침입 탐지 시스템과 침입 차단 시스템의 연동을 통한 네트워크 보안 시뮬레이션

서희석*, 조대호*, 이용원*
Seo, Hee Suk , Cho, Tae Ho and Lee, Yong Won
*성균관대학교 전기 전자 및 컴퓨터 공학부
(histone@peter.skku.ac.kr , taecho@ece.skku.ac.kr , ywlee@peter.skku.ac.kr)

Abstract

인터넷이 생활의 중요한 요소로 자리잡기 시작하면서 네트워크의 침해 사고가 급증하고 있는 현실이다. 이러한 침해 사고를 예방하기 위해 침입 탐지 시스템(IDS)과 방화벽(Firewall)이 많이 사용되고 있다. 방화벽과 침입 탐지 시스템은 연동은 서로의 단점을 보완하여 더 강력하게 네트워크를 보호할 수 있다. 방화벽과 침입 탐지 시스템을 위한 시뮬레이션 모델은 DEVS (Discrete EVent system Specification) 방법론을 사용하여 구성하였다. 본 논문에서는 실제 침입 데이터를 발생시켜 실제 침입에 가까운 상황 가운데 침입 행위를 판별하도록 구성하였다. 이렇게 구성된 시뮬레이션 모델을 사용하여 침입 탐지 시스템의 핵심 요소인 침입 판별이 효과적으로 수행되는지를 시뮬레이션 할 수 있다. 현재의 침입은 광범위해지고, 복잡하게 되어 한 침입 탐지 시스템이 독립적으로 네트워크의 침입을 판단하기 어렵게 되었다. 이를 위해 네트워크 내에 여러 침입 탐지 시스템 에이전트를 배치하였고, 에이전트들이 서로 정보를 공유함으로써 공격에 효과적으로 대응할 수 있도록 하였다. 침입 탐지 시스템이 서로 협력하여 침입을 탐지하고, 이런 정보를 침입 차단 시스템에게 넘겨주게 된다. 이와 같은 구성을 통해서 공격자로부터 발생된 패킷이 네트워크 내로 들어오는 것을 원천적으로 막을 수 있도록 하였다.

Keyword

Intrusion Detection System(IDS), Firewall, Collaboration, Denial of Service(DoS), Distributed Attack

1. 서론

인터넷 전자 상거래가 급증하고 네트워크 이용이 크게 증가하면서 외부 침입 및 내부자에 의한 중요 기밀 문서의 외부 유출이 중요한 사회적 문제로 부각되고 있다[1][6][11]. 바이러스와 해킹 사고의 증가 폭이 기하급수적으로 증대되고 있는 현 상황에서 시스템의 보안은 매우 중요한 요소로 부각되고 있다.

본 논문에서는 시뮬레이션 모델을 통해 네트워크의 보안 성능을 평가할 수 있는 시뮬레이션 환경을 소개할 것이다. 네트워크의 속도가 급속하게 증가하고 발전하는 상황에서 많은 양의 데이터를 처리해야 하는 보안 시스템을 직접 사용해 성능을 평가하는 것은 효율적이지 못하다. 이를 해결하기 위해 DEVS (Discrete EVent system Specification) 방법론을 사용하여 시뮬레이션 모델을 구축하고, 이를 기반으로 하여 네트워크 보안 모델을 구축하였다. 시뮬레이션 모델은 추상화 과정을 거쳐 완성된다. 즉 모델에 사용되는 입력 및 출력을 추상화하여 사용하는 것이 일반적이다. 그러나 본 시스템을 실제 환경과 가깝도록 구성하기 위해서 시뮬레이

선 모델에서 사용하는 패킷을 네트워크에서 수집한 실 패킷(real packet)을 사용하였다.

