□정보산업동향□

네트웍 및 애플리케이션 보안

김 형 만†

◈ 목 차 ◈

1. 파이어월

국내에도 불어닥치기 시작한 인터넷 열풍이 최근 들어 그 열기가 한층 달아오르고 있다. 인터넷이라는 '정보의 보고'로부터 최신 정보를 얻으려는 인터넷 접속자가 해마다 늘고 있으며, 기업 차원에서는 원활한 정보의 상호교환을 통해 기업의 경쟁력 향상과 이미지 제고를 목적으로 자체 내부망(프라이빗 네트웍)을 외부망인 인터넷에 연결하려는 움직임이 활발해지고 있다.

현재 인터넷의 수요는 전세계적으로 3-4천만명에 이르고 있으며, 매년 25%의 지속적인 성장세를 보이면서 2000년경에는 8억 이상의 인구가 인터넷에 접속하게 될 것이라는 통계도 나오고 있다. 이렇듯 인터넷 열풍에 편승, 한편에서 급부상하고 있는 것이 바로 보안 솔루션이다. 외부와의 접속이 일반화되면서 사용자들로 하여금 그 어느 때보다 보안의 중요성과 필요성을 동시에 일깨우는 결과를 초래하고 있다.

세계와 단절되지 않기 위한 외부와의 연계는 필연적이지만 외부 접속시 발생하게 될지도 모르는 불법침입자의 해킹 위협이 뒤따르기 때문에 업계의 한 관계자는 인터넷을 '필요악'이라 지칭하기도 한다.

인트라넷 기본 요소로 자리매김

인터넷이라는 외부망을 이용, 산업 스파이나 정체를 알 수 없는 인터넷 해커 등의 불법 침입에 의해 어느 기업의 귀중한 정보가 유출되었다고 하자. 회사의 기밀사항이 경쟁사에 노출되고, 결국 그 기업은 이미 세워놓은 사업전략에 차질을 빚어 도산위기를 맞게될 지도 모른다. 그렇다면 그것은 과연 누구의 책임인가. 무슨 수로 초대하지 않은 외부손님의 침투에 의한 네트웍 자원이나 조직의 노출을 막을 수 있을 것인가.

물론 가장 확실하고 완벽한 보안은 외부와의 접속을 원천봉쇄하는 길일 것이다. 그러나 네트웍 컴퓨팅 환경 활성화, 인터넷 접속 필요성이 증대되고 있는 가운데 과거 중앙집중식 컴퓨팅 환경을 고수할 수 없는 법. 사용권한이 부여된 한정된 사용자만이 내부망의 접속이 가능하도록 하는 인증기능이 포함된 방패막이 절실히 요구되고 있는 것이다.

현재 가장 효과적인 해결책으로서 외부로부터의 불법 침입자를 단계적으로 차단해 주는 방화벽(Firewall)이라 일컬어지는 보안 솔루션이 제시되고 있다. 파이어월은 근본적으로 인터넷의 오픈

† 정회원 : 격주간 네트웍컴퓨팅 취재부 차장

성에 위배되는 개념이지만 인터넷이 좋지않은 목적으로 사용되는 경우를 대비한 보안 솔루션의 하나이다. 파이어월은 인터넷과 인트라넷의 경계에 위치, 내부 네트웍에서 외부를 연결할 수 있는 유일한 창구로서 네트웍 보안 관리자가 네트웍간 정보흐름을 제어하고 감시할 수 있도록 한다.

여러 보안제품 중 인터넷과 긴밀한 연결고리를 맺고 있는 파이어월은 인터넷이 확산되면서 필요성이 절실히 요구되고 있으며, 인트라넷을 구성하는 기본적인 요소로서 자리매김하고 있다.

1.1 개념

파이어월은 조직 안팎을 넘나드는 모든 데이타와 트래픽을 점검하고, 서비스 권한을 제한함으로써 네트웍을 외부로부터 보호하는 기능을 담당한다.

'명백히 금지되지 않은 것은 허용한다' 는 설계 원칙을 지키며, 방어 대상에 따라 개별 방어와 경계선 방어가 이루어지도록 한다. 개별 방어는 네트웍 상에 연결된 호스트에 대한 개별적 방어를 말하며, 경계선 방어는 네트웍에 연결된 경로를 방어한다는 의미로 경계선안에 있는 호스트는 상호 신뢰할 수 있다.

파이어월은 패킷 필터링(Packet Filtering), 애플리케이션 게이트웨이(Application Gateway), 서킷 게이트웨이(Circuit Gateway), 하이브리드(Hybrid) 방식 등 크게 4가지 방식으로 구분된다. 이전까지만 해도 이 네가지 방식은 엄밀히 구분되었으나, 최근에는 각각의 방식들이 결합되고 있어 서로 각각의 기능들을 조금씩 포함하고 있다.

패킷필터링 방식은 라우터와 호스트 혹은 라우터 단독으로 구성되며, 소스 어드레스와 포트가 목표 어드레스와 포트로의 접근을 허용할 것인지의 여부를 결정한다. 이 방식의 장점은 처리속도가 빠르고 투명성이 보장되며, 보안 정책 변경이나 새로운 서비스 추가가 용이하다는 것이다. 반면, 경계선 방어가 되지 않으며 해커에 의해 소스와 목표 어드레스 및 포트 조작이 가능하다는 것이 약점으로 작용한다.

서킷 게이트웨이 방식은 방화벽으로 동작하는 시스템에 내부 시스템이 외부망과의 접속을 의뢰하고 방화벽 시스템은 요구에 따라 외부망과의 접속을 수행한다. 이 방식의 단점은 애플리케이션 레벨에서 트래픽을 감시, 통제하지 못하며, 투명성을 보장하지 못한다는 것이다.

보안성 측면이 비교적 우수한 애플리케이션 게이트웨이 방식은 애플리케이션 레벨에서 보안 서비스를 제공하며, 네트웍간의 모든 통신이 단절되는 대신, 프록시라고 부르는 애플리케이션 데이타 브리지를 통해 네트웍 서비스가 개별적으로 허용된다.

이 방식은 경계선 방어를 제공하며, 애플리케이션 레벨의 로깅 및 감사 기능을 제공하나, 비교적 속도가 느리고 제한된 프로토콜에서 운영되며, 투명성이 보장되지 않는 단점이 있다.

