통합보안관리 시스템 보안성 평가모델

강상원*, 전인오**, 양해술**
*호서대학교 혁신기술경영융합대학원
**호서대학교 벤처전문대학원
e-mail:myksangwon@paran.com, hsyang@office.hoseo.ac.kr

Unified Threat Management System Security Evaluation Model

Sang-Won Kang* In-Oh Jeon** Hae-Sool Yang**
*Graduate School of Multidisciplinary Technology and Management, Hoseo Univ
**Graduate School of Venture, Hoseo Univ

요 약

본 논문에서는 통합보안관리 시스템에 대해서 주요 기능을 분석하고 시장동향을 조사하였으며, 기존의 소프트웨어 품질 평가 기술 및 표준화에 관한 연구를 추진하고, 통합보안관리 시스템의 보안성 품질 평가 모델을 개발하였다. 본 연구를 통하여 도출된 통합보안관리 시스템의 보안성 품질 평가 모델을 통하여 통합보안관리 시스템의 품질을 향상시키는데 중요한 역할을 할 것으로 본다.

1. 서 론

지금까지 출시된 보안 제품으로는 상당히 많은 종류들이 있으며 이미 진출한 상태이나 이 모든 제품들을 설치했다고 하더라도 각각의 솔루션은 보안 취약점을 가지고 있으므로 결코 견고한 시스템이라 고할 수 없다. 보안 제품의 조합이 결코 효율적으로 기능을 제공한다고 보장할 수 없다. 더욱이 컴퓨터 공격의 대다수가 지능형으로 진행하기 때문에 새로운 공격을 효과적으로 차단할 장비가 요구되고 있다.

그러므로 기존의 모든 기능을 흡수하며 더불어 능동적으로 모든 조건을 실시간으로 자동 방어할 수 있는 시스템의 필요성이 부각되고 있다.

이와 더불어 통합보안관리(Unified Threat Management)는 보안솔루션의 통합이라는 개념에서 각광받고 있다. 보안 침해 사건마다 등장하는 새로운 솔루션의 출현으로 보안 시스템은 복잡해지지만 하고, 이러한 시스템을 관리 및 유지하는데 많은 인력과 자원이 요구된다. 이러한 측면에서 통합이란 복잡한 장비들을 감당하기 힘든 상황에서 해소할 수 있는 해결책으로 등장하였다.

본 연구에서는 이러한 제품들의 품질을 평가할 수 있는 모델을 연구하여 기술에 대한 품질을 인정받을 수 있도록 하였다.

† 본 연구는 지식경제부와 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2009-(C1090-0902-0032))

2. 통합보안관리 시술 및 산업 동향

최근의 다양한 보안 이슈중 주목할 만한 것은 여러 가지 공격 기법이 결합된 지능적인 혼합, 변조 공격 사례가 급증하고 있으며 이에 대한 강력한 방어와 효율적으로 대처할 수 있는 통합보안관리 솔루션에 대한 관심이 높아지고 있다. 이는 손쉬운 설치와 뛰어난 관리 편의성 뿐 아니라, 낮은 투자 비용으로 높은 성능을 기반으로한 다양한 보안 기능을 제공하는 통합보안관리의 장점 때문이다.

이장에서는 통합보안관리에 대한 기술 동향과 산업 동향에 대해서 기술하였다.

2.1. 통합보안관리 기술 개요

UTM(Unified Threat Management)은 “파이어월, VPN, IDS/IPS, 안티바이러스, 안티스팸과 같은 다양한 보안기능을 단일 어플라이언스 형태로 통합해 관리 복잡성을 최소화하고, 복합적인 위협요소를 효율적으로 방어하기 위한 통합보안솔루션”을 말한다.

통합보안관리의 출현 배경은 웜/바이러스, 트로이 목마, 스파이웨어 등 보안 위협의 다양화와 증대, 이에 따른 복합화된 보안 위협에 대응하기 위한 통합 보안솔루션의 요구 증대, 보안 관리의 편의성과 보안 장비 관리/운영 비용 절감에 대한 요구가 증대됨을 들 수 있다.

다양한 기능을 수행하고 보안 관리 편리성과 관리 비용 절감면에서는 효과적이라는 분석과 함께 보안 기능 집중화에 대한 역기능(SPF 등), 단일 장비에서 다기능 수행에 대한 성능과 신뢰성 대두는 고려할 사항임을 제시하고 있다.

