Proceedings of the 2012 Winter Simulation Conference
C. Laroque, J. Himmelspach, R. Pasupathy, O. Rose, and A.M. Uhrmacher, eds

A MODELING METHODOLOGY FOR CYBER-SECURITY SIMULATION

Ji-Yeon Kim and Hyung-Jong Kim

Seoul Women's University
621 Hwarangro, Nowon-Gu
Seoul, Republic of Korea

ABSTRACT

With the increasing occurrence of various cyber-attacks such as distributed denial of service (DDoS) and worm attacks, simulations are being used to develop security techniques and policies against such attacks. In a cyber-security environment, there are many entities that have different resources and behaviors; attack and defensive behaviors are exhibited upon interaction with other entities. In order to design simulation models for various cyber-security simulations, not only a generalized model that can represent various attacks and target entities but also a modeling method that considers different types of interactions between entities to make simulation models should be developed. In this paper, we describe a modeling methodology for the cyber-security simulation based on discrete event system specification (DEVS) formalism.

1 CYBER-SECURITY MODELING AND SIMULATION (CYBERSECURITY M&S)

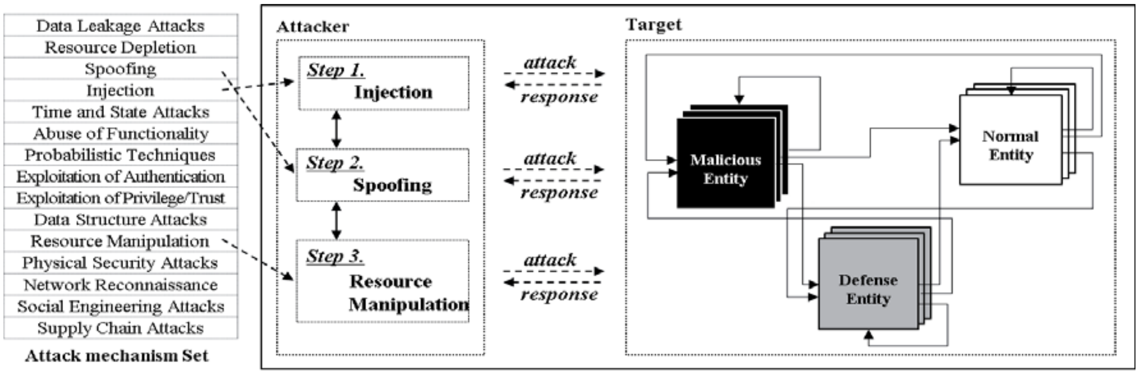

Figure 1. A **cyber-security** environment and components

Problem definition – There are various mechanisms of cyber-attacks, each of which can be composed of two or more mechanisms. As shown in figure 1, an attacker interacts step by step with a target composed of various entities; the result of each step can be a critical factor that determines the final result. With regard to the target, entities have different responses to an attack depending on their inherent characteristics, such as vulnerability and capability to defend or attack. In addition, these characteristics can be changed as the attack progresses. Therefore, it is necessary to develop a simulation model that can observe interactions between an attacker and a target as well as represent various attack mechanisms and characteristics of targets.

Objectives – A cyber-security simulation can be modeled using a modeling methodology for discrete event system, because the simulation progresses based on the interactions that have occurred during attack events. Using this methodology, we can trace changing state variables of an attacker and the target models during the simulation. In this study, we use the discrete event system specification (DEVS) formalism for the modeling, and suggest a method for developing a DEVS atomic model considering various characteristics of entities and their interactions.

978-1-4673-4781-5/12/$31.00 ©2012 IEEE

2 DEVS MODELING OF CYBER-SECURITY SIMULATION

Design of entities – Attributes of entities can be classified into physical and behavioral attributes. All entities can have physical attributes such as identification and resources, whereas behavioral attributes can be found in entities that can trigger events. In this paper, we define two types of entities, *subject* and *target*.

- *Subject* – an active entity that can manipulate other entities, *e.g.*, thread, process, system, and network.
- *Target* – a passive entity that can only be manipulated by a *subject*, *e.g.*, application, file, code, command, etc.

