유무선 및 통합환경에서의 보안제품 트렌드 분석

박종일*°, 장봉덕*, 이기영*, 백혜원*, 고훈**, 원우재***, 신용태*

*숭실대학교 IT학부, **한국정보통신대학교 공학부, ***한국정보보호진흥원

A Trend Survery on the Security Products in Wire/Wireless and Unification Environment

Jongil Park*°, Kiyoung Lee*, Fengde Zhang*, Hyewon Baek*, Hoon Ko**, Yoojae Won***, Yongtae Shin*,

*Soongsil University, **Information & Communications University, ***KISA

E-mail : {jipark, willlee04, fengde, hyewon100, shin}@cherry.ssu.ac.kr, skoh21@icu..ac.kr, yjwon@kisa.or.kr

요 약

현재의 많은 보안 제품들이 있으며, 유사한 기능들을 수행하는 많은 제품들이 있다. 그러나, 이러한 제품들에 대해서 정리가 되어 있지 않은 상태에서, 최근에는 ESM이라는 통합 보안제품이란 이름으로 새로운 트렌드를 형성하고 있다. 본 논문의 목표는 유·무선 및 통합환경에서의 보안제품의 특징 및 동향에 대하여 조사·분석하고, 이에 관련된 로드맵을 그려보고자 한다.

1. 서론

정부는 국민소득 2만달러 시대를 이끌 IT839 전략을 추진하고 있는데, 이는 BcN(Broadband Convergence Network), IPv6, USN(Ubiquitous Sensor Network)의 3대 인프라를 기반으로 휴대인터넷, 홈네트워크, 텔레매틱스, 인터넷전화 등과 같은 8대 신규서비스를 제공한다. 그리고, 이를 기반으로 9대 신성장동력 산업을 활성화하고자 하는 것으로 통신 서비스 품질과 H/W, S/W 제품의 경쟁력을 동반 강화하여 IT산업의 순환발전구조를 지속적으로 유지하려는 정책이다. 이러한 IT839전략의 각 요소들은 정보보호 측면에서 바라볼 때 여러 가지 우려되는 위협요소를 가지고 있다. 이러한 위협요소는 각 분야별로 존재하는데, 먼저, 인프라 측면의 위협을 보면, 새로 구축되는 인프라는 사이버공격 범위가 확대되고 공격형태가 다양화되면서 기존의 위협보다 더욱 확산될 수 있는 구조가 된다. 그렇기때문에 새로운 인프라가 구축되면 사이버공격으로 인한 기존의 개별망의 피해가 유·무선 통합망으로 확산되고 나아가 방송망, USN까지 확산 가능할 수 있다는 점이다. 따라서, 향후 이러한 위협으로부터 근본적으로 벗어나고자 정보보호 표준화현황 및 미래를 전망하는 보안제품맵이 필요하여, 본 연구를 진행하였다.한다. 본 논문의 구성은 다음과 같다. 2장에서는 정보보호 제품의 현황에 대해서 설명하고, 3장에서는 정보보호 제품맵 구성을 위한 분류 기준을 설명한다. 4장에서는 제안한 분류 기준에 근거하여 작성한 맵들을 보여주고, 마지막으로 5장에서는 결론을 맺는다.

본 연구는 정보통신 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음.
[2005-S-091-02, IPv6 기반 멀티캐스트 보안 기술 개발]

2. 정보보호 제품현황

국내 주요 연구기관마다 정보보호 제품에 대한 분류는 조금씩 다르다. 본 보고서에서 제품의 현황을 파악하기 위하여 한국정보보호산업협회 제품 분류를 참조하였다. 한국정보보호산업협회는 정보보호산업의 특성상 제품과 서비스의 통합화, 융합화가 매우 빠르게 진행되고 있는 현실을 반영하고 하나의 제품으로 통합되어 있는 것에서 하드웨어, 소프트웨어를 분리해 내는 작업이 사실상

무의미하여 기존의 정보보호 하드웨어, 정보보호 소프트웨어 및 정보보호 서비스의 3대 대분류 원칙을 시스템 및 네트워크 정보보호 제품과 정보보호 서비스로 변경하였다. 제품 현황 조사에 적용된 제품 분류표 <표3-1>는 다음과 같다.

