Configuration management (plan, CM system) Secure configuration of component products Reuse of product evaluation results
Tests (ATE)	Operational system test (AOT)	Functional, coverage and depth test for SSFs Independent testing for SSFs Regression testing at maintenance/modification time
Vulnerability assessment (AVA)	Operational system vulnerability assessment (AOV)	Detection of insecure states and their recovery Penetration testing
Composition (ACO)	None	Not applicable to operational systems
	Preparation for live operation (APR)	Awareness training and Communication of SSFs Confirmation and verification (operation time)
	Records on operational system (ASO)	Records of SSFs log Management review on SSFs Independent verification of SSFs Confirmation and verification of records

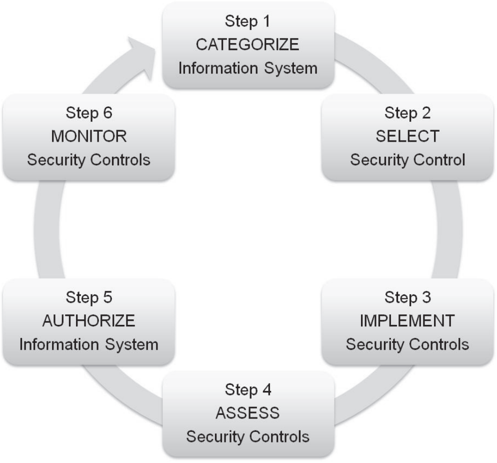


Fig. 6 Risk accreditation.

they are appropriate for the system to be used in live operation.

However, ISO/IEC TR 19791 does not provide techniques or models for accreditation. In this research we have implemented a Risk Management Framework (RMF) based on NIST SP 800-37 [19]. **Figure 6** shows the tasks required to apply the Risk Management Framework to information systems.

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. The security assurance requirements are cataloged and organized in Classes and Families. In addition, this part also defines the evaluation criteria for protection profile (PP) and ST. There are seven predefined assurance packages, usually called Evaluation Assurance Levels (EALs).

The assurance classes ISO/IEC 19791 are based on assurance classes from ISO/IEC 15408, but generalized for applicability to both technical and operational security measures. Security assurance can be considered from two aspects, correctness and effectiveness. Correctness means that the security mechanisms have been implemented correctly. Effectiveness means that the security mechanisms work against security threats and vulnerabilities and prevent unauthorized processes. Assurance can be gained from activities across all phases of the system life cycle. **Table 6** shows comparison of the assurance class.

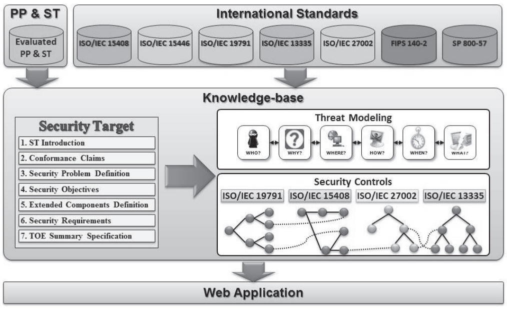


Fig. 7 Web application structure.

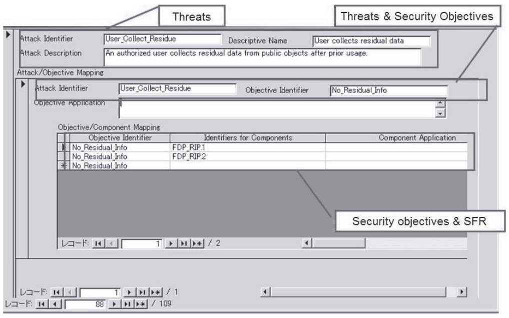
4. Model Implementation and Evaluation

This section introduces our knowledge base application. **Figure 7** shows the system architecture. Based on international standards and products evaluated by Common Criteria, we create a knowledge base including the threat model and security control. Using the threat classification described in Section 3, we 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 STOE under evaluation.

The objective in creating this web application is to support the developer to describe the SPD for evaluation by ISO/IEC 19791. In the SPD section of the SST, the SST 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.

4.1 Knowledge-base

This knowledge-base tool provides access to information about threats that affect an STOE. Developers can search for threats by selecting some parameters. In addition, the threats have been



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		

Fig. 8 Threats security control mapping.

classified into five categories: system administrator, authorized user, physical environment, systems hardware, and malicious unauthorized individual.

ST developers can select the appropriate threat from the knowledge base. SST 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.

The knowledge base of risk information was created by analyzing the information on threats of 170 STs evaluated by Common Criteria [4]. Then, in order to reduce the risk, we are mapping each identified risk to one or more security controls. Our knowledge base also includes a list of security policies based on international standards, including ISO/IEC 15408. **Figure 8** shows the screen-shot of the application. By using this application developers are able to access detailed information concerning the risk. Then, for each specific risk, it is possible to know the necessary security objectives to meet the identified risk. Finally, the list of security controls to address the security objectives are displayed.

4.2 Web Application

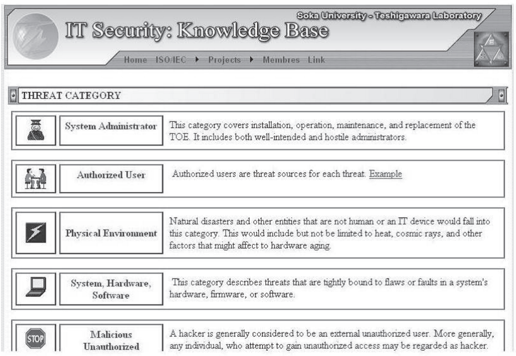
The web application was developed based on the knowledge base described above. This application was developed in ASP 2.0. This system uses a membership function, one of the personalization functions of ASP.NET 2.0. Using this personalization function it becomes possible to provide different information according to the current user. In addition, it can suit the user's proficiency in the web interface because it can customize the interface to each user. Moreover, ASP.NET 2.0 corresponds to various data bases such as SQL server, Microsoft Access, and XML. The first version of this system, information on international standards was managed by using Microsoft Access and XML, and the user's information was managed by using SQL server. However, in the new version of the system, all international standards information were managed by using XML.

