시뮬레이션 기반 진화기법을 이용한 최적 보안 대응전략 자동생성

이장세* · 황훈규** · 윤진식** · 박근우**

Automated Generation of Optimal Security Defense Strategy using Simulation-based Evolutionary Techniques

Jang-se Lee* · Hun-Gyu Hwang** · Jin-Sik Yun** · Geun-Woo Park**

이 논문은 2007년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임.
(KRF-2007-313-D00762)

요 약

본 논문은 진화기법을 이용하여 최적의 보안 대응전략을 자동생성 하는 방법의 제안을 목적으로 한다. 정보통신 환경에 대한 침해에 의한 피해가 급증함에 따라 다양한 보안 기술에 대한 연구가 활발히 이루어지고 있다. 그러나 다양한 네트워크 환경에 대한 보안 기술들의 연동 상황을 고려한 최적의 대응 전략을 생성하는데 어려움이 있다. 따라서 본 논문에서는 대응방법을 유전자로 표현하여 유전 알고리즘을 적용함으로써 대응방법들에 대한 최적의 조합으로서 최적 대응 전략을 생성하였다. 또한 시뮬레이션을 이용하여 다양한 상황에 대한 대응방법의 적용에 따른 취약성을 정량적으로 평가함으로써 적합도를 평가하였다. 끝으로 제안한 방법을 구현한 시스템에 대한 실험을 통하여 타당성을 검토하였다.

ABSTRACT

The objective of this paper is to propose the methodology for automated generation of the optimal security defense strategies using evolutionary techniques. As damages by penetration exploiting vulnerability in computer systems and networks are increasing, security techniques have been researched actively. However it is difficult to generate optimal defense strategies because it needs to consider various situations on network environment according to countermeasures. Thus we have adopted a genetic algorithm in order to generate an optimal defense strategy as combination of countermeasures. We have represented gene information with countermeasures. And by using simulation technique, we have evaluated fitness through evaluating the vulnerability of system having applied various countermeasures. Finally, we have examined the feasibility by experiments on the system implemented by proposed method.

키워드
정보보안, 대응전략, 진화기법, 시뮬레이션

Key word
Information Security, Defense Strategy, Evolutionary Technique, Simulation

* 한국해양대학교 IT공학부(교신저자, jslee@hhu.ac.kr)
** 한국해양대학교 대학원 컴퓨터공학과

접수일자 : 2010. 10. 22
심사완료일자 : 2010. 10. 25

Ⅰ. 서 론

전 세계적으로 정보통신환경에 대한 의존도가 증가함에 따라 다양한 분야에서의 사이버 보안 사고의 피해가 급증하고 있으며, 이를 극복하기 위하여 다양한 보안기술 및 시스템에 대한 연구 및 개발이 국내외에서 활발히 진행되고 있다[1,2].

다양한 보안기술 및 시스템이 제공하는 비밀성, 무결성, 가용성, 접근통제 등의 기능은 상호간의 연동을 통하여 더 큰 효과를 가질 수 있다. 그러나 이를 운영하는 관리자가 다양한 보안기술 및 시스템의 특성을 이해하고 운영하는데 어려움이 있어 통합보안관제시스템(Enterprise Security Management System) 등이 개발되고 있다[1,3,4]. 기존의 ESM 연구는 다양한 보안기술 및 시스템의 연동에 초점이 맞추어져 있어 활용 효과에 한계가 있으며 이를 보완하기 위한 연구가 이루어지고 있다[4,5]. 특히, [5]에서는 모델링 및 시뮬레이션 기술을 통해 다양한 연동 상황을 고려한 대응전략을 수립하여 지능적으로 관리하는 시스템을 제안한 바 있으나, 모든 가능성을 고려한 최적의 대응전략을 자동으로 수립하여 모든 컴퓨터 및 네트워크를 효과적으로 관리하는 데에는 한계가 있다.