표 1. 정보보호제품 분류

*정보보호산업협회(2006)

대분류	소분류
시스템 및 네트워크정보보호 제품	침입차단(방화벽)시스템
	침입방지시스템(IPS)
	보안관리
	가상사설망(VPN)
	인증제품
	Anti-Virus
	Anti-Spam
	보안운영체제(Secure OS)
	PC보안
	컨텐츠 보안
	공개키기반구조(PKI)
	접근관리
	무선/모바일 보안
	바이오인식 제품
	기타 제품
정보보호서비스	인증서비스
	보안관제
	보안컨설팅
	유지보수
	기타 서비스

3. 정보보호 제품맵 구성 분류

3.1 계층에 따른 분류

OSI 계층에 따른 보안 기능/기술을 나열하여 보고, 각 기능의 역할에 대해서 정리한다. 그리고, 보안 제품을 분석하여 각 계층별별로 어떠한 보안기능이 있는지 분석한다.

근거 : OSI 계층은 나름대로 네트워킹 기능이 있다. 네트워크 위협은 특정한 어떠한 계층에서 발생되는 것이 아니고, 각 계층의 특징에 따라서 위협요소가 있다(본 장에서는 OSI 7계층의 각 역할에 대한 설명은 생략한다). 보안제품은 각 계층의 위협요소를 분석하여 이러한 위협요소를 방어할 수 있는 기능이 탑제된 제품을 의미하게 된다. 그러나, 현재 출시되어 있는 보안제품들은 이러한 계층별로의 위협요소를 완벽하게 방어하지 못하고, 각 계층별로 처리하는 보안기능, 처리하지 못하는 보안기능이 있다. 본 절에서 정의하는 '계층에 따른 분류'에서는 각 보안제품들의 기능을 계층별로 파악하고자 한다. 파악된 정보를 이용하여 보안제품맵에 적용하여, 현재 출시되어 있는 보안제품들이 OSI 계층별로 어느 계층에서 어떠한 기능을 하는지 분석하고자 한다. 예를 들면 방화벽의 경우, 출시된 모든 제품이 OSI 7계층 전반에 걸쳐서 보안기능을 수행하지는 않는다. 따라서, 본 과제에서는 출시된 방화벽제품의 계층별 기능을 파악하여 제품맵에 나열하면, 각 제품별로 어느계층에서 장/단점(처리/미처리)이 있는지 쉽게 파악할 수 있다. 결국, 해당제품의 부족한 부분이 무엇인지를 파악하여 향후 부족한 부분을 중점 투자하여 개발할 수 있다.

장점 : 각 계층별로 어떠한 보안제품이 어떠한 기능을 하는지 한눈에 파악할 수 있다.

3.2 보안기능에 따른 분류

현재의 보안기능들을 나열하여 보고, 각 보안 기능에 따른 제품군의 종류와 각 보안기능에 어떠한 제품과 어떠한 계층에서 보안기능 역할을 하는지 파악한다.

근거 : 보안 기능은 많이 있다. 인가, 인증, 암호화 등등,. 또한 방화벽에서 사용되는 인증과 IDS에서 사용되는 인증이 있다. 물론 개념은 같을 수 있지만, 사용하는 환경이나 방법에서는 차이가 있다. 그리고, 기존의 네트워크 환경에서 처리되는 인증에서 향후 변화되는 네트워크 환경에서 처리되는 인증으로 진화해야 한다. 따라서 '보안기능에 따른 분류'에서는 각 보안기능별로 어떠한 제품들이 있는지를 분석하고자 한다. 즉, '인증'이란 보안기능을 이용하는 제품들에는 어떻한 것들이 있는지 파악할 수 있게 된다. 또한 본 제품맵을 이용하면 향후 어떠한 기능으로 진화할 것인지와 현재의 트랜드를 분석가능 하다.

