□ 기술해설 □

보안 제품에 대한 동향

아이에스케이(주) 박태완*

● 목 차 ●

1. 머리말
1.1 정보보호의 개념
2. 보안 제품 동향
2.1 하드웨어 보안 제품
2.2 운영체제 보안 제품
2.3 데이타베이스 보안 제품
2.4 응용 시스템 보안 제품
2.5 PC 보안 제품
2.6 네트워크 보안 제품
3. 맺음말

1. 머리말

최근의 해커 혹은 컴퓨터 관련 사고의 증가로 인하여 정보보호에 대한 관심이 증대되고 있으며 이로 인하여 보안 제품을 구매하고자 하는 욕구가 일어나고 있다. 따라서 여기서는 국내외의 보안 제품에 대한 동향을 소개해 보고자 한다.

보안 제품에 대한 동향을 소개하기 전에 보안 관련 제품들을 성격별로 분류하여 볼 수 있도록 정보보호의 개념 및 분야에 대하여 잠시 다루어 본다.

1.1 정보보호의 개념

1.1.1 정보보호(Information Security)의 정의

미국에서 널리쓰이는 정보보호의 정의는 "데이타 및 시스템을 고의적 혹은 실수에 의한 불법적인 공개(노출), 변조, 파괴 및 지체로 부터의 보호"이며 영국을 중심으로 한 유럽에서 널리 쓰이는 정의는 "전자적인 형태의 정보를 처리, 저장 및 통신의 모든 단계에 걸쳐서 보호하는 것" 이다.

또한 급변하는 정보 기술의 발달에 비례하여 정보보호의 주 대상도 변화되어 왔다. 전산부서의 영어 이름이 EDPS-DP-IS(Information Systems)-IT(Information Technology)부서로 발전되어 왔듯이 사실은 정보보호(Information Security)란 말도 Computer Security (1970년대)-Data Security(1980년대)-Information Security(1990년대)로 바뀌어져 온 것이다.

1.1.2 정보보호의 목표

정보보호의 정의인 "데이타 및 시스템을 고의적 혹은 실수에 의한 불법적인 공개(노출), 변조, 파괴 및 지체로 부터의 보호"에서 데이타 및 시스템을 고의적 혹은 실수에 의한 불법적인 공개로 부터의 보호를 한 단어로 표현해 보면 데이타 및 시스템의 "보안성(Confidentiality)"확보이며 데이타 및 시스템을 고의적 혹은 실수에 의한 불법적인 변조로 부터의 보호를 한 단어로 표현해 보면 데이타 및 시스템의 "무결성(Integrity)"확보 그리고 데이타 및 시스템을 고의적 혹은 실수에 의한 불법적인 파괴로 부터의 보호를 한 단어로 표현해 보면 데이타 및 시스템의 가용성(Availability)을 확보하는 것이다. 따라서 정보보호의 목표는 데이타 및 시스템의 보안성, 무결성, 가용성을 확

*비 회 원

보하는 것이다.

1.1.3 정보보호의 분야

전형적인 정보 시스템은 그림 1과 같은 층으로 구성된다. 따라서 정보보호는 각 층에 적절한 대책들이 구현되어야 하며 아울러 그 대책들이 모두 조화를 이루어 작동되어야만 효과적인 정보보호 체계를 이룰수 있다.

따라서 정보보호는 논리적으로 아래와 같은 관련 분야로 나누어 볼 수 있다.

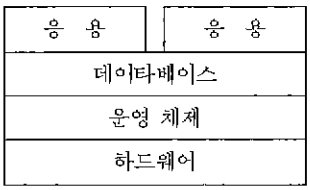

그림 1

가. 보안 관리(Security Management)

이 분야는 정보보호에 있어서의 관리적인 측면을 다루는 것으로 경영층의 입장에서 가장 경제적이면서도 효율적으로 회사의 정보 자산을 보호 하기 위한 조직의 역할과 책임, 정보보호 정책/표준/절차의 제정, 교육/훈련, 경영관리 등에 관한 사항을 다루는 분야이다.

나. 응용 시스템 보안(Applications Security)

예를들면 EDI , 전자메일, 전자 결재 시스템에서의 보안 기능을 다루는 것으로 특정 응용 시스템상에서 요구되는 보안 기능의 구현을 다루는 분야이다.

다. 데이타베이스 보안(Database Security)

데이타 베이스상에서 요구 혹은 구현 되어야 할 보안 기능들을 다루는 분야.

