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

InJung Kim[1], YoonJung Chung[2], YoungGyo Lee[1], Eul Gyu Im[3], and Dongho Won[1,*,**]

[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.

M. Gavrilova et al. (Eds.): ICCSA 2006, LNCS 3982, pp. 54 – 63, 2006.

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.

2.2 SPICE Modeling

The Simulation Program with Integration Circuit Emphasis, or SPICE [8], is a program to simulate simple electronic circuits based on equivalent circuits for the respective elements. With SPICE, users can design, edit, and simulate electronic circuits, and users can compile characteristics of elements and circuit configurations in a library for later analysis. However, the SPICE model may contain excessive unnecessary information assets to cover each asset in the entire information systems and may contain more complex designs than network layouts. This may cause difficulties in analysis of the routes for cyber intrusions and damage incurred by the intrusions. Therefore, a new modeling technique is required for simple and easy analysis of damage routes, so that the modeling technique can be used for risk analysis of information systems.

2.3 Risk Analysis

Many studies on risk analysis of information systems are currently in progress in different fields. The major three domains are as follows:

- Risk analysis processes and risk-level calculation
- Design and development of risk analysis tools
- Studies on control items and guidelines

Several risk analysis processes have been developed, including GMITS [9], CSE (Communications Security Establishment) [10], HAZOP (Hazard and Operability study) [11], FTA (Failure Model and Effect Criticality Analysis) [12], OCTAVE [13], and CORAS [14]. In Korea, a process called PRAHA [15] has been developed and utilized for analysis and assessment of vulnerabilities of systems in governmental or public organizations. Risk analysis tools include CRAMM (CCTA Risk Analysis and Management Methodology) [16], BDSS [17], and Buddy System [18]. The BS7799 [19] and IT Baseline Protection Manual from BSI [20] are under study for control items and calculation of criteria. Most of the above processes or tools can be used for risk analysis; however, they are somewhat limited in their analysis of the scope of damage and effects caused by intrusions.

2.4 Intrusion Damage Estimation

The damage calculation proposed in [21] simply calculates the values of damaged assets, labor costs, recovery expenses in a quantitative manner for the duration of intrusions. This methodology does not really contain a technique for real-time analysis of the rapid changes in information systems because of different intrusion accidents; nor is it capable of analyzing the routes and affects of damage incurred. Some studies [22] are currently in progress to analyze the extent of damage using the propagation model for worms by making use of certain epidemic models [2], and estimate the levels of damage through real-time analysis of the availability of information systems. However, no study on overall damage propagation has yet been completed.

3 Information System Modeling

The modeling of information systems is a must for the analysis of the propagation effect and level of damage caused by intrusion. To model systems, it is necessary for the target systems and assets to be defined, while the functional restrictions of systems such as objectives and configuration shall be explicitly specified. However, the authors of the study illustrate the mutual reliance between the assets comprising a system and the similar functions of the assets in a block diagram [23]. To do this, the authors illustrate system modeling as shown on Fig. 1, define the elements as follows:

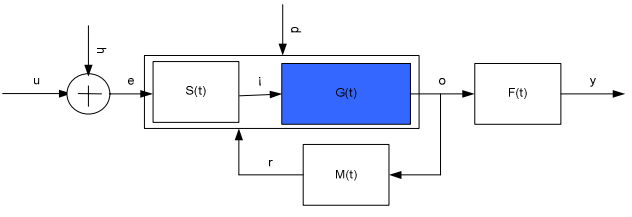

Fig. 1. Structure of information system

Info-Infra Model IM = <G(t), S(t), M(t), F(t), e, r, y, t>

- G(t): Information system
- S(t): Information security system or encryption system
- M(t): Monitoring or control system
- F(t): Communication system or security guard for output data
- e: Input into information security system
- r: Input from monitoring or control system
- y: Output of information system or input of linked system
- h: Hacking from outside of system
- d: In-house intrusion accident
- u: Control level of input of, or access from, users
- t: Time

Where, $\{G_i\}$ is elementary assets including servers, networks and PCs.