장점 : 특정 보안기능이 어떠한 계층에서 역할을 하고, 이에 해당되는 제품에는 어떠한 것들이 있는지 파악하기 쉽니다

3.3 제품군에 따른 분류

분석할 때 가장 쉬운 방법이다. 보안 제품들을 그룹으로 묶어서, 각 제품군에 어떠한 제품들이 있는지 파악할 수 있다. 즉, 방화벽 제품군, 백신 제품군 등으로 분류를 하는 방법이다.

근거 : 일반 사용자관점으로 봤을때 가장 일반적인 분류 방법이다. 왜냐하면 일반 사용자들은 각 제품의 자세한 기능에 대해서는 잘 모르고, 단지 각 제품군의 역할만을 알고 있을 확률이 높기 때문이다. 따라서, '제품군에 따른 분류' 근거는 단순히 각 제품의 역할에 따라서 분류한 내용이다.

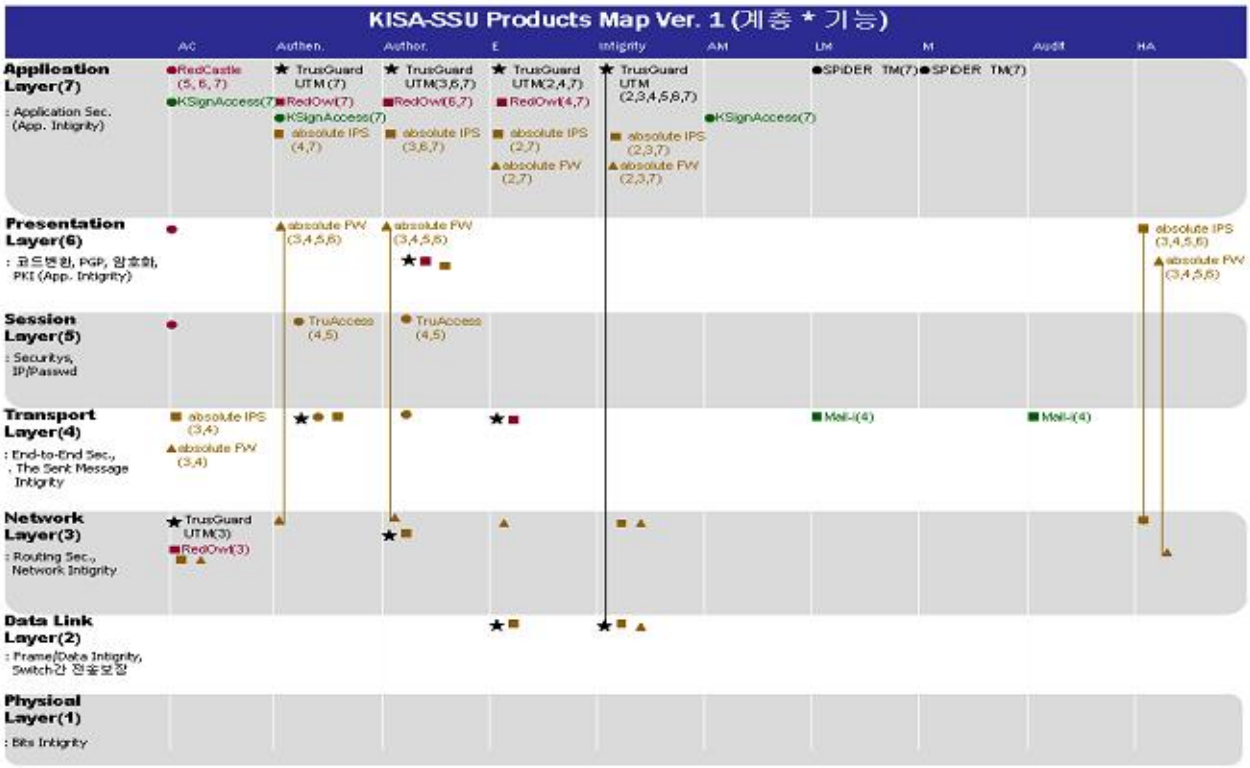

그림 1. 계층*보안기능*제품군을 이용한 맵 (*()안은 OSI 7계층에서의 역할)

