한국시뮬레이션학회 '00추계학술대회 논문집 2000.11.11 아주대학교

SES/MB 프레임워크를 이용한 네트워크 보안 모델링 및 사이버 공격 시뮬레이션*

Network Security Modeling and Cyber Attack Simulation Using the SES/MB Framework

정기찬, 이장세, 김환국, 정정례, 박종서, 지승도
한국항공대학교 컴퓨터공학과
Tel: 02-3158-4866 Fax: 02-3158-6748
E-Mail : prayccc@mail.hangkong.ac.kr

Ki-chan Jung, Jang-se Lee, Hwan-kuk Kim, Jung-rea Jung, Jong-seo Park, Sung-do Chi
Department of Computer Engineering
Hangkong University, Seoul, KOREA

요 약

본 논문은 계층 구조적이고 모듈화 된 모델링 및 시뮬레이션 프레임워크를 이용한 네트워크 보안 모델링과 사이버 공격에 대한 시뮬레이션 기법의 연구를 주목적으로 한다. 단순한 네트워크 모델에서의 원인-결과 모델을 대상으로 시뮬레이션 하는 기존의 접근방법과는 달리, 복잡한 네트워크 보안 모델과 모델 기반의 사이버 공격에 대한 시뮬레이션 기법은 아직까지 시도된 바가 없는 실정이다. 따라서, 본 논문에서는 첫째, System Entity Structure/Model Base(SES/MB)을 통하여 계층 구조적, 모듈화, 객체지향적 설계를 하였고 둘째, 해킹 행위의 상세분석을 위해 취약성을 고려한 명령어 수준의 네트워크 보안 모델링 및 시뮬레이션 방법론을 제안하였다. 마지막으로, 사이버 공격 시나리오를 이용한 사례연구를 통하여 타당성을 검증하였다.

I. 서론

정보화의 진전에 따라 사회시설 전반이 정보통신기반 기술을 이용하여 자동화되고, 이에 따라 점점 더 정보시스템 및 정보통신망에 의존하고 있으며, 이러한 기반시설들이 국가의 경제 및 안보에 막대한 영향을 미치고 있는 실정이다. 한편, 주요 기반 구조를 구성하는 네트워크 구성요소가 검증이 안된 상용의 정보통신기반 시스템 제품을 사용함에 따라 기반구조는 외부의 공격에 취약성을 띠게 되어, 지난 수년간 이에 관련된 해킹사례가 급증하고 있다. 이러한, 해킹 및 사이버테러 등 주요 기반구조 침해위협을 방지하기 위해서는 주요 기반구조를 소유, 운영 및 관리하는 공공기관 및 산업체의 보호노력을 통합하고 조정하는 노력이 필요하다. 이와 같은 정보보증 달성 방법중의 하나가 정보기반구조의 모델링 및 시뮬레이션 접근으로서, 이를 통하여 정보기반구조에 대한 다양한 위협영향 평가는 물론 현재의 보안 대책의 평가 및 대안 제시에 효과적으로 활용할 수 있을 것으로 인식되고 있다[1]. 최근에 Cohen[2]은 보안관련 모델링과 시뮬레이션 수행 시 모델의 정확성, 데이터의 정확성 및 방대한 시뮬레이션 스페이스 등의 제한이 문제가 된다고 지적하였고 이러한 이유에서 노드와 링크만으로 표현되는 네트웍 모델, 원인-결과 모델, 특성함수들, 의사난수 발생기만으로 구성되는 단순한 네트웍 모델을 제안하여 주목받은 바 있다. 그러나 원인-결과 모델[2]을 기반으로 한 사이버 공격과 방어의 표현은 너무 단순하

* 본 연구는 정보보호센터 위탁과제로 수행 중인 "정보통신기반 네트워크 모델링 및 검증"에 관한 연구로 수행됨

기 때문에 실제 적용을 하는데 어려움이 있다. 그리고 Amoroso가 제안한 침입 모델[3]은 침입을 연속적인 행동으로 나누어 볼 수 있다는 장점을 가지는 반면, 보안 메커니즘 중심의 표현으로 인해 컴퓨터 시뮬레이션 접근이 분명치 않은 단점을 가진다. 마지막으로 Nong Ye[4]의 접근은 복잡한 시스템에 대한 단계적 접근으로의 제안이 돋보이지만 이러한 단계를 적용한 모델링 및 시뮬레이션 기법에 대한 구체적인 제시가 없는 실정이다. 따라서 본 연구에서는 사이버 공격에 대한 명령어 수준의 접근을 통해서 모델링을 시도하고 이산 사건 시뮬레이션 기법을 적용하여 현존하는 해킹에 대한 취약성을 고려한 네트워크 보안 모델링을 하고 시뮬레이션을 수행하였다.

