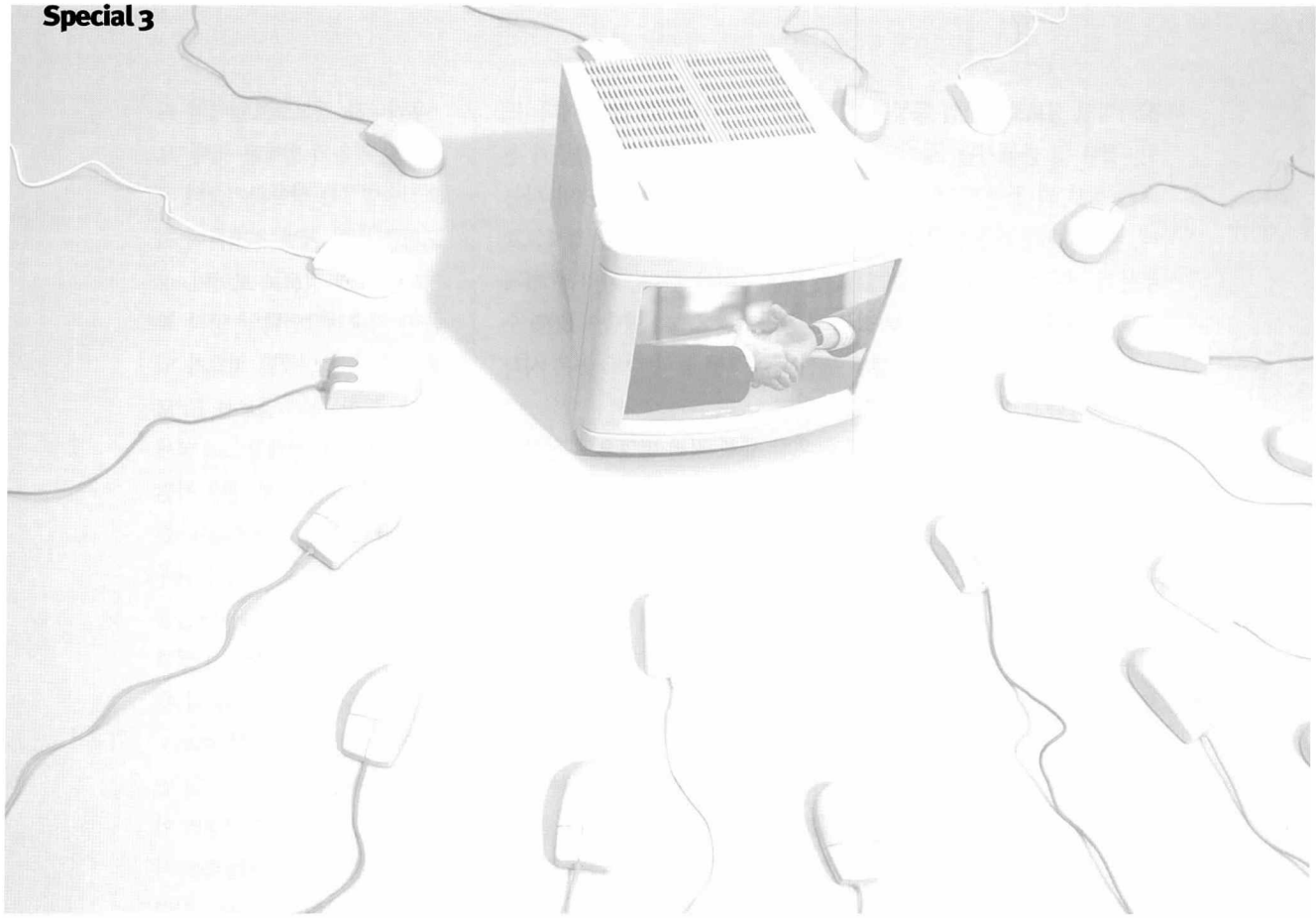


임송환 | (주)한국전자인증

정보보호 기술 동향

1. 들어가는 말

기술의 진전과 소비자 수요가 늘어남에 따라 정보화사회가 구현되었으나, 정보의 무단 해킹, 온라인 상에서의 내용부인, 사용 방해 등 정보통신시스템 자체의 안전이나 개인의 프라이버시, 또는 건전한 전자상거래 등을 위협하는 요소들이 나타나고 있다. 이에 따라 이를 해결, 극복하고 온라인상에서 안전하게 정보를 주고 받을 수 있도록 하는 정보보호산업이 등장하게 되었고, 2000년 말 58억달러 규모였던 세계 정보보호 시장은 2005년에는 210억 달러로 매년 약 30%씩의 성장[1]이 예상될 정도로 그 중요성과 규모 면에서 주목받고 있다. 정보보호란 온라인상에서 정보의 기밀성과 무결성을 유지하고 시스템의 가용성을 보장하는 것을 말하는데, 여기에서는 크게 정보보호의 세 가지 분야– 암호/인증, 바이러

1) IT 정보센터, 주간기술동향 통권 1024, 2001.11. 2.

