TS 기반의 정보보호수준 평가 방법론 개발에 관한 연구

성 경* · 김석훈**

A Study on the Evaluation Methodology for Information Security Level based on Test Scenarios

Kyung Sung* · Seok-Hun Kim**

요 약

조직의 정보보호 목표를 효율적이고 효과적으로 달성하기 위해서는 조직의 정보보호 수준을 정확히 평가하고 이를 개선시킬 방향을 제시하는 기준이나 평가모델이 필요하다. 또한 이를 위해 부문별 정보보호 수준을 평가하고 개선할 수 있는 평가지표나 기준이 필요하고 우리나라에서 적용 가능한 정보보호 시스템들의 평가방법론이 연구되어야 한다. 본 연구에서는 다양하고 복잡한 네트워크 보안성과 보안성능부분에 초점을 맞추어 네트워크 보안성을 평가하기 위해 필요한 평가 시스템들을 추출하고 이들 각각을 평가할 수 있는 체크리스트와 각 시스템들이 네트워크 보안성에 얼마만큼 기여하는지를 결정하여 네트워크 보안성을 평가할 수 있는 방법을 제시하였다. 또한 네트워크 보안성능을 평가할 수 있는 평가 모델과 테스트 시에 필요한 테스트 시나리오를 제시하였다.

ABSTRACT

It need estimation model who is efficient and estimate correctly organization's information security level to achieve effectively organization's information security target. Also, estimate class information security level for this and need reformable estimation indicator or standard and estimation methodology of information security systems that application is possible should be studied in our country. Therefore many research centers including ISO are preparing the measuring and evaluating method for network quality. This study will represent an evaluating model for network security based on checklist. In addition, we propose an measuring and evaluating method for network performance. The purpose of two studies is to present the evaluating procedure and method for measuring security of network on set workwill be identified and a measuring method and procedure will be proposed.

키워드

Security Level, Network Security, Security Evaluation, Evaluation Method, Control Object

Ⅰ. 서 론

정보기술의 발달과 정보화의 확대로 인하여 국가 및 사회, 개인간의 정보경쟁이 치열해짐에 따라 정보보호의 중요성이 더욱 높아지고 있으며, 이에 정보보호시스템의 사용이 증가되고 있다.

조직의 정보보호 목표를 효율적으로 달성하기 위해서는 조직의 정보보호 수준을 정확히 평가하고 이를 개

* 목원대학교 컴퓨터교육과

** 대전보건대학 멀티미디어과

접수일자 : 2006. 11. 12

선시킬 방향을 제시하는 기준이나 평가모델이 필요하다. 또한 이를 위해 부문별 정보보호 수준을 평가하고 개선할 수 있는 평가 지표나 기준이 필요하고 우리나라에서 적용 가능한 정보보호 시스템들의 평가방법론이 연구되어야 한다.

정보보호시스템 제품은 특성상 일반적인 제품의 시험인증 체계와는 다른 체계를 가진다. 기존에는 네트워크정보보호제품의 보안성에 중점을 두어서 시험이 이루어져 왔다. 이러한 보안성 평가 인증에 사용되는 기준으로는 TCSEC, ITSEC 등을 사용하여 왔고, 점차 공동평가기준(CC)을 사용하는 추세이다[1].

국내 정보보호시스템 평가제도는 검증된 정보보호 시스템을 공급하기 위한 목적으로 운영되고 있지만, 민간분야에서 요구하는 다양한 제품의 평가가 이루어지고 있지 않고, 제품평가에 소요되는 시간과 비용이 많으며, 평가된 제품이 국제적으로 상호인정 되지 않는다는 문제점을 가지고 있고, 이러한 평가들은 정보보호 제품들에 관련된 사항들에 중점을 맞추어 평가가 되어 지고 있을 뿐 이들이 유기적으로 결합되어 있는 네트워크 수준의 보안성 평가나 보안성능에 초점을 맞춘 평가는 제대로 이루어지지 않고 있는 상황이다.