II. SES/MB를 이용한 네트워크 보안 모델링 방법론

SES/MB는 Zeigler에 의해 제안된 개념으로 시뮬레이션의 동역학적 방법론과 AI의 기호적 방법론을 체계적으로 통합함으로써 시스템 모델링 및 시뮬레이션 환경을 제공한다. SES/MB는 System Entity Structure와 Model Base의 두 구성원으로 이루어진다. SES는 시스템의 구조적 특성을 나타내는 것으로 선언적 성격을 가지며 구성관계, 구성원의 종류, 구성원들의 결합구조, 그리고 제약조건 등의 구조적 지식을 표현할 수 있는 수단을 제공한다. MB는 시스템의 행위적 특성을 나타내는 것으로서 절차적 성격을 가지며 동역학적이고 기호적으로 행위를 표현할 수 있는 수단을 제공하는 모델들로 구성된다[5,6].

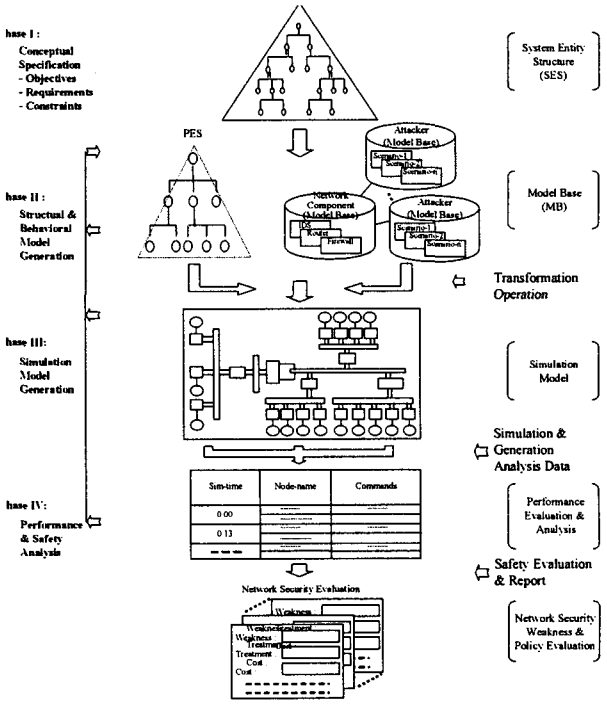

그림 1. 시뮬레이션 모델링 방법론

본 논문에서 제안하는 시뮬레이션 모델링 방법론의 개념도는 그림1과 같다. 그림 1의 Phase I은 개념 명세화 단계로서, 정보통신기반 네트워크의 전반적인 구조를 도식화하는 단계이다. 이 단계에서는 시스템의 구성관계, 구성원의 종류, 구성원들의 결합구조, 그리고 제약조건 등의 구조적 지식의 표현수단을 제공한다. Phase II는 이미 라이브러리화 되어 있는 Attacker 모델베이스의 각종 사이버 공격 시나리오 데이터 및 컴포넌트 모델들을 Phase I의 구조로부터 얻어진 PES 즉, 시뮬레이션 대상 네트워크 구조와 통합시키는 단계로서, 사이버 공격 시나리오 모델, 네트워크 컴포넌트 모델 등을 포함하고 있다. 이러한 데이터 와 구조적 및 동역학 모델들을 통합시킴에 의해 Phase III에서의 최종적 시뮬레이션 모델이 생성되어 시뮬레이션이 수행된다. 마지막 Phase IV에서는 시뮬레이션 수행 결과에 대한 통계 자료를 제공함으로써 정보기반구조에 대한 다양한 위협영향 평가는 물론 현재의 보안 대책의 평가 및 대안 제시에 효과적으로 활용할 수 있다.

