Research on verification by the theorem proof of the data security in an organization

Taku Tokuda (410086)

School of Information Science,
Japan Advanced Institute of Science and Technology

February 9, 2006

Keywords: jaist-e-master-abstract.sty, title, author, school, keywords.

1 Background and Purpose

It is important to realize "high reliability society" for economy or society. An information security is maintaining reliability. " Information security " means to keep " confidentiality " , "integrity " and "availability ". The Common Criteria (ISO/IEC 15408) is the set of IT security standard. The CC is applicable to IT security measures implemented in hardware, firmware or software. Protection Profile (PP) and Security Target (ST) are specifications made based on a set of security requirements from the CC. And they are examined and approved. So it is said that approved PP and ST are design specifications which are meeting the standard of security.

On objective oriented development , the analysis model of a system is built by the modeling language represented by UML. Research of formal verification, such as model checking, theorem proof, etc. to show guaranteeing that a system fulfills specification, is done. Yatake and others built the object-oriented theory for the proof based on the collaboration between objects as a theoretical module on the theorem prover HOL. It proves that a system fills the security demand a system is indicated to be by ST. The purpose of research is proving filling the security and functional demand a system is indicated to be by specification based onST.

2 Procedure of research

It is premised on existence of ST of FW server system, and Technology which forms object-oriented theory into a theoretical module on a theorem prover HOL in this research.

This research advanced research in the following procedures.

- assume the specifications according to ST of FW server system.
- make a model by UML based on specifications, and make a class figure and a collaboration figure.
- code in ML form what was modeled using object-oriented theory.
- do an easy execution test using ML compiler. and remove a bug which happens by coding.
- rewrite a code in HOL form.
- set up a proposition in the predicate on a system for proving the contents of specifications.
- prove a proposition by the deductive technique on HOL.

ST of FW server system is written by natural language and drawn by figures and tables. FW server system is realized by the basic function of packet filtering, identification and authentication, and audit, and the access control function to them. About the basic function of packet filtering, identification and authentication, and audit, the model was made so that the contents of specifications might be realized. Moreover, the concept of Role Based Access Control was taken in and modeled about the access control function.

The object-oriented model in ML form and HOL form is realized by the logic module which makes object-oriented theory possible. Thereby, a concept object-oriented in a HOL top can be used.

It proved by making into a proposition whether for the function of a model to fill the demand of specifications. Thereby, when it cannot prove, it can be shown that a model does not fill a security demand and a functional demand, and the fault of a model can be pointed out. Moreover, a

model can prove filling the security demand shown by ST, and a functional demand by the ability proving. Fulfilling the specification shown by ST means that fulfilling the standard of security. Thereby, the model which is filling the security demand and the functional demand can be obtained. In addition to the setup of the general proposition by eternal manifestation and the deductive technique, a setup of some propositions was proposed and proved in this research. These were able to show that the model was filling some security functions. However, since big human and time cost is required for verification, it did not come to be shown that the model is filling the demand of all specifications correctly. ST mainly consists of natural language, a figure, a table, etc. The essential portion of this research is how to choose the contents which should be proved from these specifications, and how to express as a logic type.

3 Result

A setup of a proposition by eternal manifestation and the proof by induction are general methods in theorem proof. However, just this is insufficient for making the proposition about a security demand or a functional demand. From now on, we have to consider the contents which can be proved to be the expression method by the logic type.

4 Future work

The work of the proof by HOL spends very big human and time cost. Utilization is impossible if unreal cost is required, though theory is right and can prove correctly about the contents of ST how much. From now on, the research on a tactics which performs proof more efficiently, and research of automation will be required.