보안 시뮬레이션을 위한 네트워크 모델 설계 및 구현

신동훈, 김형종*

*한국정보보호진흥원

Design and Implementation of Network Model for Security Simulation

DongHoon Shin, HyungJong Kim

*Korea Information Security Agency

요 약

취약성 진단을 위한 시뮬레이션 시스템의 주요 구성 요소인 네트워크 모델의 설계 및 구현을 소개한다. 특히, 네트워크에 존재하는 취약점을 진단, 분석하기 위한 모델링 방법론을 제시하고, 구체적인 모델의 설계와 구현을 수행하였다. 네트워크 모델은 네트워크 구성요소인 허브, 라우터 및 네트워크 호스트들을 추상화한 모델들의 결합(Coupling) 형태로 구성되며, 각 구성 요소들은 각자의 취약성을 가지고 있다. 본 연구에서는 이러한 각 구성요소의 취약성의 집합으로 네트워크를 표현하고, 취약성을 기반으로 한 네트워크 모델의 구조적인 특성과 동적인 특성을 제시한다. 취약성 진단을 위해 제시된 모델링 방법을 통해 구현된 네트워크 모델은 시뮬레이션 실행을 통해 분석되어 그 유효성을 검증하였다.

1. 개요

인터넷의 급속한 발전과 더불어 우리는 많은 생활의 편의를 갖게 되었다. 하지만, 인터넷과 네트워크의 편의성과는 반대로, 이를 이용한 역기능도 증가하여 많은 혼란을 초래하게 되었다. 인터넷의 역기능 현상은 국가 주요 정보통신 기반에 대한 사이버 공격의 증가에서도 쉽게 알 수 있다[1][2]. 이러한 배경에서, 급격히 증가하는 위협, 침해 공격으로부터 인터넷과 네트워크 자원을 보호하기 위한 연구의 일환으로써, 본 논문에서는 보안 시뮬레이션 방법론을 제시하고, 네트워크 상에 존재하는 취약점들을 분석하기 위해 네트워크 모델을 구성하고, 실험을 통해서 네트워크 상에 존재하는 취약점들을 진단하여 보다 견고하고 안전한 네트워크를 구성하도록 제공한다.

2. 시뮬레이션 방법론

본 논문에서 제시하는 보안 시뮬레이션을 위해서 이산사건 모델링 방법인 DEVS (Discrete Event System Specification) 형식론[3]을 적용한다.

DEVS는 계층적이고 모듈화된 이산 사건모델을 위해 정의된 이론이다. 일반적으로 시스템은 시간의 흐름에 따라 입력, 상태, 출력, 상태 전이 함수들을 갖는다. DEVS 형식론은 시스템이 일반적으로 갖는 특성들을 정의하여 시스템을 모델링할 수 있는 기반을 제공하고 있다. DEVS 형식론에서는 두 가지 종류의 모델을 정의하였다. 하나는 기본(Basic) 모델이고, 다른 하나는 커플된(Coupled) 모델이다. 기본 모델의 구성은 다음과 같다.

$$M = < X, S, Y, \delta int , \delta ext , \lambda, ta >$$

이때, X는 입력 사건의 집합을, S는 순차적 상태의 집합을, Y는 출력 사건의 집합을, δint는 $S \rightarrow S$의 내부 전이 함수를, δext는 $Q \times X \rightarrow S$의 외부 전이 함수를, λ는 $S \rightarrow Y$의 출력 함수를, ta는 $S \rightarrow R+0 \rightarrow \infty$의 시간 진행 함수를 나타내고, 이때 집합 Q 는 $\{(s,e) \mid s \in S, 0 \le e \le ta(s)\}$이고, e 는 최근 상태전이 이후로 흐른시간을 나타낸다.

커플된 모델의 구성은 다음과 같다.

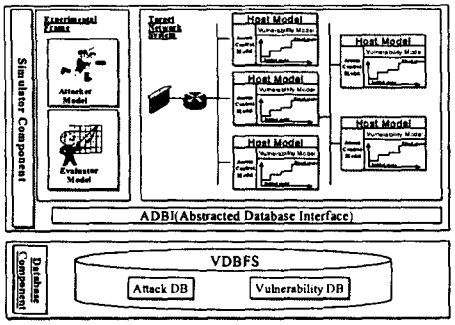
$$DN = < D, \{Mi\}, \{Ii\}, \{Zi,j\}, select>$$

이때, D 는 커플된 모델의 구성요소인 모델 i에 대한 이름의 집합을, Mi는 구성요소가 되는 기본 모델을, Ii는 모델 i의 영향을 받는 모델들의 집합을, Zi,j는 Ii의 원소 각 j에 대해서 i에서 j로의 출력 번역 함수를, Select : 타이 브레이킹 함수를 나타낸다.