The modeling of information systems for risk analysis is configured in a block diagram. As shown in Fig. 2, it is assumed that a web server, an application server and a database server reside inside an information system. Users are allowed to access the Internet while they perform e-library jobs. However, there are difficulties in analyzing the propagation effects and levels of damage caused by cyber intrusions in information systems with the block diagram of the information system. Representing the information system using modeling as shown in Fig. 3 may cause hacking threats from the Internet; therefore, it should be possible to easily recognize in-house intrusion accidents and clearly acknowledge target assets protected by the information system. Therefore, this simple network block diagram enables analysis of the propagation effects and levels of damage.

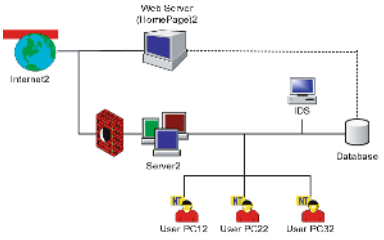

Fig. 2. Block diagram of a common information system

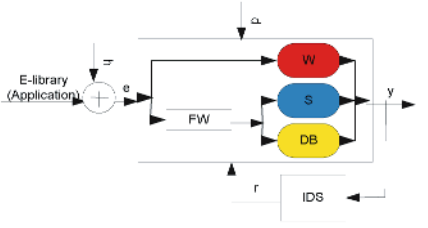

Fig. 3. Configuration of information system through modeling

4 Analysis of Levels of Damage

To analyze the propagation effects of damage using the suggested modeling, each asset and network features should be configured in the modeling. For this purpose, we define levels of damage to information systems as follows:

The fault conditions and the range of assets subject to damage should be identified in order to analyze the entire level of damage to an information system. The current epidemic model is as shown in Fig. 4:

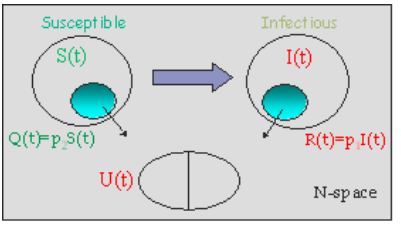

Fig. 4. Epidemic model

The epidemic model allows analysis of the infection feasibility of susceptible assets from those infected by worms, and calculation of the number of infected assets based upon the results of the analysis. Assets can be removed after infections. The equation is as follows:

$$\dot{I(t)} = \beta I(t)S(t) - \dot{U(t)}$$
$$U(t) = Q(t) \bigcup R(t) = \{p_2 \bigcap S(t)\} \bigcup \{p_1 \bigcap I(t)\}$$
$$S(t) \bigcup I(t) \bigcup U(t) = N$$

$S(t)$: susceptible Assets, $I(t)$: Infectious Assets,
$U(t)$: removed Assets from Infection, N : Total Asset Number,
β : Infection Ability, p_1, p_2 Recovered Ability

This model does not suggest the propagation effect and level of damage occurred during a period of activities such as analyzing the causes of intrusion, establishing

safeguards, and recovering the systems from damage. Furthermore, this model is applicable to worms only, and is not capable of identifying the damage probabilities of different intrusions or the levels of damage to entire systems. Therefore, additional elements should be defined to expand the model to other cases. We expanded the epidemic model to include the following factors for intrusion:

1. Levels of damage by judging if damage is caused by normal operations or by intrusions when the assets are loaded
2. A scope and levels of asset infections when an intrusion takes place
3. Levels of protection in phases of intrusion elimination after the causes of intrusions have been identified

Each asset will be infected if it is susceptible to intrusions. In such cases, the level of damage to each asset is calculated using a relational function with the uncertainty of asset infections. The level of damage to the entire information system is calculated using functions relevant to existing safeguards and the level of recovery attained through the safeguards. An information system is the sum of its assets: each asset faces unique threats and it is vulnerable and subject to damage due to these threats and its vulnerabilities. The level of damage of a system over time can be represented in a function. The final results of the analysis are as follows when the probability and the uncertainty of infection are included.