하이브리드 방식은 패킷 필터링과 애플리케이션 게이트웨이 방식을 혼합한 것으로 양쪽 방식의 장점을 갖을 수 있는 동시에 단점을 수반하고 있다.

1.2 국내시장 현황 및 전망

제한된 소수에 의해 연구목적의 학술망으로 사용되기 시작한 인터넷이 상업적인 목적으로 그 용도와 포용범위를 확장함과 더불어 TCP/IP 프로토콜을 이용한 네트웍 개방성에 의해 소스 분석이 가능해지면서 해킹 가능성도 심각한 고려 대상이 되었다. 80년대 중반 실제로 해커들에 의해 주요기관의 내부 네트웍 정보가 파괴됨에 따라 외부로부터의 해킹을 차단하기 위한 최적의 솔루션으로서 제시된 개념이 파이어월이다.

파이어월은 어느날 갑자기 생겨난 개념은 아니

다. 90년대 들어 라우터를 이용한 가장 단순한 형태의 패킷 필터링 방식과 유닉스 시스템 자체 보안을 목적으로 한 애플리케이션 게이트웨이 방식의 파이어월은 이미 존재하고 있었으나, 사용자들의 보안에 대한 인식이 그다지 높지 않았기 때문에 현재와 같은 붐 조성은 이루어지지 않았다.

그러다가 파이어월이 보안 시스템으로서 각광받기 시작한 것은 그리 오래전의 일이 아니며 기껏해야 1년 남짓밖에 되지 않았다. 파이어월이 각광받기 시작한 것은 무엇보다 웹의 등장과 관련깊다. 웹을 통해 호스트까지도 인터넷에 오픈되어 내부시스템까지 외부로의 개방이 가능해졌기 때문이다.

초기 시장 형성

국내에도 1-2년 사이에 인터넷 활용이 보편화되고, 주요 기관의 해킹 사례가 발표되면서 보안에 대한 관심이 집중, 95년 말부터 파이어월에 대한 필요성이 제기되었다. 이전까지만 해도 낯선 개념이었던 파이어월에 대한 관심이 급격히 확산된 것은 국내 파이어월 공급업체인 사이버텍홀딩스에 의해 '보안 방화벽 기술 세미나'가 대대적으로 개최된 것이 견인차 역할을 했다.

이후 등한시됐던 보안문제의 해결책을 찾으려는 업계의 활발한 움직임이 일기 시작했으며, 한국의 독자적인 암호체계 정립을 통해 정보보호산업 육성에 일조하기 위한 목적으로 96년 4월 한국정보보호센타가 설립되기도 했다.

대정정보통신이 국내 최초로 파이어월 국산화에 성공했다고는 하나, 국가적인 차원에서도 중요한 부분을 차지하고 있는 보안분야에서 국산제품이 전무한 현실로 인해 우려의 목소리도 적지않게 들려오고 있다.

대정정보통신이 특정 사용업체의 요구에 맞게끔 파이어월 기능을 취합해서 탑재하는 형태의 파이어월 국산화를 처음으로 시도한 이래 파이어월의 국산화는 지속적으로 이루어져 왔다. 현재 한국정보공학이 정보통신부에서 10억원 규모의 국책자금을 지원받아 국산 파이어월 제품을 발표할 채비를 갖추고 있으며, TIS 건틀릿을 공급하고 있는 한일정보통신과 블랙홀을 삼성 전그룹사에 설치한 바 있는 삼성전자가 본사와 소스 라이센스 계약을 각각 체결하고 국내 환경에 맞는 한국형 파이어월 개발에 박차를 가하고 있다.

그러나 파이어월 국산화에 대해 업계의 시각이 긍정적이지만은 않다. 국산제품이 발표된다고 해도 사용자가 과연 제품에 대해 얼마만큼 신뢰하고 사용할 것인가에 대한 의문이 제기되고 있기 때문이다. 업체 관계자들은 파이어월 국산화를 흔히 타이컴 국산화에 비유하는데 이는 많은 투자를 통해 국산화에 성공하더라도 막상 시장성이 없어 활성화하는데 실패한 선례 때문이다.

국산화에 성공하기 위해서는 무엇보다 자체 기술력의 확보, 사용자들의 국산제품에 대한 신뢰가 기본적으로 밑바탕에 깔려있어야 할 것이다.

96년 하반기 110억 규모 예상

국내 시장에서의 파이어월에 대한 관심은 집중되고 있는 반면, 실질적인 매출로 이어지지는 못해 95년 국내 파이어월 시장은 극히 미미한 수준에 이르렀다. 아니, 거의 매출이 일어나지 않았다고 해도 과언이 아니다.

공급업체들 대부분이 95년 말이나 96년 초부터 파이어월 제품을 본격 공급하기 시작했으며, 95년은 사용업체들이 파이어월 도입을 검토하고, 예산을 책정했던 기간이었다는 것이 그 원인이라고 할 수 있다. 아직까지도 국내에는 파이어월에 대한 관심만큼 파이어월 구축의 활발한 움직임은 보이고 있지 않다.

국내 파이어월 시장 규모는 보안상의 이유로

공급업체들이 매출액 밝히기를 꺼려해 정확한 액수를 산출해 내기는 어려우나, 관련업체의 의견을 토대로 추정해본다면 96년 상반기에 50억원 시장이 형성됐으며, 하반기에 110억원 정도의 시장이 형성됐다. 이는 무엇보다 국내에도 인터넷에 접속하려는 업체가 해마다 늘고 있으며, 인트라넷 솔루션 구축의 일부로서 파이어월 도입을 검토하는 경향이 부쩍 늘어난데 기인한다.

현재 파이어월 공급업체는 사이버텍홀딩스, 한일정보통신, 삼성전자, 두산정보통신, 한국정보공학, 한국엑시스, 한국IBM, 한국디지탈, 한국썬마이크로시스템즈, 닉스테크, 대정정보통신 등 13여개 업체들이 이에 포함된다.

95년부터부터 파이어월 제품을 공급하기 시작한 한국엑시스, 사이버텍홀딩스, 한국IBM, 한국정보공학 등에 이어 96년부터 파이어월 시장에 본격적으로 진출한 한일정보통신, 두산정보통신, 닉스테크 등이 가세하면서 점차 시장이 활기를 띠고 있다.