스 백신, 네트워크 보안의 개요와 동향에 대하여 살펴 보기로 한다.

2. 암호/인증

- 암호(Cryptography)

암호화 기술은 거의 모든 정보보호기술의 기반이 되는 기술이며 인가된 사람만이 보유하고 있는 정보를 이용하여, 보호하고자 하는 자료를 임의로 변형하여 인가되지 않은 자에 대하여 아무런 정보도 노출시키지 않는 기술이다. 암호화 기술을 구현하기 위한 방법은 사용되는 키에 따라 암/복호화 키가 같은 대칭키 암호화(Symmetric Key Cryptography)와 암/복호화 키가 서로 다른 비대칭키 암호화(Asymmetric Key Cryptography)로 나누어진다.

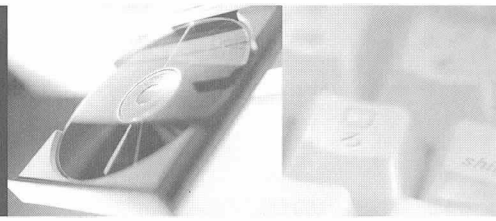
비대칭형 암호 알고리즘의 경우 현재 상업적으로 사용하기위한 안전한 키길이는 128bit 이상인 알고리즘을 사용하고 있는데, 64bit의 키길이를 가지는 DES(Data Encryption Standard)를 세 번 적용하여 키의 길이를 증가시킨 3DES가 대표적이다. 그러나 1998년을 기점으로 NIST(National Institute of Standards and Technology)가 정한 DES의 표준 기한이 만료되어 향후에 사용될 수 있는 차세대 암호 표준(AES : Advanced Encryption Standard)을 공모하여 벨기에에서 제안된 RIJNDAEL이 선정되었으며, 우리나라에서는 키길이 128비트인 SEED가 국내 표준 비밀키 알고리즘으로 현재 다양한 분야에 이용되고 있다.

공개키 암호 알고리즘은 비밀키 암호 알고리즘에 비해 속도가 느린 반면 키분배가 용이한 장점이 있으므로 데이터의 암호화보다는 대칭키 암호화를 위한 키교환이나 전자서명에 주로 이용되고 있다. 현재 가장 널리 이용되고 있는 공개키 암호 알고리즘인 RSA는 빠른 시간내 해독의 가능성과 512bit에 대한 비보안성에 대한 인식으로, 상업적인 목적의 안전한 보안을 위해서는 1,024 혹은 2,048bit까지의 키길이를 이용할 것을 권장하고 있다. 그러나 키길이의 증가에 따른 H/W, S/W적인 비효율성의 문제가 생기므로 RSA보다 훨씬 짧은 키길이로도 동일한 안전성을 제공하는 타원곡선암호(ECC:Elliptic Curve Cryptograph)방식이 대안으로 대두되었고 다양한 환경에서의 적용을 위한 연구가 진행중이며, 이미 일부 분야에서는 적용이 되고 있다.

〈동등한 보안성을 제공하는 암호화 키길이 비교[2]〉

ECC	RSA
160 bit	1,024 bit
224 bit	2,048 bit
256 bit	3,072 bit
384 bit	5,360 bit
512 bit	

온라인 상에서 안정하게 정보를 주고 받을 수 있도록 하는 정보보호산업이 등장하게 되었고, 2000년 말 58억달러 규모였던 세계 정보보호 시장은 2005년에는 210억 달러로 매년 약 30%씩의 성장이 예상될 정도로 그 중요성과 규모 면에서 주목받고 있다.



- 인증(Authentication)

인증 기술은 온라인이라는 비대면의 환경에서 시스템에 접근하고자 하는 사용자나 통신 주체의 진위여부를 확인할 수 있는 기술로써, 아는 것을 통한 인증, 소유하고 있는 것을 통한 인증, 개체의 특징을 이용한 인증으로 구분될 수 있다. 아는 것을 통한 인증은 패스워드를 이용하는 단방향 인증, 일회용 패스워드를 이용하는 양방향 인증 등이 있으며, 소유하고 있는 것을 통한 인증은 스마트카드, IC 카드, 개인용 토큰 등을 이용하며 개체의 특징을 이용

2) 기술정보센터, 주간기술동향 통권 916호, 1999. 10.