2. 배경 이론

2.1 DEVS 방법론

Zeigler에 의해 정립된 DEVS 방법론은 연속적인 시간상에서 발생되는 이산 사건을 처리하는 시스템을 시뮬레이션 하기 위해 이론적으로 정립된 모델링 방법론이다[5][9][12]. 이는 모델의 구조와 행동을 시뮬레이션 수행으로부터 추상화시키기 위해 모델을 집합 이론적 방법으로 이용한 것으로, 시스템을 계층적(hierarchical)이고 모듈화(modular)된 형식으로 기술한다.

DEVS에서는 기본(Basic) 모델과 결합(Coupled) 모델을 정의한다. 기본 모델은 시스템의 동적인 특성을 표현하기 위한 모델이고, 결합 모델은 시스템의 구성 요소간의 상호 작용을 표현하기 위한 모델이다. 이 모델들은 다음의 항들로 명세 할 수 있다.

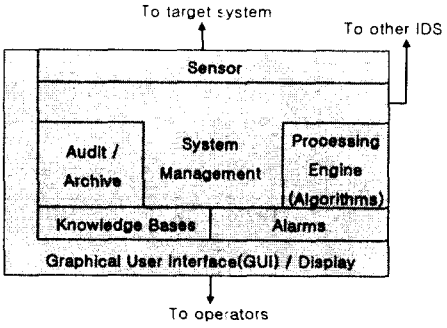
$M = < X, S, Y, \delta_{int}, \delta_{ext}, \lambda, t_a >$
- X : 입력 사건의 집합
- S : 상태들의 집합
- Y : 출력 사건의 집합
- δ_{int} : 내부 상태 변이 함수
- δ_{ext} : 외부 상태 변이 함수
- λ : 출력 함수
- t_a : 시간 갱신 함수

$DN = < D, \{M_i\}, \{I_i\}, \{Z_{ij}\}, select >$
- D : 구성 요소 이름의 집합
- M_i : 구성 모델
- I_i : 모델 i와 연관된 모델의 집합
- Z_{ij} : 모델 i와 j모델간의 연결 함수
- $select$: $tie-breaking\ selection$ 함수

2.2 침입 탐지 시스템

침입 탐지 시스템(IDS : Intrusion Detection System)[1][2][3][6]은 외부의 침입에 대해 능동적으로 대처하는 시스템으로 방화벽과 함께 활용되는 네트워크 보안 솔루션이다. 침입 탐지 시스템은 방화벽의 앞 또는 뒤에서 침입 사실을 탐지해 침입자의 공격에 대응하기 위한 솔루션이다.

<그림 1>은 침입 탐지 시스템의 일반적인 구성요소를 나타낸 그림이다[2].



<그림 1> 침입 탐지 시스템의 구성

침입 탐지 시스템의 분류는 크게 데이터 소스를 기반으로 분류하는 방법과 침입 모델을 기반으로 분류하는 방법이 있다. <표 1>은 침입 탐지 시스템의 분류를 나타낸 것이다.

<표 5> 침입 탐지 시스템의 분류

구분 / 분류 방법	분류된 종류
데이터 소스를 기반으로 분류	· 단일 호스트 기반의 IDS · 다중 호스트 기반의 IDS · 네트워크 기반의 IDS
침입 모델 기반으로 분류	· 비정상적인 침입 탐지 기법 (Anomaly Detection Technique) · 오용 침입 탐지 기법 (Misuse Detection Technique)

2.3 침입 차단 시스템

인터넷 방화벽[13][14]은 외부 네트워크와 내부 네트워크 사이 혹은 네트워크 간에 설치되어 관리자의 정책에 따라 트래픽의 흐름을 막거나 허용하는데 사용된다. 즉 방화벽은 외부에서 내부로 들어오는 트래픽에 대해서 제약을 가할 수 있을 뿐만 아니라 내부 사용자가 외부 네트워크로 접속하여 기밀 정보를 외부로 보내는 것을 막을 수 있다. 방화벽 시스템은 그 동적 계층에 따라 몇 가지로 나눌 수 있다. 대표적 방식으로는 네트워크 계층에서 동작하는 방화벽, 전송 계층에서 동작하는 방화벽, 그리고 응용 프로그램 계층에서 동작하는 방화벽