아직까지 국내시장 자체의 규모가 크지 않기 때문에 제품의 시장 점유율을 매기는 것 자체에는 의미가 없으나, 현재 두각을 나타내고 있는 제품은 체크포인트 파이어월-1, TIS 건틀릿, BNT 보더웨어, 사이버가드 사이버가드 방화벽 등이 그것이다.

그러나 아직은 초기 시장이기 때문에 여러 공급업체들이 난립, 각기 다른 기능을 보유한 파이어월 제품을 공급하고 있어 사용자들을 혼란스럽게 하고 있다.

파이어월 시장은 인터넷 가입업체 모두를 구축대상에 포함할 수 있어 성장잠재력이 풍부한 시장이라 할 수 있다. 인터넷을 사용하는 도메인수는 95년 말 500여개사에서 96년 들어 300% 증가한 1,500여개사에 이르며, 이중 최대 파이어월 구축 수요는 30%정도인 350-450여개사에 이를 전망이다.

국내에서 파이어월 구축이 비교적 활발한 사이트는 주로 학교, 기업체, 정부기관 등이며, 규모면에서 거대시장이라 할 수 있는 금융기관의 경우 현재 특유의 보수적인 성향때문에 인터넷을 통한 내부 정보의 공개를 꺼려하고 있으나, 전자상거래의 활성화를 통한 금융시장의 개화가 향후 파이어월 시장 활성화와 더불어 보안 마인드 확산에 일익을 담당할 것으로 기대되고 있다.

한 외신에 따르면 이미 파이어월을 설치한 업체의 30% 이상이 해킹당했다는 놀라운 사실을 전해 주었다. 이는 파이어월을 설치했다고 해서 완전무결한 보안이 이루어지지 않을 수 있다는 사실을 반증한다.

1.3 제품 동향

◆ 체크포인트 「파이어월-1」

전세계적으로 높은 시장 점유율을 보이고 있는 파이어월-1은 2.0버전부터 애플리케이션 게이트웨이 방식을 취해 패킷필터링과 애플리케이션 게이트웨이의 장점을 통합하고 단점을 보완했으며, 지원 서비스의 폭이 넓고 새로운 서비스 추가 및 변경이 용이한 장점을 갖고 있다.

지사 또는 원격사용자를 위한 클라이언트 인증 기능, 버추얼 프라이빗 네트웍 및 인터넷 상거래를 위한 암호화 기능을 포함하는 인터네트워킹 보안 특성들을 탑재하고 있으며, 모든 암호화 기능들은 설치, 관리, 통제가 간단한 GUI 룰 베이스 에디터 및 로그 뷰어에 통합돼 있다.

최신 버전인 2.1버전에는 윈도우 NT, 윈도우 95 등 지원 플랫폼의 확장, 로그 기능 강화, 리얼오디오, VOD 서비스 등과 같은 새로운 애플리케이션이 추가 지원된다. 파이어월-1의 관리모듈은 윈도우 NT, 솔라리스 2, 썬OS 4, HP-UX 및 베이 네트웍 라우터 상의 게이트웨이를 제어할 수 있

으며, 버추얼 프라이빗 네트웍 솔루션은 데스크탑, 랩탑 등으로 확장돼 원격사용자에게 안전한 접속이 가능하도록 한다. 3.0버전이 출시될 예정이다.

파이어월-1을 공급하는 사이버텍홀딩스는 나래이동통신, 삼보컴퓨터, 아이네트기술 등 13개 회사가 지분을 투자하여 설립한 회사로 국내 파이어월 시장을 공략하는데 다른 업체보다 비교적 유리한 입지를 확보하고 있다.

파이어월 단품 공급에 중점두기 보다는 전자상거래를 위한 일부 솔루션으로서 판매를 확대해 나간다는 방침을 확고히 하고 있다. 보안 관련 세미나 개최를 통한 네트웍 보안의 필요성을 고조시켜 국내 파이어월 시장 활성화를 선도하겠다는 방침이다.

현재까지 교육, 금융/증권사, 네트웍업체, 그룹 연구망 등 20여개 사이트에 구축을 완료했으며, 앞으로 인터넷 전자상거래를 위한 솔루션 전문업체와의 긴밀한 협력관계를 유지해나갈 계획이 다.

◆ 썬마이크로시스템즈 「파이어월-1(OEM)」, 「썬스크린 SPF-100G」

한국썬마이크로시스템즈는 체크포인트의 파이어월-1과 썬스크린 SPF-100G라는 자사제품을 함께 공급하고 있다.

하드웨어와 소프트웨어로 구성된 패킷 필터링 방식의 보안 전용서버인 썬스크린 SPF-100G는 기존 SPF-100에서 보안 레벨을 낮춘 대신 암호화 레벨을 높인 것으로 G는 글로벌 버전을 의미한다.

5개의 10Mbps 이더넷 포트를 지원하며, 모든 이더넷 포트는 패킷을 스크리닝하여 IP 어드레스를 숨겨 외부 해킹을 방지한다. 썬스크린 스테이션 G에 의해 SPF-100G의 관리가 이루어지고, 하나의 SPF-100G가 멀티플 SPF-100G를 리모트로 관리할 수 있다.

한국썬마이크로시스템즈는 국가기관이나 연구소, 대기업을 주 타겟시장으로 파이어월 제품 판매를 강화할 계획이다. 기술지원에 있어서는 썬 서비스라는 조직을 통해 사후 유지보수가 이루어지고 있으며, 썬 서비스 하부에 썬 프로페셔널이라는 인티그레이션 전문부서를 두어 보안 컨설팅이 전문적으로 이루어지도록 하고 있다.

◆ TIS 「건틀릿」

하드웨어와 소프트웨어 기반의 애플리케이션 게이트웨이 방식 파이어월인 건틀릿은 애플리케이션 레벨에서 보안 서비스를 제공하며, 조직의 보안 정책을 준수한 양방향 통신을 조절한다. 이 제품에는 BSD/OS를 탑재한 펜티엄, 썬, HP, SGI 버전 등 다양한 하드웨어 플랫폼이 제공된다. 소스코드가 공개돼 있어 사용자들에게 친숙한 TIS의 인터넷 파이어월 툴킷은 건틀릿 핵심기능의 기반이 되고 있다.

