

Study on a Knowledge-base System and Threat-Countermeasure Model for Security Evaluation Based on International Standards

国際標準に基づくセキュリティ評価のための 知識ベースシステムと脅威・対策モデルに関する研究

04D5106 ラミレス カセレス ギジェルモ オラシオ 指導教授 勅使河原 可海

ABSTRACT

情報セキュリティは、情報システムの能力のようなものとして捉えることができる。その能力とは、送信中のデータや保存データ、及び可用性・完全性・機密性を損なわせる事故や意図的な行為から通信サービスを守る能力である。セキュリティに関する多くの国際標準が存在するが、本研究では、ISO/IEC 15408, 15446, 19791, 13335, 27001 および 27002 を使用している。本研究では、これらの脅威から情報システムを防御するために、ユーザの情報システム環境に柔軟に適応可能なセキュリティポリシーの作成を提案する。さらに、国際標準の必要な情報を参照できるようにナレッジベースツールを開発した。本ナレッジベースツールでは、様々な環境の脅威を容易に識別するために、国際標準に基づいた脅威モデル機能を開発した。このモデルを用いることにより、開発者だけでなく一般ユーザのような特別な知識を持っていないユーザでも様々な脅威の基本的な特徴を選択するだけで、容易にユーザの環境における脅威を識別することが出来る。さらに、これらの脅威に対してユーザはユーザの環境に適応したセキュリティポリシーを、有効かつ素早く適切に選択することができる。ここで脅威とポリシーの関係は、国際標準に基づいたものになっている。

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 17799 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, we propose a security guideline tool based on such knowledge base.

2. Research background

2.1. International Standards

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.

2.2. Security Concepts

As shown in Figure 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 a lot of 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 are applied 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.

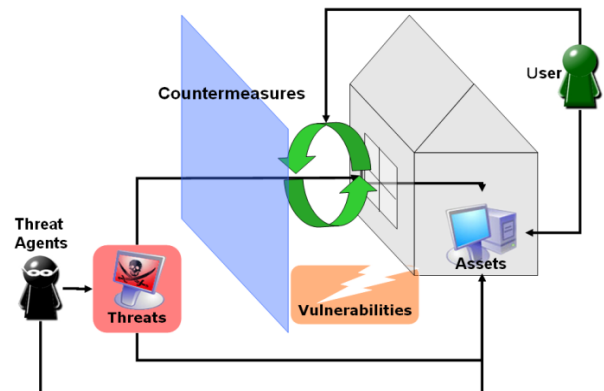


Figure 1 Security Concepts

Research Objectives

The issues described in Section 2 motivated us to develop a knowledge-based tool to help users to implement a security system. In this research, we propose a security guideline tool by implementing a Protection Profile (PP) for home user systems. This tool was developed in order to support users to understand the threats which affect their environment and select the appropriate security policies. By using this tool, users can access information about international standards in accordance to their level of knowledge. Figure 2 shows the architecture of the proposed security guideline tool.

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.

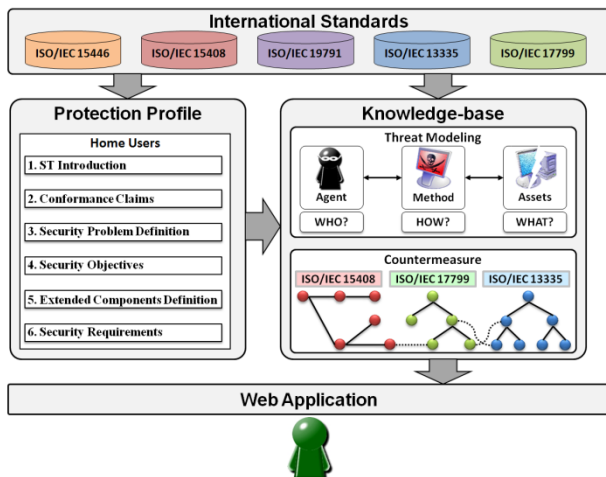


Figure 2 The proposed Knowledge-base model

3. Our Approach

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 application was developed in 3 basic steps.

First, a PP for home user systems was created on the basis of the international standard ISO/IEC 15408 in order to allow the understanding of basic security issues regarding each type of home IT environment.

Then, we created a knowledge base including the PP information, as well as a security policy including other international standards, as mentioned above. Our proposed method has been divided into another two steps. The first step identifies and specifies the threats which affect the IT environment by using a threat model. Each of the identified threats is addressed by at least one objective. The second bstep specifies the countermeasures, also called security objectives, which are suitable for implementation with regards to the identified threats [10].

Finally, we created a web application tool to be used as a security guideline for home users. By using this tool, users can access the details regarding the most common threats to information systems and subsequently select an appropriate security policy in response to threats for home user environments on the basis of international

standards, including ISO/IEC 15408.

4. Protection Profile for Home User Systems

A Protection Profile defines an implementation-independent set of security requirements and objectives for a category of products or systems which meet similar consumer needs with respect to IT security. A PP is designed to be reusable, and its purpose is to define the requirements which are known to be useful and effective for meeting the identified objectives. In order to describe the security requirements for home user systems, we construct the PP for home user systems on the basis of ISO/IEC 15408 and ISO/IEC 15446 [7]. This PP was evaluated according to the Common Methodology for Information Technology Security Evaluation (CEM) [8]. This PP consists of approximately 160 pages categorized in 6 chapters. The content of the PP is shown in Table 1.