III. 네트워크 보안 모델링

3.1 네트워크 구조 모델링

정보통신기반 네트워크의 전반적인 구조인 시스템의 구성관계, 구성원의 종류, 구성원들의 결합구조, 그리고 제약조건 등은 구조적 지식의 표현수단을 통하여 모델링한다.

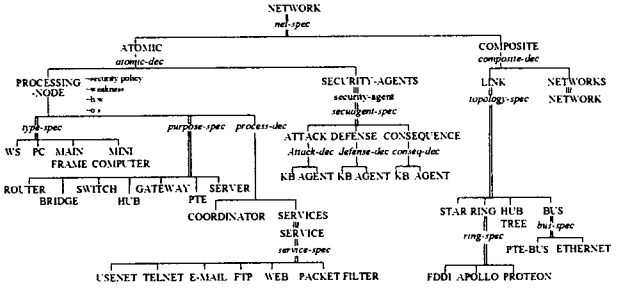

그림 2. 네트워크 보안 모델의 SES

그림 2은 정보통신기반 네트워크 보안 모델의 SES를 나타낸다. 최상위 *entity*인 NETWORK은 단일 네트워크로 구성되는 ATOMIC과 다중 네트워크로 구성될 수 있는 COMPOSITE의 두 구성원으로 분할되고 있다. ATOMIC은 다시 PROCESSING-NODE와 보안 요소를 고려한 *multiple entity*인 SECURITY-AGENTS로 분할되는데, PROCESSING-NODE는 다시 COORDINATOR와 다수의 SERVICES로 분할되며 type과 purpose에 따라서 분류될 수 있다. COMPOSITE은 여러 다중의 네트워크 그룹을 연결할 수 있는 *multiple entity*인 NETWORKS 노드와 이들을 연결시킬 수 있도록 LINK로 분할된다.

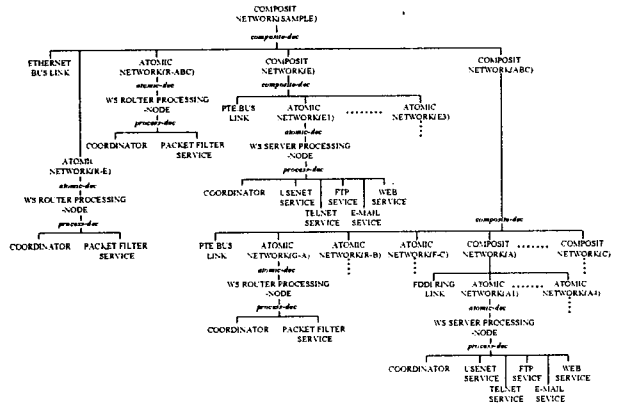

그림 3. 네트워크 보안 모델의 PES

그림 3은 이와 같이 구축된 SES에 pruning 과정을 적용하여 얻은 하나의 Sample 네트워크의 구조를 나타낸 것으로 이렇게 생성된 대상 시뮬레이션 구조상의 각 en-tity마다 동역학 모델이 합성됨에 의해 최종적 시뮬레이션 모델이 구축될 수 있다.

3.2 네트워크 컴포넌트 모델링

네트워크 상에 존재하는 여러 구성원 PC, Server, Workstation, Main Frame, Printer 등을 행동적인 특성에 따라 모델링 한다.

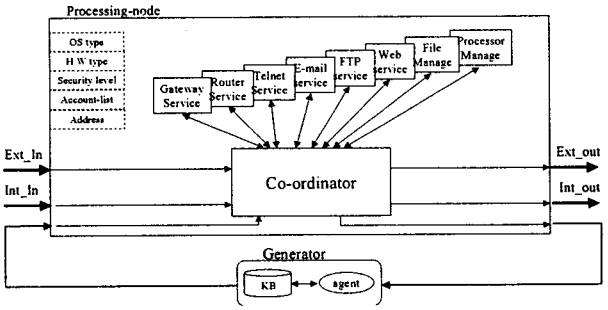

그림 4. 모델의 행동적 특성(프로세스 노드)

그림 4는 네트워크 망의 노드에 대한 동역학 모델의 행동적 특성을 나타낸 것이다. 모든 노드는 통일된 형태를 가지면서 제공하는 서비스의 존재 여부로 그 특성이 결정되며, 노드는 각각 O/S type, H/W type, Address, Account list, 시스템 파일 같은 여러 속성을 가진다. 또한 제공할 수 있는 서비스로 표현될 수 있는 여러 모델을 가지고 있으며, 이 모델들을 통해서 서비스를 할 수가 있게 된다. 그리고 packet을 생성하는 Generator 모델을 통해서 다양한 packet을 생성함으로 시뮬레이션을 진행할 수 있게 된다.

