네트워크 보안성능 및 보안성 평가 방법에 관한 연구

정지환, 김상영, 황선명°
대전대학교 컴퓨터공학과

A Study on Evaluation Methodology for Security Performance and Property

JiHwan Jung, SangYoung Kim, SunMyung Hwang°
Dept. of Computer Engineering, Daejeon Univ.

요 약

인터넷의 발달로 네트워크 업무가 점점 더 많이 도입이 됨으로써 네트워크 상에 노출되어 있는 데이터와 시스템들의 보안은 중대한 문제로 대두되기 시작했다. 그러나 장비나 소프트웨어 등의 보안성과 보안성능 평가에 대한 기준이 명확하지 않아 이들의 객관적인 평가에 많은 어려움이 따르고 있다. 본 논문에서는 관련 연구 기관들의 평가 방법들을 분석하여 이들을 객관적으로 평가 할 수 있는 방법을 제시하고자 한다.

1. 서론

인터넷이 보편화 되면서 많은 조직들의 업무를 확대시켜 네트워크에 좀더 의존적이게 되어가고 있다. 이런 변화는 업무의 효율성과 편리성을 높이는 반면에 중요한 데이터들이 네트워크에 노출되는 위험성을 안게 되었다. 또한 업무에 많은 부하가 걸릴 경우에는 업무가 제대로 이루어지지 않는 부작용들이 속속들이 들어 나고 있다. 최근에는 이러한 약점을 이용하여 네트워크상에 드러난 중요한 데이터들과 장비들을 공격하는 해킹과 바이러스, 웜 등이 점점 늘어나고 있는 추세이다.

이와 같은 일들로 인하여 네트워크 상에 드러난 중요한 데이터들과 장비들을 외부의 공격으로부터 보호하는 네트워크 보안에 대한 사항들이 대두되고 있다. 그러나 이러한 네트워크 보안에 관련된 사항들을 객관적으로 평가할 수 있는 방법이 제시되고 있지 않은 상황이기 때문에 각 업체나 기관이 제시하는 방법들로 평가 할 수 밖에 없다. 이는 평가 하고자 하는 조직들의 보안 등급이 객관적으로 결정될 수 없다는 것이다.

본 연구에서는 이러한 보안 평가 방법의 문제점을 해결하고자 네트워크 보안성과 네트워크 보안 성능에 대한 객관적인 평가 방법을 제시하고자 한다.

2. 국제 표준 및 연구기관 동향

아래의 표 1. 에서 보는 바와같이 ISO/IEC 9126과 ISO/9646은 시험 기관은 아니지만 시험에 사용할 수 있는 품질 요소들에 관련된 국제 표준, 네트워크 제품의 적합성 시험에 대한 국제 표준이다.

본 연구는 한국과학재단 목적기초연구(R01-2001-000-00343-0(2003))지원으로 수행되었음

표1. 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	제조 프로세스	
ISO/IEC 9646	기본상호접속 능력 동작 적합성 분석	네트워크제품	네트워크 제품의 적합성 시험 방법론
JIST (미국)	표준 적합성 개발 상호운용성 운영 검증	IT 제품	국방성 C4I 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 상호운용성	정보보호 제품 대상(IDS, PKI, Firewall 암호 제품)	
Tolly (미국)	성능 상호운영성	네트워크제품	
BSI (독일)	보안성 인증	정보보호제품	
TTA-NECT (한국)	적합성 상호운용성 성능 기능	네트워크제품	기능시험과 성능시험 위주 Tolly Group과 상호제휴

그 외에 다른 기관들을 모두 네트워크 장비에 대한 인증들을 하고 있지만 네트워크 보안성에 관련된 부분을 인증하는 기관은 NIST와 BSI 뿐이다. 이는 네트워크 보안성에 대한 기준을 세워놓고 인증을 하고 있는 기관이 거의 없다는 사실을 보여주고 있으며 BSI 같은 경우 보안성에 관련된 인증을 하고 있지만 문제는 보안성에 대한 평가 기준이 객관적이지 않은 주관적인 판단에 의거하여 평가 한다는 점이다.