$$\{I_i(t)\} = \{P_i(t)\} \bigcap \{X_i(t)\}$$
$$\{R_i(t+d)\} = f_{R1}[\{I_i(t+d)\},\ \{\epsilon_i(t+d)\}] \ +\ f_{R2}[\{I_i(d)\},\ \{\epsilon_i(d)\}]$$
$$\{G_i(t)\} = f_T[\{A_i(t)\},\ \{Z_i(t)\},\ f_R[\{P_i(t) \bigcap X_i(t)\},\ \{\epsilon_i(t)\}]]$$
$$= f_T[(\{\rho_i(t) \bigcap \{A_i(t)\}), (\{\sigma_i\} \bigcap \{Z_i(t)\}),\ f_R[\{P_i(t) \bigcap X_i(t)\},\ \{\epsilon_i(t)\}]]$$

$$M(t) = G(t)/N \ \times\ 100$$

$\{P\}$: Intrusion, $\{X\}$: Weaknesses attributed to intrusion
$\{R\}$: Level of damage to infected asset, $\{\epsilon\}$: Uncertainty of infection,
$\{A\}$: Level of existing safeguards, $\{d\}$: Time delay in analyzing infection,
$\{R\}$: Level of future safeguards, ρ, σ : Probability of infection
M : Level of damage (%)

5 Damage Propagation and Calculation Using Modeling

We have performed the following case study for the analysis of security risks using the suggested modeling. The test environment for the case study was configured as shown in Fig. 5, and modeling was performed as shown in Fig. 6. The in-house network is employed for business management, and the home page is operated in the outside network. The data protection system is installed and operated on each client. The switches and hubs at both ends to build the information security system are removed from the major asset list, since they are not regarded as major assets. The systems operating in a duplex structure and a dual configuration are indicated as overlapping, since they are identical in terms of the probabilities of threats and vulnerabilities.

Configuring the information system in the manner illustrated above allows us to analyze the propagation effects and levels of damage as well as assets, threats, vulnerabilities, and safeguards.

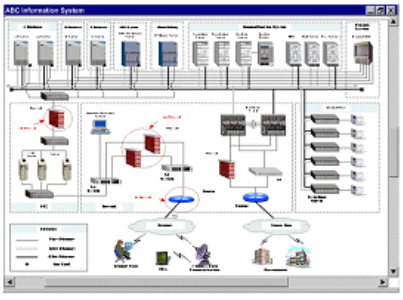

Fig. 5. Configuration diagram of a information system

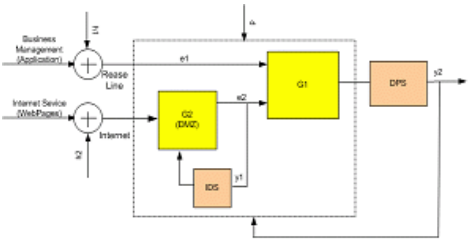

Fig. 6. Modeling of a information system

5.1 Structure of Assets

The structure of assets is as follows: threats and vulnerabilities regarding an intrusion in question are distinguished, and the probability of infections of the distinguished items is defined. Table 1 contains an example of the asset parameters for a Windows 2000 server. As shown in Table 1, the Windows 2000 Server in an information system is subject to threats of improper password control (2.19), an absence of logging policies (2.35), and a deficiency in training programs for operators (3.09). Infection information and a scope, and relational functions are recorded with time intervals. The system is susceptible to buffer overflow attacks and format string attacks, which can cause damage of up to 70% and 40% of the server assets respectively.

