A Security Requirement Management Database Based on ISO/IEC 15408

Shoichi Morimoto[1], Daisuke Horie[2], and Jingde Cheng[2]

[1] Advanced Institute of Industrial Technology,
1-10-40, Higashi-ōi, Shinagawa-ku, Tokyo, 140-0011, Japan
morimo@aise.ics.saitama-u.ac.jp
[2] Department of Information and Computer Sciences, Saitama University,
Saitama, 338-8570, Japan
{morimo, horie, cheng}@aise.ics.saitama-u.ac.jp

Abstract. With the scale-spreading and diversification of information systems, security requirements for the systems are being more and more complicated. It is desirable to apply database technologies to information security engineering in order to manage the security requirements in design and development of the systems. This paper proposes a security requirement management database based on the international standard ISO/IEC 15408 that defines security functional requirements which should be satisfied by various information systems. The database can aid design and development of information systems that require high security such that it enables to suitably refer to required data of security requirements.

1 Introduction

Nowadays, in design and development of various information systems, it is necessary to take security issues into consideration and to verify whether or not the systems satisfy stringent security criteria. Thus, ISO/IEC 15408 was established as a criterion for evaluating the security level of IT products and information systems [7]. ISO/IEC 15408 defines security functional requirements which should be applied to validate an information system. Developers have to make a security design document for evaluation of ISO/IEC 15408. The process of making the documents is very complicate. Moreover, they must also decide by themselves which security functional requirements are necessary to their systems. As it is, it is difficult to determine which requirements are required. Thus, it is a very hard task and difficult to develop information systems which comply with ISO/IEC 15408.

On the other hand, in software engineering, especially in requirement engineering, some databases have been proposed in order to collect, manage and reuse the past knowledge/experience in information system design and development, e.g., [8, 6, 13]. Database technologies have successfully been applied to software engineering. Similarly, one can manage the knowledge/experience for security requirements in information system design and development that comply with ISO/IEC 15408 by a database.

M. Gavrilova et al. (Eds.): ICCSA 2006, LNCS 3982, pp. 1–10, 2006.

This paper proposes a security requirement management database based on the international standard ISO/IEC 15408, named "ISEDS (Information Security Engineering Database System)." Users of ISEDS can collect, manage and reuse security requirements. Thus, ISEDS can aid design and development of secure information systems, which satisfy the security criteria of ISO/IEC 15408.

2 ISO/IEC 15408

We herein explain ISO/IEC 15408 which is the base of ISEDS. ISO/IEC 15408 consists of three parts, i.e., "Part 1: Introduction and general model," "Part 2: Security functional requirements," and "Part 3: Security assurance requirements." Part 1 is the introduction of ISO/IEC 15408. Part 1 provides that sets of documents, so-called 'security targets,' must be created and submitted for evaluating information systems by ISO/IEC 15408. In order to simplify the creation of security targets, Part 1 also proposes templates called 'protection profiles.' Part 2 establishes a set of functional components as a standard way of expressing the functional requirements for target information systems. In other words, Part 2 defines the requirements for security functions which should be applied to validate an information system. Part 3 establishes a set of assurance components as a standard way of expressing the assurance requirements for target information systems.

We defined the structure of ISEDS according to the structure of the documents and Part 2.

2.1 The Documents for Evaluation of ISO/IEC 15408

Applicants who apply to obtain the evaluation of ISO/IEC 15408 have to describe and submit a security target to the evaluation organization. A security target, ST for short, must describe range of a target information system which is evaluated (target of evaluation, TOE for short), assumed threats in TOE, security objectives to oppose these threats, functions required for achievement of these objectives, cf., Fig. 1 on the next page. In particular, the required security functions must be quoted from security functional requirements of Part 2.

A protection profile, PP for short, defines a set of implementation independent IT security requirements for a category of information systems, e.g., OS, DBMS, Firewall, etc. A PP consists, roughly speaking, of threats which may be assumed in the PP's category, security objectives that oppose the assumed threats, and functions required in order to achieve the security objectives. An ST is then created by instantiating a PP. In the documents complying with ISO/IEC 15408, security requirements are analyzed and defined in the above procedure.

2.2 The Structure of Security Functional Requirements

Part 2 has a hierarchical structure which is composed by classes, families, components, and elements in the order (Fig. 2).

