정보보호 시스템 평가 도구 설계

정연서* · 김환국* · 서동일*
*한국전자통신연구원

A Design of Evaluation Tool for Information Security System

Youn-Seo Jeong* . Hwan-Kuk Kim* . Dong-il Seo*
*Dept. of Network Security Research, ETRI
E-mail : jys847@etri.re.kr

요 약

컴퓨터와 네트워크 기술이 급속도로 발전하고 있다. 시간이 흐를수록 다양한 해킹 수법들이 발생하고 있으며, 이에 따라 사람들의 보안에 대한 관심이 높아지고 있다. 네트워크보안 시스템들은 네트워크에 많이 설치되어 사용되고 있다. 그러나, 이러한 보안시스템들을 평가할 수 있는 객관적인 성능평가 체계가 정립되어 있지 않아 제품선정에 어려움을 겪고 있다. 본 논문에서는 침입차단시스템과 침입탐지시스템, 침입방지시스템 등의 네트워크 보안제품들의 기능과 성능을 시험할 수 있는 시험도구를 설계하였다.

ABSTRACT

Computing and Networking technologies are rapidly developed. A lot of hacking events are occurring. As a result, people have a interesting for security in these days. Network security systems have come to be widely used in our networks. But, objective testing method to evaluate network security system is not established. Therefore we have difficulties that select a system. In this paper, we investigate evaluation methods for network security systems(Firewall, IDS, IPS etc.) and, design a evaluation tool for network security systems.

키워드
네트워크 보안, 시험도구, 해킹

I. 서 론

인터넷이 발전되고 확대되어감에 따라 보안장비의 종류와 제품의 수가 늘어나게 되었다. 그러나 이러한 제품들의 기능과 성능을 평가하는 기준이 마련되어 있지 않고 그 측정 방법도 개발사에 따라 다양하게 이루어지고 있어 장비의 선택시 많은 어려움을 겪고 있다. 이에 본 논문에서는 침입차단시스템(방화벽), 침입탐지시스템(IDS), 침입방어시스템(IPS) 등과 같은 네트워크보안제품들을 평가 할 수 있는 시험 도구를 분석하고 설계하고자 한다.

II장에서 현재 보안제품의 평가방법들에 대해서 기술하고, III장에서 도구 개발에 필요한 시험항목들을 분석하고, 평가 도구를 설계한다. 그리고, 마지막으로 IV장에서 결론을 맺는다.

II. 네트워크 보안장비 평가 체계[3][4]

1. 국내의 정보보호시스템 평가체계

우리나라에서는 정보의 안전한 유통을 위하여 정보보호에 필요한 시책의 수립과 시행을 통하여 건전한 지식정보화 사회의 발전과 정보화의 역기능을 최소화하기 위한 취지를 포함하는 정보화촉진기본법(법률 제 5669호,'99. 1개정. '95. 8 제정)이 제정되었다. 이 법률의 시행을 위한 시행령(대통령령 제 16,458호, '99.6) 제 15조(한국정보보호진흥원의 업무등)와 제 16조(정보보호시스템의 보완등)에서는 정보 시스템의 안전 운영에 필요한 보안요구수준에 상응하고 신뢰성 있는 정보보호시스템 보급 확대를 도모하고 정보보호시스템의 성능과 신뢰도에 대한 평가기준을 제공하여 이용자의 인지

도 및 선택상의편익을 향상시키기 위하여 관련 기술 기준에 대한합치여부 평가 또는 인증 업무를 한국정보보호진흥원(KISA)이 수행하도록 하고 있다. 이에 따라, 정보통신망 침입차단시스템 평가가지침서(정보통신부고시 제 1998-20호('98. 2. 23))를 운영하여 오다가 침입차단시스템을 포함한 정보통신망에 사용하는 정보보호시스템 평가·인증지침(정보통신부고시 제 2000-15 호, 2000.2)으로 개정하여 운영하여 오고 있다. 이의 세부 기술 기준으로서는 정보통신망 침입차단시스템 평가기준(2000. 2 개정), 정보통신망 침입탐지시스템 평가기준(2000. 7)이 고시, 운영되고 있다. 정보보호시스템의 평가·인증지침에서는 평가대상 제품에 대하여 주로 보안 기능과 보증에 관한 시험을 하여 그 결과를 인증하게 된다. 그러나, 이 지침에서는 정보보호시스템에서 정보보호기능의 구현과 관련하여 해당 표준에 대한 적합성 시험은 별도의 조항으로 규정하지 않고 있다.

최근에는 정보통신부는 올해부터 본격적으로 국제공통평가 기준(CC)에 따른 평가가 시행됨에 따라 앞으로 국내 평가체계가 급속히 CC 환경으로 전환될 것으로 보고 정보보호 제품에 대한 평가체계를 이에 맞게 재정비할 계획으로 있다.