장점 : 각 보안제품군들을 봄으로써 해당 제품에 어떠한 것들이 있는지 쉽게 파악할 수 있다

4. 정보보호 제품맵

4.1 계층*보안기능*제품군을 이용한 맵

맵 작성을 위하여 총 13개의 그룹군과 세부 5개의 제품씩 총 65개의 제품에 대해서 각 회사에 이메일을 통하여 정보를 수집하였고, 2007. 10. 13. 현재 15개의 제품들의 정보를 입수하였다. 이중 유효하다고 생각되는 정보는 7-8개 정도로 파악되고 있고, 계속 정보를 수집 중이다. 제품맵을 그리기 위해서 3개 Factor를 이용한다. 계층(왼쪽), 기능(위), 제품군(오른쪽)을 이용하여 작성한다. '계층(왼쪽)'에서는 OSI의 계층을 나열한다. 그리고, 보안 제품들이 각 계층에서 처리하는 보안기능을 표시한다. 보안기능의 정의는 '기능(위)'에서 정의하게 되며, 보안기능에 해당되는 보안 제품을 계층별로 나열하게 된다. '제품군(오른쪽)'에서는 각 제품군에 속해 있는 제품명을 정의하게 되며, 해당 제품들이 기능과 계층에 따른 역할의 위치를 파악할 수 있다[그림 1]. 예를 들어,

Ex1) 계층에 따른 보안 기능을 알고자 할때, 맵의 왼쪽에서부터 해당 계층을 찾아보면 쉽게 해당계층에서 처리하는 기능과 제품을 쉽게 파악할 수 있다.

Ex2) 기능에 따른 계층별 위치하고 이에 해당하는 제품을 찾고자 할때는, 위쪽의 기능을 찾아서 파악할 수 있다. 즉, 기능과 계층의 접속점에 있는 라인을 따라서 오른쪽으로 이동하여 보면 해당 제품들을 파악할 수 있다.

Ex3) 특정 제품이 어떠한 보안기능과 어떠한 계층에서 역할을 하는지 분석하고자 할때에는 오른쪽에서부터 왼쪽으로 찾아가면서 분석할 수 있다.

4.2 제품군에 따른 트렌드

본 연구에서의 제품군 분류는 총 13개로 구성되어 있다. 본 맵에서는 현재까지 분석된 내용을 이용하여 작성하였으며, 보안취약점 분석도구군(Group #5), 접근제어시스템군(Group #4)/침입탐지시스템군(Group #3), 통합보안시스템군(ESM, Group #1)으로 구성되어 있다[그림 2]. 보안기능은 오래전부터 사용되었지만, 이들을 활용한 보안 제품으로의 탄생은 1990년대부터 본격적으로 출시되었음을 볼 수 있다. 제일 먼저 인증/인가 등을 탑재한 방화벽제품이 먼저 사용됨을 볼 수 있다. 본 제품군의 경우 향후 다양한 제품의 단일화를 이뤄야 하는 과제를 안고 있다. 가장활발한 개발을 이루는 제품군에 속하기도 한다. 21세기 들어서면서, 통합보안 시스템군이 고개를 들기 시작했다.

