SECUSIM: A Tool for the Cyber-Attack Simulation

Jong Sou Park, Jang-Se Lee, Hwan Kuk Kim,
Jeong-Rye Jeong, Dong-Bok Yeom, and Sung-Do Chi

Department of Computer Engineering
Hangkong University, Seoul, KOREA
{jspark, jslee2, rinyfeel, harusali, dbyeom,
sdchi}@mail.hangkong.ac.kr

Abstract. The cyber attack simulation tool, SECUSIM, is presented for specifying attack mechanisms, verifying defense mechanisms, and evaluating their consequences. The tool has been successfully developed by employing the advanced modeling and simulation concepts such as SES/MB (System Entity Structure / Model Base) framework, DEVS (Discrete Event System Specification) formalism, and experimental frame. SECUSIM is currently implemented on the basis of Visual C++ and enables a simulation of twenty attack scenarios against hundreds network components.

1 Introduction

As we increasingly rely on information infrastructures to support critical operations in defense, banking, telecommunication, transportation, electric power and many other systems, cyber attacks have become a significant threat to our society with potentially severe consequences [1]. A computer and network system must be protected to assure security goals such as availability, confidentiality and integrity. That is, the deep understanding of system operation and attack mechanisms is the foundation of designing and integrating information protection activities [2]. Therefore, the advanced modeling and simulation methodology is essential for classifying threats, specifying attack mechanisms, verifying protective mechanisms, and evaluating their consequences. That means, we need to establish the advanced simulation system for analyzing vulnerabilities of given infrastructure as well as the expected consequences of successful attacks and the effect of the defense policy [3].

Cohen [3], who was a pioneer in the field of network security modeling and simulation, interestingly suggested a simple network security model. However, cyber attack and defense representation that is based on cause-effect model [3] is so simple that practical difficulty in application comes about. Amoroso suggested that the intrusion model [4] should be represented by sequence of actions, however, the computer simulation approach was not considered clearly. Wadlow [5] suggested an intrusion model, but it failed to go beyond the conceptual modeling level. Finally, Nong Ye [2] noticeably proposed a layer-based approach to complex security system, but failed to provide a practical modeling and simulation techniques of the relevant layers.

S. Qing, T. Okamoto, and J. Zhou (Eds.): ICICS 2001, LNCS 2229, pp. 471-475, 2001.

In order to deal with those restrictions and limitations, we have been successfully developed the network security simulation tool, SECUSIM, that is able to specify attack mechanisms, verify defense mechanisms, and evaluate their consequences. To achieve this, we first have defined the node and link vulnerability metrics for providing the proper mechanisms for evaluating the given information infrastructure. Then behaviors of the cyber-attack, defense, and consequences are coherently characterized within the state transition diagram of discrete event model. We also proposed the functional level of modeling complexity so that we can make it not too complex but meaningful enough. Such a functional level has been successfully developed using the hierarchical and modular discrete event simulation environment underlying DEVS formalism [6,7,8].

2 Simulation Methodology

Fig.1 shows the overall methodology using the SES/MB [6]. Phase I represents the conceptual specification stage, in which the decomposition, taxonomies, coupling specification and constraints of given information network system can be specified by SES (System Entity Structure) [6]. In Phase II, the network component models as well as the attacker models, and analyzer models can be built through DEVS (Discrete Event System Specification) formalism [6,7] and saved into MB (Model Base). Especially, based on this basic behavior model for network component, command-level modeling using pre/post-condition can be accomplished by grouping and characterizing of commands that are used in various services. In phase III, the simulation model may be constructed by integrating the dynamic models in MB along with the network structure of the SES so that the cyber attack simulation can be performed. Finally, the simulation result can be analyzed in Phase IV so that the security characteristics and policies of each network component may be evaluated [8].