또한 네트워크 보안성에 관련된 평가 방법은 기준조차 잡혀있지 않은 상황이고, 평가가 이루어진다고 하여도 객관적 평가 방법이 아닌 평가자의 주관적인 평가 방법에 의존하고 있으며 네트워크 보안성능 평가는 제품의 성능평가 방법이 보안성능 평가방법이 대체되어 평가 되어 지고 있다[2].

따라서 현재 평가 되어 지고 있는 네트워크 보안성능과 보안성에 관련된 정확한 정의와 이를 평가할 수 있는 객관적인 평가 방법을 제시함으로써 보다 정확한 평가를 내릴 수 있는 연구가 필요하다[8,9].

본 논문의 구성은 2장에서는 정보보호수준 평가 방법론을 위한 정보보호 수준평가의 개념과 정보보호 지표 및 성숙모형과 정보보호시스템 보안 요구사항에 대하여 조사 및 분석한 결과를 보인다. 3장에서는 정보보호 수준 평가 성능시험 과정과 메커니즘을 제시하며, 4장에서 시험 시나리오 기반의 정보보호 수준 평가 방법론인 성능시험 지표와 성능시험 구성, 시험 시나리오를 적용한 결과를 보이고 성능시험 기준평가 결과를 분석한 후 끝으로 결론을 맺는다.

II. 관련 연구

2.1 정보보호 수준평가

기업의 정보보호수준을 종합적이고 체계적으로 측정할 수 있는 평가체계는 아직까지 없지만 제품의 기술적 수준을 측정하기 위해서 TCSEC(Tru-sted Computer System Evaluation Criteria), IT-SEC(Information Technology Security Criteria), CC(Common Criteria), BS7799 등의 평가체계가 사용되어져 왔으며, 사)기업정보화지원센터 에서는 기업정보화수준평가의 일부로서 정보보호수준지표가 활용되고 있다.

TCSEC, ITSEC, CC는 각국의 보안 제품 및 시스템 평가를 위한 평가체계로 기본적으로 제품이라는 기술적 부분에만 한정되어 평가를 하는 반면에 BS7799는 영국의 상무성 주관으로 '정보보안관리 실무규범'이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용되도록 개발되어진 권고안의 성격을 지니고 있다[3,4]. 정보화수준평가의 일부로 측정되는 정보보호수준지표는 평가지표가 10개밖에 안되어 전반적인 정보보호 수준을 측정할 수는 없지만 개략적으로 기업의 정보보호 수준을 평가하고 있다.

정보보호 수준평가에 관련된 기존 연구를 정리하면 표 1과 같다.

표 1. 정보보호 수준평가 관련연구
Table. 1 Information Security Level Methodology

	내 용
TCSEC	• 미국에서 개발된 세계 최초의 평가기준 • 미국방성 컴퓨터 시스템의 보안성을 평가하기 위하여 개발 • 정보보호의 요소 중 기밀성만을 강조하여 민간기업에는 적용하기가 어려움
ITSEC	• 유럽국가들이 보안성 기준을 통합하기 위하여 개발된 세계 최초의 국제 통합기준 • 단일 기준으로 모든 정보보호제품을 평가 • 보안보증 부분만으로 제품에 대한 평가를 수행
CC	• CTCPEC, TC, TCSEC, ITSEC의 단일 평가 기준으로 국제공통 평가기준
BS7799	• 정보보안을 유지하고 구현하는 관리자를 위한 보편적인 기준 • 기업이 선택해야 하는 지침과 권고안의 성격 지님 • 평가대상이 IT 보안에 집중되어 주로 높은 수준에 정보보호 기준을 제공
정보보호 수준지표	• 사)기업정보화지원센터에서 매년 정보화수준평가의 일환으로 정보보호 투자정도, 정보보호 제도 및 운영, 정보보호시스템 구축정도를 평가