2. 정보보호 성능평가 체계의 필요성

현재 정보보호 장비의 성능을 측정하는 방법과 관련해서는 이렇다할 표준이 확립되어 있지 못하다. 정보보호에 대한 인식이 확산되면서 정보보호 제품의 수요가 늘고 있으나 객관적인 성능평가 체계가 정립되어 있지 않아, 업체의 제시 자료에 의존하거나 자체의 BMT를 실시하여 제품을 선정하고 있는 현실이다. 몇몇 사설 테스트 기관에서 자체의 시험 방법과 기준에 의해 제품들의 성능 비교 시험을 한 후 이 결과를 배포하는 곳도 있다. 그리고, 정보보호 제품에 대한 '성능'의 개념조차 각 회사들이 이야기하고 있는 기준이 모호하고 정립되어 있지 않으며, 네트워크의 성능 측정 장비를 이용한 측정과 기능 확인 정도의 수준에서 정보보호 제품의 시험을 시행하고 있어 정보보호 제품의 시험을 위한 전용툴과 장비의 개발이 필요하다.

그 동안 국내에서는 정보보호 제품에 대한 평가는 국가정보원이 주관하는 보안성 평가가 주를 이뤄왔다. 하지만 국정원의 보안성 평가와 성능평가는 개념이 다르다. 오히려 성능과 보안성은 반비례한다고 볼 수 있다. 따라서 보안성 평가와는 별도로 제품의 성능을 객관적으로 평가할 수 있는 체계마련이 필요하다. 국내에서는 현재 TTA가 방화벽과 VPN에 대해 시험인증서비스를 제공하고 있으나 외국의 경우는 마이어컴(Miercom)이나 톨리(Tolly)·익사(ICSA)·NSTL 같은 민간 기관이 맡고 있다. 국내에는 이 같은 평가인증 기관이 없어 정보보호 업체들은 주로 ICSA, 톨리 등의 해외 사설 기관에서 평가받아 인증을 획득하거나 성능 시험을 의뢰하고 있다.

3. 보안장비 평가방법

본 논문에서는 네트워크 보안장비들에 관하여 분석하고 바이러스 관련 제품이나 인증, 암호화 제품들은 다루지 않기로 한다. 다음에서는 대표적인 네트워크 보안장비들인 침입탐지시스템, 침입차단시스템, 침입방어시스템의 일반적인 시험방법에 대하여 조사 분석하였다.

3.1 침입탐지시스템

IDS 제품의 평가에 관한 연구는 오래전부터 지속적으로 이루어져 왔다. 1993년부터 미국 NSA에서 연구를 시작하여 1998년 이후에는 DARPA 주도하에 MIT, AFRL(Air Force Research Lab.)에서 각각 online, offline 평가 방법을 연구수행하였다. 이외에도 각 IDS 제작사나 NSS, Nettwork Computing, Tooly 등의 보안 관련 기관 등에서 관련 연구와 보고서를 발표하고 있다. 국내의 경우 2000년에 들어서 침입탐지시스템의 보안기능 평가를 위해 "정보통신망 침입탐지시스템 평가기준"을 고시하고 제품평가에 이를 반영하고 있다. 침입탐지시스템의 보편적인 측정방법은 다음 그림과 같이 설치되고 진행이 이루어지고 있다. 시험을 평가하는 기관에서는 특정 공격코드를 선정해서 이를 시스템이 정확하게 탐지하는지의 여부와 트래픽 발생기를 이용하여 과다한 패킷을 발생시키고 이러한 환경 하에서 검출되는 공격의 수를 측정하여 시스템의 기능과 성능을 측정하게 된다.

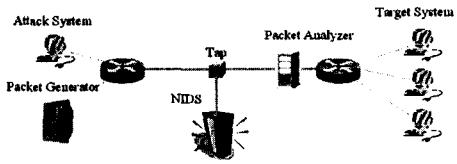

그림 1. 침입탐지시스템 시험 구성도[2]

3.2 침입차단시스템

침입차단시스템은 패킷이 통과하는 위치에 설치되어 패킷의 통과 여부를 결정하는 시스템으로 보안정책을 적용시킨 후 얼마나 많은 양의 패킷을 시간내에 처리할 수 있는지의 패킷 처리 성능 측정 여부가 중요한 항목이다.

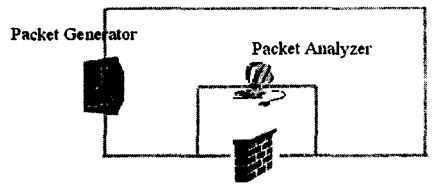

그림 2. 침입차단시스템 시험 구성도[5]

위 그림 2와 같이 패킷발생기에서 패킷을 발생시켜 시스템에서 처리되는 패킷을 분석하는 구성으로 평가가 이루어지고 있다.

3.3 침입방어시스템

IPS라고 알려진 침입방어시스템은 침입차단시스템과 침입탐지시스템을 결합하여 놓은 형태의 새로운 네트워크보안제품으로 일반 방화벽과는 달리 3 Layer에서 패킷을 필터링하는 것이 아니라 7 Layer까지 패킷을 분석하여 유해 패킷으로 판단될 경우 침입탐지시스템과는 달리 이를 폐기하여 내부 네트워크로 통과시키지 않는 시스템이다. 침입탐지시스템의 시험 구성과 유사하며 시스템 뒷단에 패킷분석기를 설치하여 패킷의 처리 상태를 분석하게 된다.