Table 1. File structure of the asset Parameters

```
! Windows2000 Server
! PARAMETER DATA
! Threat Table
! Table number: Threat factor (1-5):
  Damage_factor (%)
2.19: 1, 2, 2, 3, 4, 5: linear_function (a)
2.35: 1, 2, 3, 4, 5, 5: exp_function (a)
3.09: 1, 3, 5: log_function (a)
... ...
! Vulnerability Table
! CVE ID: Threat_factor (1-5):
Damage_factor (%)
CAN-2000-1186: 4: 70
CAN-2003-1022: 3: 40
... ...
! Risk Table
...
! Damage Table
...
! SafeGuard Table
...
```

Table 2. Modeling results for each asset

```
! Information System Net-list
DIM
1 min! Time Interval
IN      0    1 Attack
OUT   0    1 Risk, Damage
! Assets
SERVER 1 2  S(WIN2000, SP2)          !S
DB          2 3  D(ORACLE, V8.0)         !D
PC          2 4  PC(WINXP, 3)    !PC set 3
SERVER 1 3  S(HP, SP3, APACHE)   !S
......
```

5.2 Netlist File

A netlist file is defined as a basic network-structured input file for an information system. When an information system is developed as shown in Fig. 5 with a netlist file as shown in Table 2, details are displayed as follows. Since most of assets are connected with switches or hubs, location determinations of switches and hubs as nodes allow simple development of netlist files.

First of all, identify the assets currently used by the information system, and mark the asset type, and the numbers and the values of adjacent nodes where the assets reside. The core of the netlist file illustrates the information system based on node numbers.

The modeling of the information system as shown in Fig. 5 is displayed as shown in Fig. 7, and simulation is made for the propagation effects and calculations of damage to show the results as in Fig. 8. The results indicate that the level of damage to the information system escalated from 1 to 5 in 120 seconds after the intrusion, with the total damage exceeding 80%. However, operations for the emergency recovery measures make the entire damage level become 2 and reduce the damage to 40%. As described above, the modeling of an information system enables convenient real-time analysis of the scopes and levels of damage.

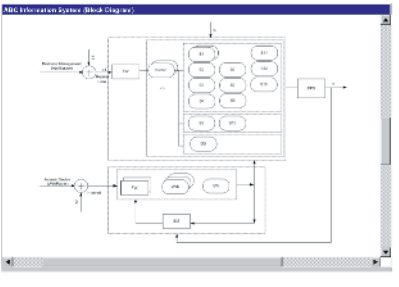

Fig. 7. Modeling of an information system

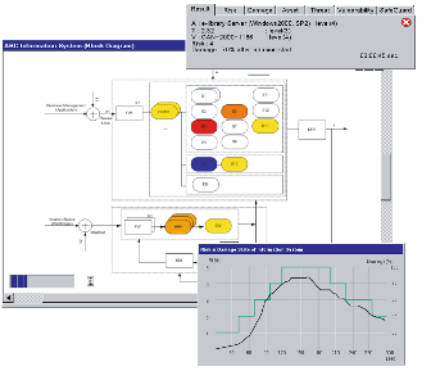

Fig. 8. Propagation effects and levels of damage

6 Conclusions

Security risk analysis of information systems is an essential task. However, the current analytic techniques are, in general, of a static nature, and are not capable of illustrating the propagation effects of damage to information systems and the appropriateness of role operations for information security systems. We suggest techniques to analyze the propagation effects and levels of damage while resolving the above problems.

The techniques suggested in this study have been shown to be capable of analyzing the damage flow within information systems and the effects of damage in a given time interval. This means that when an intrusion takes place, the level of infection and its route are analyzed by identifying the threats and vulnerabilities of various types

and levels of intrusions, while the variation in levels of damage and damage propagation effects are analyzed by employing pre- and post-information safeguards. In short, these techniques allow safeguards for information systems to be defined in a relatively short period of time as well as real-time analysis of appropriateness of the safeguards in order to execute more stable and efficient security risk analysis.