2.2 정보보호 지표

정보보호 지표에 대한 연구는 크게 정보화지표와 BS7799로 관련된 연구로 나누어진다. 한국전산원은 매년 정보화를 구성하는 정보설비, 정보이용, 정보투자분야의 각 측면에 대해 정의에 맞는 통계 항목을 측정하여 효과적인 지표를 산출하고 있으며, BS7799는 조직이 효과적인 정보보호관리 체계를 수립, 수행, 감시하기 위한 종합적인 가이드라인을 제공하고 조직 상호간의 신뢰성 있는 거래를 위한 기반을 제공하기 위한 보안정책, 보안조직, 자산분류 및 통제, 인적보안, 물리적 및 환경적 보안, 의사소통 및 운영관리, 접근통제, 시스템 개발 및 유지보수, 업무지속성관리, 준수의 10가지 분야에 대한 통제항목을 제시한다. 정보보호 지표에 관련된 연구결과는 표 2와 같다.

표 2. 정보보호 지표
Table. 2 Information Security direction

	내 용
정보화 지표	• 정보통신기술을 이용한 전자계 정보화를 중심으로 정보설비, 정보이용, 정보투자지표 분야로 설정하여 각 분야별 구체적인 항목을 제시
BS7799	• 조직의 효과적인 보호관리 체계를 위한 종합적인 가이드라인 제공 • 보안정책, 보안조직, 자산분류 및 통제, 인적보안, 물리적 및 환경적 보안 등 10가지 분야에 대한 통제항목 제시

2.3 정보보호 성숙모형

정보기술 환경의 급속한 발달과 더불어 고객의 요구사항이 다양해지고, 정보화가 지원하는 영역이 점진적으로 확대되면서, 이러한 요구사항에 대응하기 위하여 정보화 수준 또한 점진적으로 성숙되어 가고 있다. 이에 따라 이러한 성숙도를 표현할 수 있는 모델이 필요하게 되었는데, 본 논문에서는 미국의 NIST가 제시하는 컴퓨터시스템의 라이프 사이클의 성숙단계와 SSE-CMM이 제시하는 조직의 보안공학 프로세스의 성숙단계를 바탕으로 네트워크 시스템들의 각각 요구사항을 평가할 수 있는 방법으로 요구사항별 체크리스트를 제시하여 이를 평가할 수 있는 성능지표를 제시하고자 한다.

미국의 NIST는 컴퓨터 시스템의 라이프 사이클에서 보안과 계획에 관한 개략적인 절차를 제공하는데 NIST의 컴퓨터 라이프 사이클은 크게 시작, 개발 및 도입, 구현, 운영 및 유지보수, 폐기의 총 5단계로 구분되어진 성숙단계를 제시하고 있다. SSE-CMM은 조직의 보안공학 프로세스의 핵심적인 특징을 묘사하고 있으며, 비공식적으로 수행되는 수준1, 계획되고 관리되는 수준2, 잘 정의되는 수준3, 정량적으로 통제되는 수준3, 지속적인 개선의 총 5단계 보안 성숙도 모형을 제시하고 있다.

2.4 정보보호시스템 보안 요구사항

• 서버의 보안 요구사항

- 서버 취약성 관리 : 서버의 취약성 관리는 서버에서 제공하는 서비스들 중 보안 취약점이 있는 서비스를 하는지, 불필요한 명령들을 사용할 수 있게 해놓았는지 주기적으로 보안 취약성에 관련된 문제들에 대해서 점검하고 있는지에 관하여 체크한다.

- 사용자 계정 관리 : 사용자 계정에 관련하여 접근제어에 관련된 정책이 이루어지는지 사용하지 않는 불필요한 계정이 존재하는지에 관하여 체크한다.

- 패스워드 보안 : 패스워드 보안에 대해서는 패스워드의 사용에 대한 정책에 관련된 사항들을 체크한다.