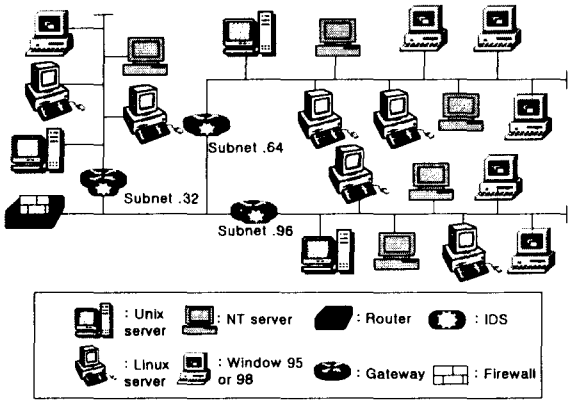
이다. <표 2>는 종류별 방화벽의 특징을 나타낸 것이다.

<표 6> 종류별 방화벽의 특징

방화벽의 종류	특 징
네트워크 계층 방화벽	· 패킷의 정보를 기반으로 정책 적용 · 세부적 정책 설정 불가능
전송 계층 방화벽	· 전송 계층에서 얻어지는 정보를 기반으로 정책 적용 · 인증 기능 제공 가능
응용 계층 방화벽	· 다양한 정책 설정 가능 · 각 응용 프로토콜에 대해 선별적 정책 적용 가능
하이브리드 방화벽	· 보안상 가장 효율적 · 시스템 구현의 어려움

3. 네트워크 보안 모델

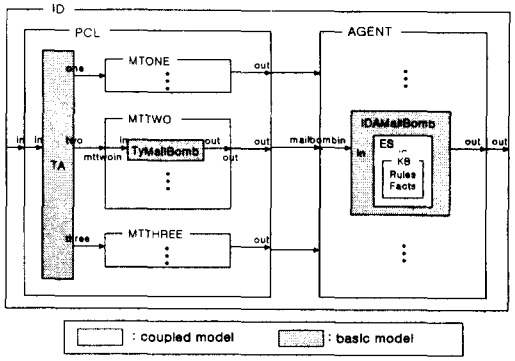
3.1 대상 네트워크의 구성



<그림 2> 네트워크 구성도

<그림 2>는 3개의 서브넷을 갖는 대상 네트워크의 구성도이다. IDS, Firewall, Gateway 모델이 구현되어 있다.

3.2 침입 탐지 모델



<그림 3> ID 모델 구성도

<그림 3>은 Gateway에 탑재된 침입 탐지 모델의 구성도이다. 침입 탐지 모델이 새로운 공격을 탐지하도록 하기 위해서는 네트워크 시스템 관리자가 공격 형태를 분류하고, 기본 모델을 구성하여 PCL 모델과 AGENT 모델에 첨가하면 된다.

3.2.1 PCL(Packet Classify Library) 모델

PCL 모델은 AGENT 모델에서 사용될 패킷을 분류하고, 필터링하는 역할을 수행하는 모델이다. mailbomb 공격을 예로 들어 본다. mailbomb 공격은 메일 서버에 많은 양의 메일을 보내 메일 서버의 작동을 느리게 하거나, 전복시키는 서비스 거부 공격(Denial of Service)의 일종이다. 한 사용자가 다른 사용자에게 전자 메일(e-mail)을 보내기 위해서는 TCP 프로토콜을 사용하여야 하고, 포트(port)는 25번을 사용해야 한다. 그러므로 PCL 모델의 TyMailBomb 모델은 TCP 프로토콜을 사용하고, 포트 25번을 사용하는 패킷만을 IDAMailBomb 모델에게 전달하게 된다.

