네트워크 침입 탐지 및 방어를 위한 인터렉티브 시뮬레이션 프레임웍

이재혁° 윤주범 서정택 박승규° 최경희° 정기현°
아주대학교 정보통신 전문대학원°, 국가보안기술 연구소 정보보증연구부
{maestus°,sparky°, khchoi°, khchung°}@ajou.ac.kr, {netair ,jtseo}@etri.re.kr

Interactive Simulation Framework for Network Intrusion Detection and Defense Simulation

JaeHyuk Lee° JooBeom Yun JungTeak Seo SeungKyu Park° KyungHee Choi° Gihyun Jung°
Graduate School of Information and Communication Ajou University°, National Security Research Institut

요 약

네트워크 침입 탐지와 방어를 위한 연구는 실제 네트워크 환경을 구성하고, 실제 네트워크 침입을 통해 네트워크 침입 탐지와 방어 기법을 연구하는 것이 가장 좋은 방법이다. 하지만, 실제 네트워크 환경에서 대규모 네트워크를 구성하고, 네트워크 침입을 시도하여, 침입이 네트워크에 미치는 영향과 침입을 탐지하고 방어하는 방법은 많은 시간과 비용이 필요하게 된다. 그 대안으로 제안하는 시뮬레이션을 통한 연구는 시간과 비용은 줄이면서, 실제와 근사한 결과를 얻을 수 있다. 본 논문에서 제안하는 시뮬레이션 프레임웍은 대규모 네트워크 환경을 구성하고, 구성한 네트워크 환경 위에서 특정한 호스트로 네트워크 침입을 시도할 때, 네트워크 침입을 탐지 및 방어하기 위한 적절한 방법을 연구하기 위한 프레임웍으로, 특정한 공격의 목표가 된 호스트상에 IDS(Intrusion Detection System)나 Firewall을 설치하고, 시뮬레이션의 진행 중 실험자가 원하는 시간에 공격을 잠시 중단 시키고, 방어나 침입 탐지를 위한 IDS나 방화벽의 룰셋을 변경해 주는 방법을 통해 네트워크 침입 탐지 및 방어에 관한 유효적절한 방법을 실험 할 수 있게 해 준다. 본 시뮬레이션 프레임웍을 사용하여, 이후 좀 더 다양한 네트워크 침입 구현을 통해 다양한 침입 행동에 대한 적절한 침입 탐지 및 방어 기법에 관한 연구에 많은 도움이 될 것이다.

1. 서 론

인터넷의 발전으로 인해, 우리는 많은 정보를 네트워크를 통해 얻을 수 있게 되었다. 반면, 이러한 인터넷 환경을 통해 예전까지는 제한적이던 네트워크 침입의 위험에도 노출 되게 되었다. 하지만, 현대 네트워크의 방대함, 침입과 방어에 대한 이론적 체계의 부족, 침입과 방어의 복잡성과 다양성, 그리고 침입에 대한 정보 부족 등으로 인하여 아직까지 많은 연구의 진척이 없는 분야이기도 하다.

이러한 네트워크 침입 탐지와 방어를 위한 연구는 네트워크 환경을 구성하고, 구성한 네트워크 환경에서 특정한 공격 목표에 네트워크 침입을 시도하고, 방어하는 방법을 통해 이루어지고 있다. 하지만, 실제 대규모 네트워크 환경에서 이러한 실험을 하는 것은 현실적으로 불가능하거나, 많은 비용이 든다. 이에 실제 네트워크 환경과 유사한 동작을 하는 시뮬레이션을 통해 네트워크 침입 탐지와 방어에 대한 연구를 하는 것이 현실적으로 가장 적절한 방법이다. 현재 네트워크 침입 시뮬레이션에 대한 많은 연구가 이루어지고 있으며, 다양한 방법들이 사용되어지고 있다.[1,2]