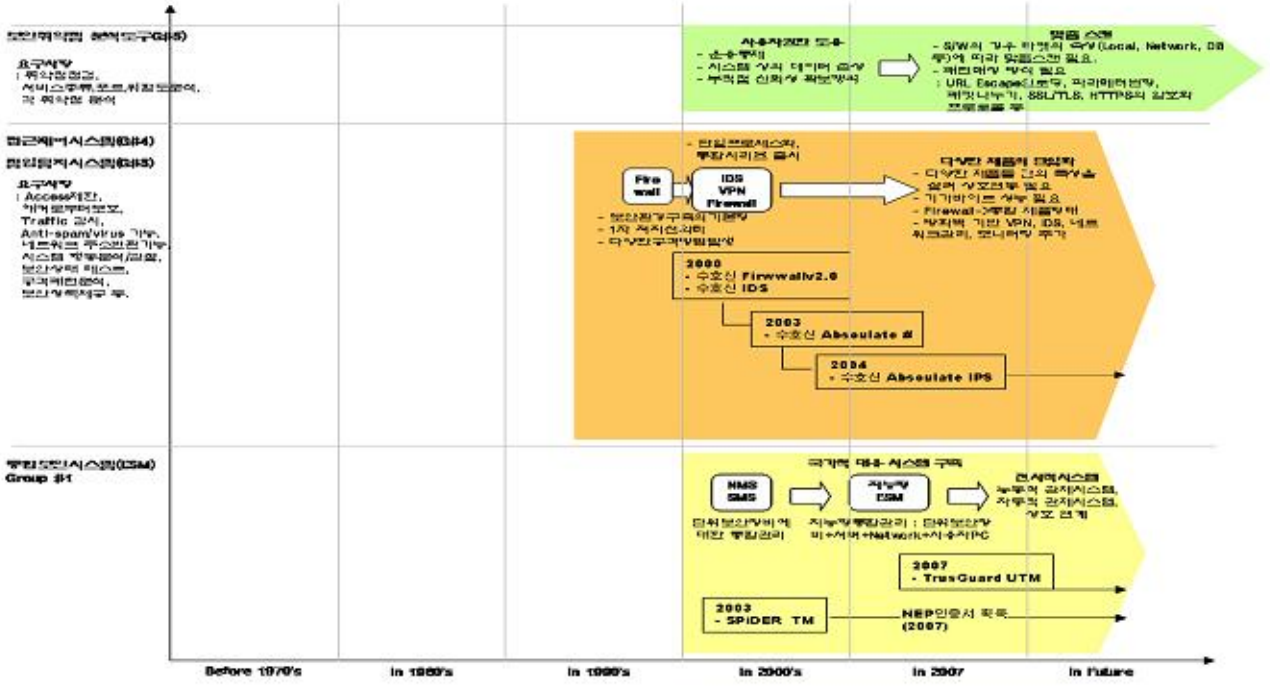

그림 2. 제품군에 따른 트렌드

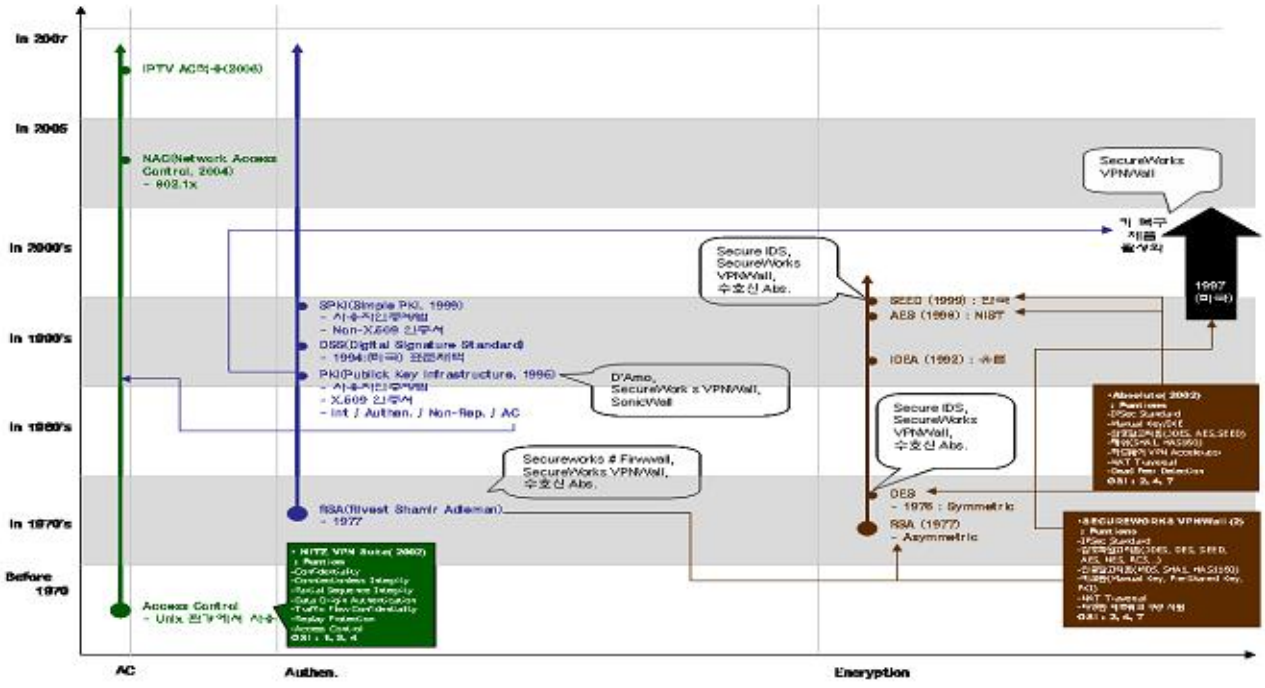

그림 3. 보안기능의 탄생시기와 제품관계

통합보안 군은 T*(검정별)와 S*(검정원)으로 2가지 제품을 담았다. 그림 1은 OSI 7계층에 따른 보안기능도 분석된 그림이다. T*의 계층별 기능을 살펴보면, AC(Access Control), Authen(Authentication), Author (Authorization), E(Encryption), Intigrity의 기능을 가지고 있음을 알 수 있다. 예를 들어 T*의 Authen에 대한 내용을 보면, Application Layer와 Transport Layer에서만 처리함을 알 수 있다. 같은 방법으로 Author.의 경우는 App. layer, Presen. layer 그리고 Network layer에서 인가기능을 처리함을 알 수 있다. 나머지의 제품들도 같은 방법으로 분석 할 수 있다.

즉 이러한 방식으로 분석하면서, 각 제품군 혹은 제품들이 어느계층에서 어떠한 보안기능을 하는지 파악할 수 있고, 향후, 어느 부분에 대해서 더 많은 개발을 해야 하는지 파악할 수 있다. [그림 3]의 보안기능의 탄생시기와 제품은, 현재까지 분석된 보안기능은 총 78여개가 된다. 각각의 기능에 대해서 언제 처음 탄생되었는지와 해당 기능이 언제 어느 제품으로 생산되었는지를 분석하기 위하여 작성하였다. 현재 그림에서는 3개의 기능을 이용하여 작성하였다.

5. 결론.

본 논문에서는 현재 개발되었고 활용/사용되고 있는 보안 제품을 기능에 따라 조사하였고, 어느부분에서 어떻게 사용되고 있는지를 조사하였다. 또한 각 보안 기능의 종류를 파악하였다. 그러나, 현재까지의 작업은 국내의 제품을 대상으로 조사하였고, 향후 국내는 물론 국외의 제품에 대해서도 조사하여 본 제품맵에 적용할 필요가 있다. 본 연구 결과로 생성되는 정보보호분야의 제품로드맵을 활용하면 향후 정보보호 제품의 기술 방향을 예측할 수 있어, 정보보호 제품 개발업체들의 향후 제품의 개발방향을 가늠할 것으로 기대된다.

[참고문헌]

[1] 염흥열, 2004년도 정보보호일반 표준화 로드맵, TTA, 2004.

[2] KISA, 정보보호 표준화 로드맵, 2004. 7.

[3] "Enterprise Smartphone Security: What to look for in end-to-end solution : White paper," Trust Digital, 2007.

[4] Alan Goode, "Mobile Data Protection," Juniper Research, 2006.

[5] John Girard, "Implementation advice for mobile data protection, 1H06," Gartner RAS Core Research, August 2006.