한 인증은 지문이나 성문 또는 홍채인식을 이용한 생체 인증 기술로 최근 활발히 연구되고 있는 영역이다.

ITU(International Telecommunication Union)에서는 인증에 대한 표준으로 X.509를 제정하였으며, IETF(Internet Engineering Task Force)에서는 PKIX(Public Key Infrastructure(X.509))라는 Working Group을 결성하여 공개키 기반의 인증시스템에 대한 표준화 작업을 추진하고 있다. 또한 전자서명 등 공개키 암호화 기술의 활용에 대해서는 RSA사에서 제안한 PKCS(Public-Key Cryptography Standards)가 사실표준으로 수용되고 있다.

세계 인증시장은 BTB에 강점을 보이고 있는 Entrust와 BTC에 강점을 가지고 있는 VeriSign이 양분하는 양상을 보이고 있으며, 이중 현재 국내에는 VeriSign만이 국내업체를 통해 자체 솔루션을 공급하고 있다. 한편, 우리나라에서도 전자서명법의 제정과 전자정부를 위한 정부의 정책으로 한국정보보호진흥원을 최상위 인증기관으로 하는 자체 인증체계를 갖추어 인터넷 뱅킹, 사이버 주식거래, 전자입찰 등 다양한 분야에 적용되고 있으며, 더욱 더 확산되어가는 추세를 보이고 있다. 반면에 국가간의 상호 인정 문제와 6개 인증기관 상호간의 연동 문제는 여전히 풀어야할 숙제로 남아있다.

3. 바이러스 백신

P2P, 네트워크 등 다양한 기술을 응용하여 빠르게 확산되고 다양한 형태를 취하는 바이러스의 등장에 따라 바이러스의 패턴에 근간한 검사 기술에서 출현 가능한 바이러스에 대한 검사를 위한 기술들이 AV(Anti-Virus)업계에서 활발히 연구 및 개발되고 있다. AV관련 기술에 있어 국내 기술 수준은 주요 기술에 대해서는 기 보유하고 있으며 일부는 현재 개발 중에 있는 상태이다. 현재 시장에서는

〈AV관련 주요기술 및 특성[3]〉

기 술	설 명	국내수준
Signature-based Scanning	- 기 분석된 바이러스의 패턴이나 "masks"를 기반으로 바이러스를 검사하는 기술 - 알려진 바이러스를 검사하고 치료하는데 있어 강점이 있는 기술임	기술보유
Heuristic Analysis	- 바이러스 또는 악성코드와 관련이 있는 것으로 알려진 기능이나 행위에 대한 분석을 바탕으로 알려지지 않은 바이러스도 발견해 낼 수 있는 기술 - 통계를 바탕으로 바이러스 "감염가능성"에 대해 판단하므로 잘못된 판단을 내릴 가능성이 존재함	개발중 (일부보유)
Vaccination Technology	- 응용 프로그램을 수정하여 자가 진단할 수 있는 코드를 삽입하는 기술로 프록램의 순서 등이 바뀌었을 때 감염 가능성을 파악하는 기술 - 부트 섹터 바이러스 등 응용 프로그래머에게 제어가 넘어오기 이전 단계에서 감염되는 바이러스에 대해 처리불가	기술보유
Snapshot Technology	- Critical한 정보에 대한 로그를 주기적으로 스냅샷을 떠 바이러스 또는 악성코드의 존재 여부를 검사하는 기술 - 구현 방법의 어려움으로 안티바이러스 분야에서는 많이 사용되지 않으나 IDS 등 시스템 Audit을 중요시하는 분야에 적용됨	기술보유
Sandbox Technology	바이러스가 의심스러운 코드를 샌드박스에서 실행하면서 코드의 영향을 모니터링하여 바이러스 여부를 검사하는 기술	개발중 (일부보유)
Behavior Blockers	메모리에 프로그램을 상주시켜 MBR에 대한 쓰기, TSR(Temminate-and-Stay)프로그램으로 등록 등을 검사하여 잠재된 바이러스의 위험으로 등을 경고하는 기술	개발중

3) 한국정보보호산업협회, 2002년 정보보호산업동향, 2002. 10.