따라서 본 논문에서는 네트워크 및 호스트에 대한 최적의 보안 대응전략을 자동으로 수립하는 방법을 제안한다. 이를 위하여 최적화 기법의 하나인 진화 알고리즘을 적용하여 다양한 보안 대응방법으로부터 최적의 전략을 생성한다. 다양한 대응전략을 유전 정보로 표현하여 세대를 구성하고 유전 알고리즘을 적용한 진화과정을 통하여 대응전략의 최적화를 유도한다. 또한, 대응전략을 적용하여 관리 대상 호스트 및 네트워크에 대한 시뮬레이션을 수행하고[5] 취약성을 점수화함으로써 적합도를 평가하였다. 이와 같이 시뮬레이션 기반 진화기법을 적용한 본 연구는 기존 연구와 달리 첫째, 정량적으로 취약성을 평가할 수 있으며 둘째, 보안기술 및 시스템의 다양한 연동상황을 반영한 대응전략을 수립할 수 있고 셋째, 정량적인 취약성 요구조건을 만족하는 최적의 대응 전략을 자동으로 수립할 수 있는 장점을 갖는다.

본 논문의 구성은 다음과 같다. 제2장에서는 관련연구로서 모델링 및 시뮬레이션을 위한 SES/ MB 프레임워크를 설명하고 유전 알고리즘의 적합도 평가를 위한 취약성 평가 매트릭스에 대하여 설명한다. 제3장에서 최적 대응전략 자동생성 방법을 제안하고 제4장에서 구현 및 실험을 통하여 타당성을 검토하고 제5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 SES/MB 프레임워크

분석대상의 네트워크 및 호스트에 대한 시뮬레이션을 위하여 분석대상의 구조와 행위에 대한 모델링 방법이 요구된다. Zeigler에 의해 제안된 SES/MB 프레임워크[6,7]는 대상 시스템에 대한 구조와 행위를 체계적으로 모델링하고 시뮬레이션을 할 수 있는 방법을 제공한다. SES/MB는 시스템의 구조 모델링을 위한 수단을 제공하는 SES (System Entity Structure)와 시스템의 행위 즉 시스템을 구성하는 요소들에 대한 동역학적 특성 모델링을 위한 수단을 제공하는 MB (Model Base)로 구성된다.

그림 1은 SES/MB 프레임워크의 예를 나타낸다. 시스템의 구조는 개체 구조 베이스(Entity Structure Base)에 저장되며 단말 노드들의 행위 모델은 모델베이스(Model Base)에 저장된다. 변환과정을 통하여 대상 시스템의 구조에 모델이 결합된 시뮬레이션 구조를 생성함으로써 다양한 구조 및 모델에 대한 시뮬레이션이 가능하다[5,6,7].

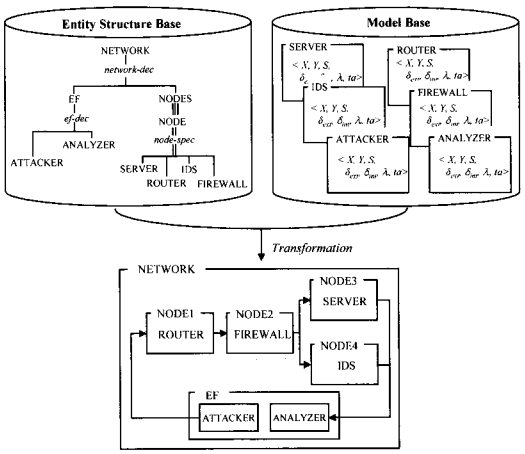

그림 1. SES/MB 개념
Fig. 1 Concept of SES/MB

2.2 취약성 평가 매트릭스

취약성에 대한 연구는 주로 정성적인 특성에 따라 취약성을 분류하는 연구가 이루어지고 있으나[8,9] 네트워크 및 시스템에 대한 위험을 평가하고 대응을 자동화하기 위하여 취약성에 대한 정량적인 평가가 필수적이다. 최근 FIRST(Forum of Incident Response and Security Teams)에서는 취약점에 대한 일반화된 점수를 제공할 수 있는 CVSS(Common Vulnerability Scoring System)을 제안한 바 있다[10]. CVSS는 3가지의 매트릭스 그룹을 이용하여 취약성을 정량적으로 평가한다.

