

SIMVA를 이용한 시뮬레이션 기반의 네트워크 취약성 분석*

유용준[”], 이장세[“], 지승도[”]

Simulation-based Network Vulnerability Analysis Using the SIMVA

Yong-Jun You, Jang-Se Lee, Sung-Do Chi

Abstract

The major objective of this paper is to analyze network vulnerabilities using the SIMVA (SIMulation-based Vulnerability Analyzer). SIMVA is capable of monitor network status and analyze vulnerabilities automatically. To do this, we have employed 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 for developing network security models and simulation-based analysis of vulnerability. SIMVA can analyze static vulnerability as well as dynamic vulnerability consistently and quantitatively. In this paper, we verified and tested the capability of application of SIMVA by slammer worm attack scenario.

Key Words: Vulnerability Analysis, Network Security, SES/MB, DEVS,

* 본 논문은 한국시뮬레이션학회 2004년 춘계 학술대회에서 발표한(우수논문상 수상) 내용을 보완한 것임.

** 한국항공대학교 전자정보통신컴퓨터공학부

*** 한국해양대학교 IT 공학부

1. 서 론

컴퓨터 환경의 개선과 인터넷의 폭발적 사용 증가에 따라 네트워크 의존도가 높아진 반면, 인터넷에 연결된 대부분의 시스템이 외부 침입에 노출됨에 따라 이를 이용한 사이버 공격에 대한 피해가 급증하고 있다[1,2].

지금까지의 Aslam[3], Bishop[4]과 Krsul[5] 등의 취약성 분석 관련 연구에서는 호스트에 존재하는 취약성을 탐지하고 제거하기 위하여 정성적 특성들에 의한 취약성 분류에 초점이 맞추어져 있었으며, 최근 Hariri[6]는 실제 시스템에 대한 모니터링 정보를 토대로 시스템의 취약성을 정의하고 정량적인 분석을 시도한 바 있으나 각 구성요소의 구체적인 변화와 서로 간의 상호 작용을 고려하여 사전에 취약성을 분석할 수 없다. 한편, 이와 같은 연구 결과에 기반을 두고 개발된 스캐닝 도구들은 실제 시스템의 정성적 분석에 효과적으로 적용될 수 있으나 다양하게 변화하는 정교한 해킹 기법에 대처하고, 다양한 경로를 제공하는 인터넷 기반 구조에 대한 침해 등에 적용하기에는 미흡하다.

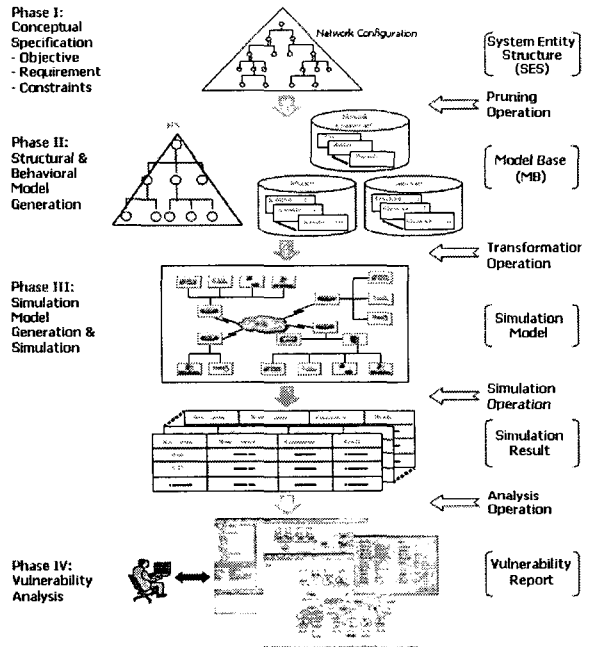
이를 극복하기 위하여 네트워크를 모니터링하고 그 취약성들을 자동적으로 분석할 수 있는 SIMVA(SIMulation Vulnerability Analyzer)라는 네트워크 취약성 분석 도구를 성공적으로 개발한 바 있다[7]. SIMVA는 SES/MB(System Entity Structure / Model Base) 프레임워크 및 DEVS(Discrete Event System Specification) 이론을 적용하여 네트워크 보안 모델링을 수행할 수 있으며, 취약성 매트릭스를 통하여 정량적으로 취약성을 분석할 수 있다[8,9,10].