라. 컴퓨터 보안(Computer/Operating System Security)

예를들면, 유닉스 보안과 같이 특정 컴퓨터 혹은 O.S.상에서의 보안 기능을 다루는 분야로 기존의 상업적으로 사용되는 시스템 혹은 O.S.가 제공하는 보안 기능들에 대한 연구, 특히 이들의 사용 시에 어떠한 약점들이 있으며 이를 보강하려면 어떻게 하여야 하는지를 다루는 분야이다.

마. 네트워크 보안(Network Security)

네트워크를 통한 데이타의 전송에 관련하여 요구되는 보안 기능을 다루는 분야로서 근거리 통신망 보안, 무선 근거리 통신망, WAN상에서의 사용자 인증, 컴퓨터간의 인증, 암호화 등이 다루어 진다.

바. 개인용 컴퓨터 보안(Workstation/PC Security)

이 분야는 처음에는 컴퓨터 보안의 한 부분으로 다루어 졌으나 최근의 PC 및 노트북 컴퓨터의 보급 확산 그리고 바이러스로 부터의 위협 등으로 인하여 별개의 분야로 다루어 지기 시작하였다. 여기서는 주로 접근 통제, 컴퓨터 바이러스, 복제 방지, 자료 소거 등의 문제들을 다루고 있다.

사. 암호학(Cryptography)

정보보호의 목표중 보안성과 무결성을 확보하기 위한 기술적 대책으로 암호화 기술이 널리 쓰이고 있으며 이와 관련된 분야를 다루고 있다.

아. 물리적 보안(Physical Security)

주로 물리적인 접근 혹은 피해로 부터의 보호를 다루는 분야로 빌딩, 사무실에의 접근 통제, 또는 도범 혹은 불법 파업 중인 조합원 등으로 부터의 전산 시스템, 고가 장비 등의 분실내지는 손괴로 부터의 보호를 다루는 분야이다.

자. 보안 평가(Security Evaluation)

컴퓨터 업체들은 나름대로 자사의 컴퓨터가 보안성이 높다고 주장하고 있으나 이에 대한 객관적인 보안성 평가가 필요하게 되었으며 미국 정부는 이를 위해 기준(TCSEC, Trusted Computer Security Evaluation Criteria)을 만들어 이를 근거로 시스템을 평가하고 있으며 유럽은 독일의 기준을 근간으로 나름대로의 기

준(ITSEC, Information Technology Security Evaluation Criteria)을 만들어 사용하고 있으며 주로 이와 관련된 분야를 다룬다.

차. 법적/윤리적 문제(Legal/Ethical Issues)

정보보호란 기술적인 대책 만으론 해결이 불가능하며 부정 경쟁 방지법, 통신 및 기타 컴퓨터 범죄 관련법 등과 관련된 법적 그리고 윤리적인 접근 또한 중요한 것으로 이를 다루는 분야이다.

2. 보안 제품 동향

보안 제품들은 앞에서 언급한 각 층으로 분류하여 볼 수 있으며 또한 수행하는 기능에 따라 사용자 인증용, 암호화용 등으로 나누어 볼 수도 있다. 특히 최근에는 앞에서 언급한 각 층에 걸쳐서 보안 기능을 수행하는 제품들이 선을 보이고 있으나 대부분의 보안 제품들은 앞에서 언급한 각 분야별로 나누어 볼 수 있다.

2.1 하드웨어 보안 제품

하드웨어 보안 제품들 중 외국에서 가장 널리 사용되고 있는 것은 고가의 워크스테이션 등을 도난으로 부터 보호하기 위하여 물리적으로 책상 등에 고정시킬 수 있는 제품 그리고 불법적 자료의 복사 및 유출을 방지하기 위하여 디스켓 드라이브에 열쇠를 채울수 있는 제품 등이 있다.

2.2 운영체제 보안 제품

운영체제 보안 제품들은 주로 기존의 운영체제가 제공하는 보안 기능들이 사용자의 요구조건을 만족하지 못하여 이를 보완해주는 것들로서 IBM 대형 시스템에 널리 쓰이는 RACF, ACF2, Top-Secret 등이 있고, 유닉스 환경에는 BoKs, Cybersafe, Unicenter 등이 있으며 이와 유사한 제품들이 모든 운영체제에 걸쳐서 있다.

2.3 데이타베이스 보안 제품

현재 기존에 널리 쓰이는 데이타베이스에는 이미 우수한 보안 기능들이 제공되고 있으며 따라서 이 기능들을 이용하여 상당한 보안 수준을 달성할 수 가 있다. 그러므로 운영체제 보안 제품들 같이 추가의 보안을 향상시켜주는 제품들은 없는 실정이다. 그러나 유일하게 오라클사에서는 자사의 오라클 데이타베이스의 보안성을 높인 Trusted Oracle이라는 제품을 선보이고 있다.

