A Security Specification Verification Technique Based on the International Standard ISO/IEC 15408

Shoichi Morimoto, Shinjiro Shigematsu, Yuichi Goto, and Jingde Cheng
Department of Information and Computer Sciences
Saitama University, Saitama, 338-8570, Japan
{morimo, shigematsu, gotoh, cheng}@aise.ics.saitama-u.ac.jp

ABSTRACT
This paper proposes a security specification verification technique based on the international standard ISO/IEC 15408. We formalized the security criteria of ISO/IEC 15408 and developed the verification technique of security specifications based on the formalized criteria with formal methods. With the technique, one can formally verify whether or not specifications satisfy the security criteria of ISO/IEC 15408. Ambiguity and/or oversight about security in specifications written in natural language can also be detected.

Categories and Subject Descriptors
D.2.4 [Software Engineering]: Software/Program Verification—Formal methods

General Terms
Security, Verification

Keywords
Common Criteria, Z notation, Theorem-proving

1. INTRODUCTION
Security specifications and their verification have become an important issue in information security engineering. However, it is not clear what security criteria are, and it is difficult to define security criteria. In order to solve the problems, we propose adopting the international standard ISO/IEC 15408 as the criteria of the security which should be applied to validate an information system. ISO/IEC 15408 was established as a set of criteria for evaluating the security level of IT products [5]. However, because ISO/IEC 15408 is written in natural language, it is difficult to use ISO/IEC 15408 in formal verification of security specifications.

In this paper, we propose a security specification verification technique based on ISO/IEC 15408 with formal methods. We formalized beforehand all 251 criteria of ISO/IEC 15408 as formal criterion templates which are necessary to any verification of security specifications based on ISO/IEC 15408. For the formalization, we used Z notation [4, 10], one of the formal methods, which have produced actual results in the verification of software reliability with theorem-proving [2].

2. THE VERIFICATION TECHNIQUE
Here we describe the verification technique and the formalized criteria of ISO/IEC 15408.

2.1 Outline of the Verification Technique
The following is the procedure of the verification technique.
1) Select required formalized criteria (templates).
2) Formalize the specification of a target system in Z.
3) Materialize the selected criterion templates.
4) Verify the formalized specifications against the materialized criteria.

To verify a security specification of a target system, users first select criterion templates which are required in the system. Secondly, the users formalize the specification of the system in Z, somewhat taking the selected criterion templates into consideration. In the third step the users must materialize the selected criterion templates in order to fit them into the formalized specification. Then the users verify whether or not the materialized criteria are deducible from given axioms and the formalized specification as premises with theorem-proving, e.g., the verification tool Z/EVES [6].

2.2 The Formal Description of the Criteria
In order to explain how the criteria were formalized, we show a formalization example of a criterion in ISO/IEC 15408. The original text of the criterion FDP_RIP.1.1 is as follows.

FDP_RIP.1 Subset residual information protection
FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] the following objects: [assignment: list of objects].

In the original text, TSF means a security function of systems, the selection is the specification of one or more items from a list in the systems, and the assignment is the specification of an identified parameter in the systems. Thus,
the criteria of ISO/IEC 15408 are very abstract. It is probably impossible to understand at a glance, what is meant. The detailed usage of them is not described in themselves. Therefore, we formalized the criteria as templates after we had extracted the substantive meaning of them in the context of many actual public specifications [3] for which it is used.

FDP, RIP.1.1 specifies that systems must make any previous information content of a resource unavailable, when allocation of the resource to the following objects or deallocation of the resource from the following objects occurs. In other words, after allocation or deallocation occurs, it is impossible to refer to all previous information content of a resource. The following is the formula in Z converted from this interpretation.

**Template:** FDP_RIP.1.1
∀ System | Allocation or deallocation operation • ∀ previous information content ∈ Resource • unavailability conditions

This template formula means that after performing Allocation or deallocation operation, it is safe to say that all previous information contents included in Resource satisfy unavailability conditions in System.

Thus, all 251 criteria of ISO/IEC 15408 were formalized as templates.

### 2.3 Materialization of the Criteria

The formalized criteria are merely templates so that any specification can use them. Therefore, when using them, users have to materialize them to fit each target system. Here we describe the way of the materialization.

In the templates, an italic bold word denotes a state schema, a bold word denotes an operation schema, an italic word denotes a set, a sans-serif font word denotes a logic expression or a type schema, a normal font word denotes the other component in Z specifications. For example, there are the following template and Z specification, provided that they do not have any meaning.

∀ State': variable | An_operation • elements ∈ Set ∧ conditions

When this template is materialized so that it can fit into this specification, State can be replaced by the state schema Object, An_operation can be replaced by the operation schema Operation, Set can be replaced by the set entity2, conditions can be replaced by the type schema Type or a logical expression which consists of components in the Z specification, variable can be replaced by the entities entity1 or entity2 in Object, elements can be replaced by the element entity1 which can be included in the set entity2. Users verify whether or not the formula that is materialized in this way is deducible in the Z specification by theorem-proving.

### 3. CONCLUDING REMARKS

In this paper, we have proposed a security specification verification technique based on the international standard ISO/IEC 15408. With this verification technique, one can verify whether or not specifications satisfy the criteria of ISO/IEC 15408. Verifiers do not need to make verification criteria from scratch. At least, specifications verified by the verification technique can be considered to be security specifications certified by ISO/IEC 15408. Moreover, since the criterion templates of ISO/IEC 15408 in Z are represented by first-order predicate logic, the verification technique may also be applied to other formal descriptions. We are considering so that the templates can be used not only by Z but by all formal methods.

Since the technique is not suitable for verification of dynamic behavior in systems, we have tried to introduce model-checking to the technique [9]. When users use the technique, they then must select required criteria and formalize target specifications. However, it is not so easy. Therefore, we have developed a database that stores dependencies of the required criteria and system categories and supports the selection of the required criteria [1]. Additionally, we have proposed a method which simplifies creation and formalization of security specifications [7] and have verified the specifications using the method by the technique [8].

### 4. REFERENCES