본 연구에서는 SIMVA를 이용하여 최근 네트워크 보안 문제에 심각한 영향을 미치는 슬래머 웹 공격 시나리오에 대한 취약성 분석을 수행함으로써, SIMVA의 검증 및 적용 가능성을 제시한다.

2. 관련연구

2.1. 시물레이션 기반 취약성 분석 방법론

<그림 1>은 SIMVA에 적용된 시물레이션 기반의 취약성 분석 방법론을 나타낸다.



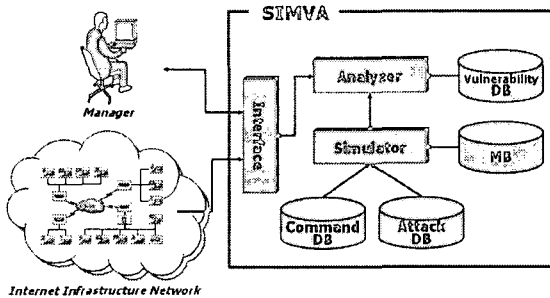
<그림 1> 시물레이션 기반 취약성 분석 방법론

1단계는 개념적인 명세 단계를 보여준다. 이 단계에서 해당 네트워크 시스템의 분할, 분류, 커플링 등의 관계들이 SES에 의해 명시될 수 있다. 2단계에서는 공격자와 분석자 모델뿐만 아니라 네트워크의 각 구성 요소들의 모델들이 DEVS 형식론으로 생성되고 MB안에 저장된다. 특히 선/후행처리 조건을 사용한 명령어 레벨 모델링은 다양한 서비스에서 사용된 명령어들을 그룹 단위로 묶고, 명령어들을 분류하는 것으로 이루어진다. 3단계에서는 SES로 정의된 네트워크 구조에 따라 MB안에 저장되어 있던 모델들을 통합함으로써 시물레이션 모

델이 생성된다. 이로써 다양한 사이버 공격에 대한 시뮬레이션을 수행할 수 있다. 마지막으로 4단계에서 시뮬레이션 수행의 결과에 취약성 매트릭스를 적용함으로써 각 네트워크 구성 요소들의 취약성들을 정량적으로 분석한다 [11,12].

2.2. SIMVA 소개

시뮬레이션 기반의 네트워크 취약성 분석 시스템인 SIMVA는 현재 Visual C++로 구현되었으며, <그림 2>는 SIMVA의 구조도를 나타낸다.



<그림 2> SIMVA의 구조도

Analyzer는 먼저 Interface를 통해 Internet Infrastructure Network에서 수집된 정보를 받고 그 정보를 Simulator에게 보내게 된다. Simulator는 MB로부터 주어진 네트워크의 모델 구조를 생성하고, 각 모델들을 초기화한다. 그 후 Simulator는 Attack DB와 Command DB를 이용하여 사이버 공격에 대한 시뮬레이션을 수행하게 된다. 그리고 그 결과를 Analyzer에게 보고한다. Analyzer는 Vulnerability DB를 사용하여 취약성 매트릭스를 시뮬레이션 결과에 적용하고, 정량적인 방법으로 각 구성 요소의 취약성들을 분석한다. 끝으로 분석 결과는 Interface를 통해 관리자에게 보고된다.

<그림 2>에 나타난 주요 모듈 및 DB에 관한 설명은 다음과 같다.

- Interface : 관리자와 시스템 간의 의사

소통을 지원한다.