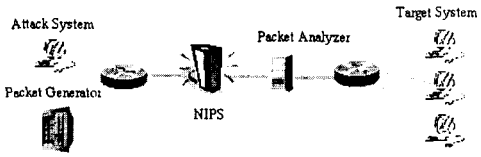

그림 3. 침입방어시스템 평가 구성도[2]

III. 시험 도구 설계

1. 요구사항

네트워크 보안제품을 평가하기 위해서는 다양한 취약점을 공격할 수 있는 공격기능과 주어진 시간에 얼마나 많은 양의 패킷을 처리할 수 있는지의 처리 성능 측정 기능이 요구된다.

기존의 시스템 평가 자료들을 분석하여 필요 기능을 정리해 보면 다음과 같다[1][2][5].

- 취약점 분석 기능
  대상 시스템의 자체 안정성을 측정하기 위하여 취약성을 찾아내는 기능이다.
- 취약점 공격 기능
  기존에 알려진 시그너쳐 기반의 다양한 공격들과 아노말리 공격, 우회공격, False positive(침입이 아닌데도 침입으로 판단하여 오경보 발생) 등을 시험하기 위한 기능이다.
- 트래픽 발생 기능
  시스템의 패킷 처리 성능을 시험하기 위해 다양한 크기의 패킷을 발생시키는 기능이다.

2. 구조

본 논문에서 제안하는 시스템은 실제 공격코드를 생성하고 트래픽을 발생시키게 되는 에이전트와 다수의 이들을 관리할 수 있는 마스터로 구성된다.

그림 4. 시험도구 구조

먼저, 공격유형관리 블록에서는 많은 수의 공격코드들 중에서 최근 빈도가 잦은 코드들이나 특정 공격 유형들을 선택하여 시험할 수 있으며, False Positive를 시험하기 위해서 가짜공격도 발생시키게 된다. 그리고, 트래픽 유형관리 부분에서는 트래픽발생시 좀 더 실제 환경에 접근될 수 있도록 다양한 크기의 패킷을 혼합하여 생성되도록 설계하였다. 또, 보안 시스템을 우회하는 공격들을 시도할 수 있도록 설계하였다. 마스터에서 이와 같이 공격 유형을 선택하게 되면 분산된 여러 에이전트들에서는 실제 공격과 트래픽 발생을 마스터의 동작 지시에 따라 시행하게 된다. 그리고 마스터의 모니터링 블록에서는 각 에이전트들로부터 수집된 정보로 현재 상태를 모니터링하고 이를 화면에 실시간으로 보여주게 된다.

아래 그림 5에 시험환경 구성도를 나타내었다.

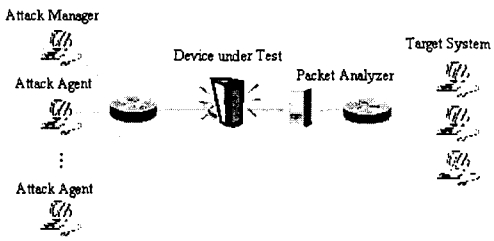

그림 5. 시험환경 구성도

3. 공격 시나리오[2]

대상 시스템에 대한 공격 분류는 크게 다음과 같다. 시스템의 종류에 맞추어 상세한 공격방법을 선정하여 시험하면 된다.

침입탐지시스템은 (1), (2), (3)의 항목들을 이용하며, 침입방어시스템의 경우는 (1), (2), (3), (4)의 항목들을 이용한다. 침입차단시스템의 경우는 (2), (3), (4)의 항목을 조합하여 시험 시나리오를 구성하면 된다.

(1) 침입탐지

1.1 attack recognition

1.2 Resistance To False Positive

(2) 패킷처리성능

2.1 UDP Traffic To Random Valid Ports

2.2 HTTP Traffic with No Transaction Delay
2.3 HTTP Traffic with Transaction Delay
2.4 Protocol Mix Traffic
2.5 Real World Traffic

(3) 우회공격

3.1 Packet Fragmentation
3.2 URL Obfuscation
3.3 Miscellaneous Evasion Techniques

(4) Stateful Operation Test

4.1 Attack Replay
4.2 Simultaneous Open Connections

IV. 결 론

본 논문에서는 네트워크 보안제품의 기능과 성능을 시험할 수 있는 도구를 설계하고 제안하였다. 차후, 상세한 시험 시나리오를 만들고 도구를 이용하여 실제 시험을 수행할 예정이다. 여기서 나온 결과를 분석하고 이를 토대로 도구의 기능을 추가시켜 나갈 예정이다.

참고 문헌

[1] Gigabit Intrusion Detection Systems Group Test(Edition2), NSS Group Report, 2003. 7
[2] NTP ATTACKS, Network Computing, 2004. 9
[3] 전자신문 " 정보보호제품 성능평가체계 마련 급하다" - 2002. 8
[4] 정보보호21 " 정보보호솔루션 성능평가 활성화되나" - 2003. 7
[5] Tolly Test summary (secuiWALL vs Netscreen-100), 2003. 3