3. 보안성 평가 절차와 대상

일반적으로 사용되어 지고 있는 평가 절차는 다음의 그림 1. 과 같다. 그림에서 알 수 있듯이 본 연구에서 접근하는 부분은 시험 대상을 선정하고 시험 기준을 확정하고 시험 방법을 결정하는 부분만을 연구 대상으로 삼고 있다.

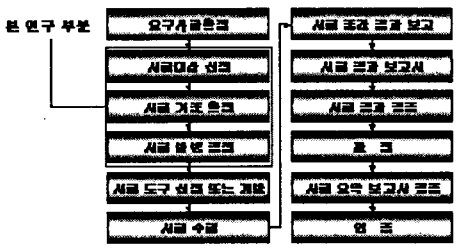

그림 1. 보안성 평가 절차

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.

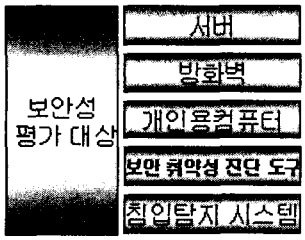

그림 2. 보안성 평가 대상

평가 대상으로는 서버와 방화벽, 개인PC, 보안 취약성 진단 도구, 침입탐지 시스템의 5가지 부분으로 분류 하였고 이들에 대한 상세한 체크리스트를 두어 이를 체크하여 평가 할 수 있게 하였다.

또한 보안 성능 평가는 라우터, 스위치, 파이어월의 세가지를 평가 대상으로 하여 장비에 대한 성능 위주의 평가를 할 수 있는 테스트 방법을 결정할 것이다.

3. 네트워크 보안성 평가 세부사항

3.1 서버

- 취약성 관리 : 네트워크 상으로 공격 가능한 서버의 취약성들에 관해서 평가
- 사용자 계정 관리 : 서버에 접속할 수 있는 권한을 가지고 있는 사용자들의 계정들에 대한 관리가 제대로 이루어지고 있는지를 평가
- 패스워드 보안 : 사용자들의 패스워드가 암호화 되어 보관 되어지고 사용자들 또는 관리자들의 암호가 유출되어 있는지 들을 평가

3.2 방화벽

- ⓐ 보안정책 : 방화벽의 보안 정책들이 외부로부터 공격 가능한 모든 부분을 방어하고 있는지 또는 감시할 수 있는지 정책이 효율적으로 이루어져 있는지에 대한 평가
- ⓑ 로깅 : 보안에 필요한 로깅 데이터들이 정확하게 기록되어지고 있고 이들을 관리하는지에 대한 평가
- ⓒ 운영 : 방화벽 사용에 대한 운영 기능의 사용성들을 평가
- ⓓ 필터링 : 패킷 필터링에 관련된 규칙들의 설정이 제대로 이루어지는지 또한 효율적으로 규칙을 설정하였는지에 대한 평가

3.3 개인용 컴퓨터

- ⓐ 사용자 접근통제 : 개인용 컴퓨터들의 사용자들에 대한 접근 통제가 이루어지고 있는지에 대한 평가
- ⓑ 해킹 프로그램 진단 및 삭제
- ⓒ 공유폴더 정보 : 공유폴더의 정보 및 로깅 데이터에 대한 기록들이 이루어지고 있는지를 평가

3.4 보안 취약성 진단도구

- ⓐ 사용의 용이성
- ⓑ 사용자 접근통제 : 사용 허가가 있는 사용자에게만 접근 및 통제가 가능하게 관리되어지고 있는지를 평가
- ⓒ 진단 취약성의 다양성 : 다양한 보안 취약부분을 진단할 수 있는지를 평가
- ⓓ 원격진단 기능 : 정검 결과를 원격지의 관리자에게 보낼 수 있는지 또한 안전하게 관리자에게 결과 데이터를 보낼 수 있는지를 평가