그러나, 이러한 시뮬레이션 방식들은 침입 시나리오에 따라 순차적으로 또는 맹목적으로 시뮬레이션을 수행하기 때문에, 침입에 대한 탐지와 방어를 위한 실험에서 다양한 공격 패턴들과 기술들에 대해 실시간으로 방어와 탐지 기술들을 적용하기에는 어려움이 많다. 실시간으로 방어와 탐지 기술들을 시뮬레이션에서 수행하는 침입에 적용시켜 보기 위해서는 시뮬레이션 도중에 IDS (Intrusion Detection System)이나 Firewall 과 같은 방화벽의 룰셋을 바꾸는 것을 통해 구현 할 수 있다. 본 논문에서는 사용자가 원하는 시간 동안 다양한 침입을 첨가한 시나리오를 통해 특정 호스트를 공격할 때, 침입을 받는 특정 호스트에 설치된 IDS나 방화벽의 룰셋을 사용자가 희망하는 순간에 교체 하여, 침입에 대한 탐지와 방어의 유효성을 검사할 수 있는 시뮬레이션을 제안한다. 본 시뮬레이션을 사용하여, 이후 다양한 침입의 구현을 통해 새로운 침입 기법이나 기술들에 대한 탐지 및 방어 실험에 사용할 수 있을 것이다.

2. 관련연구

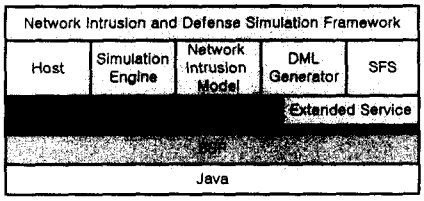
본 시뮬레이션 프레임웍은 SSFNet(Scalable Simulation Framework Net)을 기반으로 구현되었다.[3] SSFNet은 프로세스 기반 이산 사건 중심 시뮬레이션 커널(Process-based Discrete Event- oriented Kernel)이다. 네트워크의 시뮬레이션을 지원하는 라우터 링크 네트워크 인터페이스 카드 등 대부분의 인터넷 서브시스템들을 시뮬레이션 하는데 필요한 다양한 객체들이 Java로 구현되어 있어 시뮬레이션 특성에 맞추어 그들의 특성을 변경할 수 있다는 장점을 가지고 있다. SSFNet은 DML이라는 네트워크 토폴로지 설정 스크립트를 사용하여 대규모 네트워크 토폴로지를 구성하기 쉽고, 간단한 환경 설정을 사용해 1만개 노드 이상의 네트워크 환경에서도 빠르고 정확한 시뮬레이션 결과를 제공한다. 하지만, SSFNet은 네트워크 침입 및 방어 시뮬레이션을 위한 모듈들을 지원하지 않고 있고, 네트워크 침입의 특성을 고려한 구조를 가지고 있지 않다. 본 논문에서는 이러한 SSFNet의 단점을 보완하여, 네트워크 침입을 위한 인터렉티브 시뮬레이션에 적절한 프레임웍을 구현하였다.

본 논문에서 제안한 시뮬레이션 프레임웍은 다이나믹한 구조를 가지고, 시뮬레이션의 진행을 잠시 멈추고, 방화벽의 룰셋이나, 호스트의 정보, 네트워크 정보를 수정한 후, 다시 재실행이 가능한 형태를 제공하고, 이전의 시나리오로 롤백하는 기능

을 제공한다. 이러한 기능은 위에서 언급한 것과 같이 프레임웍이 다이나믹한 구조를 띄게 되며, 하나의 침입 시나리오에 대해 방어 기법의 변화나 호스트 정보의 변화, 네트워크 환경의 변화와 같은 시뮬레이션 환경의 변화가 시뮬레이션 도중에 변경 가능해 진다. 또한, 방화벽의 룰셋을 사용하여 방어 기법을 연구하는 것으로 인해, 제안한 프레임웍을 사용한 시뮬레이션 결과를 방화벽에 바로 적용 가능해 진다.

3. 시뮬레이션 프레임웍

본 논문에서 제안하는 인터렉티브 시뮬레이션 프레임웍은 SSFNet을 기반으로 구현된 시뮬레이션 프레임웍이다.



[그림 2 시뮬레이션 시스템 구조]

[그림 2]는 시뮬레이션 시스템의 구조를 보여준다. 기본적으로 JAVA로 구현된 SSF 시뮬레이션 프레임웍을 기반으로 하여, SSFNet위에 네트워크 침입 및 방어를 위한 인터렉티브 시뮬레이션 프레임웍을 구현한 시뮬레이션 프레임웍 구조이다.[4]

[그림 2]의 시스템 구성은 Host, Simulation Engine, Network Intrusion Model, DML Generator, SFS, Extended Service로 구성되어진다.