건틀릿의 설계 철학은 통신, 컴퓨터, 네트웍 보안 연구 분야에서 다년간 쌓아온 TIS의 경험에서 출발한다. 무엇보다 보안에 위배되는 어떠한 서비스도 금지되는 보수적 접근방법, 확실히 허용되지 않은 것은 금지하는 최소화, 작은 소프트웨어 모듈로 구성한다는 단순화 등에 개발 초점을 맞추고 있다. 크리스탈 박스를 통해 보안 시스템을 구현하는 소스코드와 알고리즘 분석이 가능하도록 하는 등 다른 업체의 보안제품과는 달리 자사 제품의 소스코드를 공개하는 것은 소스코드 자체에 대한 TIS의 자신감이 반영되 있다고 유추해볼 수 있다.

터미날 서비스, FTP, SMTP, NNTP, 고퍼, X.11 등 다양한 서비스를 지원하는 건틀릿은 여러 형태의 사용자 인증을 위한 인터페이스 제공으로 강력한 사용자 인증기능과 내장된 침입경보 기능, 접속의 투명성, 통합된 관리도구 등을 주요 특징

으로 한다.

제품 업그레이드에 있어서는 SQL 넷 프록시와 노츠 프록시가 추가 제공되며, 하드웨어 플랫폼으로는 솔라리스 2.x와 운영체제로는 윈도우 NT가 새로이 지원될 예정이다.

국내 공급을 담당하고 있는 한일정보통신은 그룹 SI업체, 정부기관, 관공서 등을 주 타겟으로 한 적극적인 영업활동을 펼치며, 향후 주요 하드웨어 업체와 협력관계를 추진하여 영업력 강화에도 힘쓸 방침이다. 또한 동남아 판권을 보유하고 있어 동남아 진출계획도 갖고 있다.

현재 자사의 보안 전문팀과 함께 보안 전문 컨설팅 회사인 TIS, ISS와의 협력관계를 통한 보안 컨설팅이 이루어지고 있는 가운데, 한일정보통신은 보안 제품 공급이외에 컴퓨터, 통신, 네트웍에 대한 보안 컨설팅 사업도 본격적으로 강화해나갈 계획이다.

◆ 보더웨어「보더웨어 파이어월 서버」

보더웨어는 기존 파이어월 서버 보다 단순함과 보안 측면을 강조한 파이어월 서버이다. 즉, 방화벽 실행에 필요한 것 이외의 모든 기능은 제거한 자체 OS를 갖고 있어 별도의 OS 설치가 불필요하므로 설치 및 관리가 용이하다. 대부분의 다른 파이어월 제품들이 유닉스에서 운영되는데 반해 PC에서 운영되기 때문에 우수한 성능대 가격비를 강점으로 내세우고 있다.

보더웨어는 패킷 필터링, 애플리케이션 게이트웨이, 서킷 게이트웨이를 통합한 시스템으로서 가격대 효율성이 높으며, 효율적인 사용자 인터페이스로 구성 복잡도를 줄이고 메일 서버, 네임 서버, FTP, 텔넷 등 내장된 응용서버들은 추가 기능 및 보안성을 제공한다.

보더웨어의 대표적인 보안 특징 중 하나인 안전한 인터넷 서비스 제공을 위해 내부 네트웍과 독립된 별개의 네트웍인 SSN(Secure Server Net)을 구축, 내부 네트웍을 더욱 안전하게 보호할 수 있다. 이 시스템은 TCP/IP 서버들을 각 회사나 기관에서 메뉴 구동 방식의 인터페이스를 이용, 자체 정의된 프록시들을 적합한 형태안에서 SSN에 접근할 수 있도록 한다.

네트웍 주소의 자동변환, 내부 도메인 정보 숨김, 메일 헤더 절단, 감사추적과 경고 등의 솔루션이 포함된 진일보한 파이어월로 인식되고 있다.

두산정보통신은 보더웨어의 가격경쟁력을 내세워 인터넷 통합 솔루션의 일부분으로 제품 공급에 주력한다는 입장을 밝히고 있다. 올해에는 특히 제품의 인지도 확산에 주력할 예정이다.

도로공사, 대한생명 등에 구축을 완료한 두산정보통신은 하드웨어 벤더와 공급계약 체결로 영업을 강화해 나갈 방침이며, 올해 30개 사이트를 목표로 하고 있다.

◆ 사이버가드「사이버가드」

닉스테크, 한화, 데이콤, 아이네트기술 등 여러 업체에서 공급하고 있는 사이버가드는 보안 솔루션만을 전문적으로 개발해온 사이버가드사 제품이다.

사이버가드는 하드웨어와 소프트웨어가 결합된 형태의 하이브리드 방식의 파이어월 시스템으로서 미 국방성 국립컴퓨터 보안 센타(NCSC)의 인증을 받은 보안 제품이다.

애플리케이션, OS, 네트웍 레이어 등 멀티-레벨 보안(MLS) 솔루션으로서 내부네트웍과 외부네트웍에 대한 확실한 분리가 가능하며, 확장성, 유연성 및 커스토마이징이 용이하다는 것이 장점으로 꼽힌다.

이 제품은 패킷 필터링, 듀얼-홈드 게이트웨이, 회선 게이트웨이, 애플리케이션 게이트웨이, 이들을 결합한 형태의 배스천 호스트로 사용 가능하다.

듀얼-홈드 게이트웨이 기능 지원을 위해 텔넷, FTP, rlogin 등의 프로토콜을 위한 여러 에이전트를 제공하고 있으며, 다른 애플리케이션 구현을 위한 개발환경을 지원하며, SOCKS와 호환되는 네트웍 프록시 기능이 포함돼 있다.

사이버가드는 일반적인 방화벽 기능외에 주소 및 호스트명 감추기 기능, 듀얼 도메인 네임 서버스, 미국 정부 기밀문서 분류에 사용되는 정책을 적용, 내부 네트웍의 운영정보를 보호할 수 있는 기능 등이 추가적으로 지원된다.