단순 AV외에 타 보안기술과의 통합제품의 요구가 점차 늘어나고 있는데, 이는 최근 바이러스의 감염 경로가 복잡해짐에 따라 IDS, Firewall, PC보안 등 타 보안 제품과의 통합제품을 선호하게 된 것으로 보인다. 따라서 앞으로의 바이러스 백신은, 잘 알려지지 않은 바이러스의 탐지 기술 개발과 중앙 집중형 관리 시스템 개발 및 서버 및 네트워크용 제품을 강화하는 방향으로 발전될 것으로 보인다. 한편 현재 AV와 관련하여 국내에는 별도의 교육기관 및 교육과정이 없어 회사 차원에서 자체적인 커리큘럼을 통해 인력을 양성하고 있으므로 신규 인력의 AV업계 진입 장벽이 높은 편이다.

4. 네트워크보안

대체적으로 방화벽 분야에서는 해외 기술 보유 보안 업체들이 국내 업체보다 오랜 연혁과 노하우를 가지고 있어 방화벽 기술은 해외 선진 기술에 비해 다소 미흡한 것으로 평가되고 있으나, 침입탐지시스템 기술은 해외 선진 기술과 대비해 매우 우수한 것으로 나타나고 있다.

솔루션 업체들은 전체 정보보호시장의 버팀목이었던 금융, 공공시장을 겨냥해 기존 제품의 속도 향상을 포함한 성능 개선과 함께 하드웨어 기반의 통합제품 출시에 나서고 있다. 네트워크 정보보호 솔루션은 하드웨어 기반의 '통합화'와 '기가비트화'로 대변되는 추세에 맞춰 발빠르게 움직이고 있다.

4-1 방화벽

방화벽 시스템은 기관의 보안 정책에 따라 인가된 인터넷 서비스에 대한 액세스는 허용하고, 인가되지않은 서비스에 따르는 트래픽을 철저하게 막음으로써 효율적인 보안 서비스를 제공하도록 한다. 물론 이 방화벽 시스템을 구현하는 것이 기관의 보안을 완전하게 보장하지는 않지만, 가장 효과적이고 비용이 비교적 적게 드는 방법이라고 할 수 있다.

- 방화벽 시스템을 구축하는 두 가지 유형

a. 네트워크 레벨(Network Level) 방화벽 시스템

낡은 방식의 네트워크 레벨의 방화벽을 제공하는 단순한 라우터는 어떤 패킷이 동작하며, 어떤 네트워크에서 왔는지를 판단하기 어렵지만, 현재의 네트워크 레벨 방화벽은 매우 복잡해져서 허용된 접속들의 상태와 어떤 종류의 데이터 내용 등을 관리할 수 있다. 한가지 중요한 차이점은 네트워크 레벨 방화벽이 라우트를 직접 제어할 수 있으며, 할당된 IP 블럭을 정당하게 사용할 수 있도록 해준다는 점이다. 네트워크 레벨 방화벽은 매우 빠르며, 사용자에게 투명한 서비스를 보장한다.

b. 응용 레벨(Application Level) 방화벽 시스템

TIS 툴킷 등에 구현된 것과 같은 초기 응용 레벨 방화벽은 일반 사용자에게 투명하지도 않으며, 어떤 연습이 필요하지만, 최근의 응용 레벨 방화벽은 투명성이 보장되며 보다 상세한 감사 보고와 네트워크 레벨 방화벽보다 보다 안전한 보안 모델을 제공하고 있다.

향후의 방화벽 시스템은 네트워크 레벨과 응용 레벨 방화벽의 혼합형에 해당된다. 이는 네트워크 레벨에서는 보다 상위의 기능을 가지려 하고 응용 레벨에서는 보다 하위 기능을 갖고자 하기 때문이다. 결국에는 매우 빠른 패킷 스크린 기능과 모든 트래픽에 대한 로그와 감사 등이 예측되며, 특히 네트워크를 통해 전달되는 트래픽의 보호를 위해 암호 기법이 사용될 것이다.

4-2 VPN

가상 사설망(Virtual Private Networks:VPN)이란 PSTN (Public Switched Telephone Network), ISDN(Integrated Services Digital Network), ADSL(Asymmetric Digital Subscriber Line) 같은 망서비스 사업자의 공중망이나 인터넷을 자사의 WAN(Wide Area Network) 백본처럼 사용하는 네트워크를 말하며, 이러한 개념은 지

난 수년간 인터넷의 급격한 성장에 따라 급속히 발전해 왔다. VPN을 이용하면 기업의 본사와 지사, 또는 지사간의 원거리 통신망을 저렴한 비용으로 구축할 수 있으므로 기업 마케팅이나 영업활동에 있어서 최소 비용으로 최대 효과를 낼 수 있는 기반이 되고 있다.