각각의 모듈은 시뮬레이션 프레임웍을 구성하고, 시뮬레이션을 구동 시키는 역할을 하고 있다.

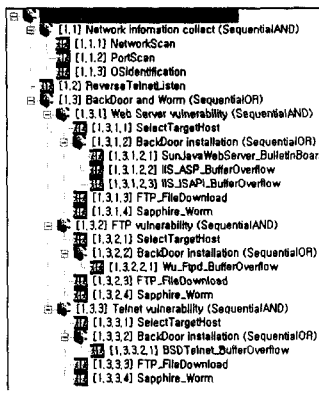
- Host : 시뮬레이션 프레임웍이 구성하는 노드를 표현한다. 노드의 네트워크 정보, OS 정보와 같은 환경정보를 구성하고 있다.
- Simulation Engine : 시뮬레이션 프레임웍의 가장 중요한 부분이다. 시뮬레이션을 구동시키고, 중지 시키는 역할을 하며, 순서대로 시나리오에 따라 시뮬레이션을 진행시켜준다.
- Network Intrusion Model : 침입 모델을 표현한다. 시뮬레이션에서 직접적인 침입 방법을 기술하고 있다.
- DML Generator : 위에서 언급했듯이 DML은 네트워크 토폴로지를 표현하는 언어이다. 구성은 도큐먼트 형식으로 이루어져있어, 표현하기 쉽고 편하다. 본 모듈은 GUI를 사용해 네트워크를 구성한 데이터를 DML로 바꾸어주는 모델이다.
- SFS : 시뮬레이션에 필요한 파일 시스템을 기술하고 있는 모듈이다. 실제 네트워크에 존재하는 호스트의 파일 시스템과 유사한 방식으로 파일 시스템을 기술하고 있다.
- Extended Service : SFSNet이 제공하는 기본적인 라우터, Http 클라이언트, Http 서버와 같은 서비스 외에 FTP, Telnet, DNS와 같은 실제 네트워크에서 침입에 많이 사용되는 서비스들을 구현한 모듈이다.

4. 인터렉티브 시뮬레이션 프레임웍

인터렉티브 시뮬레이션 프레임웍은 네트워크 시뮬레이션의 진행 중, 방화벽 룰셋이나 호스트의 환경 설정 변경과 같은 조작을 지원한다. 네트워크 시뮬레이션에서는 방화벽 룰셋이나 호스트의 환경 설정 변경을 위해서 시뮬레이션을 잠시 중단 시킨다. 변경할 방화벽 룰셋이나 호스트의 환경 설정 변경을 한 후 다시 시뮬레이션을 재개 시키면, 네트워크 시뮬레이션을 중단 시킨 시점부터 변경된 SFS 시스템을 적용시킨 시점으로 시나리오는 재개된다.

시뮬레이션 중단 과정과 시뮬레이션 재개 시점을 설정하는 방법은 아래와 같다.

[그림 3]은 GUI를 통해 보는 시뮬레이션 시나리오 트리이다.



[그림 3 시뮬레이션 시나리오 트리]

또한 [표 1]은 시나리오 데이터베이스에 포함된 시나리오의 진행을 관리하는 테이블이다.

[테이블설명]	시나리오의 각 단계에서 실행될Actor의 정보를 가진다.			
필드명	Key	Null	Type	설명
step	PK		VARCHAR(50)	Actor의 시나리오 내의 실행단계
scenario_step	FK		VARCHAR(200)	시나리오의 이름
description			VARCHAR(200)	각 공격단계의 설명
actor_name	FK		VARCHAR(200)	실행할 Actor의 이름
arg_list			TEXT	Actor의 입력인자 값들의 리스트
sub_step		Null	TEXT	현재의 Step이 하위노드로 가지는 스텝의 리스트(Ex: 1.1, 1.2)
start_time		Null	INT(10)	현재의 Step에 실행권한이 넘겨온 시간부터, 실제 작업을 수행하기까지의 시간간격
break_point			INT(1)	시뮬레이션 중단을 체크하는 변수,