3.5 침입탐지 시스템

- ⓐ 보안위반분석 : 보안에 위배되는 사항들을

자동으로 분석할 수 있는지를 평가

- 보안감사대응 : 보안 위반 발생시에 이에 대응하고 관리자에게 경고가 가능한지에 대해 평가
- 보안기록 : 침입탐지 관련 기록들을 분류하고 저장하여 관리되어 질 수 있는가를 평가
- 데이터보호 : 저장된 데이터가 안전하게 유지될 수 있는지에 대해 평가
- 보안정책 : 보안정책의 추가, 수정, 삭제가 가능한지에 대해 평가
- 자동업데이트 : 최신의 침입탐지 패턴들로 업데이트가 가능한지를 평가

4. 보안 성능평가 방법

성능 시험이란 작업처리량(throughput), 개별적 응답속도 그리고 가용성을 포함하는 컴퓨터 시스템이 총체적인 효율성을 가리킨다. 이러한 성능 시험은 장비가 외부로부터 받을 수 있는 물리적인 공격에 대하여 어느 정도의 한계를 가지고 있는가를 평가할 수 있는 척도를 마련할 수 있다.

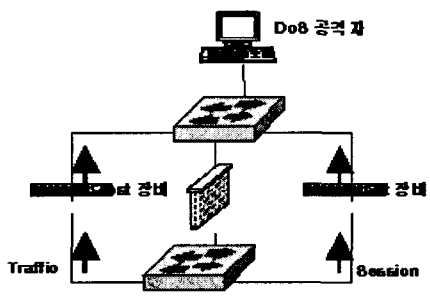

그림 3. 파이어월의 보안성능 평가방법의 예

최근 DoS(Denial of Service : 서버나 라우터 등의 리소스를 독점하거나 모두 사용, 파괴함으로써 다른 사용자들이 정상적인 서비스를 제공하지 못하게 하거나 운영이 불가능하게 만드는 공격방법) 공격에 의한 피해가 잇달아 일어나고 있어 장비의 성능 시험은 장비 자체의 보안 성능을 평가할 수 있는 지표로 사용되어지고 있다.

보안 성능평가의 대상으로는 스위치, 라우터, 파이어월의 세가지 장비에 대한 성능평가를 제시한다.

그림 3. 은 파이어월의 성능 평가를 위한 방법의 예를 들고 있다. 이와 같은 방식을 사용하여 라우터, 파이어월, 스위치가 테스트 장비를 통해 세션과 트래픽을 유발하고 DoS 공격에 대한 필터링 능력에 대한 성능을 측정하고자 한다.

5. 결론 및 향후 연구 과제

국내 외의 시험 기관들의 분석에서 알 수 있듯이 네트워크 보안과 보안성능에 대한 평가에 대한 사항들이 기관들 만다 다 다른 사항들에 대해서 평가한다는 사실을 알 수 있었다. 또한 본문에서 말한 것과 같이 객관적 판단 기준이 없다는 것 또한 사실이다.

본 논문에서는 문제점들을 해결하고자 보안성에 관련된 평가를 평가대상에 여러 개의 평가 세부항목으로 분류하여 체크리스트 형태로 객관적인 판단을 할 수 있는 방안을 제시했다. 또한 장비의 성능 평가 또한 제시하였다.

향후 이에 대한 체크리스트를 정량화 하여 평가 결과를 도출하는 방법과 성능평가 방법을 실제 적용하여 객관적으로 평가할 수 있는 테스트 모델을 적용시켜 객관적인 성능평가의 기준을 잡는 것이 필요하다고 할 수 있다.

[참고문헌]

[1] http://www.tolly.com

[2] http://www.icsalabs.com

[3] http://www.bsi.de

[4] http://www.tta.or.kr