네트워크 정보보호를 위한 교육용 시뮬레이터 개발

신동훈 김형종 고경희 김동현*
*한국정보보호진흥원
e-mail:dhshin@kisa.or.kr

Educational Simulator Development for Netwrok Security

DongHoon Shin, HyungJong Kim,
KyoungHee Ko, DongHyun Kim*
*Korea Information Security Agency

요 약

사회 기반 시설의 침해 사고의 증가로 인해 정보보호에 관한 관심이 증가하고 있다. 하지만 현재까지의 정보보호를 위한 교육용 소프트웨어에 관한 연구는 미비한 편이었다. 본문에서 정보보호의 주요 요소인 취약성, 공격, 방어에 관한 개념을 쉽게 이해할 수 있고, 각 요소들의 연관관계를 분석할 수 있는 교육용 시뮬레이터를 제시한다. 제시한 교육용 시뮬레이터에 적용된 모델링 방법론에 대해서 알아보고, 교육용 시뮬레이터의 공격자 모델의 기반이 되는 자동 공격 도구에 관한 연구 내용을 살펴보고, 네트워크 취약성을 표하는 네트워크 모델의 구조에 대해 살펴본다. 마지막으로 교육용 시뮬레이터의 구조적 특성과 기능을 분석해보고, 교육용 시뮬레이터의 활용 방안을 제시한다.

1. 서론

인터넷과 네트워크를 이용하는 침해 사고와 해킹의 증가로 인해 사회 기반 구조의 피해가 급격히 증가하고 있다. 이러한 사회적 배경에서 많은 사람들이 정보보호에 관한 관심이 증가하고 있다. 하지만, 국내의 정보보호를 위한 교육용 소프트웨어에 대한 연구 개발은 미약한 상태이다. 본 논문은 정보보호의 주요 요소인 취약성과 공격 그리고 방어의 개념을 모의 실험을 통해 쉽게 이해하기 위한 교육용 시뮬레이터에 관한 연구를 소개한다. 정보보호를 위한 교육용 시뮬레이터는 복잡한 네트워크에 내재된 예측하기 힘든 취약점을 분석하고, 기존 구성되어 있는 네트워크의 설계를 변경 할 경우나 새로운 네트워크를 구성하고자 할 경우에 발생하는 취약점의 특성과 공격에 따른 피해 상황 등을 분석할 수 있다. 또한, 정보통신 시스템에 내재되어 있는 취약점의 노출로 인해 발생하는 피해와 피해 발생으로 인한 파급효과를 예측할 수 있다. 이러한 과정을 통해서 정보통신 시스템이 갖는 정보보호 요소에 대한 명확한 이해를 할 수 있게 된다.

본문에서는 교육용 시뮬레이터에 적용된 모델링 방법론에 대한 내용을 설명하고, 네트워크에 존재하는 취약성을 진단하고 분석하기 위해 기반 연구인 자동 공격 도구에 관한 연구 내용을 살펴본다. 이후 교육용 시뮬레이터의 구조와 기능에 대해 설명하고, 교육용 시뮬레이터를 이용하여 네트워크의 정보보호 요소들에 관한 특성을 분석한 결과와 활용 방안에 대해 설명한 후 결론을 맺는다.

2. 모델링 방법론

본 논문에서 제시하는 교육용 시뮬레이터에 적용된 이산사건 모델링 방법인 DEVS (Discrete Event System Specification) 형식론[1]에 대해 알아본다. 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 모델링 할 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.

$$M = < X, S, Y, \delta_{int}, \delta_{ext}, \lambda, t_a >$$

이때, X는 입력 사건의 집합을, S는 순차적 상태의 집합을, Y는 출력 사건의 집합을, δ_{int}는 S → S의 내부 전이 함수를, δ_{ext}는 Q × X → S의 외부 전이 함수를, λ는 S

→ Y의 출력 함수를, t_a는 S → R+0 → ∞의 시간 진행 함수를 나타내고, 이때 집합 Q 는 {(s,e) | s ∈ S, 0≤e ≤t_a(s)}이고, e 는 최근 상태전이 이후로 흐른 시간을 나타낸다.