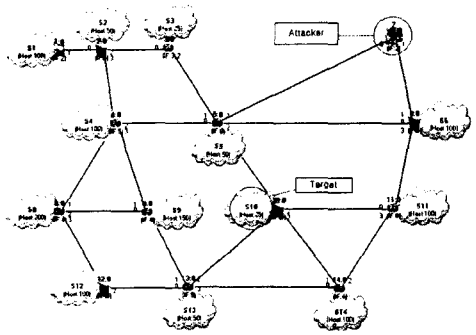
[표 1 시나리오 데이터베이스 테이블]

시나리오 트리는 [그림 3]과 같이 마이크로 소프트 윈도우 폴더 트리와 같은 형식을 가진다. 이는 시나리오의 병렬 실행이나 시나리오의 순차 실행에 있어서 시나리오의 선후관계를 잘 파악할 수 있다. 만약 사용자가 1.3.1.4의 시나리오, 즉 사파이어 웜을 퍼트리는 시점에서 중지를 요청하게 된다면, 현재 진행 중인 [표 1]의 step 에 해당하는 시나리오에서 진행이 중지되게 된다. 진행의 중지는 [표 1]의 break_point에 3을 표시하게 되며, [표 1]의 step에 해당하는 시나리오에서 시뮬레이션이 중지되었음을 알린다.

이때 시뮬레이션 엔진은 시나리오 데이터베이스에 있는 시나리오 데이터베이스의 break_point가 3인 것을 확인 한 다음, 해당 숫자를 2로 변경해 줌으로써, 시뮬레이션 엔진이 시뮬레이션을 중단 했다는 표시를 시나리오 데이터베이스에 남긴다. 이후 사용자가 환경 설정을 변경 시키고, 시뮬레이션 엔진은 네트워크 토폴로지와 SFS 시나리오를 재설정하면서, 시나리오 데이터베이스의 break_point를 살피게 된다. 이때 break_point가 2로 설정되어 있는 시나리오 테이블을 발견하게 된다면, 시뮬레이션은 해당 시나리오 스텝에서부터 시뮬레이션을 재개하게 된다.

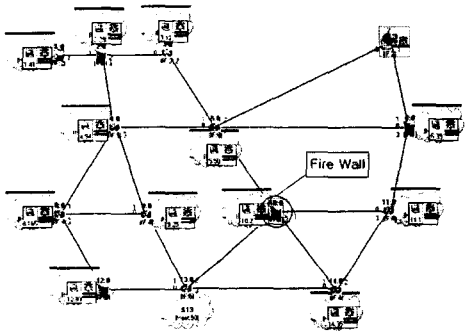
5. 시뮬레이션

본 장에서는 구현된 Interactive Simulation Framework 의 정상적인 구동과 네트워크 침입 및 방어 시뮬레이션을 테스트 하기위해 [그림 4]와 같은 네트워크 환경을 구성하고 결과를 테스트해 보았다. [그림 4]는 1750개의 호스트(구름 형태의 그림이 호스트 서브넷으로 50~100개의 호스트를 포함한다.)와 22개의 라우터로 구성된 네트워크 환경을 약 30000초 동안 시뮬레이션 하였다. 침입자는 오른쪽 상단에 표시된 호스트 그룹에 속해 있으며, 최종적으로 모든 호스트에 설치된 웹 서버에 웜 침입을 시도하고자 한다. 또한 Interactive Simulation Framework의 테스트를 위해 시뮬레이션 도중 가운데 위치한 target 서브넷의 Firewall 룰셋 변경을 통한 웜 침입 현상을 비교 분석해 본다.



[그림4 시뮬레이션 네트워크 환경]

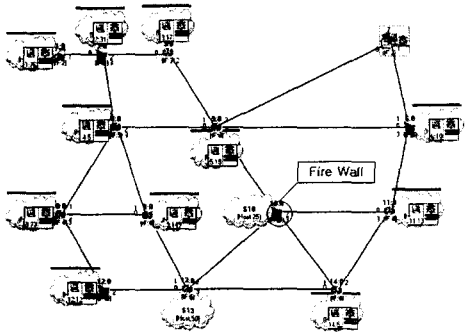
[그림 3]의 시나리오는 각각의 스텝에 해당하는 노드들이 침입 모델을 표현하고 있으며, 이러한 노드들은 모두 침입 모델로 구현되어, 침입에 해당하는 행동을 수행하게 된다. 웜은 Sapphire 웜의 행동을 사용하였으며, DNS서버에 부하를 주는 Query 패킷을 전송한다. 최종적으로 DNS서비스를 중단시키는 역할을 한다.



