Information System Modeling for Analysis of Propagation Effects and Levels of Damage

InJung Kim¹, YoonJung Chung², YoungGyo Lee¹, Eul Gyu Im³, and Dongho Won¹,*,**

¹ Information Security Group, School of Information and Communication Engineering, Sungkyunkwan University
cipher@etri.re.kr, {yglee, dhwon}@security.re.kr
² Electronics and Telecommunications and Research Institute
yjjung@etri.re.kr
³ College of Information and Communications, Hanyang University
imeg@hanyang.ac.kr

Abstract. The number of newly developed information systems has grown considerably in their areas of application, and their concomitant threats of intrusions for the systems over the Internet have increased, too. To reduce the possibilities of such threats, studies on security risk analysis in the field of information security technology have been actively conducted. However, it is very difficult to analyze actual causes of damage or to establish safeguards when intrusions on systems take place within the structure of different assets and complicated networks. Therefore, it is essential that comprehensive preventive measures against intrusions are established in advance through security risk analysis. Vulnerabilities and threats are increasing continuously, while safeguards against these risks are generally only realized some time after damage through an intrusion has occurred. Therefore, it is vital that the propagation effects and levels of damage are analyzed using real-time comprehensive methods in order to predict damage in advance and minimize the extent of the damage. For this reason we propose a modeling technique for information systems by making use of SPICE and Petri-Net, and methods for analyzing the propagation effects and levels of damage based on the epidemic model.

Keywords: Risk analysis, Intrusion, Damage propagation, Safeguard, Epidemic.

1 Introduction

Security risk analysis [1] of information systems is the best means of eliminating vulnerabilities from information security services and safely controlling the systems against potential threats. Currently, information systems operate in various environments with extended areas, a large number of assets and interoperations with heterogeneous systems such as controlling systems. This situation has enabled risk analysis

* Corresponding author.
** This work was supported by the University IT Research Center Project funded by the Korean Ministry of Information and Communication.
simulation of information systems to emerge as a field of keen interests and to bring innumerable studies and discussions. An important prerequisite to perform simulations is to create an environment in which analysis of the propagation effects and levels of damage to information systems can be analyzed. In such a simulated environment, an analysis of the activities on information systems, resources and information flow should be conducted in order to evaluate the affects of cyber intrusions on the information systems. For the analysis of activities on information systems, we model information systems through the SPICE model [3] and Petri-Net [4] for circuit design, and analyze propagation effects and levels of damage by applying the epidemic model [2][24]. The epidemic model has been studied for the propagation of worms; we will use the model to analyze all cyber intrusions as well as worms.

It is normally difficult to identify which intrusion causes damage. Once an intrusion takes place, the related functions of the information system are degraded, or the intrusion shuts down some of information systems. After recognizing the symptoms, system administrators will begin to establish safeguards for the damage. Once these safeguards have been established, recovery procedures for the affected systems may begin. Meanwhile, damage from the intrusions might have been propagated to other systems via unspecified routes, and the scope of the damage increases accordingly. In such a case, damage continues to occur until safeguards are established to prevent future intrusions.

Therefore, we propose a modeling mechanism to assist the analysis of possible intrusions in advance. Our proposed modeling mechanism will help system administrators to analyze cyber threats and establish effective safeguards for prevention and recovery from intrusions.

2 Related Work

2.1 Information System Modeling

In the most organizations, information systems are modeled to show network configurations simply using Microsoft PowerPoint or VISIO. This type of modeling is capable of showing the current status and connection features of assets only; thus, it is difficult to analyze damage propagation using this kind of modeling, since the modeling is not capable of showing job flows or predicting the propagation effects of damage occurred. Flow charts or state transition diagrams can be used to identify information flow, but these approaches have limitations to analyze and identify threats from the overall network configurations of information systems. More recently, the state transition diagrams [5] have been extended for direct representation of sequence and elements of events as well as simple illustration of behaviors and results of cyber intrusions in the systems through Deterministic Finite State Machine (DFSM) [6] or Colored Petri-Net [7]. The state transition diagram approach configures only the effects and damage routes of cyber intrusions, so it has some limitations in risk analysis: This approach is not capable of incorporating the unique features of respective assets when representing the information system as a model, and this approach illustrates the distribution of damage unevenly according the directions of propagation. To overcome these shortcomings, the SPICE model has been introduced to analyze transient effects.