정보보호 시스템의 성능평가를 위한 시험 도구의 설계

전준상*, 정연서**, 소우영*
*한남대학교 컴퓨터공학과
**한국전자통신연구원
e-mail:yeerock@neuro.hannam.ac.kr
jys847@etri.re.kr
wsoh@neuro.hannam.ac.kr

Design of Test Tool for Performance Evaluation of Information Security System

Junsang Jeon*, Younseo Jeong**, Wooyoung Soh*
*Dept of Computer Engineering, Hannam University
**Electronics and Telecommunications Research Institute

요 약

최근 정보보호에 대한 관심이 점점 높아짐에 따라 정보보호시스템에 대한 다양한 요구가 발생하고 있으며, 정보보호시스템 개발 업체들은 관련된 정보보호시스템들을 개발하여 출시하고 있다. 또한 이러한 정보보호 시스템들을 평가하고 인증하기 위한 여러 가지 방법들이 제시되고 있다. 그러나 이러한 방법들은 많은 시간과 비용이 들며, 전문적인 지식이 없는 경우에는 별로 유용하지 못한 정보가 된다. 본 논문에서는 이를 해결하기 위해서 사용자가 직접 정보보호 시스템의 성능을 평가해 볼 수 있는 시험도구를 제안한다.

1. 서론

현대 사회의 정보화가 빠르게 진행되고, 그에 대한 역기능이 발생하면서 정보보호에 대한 관심과 필요성이 급격히 증대되고 있으며, 많은 기업들이 정보보호 시스템을 도입하고 있다.

그러나 기업에서 정보보호 시스템을 도입할 때, 정보보호시스템의 성능이 기업이 요구하는 정보보호 시스템의 성능에 만족하는 지에 관한 여부를 판단하기 힘들다. 물론, 정보보호시스템 평가·인증을 통해 이 부분에 대한 해결을 모색할 수 있다.

정보보호시스템에 대한 평가·인증은 신뢰된 기관에서 담당하고 있으며, 세계적으로 공통 평가를 위한 체계를 수행 중에 있다. 가장 대표적인 것이 CC(Common Criteria)기반의 정보보호시스템 평가이다. 그러나 CC기반의 평가기준을 만족하기 위해서는 정보보호 시스템의 개발 과정을 문서화하여 제출하여야 한다. 또한 평가의 기간도 목표등급에 따라 수개월에서 수년이 걸리고, 평가에 드는 비용도 목표등급에 따라 일천만원 정도에서 수천만원정도 발생한다. 따라서 중소기업의 경우 평가·인증을 받기에는 많은 어려움이 있다. 또한 많은 평가 도구들이 개발되어져 사용되고 있으나 가격이 매우 높아 쉽게 구매를 결정하기 어렵다[1][2].

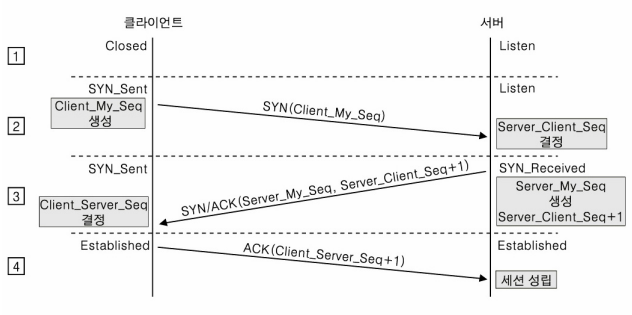
이러한 문제점을 해결하기 위하여, 본 논문에서는 정보보호시스템의 성능을 평가해 볼 수 있는 시험도구를 설계하였다. 본 논문의 2장에서는 시험도구를 개발하기 위해 사용되어지는 기술들과 기존 연구결과에 대해 조사·분석하고, 3장에서는 평가도구의 설계에 대해 제안하고, 4장에서는 본 논문의 결론 및 향후 연구 과제를 제시한다.

2. 관련연구

2.1 TCP 프로토콜

TCP 프로토콜은 연결 지향(connection oriented) 프로토콜(호스트끼리 통신을 하기 위해서는 우선 서로 연결해 놓아야 통신이 가능한 프로토콜)이며, 3

웨이 핸드쉐이크를 통해 연결이 이루어진다. 먼저 클라이언트는 서버의 응답을 받은 경우 연결이 이루어진 것으로, 서버는 자신의 응답신호에 대한 클라이언트의 응답을 받은 경우 연결이 이루어진 것으로 간주한다. 간혹 서버의 응답신호에 대한 클라이언트의 응답신호가 서버에 전달되지 않은 경우가 있는데 이런 경우 서버는 잠시 동안 불안정한 상태로 남게 되며 정상적인 작동을 하지 못할 수도 있게 된다. (그림 1)은 3웨이 핸드쉐이크 방식을 도식화 한 것이다.