• 침입탐지 시스템 보안 요구사항

- 감사 데이터 생성 기능 : 감시 대상 시스템으로부터 감사 데이터를 수집할 수 있는 기능에 대한 체크

- 보안위반 분석 : 알려진 시스템 보안위반 사건에 대한 목록을 바탕으로 보안 위반임을 판단할 수 있는가를 체크

- 보안감사 대응 : 보안 감사에 대하여 실시간으로 발견 및 조치를 취할 수 있는가에 대한 체크

- 보안정책 기능 : 보안정책의 변경 수정 삭제에 관련된 기능을 체크

- 자동 업데이트 기능 : 자동 업데이트를 통해 항상 최신의 침입탐지 패턴을 유지할 수 있는가를 체크

- 다양한 네트워크 환경 지원

• 방화벽의 보안 요구사항

- 보안정책 : 보안정책에 관련하여 지켜져야 할 정책들이 제대로 지켜지고 있는지 또는 효율적으로 이루어지고 있는지 체크한다.

- 로깅 : 보안에 필요한 로깅 데이터들이 정확하게 기

록되는지 체크한다.

- 운영 : 운영기능의 사용성에 관련된 부분들을 체크한다.
- 필터링 : 패킷 필터링에 관련된 규칙들에 대한 설정 항목들을 체크한다.

Ⅲ. 정보보호수준 평가 메커니즘

3.1 정보보호수준 평가 성능시험

성능시험용 규칙집합 DB를 작성하고, 저장된 성능시험 규칙집합을 이용하여 시험용 시나리오를 선택하면 선택한 시나리오를 생성한다. 생성된 시나리오를 이용하여 성능시험 지표에 따라 성능시험을 분석하여 해당 정보보호 시스템으로 전송하고 그 결과를 이용하여 정보보호시스템의 성능에 대한 시험을 진행할 수 있다.

정보보호시스템에 대한 성능시험을 진행하기 위한 일반적인 성능시험 절차는 그림 1과 같다.

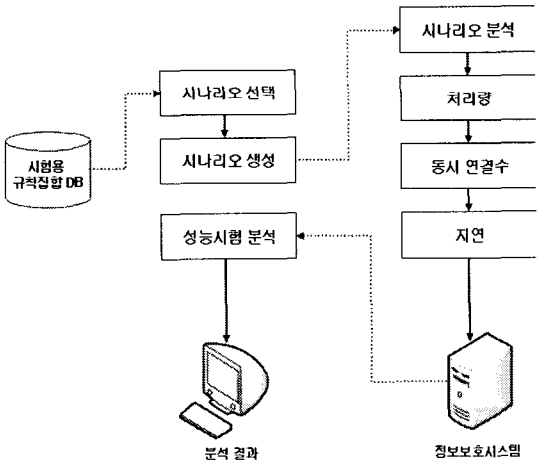

그림 1. 정보보호수준 평가 성능시험 과정
Fig. 1. Process of Information Security System Test

3.2 정보보호수준 평가 메커니즘

네트워크 보안성을 평가할 수 있는 대상들을 선별하고 대상들의 평가 요구사항들을 바탕으로 각 대상들의 각각의 요구사항을 평가할 수 있는 방법으로 요구사항별 체크리스트를 작성하여 이를 평가할 수 있는 지표를 제시하도록 하겠다.

각각의 평가 대상별 체크리스트의 체크항목은 Yes, No, N/A로 구성되어진다. 평가 대상별 체크 항목의 개수와 체크 항목 중 Yes로 체크된 항목의 퍼센트(%)율로 각 대상의 보안성을 측정하고 전체 네트워크 보안성은 각 대상별 보안성을 전체 네트워크 보안성 참여 비율로 계산한 합으로 구해질 수 있다.