공급업체중 닉스태크는 다양한 프록시 기능을 필요로 하는 금융, 정부/공공 기관, 통신사 등을 주 타겟 시장으로 공략하며, 설치 후 교육과 기술지원을 담당할 인력 보강에 만전을 기할 방침이다. 단순 보여주기식 세미나가 아닌 클라이언트 대상의 교육 프로그램을 개발 중이다.

◆ 대정정보통신「파이어월」

국내 최초로 파이어월 국산화를 시도한 대정정보통신은 외산 보안제품의 보안상 맹점을 자체 기술력으로 보완하자는 취지로 현재 지원되는 기능보다는 향후의 침입에도 지속적으로 대비할 수 있는 유용성에 개발 방향을 맞춰 국산화에 성공했다.

대정정보통신이 개발한 파이어월 제품은 단품의 형태가 아니라 각 사용업체의 환경에 맞는 파이어월 기능을 취합해 탑재하는 형태이다.

파이어월 공급업체가 아니라 SI 전문업체인 대정정보통신은 SI사업의 일부로서 지속적인 파이어월 개발에 박차를 가할 예정이다.

◆ IBM「인터넷 커넥션 SNG」

한국IBM이 공급하는 SNG는 RS/6000상에서 운영되는 소프트웨어 형태의 파이어월이다.

인터넷 환경에서 FTP와 텔넷에 대한 애플리케이션 게이트웨이 기능과 IP 패킷 필터링 기능 등 2가지 기능을 함께 수행하며, 도메인 네임 서버(DNS) 기능을 통해 내부망의 DNS와 외부망의 DNS를 구별 사용함으로써 내부망의 호스트 어드레스를 외부로부터 감출 수 있어 외부로부터의 침입이 어려워지도록 한다.

메일 처리 기능이 포함돼 있어 파이어월에 착신된 메일에 대해 수신자 주소에 따라 내부 또는 외부 목적지로 중계해 줄 수 있다.

이외에도 시큐어 터널 기능으로 보안기능이 강화된 망 사이에 보안성이 결여된 망이 개입돼 있을 때 자료를 암호화하여 송수신함으로써 보안을 유지하며, 로깅 기능으로 연결 발생, 사용자 자격검증 등 주요한 이벤트에 대한 기록이 가능하다.

현대, 대우자동차, 원자력연구소, 삼성항공 대전연구소 등 5-6개 사이트에 이미 구축을 완료한 바 있는 한국IBM은 기존 고객을 대상으로 직판과 인성정보, 인터링크시스템 등 네트웍, 인터넷 관련 경영동반자를 통한 파이어월 영업 강화에 나설 예정이다.

◆ 디지탈「디지탈 파이어월 서비스」,「유닉스용 파이어월」,「보더웨어 파이어월 서버」

디지탈의 파이어월 제품군은 크게 3가지로 나눌 수 있다. 하이엔드 파이어월 제품인 디지탈 파이어월 서비스는 게이트 키퍼, 게이트, 메일게이트 등 3개 플랫폼과 서비스로 구성되어 있다. 미드 레인지급으로는 유닉스용 파이어월이 있고, 엔트리 레벨로는 설치가 용이하고 저가형인 보더웨어 파이어월 서버가 있다.

유닉스용 파이어월은 손쉽게 하이엔드로 확장이 가능하며, 커스토마이징하는데 유연성을 제공한다. 메일, 텔넷을 위한 애플리케이션 게이트웨이 방식으로 FTP나 텔넷용 인증 서비스 제공과 더불어 로깅, 감사, 알람 보호 기능 등이 강력한

장점이다. 유닉스용 파이어월은 알파시리즈, 유닉스, 윈도우 NT, 인텔 등의 플랫폼을 지원하며 썬에도 곧 포팅될 예정이다.

디지탈의 경우 파이어월과 관련된 전문적인 사업을 추진하고 있지는 않으나, 토탈 솔루션을 제공한다는 차원에서 인터넷 비즈니스 솔루션의 일부로 갖춰진 파이어월 제품을 공급하고 있는 실정이다. 주로 다국적 기업, 무역회사 등의 사이트를 확보하고 있다.

◆ 랩터 시스템즈「이글」

랩터 시스템즈의 파이어월 솔루션인 이글 시스템은 애플리케이션 게이트웨이, 듀얼 홈드 게이트웨이를 구현하며 이중 네트웍간의 트래픽과 이에 대한 자세한 로그기록 및 관리 기능 등이 지원하는 프록시를 실행한다.

이글 시스템은 4가지 형태로 구성이 가능하다. 외부로부터 내부시스템을 보호하는 이글 엔터프라이즈, 특정 서버에 대해 이중으로 보호하는 이글 웍그룹, 해외지사나 국내지사 등 리모트 지역의 정보제공 서버를 보호하는 이글 리모트, 노트북을 사용하는 국내외 출장자들이 내부시스템 사용시 활용되는 이글모빌 등이 그것이다. 이들 제품군은 내부 시스템 및 각 지점 정보제공 서버 모두에 대한 보호가 가능하며, 내부 시스템 및 지점 시스템의 확장으로 인한 방화벽 시스템 관리도 네트웍 세그먼트가 구분돼 있어 용이하고 서비스 제공 시스템이 네트웍상에 별도로 존재하므로 내부시스템이 안전하게 보호된다는 장점이 있는 반면, 파이어월 설치시 5% 정도의 트래픽 로드가 발생한다는 것이 단점으로 작용한다.

이글의 국내 공급 뿐만 아니라 국산 파이어월 개발에도 총력을 기울이고 있는 한국정보공학은 현재까지 언론사, 관공서, 대기업, 학교, 정부기관 등 다양한 사이트에 공급한바 있으며, 직판 위주의 영업활동에 주력하고 있다

◆ 밀키웨이「블랙홀」

하드웨어와 소프트웨어가 결합된 턴키방식으로 공급되고 있는 블랙홀은 네트웍 구성의 최종단에 위치, 사용권한이 블랙홀 시스템의 인증절차를 거쳐 인증된 개별/그룹 사용자에 대해서만 제한적으로 내, 외부 네트웍과의 통신을 가능케하는 애플리케이션 레벨 파이어월 제품이다.

