가상사설망(VPN)시스템의 보안성 품질평가모델 개발

마쯔종*,김금옥**,양해술*
*호서대학교, **호남대학교 정보통신대학
e-mail:libobbll99@naver.com, tyhjc@naver.com, hsyang@hoseo.edu

VPN secure quality evaluation system development

Zhi-Zhong, Ma*, Jin-Yu, Jin**, Hae-Sool, Yang*
*Hoseo University, **Honam University

요 약

가상사설망(VPN)시스템은 기존 사설망의 고비용과 비효율적인 관리를 해결하기 위해 인터넷망을 마치 전용선으로 사설망을 구출한 것처럼 개발한다. 본 연구에서는 ISO/IEC 9126과 ISO/IEC 25000 를 기반을 둔 객관성 있는 품질평가 방법을 구축하고 가상사설망시스템 제품 고유의 보안특성을 접목한 품질평가 체계를 구축함으로써 객관성과 타당성을 갖춘 평가모델을 개발하였다.

1. 서론

가상사설망은 기업은 지사나 영업소 또는 이동근무자가 지역적 제한없이 업무를 수행할 수 있도록 통신 사업자에게 전용회선을 임대하여 원격지까지 연결하는 방식으로 구축하는 기존 사설망이 다르고 가상사설망은 기업의 통신망과 인터넷 서비스 제공자와 직접 연결하면 되기 때문에 별도로 값비싼 장비나 소프트웨어를 구입하고 관리할 필요가 없어 기존의 사설망 연결방식보다 비용이 대폭 절감되는 효과를 기대할 수 있으며 일반기업에서는 확보하기 어려운 정보통신 관련 전문기술을 활용할 수 있다.

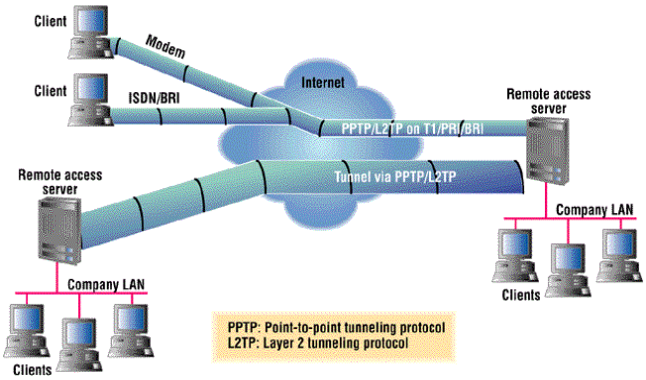
또한 재택 근무자, 출장이 잦은 직원, 현장 근무자들이 인터넷 서비스 제공자와 전화로 접속한 다음 인터넷을 통하여 회가와 연결할 수 있고 즉, 공중망을 이용하기 때문에 사용자가 늘어나거나 장소를 옮기더라도 유연하게 통신망을 사용할 수 있어 본사와 지사, 지사와 지사간의 자료 공유가 훨씬 용이해진다.

본 연구에서는 이러한 가상사설망(VPN)시스템의 품질수준 평가의 체계를 잡기위해 가상사설망(VPN)시스템의 보안성 품질평가 모델을 개발하였다.

2. 가상사설망(VPN)시스템 핵심기술

가. 터널링(Tunneling)기술

터널링 기술은 시작 지점에서 목표 지점까지 가상적인 터널을 형성하여 정보를 주고받도록 하는 기술로서 가상의 터널을 만들어 제3자의 접근을 막는 비밀 통로 역할을 한다. 즉, 송신자가 보내는 데이터 패킷에 보안 헤더를 추가하여 원래 패킷을 캡슐화하는 방식으로 사전에 약속된 수신자 이외에는 알아 볼 수 없도록 패킷을 전송하는 기술이다.



(그림 1) 터널링 기술

3. 가상사설망(VPN)시스템 보안성 평가모델

가상사설망은 인터넷이라는 공중망을 기본으로 하기때문에 적절한 통신속도 및 대역폭의 보장과, 무엇보다 정보에 대한 보안이 확실하지 않다는 점이 단점이다.

그래서 가상사설망시스템 보안성에 대한 품질평가는 세부적으로 해야 한다고 가상사설망시스템 보안품질 전체적인 향상을 필요하다.

가. 보안성 평가항목 분석

보안성이란 권한이 없는 사람 또는 시스템은 정보를 읽거나 변경하지 못하게 하고, 권한이 있는 사람 또는 시스템은 정보에 대한 접근이 거부되지 않도록 정보를 보호하는 소프트웨어의 능력을 의미한다.

부특성	평가항목의 목적	평가 항목명
보안 감사성	보안문제의 감사레코드를 생성하고 감사된 보안 위반을 대응행동을 수행하는 능력	보안 경보, 감사 데이터 생성, 규칙 위반 지적, 검사 검토, 저장소 보호, 대응 행동, 손실 방지

암호지원	가상사설망을 사용할 때 외부에 대한 보안을 통해 정보가 노출되지 않은 능력	암호키 생성, 암호키 분배, 암호키 파기, 암호 연산
사용자 데이터 보호	객체에 대한 무결성 오류에 대해 사용자 데이터를 검사하고 오류 탐지시 대응행동을 수행하는 능력	정보흐름 통제, 보안 속성에 따른 통제
식별 및 인증	사용자의 신원을 식별 및 인증을 제공하는 능력	인증 실패처리, 사용자 보안속성 유지, 비밀정보 생성, 사용자 인증, 인증 피드백 보호
보안 관리성	해당 지식정보보안 제품의 보안기능, 보안 역할 등 관리하는 능력	보안기능 관리, 보안속성 관리, 디폴트 값제공, 데이터 관리 제한, 한계치 관리 제한, 관리기능 수행, 관리자 역할 유지
보안기능 보호	주기적 또는 관리자의 요구에 따라 무결성을 검증하는 능력	재사용 탐지, 재사용 대응, 자체 시험
접근통제성	정보흐름을 중재하기 위해 패킷필터링 등을 통하여 외부망으로부터 내부망을 보호하는 능력	세션 잠금

나. 보안성 메트릭

(1) 보안 경보(보안감사성)

보안 경보: 보안위반 탐지시 대응행동의 목록을 어느 정도 취하는가?