- 각 대상별 보안성 측정방법

$$\frac{\text{Yes로체크된체크항목의개수}}{\text{전체체크항목의개수(N/A로체크된항목은제외)}} \times 100$$

- 전체 네트워크 보안성 측정방법

$$\sum(\text{평가 대상별 보안성} \times \text{각 대상별 weight값})$$

- 각 대상별 가중치 값 : 서버(15%), 방화벽(40%), 개인용컴퓨터(10%), 보안취약성 진단 도구(15%), 침입탐지 시스템(30%)

Ⅳ. TS 기반의 정보보호 수준 평가 방법론

4.1 정보보호 수준 평가 성능시험 지표

- 처리량(throughput)

DUT(Device Under Test)/SUT(System Under Test)가 패킷을 폐기(drop)하지 않으면서 처리할 수 있는 최대량

- 동시 연결수(concurrent connection)

호스트들 혹은 호스트와 DUT/SUT 사이의 연결의 총합. '연결(CONNECTION)'은 호스트 혹은 호스트 와 DUT/SUT 사이에서 알려진 프로토콜을 이용하여 데이터를 교환하도록 합의한 상태를 의미하지만, 동시 연결에서는 모든 존재하는 연결이 데이터를 전송할 수 있는 상태라는 것을 의미한다. 즉, 연결이 데이터를 전송하지 못한다면, 그 연결은 동시 연결 수에서 제외.

- 지연(latency)

DUT/SUT가 패킷을 받아서 목적하는 인터페이스로 전송하는 사이에 걸리는 시간. DUT/SUT의 패킷 처리 방식에 따라 컷 스루우(cut through)방식으로 구분되나, 일반적으로는 다음과 같이 정의할 수 있다.

지연 시간 = 수신 시간 - 송신 시간

4.2 정보보호 수준 평가 성능시험 구성

• 시험구성

시험구성에서 Tester는 하드웨어 기반의 시험장비이고, SUT(System Under Test)가 시험 대상인 침입차단 시스템이다. PC1, PC2, PC3은 애플리케이션 레이어에서의 시험에서, 애플리케이션 테스트 제품을 설치하여 사용한다. Tester는 두 개의 시험 포인트(testing point)를 가지는데, 시나리오에 따라서 두 지점을 입력과 출력으로 연결하여 시험한다.

• 규칙 집합

처리량 시험에 많이 사용되는 침입탐지시스템 단일 규칙(single rule)은 다음과 같다. 즉, 각각의 인터페이스에서 출발지 주소, 목적지 주소, 사용하는 프로토콜이나 포트번호에 상관없이 무조건 허용하는 규칙이다. 일반적인 침입탐지시스템 성능시험 시에 자주 사용되는 단일 규칙대신에 제안하는 50개의 규칙집합은 대략 다음과 같이 비교적 실제 환경에 적용 가능한 규칙들로 구성하였다.

내부 → DMZ: 주요 서비스만 허용
(예: HTTP, telnet, ftp, DNS, SMTP, POP3 등)
내부 → 외부: 주요 서비스만 허용
(예: HTTP, telnet, ftp, DNS, SMTP, POP3 등)
외부 → DMZ: 주요 서비스만 허용
(예: HTTP, telnet, ftp, DNS, SMTP, POP3 등)
DMZ → 내부: 모든 서비스 거부
DMZ → 외부: 주요 서비스만 허용
(예: DNS, SMTP, POP3 등)
Default로 위의 규칙에 해당하지 않는 모든 패킷은 거부

표 3과 같이 시험용 규칙 집합은 1번부터 순서적으로 비교를 한다. 규칙에 일치(match)하는 것이 있으면, 정책에 따라서 패킷의 허가(allow)/거부(deny)를 결정한다. 규칙이 일치하지 않으면, 다음 규칙을 비교하고, 마지막 규칙의 비교가 끝나면 기본(default)정책에 따라서 허가/거부가 결정된다.