References

[1] Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim, "Security Risk Analysis Model for Information Systems," LNCS 3398, Systems Modeling and Simulation: Theory and Applications: Third Asian Simulation Conference, AsianSim 2004.

[2] Yun-Kai ZHANG, Fang-Wei Wang, Yu-Qing ZHANG, Jain-Feng MA, "Worm Propagation Modeling and Analysis Based on Quarantine," Infosec04, November 14-16, 2004, ACM ISBN:1-58113-955-1.

[3] Kwang Min Park, Dong Kwang, PSpice Understanding and Application (revised), 1992, ISBN 89-85305-02-6.

[4] W. Reisig, Petri Nets, An Introduction, EATCS, Monographs on Theoretical Computer Science,W.Brauer, G. Rozenberg, A. Salomaa(Eds.), Springer Verlag, Berlin, 1985.

[5] Edward Yourdon, Modern Structured Analysis, Prentice-Hall, 1989.

[6] Paul E. Black, ed, "Deterministic finite state machine", Dictionary of Algorithms and Data Structures, NIST. http://www.nist.gov/dads/HTML/determFinitStateMach.html

[7] L.M. Kristensen, S. Christensen, K. Jensen: The Practitioner's Guide to Coloured Petri Nets. International Journal on Software Tools for Technology Transfer, 2 (1998), Springer Verlag, 98-132.

[8] Paul Tuinenga, SPICE: A Guide to Circuit Simulation and Analysis Using PSpice (3rd Edition), Prentice-Hall, 1995, ISBN 0-13-158775-7.

[9] ISO/IEC TR 13335, Information technology - Guidelines for the management of IT Security: GMITS, 1998.

[10] CSE (Canadian Secutiy Establishment), “A Guide to Security Risk Management for IT Systems”, Government of Canada, 1996.

[11] MacDonald, David/ Mackay, Steve (EDT), Practical Hazops, Trips and Alarms (Paperback), Butterworth-Heinemann, 2004.

[12] RAC, Fault Tree Analysis Application Guide, 1991.

[13] CMU, OCTAVE (Operationally Critical Threat, Assets and Vulnerability Evalustion), 2001. 12.

[14] Theo Dimitrakos, Juan Bicarregui, KetilSt•len. CORAS - a framework for risk analysis of security critical systems. ERCIM News, number 49, pages 25-26, 2002.

[15] Young-Hwan Bang, YoonJung Jung, Injung Kim, Namhoon Lee, GangSoo Lee, "Design and Development of a Risk Analysis Automatic Tool," ICCSA2004, LNCS 3043, pp.491-499, 2004.

[16] http://www.cramm.com, CRAMM

[17] Palisade Corporation, @RISK, http://www.palisade.com.

[18] Countermeasures, Inc., The Buddy System, http://www.buddysystem.net

[19] Information Security Management, Part 2. Specification for Information Security Management System, British Standards Institution (BSI).

[20] BSI, http://www.bsi.bund.de/english/gshb /manual/index.htm, 2003.

[21] Thomas Dubendorfer, Arno Wagner, Bernhard Plattner, "An Economic Damage Model for Large Scale Internet Attacks," Proceedings of the 13th IEEE International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprise (WET ICE'04) 1524-4547/04.

[22] InJung Kim, YoonJung Chung, YoungGyo Lee, Dongho Won, "A Time-Variant Risk Analysis and Damage Estimation for Large-Scale Network Systems," ICCSA2005, LNCS3043, May 2005.

[23] Injung Kim, YoonJung Jung, JoongGil Park, Dongho Won, "A Study on Security Risk Modeling over Information and Communication Infrastructure," SAM04, pp. 249-253, 2004.

[24] M. Liljenstam, D.M. Nicol, V.H. Berk, and R.S. Gray, "Simulating Realistic Network Worm Traffic for Worm Warning System Design and Testing," In Proceedings of the 2003 ACM workshop on Rapid Malcode, pp.24-33, ACM Press. 2003