그림 5. 가상 패킷

그림 5는 시뮬레이션 수행 시 노드간의 통신을 위하여 사용되는 가상 패킷을 나타내고 있다. 패킷은 인터넷 프로토콜 IPV4를 일반적으로 사용하고 있으며 이에 상위 계층이나 하위계층에 따라서 패킷의 헤더부분을 추가하거나 제거하게 된다[7]. 그러나 네트워크 보안 모델링이 일반 네트워크의 성능 분석 모델링과는 다른 목적을 가짐으로 시뮬레이션에 사용되는 패킷을 실제 패킷의 형태 중에서 네트워크 보안 시뮬레이션을 하는데 필요한 부분만을 모델링 하였다.

3.3 명령어 모델링

네트워크 구성요소들에 대한 사이버 공격 시나리오에 의한 명령어 수준의 시뮬레이션을 위하여 먼저 시스템에서 사용되는 명령어를 그룹화하고 특성화하였다. 구성요소의 한 종류로 설정한 유닉스 시스템은 수많은 명령어를 가지고 있지만 본 연구에서는 그중 일부분에 대하여 선후행조건 모델링을 수행하였다.

[표 1] Telnet 명령어의 선후행조건 모델링

명령어	선행조건	결과	후행조건
more		파일들의 리스트 한 페이지씩 출력	
pwd	작업 디렉토리 확인	현재의 작업 디렉토리 출력	
rmdir	디렉토리 확인	디렉토리 제거	디렉토리 속성 변경
cd	디렉토리 존재 여부 확인	디렉토리 이동, 변경	디렉토리 속성 변경
vi	파일 존재 여부 확인	파일 편집	파일관련 속성 변경
mv	파일 존재 여부 확인	파일 이름 바꾸기	파일관련 속성 변경
rm	파일 존재 여부 확인	파일 삭제	파일관련 속성 변경
chmod	파일 존재 확인	파일의 허가권 변경	파일 소유 변경

표 1은 Telnet 명령어를 선행조건과 결과, 후행조건으로 분류한 선후행조건 모델링 표이다. 각각 1) 선행조건은 명령어가 실행되기 위한 조건에 대한 내용, 2) 결과는 명령어의 처리로 나오는 결과 내용, 3) 후행조건은 명령어를 수행한 후에 그 명령어로 인해서 변경되는 노드나 서비스의 속성에 대한 내용을 나타낸다. 예를 들어서 rmdir 명령어를 실행하려면 선행조건으로 삭제하려는 디렉토리가 존재해야 하며 그 결과로 디렉토리 제거라는 결과가 반환이 되며 마지막, 후행조건으로 디렉토리의 속성을 변경하게 된다. 노드에서 필요한 명령어를 표 1과 같은 형태로 분류를 하는 것은 사이버 공격 시나리오를 가지고 시뮬레이션 하는데 정형화된 방법을 제공할 수 있는 장점을 가진다.

3.4 취약점 모델링

표 2는 Telnet 서비스에서 발생할 수 있는 취약점을 나타낸다. 노드에는 관리자의 설정상 실수로 인한 취약점 또는 시스템이 가지는 버그로 인한 취약점 등의 여러 가지 이유로 취약점이 존재하게 된다. 이러한 취약점 항목은 노드의 속성으로 표현되어 노드의 취약점을 나타내며 이는 시뮬레이션에 사용된다. 취약점은 모두 3 단계로 정의될 수 있는데 1) 가장 취약한 '취약'단계, 2) 주의를 요하는 '주의'단계, 3) 안전한 '안전'단계로 분류 된다. 각 단계를 나누는 기준은 시스템의 용도나 중요도에 따라 정할 수 있다.