VPN을 구성하는 기반 기술로는 터널링 기술, 키 관리 기술, VPN 관리기술 등이 있으며, 이외에 VPN을 구현하기 위해서는 인증 및 암호화 기술이 필요하며, 부가적으로 라우터나 방화벽에서 제공하는 일부 보안 기술도 병행하여 VPN을 구성할 수 있다. VPN 구성에 있어서는 특히 상호운용성, 확장성, 가용성 측면이 강조되고 있는데, VPN 구현과 관련된 주요 이슈로는 최신 보안 모델의 변화 움직임, 하드웨어 기반 암호화 기술의 구현 가능성, MPLS(Multiple Protocol Label Switching) VPN과 IPSec VPN의 적절한 이용을 통한 전체 VPN 서비스 망 구축 추진 방안 등이 검토되고 있다. VPN과 관련한 새로운 기술들의 목표는 보안성 증진과 상호운용성, 확장성, 안전성 및 관리상의 문제개선에 있으며, 인터넷 기반의 엑스트라넷 VPN을 지향하여 보안성과 QoS(Quality of Service)보장에 중심을 두고 있다. 최근 들어 네트워킹 분야에 있어서 주요 핵심 이슈 가운데 하나로 등장하고 있는 IP VPN이 향후 전체 기업 네트워킹에서 가장 중요한 분야가 될 것으로 보이는데, 이는 인터넷 보안기능을 적용하여 공중망을 전용선처럼 사용할 수 있는 장점을 갖고 있기 때문이다. 그리고, 향후 IP 기반의 VPN은 방화벽, 라우터, ATM 스위치, 다중 서비스 플랫폼 등 수많은 다른 네트워킹 기술 및 장비들과 통합되어 보다 향상된 기능을 전개할 것으로 예상된다.

5. 맺는말

이상 정보보호 기술의 몇 가지 분야에 대해 간단히 살펴보았다.

전체적으로 최근 정보보호 솔루션의 발전 방향은 크게 5가지 정도로 정리할 수 있는데, 첫째 S/W기반에서 H/W기반으로의 변화이다.

S/W기반의 솔루션은 빠르게 좋아지고 있는 네트워크환경을 미처 따라가지 못하고 있으므로 제품의 퍼포먼스 향상을 위해 H/W 기반의 방식으로 이동하고 있으며, H/W의 대량생산으로 가격인하를 이루어 솔루션 도입 자체를 확산시키는 방향으로 이루어지고 있다.

둘째로는 각각의 단위제품에서 통합보안관리(ESM:Enterprise Security Management)로의 변화이다. 이는 각각의 세부분야에서 비교우위를 보이는 서로 다른 기종의 솔루션들로 이루어진 시스템의 상호 연동을 용이하게 하며, 하나의 console을 이용한 관리의 용이함을 제공할 수 있다는 측면에서 환영받고 있다.

세번째는 기업용 시스템뿐 아니라 개인 PC에 대한 보안인식이 확산됨에 따른 솔루션의 개발이다. 현재, 그리고 추후에 사용될 PC는 과거와는 비교도 되지 않을 정도의 성능을 가지고 있고 이를 이용한 다양한 기능의 구현, P2P 통신의 확대, 초고속 인터넷망의 확산으로 인해 이제 PC도 해킹의 대상이되고 있는 것이 현실이며, 이에 대비한 보안 솔루션의 연구, 개발이 이루어지고 있으며, 더욱더 확산될 것이다.

마지막으로 공통평가기준(CC :Common Criteria)을 비롯한 관리 인증이 중요하게 부각되고 있다는 것이다.

국산 솔루션과 외국의 솔루션과의 경쟁이 불가피한 상황에서 국내의 평가기준만으로 솔루션을 평가하는 것은 자칫 국수주의나 우물안 개구리와 같은 결과를 초래할 수 있다. 이에 국제적으로 통용될 수 있는 국제공통평가기준을 통한 솔루션의 평가를 통해 국내 솔루션과 해외의 솔루션의 자율경쟁에 대비해야 할 것이다.

또한, 이제는 어떤 솔루션이 좋고 나쁨보다 그 솔루션의 도입 필요성을 인식하고 그에 대한 관리적인 전체적 플랜을 수립하고 그 플랜 자체를 평가받는 관리 인증이 이슈로 등장하고 있다.