네트워크 보안성능 및 보안성 평가에 관한 연구

황선명* · 정연서** · 서동일**
*대전대학교 컴퓨터공학과
**한국전자통신연구원 네트워크보안연구부

A Study on Evaluation for Network Security Performance and Property

Sun-Myung Hwang* · Youn-Seo Jung**· Dong-il Seo**
*Dept of Computer Engineering, Daejeon University
**Network Security Department, ETRI
E-mail : sunhwang@dju.ac.kr

요 약

컴퓨터 네트워크 기술의 발달은 기업 또는 단체들의 사업 환경을 변화시키고 그 범위를 점점 넓혀나가고 있다. 인터넷을 이용한 업무 시스템의 응용은 보다 편리한 환경을 제공하지만 이에 앞서 데이터들이나 장비들의 안전성을 고려하지 않는다면 컴퓨터 네트워크의 수많은 보안 위험 요소에 직접적으로 노출되어진다. 본 논문에서는 이러한 데이터들이나 장비들의 안전성을 위해 네트워크의 보안성과 보안성능을 측정할 수 있는 방법들을 제시하고자 한다.

ABSTRACT

The rapid progress of computer networking technology is changing the environment of today's business and its influence is spreading out widely. Although the practical use of business system using the Internet technology is providing easy going infrastructures, many security problems of data or equipment in the open field will be exposed if we do not give serious considerations to their securities. In this paper, we suggest advanced methods to measure the network security capability with considerations for the security of data or equipments.

Ⅰ. 서 론[1)]

인터넷과 컴퓨터 기술 발전은 지역적이나 시간적 제약이 있었던 각 조직의 사업 환경을 점차 변화시키고 있다. 선진국 정부기관으로부터 기업, 금융, 교육 등의 조직들이 인터넷 환경을 기반으로 그 응용범위를 확대시키고 있다.

특히 정보통신, 금융, 에너지, 운송, 전자정부 등 사회의 기반구조의 인터넷 의존도가 높아지고 있다.

최근 몇 년 사이 해킹 및 바이러스에 의한 피해 사례가 점점 증가하는 추세에 있으며 2003년 초부터 발생한 MS SQL 보안 취약점을 이용한 Slammer 웜 공격으로 인한 전 세계적인 인터넷 장애 사건, 국내 ADSL 인터넷 가입자망 장애 사건, 무선 LAN 장애사건 등 사이버 공격에 의한 인터넷 마비 또는 장애 사고가 점차 대형화되고 있다. 이와 같은 대형화된 네트워크 장애가 얼마나 큰 사회 문제를 야기 하는지를 실감하게 되었다[1].

이러한 일련의 사건들로 인하여 네트워크와 컴퓨터에 대한 보안과 보안성능에 대하여 문제가 꾸준히 제시가 되고 있지만 이에 대한 구체적인 평가 방법에 대한 표준이 없기 때문에 컴퓨터 네트워크에 보안성과 보안성능을 평가하기가 어려운 실정이다.

1) 본 연구는 한국전자통신연구원 "네트워크 보안성능 및 보안성 평가에 관한 연구" 지원으로 수행되었음

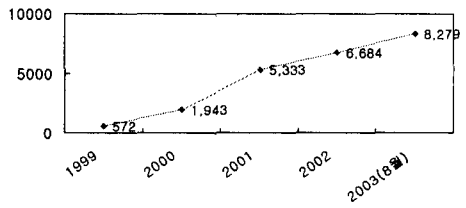

그림 1. 해킹피해 규모

본 연구에서는 컴퓨터 네트워크에 대한 보안성과 네트워크 장비들의 성능을 평가 할 수 있는 장비들의 보안 성능에 관한 평가 방법에 대하여 연구하였다.

II. 관련 연구기관 및 표준 현황

우선 ISO/IEC 9126과 ISO/IEC 9646은 시험 기관은 아니지만 시험에 사용할 수 있는 품질 요소들에 관련된 국제 표준, 네트워크 제품의 적합성 시험에 대한 국제 표준이다.

Tolly Group은 미국의 사설 테스트 기관으로서 다양한 제품에 대해 시험 인증을 하고 있으며 주로 성능 시험과 인증을 담당하고 있다[2][3]. ICSA는 미국의 사설 테스트 기관으로서 기능시험과 상호운영성을 시험하고 있다[4]. BSI는 독일의 국가 기관이다. 주로 정보보호제품의 보안성 평가 및 인증 부분을 담당 하고 있다[5]. 국내에는 TTA NETC (Network Test Center)가 있는데 여기서는 네트워크 제품들을 중점으로 시험하고 있으며, Tolly Group과 상호 제휴하여 기능성 위주의 시험을 하고 있다[6]. 표 1. 에 관련 기관들에 대해 정리해 보았다.