측정 항목	A	보안 위반 탐지 수		
	B	대응행동 목록을 취한 경우의 수		
계산식	- 보안 경보 = B/A			
결과 영역	0 ≤ 보안 경보 ≤ 1		결과값	

(2) 암호키 분배(암호지원)

암호키 분배: 명세된 암호키 분배 방법에 따라 암호키를 분배하는가?

측정 항목	A	암호키 분배 규정에 따라 암호키를 분배하는지의 여부	
계산식	- 암호키 분배 = A		
결과 영역	암호키 분배 = Yes or No	결과값	

(3) 보안 속성에 따른 통제(사용자 데이트 보호)

보안속성에 따른 통제: 보안속성에 따라 정보흐름을 통제하는가?

측정 항목	A	정보흐름에 관련된 모든 오퍼레이션의 수		
	B	정보흐름이 보안속성에 따라 통제되는 오퍼레이션의 수		
계산식	- 보안 속성에 따른 통제 = B/A			
결과 영역	0 ≤ 보안 속성에 따른 통제 ≤ 1		결과값	

(4) 사용자 보안속성 유지(식별 및 인증)

사용자 보안속성 유지: 각 사용자에 대해 규정된 보안속성 목록을 유지하는가?

측정 항목	A	사용자별 보안속성 목록유지 여부		
		- 보안속성 : 디폴트값 변경, 질의, 변경, 삭제 등		
계산식	- 사용자 보안속성 유지 = A			
결과 영역	사용자 보안속성 유지 = Yes or No		결과값	

(5) 데이터 관리 제한(보안 관리성)

데이터 관리 제한: 식별 및 인증 데이터의 관리를 인가된 관리자로 제한하는가?

측정 항목	A	비인가자의 식별 및 인증 데이터 관리 차단 여부		
계산식	- 데이터 관리 제한 = A			
결과 영역	데이터 관리 제한 = Yes or No		결과값	

(6) 재사용 탐지(보안기능 보호)

재사용 탐지: 식별된 실체 목록에 대한 재사용을 어느 정도 탐지하는가?

측정 항목	A	실체 목록 재사용 시도 회수		
	B	재사용되지 않는 경우의 회수		
계산식	- 재사용 탐지 = B/A			
결과 영역	0 ≤ 재사용 탐지 ≤ 1		결과값	

(7) 세션 잠금(접근통제성)

세션 잠금: 관리자 비활동 기간 후에 세션을 잠가 활동을 무력화시키는가?

측정 항목	A	비활동 상태로 규정된 시간 경과후 세션 잠금이 수행되는지 여부		
		- 세션 : 망 환경에서 사용자 간 또는 컴퓨터 간의 대화를 위한 논리적 연결. 프로세스들 사이에 통신을 수행하기 위해서 메시지 교환을 통해 서로를 인식한 이후부터 통신을 마칠 때 까지의 기간		
계산식	- 세션잠금 = A			
결과 영역	세션잠금 = Yes or No		결과값	

5. 결론

지금 소프트웨어 분야의 급격한 발전으로 인해 국제표준의 변화가 불가피하였기 때문에 표준의 구성이나 내용이 지속적으로 변화되어 왔고 이러한 변화를 수용한 평가방법의 구축도 필요한 실정이다. 이러한 관점에서 볼 때, 가상사설망(VPN)시스템 제품은 보안성과 성능 측면에서 일반적인 소프트웨어 제품의 특성과는 다른 속성들을 가지고 있으므로 기존의 ISO/IEC 9126의 품질특성 체계를 기반으로 품질평가를 수행하기에는 지식정보보안 제품의 특성을 제대로 반영하지 못한다는 한계가 있다.

가상사설망(VPN)시스템 제품은 빠른 성장세를 보이고 있으나 그 동안 질적인 품질을 고려하는 노력이 미흡한 것이 사실이었다. 따라서, 본 연구에서는 지식정보보안 제품의 질적인 면을 평가하여 품질수준을 파악하여 개선방향을 도출함으로써 품질향상을 지원할 수 있는 평가모델을 개발하기 위해 가상사설망(VPN)시스템 제품의 동향 및 기술적인 요소들을 조사 분석하고, 평가방법론 구축의 근간이 되는 국제표준의 동향을 분석 하였다.

본 연구가 가상사설망(VPN)시스템 품질평가를 지원하여 국내 가상사설망(VPN)시스템 제품의 품질향상에 기여할 수 있기를 기대하며, 향후 연구 방향을 제시하기 위해 본 연구의 한계점을 제시하고자 한다.

참고문헌

[1] ISO/IEC 9126, “Information Technology - Software Quality Characteris- tics and metrics - Part 1, 2, 3″

[2] 양대일 외, “정보 보안 개론과 실습 - 인터넷 해킹과 보안”, 한빛미디어, 2005.

[3] KISA 연구보고서, “통합시스템 보안성 평가체계 및 방법 연구”, 2006.

[4] 구본승, “SSL, VPN 구현기술 분석”, 동국대학교 영상정보통신대학원 석사학위 논문, 2006.

[5] 양해술, “SW 품질 비용 리포지토리 구축 연구”, 한국소프트웨어 진흥원, 최종보고서, 2008. 12.