Application of Aspect-Oriented Technology to the Security Verification by Model Checking Technology

Hiroyuki Kosaka (0710029)

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

February 5, 2009

Keywords: Misuse case, Security, Aspect, Model Checking.

This paper discusses the design approach for improving the security of software using aspect-oriented technolory.

In recent years, various devices are connected to networks, and this makes the software security more and more important. In the field of Security Requirements Engineering, the idea of the "misuse case" that describes undesirous situation for a system is studied, and is used for the extraction of the potential threat for a system.

On the other hand, in Software Engineering field, the reserarch on method for developing secure software is also examined. In the field, a study dealing with a misuse case or an aspect-oriented technology is also performed. For example, there proposed a design method for secure software in which they utilize aspect oriented technologies with the scenario.

We believe that scenario in the designing method is good understandability. However, a state machine diagram is well used for a design, therefore, related research has low affinity with that case.

In this study, we propose an approach in which we design the system using state machine diagram. The feature of the proposal technique is that it altered the system model to the state machine diagram base from the scenario base.

In this related work there proposed important concepts. In our research, we use the following concepts: A misuse case and mitigation use a sce-

nario, "sequence pointcut" that defines a pointcut in a mitigation scenario in terms of the sequence of messages. "Any fragment" that defines any sequence of messages.

In this study, we propose a technique of weaving an aspect scenario into state machine diagrams. In order to achieve the approach, it is necessary to identify positions pointed out by "a sequence pointcut" specified on an aspect scenario on the state machine diagram. We utilize SPIN model checker to exhaustively check behavior specified by state machine diagram to identify these positions. Though SPIN is originally a tool for verifying the correctness of a design of software, we utilize this capability to carrying out complete coverage search of all the states of an test subject. By utilizing SPIN to execute complete coverage search of all the possible execution paths denoted by state machine diagrams using the feature, we inspect places on state machines that corresponds to "sequence pointcut". As the model which can be inputted into SPIN is a Promela language, processing to convert the state machine diagram into Promela is performed. The processing is performed in an manual.

By the above approach, it was possible to identify positions in the state machine diagram that correspond to positions on aspect scenario pointed out by the pointcut. Weaving processing of the aspect scenario is performed with respect to the analyzed pointcut on the Promela.

Here, an Aspect Promela tool supporting weaving on Promela is used. This Aspect Promela is a tool developed by Ohno in our laboratory. We define the weaver proposed by this study, which has tasks from analysis of the real matrices of the state machine diagrams by SPIN to application of Aspect Promela.

In order to evaluate the availability of the proposed approach, we have applied it to an electronic voting system example. We have prepared voting system and a scenario that represents a threat to the system. Then, we define mitigation scenario and weave the scenario the voting system. As a result, we can weave it at places specified by the aspect scenario. We can also verify that weaved voting system can avoid the threat. Also, it was confirmed that the weaved system had a design for preventing the thread, by a verification experiment.