표 1. 시험 기관별 시험 현황

기관	시험분류	시험대상	비고
ISO/IEC 9126	기능성 신뢰성 사용성 효율성 유지보수성 이식성	소프트웨어 제품	기능성 : 적합성, 상호운용성, 보안성, 정확성, 준수성의 부특성으로 구성
	일관성 생산성	제조프로세스	
ISO/IEC 9646	기본상호접속 능력 동작 적합성 분석	네트워크제품	네트워크 제품의 적합성 시험 방법론
JITC	표준 적합성	IT 제품	국방성 C4I
(미국)	개발 상호운용성 운영 검증		시스템 구축용
NIST (미국)	암호안정성	암호모듈	CMVP 운영
	상호운용성	PKI, S/MIME, IPSec	Cerberus, PlutoPlus, IPSec-WIT
	보안성	Firewall, IDS, VPN	NIAP 운영
ICSA (미국)	기능 상호운영성	정보보호 제품 대상 (IDS, PKI, Firewall 암호 제품)	
Tolly (미국)	성능 상호운영성	네트워크제품	
BSI (독일)	보안성 인증	정보보호제품	
TTA-NETC (한국)	적합성 상호운영성 성능 기능	네트워크제품	기능시험과 성능시험 위주 Tolly Group과 상호제휴

표 1. 을 보면 알 수 있듯이 각 시험기관들 마다 시험 하는 항목이 다르며 시험 대상도 다양하다는 사실을 알 수가 있다. 특히 보안성과 보안성능을 시험하는 기관들조차 객관적 평가가 아닌 평가자의 주관적인 판단을 기초로 하고 있어 객관적으로 평가 결과를 판단할 수 없다.

III. 보안성 평가

일반적인 보안성 평가 절차는 다음의 그림 2. 와 같다.

본 논문에서는 연구 범위는 시험대상을 선정하고 시험 기준을 확정하고 시험 방법을 결정하는 세 부분만으로 할 것이다.

그림 2. 보안성 평가 절차

보안성 평가에 관한 일반적 평가 요구사항들을

정리해 보면 다음과 같다.

- 외부로부터 내부로의 불법적인 접근은 원칙적으로 차단
- 모든 응용 및 시스템 사용시 접근통제 실시
- 실시간 모니터링을 통한 상황 파악 및 대처
- 주기적인 보안 점검 실시
- 개인용 컴퓨터의 보안 강화
- 관리적 대책

위의 사항들을 기준으로 보안성을 평가할 대상을 선정하고 각 대상별로 평가할 항목들에 대한 평가 방법들을 제시할 것이다.

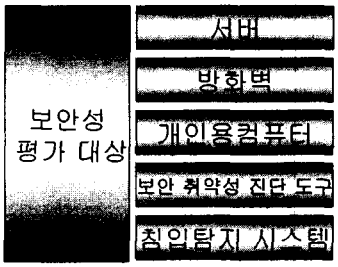

그림 3. 보안성 평가 대상

보안성 평가 대상들의 평가할 항목들을 대략적으로 표 2. 에 나열하였다.

표 2. 보안성 평가 대상의 항목

보안성 평가 대상	대상별 항목	비고
서버	취약성 관리	서버에서 발견될 수 있는 취약점들에 관련된 사항을 점검
	사용자 계정관리	서버의 사용자 계정에 접근 권한 및 보안 설정들을 점검
	패스워드 보안	패드워드의 보안 설정들을 점검
방화벽	보안정책	방화벽의 보안정책이 효율적으로 이루어지는지 점검
	로깅	보안에 필요한 로깅 데이터들이 정확하게 기록되어지는지 점검
	운영	방화벽 운영기능의 사용성들을 점검
	필터링	패킷 필터링에 관련된 규칙들에 설정들을 점검
개인용 컴퓨터	사용자접근 통제	PC를 사용할 수 있는 사용자들 관리하여 접근
		제어 및 통제의 가능여부 점검
	해킹프로그램 진단 및 삭제	PC에 설치된 해킹, 바이러스, 웜 등을 진단하고 치료할 수 있는지를 점검
	공유폴더 정보	공유폴더의 정보 및 로깅 데이터에 대한 기록에 대한 점검
	환경설정	PC보안에 관련된 사항들을 설정할 수 있는가를 점검
보안 취약성 진단도구	사용의용이성	진단도구의 사용성에 관련된 사항을 점검
	사용자접근 통제	사용 허가가 있는 사람만이 접근제 및 통제가 가능하게 관리 되어지는지를 점검
	원격진단기능	원격으로 보안취약성을 진단 가능한지의 여부를 점검
	다양한 보안 취약성 진단	다양한 보안 취약부분을 진단할 수 있는지를 점검
	암호화 기능	점검 결과 데이터를 안전하게 관리자에게 보낼 수 있는지 점검
	진단항목선택	진단할 항목을 선택하고 그룹으로 관리할 수 있는지 점검
	사용자관리	도구를 사용할 수 있는 사용자를 관리할 수 잇는지를 점검
침입탐지 시스템	보안위반분석	보안에 위배되는 사항들을 분석할 수 있는지를 점검
	보안감사대응	보안 위반 발생시에 이에 대응하고 경고가 가능한지 점검
	신변확인	사용자에 대한 인증과 접근제어 및 통제가 가능한지 점검
	보안기록	침입탐지 관련 기록들을 분류 저장이 가능한지 점검
	데이터보호	탐지 시스템에서 저장된 데이터의 안정서에 대해 점검
	보안정책	보안정책의 추가, 수정, 삭제 가능 여부를 점검
	자동업데이트	최신의 침입탐지 패턴들로 업데이트 가능한지 점검