IV. 사례연구

4.1 네트워크 예

본 절에서는 임의의 가상 네트워크에 대한 사례연구를 통하여 제안한 방법론의 타당성 검토와 함께 가상 네트워크에 대한 사이버 공격 시나리오를 시뮬레이션 수행하였다.

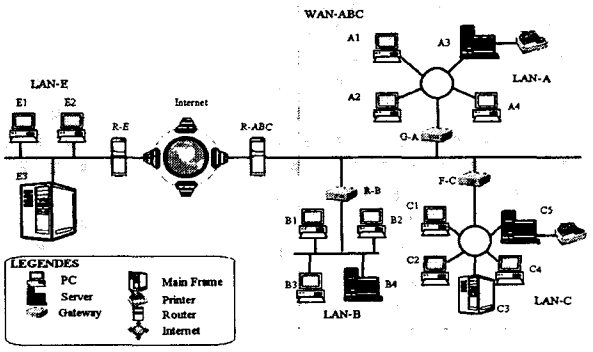

그림 6. 가상 네트워크

그림 6은 시뮬레이션을 수행할 가상 네트워크를 나타내고 있다. 가상 네트워크의 구성은 여러 대의 컴퓨터와 서버로 이루어진 LAN, 그리고 Ring, bus같은 Topology, 여러 개의 LAN으로 이루어진 WAN이 인터넷을 사이에 두고 라우터를 통한 연결로 이루어진다. 또한 각각의 노드마다 패킷생성기(공격자)가 연결이 될 수 있어서 어떤 노드든지 패킷을 생성할 수 있으며 노드에 연결이 되어 있는 패킷생성기(공격자)가 패킷을 생성하게 되면 그 패킷은 노드 모델, Topology 모델, 라우터 모델 등을 통하여 목표 노드 모델로 이동하게 된다. 패킷을 입력받은 노드 모델은 그 패킷에 입력된 명령어에 대한 처리를 한 후 같은 방법으로 응답을 하게 된다.

[표 2] Telnet 서비스 취약점에 관한 분류

취약점 항목	취약점 항목 상세 설명	단계	조건
패스워드	패스워드가 없는 사용자 일반단어(영어/한글)를 패스워드로 사용하는 사용자 아이디와 비밀번호가 같은 사용자가 존재하는가?	안전	없음
		주의	5명 이내 존재
		취약	5명 이상 존재
시스템 부팅 패스워드	시스템 부팅 패스워드가 등록되어 있는가?	안전	등록됨
		주의	
		취약	등록 안됨
패스워드 파일	/etc/passwd 파일의 변조 및 구조적 문제점이 있는가?	안전	root만 권한
		주의	root외 권한 3명 이하
		취약	root외 권한 3명 이상
사용자 홈 디렉토리	사용자 홈 디렉토리의 존재여부 및 접근권한 설정상의 취약점이 있는가?	안전	사용자 소유자 동일
		주의	사용자 소유자 다름5명이하
		취약	사용자 소유자 다름 5명 이상
사용자 파일	.login, .profile, .cshrc, rhosts 등 사용자 홈 디렉토리에 있는 각종 환경 파일에 접근 가능한가?	안전	모든 사용자 접근 안됨
		주의	모든 사용자 접근 2명이하
		취약	모든 사용자 접근 가능

4.2 사이버 공격 시나리오

사이버 공격 시나리오는 사이버 공격을 연속적인 행동으로 표현하며, 이를 통하여 사이버 공격 시뮬레이션을 수행할 수 있다. 사이버 공격 시뮬레이션 테스트를 위하여 다양한 시나리오에 따른 실험이 가능하나, 본 논문에서는 제한된 지면관계로 다음과 같은 간단한 시나리오의 경우를 가지고 설명한다.

시나리오 : SUN에서 오래된 버그를 통해 어떻게 사용자 계정이 없는 시스템에 일반 계정을 획득하여 시스템에 액세스하는지에 대한 경우[8,9,10,11,12].