3. 네트워크 모델 구성

3.1 보안 시뮬레이션 시스템

보안 시뮬레이션 시스템의 구성은 아래 (그림 1)과 같다.

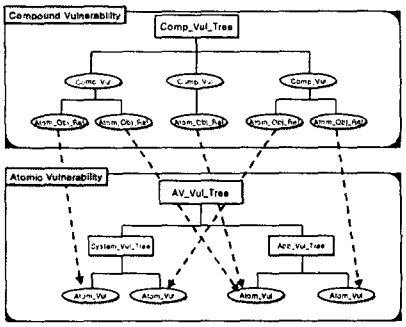


(그림 1) 보안 시뮬레이션 시스템

전체 보안 시뮬레이션 시스템은 크게 시뮬레이터 부분과 취약성 데이터 베이스 부분으로 구성된다. 우선, 취약성 데이터 베이스 부분은 보안 시뮬레이션 시스템의 지식 베이스로 사용하기 위해서 구축되었고, 네트워크상에서 존재하는 다양한 형태의 취약성 정보들로 이루어진 취약성 데이터 베이스 (Vulnerability DB)와 공격자가 대상 네트워크를 공격할 때 이용하는 공격 데이터 베이스(Attack DB)로 구성되어 있다. 보안 시뮬레이션 시스템의 또 다른 구성요소인, 시뮬레이터 부분은 실험 평가 모델 부분과 대상 네트워크 모델 부분으로 구성된다. 실험 평가 모델 부분은 공격 데이터 베이스를 지식 베이스로 이용하여 공격 패킷을 생성하고, 이 공격 패킷을 사용하여 대상 네트워크에 유해한 공격을 하는 공격자 모델과 공격자 모델의 공격이 얼마나 성공하고 있는지, 대상 네트워크의 상태가 공격자의 공격 패킷으로 인해 어떤 영향을 받고 있는지를 분석하는 평가 모델로 구성된다. 대상 네트워크 모델 부분은 호스트 모델, 보안 시스템 모델, 네트워크 디바이스 모델들로 구성된다. 호스트 모델은 네트워크 호스트가 갖는 취약성과 네트워크 호스트 기반의 방어 기법을 표현한다. 보안 시스템 모델은 네트워크 상에 존재하는 공격자의 공격 경로를 차단하여 대상 네트워크를 보호하기 위한 모델로, 접근 제어 시스템의 특성을 추상화하여 구성한다. 네트워크 디바이스 모델은 네트워크 상에서의 호스트 모델과 보안 시스템 모델들의 연결 정보를 표현하는 모델로 라우터 모델과 허브 모델로 구성된다.

3.2 네트워크 취약점 표현

보안 시뮬레이션 방법을 적용하기 위해서 네트워크에 존재하는 취약점들을 복합 취약점 (CV : Compound Vulnerability) 과 단위 취약점(AV : Atomic Vulnerability) 라는 개념을 사용하여 표현하였다. 복합 취약점은 흔히 우리가 "취약점"이라고 불리는 개념의 취약점을 말한다. 단위 취약점은 복합 취약점을 좀더 세밀히 분석하여 정의한 것이다. 하나의 취약점을 다수의 요소들을 말한다. 아래 (그림 2)는 복합 취약점과 단위 취약점과의 관계를 나타내고 있다.

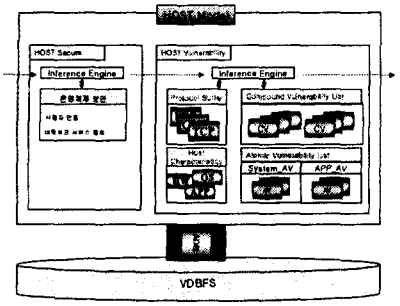


(그림 2) 복합 취약점과 단위 취약점

네트워크 모델은 네트워크에 존재하는 취약점을 분석하여 취약점 트리로 구성하여 관리한다. 복합 취약점은 다수의 단위 취약점들로 구성되고 단위 취약점은 다수의 복합 취약점 구성 요소로 사용된다. 또한 단위 취약점은 특성에 따라서 시스템 구성으로 발생된 것인지, 서비스에 의해서 발생된 것인지에 따라 시스템 취약점 트리 혹은 서비스 어플리케이션 취약점 트리에 속하게 된다. 이러한 취약점 트리 구조를 사용하여 보안 시뮬레이션에서는 대상 네트워크의 취약점을 진단하게 된다.