- 기본 매트릭스 : 시간과 사용자 환경에 의해 변하지 않는 근본적인 취약점 특징을 나타낸다.
- 임시 매트릭스 : 시간의 흐름에 따라 변경되는 취약점 특징을 나타낸다.
- 환경 매트릭스 : 특정한 사용자 환경에 유일하게 관련 있는 취약점 특징을 나타낸다.

본 논문에서는 CVSS의 매트릭스 중 기본 매트릭스를 이용하여 각각의 명령어에 대한 취약성 점수를 부여하고 시뮬레이션을 수행함으로써 시간 및 환경의 변화가 반영된 점수화를 시도하였다. 기본 매트릭스는 표 1과 같이 총 6가지의 구성요소로 이루어진다. 각각의 구성요소는 등급에 따라 점수가 부여되며 표 2의 계산법에 의하여 취약성이 점수화된다.

표 1. 기본 매트릭스
Table. 1 Base metrics

요소 이름	약자	등급	점수	내용
Access Vector	AV	L(ocal)	0.395	공격 수행위치
		A(djacent Network)	0.646	
		N(etwork)	1.0	
Access Complexity	AC	H(igh)	0.35	공격 복잡도
		M(edium)	0.61	
		L(ow)	0.71	
Authentication	AU	M(ultiple)	0.45	인증 필요여부
		S(ingle)	0.56	
		N(one)	0.704	
Confidentiality Impact	C	N(one)	0.0	공격영향-기밀성
		P(artial)	0.275	
		C(omplete)	0.660	
Integrity Impact	I	N(one)	0.0	공격영향-무결성
		P(artial)	0.275	
		C(omplete)	0.660	
Availability Impact	A	N(one)	0.0	공격영향-가용성
		P(artial)	0.275	
		C(omplete)	0.660	

표 2. 기본 매트릭스 계산법
Table. 2 Base scoring

BaseScore = round_to_1_decimal(((0.6×Impact)+(0.4×Exploitability)-1.5)×f(Impact))
여기서, Impact = 10.41×(1-(1-ConfImpact)×(1-IntegImpact)×(1-AvailImpact)),
Exploitability = 20×AccessVector×AccessComplexity×Authentication,
Impact = 0 이면 f(Impact) = 0,
그렇지 않으면 f(Impact) = 1.176

Ⅲ. 최적 보안 대응전략 자동생성 방법

그림 2는 시뮬레이션 기반 진화기법을 적용한 최적 대응전략 자동생성 방법에 대한 개념을 나타낸다. 그림에서 1단계는 요구 명세화 단계로서, 최적 대응전략 자동생성을 위하여 필요한 요구사항, 제약조건 등을 명세하는 단계이다. 2단계는 SES/MB 프레임워크를 이용하여 분석 대상이 되는 네트워크에 대한 구조적 표현과 네트워크 구성원 모델 및 공격자 모델 등을 결합하여 시뮬레이션 구조를 생성한다. 3단계는 2단계에서 생성된 시뮬레이션 구조를 기반으로 GA를 적용하는 단계이다. GA 컨트롤러는 대응전략을 나타내는 유전자들(Gene)로 구성된 Gene Pool로부터 개체들을 생성하여 세대를 구성한다. 세대를 구성하는 개체들은 각각의 GA 에이전트에 할당되며 GA 에이전트는 개체의 유전자에 따라 대응전략을 적용하여 시뮬레이션을 수행한다. 모든 개체의 시뮬레이션이 종료되면 GA 컨트롤러는 시뮬레이션 결과로부터 취약성을 점수화하는 적합도 함수에 따라 선택과 유전연산을 적용하여 다음 세대를 구성함을 반복한다. 최종적으로 4단계에서 GA 적용에 따른 결과로서 최적의 대응 전략을 얻게 된다.