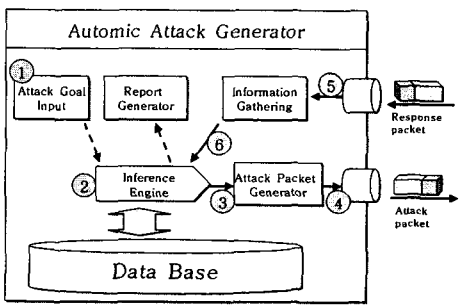
커플된 모델의 구성은 다음과 같다.

DN = < D, {M_i}, {I_i}, {$Z_{i,j}$}, select>

이때, D는 커플된 모델의 구성요소인 모델 i에 대한 이름의 집합을, M_i는 구성요소가 되는 기본 모델을, I_i는 모델 i의 영향을 받는 모델들의 집합을, $Z_{i,j}$는 I_i의 원소 각 j에 대해서 i에서 j로의 출력 번역 함수를, Select : 타이브레이킹 함수를 나타낸다.

3. 자동 공격 생성기(Automatic Attack Generator)

정보통신 시스템이 갖는 취약점에 대한 진단, 분석하기 위한 기반 연구인 자동 공격 생성기에 대해 알아보자. 자동 공격 생성기의 구조는 아래 (그림1)과 같다. 자동 공격 생성기는 사용자로부터 공격 목표를 입력받는 부분과 입력받은 공격 목표, 데이터 베이스에 저장되어 있는 공격 목표에 해당하는 공격 방법, 생성된 공격 패킷의 응답 패킷의 정보를 이용하여 적절한 공격 패킷을 생성하기 위한 정보를 추론하는 부분과 추론된 정보를 사용하여 공격 패킷을 생성하는 부분과 공격 패킷에 대한 대상 정보통신 시스템의 응답 패킷 정보를 수집하는 부분, 그리고 결과 보고서를 작성하는 부분으로 구성된다. 자동 공격 생성기는 사용자의 입력을 통한 공격 목표 - 즉, 분석 목표 -를 갖고 공격 패킷을 생성하여 대상 정보통신 시스템의 반응을 기반으로 하여 네트워크와 정보통신 시스템에 존재하는 취약성을 추론하고 추론 결과를 최종 보고서의 형태로 사용자에게 제시된다.

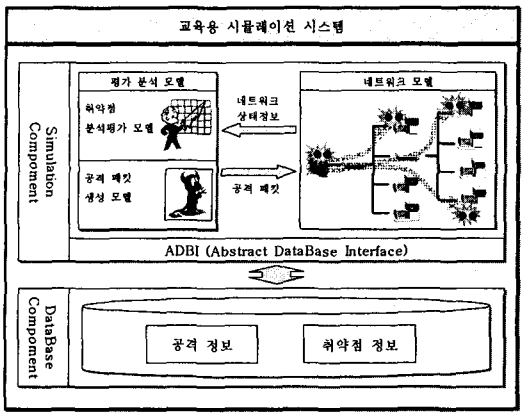


(그림 1) 자동 공격 생성기의 구조

자동 공격 생성기의 동작을 살펴보자. 우선, ①과 같이 자동 공격 생성기는 사용자로부터 취약성 분석 대상 정보통신 시스템의 IP 주소 범위와 분석 목적에 해당하는 공격 목표를 입력받는다. 다음으로 ②와 같이 공격 목표와 이미 수집된 정보 등을 이용하여 공격 패킷 생성을 위한 정보를 추론한다. 추론된 정보를 이용하여 ③에서는 공격 패킷을 생성하고, ④와 같이 자동 공격 생성기와 연결된 네트워크를 통해서 패킷을 전송한다. 대상 정보통신 시스템의 공격 패킷에 대한 응답 패킷의 정보를 ⑤와 같이 수집한다. 수집된 정보는 ⑥과 같이 다음 공격을 생성하는데 이용할 수 있도록 추론엔진으로 전달된다. 자동 공격 생성기는 위의 과정을 계속 반복하면서 분석 대상 네트워크에 존재하는 취약점을 분석해낸다. 이러한 분석에 사용되는 공격 방법에 관한 정보와 추론의 기반의 되는 지식은 자동 공격 생성기가 갖고 있는 데이터베이스를 기반으로 한다. 자동 공격 생성기에서 사용하는 공격 방법들은 이미 알려 진 공격 방법들을 데이터베이스로 구축하였다가 자동 공격 도구가 공격을 생성할 경우에 사용하고, 그 공격에 대한 응답에 대한 지식을 구축하였다가 자동공격 생성기에 의해 수집된 네트워크 정보를 분석, 추론하여 네트워크에 내재된 취약점에 관한 정보를 사용자에게 제시한다.