3 Main Features of SECUSIM

SECUSIM is currently implemented on the basis of Visual C++ and enables a simulation of twenty attack patterns against hundreds network components. The software architecture of SECUSIM (Fig. 2) consists of the following five modules;

- **GUI**: It basically has the functionality for initialization and modification of network components attributes based on the simulation condition and result. It also supports the packet level graphic animation during simulation.
- **Network Configurator**: It provides graphic editing capabilities for constructing the network structure.
- **Simulation Engine**: It proceeds the simulation by executing the network component models based on the given attack scenario. It also produces the simulation results for the GUI.

- **Component Model Base**: It is a model base that contains behavior characteristics represented by DEVS formalism. It basically consists of various servers, routers, gateways, firewalls, links, etc.
- **Attack Scenario Database**: It is a database that contains command-level cyber attack scenarios in order to inject the cyber attack commands to the given network via simulation.

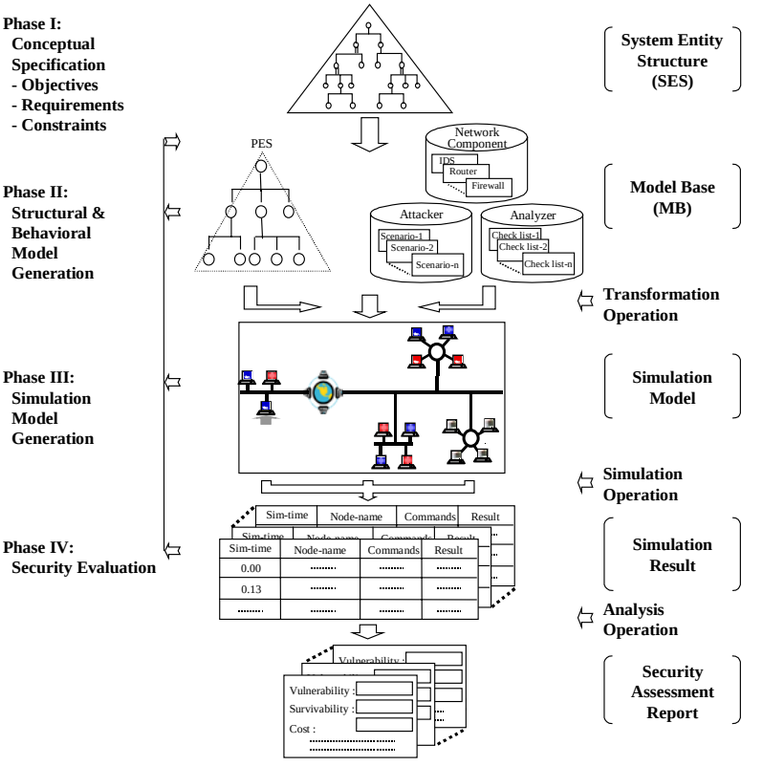

Fig. 1. Overall methodology

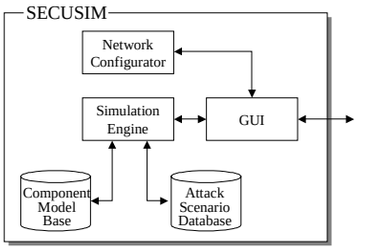

Fig. 2. The software architecture of SECUSIM

SECUSIM supports five modes of usages for allowing the step-by-step analysis (see Fig.3) as follows;

(1) *Basic Mode*: It provides basic knowledge of cyber-attack mechanisms by retrieving the scenario database.
(2) *Intermediate Mode*: It allows the cyber attack simulation of a given network by selecting arbitrary attacker model and target host as well as setting the attack scenario.
(3) *Advanced Mode*: It support for direct command-level testing of given cyber-attack into the given network models.
(4) *Professional Mode*: It provides advanced analysis for link and node vulnerability of given network by allowing multiple cyber-attack simulation.
(5) *Application Mode*: It allows graphic editing capabilities for users to create and simulate their own network configurations.