표 3은 일반계정 획득 시나리오에 대한 가상 공격 시나리오를 선후행조건 모델링으로 표현한 것이다. 먼저 showmount의 결과를 통해서 마운트를 할 수 있는 디렉토리를 확인하고, mkdir을 통해서 마운트를 할 디렉토리를 해커의 시스템에 생성하여 mount 명령어를 통하여 마운트를 할 수 있는 디렉토리를 해커의 시스템에 마운트 한다. 이를 통하여 목표 사이트의 홈 디렉토리를 해커 컴퓨터에 생성된 디렉토리로 마운트 시키게 된다. 다음으로 어떠한 파일이 있는지 ls를 통해서 확인하고 해커의 시스템에서 어떤 사용자로 로그온 했는지 id로 확인한 후에 echo 명령을 통해서 etc/passwd 파일에 사용자 정보를 불법으로 입력하고, su를 통해서 그 사용자로

[표 3] SUN O/S 명령어의 선후행 조건 분석표(일반계정 획득 관련)

순서	명령어	선행조건	결과	후행조건
1	showmount	가능한 디렉토리 확인	디렉토리 출력	
2	mkdir	같은 디렉토리 확인	디렉토리 생성	디렉토리 속성 변경
3	mount	디렉토리 권한 확인	디렉토리 마운트	마운트 속성 변경
4	ls		파일 리스트 보여줌	
5	id		현재 사용중인 사용자, 그룹 표시	
6	whoami	아이디 존재 확인	로그인한 아이디 표시	
7	echo	파일에 쓸 권한 확인	파일에 정보를 씀	파일 속성 변경
8	su	사용자 존재 확인	사용자가 바뀐다	현재 사용자 속성 변경
9	echo	파일에 쓸 권한 확인	rhost에 정보를 씀	파일 속성 변경
10	rlogin	IP 확인	접속 성공	

상태를 변경한 다음, rhost 파일에 모든 사용자가 다 액

세스 가능하도록 편집을 수행하게 되면 최종적으로 사용자로 등록되어 있지 않은 사이트에 rlogin을 통해서 액세스를 할 수 있게 된다.

4.3 시뮬레이션 테스트

표 4는 표 3의 사이버 공격 시나리오에 대한 시뮬레이션 결과를 Cohen의 시뮬레이션 결과[2] 형태로 나타낸 것이다. What은 노드가 어떤 상태(Attack, Process)인지를 나타내며 Node는 현재 시뮬레이션 결과를 보여주는 노드의 이름, Time은 시뮬레이션 시간, 두 번째 What은 포트를 통하여 입력된 명령어와 출력된 결과를 나타낸다. 또한 Details는 명령어로 인한 노드의 변화를 자세히 나타낸다. 가상 공격 시뮬레이션은 두 개의 노드(Genr-PC1E와 TELNET_PS1C)가 패킷을 주고받으면서 진행이 되며 Genr_PC1E 모델이 TELNET_PS1C 모델을 향하여 showmount라는 명령어를 패킷에 실어서 보내게 되면 이 패킷은 링크 모델과 라우터, 게이트웨이 모델 등을 거쳐 TELNET_PS1C 모델의 포트를 통해서 입력되게 된다. 이 패킷에 대해서 TELNET_PS1C 모델은 패킷에 있는 명령어를 처리하여 그 명령어가 처리되었다는 결과를 다시 링크 모델과 라우터, 게이트웨이 모델 등을 통해서 Genr_PC1E 모델로 전달하게 된다. 이와 같이 Genr_PC1E와 TELNET_PS1C 모델은 보내고 받은 패킷을 통해 명령어를 처리하면서 시뮬레이션을 진행하게 되며, 시나리오 중 TELNET_PS1C 모델의 경우 포트를 통해서 받은 패킷에 있는 명령어인 echo 'rapper::102:2::/tmp/mount:/bin/csh' >> /etc/p-asswd,에 의해 '/etc/passwd' 파일에 'rapper::102:2::/tmp/mount:/b-in/csh'라는 내용을 입력하여 파일의 속성이 변경된다.

본 연구를 통한 사이버 공격 시나리오의 시뮬레이션 결과는 앞서 설명했던 원인-결과 모델을 통한 시뮬레이션의 결과와 비교하였을 때 공격에 대한 원인이 바로 결과로 나오는 단순한 형태의 접근을 하는 것과는 달리 사이버 공격 행동을 형성하는 여러 연속적인 명령어에 대한 생성과 처리 결과를 볼 수 있기 때문에 더욱 상세하게 공격에 의한 시스템의 변화와 명령어의 결과를 알 수가 있고 더불어 노드에 내포된 취약점의 변화를 분석할 수 있다는 장점이 있다.