Each element is an indivisible security requirement. The components consist of the smallest selectable set of the elements that may be included in specifications. Furthermore, the components may be mutually dependent. The families

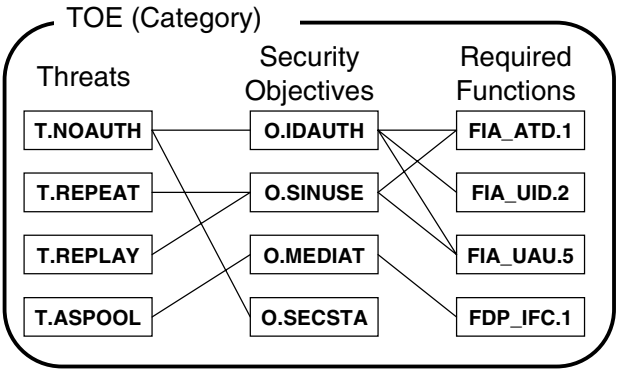

Fig. 1. The document structure of STs or PPs

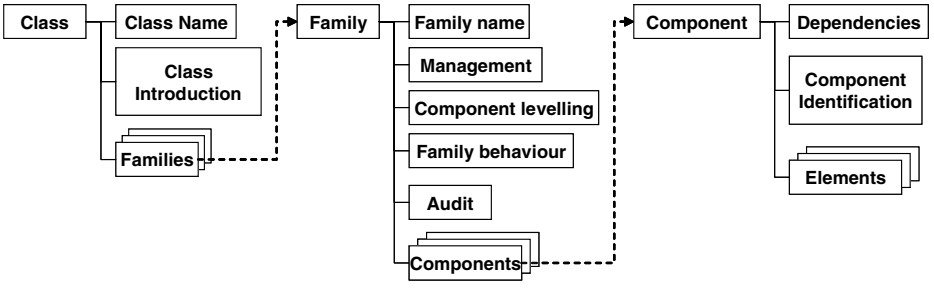

Fig. 2. The hierarchical structure of ISO/IEC 15408 Part2

are a group of the components that share security objectives but may differ in emphasis or rigor. The classes are a group of the families that share common focuses. Security functional requirements exactly and directly are described in the elements of the bottom layer. The following text is one of the security functional requirements.

Class FCO: Communication
This class provides ... (omitted)
FCO_NRO Non-repudiation of origin
Family behavior
...
Management: FCO_NRO.1, FCO_NRO.2
...
Audit: FCO_NRO.1
...
FCO_NRO.1 Selective proof of origin
Hierarchical to: No other components.
FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [assignment: list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]].
...
Dependencies: FIA_UID.1 Timing of identification

This text shows the element FCO_NRO.1.1, the component FCO_NRO.1, the family FCO_NRO, and the class FCO. The element directly describes the requirement in natural language.

We adopted the structure of the documents and the security functional requirements as the structure of ISEDS. Since it is suitable for expressing the above structures, we developed ISEDS as a relational database.

3 Design and Implementation of ISEDS

We designed ISEDS based on the structures mentioned above. The following is the detail of the design and the implementation.

3.1 The Schema Design

We defined the structure of ISEDS as a set of a category, threats, objectives, and functions. We show some examples of STs or PPs in order to clarify the structure. The original text delineating one of the threats in a traffic-filter firewall PP is as follows [5].

> **T.NOAUTH** Illegal access
> An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.NOAUTH specifies that unauthorized persons may attack the system. One of the security objectives which resist this threat is described as follows.

> **O.IDAUTH** Authentication
> The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions. This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.

The other objectives are described as O.SECSTA, O.ENCRYP, O.SELPRO, O.SECFUN, and O.LIMEXT. Contrary, one security objective may resist many threats. Thus, the relationship of threats and objectives is M:M (many to many).

In order to achieve O.IDAUTH, the PP describes that the elements FIA_ATD.1.1, FIA_UID.2.1, FIA_UAU.5.1, and FIA_UAU.5.2 are required. On the other hand, one element may be required for achievement of many objectives sometimes. Thus, the relationship of objectives and elements is M:M as well as threats and objectives.

For implementation of the required elements, an ST must describe that they are actually implemented as what functions in information systems. These functions are called TOE security functions, TSF for short. The following is a certain TSF in an ST of PKI software for smart cards [9].

SF.PINLENGTHMANAGE
SF1
Issuer can set Minimum length of administrator/normal user PIN before issuing the MULTOS smart card. After the MULTOS smart card is issued these values cannot be changed.
SF2
When administrator/normal user tries to change one's PIN and inputs new PIN shorter than Minimum length of administrator/normal user PIN, the TOE denies the change of PIN.