(그림 1) 3웨이 핸드쉐이크

이와 같은 과정을 통해 TCP프로토콜은 연결이 이루어지게 된다.

2.2 패킷 스니핑

스니퍼는 컴퓨터 네트워크상에 흘러 다니는 트래픽을 엿듣는 도청장치라고 말할 수 있다. 그리고 스니핑(Sniffing)이란 이러한 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 말한다.

스니핑은 LAN 상에서 개별 호스트를 구별하기 위한 방법으로 이더넷 인터페이스는 MAC(Media Access Control) 주소를 갖게 되며, 모든 이더넷 인터페이스의 MAC 주소는 서로 다른 값을 갖는다. 따라서 로컬 네트워크상에서 각 각의 호스트는 유일하게 구별될 수 있다. (그림 2)는 이더넷(ethernet) 프레임의 포맷을 나타낸다.

Destination Mac Addr 6 Byte	Source Mac Addr 6 Byte	Type 2 byte
Data 46-1500 Byte		CRC 4 Byte

(그림 2) 이더넷 프레임 포맷

이더넷 포맷은 type에 따라 (그림 3)과 같은 3가지로 구성된다.

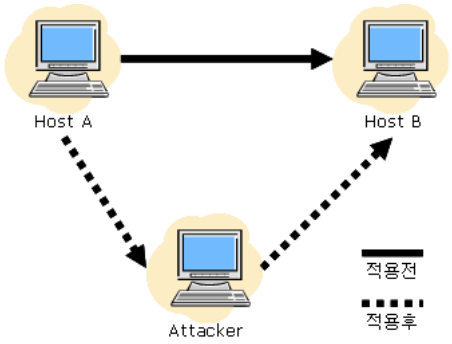
Type 0800	IP Datagram 46-1500 Byte	
Type 0806	ARP request/reply 28 Byte	PAD 18 Byte
Type 8035	RARP request/reply 28 Byte	PAD 18 Byte

(그림 3) 이더넷 포맷의 3가지 타입

이더넷은 로컬 네트워크내의 모든 호스트가 같은 선(wire)을 공유하도록 되어 있다. 따라서 같은 네트워크내의 컴퓨터는 다른 컴퓨터가 통신하는 모든 트래픽을 볼 수 있다. 하지만 이더넷을 지나는 모든 트래픽을 받아들이면 관계없는 트래픽까지 처리해야 하므로 효율적이지 못하고 네트워크의 성능도 저하될 수 있다. 그래서 이더넷 인터페이스(LAN 카드)는 자신의 MAC address를 갖지 않는 트래픽을 무시하는 필터링 기능을 가지고 있다. 이 필터링 기능은 자신의 MAC address를 가진 트래픽만을 보도록 한다. 또한 이더넷 인터페이스에서 모든 트래픽을 볼 수 있도록 하는 기능인 프로미시우스 모드(promiscuous mode)로 설정하여 로컬 네트워크를 지나는 모든 트래픽을 도청할 수 있게 된다[3][4][5].

2.3 IP 스푸핑

IP 스푸핑(Spoofing)이란 IP속이기란 의미이다. 즉, 타겟호스트와 신뢰관계를 맺고 있는 다른 호스트로 IP를 속여서 들어가는 걸 의미한다. 미 국방성의 TCP/IP 프로토콜 표준은 1979년 인터넷을 구현하기 위해서 디자인되었다. 가장 많이 쓰이는 TCP/IP는 4.2BSD 시스템에서 구현된 것으로 Bell Lab과 미국방성 네트웍에서 사용되었다. 4.2BSD 유닉스 TCP/IP 프로그램은 매우 유동적이며 사용하기 편리하지만 보안측면에서는 많은 약점을 가지고 있다. 이 약점의 하나를 공격하는 IP 스푸핑 Attack은 1985년 Morris에 의하여 아이디어가 처음 지적되었고 실제로 1995년도에 사용되었다.