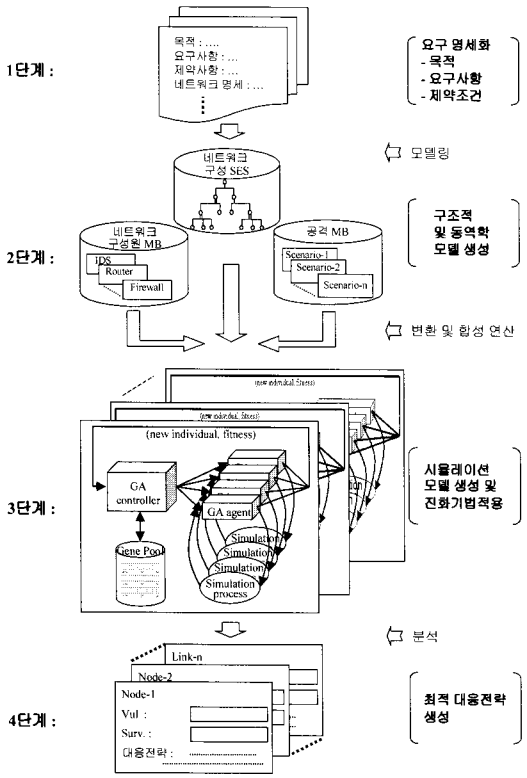

그림 2. 최적 대응전략 자동생성 방법
Fig. 2 Methodology for automated generation of optimal defense strategy

Ⅳ. 구현 및 실험

본 장에서는 진화기법을 적용하는 방법을 설명하고 구현된 시스템을 통하여 최적 대응전략을 생성하는 실험을 수행한다.

4.1 세대 생성

본 논문에서는 5가지의 대응방법에 대한 최적의 조합을 대응전략으로 생성하는 것을 목적으로 하였다. 이를 위하여 각각의 대응방법을 유전정보로 표현하였다. 그림 3은 각각의 대응방법을 의미하는 5개의 유전자로 구성된 염색체를 나타낸다. 각 유전자는 1과 0의 값을 가질 수 있으며 대응방법의 실행 유무에 따라 1은 on, 0은 off를 의미한다.

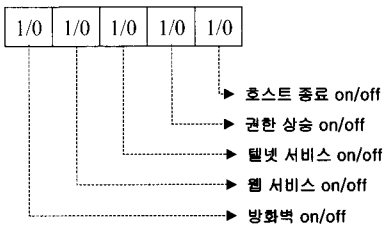

그림 3. 염색체의 유전자 정보
Fig. 3 Gene information of chromosome

4.2 적합도 평가

각 개체의 염색체에 의한 대응방법을 적용하여 각각 시뮬레이션을 수행하고 시뮬레이션 수행 결과에 따른 취약성 값에 의하여 각 개체의 적합도를 평가하였다.

표 3은 시뮬레이션에 사용되는 공격시나리오를 구성하는 명령어들을 CVSS의 기본 매트릭스 구성요소에 따라 분석한 일부를 나타낸다. telnet의 경우 공격 수행위치 점수(AV)는 N등급으로 1.0의 점수가 부여되며 공격 복잡도 점수(AC)는 M등급으로 0.61의 점수가 부여된다. 인증 필요 여부(AU)는 N등급으로 0.704, 기밀성 점수(C)는 N등급으로 0.0, 무결성 점수(I)는 P등급으로 0.275, 가용성 점수(A)는 P등급으로 0.275의 점수가 각각 부여됨을 알 수 있다(표 1의 등급별 점수 참조). 또한 표 4는 시뮬레이션을 통하여 telnet 명령어가 수행된 경우 기본 매트릭스 계산법(표 2 참조)에 따라 취약성이 평가된 예를 나타낸다. 이와 같이 시뮬레이션에 적용된 대응방법에 따라 공격 시나리오의 명령어의 수행여부가 달라지며 그에 따른 취약성이 변하게 된다.