Table 1 Content of the Protection Profile

1	PP introduction
2	Conformance claim
3	Security problem definition
4	Security objectives
5	Extended components definition
6	Security requirements

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 Figure 3. 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)

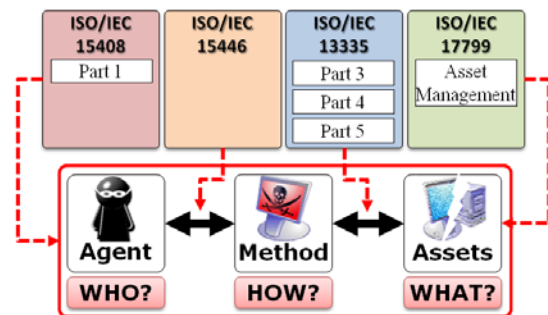


Figure 3 Threat Model and ISO Relationship

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

5.1. 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 [9]. As shown in Figure 4, 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.

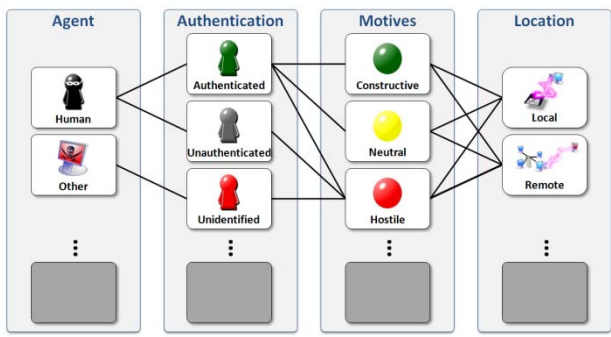


Figure 4 WHO Classification

5.2. 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.

5.3. 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 Figure 5, we use 3 parameters to define “WHAT” is the asset exposed to the threat. 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.

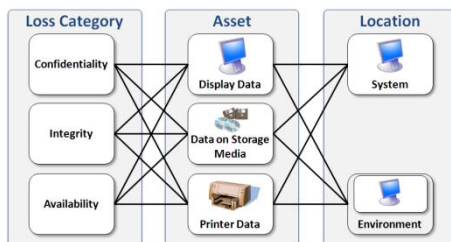


Figure 5 WHAT Classification

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 and ISO/IEC 13335 part 4 and 5.

6.1. 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 parts of the recognition arrangements 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.

6.2. 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.

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 Figure 6, 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 the necessary security objectives easily and quickly.

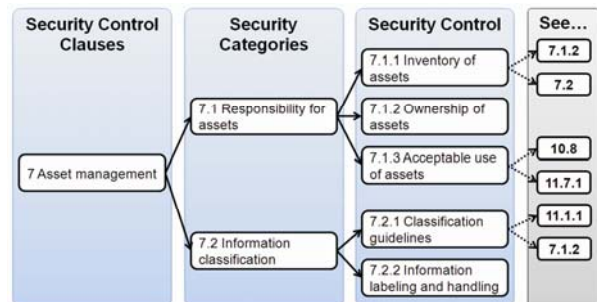


Figure 6 Clause 7 structure and reference

6.3. 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.

As shown in Figure 7, 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 among different standards, as shown on the right side of Figure 7.

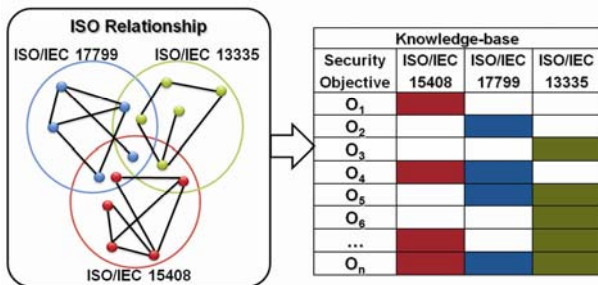


Figure 7 Knowledge base of security objectives

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. The threats have been classified into 5 categories: system administrator, authorized user, physical environment, system hardware and malicious unauthorized individual. 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. The user abuses authorization to improperly collect sensitive or security-critical data. More specifically, the 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.”

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

In this research, we have developed a web application tool based on this knowledge-base. Figure 8 shows the user interface of our proposed model. This tool allows users to search for threats and to select the appropriate security policies.

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.

Safeguarding assets of interests are 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 the future work.

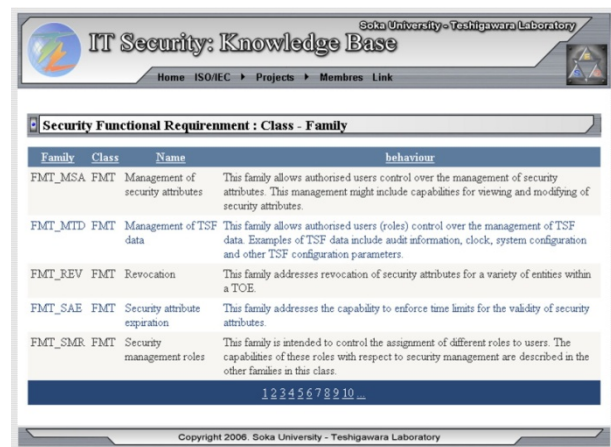


Figure 8 Web Application

9. References

- [1] ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation Part 1~3 Version 3.1, July 2009
- [2] ISO/IEC TR 15446. Information technology - Security techniques - Guide for the production of protection profiles and security targets, 2004
- [3] ISO/IEC TR 17991. 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] CEM v3.0 (2005) “Common Methodology for Information Technology Security Evaluation”, July 2005
- [9] Mitnick, K. D. and Simon, W. D.(2002), The Art of Deception, Wiley Publishing.
- [10] Guillermo Horacio Ramirez Caceres and Yoshimi Teshigawara, “Design and development of a knowledge-based tool based on multiples international standards”. The 8th International Common Criteria Conference (8thICCC). September 2007.