First, an ST describes high level TSFs, e.g., SF.PINLENGTHMANAGE. Next, it details a high level TSF as low level TSFs with top-down, e.g., SF1 and SF2. That is, the relationship of high level TSFs and low level TSFs is 1:M (one to many). Moreover, one element matches many high level TSFs. Contrary, one high level TSF may implement many elements. Thus, the relationship of them is M:M.

As mentioned above, it turns out that entities of ISEDS are classified as follows.

(a) TOEs, **(b)** Threats, **(c)** Security objectives, **(d)** High level TSFs, **(e)** Low level TSFs, **(f)** Classes, **(g)** Families, **(h)** Components, **(i)** Elements

The cardinality of these entities also becomes clear in Table. 1.

Table 1. The cardinality of the entities

	a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
a	-	1:M	1:M	1:M	-	-	-	-	-
b	1:M	-	M:M	-	-	-	-	-	-
c	1:M	M:M	-	-	-	-	-	-	M:M
d	1:M	-	-	-	1:M	-	-	-	-
e	-	-	-	1:M	-	-	-	-	M:M
f	-	-	-	-	-	-	1:M	-	-
g	-	-	-	-	-	1:M	-	1:M	-
h	-	-	-	-	-	-	1:M	M:M	1:M
i	-	-	M:M	-	M:M	-	-	1:M	-

We designed these entities as schemata in a database model based on Fig. 2 and Table. 1 (cf., Fig. 3).

Fig. 3 was drawn with Microsoft Visio Professional 2002. Visio can clearly and easily design accurate database model diagrams in IDEF1X and relational notation [2]. Visio can also automatically generate SQL sentences from the database model diagrams. In Fig. 3, PK denotes primal key and FK denotes foreign key

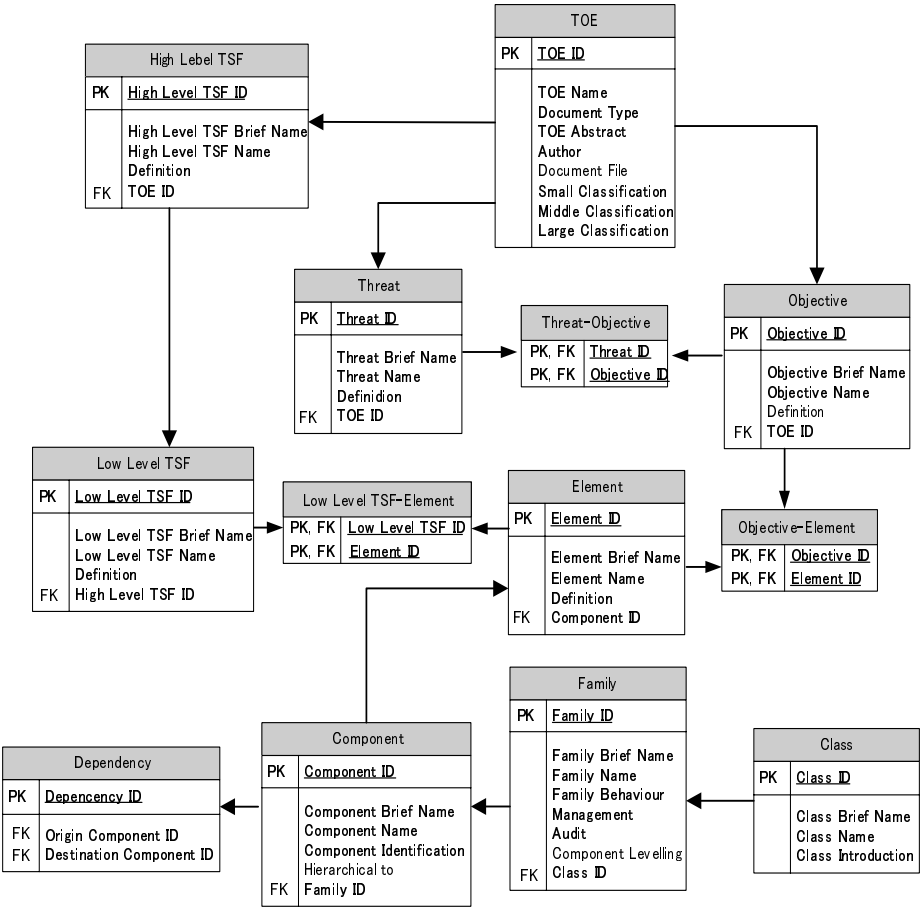

Fig. 3. The database model diagram

in a schema. Attributes in the bold font mean indispensable items of a schema. An arrow denotes a relationship between schemata. The tip of an arrow shows the cardinality M and the starting point of the arrow shows the cardinality 1.