표 3. 공격 시나리오 명령어의 기본 매트릭스 분석예
Table. 3 Example of analysis on commands of attack scenario using base metrics

명령어	기본 매트릭스
telnet	AV:N / AC:M / AU:N / C:N / I:P / A:P
login	AV:N / AC:H / AU:S / C:N / I:P / A:P
…	…
chmod	AV:N / AC:H / AU:S / C:C / I:N / A:N
export	AV:N / AC:L / AU:S / C:P / I:C / A:N
…	…

표 4. telnet 명령어에 의한 취약성 점수 계산의 예
Table. 4 Example of base scoring on telnet

telnet : AV:N/AC:M/AU:N/C:N/I:P/A:P
AV:N(1.0) AC:M(0.61) AU:N(0.704) C:N(0.0) I:P(0.275) A:P(0.275)
BaseScore = ((0.6×10.41×(1-(1-0)×(1-0.275)×(1-0.275))) + (0.4×20×1×0.61×0.704)-1.5)×1.176 = (2.962946+3.43552-1.5)×1.176 = 5.760596

4.3 유전 오퍼레이션

진화를 위한 다음 세대는 시뮬레이션 수행 결과에 따라 취약성 값이 작은 순서대로 전체 개체수의 절반을 선택하여 구성하고 나머지 절반은 선택된 개체들에 대한 교배와 돌연변이 오퍼레이션을 통하여 새로이 생성된 개체로 구성하였다.

그림 4는 선택되어진 개체(P1, P2)를 임의 인덱스 선택법으로 교배 오퍼레이션을 적용하는 과정을 나타낸다. 그림과 같이 염색체 내의 유전자의 인덱스를 임의로 지정하여 지정된 인덱스 번호의 앞과 뒤를 서로 교환하여 새로운 개체(C1, C2)를 생성하였다. 또한 설정된 비율에 따라 염색체의 임의의 비트를 1↔0으로 변경하는 돌연변이 오퍼레이션을 적용하였다.

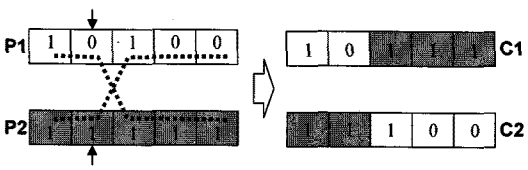

그림 4. 교배 연산
Fig. 4 Mutation operation

4.4 실험

그림 5는 구현된 시스템의 메인화면을 나타낸다. 메인화면은 대상 네트워크에 대한 시뮬레이션 설정 및 제어, 대응전략 생성을 위한 유전 알고리즘 설정 및 제어를 위한 메인 메뉴와 대상네트워크 설정 및 확인을 위한 네트워크 정보창, 네트워크 토폴로지를 보여주는 네트워크 구성창, 수행 결과확인을 위한 결과창으로 구성된다.

그림 6은 공격 시나리오를 적용하여 시뮬레이션을 수행한 결과화면을 나타낸다. 시뮬레이션을 통하여 시나리오를 구성하는 각 명령어의 수행결과에 CVSS를 적용한 취약성 점수를 확인할 수 있다.