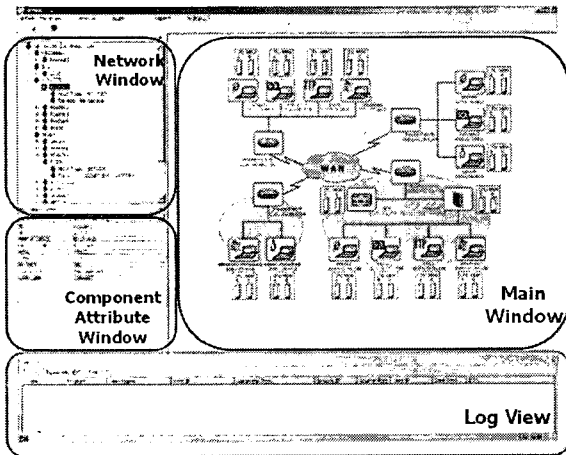
- Analyzer : Simulator에 의한 시뮬레이션을 이용하여 노드, 링크, 네트워크 취약성들을 분석한다.
- Simulator : 취약성들과 대응 전략 등을 평가하기 위한 시뮬레이션을 수행한다.
- MB : 해당 네트워크의 구성 요소들의 DEVS 모델들을 포함한다.
- Command DB : 명령어에 대한 DB로서 실행 전의 조건과 실행 후의 상태 등을 정의해 놓은 DB이다.
- Attack DB : 공격 시나리오에 대한 DB이다. 공격 시나리오는 명령어들의 집합으로 구성되어 있다.
- Vulnerability DB : 취약성들을 분석하기 위해 취약성들을 정의해 놓은 DB이다.

SIMVA는 다음과 같은 두 가지의 모드를 지원한다.

(1) 모니터링 모드

Internet Infrastructure Network와 실시간으로 모니터링 한 정보뿐만 아니라 각 구성 요소들의 속성들을 보여준다. 그림 3은 SIMVA의 메인 화면 중 모니터링 모드를 나타내고 있다. 그림 3에서 모니터링 모드의 메인 화면은 네트워크 윈도우, 컴포넌트 애트리뷰트 윈도우, 메인 윈도우 및 로그 뷰의 4가지 구성 요소로 이루어져 있다. 네트워크 윈도우는 네트워크 그룹들에 대한 정보를 트리 형식으로 보여주며 각 해당 네트워크에 연결된 호스트들을 나타낸다. 컴포넌트 애트리뷰트 윈도우는 각 호스트의 정보를 보여준다. 네트워크 윈도우나 메인 윈도우에서 관리자가 임의의 호스트를 선택하면 선택된 호스트에 대한 정보가 컴포넌트 애트리뷰트 윈도우에 나타나게 된다. 호스트의 정보로는 호스트 이름, IP 주소, OS 버전, 서비스 종류 등이 제공된다. 메인 윈도우는 모든 네트워크들의 연결 상태를 보여주며 각각의 호스트들의 상태를 그래프로 보여

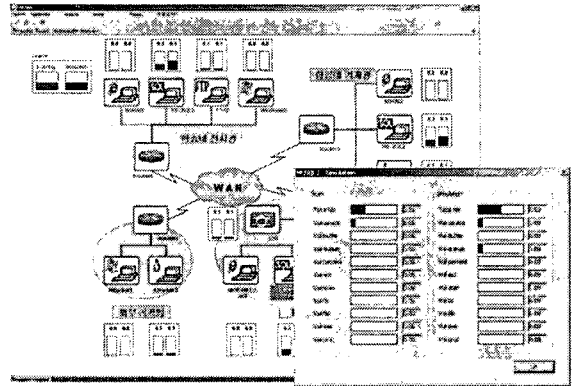
줌으로써 관리자가 위험한 호스트의 상태를 효과적으로 알 수 있도록 한다. 마지막으로 로그 뷰는 SIMVA와 연결된 호스트들로부터 주기적으로 모니터링 되는 로그 정보들을 보여주며 이 로그를 통해서 전체 네트워크의 변화를 알 수 있다.



<그림 3> SIMVA의 모니터링 모드

(2) 분석 모드 (시뮬레이션 모드)

사이버 공격 시뮬레이션을 통하여 정량적인 방법으로 해당 네트워크의 노드와 네트워크 취약성을 분석한다. 그림 4는 SIMVA의 분석 모드 화면을 보여준다. 그림 4의 메인 화면에서 각각의 네트워크 구성원은 취약성 정보를 정량적으로 나타내기 위하여 두 개의 그래프를 갖는다. 왼쪽 그래프는 분석 대상 네트워크를 스캐닝하여 분석한 정적인 취약성 값을 나타내며 오른쪽 그래프는 다양한 사이버 공격 시나리오를 적용하여 시뮬레이션을 수행한 후 분석되는 동적인 취약성 값을 나타낸 것이다. 또한, 메인 화면에서 임의의 호스트를 선택하면 선택된 호스트에 존재하는 개별 취약성 항목들에 대한 상세한 취약성 값을 확인할 수 있다.



