정보보호 가상망 모델링 및 시뮬레이션

윤호상° 장희진 김상수 박재근 김철호
국방과학연구소
{yunhs°, janghj}@add.re.kr, wisdory@naver.com, parkjaek@korea.com, cheolkim@add.re.kr

CyberSecurity Virtual Network Modeling and Simulation

Hosang Yun°, Heejin Jang, Sangsoo Kim, Jaekeun Park, Cheolho Kim
Agency for Defense Development

요 약

국방정보보호 통합관리 기술을 개발하기 위한 테스트베드 구축에서 중요한 부분 중에 하나인 정보보호 가상망 모델링 시뮬레이션 시스템을 개발하였다. 본 시스템은 실재 망과 유사한 정보보호 환경을 제공하기 위하여 정보보호 환경을 구성하는 정보보호 객체(호스트, 네트워크, IDS, IPS, FW, VW 등)를 모의하고 망의 트래픽(평상시, 사이버 공격 시)을 모의하는 등의 기능을 제공하고 외부의 보안관제 체계 및 모의 공격기와 연동하는 인터페이스를 제공하여 외부 침입탐지체계의 성능을 검증하거나 취약점 분석을 위한 환경을 제공한다.

1. 서 론

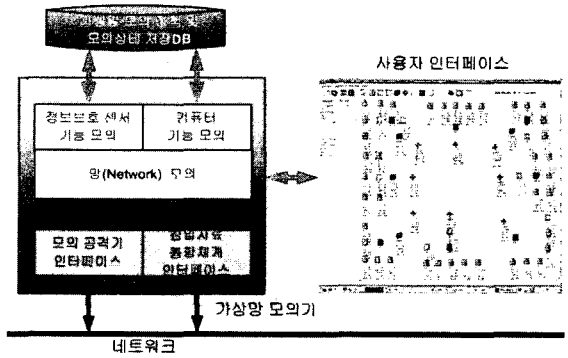
국방정보보호 통합관리 기술을 개발하기 위한 테스트베드 구축에서 중요한 부분은 개발 기술이나 장비 등의 기능을 시험하기 위한 망(network)이 필요하다. 그러나 기존의 망을 시험용으로 사용하기에는 문제점이 많고 별도로 구축하는 데는 비용과 시간이 많이 들기 때문에 정보보호 기술개발을 위해서는 가상의 망을 구축하여 정보보호 객체(호스트, 네트워크, IDS(Intrusion Detection Syetem, IPS(Intrusion Prevention System), FW(Fire Wall), VW(Virus Wall)등)를 모의하고 망의 트래픽(평상시, 사이버 공격 시)을 생성하는 등의 기능을 수행하여 실재 망과 유사한 정보보호 환경을 제공하여야 한다.

정보보호 영역에서의 모델링 및 시뮬레이션의 예는 다음과 같이 구분할 수 있다[1].

1) Packet Wars[2]: 네트워크 레벨의 공격과 방어가 가능한 실재 시스템을 이용하여 훈련한다.
2) Sniffers + Network Design Tools: 실 네트워크 데이터를 수집하여 네트워크 설계 도구에 입력하여 네트워크 환경을 분석한다.
3) Canned Attack/Defend Scenarios[3]: 게임과 같이 단독으로 정보보호 환경 모의한다. 정해진 공격과 방어기술을 이용하여 훈련한다.
4) Management Flight Simulators[4]: 정보보호를 위한 각 구성요소를 동적/이산적 도구를 이용하여 모델링하여 공격이 조직, 장비 및 데이터에 미치는 영향을 분석한다.
5) Role-playing[5], 정보보호를 위한 인력의 훈련을 위하여 각 담당의 역할훈련을 수행한다.

본 연구에서 개발한 가상망 모의시스템은 정보보호 측면의 가상망에서 필요로 하는 정보보호 객체 및 침입탐지 관련 망 트래픽을 모델링하고 시뮬레이션 하는 시스템으로 정보보호 통합관리 기술 개발에 필수적인 시스템이다.

정보보호 가상망 모델링 및 시뮬레이션 시스템은 크게 망객체 모의 부분과 망 트래픽 모의 및 외부 인터페이스로 구분된다. 망객체 모의 부분은 정보통신망에 존재하는 다양한 객체 중에서 정보보호 시스템과 관련 있는 객체를 식별하고 이 객체들의 통신망 내에서 동작과 기능을 모델링하였으며, 망 트래픽 모의 부분은 정보통신망의 평상시의 트래픽에 대한 모델링과 사이버공격이 발생하였을 때의 트래픽을 모델링하고 구현하였다.



<그림 1> 정보보호 가상망 모의기 구성도

또한 가상망의 망 트래픽 모의를 위한 모의정책을 시간별/날짜별/프로토콜별 트래픽 모의가 가능하도록 설계하였으며 외부 정보보호 통합 관리 인터페이스와 모의공격기 인터페이스를 이용한 상호운용이 편리하도록 설계하였다.