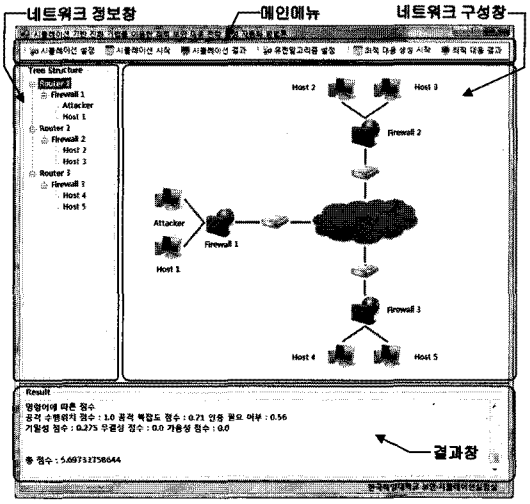

그림 5. 구현된 시스템의 메인화면
Fig. 5 Main screen shot of implemented system

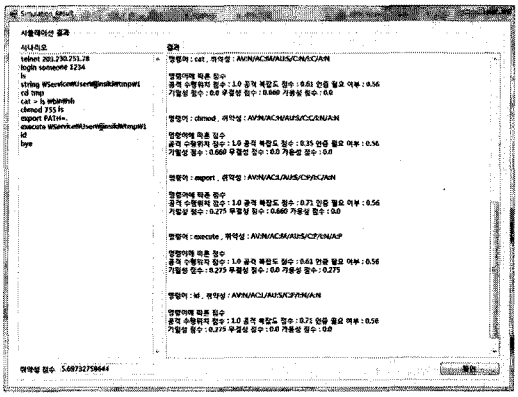

그림 6. 시뮬레이션 결과 보기 화면
Fig. 6 Screen shot of simulation result view

그림 7은 최적 대응전략 생성을 위하여 유전 알고리즘을 설정하는 대화상자이다. 종료조건으로서 세대 수 또는 취약성 점수를 설정할 수 있으며 돌연변이율을 설정할 수 있다.

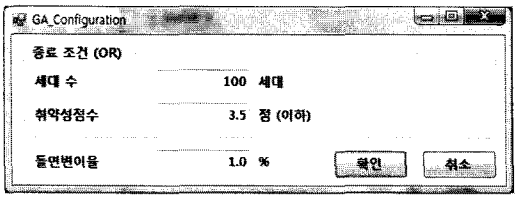

그림 7. 유전알고리즘 설정 화면
Fig. 7 Screen shot of GA configuration

그림 8은 종료조건으로 세대 수가 100세대가 되거나 희망 취약성 점수를 3.5점 이하로 설정하고 돌연변이율은 1%로 설정하여 최적 대응전략 생성을 수행한 결과이다. 최적 대응전략으로 생성된 개체의 염색체는 "11010"이며 방화벽과 웹서비스는 'on'으로 설정, 텔넷서비스는 'off'로 설정하고 권한설정을 강화하여 호스트를 사용하는 최적 대응전략이 생성되었으며 취약성 점수는 희망 취약성 점수 이하인 3.2임을 알 수 있다.

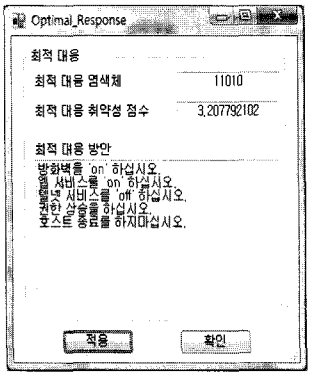

그림 8. 최적 대응 전략 보기 화면
Fig. 8 Screen shot of optimal defense strategy view

V. 결 론

정보통신기술의 발달과 보급에 따른 역기능으로 다양한 보안 위협이 대두되고 있으며 그에 따른 피해가 급증하고 있다. 이에 다양한 보안 기술에 대한 연구가 활발히 이루어지고 있다. 하지만 다양한 네트워크 환경에 다양한 보안기술을 적용하기 위해서는 네트워크와 개별 보안기술에 대한 폭넓은 지식과 더불어 상호 연동 상황에 따른 모든 가능성에 대한 고려가 요구되므로 다양한 보안 기술을 적용하여 네트워크를 효과적으로 관리하는데 어려움이 있다.