<그림 4> SIMVA의 분석(시뮬레이션) 모드

3. SIMVA를 이용한 취약성 분석 : Slammer Worm의 예

본 논문에서는 지난 2003년 1월 25일에 발생한 Slammer Worm 바이러스에 의한 공격을 모델링하고 시뮬레이션을 수행하여 취약성을 분석하였다.

3.1. 테스트베드의 구성

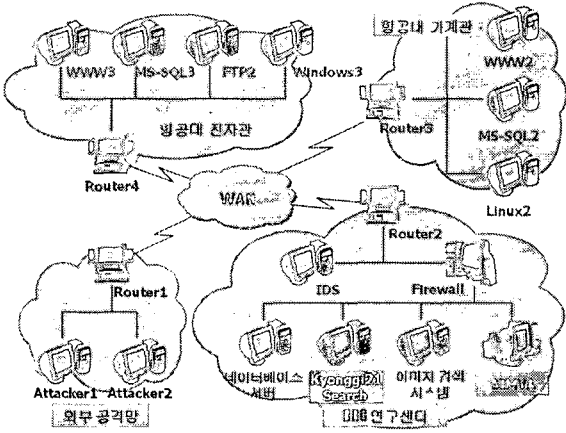
테스트베드는 그림 5와 같이 공격자가 포함된 외부 공격망과 공격의 대상이 될 수 있는 3개의 네트워크(전자관, 기계관, RRC 연구센터)로 구성된다. 각 네트워크는 MS-SQL 서버를 포함한 리눅스 서버, 웹 서버, 윈도우 서버 등으로 구성되며, MS-SQL 서버들은 패치가 이루어지지 않은 상태로 설정하였다.

3.2. 시뮬레이션의 진행

시뮬레이션의 진행은 먼저 외부 공격망의 공격자가 항공대 기계관 네트워크의 MS-SQL2 서버에 Slammer Worm 바이러스 공격을 시도하게 된다. 패치가 이루어지지 않은 MS-SQL2 서버는 공격에 그대로 노출되게 된다. 공격 받은 MS-SQL2 서버는 Slammer Worm 바이러스 감염 후 무수히 많은 양의 Slammer Worm

패킷을 발생시켜 임의의 주소로 전파한다.

일정 시간의 시뮬레이션 진행 후, 시뮬레이션 결과의 분석을 통하여 예상되는 동적 취약성을 분석한다.



<그림 5> 테스트베드 구성도

3.3. 취약성 분석

SIMVA는 노드와 네트워크의 취약성 매트릭스를 이용하여 정량적으로 취약성을 분석한다[13].

3.3.1. 노드 취약성

노드 취약성은 각 네트워크 구성 요소들이 현재 뿐만 아니라 잠재적으로 가지고 있을 수 있는 포괄적인 취약성 항목을 포함한다. 현재의 취약성 항목은 시간의 흐름에 관계없이 존재하는 정적인 취약성을 의미하며, 잠재적인 취약성 항목은 시뮬레이션을 통하여 분석할 수 있는 발생 가능한 취약성을 의미한다. 네트워크에 있는 구성 요소들은 그 요소 자체의 설정값 등에 의해 취약성 항목 중의 일부 항목들을 가지게 된다.

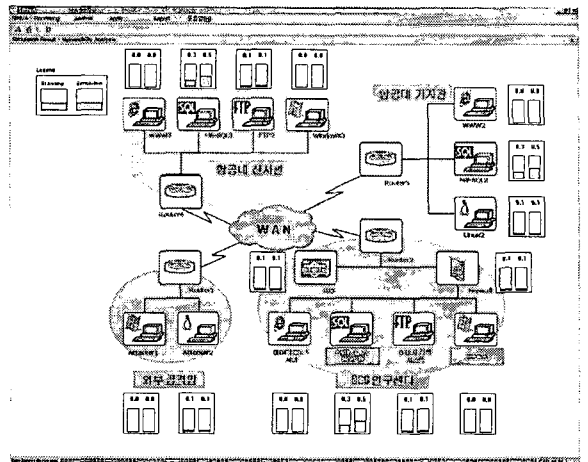
노드 취약성은 각 취약성 항목의 임팩트 값을 곱한 것의 산술평균으로 정의된다. 예를 들어, 1은 시스템의 완전한 통제 또는 마비가 가능한 정도의 취약성의 존재를 의미하고, 0.5는