표 3. 시험용 규칙집합
Table. 3 Test Rule Set

순서	인터페이스	출발지 주소	목적지 주소	프로토콜	서비스	정책
int.1	int	내부망	DMZ	TCP	80(HTTP)	허용
int.2	int	내부망	DMZ	TCP	8080(HTTP)	허용
int.3	int	내부망	DMZ	TPC	23(telnet)	허용
…	…	…	…	…	…	…
int.48	int	내부망	any	TCP	80(HTTP)	허용
int.49	int	내부망	any	TCP	8080(HTTP)	허용
int.50	int	내부망	any	TCP	23(telnet)	허용
default	int	any	any	any	any	거부
ext.1	ext	외부망	DMZ	TCP	80(HTTP)	허용
ext.2	ext	외부망	DMZ	TCP	8080(HTTP)	허용
…	…	…	…	…	…	…
ext.50	ext	외부망	DMZ	TCP	23(telnet)	허용
default	int	any	any	any	any	거부
DMZ.1	DMZ	DMZ	내부망	any	any	거부
…	…	…	…	…	…	…
DMZ.47	DMZ	DMZ	외부망	TCP	25(SMTP)	허용
DMZ.48	DMZ	DMZ	외부망	TCP	53(DNS)	허용
DMZ.49	DMZ	DMZ	외부망	UDP	53(DNS)	허용
DMZ.50	DMZ	DMZ	내부망	TCP	110(POP3)	허용
default	DMZ	any	any	any	any	거부

일반적으로 기본정책은 모든 패킷을 거부하는 것이다. 따라서 규칙 집합에서는 허용할 패킷들의 규칙을 설정하고, 여기에서 허용되지 않은 모든 패킷은 거부된다.

ext와 DMZ 인터페이스에는 내부 네트워크에서 시작한(initiate) 접속만 허용하도록 ACK 필드를 확인한다고 가정한다. 이러한 규칙 설정은 침입차단 시스템에 따라서 다양하기 때문에 여기서는 일반적인 규칙만 열거 하였다. 또한 규칙을 실제 패킷과 비교하는 경우, 각각의 인터페이스에 해당하는 규칙만을 사용하기 때문에 각각의 인터페이스별로 50개의 규칙이 있는 것으로 가정하였다.

4.3 정보보호 수준 평가를 위한 시험 시나리오

• 시험 시나리오(처리량)

1) 시험 목적

- 다양한 조건에서의 처리량 측정

2) 시험 조건

- 규칙 집합 수 변경(1, 50)
- 로깅 기능
- 패킷 사이즈 변경(64, 512, 1024, 1518 byte)

3) 시험 방법

- 규칙 집합이 50개인 경우, 50번 규칙에 의해서 허용되는 패킷을 사용하여 시험 수행(예) 외부망에서 DMZ로의 telnet 접속 패킷

표 4. 시나리오 1
Table. 4 Scenario 1

번호	로깅	규칙집합	패킷 사이즈	처리량
1-1	Off	1	64	70
			512	48
			1024	80
			1518	90
1-2	Off	50	64	50
			512	60
			1024	70
			1518	80

• 시험 시나리오(지연)

1) 시험 목적

- 다양한 조건에서의 지연측정

2) 시험 조건

- 규칙 집합 수 변경(1, 50)
- 로깅 기능(off/on)
- 패킷 사이즈 변경(64, 512, 1024, 1518 bytes)

3) 시험 방법

- 규칙 집합이 50개인 경우, 50번 규칙에 의해서 허용되는 패킷을 사용하여 시험 수행- 시나리오 1과 동일(예) 내부 망에서 외부 망으로의 telnet 접속 패킷

표 5. 시나리오 2
Table. 5 Scenario 2

번호	로깅	규칙집합	패킷 사이즈	처리량
2-1	Off	1	64	35
			512	45
			1024	55
			1518	65
2-2	Off	50	64	45
			512	50
			1024	55
			1518	70

• 시험 시나리오(애플리케이션 처리량)