The schema *TOE* has attributes that are written to an ST or a PP, i.e., *TOE Name*, *TOE Abstract*, *Author*, *Small Classification*, *Middle Classification*, and *Large Classification*. The classifications denote TOE kinds. So far, *Large Classification* is only 'IT products' now. *Middle Classification* is 'software,' 'hardware,' 'middleware' etc. *Small Classification* shows the concrete TOE kind, e.g., Database, Firewall, IC card, OS, Copier, and so on. In addition to these attributes, we defined *Document Type* and *Document File*. *Document Type* is a flag for distinguishing an ST or a PP. *Document File* is an attribute for storing the binary file of the ST or PP. *TOE* relates to one or more *Threat*s, *Objective*s, and *High Level TSF*s.

The schemata *Threat*, *Objective*, and *High Level TSF* have their ID numbers, abbreviation names (e.g., T.NOAUTH, O.IDAUTH, or SF.PINLENGTHMANAGE), formal names (e.g., Illegal access or Authentication), texts of the definition on the documents, and foreign keys to *TOE*. The schema *Low Level TSF* is almost the same as these schemata. The schemata of security functional requirements have the attributes shown in Fig. 2. The dependencies of components are expressed as a schema, because they are the M:M self references.

3.2 The Implementation

We implemented ISEDS based on the design with PostgreSQL 8.1, because PostgreSQL is one of the eminent open source databases and can use virtual tables [12]. We stored the data of all security functional requirements in ISO/IEC 15408 Part 2 into ISEDS. Users of ISEDS can easily retrieve their required parts of Part 2. It is not necessary to turn the document exceeding 350 pages one by one.

Moreover, 653 documents about security targets [3] and 125 documents about protection profiles [4] certified by ISO/IEC 15408 are published on the common criteria portal web site as of November, 2005. We also extracted the data of all of them and stored the extracted data into ISEDS. Therefore, the users can retrieve reliable data, i.e., how threats, objectives, and TSFs were described in the certified information systems. Additionally, the users can also retrieve which security functional requirements were used in the certified information systems.

4 Benefits and Applications

ISEDS can be used as follows.

Users can retrieve what threats, objectives, or functions are required in a category of information systems. For example, it can search what threats are assumed in the firewall system category.

```
SELECT T.Threat_Name, T.Definition FROM TOE, Threat T WHERE
TOE.Small_Classification LIKE '%firewall%' AND TOE.TOE_ID = T.TOE_ID
```

The users can retrieve what category assumes threats and what objectives and functions can resist threats. For example, it can search what objectives resist to spoofing.

```
SELECT O.Objective_Name, O.Definition FROM Objective O, Threat T,
Threat-Objective R WHERE T.Definition LIKE '%spoofing%' AND T.Threat ID
= R.Threat ID AND R.Objective ID = O.Objective ID
```

The users can retrieve what objective is a countermeasure against threats and what functions implement an objective. For example, it can search which elements are required for concealment of IP addresses.

```
SELECT E.Element_Name, E.Definition FROM Objective O, Element E,
Objective-Element R WHERE O.Definition LIKE '%concealment of IP address%' AND O.Objective ID = R.Objective_ID AND R.Element_ID =
E.Element_ID
```

The users can retrieve what categories, threats, and objectives require a security function. For example, it can search what categories require the function of IP packet filtering.

```
SELECT TOE.Small_Classification FROM Low_Level_TSF L, High_Level_TSF
H, TOE WHERE L.Definition LIKE '%IP packet filtering%' AND L.High_Level_
TSF_ID = H.High_Level_TSF_ID AND H.TOE_ID = TOE.TOE_ID
```

Besides these retrievals, the users can retrieve what categories, threats, and objectives require an element. Moreover, various retrievals may be possible by using the hierarchical structure of Part 2. For example, it can search what components are dependent on the components in the family FTA_TSE.

```
SELECT C2.Component_Brief_Name FROM Component C1, Component C2,
Family F, Dependency D WHERE F.Family_Brief_Name = 'FTA_TSE' AND
F.Family_ID = C1.Family_ID AND C1.Component_ID = D.Origin_Component_
ID AND D.Destination_Component_ID = C2.Component_ID
```

Naturally, the users can update ISEDS by defining and storing a new security requirement as a set of a category (TOE), threats, objectives, required elements, and TSFs.