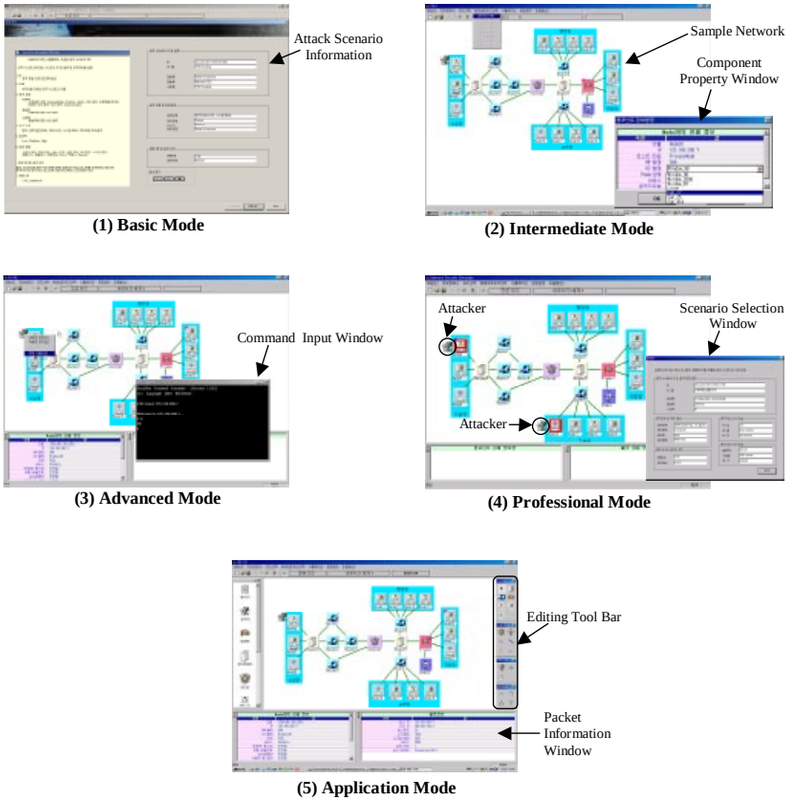

Fig. 3. Screen copies of 'SECUSIM'

4 Conclusions

We have successfully developed the cyber attack simulation tool, SECUSIM, that is able to specify attack mechanisms, verify defense mechanisms, and evaluate their consequences. The tool takes advantage of a hierarchical and modular modeling and simulation environment so that it efficiently supports to construct the security model as well as to analyze node and link vulnerabilities of given network model through simulation. SECUSIM is currently implemented on the basis of Visual C++ and enables a simulation of twenty attack patterns against hundreds network components. We leave here future further studies for automated model generation and also identification of unknown cyber-attacks through the simulation.

Acknowledgements. This work is in part of "Support Project of University Information Technology Research Center" supported by the Ministry of Information & Communication of Korea (supervised by IITA) and in part of "Internet Information Retrieval" Regional Research Center Program supported by the Korea Science and Engineering Foundation.

References

1. T. A. Longstaff, Clyde Chittister, Rich Pethia, Yacov Y. Haimes, "Are We Forgetting the Risks of Information Technology", IEEE Computer, pp 43-51, December, 2000.
2. N. Ye, C. Hosmer, J. Giordano, J. Feldman, "Critical Information Infrastructure Protection through Process Modeling and Model-based Information Fusion", Proceedings of the Information Survivability Workshop, 1998.
3. F. Cohen "Simulating Cyber Attacks, Defenses, and Consequences", IEEE Symposium on Security and Privacy Special 20th Anniversary Program, Berkeley, CA, May, 1999.
4. E. Amoroso, Intrusion Detection, AT&T Laboratory, Intrusion Net Books, January, 1999.
5. T. A. Wadlow, The Process of Network Security, Addison-Wesley, 2000.
6. B. P. Zeigler, Object-oriented Simulation with Hierarchical, Modular Models: Intelligent Agents and Endomorphic systems, Academic Press, 1990.
7. B.P. Zeigler, Multifacetted Modeling and Discrete Event Simulation, Academic Press, 1984.
8. S. D. Chi, J. S. Park, K. C. Jung, J. S. Lee, "Network Security Modeling and Cyber-attack Simulation Methodology", Lecture Notes on Computer Science series, 6th Australian Conf. On Information Security and Privacy, Sydney, July, 2001.