3.2.2 AGENT 모델

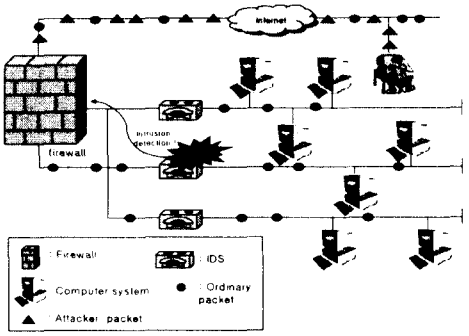
AGENT 모델은 침입 탐지 모델의 핵심 모델로 침입을 판별하는 규칙 기반 전문가 시스템(rule-based Expert System)을 내장하고 있다. AGENT 모델은 PCL 모델로부터 전달받은 패킷을 전문가 시스템에서 사용하는 사실(fact)의 형태로 전환하고, 이 사실을 전문가 시스템에게 넘기게 된다. 전문가 시스템은 자신이 갖고 있는 규칙(rule)에 이 사실을 적용하여 침입을 판별하게 된다.

여러 AGENT 모델은 블랙 보드 구조(Blackboard Architecture)[7]를 통해서 서로 정보

를 공유하는데, 블랙 보드의 단계는 Josheph Barrus & Neil C. Rowe가 제안한 Danger Values에 의해 구분되었다[3]. 각 단계는 Minimal, Cautionary, Noticeable, Serious, Catastrophic이다. 본 시스템에서는 공격의 수준이 Serious 단계를 지나게 되면 더 이상의 패킷 유입을 막아 네트워크를 보호하도록 구성하였다.

3.3 침입 차단 모델

DEVS 모델의 기본(basic) 모델로 구성되어 있는 침입 차단 모델은 <표 2> 분류의 네트워크 계층의 방화벽을 모델링한 것이다. 침입 차단 모델은 IP(Internet Protocol) 주소, 프로토콜 그리고 포트 번호에 의해 정책을 수립하도록 구성되어 있다. 본 시스템의 경우, 침입 탐지 모델이 침입을 탐지했을 경우는 공격 출발지 IP 주소를 침입 차단 모델에게 알리게 된다. 침입 차단 모델은 이 정보를 사용하여 공격이 수행되고 있는 호스트로부터의 패킷 유입을 막는다.



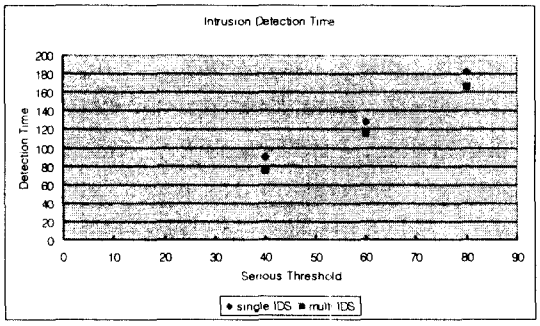
<그림 4> 침입 탐지 및 대응

<그림 4>는 침입 탐지 모델이 침입을 탐지한 경우, 침입 차단 모델과의 연동을 통해서 공격자의 패킷이 네트워크로 유입되는 것을 차단하는 상황을 묘사한 것이다.

4. 시뮬레이션

시뮬레이션 환경은 DEVS-ObjC를 사용하였고, 시뮬레이션에서 사용되는 성능 지표는 침입 탐지 시간(Intrusion Detection Time)을 사용하였다. 하나의 침입 탐지 모델이 침입을 탐지하는 경우와 여러 개의 침입 탐지 모델이 침입을 탐지하는 경우에 대해 시뮬레이션을 수행하였다. 시뮬레이션에 사용될 입력은 mailbomb 공격을 수행하는 Kaboom version 3.0을 사용하여 공격 패킷을 생성하였다.