싱글 혹은 듀얼 구성이 가능한 블랙홀 시스템은 관리하고 있는 대상항목에 따라 유저, 서비스, 알람, 리포트 등 4가지로 구분된다. 네트웍을 이용하는 모든 유저들의 형태대로 DB에 저장되며, 텔넷, FTP, NNTP 등 블랙홀이 제공하는 각종 서비스 레벨의 프로토콜과 환경 조건이 저장돼 있다. 또한 관리자가 미리 정한 조건과 부합하는 상황이 네트웍에 발생했을 경우 필요한 조치가 기록돼 있다.

블랙홀 시스템이 설치된 네트웍을 통과하고자 하는 모든 요구는 가디안이라는 대몬 프로세스(Daemon Process)에 의해 인증 처리된다.

소스 IP 어드레스, 목적지 IP 어드레스, 포트수, 서비스 ID, 유저 ID 등 풀 유저 레벨 인증을 제공하며, 유저 ID나 패스워드를 통하지 않고 인증절차를 수행, 사용자에게 투명성을 제공하고, 유저의 사용 편이성을 강조한 GUI 환경을 제공한다는 것이 최대 장점이다. 반면, 암호화 부분이 강화되어야 한다는 지적도 있다.

제품의 신뢰성, 성능, 안정성 등을 고려, 블랙홀을 국내에 공급하고 있는 삼성전자는 우선적으로 그룹사를 위주로 활발한 구축에 나서 삼성 전계열사의 파이어월 구축을 마무리하고 있다. 외부 사이트의 경우 국가기관이나 금융기관을 위주로 확보해 나갈 계획이다.

블랙홀의 소스 라이센스 계약 체결 후 자체 기

술인력을 동원, 한국형 파이어월 개발이 진행중이며, 제품이 업그레이드되면 업그레이드를 수용하면서 사용자가 원하는 기능을 포함시킨다는 기본 입장을 밝혔다.

인터넷 사업을 추진하는 데 있어 하나의 아이템으로서 파이어월 솔루션을 공급하고 있는 삼성전자는 향후 보안 컨설팅 사업에도 본격적으로 진출할 장기적인 계획을 갖고 있다.

◆ GTA「GFX 인터넷 파이어월 시스템」

전용 보안 시스템인 GFX 인터넷 파이어얼 시스템은 다른 파이어월 제품과는 달리 하드웨어 오리엔티드 방식으로 내벽과 외벽의 듀얼 시스템으로 구성되어 해킹을 효과적으로 방지한다.

GFX는 네트웍 시스템 타입에 상관없이 모든 TCP/IP 기반 네트웍에 적합한 스탠드얼론 턴키 솔루션으로 IP 패킷 필터링과 확장성 있는 드롭 세이프 로깅을 제공하며, SMTP, 텔넷, NNTP 등의 프록시를 포함하고 있다.

소프트웨어 오리엔티드 방식에 비해 장점이라면 시스템 셧다운 기능이 있어 해커가 침입했을 경우 시스템이 작동을 멈춰 해킹의 기회 제공을 원천적으로 막을 수 있다는 것이다. 또한 듀얼 시스템 중 내벽 시스템에 포함된 DAT 테입 드라이버가 해커의 경로를 저장할 수 있어 해커의 경로를 추적할 수 있다는 점이 특징적이다.

GFX에는 3가지 종류의 제품군이 있으며, 랙타입 GFX-R, 보급형 GFX-E, 리던던트 파워 서플라이를 제공하는 표준모델 GFX-S 등이 그것이다.

한국엑시스는 대기업, 금융기관, 연구소, 대학교, 관공서 등을 주 타겟으로 레퍼런트 사이트를 확보해 나갈 계획이며, 제품 판매 강화를 위해 직판과 동시에 리셀러를 모집하고 있다. GFX의 소프트웨어만 별도로 하드웨어 업체와 협력관계를 맺어 공동 공급할 예정이다.

올해부터 GTA로부터 기술을 이전받아 하드웨어를 국내에서 자체 개발할 계획이며, 소프트웨어의 경우 소스 라이센스 계약을 맺어 본사와의 협의하에 로칼라이즈화할 계획이다. 향후 국내시장 뿐만 아니라 아시아 지역으로의 수출 계획도 갖고 있다.

2. 전자우편 · 전자상거래 보안

인터넷 상에서 가장 많은 사용자들이 이용하고 있는 전자우편이나 최근들어 대두되기 시작한 전자상거래 서비스 측면에서 보면 파이어월은 그 보안성에 여러 가지 허점을 가지고 있다. 왜냐하면 전자우편의 경우는 내부망에서 작성한 데이타가 파이어월을 거쳐 외부망으로 전송되는데, 파이어월을 거칠 때까지는 안전하지만 외부망에서의 안전을 보장할 수 없게 된다. 또한 전자상거래도 마찬가지로 실제 제품을 구입하고 지불하는 과정에 대한 안전 보장을 해줄 수 없다.

전자우편이나 전자상거래를 포함해 일반적으로 정보를 보안하기 위한 가장 안전한 방식은 정보를 암호화하는 방법이다. 최근들어 정보를 암호화하기 위한 여러 가지 방법들이 나오고 있다.

2.1 암호화 시스템

분산컴퓨팅 환경에서 정보 누출에 대한 위협 요소들은 매우 다양하다. 정보 보호에 대한 권한을 가진 권한자의 특권을 대신 도용하는 경우와 같이 권리를 위장하는 경우가 있다. 또한 도청이나 불법접근에 의한 정보노출, 데이타 변경에 따른 무결성 파괴, 사용자 특권을 변경하는 권한 침해와 메시지 송신과 수신을 부정하는 부인 등이 있을 수 있다. 위협 행위들을 해결할 수 있는 방법은 현재로서는 암호화가 가장 강력한 방법으로 떠오르고 있다.

암호화 기술은 모든 정보통신 분야에서 적용할 수 있다. 즉, 디지탈 정보를 다루는 모든 분야에서 보안이 필요하다면 암호화를 응용할 수 있다는 것이다. 네트웍상에서 주고받는 정보 혹은 컴퓨터에 저장된 정보를 보호하는 암호화시스템에서 중심적으로 고려하는 내용은 다음과 같다.