4. 교육용 시뮬레이터의 구조 및 기능

교육용 시뮬레이터의 구성은 아래 (그림 2)와 같이 시뮬레이션 구성요소와 데이터베이스 구성요소로 이루어진다.



(그림 1) 교육용 시뮬레이터 구조

※ 시뮬레이션 구성 요소들

○ 공격 패킷 생성 모델 : 네트워크 모델의 정보를 수집하여 적절한 공격 패킷을 생성하여 대상 네트워크 시스템에 전송하는 역할을 하는 모델이다. 공격 패킷의 생성은 위하여 수집된 네트워크 정보와 공격 정보 데이터 베이스의 내용을 기반으로 공격 패킷 생성 모델

내의 추론엔진에서 한다.

○ 평가 모델 : 평가 모델은 공격 패킷 생성 모델의 공격에 따른 대상 네트워크 모델의 상태 변화, 공격 경로, 공격 성공 여부 등에 관한 정보를 분석하는 역할을 한다.

○ 네트워크 모델 : 네트워크 모델은 분석 대상이 되는 가상의 네트워크를 구성하기 위한 구성요소로 호스트 모델, 라우터 모델, 허브 모델, 보안 시스템인 필터 모델, 프락시 모델들의 집합으로 이루어진다. 네트워크 모델을 이루는 구성요소들에 대해 살펴보자.

⇒ 호스트 모델 : 네트워크 호스트 시스템이 갖는 특성에 따라 갖게 되는 취약성을 추상화하여 표현한다. 데이터베이스의 취약점 정보의 내용을 이용하여 구성한다. 또한 호스트 모델에서는 호스트에서 사용하는 운영체제가 제공하는 접근 제어 모듈과 사용자 인증을 통한 보안 메커니즘도 갖는다.

⇒ 네트워크 디바이스 모델 : 네트워크 모델에서 사용하는 네트워크 디바이스 모델은 라우터와 허브를 추상화하여 구성한다. 라우터 모델은 라우팅 테이블을 이용하여 패킷의 경로를 설정하고, 허브 모델은 하나의 서브넷을 구성하여 서브넷 내부에서의 패킷 전송을 담당한다.

⇒ 보안 시스템 모델 : 보안 시스템 모델은 필터와 프락시 모델이 있다. 필터 모델은 전송하는 패킷의 근원지와 목적지에 관한 헤더 정보와 패킷의 전송 간격을 기준으로 패킷의 접근 통제를 한다. 프락시 모델은 전송하는 패킷의 내용을 기반으로 하여 접근 통제를 한다.

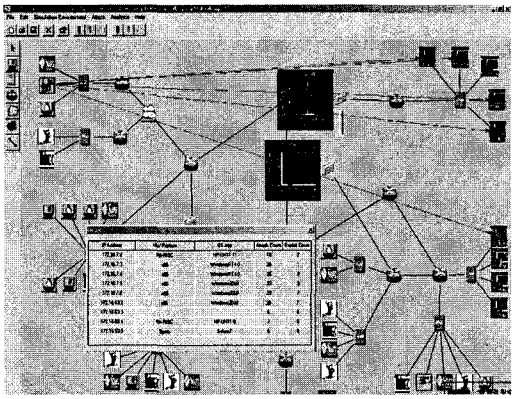
※ 데이터 베이스 구성 요소들

○ 공격 정보 데이터 베이스 : 공격 정보 데이터 베이스는 공격자 모델이 사용하는 정보들로, 대상 네트워크의 정보를 수집하는 방법, 공격자의 공격 패킷에 따른 네트워크 모델의 반응인 응답 패킷의 내용을 분석하여 다음 공격을 결정하는 추론 과정에서 사용하는 정보들로 구성된다.