따라서 본 논문은 진화기법을 적용하여 최적의 보안 대응 전략을 자동으로 생성하는 방법의 제안을 목적으로 하였다. 이를 위하여 대응방법을 유전자로 표현하고 유전 알고리즘을 적용함으로써 최적화된 보안 대응전략을 생성하였다. 또한 시뮬레이션을 이용하여 대상 네트워크에 대한 다양한 보안 기술 즉 대응방법의 연동상황에 따른 취약성을 평가하고, CVSS를 적용하여 취약성을 점수화함으로써 적합도를 평가하였다. 제안한 방법을 적용한 시스템을 구현하고 5개의 대응방법에 대한 실험을 통하여 최적의 대응전략 생성에 대한 타당성을 검토하였다. 제안한 방법은 기존 연구와 달리 첫째, 정량적으로 취약성을 평가할 수 있으며 둘째, 보안기술 및 시스템의 다양한 연동상황을 반영한 대응전략을 수립할 수 있고 셋째, 정량적인 취약성 요구조건을 만족하는 최적의 대응 전략을 자동으로 수립할 수 있는 장점을 갖는다. 제안한 방법을 통하여 자동화된 최적의 대응전략을 생성함으로써 지능적인 통합 보안 관리가 가능할 것으로 기대된다.

참고문헌

[1] 유종호, 김종현, 나중찬, "통합보안관리 및 사이버 역추적 기술 표준화 현황", *TTA Journal*, no. 118, pp. 66-74, 2008.

[2] H.S. Venter, and J.H.P. Eloff, "A taxonomy for information security technologies", *Computers & Security*, vol. 22, no. 4, pp. 299-307, 2003.

[3] 이영석, 나중찬, 손승원, "ESM 개발 동향: 이기종 보안 시스템 연동을 중심으로", *한국전자통신연구원 주간기술동향*, 통권 1096호, pp. 1-16, 2003.

[4] 최재규, "RBAC을 이용한 ESM 모델연구", *정보통신산업진흥원 주간기술동향*, 통권 1312호, pp. 1-12, 2007.

[5] J.S. Lee, D.S. Kim, J.S. Park, and S.D. Chi, "Design of Intelligent Security Management System using Simulation based Analysis", *LNAI* 3809, pp. 766-775, 2005.

[6] B.P. Zeigler, H. Praehofer, and T.G. Kim, *Theory of Modeling and Simulation,* Academic Press, 2000.

[7] B.P. Zeigler, *Multifacetted Modeling and Discrete Event Simulation,* Academic Press, 1984.

[8] S. Hansman, and R. Hunt, "A taxonomy of network and computer attacks", *Computers & Security,* vol. 24, no. 1, pp. 31-43, 2005.

[9] V. M. Igure, and R. D. Williams, "Taxonomies of attacks and vulnerabilities in computer systems", *IEEE COMMUNICATIONS SURVEYS,* vol. 10, no. 1, pp. 6-19, 2008.

[10] FIRST, Common Vulnerability Scoring System, http://www.first.org/cvss/

저자소개

이장세(Jang-Se Lee)

1997. 2. 한국항공대학교 컴퓨터공학과 (공학사)
1999. 2. 한국항공대학교 컴퓨터공학과 (공학석사)
2003. 8. 한국항공대학교 컴퓨터공학과 (공학박사)
2004. 3.~현재 한국해양대학교 IT공학부(부교수)
※관심분야 : 컴퓨터보안, 지능시스템, 모델링 및 시뮬레이션

황훈규(Hun-Gyu Hwang)

2009. 2. 한국해양대학교 IT공학부 컴퓨터정보공학전공(공학사)
2009. 3.~현재 한국해양대학교 대학원 컴퓨터공학과 석사과정
※관심분야 : 정보보안, 네트워크 시뮬레이션, 해양정보시스템

윤진식(Jin-Sik Yun)

2009. 2. 한국해양대학교 IT공학부 컴퓨터정보공학전공(공학사)
2009. 3.~현재 한국해양대학교 대학원 컴퓨터공학과 석사과정
※ 관심분야 : 정보보안, 네트워크, 포렌식

박근우(Geun-Woo Park)

2009. 2. 한국해양대학교 IT공학부 컴퓨터정보공학전공(공학사)
2009. 3.~현재 한국해양대학교 대학원 컴퓨터공학과 석사과정
※ 관심분야 : 정보보안, 네트워크, 시뮬레이션