<그림 5>에서 알 수 있듯이 여러 침입 탐지 모델이 침입을 탐지하는 경우가 하나의 침입 탐지 모델이 침입을 탐지하는 경우보다 빠르게 침입을 탐지하는 것을 알 수 있다. 침입을 빠르게 탐지 할 수 있다면 그만큼 빠르게 대응할 수 있으므로 네트워크 자원을 안전하게 유지하는데 매우 중요하다.



<그림 5> single IDS와 multi IDS의 침입 탐지 시간 비교

5. 결론 및 향후 과제

크래커에 의한 네트워크의 침입 사고가 증가하고, 침입 또한 교묘해져서 하나의 침입 탐지 시스템이 침입을 탐지하는 것보다 여러 개의 침입 탐지 시스템이 침입을 탐지하는 것이 효과적으로 네트워크를 보호하는 방법이다. 더 나아가 침입 탐지 시스템과 침입 차단 시스템의 연동으로 네트워크를 보호한다면 강력하게 시스템을 보호할 수 있다. 침입 탐지 시스템과 침입 차단 시스템이 서로 협력하므로 공격자의 패킷이 네트워크로 유입되는 것을 막을 수 있는 장점을 갖게 된다.

향후 과제로는 일반적인 시뮬레이션 환경을 구축하기 위해서 공격 툴에서 생성되는 패킷과 같은 실제 패킷을 생성할 수 있는 시뮬레이션 입력 생성(Generator) 모델의 구축이 필요할 것으로 여겨진다.

참고문헌

[1] E. Amoroso, "Intrusion Detection - An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response", Intrusion.Net Books, 1999.

[2] R. Bace, "Intrusion Detection", Macmillan Technical Publishing, 2000.

[3] J. Barrus, N. C. Rowe, "A Distributed Autonomous-Agent Network-Intrusion Detection and Response System", Proceedings of Command and Control Research and Technology Symposium, Monterey CA, June 1998, pp. 577-586.

[4] S Mclure, J. Scambray, G. Kurtz, "Hacking Exposed: Network Security Secrets and Solutions", McGraw-Hill, 1999.

[5] B. P. Zeigler, "Object-Oriented Simulation with Hierarchical, Modular Models", San Diego, CA, USA:Academic Press, 1990.

[6] S. Northcutt, "Network Intrusion Detection - An Analyst's Handbook", New Riders Publishing, 1999.

[7] G. Van Zeir, J. P. Kruth, J. Detand, "A Conceptual Framework for Interactive and Blackboard Based CAPP", International Journal of Production Research, Vol. 36(6), 1998, pp. 1453-1473.

[8] U. Lindqvist, E. Jonsson, "How to Systematically Classify Intrusions", Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, 1997.

[9] T.H. Cho, Bernard P. Zeigler, "Simulation of Intelligent Hierarchical Flexible Manufacturing: Batch Job Routing in Operation Overlapping", IEEE trans. Syst. Man, Cybern. A, Vol. 27, Jan. 1997, pp. 116-126.

[10] P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to anomalous live disturbances", Proceedings of the 20th National Information Systems Security Conference. National Institute of Standards an Technology, 1997.

[11] 서희석, 조대호, "IDS 성능 향상을 위한 DEVS 모델링", 한국 시뮬레이션 학회 2000년 추계 학술 대회 논문집, 2000, pp 125-130.

[12] Bernard P. Zeigler, "Theory of Modelling and Simulation", John Wiely, 1976, reissued by Krieger, Malabar , 1985.

[13] D. Brent Chapman and Elizabeth D. Zwicky, 채규혁역, "인터넷 방화벽 구축하기", 한빛미디어, 1998.

[14] Duan Haixin, Wu Jianping, Li Xing, "Policy based access control framework for large networks", Proceedings. IEEE International Conference on ICON 2000, Sept. 2000.

[16] P. Neumann and D. Parker, "A Summary of computer misuse techniques", In Proceedings of the 12th National Computer Security Conference, October 1989, pp. 396-407.