일반 정보의 유출이 가능한 정도의 취약성이 존재함을 의미하며 0은 취약성이 없는 경우를 나타낸다. i 번째 요소의 노드 취약성 값 NV_i 는 다음과 같이 정의된다.

$$NV_i = \frac{\sum_{j=1}^n (w_j \times vul_j)}{\sum_{j=1}^n w_j} \quad (1)$$

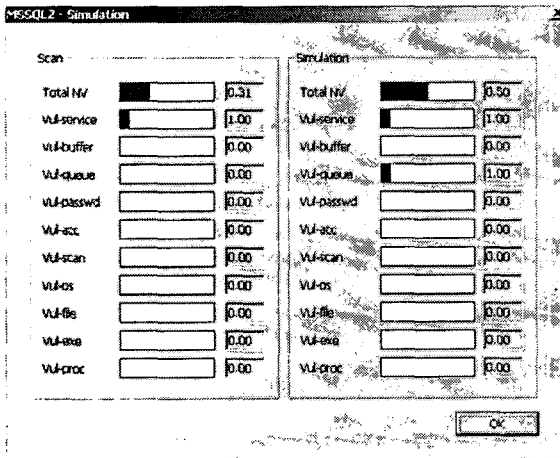
w_j 와 vul_j 는 각각 임팩트 값과 취약성 항목들 중의 j 번째 항목의 값을 나타내며, n 는 구성원에 대한 취약성 항목의 총 개수를 나타낸다. 임팩트 값은 해당 취약성을 이용한 사이버 공격이 성공했을 때 피해 정도를 나타내는 값으로서 0부터 1사이의 범위의 값을 갖는다.

<그림 6>은 시뮬레이션이 완료된 이후의 각 노드의 노드 취약성을 나타낸다. 왼쪽 그래프는 정적 취약성 값을 나타내고, 오른쪽 그래프는 정적 취약성을 포함한 동적 취약성 값을 나타낸다. MS-SQL2 서버의 경우 정적 취약성 값이 0.3이고, 동적 취약성이 0.5이다. 즉, 시뮬레이션 과정에서 취약성 값이 0.2만큼 증가됨을 통하여 변경 가능한 취약성이 존재함을 알 수 있다.



<그림 6> 취약성 분석

<그림 7>은 MS-SQL2 서버의 노드 취약성을 구성하는 취약성 항목에 따른 취약성 값을 상세히 보여준다. 그림 6에서 Scan은 정적 취약성 항목의 값을 나타내며 Simulation은 동적 취약성 항목의 값을 나타낸다. 현재 10개의 취약성 항목이 정의되어 있으며 취약성 계산을 위하여 적용된 각각의 임팩트 값은 표 1과 같다.



<그림 7> MS-SQL2 서버의 노드 취약성 항목들

<표 1> 취약성 항목들의 각각의 임팩트 값

취약성 항목	임팩트 값
Vul-service	0.5
Vul-buffer	0.1
Vul-queue	0.3
Vul-passwd	0.1
Vul-acc	0.1
Vul-scan	0.1
Vul-os	0.1
Vul-file	0.1
Vul-exe	0.1
Vul-proc	0.1

<그림 6>에서 MS-SQL2 서버의 노드 취약성 중 정적 취약성은 각 취약성 항목의 값과 (1)번 식 및 <표 1>에 의해 다음과 같이 얻을

수 있다.

$$\frac{1 \times 0.5}{(0.5+0.1+0.3+0.1+0.1+0.1+0.1+0.1+0.1+0.1)} = 0.31$$

즉, 서비스 패치와 관련된 service 취약성 항목의 값이 존재함으로 인하여 0.31의 취약성 값이 얻어지며, 이를 통하여 MS-SQL2 서버가 웹 공격과 같은 추가적인 공격이 가능한 정도의 취약성이 존재함을 정량적으로 분석할 수 있다.