본 논문의 구성은 1장 서론에 이어 2장에서 정보보호 가상망 모의시스템의 구성요소에 대하여 기술하고, 3장에서 정보보호 가상망 모의기의 설계에 대하여 설명하고 4장에서 결론을 맺는다.

2. 가상망모의시스템의 구성요소

2.1 정보보호 가상망 모의

(1) 망 모의

망 모의 구성요소는 망의 토폴로지(topology), 네트워크 장비(라우터, 스위치)모의로 구성되며 각 장비의 상태(정상, 장애)모의를 포함한다.

(2) 정보보호센서 모의

정보보호 센서로서 침입탐지장비(IDS), 침입방지장비(IPS), 방화벽(FW), 각종 상태에이전트를 포함한다.

- IDS : 침입탐지, 이벤트전송, 보안정책 관리, 침입탐지 패턴모의
- IPS : 보안정책 관리, 침입탐지/차단 모의, 침입대응 모의, 자료수집 모의, 침입탐지 패턴관리, 접근통제 규칙관리
- FW : 보안정책관리, 접근통제 모의, 침입대응 모의, 자료수집 모의, 접근통제 규칙관리
- 네트워크 상태 모니터링 에이전트 : 네트워크상태 모의, 상태정보 전송기능 모의
- 대응/역추적 에이전트 : 세션 관련성검색 기능모의, 추적결과 전송기능 모의

(3) 트래픽 모의

- 정상상태의 트래픽 모의 : 요일별/시간대(0~24)별/프로토콜(ICMP, TCP, UDP)별 데이터량 설정, 서버/클라이언트 접속비율 설정, 출발지/목적지 IP 랜덤 선택, 출발지(1024~65535)포트 랜덤 선택, 목적지포트는 서비스포트(ftp, telnet, http, pop3, icmp 등) 비율에 따라 선택, 트래픽 유지시간 랜덤 선택
- 침해상태의 트래픽 모의 : 공격에 따라 각 객체들의 침해상태 모의를 통한 네트워크 트래픽 변화 모의

(4) 호스트모의

- 취약점/보안패치 상태모의, 각 호스트별로 취약점 및 보안패치 상태 유지, 침입상태 모의
- CPU & 메모리 & 트래픽 생성 : 공격의 종류에 따라 증가 비율 설정
- 공격 경유지 모의 및 공격 희생자 모의, VW모의, HIDS(Host Intrusion Detection System)모의

2.2 기타 기능

(1) 외부 체계 인터페이스

외부의 실 침입탐지 체계 및 모의 공격기와의 인터페이스로서 가상망의 상태 및 이벤트/데이터를 전송하고 침입탐지 체계의 제어명령(관리명령, 대응명령 등) 수행한다.

(2) 패킷 수신/분석

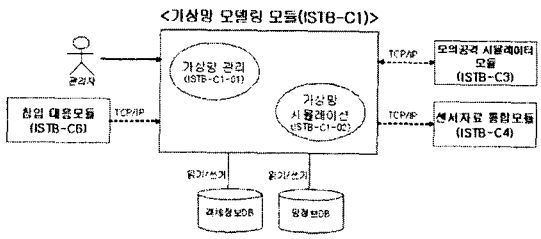
모의공격 데이터, 활동정보, 대응기능 정보, 보안패치 정보, 역추적 매니저 정보, 패킷 생성/송신, 모의공격 결과, 보안패치 결과, 역추적 매니저 결과, 이벤트 정보를 분석하여 가상망에 반영하고, 가상망의 변화에 대한 결과를 생성하여 외부에 전송한다.

(3) 시뮬레이션 관리

망 토폴로지, 노드배치, 정보보호센서 배치, 각 모의객체의 초기화 등과 같은 시뮬레이션 환경을 구축하고, 시뮬레이션 시작/ 종료 ,가상망 상황 모니터링, 정보보호센서 장비의 정책(규칙) 변경, 취약점 변경 등 시뮬레이션 진행 관리를 수행한다.

3. 설계

가상망 모델링 모듈은 가상망 관리 기능과 가상망 시뮬레이션 기능으로 구성된다.



<그림 2> 가상망 모델링 모듈

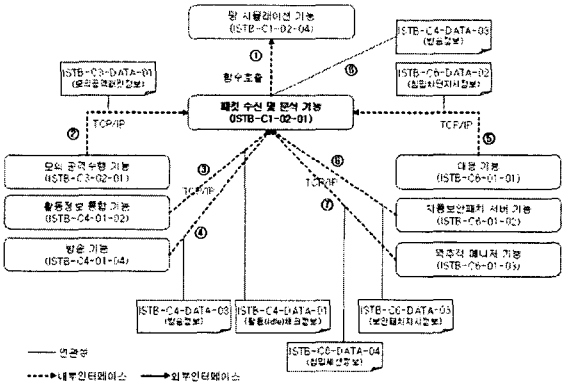
3.1 가상망 관리

망객체 인스턴스 관리 기능을 통하여 관리자가 가상망을 구성하는 객체(라우터, 호스트, FW, IPS, IDS, 망상태 수집에이전트, 역추적 에이전트) 인스턴스의 속성 및 기능을 조회/추가/변경/삭제하고, 객체(호스트) 인스턴스를 그룹화 하고 망 관리 기능을 이용하여 가상망을 조회/추가/변경/삭제할 수 있다.