○ 취약점 정보 데이터 베이스 : 취약점 정보 데이터 베이스는 네트워크 모델이 갖는 취약점에 관한 정보를 갖고 있어, 이 정보를 기반으로 네트워크 모델이 취약점 정보를 설정한다. 또한, 취약점 제거를 위한 정보도 구축되어 있어, 시뮬레이션을 실행하는 사용자에게 네트워크 시스템을 더욱 견고하게 설정, 관리할 수 있는 정보를 제공한다.

5. 교육용 시뮬레이션 실행 결과 분석

교육용 시뮬레이터의 실행 화면은 아래 (그림 3)과 같다.



(그림 2) 교육용 시뮬레이터 실행화면

교육용 시뮬레이터의 구성은 메뉴바와 도구모음 그리고 네트워크 환경을 구성할 수 있는 에디팅 캔버스로 이루어진다. 그림의 왼쪽 윗부분에 있는 도구모음을 살펴보자. 이 도구모음에는 교육용 시뮬레이터에서 사용하는 네트워크 구성요소들을 표현하고 있다. 즉, 호스트 모델, 라우터 모델, 허브모델, Firewall모델 등과 이 모델들을 연결시켜서 네트워크 상의 패킷의 흐름을 설정할 수 있는 연결 도구 그리고 인터넷(구름)모델이 있다.

(그림 3)에 나타나 있는 시뮬레이터 실행 결과는 분석해 보면, 화면의 왼쪽 상단 호스트에 공격자 모델이 위치하여 화면의 오른쪽에 있는 호스트들을 공격한 모습을 나타내고 있다. 각각의 호스트들이 공격자 모델로부터 공격받은 공격경로를 표시하여 공격경로에 대한 정보를 습득할 수 있고, 각 공격경로에 공격 시도에 대한 그래프를 보여주어 시도된 공격경로들의 안전성을 비교하여 취약한 부분에 대한 정보를 습득할 수 있도록 하였다. 이러한 교육용 시뮬레이션을 위해서 사용자가 직접 네트워크를 구성할 수 있는 기능을 제공하여 다양한 종류의 네트워크를 구성해 가면서 네트워크 보안에 관한 정보를 사용자 스스로 습득해 나아갈 수 있다.

6. 결론

이상으로 보안 시뮬레이션 방법을 적용하여 네트워크 보안교육을 위한 시뮬레이션 방법에 관해서 알아보았다. 교육용 시뮬레이터의 적용은 공격과 방어 메커니즘의 적용에 따른 대상 네트워크의 상태 변화를 유연하고, 효과적으로 분석할 수 있다는 장점이 있다. 실제 존재하지 않는 가상의 네트워크를 대상으로 시뮬레이션을 실행하기 때문에 분석 대상 네트워크의 성능에 영향을 미치지 않는

다. 또한 가상을 네트워크가 시뮬레이션의 대상이 되므로 현재는 존재하지는 않지만, 앞으로 구성하고자 하는 네트워크에 대한 취약성을 미리 분석하여 더욱 견고하고 안전한 네트워크를 설계하여 구성할 수 있도록 해준다. 보안 시뮬레이션의 적용 방법은 공격 대상이 되는 네트워크 모델의 취약성을 제거하는 방법으로 제시된 해결 방법을 사용자가 바로 적용하여 다시 시뮬레이션을 실행하면서 그 제시된 방법이 얼마나 유효한지에 대한 측정도 가능하게 해 준다. 이러한 시뮬레이터를 이용하여 네트워크 교육의 질적 향상을 기대할 수 있다.

참고문헌

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

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

[3] 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

[4] 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