통합관리의 주요 기능을 살펴보면 오늘날 통합보안관리는 흔히 통합보안솔루션과 동일한 의미로 사용되고 있다. 하지만 초창기의 통합보안관리의 정의와 기본 개념은 중심으로 VPN과 IDS/IPS, 안티바이러스 등의 보안 기능이 유기적으로 통합된 원-박스(One-Box) 형태의 보안장비이다.

2.2. 통합보안관리 시장 동향

국내에서 통합보안관리 솔루션은 점차 세분화되고 있는 보안시장에서 낮은 투자비용으로 다양한 보안 위협과 유해 트래픽을 효율적으로 차단하고, 맞춤형 보안기능 제공을 통해 주로 SOHO나 SMB 같은 중소기업을 대상으로 한 틈새시장을 형성해 왔다. 특히, 보안의 서비스화라는 개념이 확산되고, 보안 시장자체가 제품 중심으로 운영/관리 서비스로 전환되면서 통합보안관리 시스템은 IPS와 연계한 임대서비스나 보안관제 아웃소싱 서비스의 핵심 인프라로 자리잡으면서 향후 지속적인 성장세가 예상된다.

2007년 국내 보안시장은 약 2천억원 규모를 무난히 형성할 덕으로 예상하였다. 이중 통합보안관리 솔루션의 규모는 약 7백억원으로 새로운 통합 보안 솔루션 시장이 형성될 것으로 예측하였다. 2006년부터 2010년까지 네트워크 통합보안 시장은 연평균 31% 성장하면서 2010년부터는 중형 라우더 시장을 앞지를 것으로 예측하고 있다.

[표 1] 국내 네트워크 정보보호 솔루션 매출 동향

구분	2008년	2009년	2010년	2011년	2012년
통합보안솔루션(UTM)	354	394	433	473	513
가상사설망(VPN)	584	642	701	760	818
침입탐지시스템(IDS)	839	918	997	1076	1155
방화벽	777	834	891	948	1005

2.3. 통합보안관리 특성

2007 국내 정보보호산업 시장 및 동향 조사에 따르면 통합보안관리 시스템은 다중 위협에 대해 보호기능을 제공할 수 있는 포괄적인 보안 제품을 가리킨다. UTM이라는 용어는 원래 시장 규모 조사기관인 IDS(International Data Corporation)에 의해 처음 사용되기 시작했다. 통합보안관리가 제공하는 가장 주요한 장점은 단순하고, 설치 및 사용이 간결하며, 모든 보안 기능이나 프로그램을 동시에 갱신할 수 있다는 점 등을 들 수 있다. 인터넷 위협의 특질과 다양성은 보다 복잡하게 발전하고 있기 때문에, 통합보안관리 제품 역시 이 모든 위협들에 대해 적절히 대응할 수 있도록 구성 될 수 있다. 따라서, 시스템 관리자들이 오랜 기간에 걸쳐 다양한 종류의보안 프로그램들을 유지, 관리해야 하는 수고를 덜어준다.

3. 통합보안관리 보안성 품질 평가

보안성이란 권한이 없는 사람 또는 데이터나 프로그램을 권한이 없는 이용자가 사용할 수 없도록 하는 것으로 소프트웨어적인 방법으로서 이용자의 권한과 함께 패스워드를 등록해 두었다가 데이터 세트를 개시할 때나 시분할 시스템(TSS) 세션을 개시할 때 조회하는 방식 등을 의미한다. 보안성은 보안기능 보호, 접근통제성, 침입탐지 등으로 나뉜다.

3.1. 접근통제성

접근통제성이란 시스템이 정보흐름을 중재하기 위해 관련 보안 정책에 기반하여 패킷필터링 등을 통하여 외부망으로부터 내부망을 보호하는 능력을 의미한다. 접근통제성은 세션 잠금의 평가항목을 가진다.

[표 2] 접근통제성의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	보안성	접근 통제성	세션 잠금	사용자 비활동 기간 후 상호작용하는 세션을 잠가 활동을 무력화시키는지 평가	비활동 상태로 규정된 시간 경과후 세션 잠금이 수행되는지 여부

3.2. 침입탐지

침입탐지란 시스템이 보안을 위협하는 침입 행위가 발생할 경우 이를 탐지하는 능력을 의미한다. 침입탐지는 정보수집, 침입분석, 침입대응, 침입탐지 결과 검토, 침입탐지 결과 보호, 대응행동, 손실방지의 평가항목을 가진다.