1) 시험 목적

- 다양한 조건에서의 애플리케이션 처리량 측정

2) 시험 조건

- 규칙 집합 수 변경(1, 50)
- 로깅 기능(off/on)
- 패킷 사이즈 변경(64, 512, 1024, 1518 bytes)
- 애플리케이션 변경(FTP, HTTP)

3) 시험 방법

- 외부 망과 DMZ내 2대의 PC에 설치된 Chariot을 이용하여 FTP, HTTP 스크립트에 대해서 시험 수행후 측정
- 애플리케이션에 따라서, 50번 규칙 변경 하여 시험 수행

표 6. 규칙집합
Table. 6 Rule Set

순서	인터페이스	출발지 주소	목적지 주소	프로토콜	서비스	정책
ext.50	ext	외부망	DMZ	TCP	21(FTP)	허용
ext.50	ext	외부망	DMZ	TCP	80(HTTP)	허용

표 7. 시나리오 3
Table. 7 Scenario 3

번호	로깅	규칙집합	애플리케이션	처리량
3-1	Off	1	FTP	80
			HTTP	90
3-2	Off	50	FTP	75
			HTTP	85

• 시험 시나리오(세션 용량)

1) 시험 목적

- 초당 유지 가능한 세션 용량 측정

2) 시험 조건

- 단일 규칙 적용
- 로깅 기능(off/on)
- 연결 요청 비율(개/sec) 변경 (1,000~2,000)

3) 시험 방법

- 외부망과 DMZ내 2대의 PC에 설치된 Chariot을 이용하여 연결 요청 비율(개/sec)을 변경하며, 일정 시간 후 세션 수가 더 이상 증가되지 않을 때, 동시 연결(concurrent connection)수 측정
- 시나리오 3과 동일

표 8. 시나리오 4
Table. 8 Scenario 4

번 호	연결 요청 비율(개/sec)	동시 연결(개)
4-1	1,000	700
4-2	2,000	700

• 시험 시나리오(비트 전달 비율)

1) 시험 목적

- 규칙에 의해서 허가된 패킷의 처리량측정
- 거부 패킷의 비율을 증가시키며 처리량을 측정하여, DoS 공격시 침입탐지시스템의 대처 능력을 파악

2) 시험 조건

- 규칙 집합 적용(50)
- 로깅 기능(on)
- 패킷 사이즈 변경(64, 1418 bytes)
- 허용/거부 패킷의 비율 변경(0~100%)
- 최대 부하(100/1000 Mbps)

3) 시험 방법

- 허용 패킷은 50번 규칙에 의해서 허용되는 패킷 사용(예) 외부망에서 DMZ로의 telnet 접속 패킷
- 거부 패킷은 50번 규칙 이후 기본(default) 정책에 의해서 거부되는 패킷 사용(예) 외부망에서 DMZ로의 SNMP 패킷
- firewall에서 허용하는 최대부하로 시험 수행
- 시나리오 1과 동일
- 거부 비율이 100%인 경우, down되면 Dos 공격에 취약하다는 것을 알 수 있음

표 9. 시나리오 5
Table. 9 Scenario 5

번호	허용 비율	거부 비율	패킷사이즈	처리량
5-1	100	0	64	40
			1518	50
5-2	80	20	64	50
			1518	50

4.4 정보보호 수준 평가를 위한 성능시험 기준 평가

비교시험을 하는 경우에는 동일한 성능시험 지표 및 성능시험 시나리오를 사용하여 대상 제품들의 결과를 비교하면 되지만, 인증을 목적으로 한 단독시험의 경우에는 어느 정도의 성능을 기준으로 하여 통과/실패를 판정할 것인지를 정할 필요가 있다. 다음의 기준들은 실제로 제품에 적용하여 검증된 기준이 아니기 때문에, 실제 시험 및 인증을 하는 경우에는 현황에 맞도록 수정 보완이 필요할 것이다.