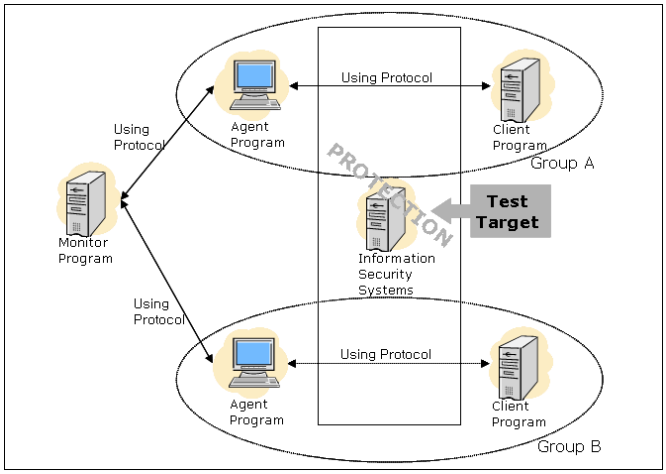
(그림 4) 스푸핑 적용 효과

(그림 4)처럼 스푸핑은 LAN 상에서 송신부의 패킷을 송신과 관련 없는 다른 호스트에게 가지 않도록 하는 스위칭 기능을 마비시키거나 속여서 자기 컴퓨터에게 그 패킷이 오도록 처리하는 것을 말한다. 이 경우 송신부에서 내 컴퓨터로 오는 패킷을 다시 수신부로 전송해야 하는데 이를 릴레이(Relay)라 한다. 릴레이를 하지 않으면 송신부와 수신부 사이에 네트워크가 마비된 것처럼 되어 버리기 때문에 반드시 릴레이를 해 주어야 한다. 그리고 릴레이를 할 경우 내 컴퓨터에서 그 패킷을 변조할 수도 있는데, 이는 TCP나 UDP 계층에서 자체적인 프로토콜의 인증 과정의 절차로 인해 수신부에서 패킷을 포기(drop)한다[6][7][8].

3. 정보보호시스템 성능평가 시험도구의 설계

3.1 전체 시스템 구성

본 논문에서 제시하는 시험도구는 스노트 룰을 이용하여 공격에 대한 정보를 수집하고, 이를 이용하여 공격 패킷을 생성하여 해당 시스템에 전송하게 된다. 그리고 전송된 결과를 수집하여 사용자에게 전송결과를 보여준다.



(그림 5) 정보보호 시스템 성능평가 시험도구의 전체 구성도

본 평가 도구의 구성을 살펴보면, 모니터 프로그램에서 공격에 대한 정보를 선택하여 에이전트 프로그램으로 명령을 하달한다. 명령을 받은 에이전트 프로그램은 UDP인 경우 공격 패킷을 생성하여 바로 전송하게 되고, TCP인 경우 3웨이 핸드쉐이킹을 통해 TCP연결을 수행한 후 공격 패킷을 전송하게 된다. 클라이언트 프로그램은 로그기록을 살펴보다가, 공격 패킷에 대한 정보가 로그에 남으면 이를 에이전트 프로그램을 통해 모니터 프로그램으로 전송한다. 모니터 프로그램은 전송된 결과를 수집하여 해당 성능평가에 대한 결과를 출력한다.

3.2 모니터 프로그램

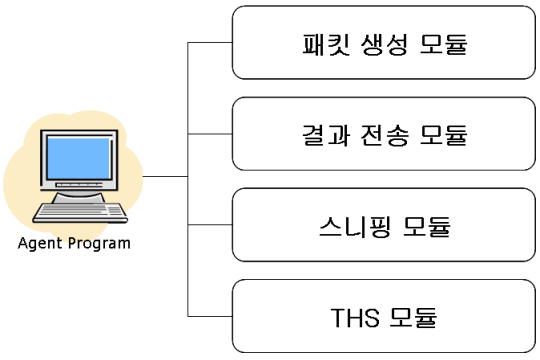
모니터 프로그램은 사용자가 명령을 내리고, 결과를 볼 수 있는 콘솔로 사용된다. 모니터 프로그램은 크게 시나리오를 작성하여 에이전트에 전송하는 시나리오 모듈과 클라이언트로부터 오는 전송결과를 수집하여 분석, 결과를 출력하는 전송결과 출력 모듈로 나눌 수 있다.