In the behavioral attributes of figure 2 (a), *intention* and *target* denote a characteristic and the target in the event, respectively. In addition, the *action*, an attribute of *behavior,* denotes event types; changing the value of *action* corresponds to a change of events.

Modeling of DEVS atomic model – We can develop an atomic model by considering the location of the *target* of a *subject* and whether the *target* is shared by other *subjects*. As shown in (b) of figure 2, if each *target* of *subject 1* and *subject 2* is located in itself, it can act as an atomic model and its events can be scheduled by that *subject.* Schematic (c) of figure 2 shows a situation where an entity can be both the *target* and the *subject*. In this situation, the *target* of *subject 2* is shared with *subject 1*. Finally, (d) shows a *target* entity located out of *subjects* that is shared by more than two *subjects*. As demonstrated using (c) and (d), an atomic model can be composed of multiple entities, and in order to schedule events considering the results of interactions between entities in the atomic model, state mapping between the model and entities is needed.

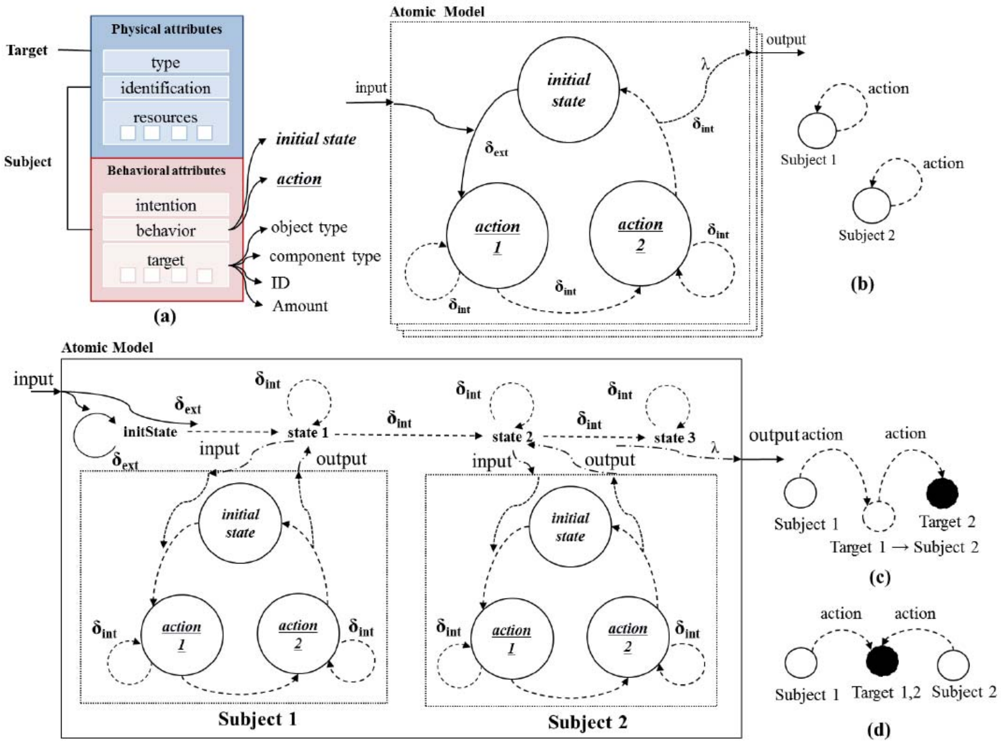

Figure 2. Modeling of a DEVS Atomic model considering the location of target and resource sharing

REFERENCES

Innacio J. Martinez-Moyano et el., “Modeling behavioral considerations related to information security”. Computers and Security, vol. 30, pp. 397-409, 2011.

Common Attack Pattern Enumeration and Classification (CAPEC), 2012. [Online]. Available: http://capec.mitre.org/

Igor Kotenko, “Agent-based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet”. Proceedings 19th European Conference on Modelling and Simulation, 2005.

B.P. Zeigler et el., Theory of Modeling and Simulation. 2nd edition, Academic Press, 2000.