[표 3] 침입탐지의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	보안성	침입 탐지	정보수집	보호대상시스템으로부터 침입탐지를 위해 필요한 정보를 수집하는지 평가	침입탐지를 위해 필요한 정보 수집 여부
2	보안성	침입 탐지	침입분석	수집 데이터에 기반하여 정해진 분석 기능을 수행하는지 평가	수집 데이터에 기반하여 정해진 분석 기능 수행 여부
3	보안성	침입 탐지	침입대응	보안위반 가능성 및 사실을 탐지하였을 경우 수행해야 할 활동을 수행하는지 평가	보안위반 가능성 및 사실을 탐지하였을 경우 수행해야 할 활동을 수행하는지 여부
4	보안성	침입 탐지	침입탐지 결과보호	인가되지 않은 삭제로부터 저장된 침입탐지 결과를 보호하는지 평가	인가되지 않은 삭제로부터 저장된 침입탐지 결과 보호 여부
5	보안성	침입 탐지	대응행동	침입탐지 결과에 대한 손실이 예측될 때 필요한 대응행동을 수행하는지 평가	침입탐지 결과에 대한 손실이 예측될 때 필요한 대응행동 수행 여부
6	보안성	침입 탐지	손실방지	침입탐지 결과 기록을 위한 저장소가 포화되거나 기타 문제 발생 시 취해야 할 행동을 수행하는지 평가	침입탐지 결과 기록을 위한 저장소가 포화되거나 기타 문제 발생 시 취해야 할 행동 수행 여부

3.3. 보안기능 보호

보호란 주기적 또는 관리자의 요구에 따라 무결성을 검증하는 능력을 의미한다. 보호는 데이터 변경 탐지, 자체 시험의 평가항목을 가진다.

[표 4] 보안기능 보호의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	보안성	보호	데이터 변경 탐지	전송 중인 모든 보안 관련 데이터의 변경 및 위조를 탐지하는 능력을 제공하는지 평가	탐지된 데이터의 수/변경 및 위조된 보안 관련 데이터의 수
2	보안성	보호	자체 시험	데이터 및 실행코드의 무결성을 검증하기 위해 자체 시험을 실행할 수 있는가를 평가	무결성 검증을 위한 자체 시험 가능 여부

3.4. 준수성

준수성이란 보안성과 관련된 표준, 관례 또는 법적 규제 및 유사한 규정을 고수하는 소프트웨어 제품의 능력을 의미한다. 준수성은 보안성 표준 준수율의 평가항목을 가진다.

[표 5] 준수의 평가항목 및 평가방법

번호	특성	부특성	평가 항목명	평가항목의 목적	평가방법
1	보안성	준수성	보안성 표준 준수율	침입탐지 시스템의 보안성 관련 표준, 기준 및 지침에 따라 시스템이 구현되어 있는지 평가	규정을 준수하는 항목의 수/준수성 관련 항목의 수

4. 통합보안관리 시스템 보안성 품질 평가모델

본 장에서는 침입방지 시스템에 대한 평가 방법모델을 제시한다. 앞장에서 소개한 바와 같이 각 주특성에 포함된 부특성의 평가 방법을 작성하였다.

4.1. 접근통제성 평가모델

다음의 표는 접근통제성의 평가모델이다.

[표 6] 접근통제성 평가모델

메트릭명	세션잠금	관리자 비활동 기간 후에 세션을 잠가 활동을 무력화시키는가?		
측정 항목	A	비활동 상태로 규정된 시간 경과후 세션 잠금이 수행되는지 여부		
계산식	- 세션잠금 = A			
결과 영역	세션잠금 = Yes or No		결과값	
문제점				

메트릭명	세션종료	사용자 비활동 기간 후에 상호작용하는 사용자 세션을 종료하는가?		
측정 항목	A	비활동 상태로 규정된 시간 경과후 세션 종료가 수행되는지 여부		
계산식	- 세션종료 = A			
결과 영역	세션종료 = Yes or No		결과값	
문제점				

4.2. 침입탐지 평가모델

다음의 표는 주특성 보안성의 부특성인 침입탐지 평가모델이다.

[표 7] 침입탐지 평가모델

메트릭명	대응행동	침입탐지 결과에 대한 손실이 예측될 때 필요한 대응행동을 수행하는가?		
측정 항목	A	침입탐지 결과에 대한 손실이 예측될 때 필요한 대응행동 수행 여부		
계산식	- 대응행동 = A			
결과 영역	대응행동 = Yes or No		결과값	
문제점				

메트릭명	침입분석	수집 데이터에 기반하여 정해진 분석 기능을 수행하는가?		
측정 항목	A	수집 데이터에 기반하여 정해진 분석 기능 수행 여부		
계산식	- 침입분석 = A			
결과 영역	침입분석 = Yes or No		결과값	
문제점				

4.3. 보안기능 보호 평가모델

다음의 표는 보안기능 보호의 평가모델이다.