첫째, 비밀보장(Confidentiality) 기능이다. 정보를 보호하는데 있어 비밀을 보장하는 것은 가장 기본이 되는 사항이다. 즉, A가 B에게 보내는 자료를 제 3자인 C가 보지 못하게 방지하는 것을 의미한다.

두번째, 무결성(Integrity)의 보장 기능이다. 무결성이라 함은 A가 B에게 보내는 자료를 제 3자인 C가 중간에서 내용을 변조하지 못하게 하는 기능이다. 자료의 내용이 노출되지 않는다 하더라도 제 3자가 자료의 내용을 삭제 또는 첨가하거나 순서를 바꾸는 등의 행위를 방지하는 것이다. 이런 것을 방지하기 위해서는 주로 메시지의 체크섬이나 메시지 다이제스트를 구해 둠으로써 메시지의 수정 여부를 확인할 수 있다.

세번째, 부인방지(Non-Repudiation) 기능이다. 이 기능은 전자상거래에서 사용이 용이하다. A가 B에게 데이타를 보내고 난후 자신은 데이타를 보내지 않았다고 부정하거나 B가 제대로 데이타를 수신하고도 정보를 받지 않았다고 부정하는 사례를 방지할 수 있는 기능이다. 전자상거래에서 특히 이 기능이 필요한 것은 구매자가 구매를 하고도 차후에 부정하는 것을 방지할 수 있고, 판매자가 제품에 대한 비용을 다 받고도 제품을 판매하지 않았다고 부정하는 것을 방지할 수 있다. 이러한 부인방지는 전자서명과 같은 방식을 이용한다.

암호화(Cryptography) 방법

앞에서 설명한 바와 같이 보안을 위한 최선의 방법이 암호화를 하는 것이다. 물론 암호화라는 것이 만병통치약처럼 모든 문제를 해결할 수 있는 것은 아니다. 역으로 암호화를 이용한 정보의 유출에 대한 문제 등으로 국내에서는 암호화 기능이 들어 있는 보안 제품에 대한 수입이 규제되고 있는 것도 현실이다.

미국에서도 암호화 제품은 수출을 규제하고 있으며, 미국외로 나가는 제품에 대해서는 40비트 길이 이하의 키를 이용할 수 있도록 하고 있다. 그러나 40비트 길이 이하의 키는 간단한 작업만으로도 해독이 가능하기 때문에 실제 미국밖으로 나가는 암호화 제품은 제대로된 암호화 기능을 수행하지 못한다고 해도 과언은 아니다.

이와 같이 모든 국가나 개인들에게 있어서도 예민한 문제가 되고 있는 암호화는 기본 데이타와 자료를 암호화하는 키, 암호화된 자료, 암호화된 자료를 원래의 자료로 복원하는 키 등으로 구성되어진다.

암호화(Encryption)는 자료의 기밀성을 보장하는 방법을 말하는 것이다. 기밀을 보장하기 위한 암호화에는 대칭형 방식(비밀키 암호화)과 비대칭형 방식(공개키 암호화) 등 두가지로 나누어 볼 수 있다. 대칭형 암호화 방식은 자료를 암호화하는 키와 암호화된 자료를 복호화시키는 키가 동일한 암호화 방식이다. 대칭형 암호화 방식은 가장 널리 사용되는 방법이기도 하다. 왜냐하면 이 방법은 암호화와 복호화가 빠르다는 장점을 가지고 있고, 여러가지 다양한 암호화 기법이 개발되어 있기 때문이다

일반적으로 사용되는 암호화 방법이 대칭형 암호화지만 이 방법도 단점을 가지고 있다. 즉, 다수의 사용자가 동일한 자료를 사용할 때 키를 공유한다는 문제가 발생한다. 많은 사람이 공유한다는 것은 그만큼 보안의 홀이 생길 수 있다는 것으로 보아도 무방하기 때문에 문제가 될 수 있다.

암호화의 또다른 방법은 비대칭 암호화 방식이다. 일반적으로 암호화 정보를 네트웍상의 상대편에게 보낼 때는 암호키까지 보내게 된다. 이러한 경우 이 암호키를 보호할 방법이 없게 되는데, 이러한 문제를 해결하기 위해 개발된 기술이 비대칭 암호화 방식이다.

비대칭 암호화 방식, 즉 공개키 암호화 방식은 데이타를 보내는 A가 자신의 프라이빗 키를 이용해 정보를 암호화하고, 데이타를 받는 B는 A의 퍼블릭 키를 이용해 암호를 해독하는 방식이다. 이 방법은 정보의 철저한 보호가 가능하지만 알고리즘이 복잡해 처리시간이 많이 걸린다는 단점을 가지고 있다. 대칭형 방식과 비대칭형 방식의 암호화를 간단히 비교하면 <표>와 같다.

정보 보안을 위한 암호화는 정보의 기밀성을 지킬 수는 있지만 정보 내용에 대한 보증을 해줄 수 없다는 약점을 가지고 있다. 즉, A로부터 정보를 받기 원하는 B가 실제로 자료를 받았는데 이것이 A로부터 보내진 것인지 전혀 다른 사람으로부터 보내진 자료인지 알 수 없다. 또한 B에게 까지 오는 중간 과정에서 내용의 수정이 없었다는 것을 보증할 방법이 없다. 이와 같이 암호화에서 해결해 줄 수 없는 문제를 해결하기 위한 방법이 메시지 인증기능과 전자서명 기법이다.

인증기능과 전자서명

중간에 데이타가 변조되는 것을 막는 보안 기능이 바로 메시지 인증기능이다. 메시지 인증기능은 메시지를 송수신하는 A와 B외에 제 3자인 C가 메시지 내용을 수정하지 못하게 하는 것에 초점을 맞추고 있다. 메시지 인증기능을 통해 메시지가 수정되지 않았는지, 메시지의 순서가 바뀌었는지에 대한 확인을 할 수 있다.

인증의 방식에는 퍼블릭 키를 이용해 메시지를 암호화하는 방법과 암호화 체크섬 이용, 해쉬함수 이용 등이 있다.