We have already proposed a security specification verification technique based on ISO/IEC 15408 [11]. We beforehand formalized all elements of ISO/IEC 15408 Part 2 as formal criteria [1]. The technique enables strict verification using formal methods and the formal criteria. With the technique, one can strictly verify whether or not information systems designed by ISEDS satisfy the elements of ISO/IEC 15408. Conversely, users of the technique can retrieve elements which are required in the certified information systems similar to a verification target information system. The weakness of the technique is that the users must decide by themselves which elements are necessary to target information systems. ISEDS solves this problem.

Additionally, we have proposed a method which simplifies creation of a security specification in information systems [10]. In the paper, we successfully classified and rearranged PPs in order to make them possible to more efficiently use. The advantage of the method is that even a developer who is relatively inexperienced in security issues can easily create specifications which satisfy security criteria with the rearranged PPs, because PP's security has been guaranteed by ISO/IEC 15408. However, it is hard to rearrange PPs, because it must be carefully considered with reference to many PPs. ISEDS also solves this

problem. Because of this contribution, anyone can easily improve PPs and may solve various security issues of information systems by the improved PPs.

5 Concluding Remarks

In order to apply database technologies to information security engineering, we have designed and developed ISEDS, a security requirement management database based on the international standard ISO/IEC 15408. Users of ISEDS can collect, manage and reuse security requirements for design and development of various information systems in the form according to ISO/IEC 15408. Since we already stored all data of ISO/IEC 15408 Part 2 into ISEDS, the users can also get their required information of Part 2 without reading vast pages of Part 2 document. Thus, ISEDS can mitigate their labor for design and development of secure information systems. ISEDS can also support design and development of information systems which satisfy the security criteria of ISO/IEC 15408. It is verifiable by our verification technique [11]. ISEDS may be applicable to various purposes. We also expect that ISEDS will be a good example for "database-izing" criteria like ISO standard. We are preparing a web site in which users can use ISEDS [1].

A subject of ISEDS is consistency of the data. Definition of threats, security objectives, and security functions in STs or PPs is different for every document case by case. Moreover, some information systems do not have clear classification. Because of the problem, retrieval of required data may be difficult. Thus, we need to define further common format for such data.

Furthermore, the structure of STs, PPs, security requirements, and the security functional requirements can be easily, exactly and rigorously expressed in XML. Therefore, we are improving ISEDS as a native XML database into which users can directly store the XML documents and are developing its web service.

References

1. Advanced Information Systems Engineering Laboratory, Saitama University.: ISEDS: Information Security Engineering Database System. http://www.aise.ics.saitama-u.ac.jp/
2. Bruce, T.A.: Designing Quality Databases with IDEF1X Information Models. Dorset House Publishing Company (1991)
3. Common Criteria Portal Org.: Evaluated product files. http://www.commoncriteriaportal.org/public/files/epfiles/
4. Common Criteria Portal Org.: Protection profile files. http://www.commoncriteriaportal.org/public/files/ppfiles/
5. Dolan, K., Wright, P., Montequin, R., Mayer, B., Gilmore, L., and Hall, C.: U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments. National Security Agency (2001)
6. International Software Benchmarking Standard Group.: Empirical Databases of Metrics Collected from Software Projects. http://www.isbsg.org/

7. ISO/IEC 15408 standard.: Information Technology - Security Techniques - Evaluation Criteria for IT Security (1999)
8. Jiao, J. and Tseng, M.: A Requirement Management Database System for Product Definition. Journal of Integrated Manufacturing Systems, Vol. 10, No. 3, pp. 146-154 (1999)
9. Miyazawa, T. and Sugawara, H.: Smart Folder 3 Security Target Version: 2.19. Hitachi Software Engineering Co., Ltd., January (2004)
10. Morimoto, S. and Cheng, J.: Patterning Protection Profiles by UML for Security Specifications. Proceedings of the IEEE 2005 International Conference on Intelligent Agents, Web Technology and Internet Commerce (IAWTIC'05), Vol. II, pp. 946-951, Vienna, Austria, November (2005)
11. Morimoto, S., Shigematsu, S., Goto, Y., and Cheng, J.: A Security Specification Verification Technique Based on the International Standard ISO/IEC 15408. Proceedings of the 21st Annual ACM Symposium on Applied Computing (SAC'06), Dijion, France, April (2006)
12. PostgreSQL Global Development Group.: PostgreSQL. http://www.postgresql.org/
13. Software Engineering Institute.: Software Engineering Information Repository. http://seir.sei.cmu.edu/