2.4 응용 시스템 보안 제품

응용 시스템 보안 제품군에는 다양한 제품들이 있다. 대표적인 것으로는 응용 시스템 상에 보안 기능을 구현할 수 있는 툴들이 여기에 속할 것이다. 예로는 응용 시스템상에 소프트웨어만으로 전자서명 기능을 제공할 수 있는 개발자용 툴이 있으며, 암호화 기능을 제공하는 하드웨어와 이를 응용 시스템과 연결시켜줄 수 있는 API를 제공하는 제품이 있다. 또다른 제품으로는 EDI 상에서 요구되는 보안 기능을 제공하는 서버의 역할을 하는 제품들도 있다. 이외는 미리 특정 응용 시스템에 보안 기능을 추가하여 보안성을 높인 제품이 있으며 이것의 대표적인 예가 PEM(Privacy Enhanced Mail)으로서 인터넷상에서 전자메일을 암호화하여 주고 받으므로서 보안성을 확보한 것이다.

2.5 PC 보안 제품

PC 보안에는 크게 바이러스, 접근 통제, 불법복제 방지의 3가지 이슈가 있으며 따라서 이 세가지 위협에 대응하는 다양한 보안 제품들이 선보이고 있다.

바이러스에 대한 대책으로는 항-바이러스 프로그램들이 있다. 항-바이러스 프로그램은 Virus non-specific (checksumming software)과 Virus specific(scanning software)으로 나누어 볼 수 있다.

Checksumming 소프트웨어는 PC 상의 모든 실행 파일의 checksum을 계산하여 보관하다가 만약 실행 파일에 쓰기 명령이 나타나면 다시 checksum을 계산 비교하여 틀릴 경우 경보를 보내는 것으로 전제 조건이 최초의 checksum 계산시 바이러스에 감염되어 있지

않아야 한다. 이 방법의 단점은 업 그레이드 등에 의한 실행 파일의 변경시마다 cheksum을 재 계산해 주어야 한다. 장점은 바이러스에 감염되기 전에 감지할 수도 있다는 것이다.

Scanning 소프트웨어는 알려진 바이러스에 대한 특징(주로 10~16 바이트의 바이러스 고유의 값)을 모든 실행 파일과 비교하여 그 특징이 있는지를 확인하는 것이다. 이것의 단점은 이미 감염된 후에 발견되며, 또한 바이러스의 특징이 알려진 것에 한하여 발견될 수 있으며 정기적으로 새로운 바이러스의 특징들을 보완해주어야 한다. 이 프로그램은 주로 외부로부터 입수된 디스켓의 검사에 효과적이다.

최근의 한국은행 하드디스크 도난 사고에서도 볼 수 있듯이 현재 PC의 취약점은 PC 사용에 대한 접근을 통제할 수 없다는 것이다. 접근 통제에 관련된 제품에는 최소한 사용자 인증 기능, 암호화 기능, 로그 기능 등이 제공되고 있으며, 소프트웨어만으로 구성된것 혹은 Add-on Card 형태의 하드웨어로 구성된 것들이 있다.

접근 통제에 관련된 또 다른 하나의 제품은 파일의 완전 소거(secure delete)를 위한 제품으로 이것은 DOS 상에서의 파일의 소거(delete)는 실제로는 파일 이름의 첫자를 소거하는 것으로 Undelete나 유틸리티 등으로 복구가 가능하다는 것은 주지의 사실이다. 위의 Undelete나 유틸리티의 사용으로 실수로 인해 소거된 파일의 복구에 아주 유용하게 쓰이나 반대로 비밀성을 요하는 문서 파일을 소거하고자 할 경우에는 이것이 문제가 된다.

민감한 파일의 확실한 소거를 위하여 외국에서는 파일 소거용 프로그램(예 ; "Secure-delete")이 널리 사용되고 있는데 이 프로그램으로 소거 명령을 하면 파일의 이름 뿐만 아니라 실제 파일이 기록되어 있는 장소를 찾아 가서 그 위에 무작위로 발생시킨 문자를 여러번 기록(overwrite)하는 것으로 다시 복구할 수 없을 뿐만 아니라 유틸리티를 이용하여 섹터별로 불러 보아도 알 수 없는 문자가 기록되어 있을 뿐이다.

불법복제 방지에는 두 가지 상충되는 관점이 있다. 기술적인 대책을 이용하여 불법 복제를 막고자 하는 측과 이로 인하여 불편함을 감수해야 하는 합법적 사용자 측이다. 이에 따라 일부 소프트웨어 회사들은 법적인 대응만을 사용하는 경우도 있다.