[그림 5 Firewall 룰셋 설정시 target 서브넷의 웜 침입 불가]

위의 시나리오에 따라 시뮬레이션을 한 결과 [그림 5,6]와 같은 결과를 보여준다. [그림 5,6]에서 노란색 벌레 모양의 아이콘은 사파이어웜이 해당 서브 네트워크를 감염 시켰다는 것을 의미한다. [그림 5]에서는 Firewall에 1434 포트로 들어오는 UDP 패킷을 거부하는 룰셋을 하였을 경우, Sapphire Worm 침입으로 인한 타겟의 네트워크 감염이 없는 것을 보여주고 있다. [그림 5]의 진행은 첫 번째로 사파이어 웜을 퍼뜨리는 1.3.1.4의 시나리오를 진행 시킨 후 시뮬레이션으로 약 200초가 지난 상황을 보여주고 있다.

이후 [그림 6]은 사파이어 웜이 퍼져나가는 도중 [그림 3]의 시나리오 트리 중 두 번째 사파이어 웜을 퍼뜨리는 1.3.2.4의 시나리오에서 Firewall에 1434 포트로 들어오는 UDP 패킷을 거부하는 룰셋을 제거하였을 경우, 웜 침입으로 인해 서브넷의 감염 여부를 보여주고 있다.



[그림 6 Firewall 룰셋 설정 부재시 target 서브넷의 웜 침입]

우리는 본 실험에서 Firewall의 룰셋 변경을 통한 Interactive Simulation Framework의 정상적인 구동을 살펴볼 수 있다.

6. 결론 및 향후계획

본 논문에서는 네트워크 침입 및 방어 시뮬레이션을 위한 프레임웍 구현과, Interactive Simulation을 위한 프레임웍 구현, 다양한 네트워크 침입 및 방어에 관련한 모델들을 구성할 수 있는 기반을 구현해 보았다. 또한, SSFNet을 기반으로 하여, 대규모 네트워크 환경에서 네트워크 침입 및 방어 시나리오를 통해 네트워크의 부하에 대한 실험을 해봄으로써, 침입 행동으로 인한 네트워크 특성의 변화를 살펴 볼 수 있었다.

향후 본 시뮬레이션 프레임웍을 기반으로 다른 종류의 바이러스나 기타 방어 모델들을 구현하고, 10만개 이상의 노드를 포함하는 네트워크 토폴로지를 사용한 시뮬레이션을 수행하기 위해 퍼포먼스를 향상 시키는 연구가 필요하다. 이러한 퍼포먼스의 향상을 위해서 클러스터링과 같은 분산 환경을 지원하는 시뮬레이션이나 멀티 프로세스를 사용한 시뮬레이션 연구를 통해 보다 대규모의 네트워크 환경에서 네트워크 침입과 방어에 관한 연구를 수행 할 수 있을 것이다.

7. 참조 문헌

[1] Shabana Razak, Mian Zhou, Sheau-Dong Lang, "Network Intrusion Simulation Using OPNET", OPNETWORK Proceedings 2002.

[2] T.Tidwell, R. Larson, K. Fitch and J. Hale, "Modeling Internet Attacks", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001.

[3] "SSF Simulator implementation", http://www.ssfnet.org/ssfImplementations.html.

[4] T.Tidwell, R. Larson, K. Fitch and J. Hale, "Modeling Internet Attacks", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001.

[5] Jan Steffan, Markus Schumacher "Collaborative Attack Modeling", 17th ACM Symposium on Applied Computing (SAC 2002), Special Track on Computer Security, Madrid, Spain, March 10-14, 2002.

[6] Donald Welch, Greg Conti, "A Framework for an Information Warfare Simulation", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001