Figure 9 shows the user interface screen of the developed web application, developers are able to search for some risks on the web application, and access the necessary information on security controls related to each risk.

For example, suppose *an authorized user improperly collects sensitive or security-critical data. More specifically, the user collects residual data from public objects.*

The threat can be classified by the following criteria.

- Who: Human, an authorized user



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 Web application.

- How: Observing residual data
- What: Sensitive or security-critical data
- Where: Local
- When: Any
- Why: Deliberate, hostile

Suggested security requirements are as follows.

ISO/IEC 15408: Eliminate residual information. Ensure there is no "object reuse": that is, ensure that there is no residual information in 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:

- Sensitive or critical business information, for example, 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;
- 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;
- Incoming and outgoing mail points and unattended facsimile machines should be protected;
- Unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented;
- Use a Knowledge-base System and Threat-Countermeasure Model for Security Evaluation Based on International Standards;
- 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.

5. 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 and STOEs. In addition, this model includes a risk methodology based on ISO/IEC 13335.

On the basis of this model, we have developed an application which an SST 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.

According to ISO/IEC 19791, the security controls of an operational system must be assessed throughout the lifetime of the system. 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.

In the case of the Common Criteria, there are more than 250 PPs of different products categories and more than 2,000 STs of products evaluated by different scheme and EALs. As a future work, we are planning to upgrade the information about threats including these new STs. In addition, while a community of experts exist to evaluate, to discuss and exchange ideas about ISO/IEC 15408 is possible, however, no such community exist for ISO/IEC 19791 on which our model is based. Therefore, currently as a member of a Common Criteria community, as second step, we are planning to implement the model in the creation of PP in some technical communities for practical use and evaluation or verification of the proposed model. Then our following task is to create a community that will test and submit feedback for the improvement of the web application.

References

[1] ISO/IEC 15408-1:2009, Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model (2009).

[2] ISO/IEC 15408-2:2009, Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components (2009).

[3] ISO/IEC 15408-3:2009, Common Criteria for Information Technology Security Evaluation – Part 1: Security assurance components (2009).

[4] The common criteria portal, available from ⟨http://www.commoncriteriaportal.org/⟩ (accessed 2013-03-16).

[5] ISO/IEC TR 19791:2005, Information technology – Security techniques – Security assessment of operational systems (2005).

[6] ISO/IEC TR 13335-1:1996, Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security (1996).

[7] ISO/IEC TR 13335-2:1997, Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security (1997).

[8] ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security (1998).

[9] ISO/IEC TR 13335-4:2000, Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards (2000).

[10] ISO/IEC TR 13335-5:2000, Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security (2000).

[11] Federal Information Processing standards publication, FIPS PUB 140-2, Security Requirements for Cryptographic Modules (May 2005).

[12] Ramirez Caceres, G.H. and Teshigawara, Y.: A Study of Threat Modeling Based on International Standards for Production of Security Targets, *DICOMO 2005*, pp.189–192 (July 2005).

[13] ISO/IEC 27002:2005, Information technology – Security techniques – Information security management systems – Requirements (2005).

[14] CERT, Software Engineering Institute: Operational Critical threat, Asset, and Vulnerability Evaluation (OCTAVE), available from ⟨http://www.cert.org/octave/⟩ (accessed 2013-03-16).

[15] Microsoft: Threat Modeling, available from ⟨http://msdn.microsoft.com/en-us/library/ff648644.aspx⟩ (accessed 2013-03-16).

[16] ISO 31000:2009, Risk management – Principles and guidelines (2009).

[17] ISO/IEC 31010:2009, Risk management – Risk assessment techniques (2009).

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

[19] NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (Feb. 2010).

Guillermo Horacio Ramirez Caceres was born in Corrientes, Argentina. In 1991, he started supporting and creating computer systems for small and middle-sized companies. Subsequently, he started teaching Programming, Mathematics, and Logic classes at senior high schools in 1996, and eventually joined the Ministry of International Trade and Industry, Argentina in 1998. He also received his B.E. degree in International trade at Nordeste University in 1999. In 2000, he came to Japan to study the Japanese language at Soka University, and joined the Network Laboratory at Soka University one year later. He received his M.E. degree in engineering in September 2003, and received his Ph.D. in March 2010 from Soka University, Japan. He is currently a researcher at the National Institute of Information and Communications Technology (NICT) Japan. His research interests are in the fields of Information Network Security, Network Management, and Human Networks. He is a member of IEICE, IPSJ, IEEE and IIIS.

Yoshimi Teshigawara has been a professor of Department of Information Systems Science, Faculty of Engineering at Soka University since 1995, and is currently a researcher of the Department of Information Systems and Multimedia Design, School of Science and Technology for Future Life at Tokyo Denki University since 2013. He began his professional career in 1970 at NEC Corporation, engaging in the design and developments of network architecture and its related products. From 1974 to 1976, Dr. Teshigawara was a visiting research affiliate with the ALOHA System at the University of Hawaii where he did research on packet radio and satellite networks. He engaged in the design and development of computer systems via satellite using VSAT. In addition, he worked on the standardization of network management as the chairmen of organized committees. His current interests are network security, e-learning, and ubiquitous computing. Dr. Teshigawara received his Ph.D. from the Tokyo Institute of Technology, Japan, in 1970.