또한, MS-SQL2 서버의 노드 취약성 중 시물레이션 후의 동적 취약성은 정적 취약성과 같은 방법으로 다음과 같이 구할 수 있으며, 시물레이션을 통하여 queue에 대한 취약성이 증가됨에 따라 0.5의 취약성 값을 얻을 수 있다.

$$\frac{(1 \times 0.5) + (1 \times 0.3)}{(0.5+0.1+0.3+0.1+0.1+0.1+0.1+0.1+0.1+0.1)} = 0.5$$

즉, 공격받은 MS-SQL2 서버는 웹 바이러스 감염 후 무수히 많은 양의 Slammer Worm 패킷을 발생시키기 때문에 큐의 용량이 초과되어 서비스 중지 상태에 이르게 될 수 있다. 이와 같이 동적 분석을 통하여 노드의 취약성을 정량적으로 예측할 수 있다.

3.3.2. 네트워크 취약성

네트워크 취약성은 네트워크의 전반적인 취약성에 대한 종합 평가를 위한 방편으로 사용될 수 있으며, 해당 노드의 취약성 값들에 대한 산술 평균으로 간단히 얻을 수 있다. 예를 들어 1은 시스템의 완전한 통제 권한 획득 또는 마비가 가능함을 의미하며, 0.5는 일반 정보 유출이 가능한 정도의 취약함을 나타내고 0은 피해 가능성이 없는 안전한 상태를 의미한다. i 번째 네트워크 취약성, $NetV_i$ 는 다음과 같이 구할 수 있다.

$$NetV_i = \frac{\sum_{j=1}^n (W_j \times NV_j)}{\sum_{j=1}^n W_j} \quad (2)$$

W_j 는 해당 네트워크에 대한 j 번째 노드의 중요도 가중치를 나타낸다.

<표 2>는 RRC 연구센터에 대한 네트워크 취약성의 예를 나타낸다. 표 2에서 가중치는 각 노드의 중요도에 따라 부여된 것이며, 노드 취약성은 SIMVA에 의하여 분석된 값이다. RRC 연구센터의 경우 0.15의 네트워크 취약성을 보임으로써 전반적인 취약성이 비교적 낮은 것으로 판단할 수 있다.

<표 2> 네트워크 취약성의 예 :
RRC연구센터

노드 이름	가중치 (W_j)	노드 취약성 (NV_j)	네트워크 취약성 ($NetV_{RRC연구센터}$)
IDS	0.5	0.1	$(0.5 \times 0.1 + 0.5 \times 0.1 + 0.5 \times 0.5 + 0.2 \times 0.1) / (0.5 + 0.5 + 0.3 + 0.5 + 0.2 + 0.5) = 0.15$
Firewall	0.5	0.1	
DB서버	0.3	0.0	
Kyonggi21 Search	0.5	0.5	
이미지검색 시스템	0.2	0.1	
SIMVA	0.5	0.0	

이와 같이 SIMVA를 이용하여 관리 대상이 되는 네트워크에 대한 각 노드의 취약성뿐만 아니라 전반적인 네트워크의 취약성을 정량적으로 분석, 평가함으로써 보안 정책에 따라 취약한 노드 및 네트워크를 효과적으로 관리할 수 있을 것으로 기대된다.

4. 결 론

네트워크에 대한 의존도가 높아짐에 따라 인터넷에 연결된 시스템의 취약성을 이용한 사이버 공격에 대한 피해가 급증하고 있는 실정이다. 기존의 취약성 분석 연구는 정성적인 연구가 대부분으로 다양하게 변화하는 정교한 해킹 기법에 대처하고, 다양한 경로들을 제공

하는 인터넷 기반 구조에 대한 침해 등에 적용하기에는 미흡하다. 이를 극복하기 위하여 네트워크 상태를 감시하고, 이를 토대로 시뮬레이션을 통하여 네트워크 취약성을 분석할 수 있는 SIMVA를 개발한 바 있다. 본 논문에서는 개발된 SIMVA를 이용하여 Slammer Worm 공격에 대한 취약성 분석을 성공적으로 수행함으로써 SIMVA의 검증 및 적용 가능성을 제시하였다.