불법복제 방지 제품으로 널리 쓰이는 것은 하드웨어 접근방법으로 프로그램 실행시 프린터 포트에 연결된 dongle이라는 하드웨어가 특정 값을 제공해 주어야만 프로그램이 실행되게 해주는 것과 소프트웨어적인 접근 방법으로 프로그램이 실행되는 시스템의 환경을 이용하는 것으로 이것의 대표적인 예가, 하드디스크 상의 마지막 섹터에 특수한 표시를 하여 프로그램의 실행시 마다 그 표시의 존재 여부를 확인하는 것이다.

2.6 네트워크 보안 제품

네트워크 보안 제품에도 다양한 것들이 있으며 특히 OSI 7 Layer모델 상에서의 어느층(layer)에 보안 기능을 구현하였는가에 따라 사용자의 관점에서 장.단점이 있다. 예를들면, 하부층(low layer)에서 구현된것으로 하드웨어적인 접근을 하는 제품은 사용자의 입장에서는 응용 시스템의 변경없이 보안 기능을 제공받을 수 있으며 상부층(high layer)에서 구현된 것일수록 응용 시스템에 변경 혹은 그 제품의 운영에 많은 노력을 기울어야 한다. 이것의 예로는 인터넷의 방화벽 제품들(Firewall-1, Black Hole, Gauntlet 등)을 들 수 있다.

3. 맺음말

보안 제품들에 대한 수요의 증가로 인하여 다양한 제품들이 선을 보이고 있으나 최근 여기에는 크게 두 가지 추세가 있는듯 하다.

첫째는 보안 기능만을 제공하는 Add-on 개념에서 미리 각 응용 시스템 소프트웨어상에 보안 기능을 삽입하여 소개하는 것으로서 최근에 Lotus Notes와 Novel Netware에 보안성을 크게 향상시킨 새로운 버젼을 소개하였다. 따라서 제삼의 회사 제품으로 보안성을 향상시켜주는 제품들은 점점 적어지고 있으며 대신에 응용 시스템상에 보안 기능을 삽입할 수 있는 개발 툴들에 대한 수요가 증대되고 있다.

두번째는 새로운 개념 혹은 기술을 적용한 제품들이 선을 보이고 있는 것으로 이것의 예로 사용자 인증에 사용자의 위치 데이타를 이용하는 것이다.

현재까지의 사용자 인증 메카니즘으로 널리 사용되어 온 것은 사용자가 알고 있는 것을 이용한 경우(예 ; 패스워드), 사용자가 가지고 있는 것을 이용한 경우 (예; 마그네틱 카드) 그리고 사용자의 신체적 특징을 이용한경우 (예 ; 지문, 목소리)이다. 그러나 이중 어느하나도 완벽한 보안성을 제공하지 못하고 있다. 예를들면, 패스워드는 추측 또는 알려지기가 쉽고, 마그네틱 카드는 분실 혹은 도난 당할 수 있으며, 보안성이 상대적으로 높은 신체적 특징을 이용한 경우에도 그 데이타의 도청(interception), 재생(replay) 등의 공격에 취약하다. 따라서 이와 같은 문제점들을 극복하기 위하여 최근에 미국에서 연구가 진행되고 있는 것은 사용자의 위치 데이타를 이용한 사용자의 인증이다. 사용자의 위치 데이타란 시스템 접근시 위치한 사용자의 경도, 위도, 고도를 근거로 사용자의 접근을 허가하는 것이다. 만약 이 시스템이 이미 실용화되어 있었더라면 최근에 일어난 러시아의 해커가 아르헨티나에 있는 은행인 척하여 미국의 시티 은행으로 부터 거액의 자금을 이체시킬 수는 없었을 것이다.

궁극적으로 정보보호는 관리적인 문제이지 기술적인 문제가 아니며 따라서 보안 제품의 구매, 설치만으로는 결코 성공적인 정보보호를 달성할 수 없음을 명심하여야 하며 암호화 등의 기술적인 접근에 반드시 인식재고를 위한 교육 등의 관리적인 접근이 병행되어야 한다.

박 태 완

1981.2 울산 공과대학 전산학과 졸업
1982~1987 홍콩상하이은행 부산/서울지점, 전산책임자
1987~1989 하이얏트 리젠시 부산, 전산실장
1989~1991 내쇼날호주은행 서울지점, 전산실장
1992~1993 영국 런던대학 공학석사(정보보호 전공)
University of London, Royal Holloway College
Master of Science(MSc) in Information Security
1994~1995 아이에스케이 대표
현재 아이에스케이(주) 이사 (컨설턴트), 공인 정보 시스템 감사사(미국), (CISA, Certified Information System Auditors), CERT-Korea 자문위원, 한국 전산원, 보안 표준 위원