[표 8] 보안기능 보호 평가모델

메트릭명		보안기능은 데이터가 전송될 때 노출, 변경으로부터 데이터를 보호하는가?		
데이터 보호				
측정 항목	A	보안기능은 데이터가 전송될 때 노출, 변경으로부터 데이터를 보호하는지 여부		
계산식	- 데이터 보호 = A			
결과 영역	데이터 보호 = Yes or No		결과값	
문제점				

4.4. 준수성 평가모델

다음의 표는 준수성의 평가모델이다.

[표 9] 준수성 평가모델

메트릭명		시스템이 보안성 관련 표준이나 규약에 따라 동작하는가?		
보안성 표준 준수율				
측정 항목	A	평가할 보안성 표준 준수 항목 수		
		- (다음과 같은 유형의 정보 제공 여부를 파악) - 보안성 표준 준수와 관련된 정보 - 소프트웨어 제품이 준수하는 보안성 관련 규정, 기준 및 사용지침		
	B	각 항목별 테스트케이스 성공률의 합		
		- 테스트케이스를 시험하여 성공한 경우를 체크		
계산식	- 보안성 표준 준수율 = B/A - B = $\sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$ - Success_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 중 성공한 건 수 - Total_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 수			
결과 영역	0 ≤ 보안성 표준 준수율 ≤ 1		결과값	
문제점				

5. 결 론

우리나라의 장비 현실은 아직도 민간,공공 부분을 막론라고 특정 벤더 즉, 인지도가 높은 벤더에 의한 독잠화가 심각한 수준에 이르렀다. 이러한 현실은 시장 왜곡과 기술 종속을 심화시킬 뿐만 아니라 통합보안관리의 품질 향상을 저해시키는 요인이 될 수 있다.

또한 우수한 품질의 제품을 선택하고자 하는 사용자 입장에서는 어느 제품이 우월한지 판단하기가 어렵다.

개발업체의 입장에서는 제품 평가 모델 개발에 대한 비용 및 인력이 부담이 된다. 특히 모든 업ㅊ에가 각기 실시한다는 것은 경제적으로도 효과적이지 못할 뿐만 아니라 신뢰성에도 부족한 상황이다. 이를 효과적으로 시행하기 위해서는 중앙집중식 평가모델의 개발이 더욱 시급한 것이다.

본 연구에서는 통합보안관리의 품질향상을 위해 평가항목을 개발하였으며, 본 자료는 통합보안관리 서비스에 활용되고 개발 산업체와 관련 연구기관의 기술 이전을 통해 활용될 것을 사료된다.

앞으로는 도출된 평가항목을 기반으로 실제 테스트가 가 이루어져야 한다. 제 3자가 객관적인 테스트를 통하여 실제로 기능들이 잘 동작하고 있는지 체크하여야 하며, 국내외 시장의 요구사항을 받아들여야 한다. 이 실험을 기초자료로 국외 특성을 분석하는 것도 좋은 사례라 보여진다.

참고문헌

[1] Eric Ahlm, Is Intrusion Prevention Changing Information Security?, Rev. ver. 1.1, March 2004, Vigilar Inc.

[2] Carl Endorf, Jim Mellander and Eugene Schultz, Intrusion Detection and Prevention, Osborne Computer Book, Jan. 2004.

[3] An NSS Group Report V 1.0 Intrusion Prevention Systems(IPS). Group Test. NSS. Jan. 2004.

[4] 정혜정외, “모바일 RFID 미들웨어 품질 평가 모델 개발”, TTA 연구과제보고서, 평택대학교, 2007년

[5] 권원일, 정창신, “소프트웨어 제품 품질에 관한 국제 표준화”, TTA 저널, 제 85호, 2003년 1월

[6] 오영배, “소프트웨어 제품 품질평가”, TTA 저널, 제105호, 2006년 6월

[7] 정연서, 류걸우, 장종수, “네트워크 보안을 위한 ESM 기술 동향”. ITFIND 주간 기술동향 보고서, 2001년, 12월

[8] 고영종외, “보안정책을 표현하는 침입차단시스템의 지식기반 모델링 미 시뮬레이션”, 한국정보보호진흥원 위탁과제연구보고서, 2001년

[9] 전용수, "통합보안시스템 성능 검증을 위한모델링 및 시뮬레이션“, 동의대학교 공학석사학위논문, 2006년