향후 연구로서 자동 모델 생성에 관한 연구와 알려지지 않은 사이버 공격을 시뮬레이션을 통해 생성할 수 있는 방안 등에 관한 연구가 요구된다.

Acknowledgement

본 논문은 과학기술부 한국과학재단 지정 경기도 지역협력 연구센터(RRC)인 한국항공대학교 인터넷 정보검색 연구센터(IRC)의 지원에 의한 것임.

참고문헌

- [1] Longstaff T.A, et. al., "Are We Forgetting the Risks of Information Technology", IEEE Computer, 2000
- [2] <http://new.itfind.or.kr/KIC/etlars/industry/jugidong/1026/102603.htm>, Dec., 2001.
- [3] Aslam, T. A, Taxonomy of security faults in the unix operating system, M.S. thesis, Purdue University, 1995.
- [4] Bishop, M. A, "taxonomy of unix system and network vulnerabilities.", Tech. Rep. CSE-95-10, Dept. of Computer Science at the U. of California at David, 1995
- [5] Krsul, I.V., Software Vulnerability Analysis, PhD Thesis, Purdue University, 1998.
- [6] S. Hariri, et. al., "A Framework for Network Vulnerability Analysis", Communications,

- Internet and Information Technology 2002, Virgin Islands, USA, Nov., 2002.
- [7] You, Y.J., J.S. Lee, and S.D. Chi, "SIMVA : A tool for the Network Vulnerability Analysis", PROCEEDING of International Conference on Internet Information Retrieval 2003, Korea, Oct., 2003.
- [8] Zeigler, B.P., Multifaceted Modeling and Discrete Event Simulation, Academic Press, 1984.
- [9] Zeigler, B.P., Object-oriented Simulation with Hierarchical, Modular Models : Intelligent Agents and Endomorphic systems, Academic Press, 1990.
- [10] Zeigler, B.P., H. Praehofer and T.G. Kim., Theory of Modeling and Simulation 2ed., Academic Press, 1999.
- [11] Chi S.D., et. al., "Network Security Model- ing and Cyber-attack Simulation Metho- dology", Lecture Notes on Computer Science series, 6th Australian Conf. On Information Security and Privacy, Sydney, July, 2001.
- [12] Chi, S.D., J.S. Park, and J.S. Lee, "A Role of DEVS Simulation for Information Assurance", Lecture Notes in Computer Science series, 4th International Workshop On Information Security Applications, Jeju Island, Korea, August, 2003
- [13] Lee, J.S., J.R. Jung, and S.D. Chi, "Vulnerability Measures for Network Vulnerability Analysis System", Proc. of 2002 IRC International Conference on Internet Information Retrieval, Korea, Nov., 2002.

주 작 성 자 : 유 용 준

논 문 투 고 일 : 2004. 05. 09

논 문 심 사 일 : 2004. 09. 03(1차), 2004. 09. 06(2차),
2004. 09. 16(3차)

심 사 판 정 일 : 2004. 09. 16

○ 저자소개 ○



유용준

2003 한국항공대학교 컴퓨터공학과 학사
 2003~현재 한국항공대학교 컴퓨터공학과 석사 과정
 관심분야 : 모델링 및 시뮬레이션, 네트워크 보안



이장세

1997 한국항공대학교 전자계산학과 학사
 1999 한국항공대학교 컴퓨터공학과 석사
 2003 한국항공대학교 컴퓨터공학과 박사
 2004~현재 한국해양대학교 IT 공학부 전임강사
 관심분야 : 모델링 및 시뮬레이션, 네트워크 보안, 지능시스템 설계, 인공생명



지승도

1982 연세대학교 전기공학과 학사
 1984 연세대학교 전기공학과 석사
 1985~1986 두산 컴퓨터 (현 한국 디지털) 근무
 1991 미국 아리조나대학교 전기전산공학과 박사
 1991~1992 미국 SIMEX Systems and S/W 회사 S/W 담당자로 근무
 1992~현재 한국항공대학교 컴퓨터공학과 교수
 관심분야 : 이산사건 시스템 모델링 및 시뮬레이션, 컴퓨터 보안, 지능시스템 디자인 방법론, 시뮬레이션 기반 인공생명, 교통 모델링