(그림 6) 모니터 프로그램

3.3 에이전트 프로그램

에이전트 프로그램은 작성된 시나리오를 바탕으로 공격에 대한 패킷을 생성하여 해당하는 클라이언트 프로그램으로 전송하는 역할을 담당하는 부분이다.

본 논문에서는 다중도메인 환경에 대한 정보보호 시스템 시험평가를 위해 하나의 에이전트 프로그램이 여러 개의 IP주소를 가지고 있는 것처럼 보이기 위해 패킷을 스니핑하는 모듈이 추가되어 있고, TCP프로토콜을 이용하는 공격을 위해 스니핑 된 정보를 이용한 IP 스푸핑 기술로 3웨이 핸드쉐이킹을 하는 모듈도 추가되어 있다.



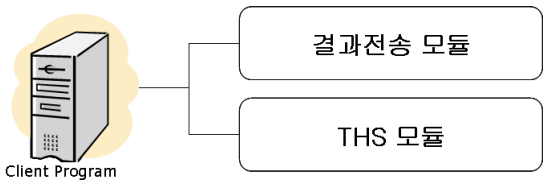
(그림 7) 에이전트 프로그램

3.4 클라이언트 프로그램

클라이언트 프로그램은 테스트 하고자 하는 정보보호 시스템들의 뒤편에 있는 시스템에 설치하는 프

로그램이다. 이를 이용하여 에이전트 프로그램에서 전송하는 공격에 대한 수신여부와 탐지여부를 파악할 수 있다.

먼저 클라이언트 프로그램은 자신에게 전송되어지는 공격에 대한 결과를 수집한다. 또한 정보보호시스템들의 로그를 분석하여 본 공격이 탐지가 되었는지 여부를 수집한다. 이렇게 수집된 결과들은 에이전트 프로그램에게 전송되어 지며, 전송되어진 결과는 에이전트 프로그램이 수집하여 모니터 프로그램에게 전송하여 출력되어진다.



(그림 8) 클라이언트 프로그램

4. 결론 및 향후연구과제

정보 기술 및 인터넷의 발달로 컴퓨터 시스템이 국경을 넘어 전 세계로 연결되어 편리하게 사용되고 있으나 해킹, 바이러스 감염, 서비스 방해, 불건전 정보 유통 등 정보화 역기능도 확산되고 있다. 현재 인터넷으로 연결되어있는 컴퓨터 시스템 자원은 보안상 취약성이 높고 위험에 노출된 상태로써 이를 효과적으로 방어할 수 있는 대응수단으로서의 정보보호 시스템이 개발되고 있다. 그리고 현재 네트워크에서의 공격은 다중도메인 환경에서 이루어지고 있으며, 이러한 공격을 막기 위해 다중도메인 환경에서의 정보보호 시스템들도 개발되어 지고 있다.

이러한 시스템들을 사용함으로써 네트워크를 효과적으로 방어할 수 있으나, 이러한 시스템들이 적합한 성능을 내고 있는지에 대한 시험이 필요하다. 또한 정보보호시스템의 평가·인증제도가 도입되어 시행되고 있지만, 중소기업의 경우에는 이를 활용하여 제품에 대한 평가·인증을 적용하기에는 어려움이 있다.

본 논문에서 제안한 정보보호시스템 성능평가 시험도구는 이러한 문제점들에 대해 해결할 수 있을 것으로 예상되며, 앞으로 이를 위해 시험도구의 구현과 그를 이용한 정보보호시스템 성능평가 방법론에 대한 연구도 진행되어야 할 것이다.

참고문헌

[1] 최용락, 소우영, 이재광, 이임영, “컴퓨터 통신보안 3판”, 그린, 2005.

[2] 한국정보보호센터, “정보보호시스템 평가·인증 가이드”, 2000

[3] Ryan Spangler, “Packet Sniffing on Layer 2 Switched Local Area Networks”, Packetwatch Research, 2003.

[4] Mikro Tik, “Packet Sniffer”, Mikro Tikls SIA, 2004.

[5] Michael J Jipping, Andrew Kalafut, “Investigating Wired and Wireless Networks Using a Java-based Programmable Sniffer”, ITiCSE'04, 2004.

[6] Anat Bremler-Barr, Hanoch Levy, “Spoofing Prevention Method”, IEEE, 2005.

[7] Josha Bronson, “Protecting Your Network From ARP Spoofing-Based Attacks”, Foundstone, 2004.

[8] Sean Whalen, “An Introduction to ARP Spoofing”, 2001.