표 10. 등급기준
Table. 10 Grade Standard

등 급	A	B	C	D	E
처리량 (Mbps)	0~45	46~60	61~75	76~90	91~100
연결(개)	0 ~ 20,000	20,000 ~ 30,000	30,000 ~ 40,000	40,000 ~ 50,000	50,000 이상
지연(%)	처리량에서 45%이상 감소	처리량에서 35%~45% 사이 감소	처리량에서 25%~35% 사이 감소	처리량에서 15%~25% 사이 감소	처리량에서 15%이내 감소

위의 기준은 다음과 같이 인증 여부를 결정하는 경우 사용될 수 있다. 즉, 인증 여부를 판단할 시나리오를 적절히 선택하고, 각각의 측정값에 대하여 등급 기준을 적용하여 A, B, C, D, E의 등급을 부여하고, 전체 시나리오에서 B등급 이상을 받은 경우에만 성능시험 기준을 만족하는 것으로 하여 인증할 수 있다. 이렇게 하여 최저 등급(B)을 만족하는 제품을 인증하고 인증을 받은 제품들의 성능을 객관적인 성능 수치로 표시 가능할 것이다.

V. 결 론

본 논문에서는 정보보호수준을 종합적이고 체계적으로 평가하기 위해 정보보호와 관련된 기술적 요소와 관리적 요소를 통하여 네트워크 보안 성능을 평가할 수 있는 테스트 시나리오를 제시함으로써 정확하고 가시화된 기업이 정보보호수준에 대한 객관적인 평가가 가능하게 되었다.

향후 연구방향으로는 이러한 정보보호수준 평가 시험 시나리오를 활용하여 기업 및 국가의 정보보호시스템을 객관적으로 측정할 수 있으며 평가 결과를 바탕으로 민간부문의 정보보호수준 제고를 위한 정보보호정책 수립에 합리적인 의사결정의 도구로 사용될 수 있을 것으로 기대되고, 제안한 평가 방법론을 실제 제품에 적용한 사례 연구가 필요하다.

참고문헌

[1] Common Criteria Project, "Common criteria for information technology security evaluation", common criteria, 1998.

[2] Silvana Castano et al., "Database security", Addison Wesly, 1994.

[3] Lynette Barnard, "The evaluation and certification of information security against BS7799", Information Management & Computer Security, pp.72~77. 1998.

[4] BSI, "BS7799", BSI, 1999.

[5] NIST, "Security Assessment Guide Information Technology Systems", NIST Special Publication, 800-26, 2001.

[6] NIST, "A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2", 800-29, 2001.

[7] 한국정보보호진흥원, http://www.kisa.or.kr

[8] Systems Security Engineering Capability Maturity Model, http://www.sse-cmm.org

[9] 김수연 외, "정보보호시스템 평가 · 인증체계 모델 제안", 한국정보보호학회지, 제14권 2호, 2004.4.

[10] 정민아 외, "역할기반 접근 제어를 적용한 데이터베이스 보안 시스템에서의 보안 정책 최소화" 한국해양정보통신학회 논문지, 제9권 6호, pp.1364~1370, 2005.

저자소개

성 경(Kyung Sung)

1993년 경희대학교 전자계산학과 (이학석사)
2003년 한남대학교 컴퓨터공학과 (공학박사)
1994년~2004년 동해대학교 컴퓨터공학과 교수
2004년~현재 목원대학교 컴퓨터교육과 교수
※관심분야 : 정보보호 및 정보관리, 컴퓨터네트워크, 신경회로망, 컴퓨터교육

김 석 훈(Seok-Hun Kim)

2001년 배재대학교 정보통신공학과 (공학사)
2003년 한남대학교 컴퓨터공학과 (공학석사)
2006년 한남대학교 컴퓨터공학과(공학박사)
2006년~현재 대전보건대학 멀티미디어과 겸임교수
※관심분야 : Mobile Computing, VoIP, XML, Web-GIS, Web DB, 정보보호