보안성 평가 대상에 각 평가 항목들의 세부 항목들은 일반적인 체크리스트의 성격을 가지고 있다. 이 체크리스트의 만족정도로 평가 대상의 보안성 평가의 지표로 삼을 수 있다.

Ⅳ. 보안성능 평가

성능 시험이란 작업처리량(throughput), 개별적 응답속도 그리고 가용성들을 포함하는 컴퓨터 시스템의 총체적인 효율성을 가리킨다[6].

특히 파이어월의 경우 DoS (Denial of Service : 서버나 라우터 등의 리소스를 독점하거나 모두사용, 파괴함으로써 다른 사용자들이 정상적인 서비스를 제공하지 못하게 하거나 운영이 불가능하게 만드는 공격방법[6])와 같은 공격방법에 대응할 수 있는가에 대한 성능을 평가함으로써 장비 자체의 보안 성능을 평가할 수 있는 지표로 삼고 있다.

아래의 그림 4. 은 파이어월의 보안성능을 평가 방법을 그림으로 표현해 보았다. 위의 그림에서 알 수 있듯이 파이어월의 트래픽과 세션에 대한 성능을 측정 할 수 있으며 DoS에 대한 공격의 필터링 능력을 측정할 수 있다.

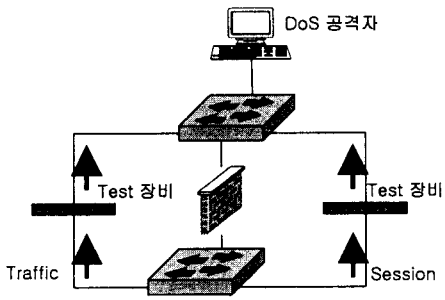

그림 4. 파이어월의 보안성능 평가 방법

Ⅴ. 결론 및 향후 연구과제

과거와 달리 점점 더 많은 업무들이 네트워크를 이용한 방법을 적용하기 때문에 점점 네트워크의 보안성과 보안성능의 중요성은 갈수록 높아만 지고 있다. 하지만 이러한 보안성과 보안성능을 평가하는데 있어 어떤 정해진 표준이 있는 것이 아니기 때문에 관련 연구기관 마다 평가하는 방법들이 상이하다. 또한 보안성 평가 방법의 경우에는 평가 자체를 객관적인 근거에 의한 평가 방법이 아닌 평가자의 주관적 판단을 기준으로 하기 때문에 객관적인 평가 결과를 얻어낼 수 없다.

본 논문에서는 이러한 보안성에 대해 적용할 평가 대상과 각 대상별 평가해야 할 평가 항목을 정의하였다. 또한 보안성능 평가에 있어서는 파이어월의 트래픽이나 세션에 대한 성능과 DoS 공격에 대한 필터링 능력을 측정할 수 있는 방법을 제시하였다.

향후 연구 방향으로는 이렇게 정의된 항목들의 평가 결과에 대한 객관적 판단 기준을 제시하여야 하고 보안성능에 있어서 파이어월 뿐만이 아닌 라우터나 스위치 등과 같은 다른 장비들의 성능까지 측정할 수 있는 평가 방법 그리고 방법을 직접 시험해 봄으로써 객관적으로 장비를 평가할 수 있는 기준을 제시해야 할 것이다.

참고 문헌

[1] 2003년 8월 해킹바이러스 통계 및 분석 월보. 한국정보보호진흥원. 8. 2003.
[2] Tolly 보고서, "NetScreen Technologies Inc. Test summary", 2001.
[3] http://www.tolly.com
[4] http://www.icsalabs.com
[5] http://www.bsi.de
[6] http://www.tta.or.kr