V. 결론

본 논문에서는 네트워크 보안 모델링 및 사이버 공격 시뮬레이션을 수행하는데 있어 SES/MB 프레임워크를 이용한 모델링 방법론의 제시와 함께 사이버 공격 시나리오를 통한 사례연구로 방법론에 대한 검증을 수행하였다. 본 연구는 기존의 연구에 비하여 1)SES/MB를 기반으로 시스템 이론적이며 소프트웨어공학적인 접근을 시도하였

[표 4] 시뮬레이션 결과의 예 : "일반계정 획득 시나리오"

What	Node	Time	What	Details
Attack	Genr_PC1E	0.000	showmount -r 204.253.148.004	Command of showmount
Process	TELNET_PS1C	1.300	showmount -r 204.253.148.004 Processing OK	Processing showmount command
Attack	Genr_PC1E	3.400	mount -nt nfs 204.253.148.004:/home /tmp/mount	Command of mount
Process	TELNET_PS1C	8.400	mount -nt nfs 204.253.148.004:/home /tmp/mount Processing OK	Mount dir
Attack	Genr_PC1E	10.500	echo 'rapper::102:2::/tmp/mount:/bin/csh' >> /etc/passwd	Command of each write file
Process	TELNET_PS1C	15.500	echo 'rapper::102:2::/tmp/mount:/bin/csh' >> /etc/passwd Processing OK	Processing each command then write data the file
Attack	Genr_PC1E	17.600	echo '+ +' > rapper/.rhosts	Command of each for write file
Process	TELNET_PS1C	22.600	echo '+ +' > rapper/.rhosts Processing OK	Rhost = SourceAddress
Attack	Genr_PC1E	24.700	rlogin 204.253.148.004	Command of rlogin
Process	TELNET_PS1C	29.700	rlogin 204.253.148.004 Processing OK	Check if(Rhost == inpak.SourceAddress) then user login

으며, 2) 명령어 수준의 상세 모델링을 통한 사이버 공격에 대한 세밀한 분석이 가능하고, 3) 다양한 공격 시나리오를 통한 사이버 공격 시뮬레이션이 가능하다는 특징을 갖는다. 향후 연구방향으로는 다양한 컴포넌트에 대한 모델링과 다양한 사이버 공격 시나리오에 대한 연구 그리고 개별 노드의 취약점을 통해 전체 네트워크에 대한 취약점 도출에 대한 깊이 있는 연구가 진행되어야 하겠다.

VI. 참고문헌

[1] 이철원, 김홍근, *정보보증:컴퓨터보안의 새로운 패러다임*, 정보과학회지, 제18권 제1호, pp53~61, 1월, 2000.

[2] Fred Cohen *Simulating Cyber Attacks, Defenses, and Consequences.*, 1999 IEEE Symposium on Security and Privacy Special 20th Anniversary Program, The Claremont Resort Berkeley, California, May 9-12, 1999.

[3] Edward Amoroso, *Intrusion Detection,* AT&T Laboratory, Intrusion Net Books. January, 1999.

[4] Nong Ye, Joseph Giordano, *CACS - A Process Control Approach to Cyber Attack Detection,* Communications of the ACM.

[5] B.P. Zeigler, *Object-oriented Simulation with Hierarchical, Modular Models: Intelligent Agents and Endomorphic systems*, Academic Press, 1990.

[6] S.D. Chi, *Modeling and Simulation for High Autonomy Systems,* Ph.D. Dissertation, Dept. of Electrical and Computer Engineering, Univ. of Arizona, 1991.

[7] 차동완, *개념으로 풀어본 정보통신 세계*, 영지문화사, 1996

[8] Anonymous, *리눅스 보안의 모든 것*, 인포북, 2000

[9] Welsh, Kaufman, *Running LINUX*, Oreilly, 1999

[10] 김효원, *쉽고 빠른 레드햇 리눅스 6.1*, 컴앤북스, 1999

[11] 다이구지 이사오, *통신 네트워크 시큐리티*, 도서출판 동서, 1998

[12] 권인택, *해커를 위한 파워 핸드북*, 파워북, 1999