3.2 가상망 시뮬레이션

(1) 패킷 수신 및 분석 기능

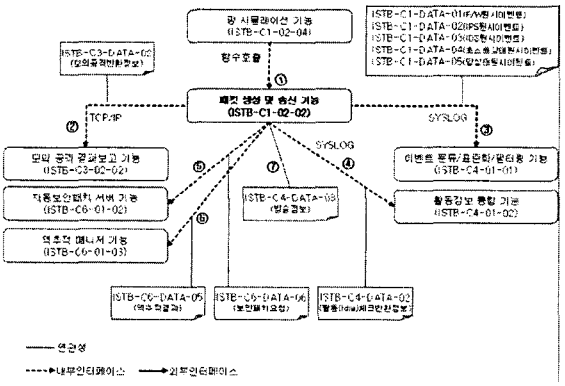
타 기능에서 전송한 패킷을 수신/분석하여 추출된 데이터를 망 시뮬레이션 기능으로 전달하는 기능이다.



<그림 3> 패킷 수신 및 분석 기능

(2) 패킷 생성 및 송신 기능

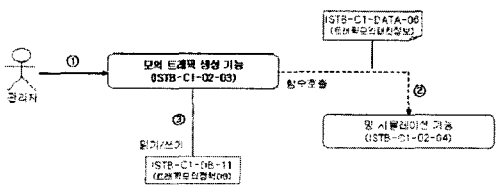
망 시뮬레이션 기능으로부터 전달받은 데이터를 참조하여 패킷을 생성하고 타 기능으로 전송하는 기능이다.



<그림 4> 패킷 생성 및 송신 기능

(3) 모의 트래픽 생성 기능

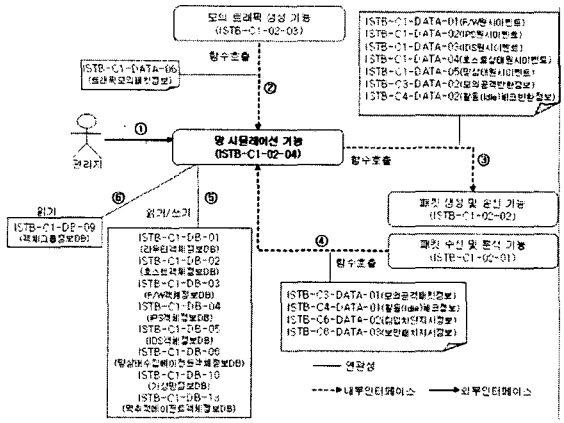
설정한 모의 트래픽 정책에 따라 트래픽을 모의하는 기능이다.



<그림 5> 모의 트래픽 생성 기능

(4) 망 시뮬레이션 기능

패킷 수신 및 분석 기능으로부터 전달받은 데이터를 이용하여 망을 시뮬레이션하고, 망 시뮬레이션 결과 데이터를 패킷 생성 및 송신 기능에게 전달한다.



<그림 6> 망 시뮬레이션 기능

4. 결론

본 논문에서는 국방정보보호 통합관리 기술을 개발하기 위한 테스트베드 구축에서 중요한 부분 중에 하나인 정보보호 가상망을 구축하여 정보보호 객체를 모의하고 망의 트래픽(평상시, 사이버 공격 시)을 생성하는 등의 기능을 수행하여 실재 망과 유사한 정보보호 환경을 제공하였다. 또한 정보보호 네트워크 취약점 분석이나 위협분석과 같은 분석 기술을 개발하는데 중요한 데이터를 제공할 수 있으며 사이버침입 탐지 모의 훈련체계 개발에 필요한 모의 기술에도 많은 기여를 할 것으로 판단된다.

[참고문헌]

[1] John H. Saunders, *The Case for Modeling and Simulation of Information Security*, National Defense University, 2002.

[2] Hill, John M.D. et al. *Using an Isolated Network Laboratory to Teach Advanced Networks and Security,* Unpublished paper. Contact hillj@cs.tamu.edu. 2000.

[3] Waag, Gary L. et al. *Modeling and Simulation for Information Assurance: State-of-the-Art Report*, IATAC, Defense Technical Information Center, Ft Belvoir, VA. 2001.

[4] Saunders, John. Management Flight Simulators. Info Tech Talk. Spring 1998.

[5] Roberts, Roxanne. A War Game to Send Chills Down the Spine. The Washington Post. October 23, 2001.