3.3 호스트 모델

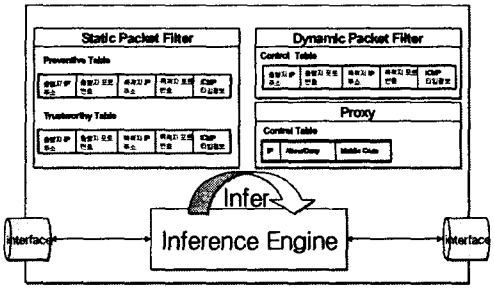
호스트 모델의 구성은 아래 (그림 3)와 같다. 호스트 모델은 사용자 인증과 네트워크 접근 통제를 수행하는 호스트 보안 모델, 호스트 하드웨어/소프트웨어적인 구성과 제공하는 서비스에 관한 특성을 표현하는 부분, 호스트 특성에 따라 존재하는 취약성들에 대한 정보를 표현하는 복합 취약점과 단위 취약점들의 리스트와 공격자의 공격 패킷에 따른 호스트 모델의 반응을 결정하는 추론 엔진으로 구성된다. 호스트 모델의 특성은 네트워크 시스템에서 사용하는 운영체제 정보, 하드웨어 플랫폼 정보, 인터넷의 주소를 표현하고 네트워크 주소에 관한 정보를 표현하고 있는 IP 주소 정보, 그리고 호스트 모델에서 운영하는 응용 프로그램에 따라 제공하는 서비스 종류와 각 서비스에서 사용하는 시스템 자원 정보의 조합으로 구성한다. 호스트 자원 모델은 호스트 모델의 네트워크 자원을 추상한 모델로 서비스 거부 공격에 따른 자원 점유율을 분석하기 위한 모델이다. 호스트 보안 모델은 사용자 인증과 네트워크 접근 제어를 통하여 네트워크 호스트 시스템에서 행하는 접근제어 메커니즘을 분석하기 위한 모델이다. 또한 호스트 모델은 자신이 특성 정보에 따라 발생하는 취약점 정보를 추상화하기 위해 앞에서 설명한 취약점 트리를 구성한다.



(그림 3) 호스트 모델 구조

3.4 보안 시스템 모델

네트워크의 자원을 보호하기 위한 보안 시스템 모델의 구조는 아래 (그림 4)와 같다.



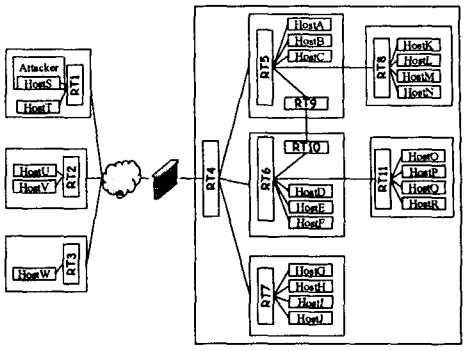
(그림 4) 보안 시스템 모델의 구조

보안 시스템 모델은 정적 패킷 필터와 동적 패킷 필터, 그리고 프락시 모델로 구성된다. 정적 패킷 필터는 패킷의 헤더 정보의 주소 값을 사용하여 IP Filtering, Port Filtering을 수행한다. 동적 패킷 필터링의 SYN Defender Relay, SYN Defender Gateway 기능을 수행한다. 각 보안 시스템은 그림에서 보는 바와 같이 자신의 규칙 테이블을 기반으로 추론 과정을 통해 접근 제한 여부를 결정하게 된다.

4. 네트워크 구성 및 실험 결과

4.1 네트워크 구성

본 논문에서 제시한 보안 시뮬레이션 시스템의 취약성 분석 대상이 되는 네트워크 구조는 아래 (그림 5)와 같다.

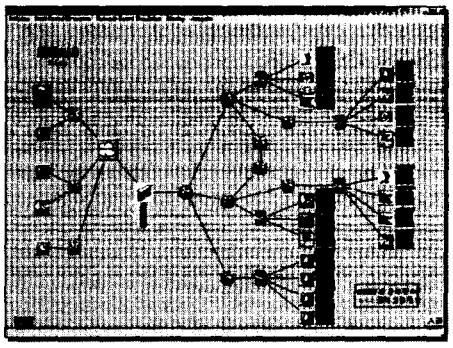


(그림 5) 시뮬레이션 대상 네트워크 구성

(그림 5)는 이제까지 설명한 모델들을 이용하여 시뮬레이션 대상이 되는 네트워크를 구성한 것이다. 위의 그림을 통해서 시뮬레이션 대상 네트워크를 구성하는 모델들의 연결 관계를 알 수 있다. (그림 5)는 시뮬레이션 대상 네트워크를 구성하는 다수의 서브넷과 보안 시스템 모델인 Firewall, 그리고 서브넷을 구성하는 호스트 모델들의 연결 관계, 호스트 모델을 사용하는 공격자 모델의 연결 관계 등을 나타낸다.

4.2 결과 및 분석

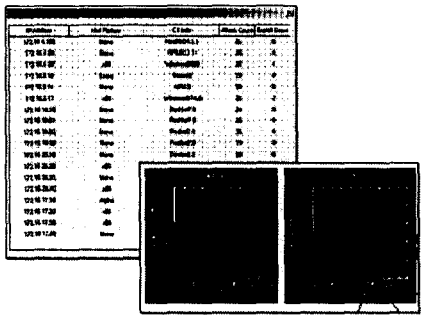
아래 (그림 6)은 시뮬레이션을 위해 구성된 모델들을 이용하여 대상 네트워크를 보안 시뮬레이션 환경으로 구성한 모습을 나타낸다. (그림 6)의 왼쪽 위 부분에 있는 노드에서 공격자가 공격을 하고 있고, 공격대상이 되는 네트워크에서의 공격 성공률과 공격에 따른 권한 상실, 그리고 서비스 거부 공격에 따른 자원 점유율 등을 나타내고 있고 화면 중앙에 있는 Firewall에서는 보안 관리자가 설정한 보안 정책에 따라 공격자의 공격 패킷을 차단하고 있는 모습을 보이고 있다.



(그림 6) 보안 시뮬레이션 실행 화면

아래 (그림 7)의 그래프는 Firewall과 공격 대상 호스트의 네트워크 접근 통제 모델의 결과를 나타낸다. 그래프의 값은 공격 패킷의 허용율을 나타내고 있다. 그림의 테이블은 공격자 모델에

의해서 공격당한 호스트들의 취약성을 분석하여 각 취약성에 대한 해결책을 제시하는 화면이다.



(그림 7) 실험 결과

5. 결론 및 향후 연구 과제

인터넷에 대한 침해사고 증가에 따라 네트워크 보안에 대한 연구가 활발히 진행 중이다. 이러한 연구의 일환으로 본 연구에서는 시뮬레이션 방법론을 이용하여 네트워크에 내재된 취약점을 효율적으로 진단하기 위해서 보안 시뮬레이션 방법을 소개하였고, 보안 시뮬레이션 시스템의 주요 구성요소인 네트워크 모델들을 설계 및 구현하고, 실험을 통해서 검증하였다. 구현된 네트워크 모델들을 이용하여, 실험 대상 네트워크를 구성하여 대상 네트워크에 존재하는 취약성을 진단하여 보았다. 또한 네트워크에 존재하는 취약점들을 표현하기 위해 단위 취약점과 복합 취약점이라는 개념을 사용하여 네트워크 모델에 존재하는 취약점들을 좀더 자세히 표현하였다.

향후 보안 시뮬레이션 시스템의 분석대상이 되는 네트워크 모델을 실제 네트워크와 연동을 통해서 구성하고, 실시간 시뮬레이션의 수행을 통해 실세계의 시스템의 정보를 참조하여 시뮬레이션을 수행하고 시뮬레이션 결과를 실세계 네트워크의 보안 정책이나 환경 설정에 반영하기 위한 연구를 보완할 예정이다.

참고문헌

[1] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network Intrusion Detection", IEEE Network, Vol. 8, No. 3, pp26-41, May/June 1994.

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

[3] B. P. Zeigler, Theory of Modeling and Simulation, John Wiley, NY, USA, 1976, reissued by Krieger, Malabar, FL, USA, 1985.

[4] HyungJong Kim, KyoungHee Ko, DongHoon Shin and HongGeun Kim, "Vulnerability Assessment Simulation for Information Infrastructure Protection", LNCS 2437 p145-161.

[5] HyungJong Kim, HongGeun Kim and Taeho Cho, "Simulation Model Design of Computer Network for Vulnerability Assessment," International Workshop on Information Security Applications, Sep. 13-14, 2001

[6] Taeho Cho, HyungJong Kim, "DEVS Simulation of Distributed Intrusion Detection System," Transactions of the Society for Computer Simulation International, vol. 18, no. 3, September, 2001