먼저 퍼블릭 키를 이용해 암호화하는 방법은 A가 자신이 가지고 있는 프라이빗 키를 이용해 데이타를 암호화, B에게 보내면 B는 A가 이미 알려준 퍼블릭 키를 통해 데이타를 복호화 할 수 있다. 복호화가 제대로 이루어진다면 서로가 원하는 상대와 데이타 송수신을 한 것이지만 만일 복호화가 제대로 이루어지지 않는다면 데이타가 A로부터 온 것이 아니거나, 수신자가 B가 아닐 수 있는 것이다.

이것이 바로 전자서명의 기능이다. 그러나 퍼블릭 키를 이용하는 방법도 앞에서 언급했듯이 알고리즘이 복잡해 처리시간이 많이 걸린다는 단점을 가지고 있다. 또한 퍼블릭 키는 공개하는 키이기 때문에 비밀 보장성이 떨어진다.

이러한 단점을 보완하기 위해 A가 프라이빗 키로 암호화, 이것을 다시 B의 퍼블릭 키로 암호화하는 이중 과정을 통해 B에게 메시지를 보내고 B는 다시 자신의 퍼블릭 키로 복호화하고, 또한번 A의 퍼블릭 키로 복호화 하는 과정을 중복해서 수행하게 함으로써 인증기능, 전자서명 기능, 기밀성 보장 등의 모든 기능을 보장할 수 있도록 할 수도 있다.

암호의 체크섬을 이용하는 방법은 MAC(Message Authentication Code)를 구해 사용할 수 있다. 메시지를 주고받는 A, B가 동일한 키를 가지고 있다면 A는 메시지의 체크섬, 즉 MAC를 구한 후 그 내용을 암호화해서 메시지에 붙여 보내면 B는 그 값을 해독해서 메시지의 체크섬을 새로이 계산해 보고 동일하면 메시지의 변경이 없었음을 증명하는 방법이다.

해쉬함수 이용법은 체크섬 대신 원웨이 해쉬함수를 이용해 MAC 데이타를 생성하는 방식이다. 이 방법은 최근들어 많이 사용되고 있는 방식이

기도 하다.

전자서명은 메시지를 송수신하는 당사자간에 상호 메시지의 신빙성 여부에 대한 보증을 하도록 하는 것에 초점을 맞추고 있다. 전자서명은 일반적으로 퍼블릭 키 암호화 방식을 이용해서 이루어진다. 즉, A가 프라이빗 키로 암호화해서 보내면 B는 A의 퍼블릭 키를 이용해 복호화하기 때문에 A는 자신이 이 내용을 보냈다는 것에 대해서 부인할 수 없게 되는 것이다.

2.2 전자우편 보안

전자우편은 인터넷을 이용한 사용자들이 가장 많이 사용하는 서비스이다. 가장 많은 사람이 사용한다는 것은 가장 많은 사람에게 공개되어 있으며, 보안에 있어 가장 많은 홀을 가지고 있다는 말로 대변될 수 있다. 그렇기 때문에 인터넷을 이용한 전자우편 자체가 보안의 홀이라고 말할 수 있다.

현재 사용되고 있는 전자우편의 보안은 암호화 알고리즘이 유일한 방법이라고 전문가들은 말한다. 전자우편을 사용하는 송신자와 수신자가 전용의 네트웍을 가지고 통신하지 않는 이상, 전송되는 메일은 수신자를 찾기 위해 수많은 호스트들을 거치게 되고, 이 과정에서 불순한 의도를 가진 자에 의해 전송이 불가능해지거나 내용이 변조되는 등의 사고가 발생하는 것이다. 전자우편에서 이러한 문제들이 더욱 심각해지는 것은 송신자나 수신자 모두 메일이 외부 침입자에 의해 공격을 받았다는 사실조차 감지하지 못한다는 것에서 발생한다.

전자우편에서 가능한 공격들은 크게 세가지 정도로 구분할 수 있다. 송신자 A가 수신자 B에게 보낸 메일의 전송만을 차단하는 전송차단이 첫번째이다. 두번째로는 메일을 가로채 원래 메일을 차단할 수도 있고, 내용만 확인해 보고 그냥 보낼 수도 있는 가로채기가 있다. 마지막으로는 메일을 가로채 내용을 변조한 후 변조된 메일을 수신자인 B에게 보내는 변조방법이 있다.

다양한 전자우편 보안

전자우편에서 필요로 하는 보안 기능들은 앞에서 설명한 보안기능들, 특히 암호화 기능을 기본으로 하고 있다. 메시지에 대한 기밀성을 보장해야 하며, 메일을 보낼 때 자신의 서명을 함께 보내 전송도중 메일이 변경되었는지를 확인할 수 있는 메시지 인증기능들이 보안기능으로 제공돼야 한다.

송신자 인증기능, 송신부인방지, 수신부인방지, 리플레이 공격방지 또한 전자우편 보안을 위해 제공해야 할 기능들이다. 모든 기능들은 현재 기술로 제공이 가능하다. 그러나 수신자가 수신을 부인할 때의 수신자부인방지 기능과 메일이 전송되는 도중에 제 3자가 메일을 복사해 놓았다가 후에 계속해서 메일을 보내는 리플레이 방지 기능은 현재까지 구현이 불가능하다.

전자우편 보안 기능을 수행하기 위한 보안 제품들은 PEM(Privacy Enhanced Mail)과 PGP(Pretty Good Privacy)가 현재 발표되어 있다. 이들은 모두 메일을 암호화함으로써 메일의 보안을 보장해 주는 기능을 수행하는 제품이다.

또한 네트웍 보안 제품인 파이어월로도 전자우편의 기본적인 보안은 가능하다. 방화벽을 두고 전자메일 보안을 하는 경우는 응용게이트웨이와 전자메일 서버를 별도로 두어 보안 기능을 수행할 수 있다. 내부전산망에 있는 사용자가 POP3 클라이언트를 이용해 메일 서버에서만 메일정보를 가져다 보게 함으로써 보안을 유지할 수 있다. 이러한 경우는 응용게이트웨이에 로그자료가 남아 있어 사용자의 정보를 찾아 볼 수 있다.

PEM은 IETF에서 인터넷 표준으로 지정한 보안

제품으로 강력한 공개키 인증 시스템을 제공한다. 공개키 인증은 매우 높은 등급의 보안성을 유지하지만 구현에 어려움이 있다는 것은 앞에서도 설명한 바 있다. 이러한 복잡성 때문에 인터넷 사용자들 사이에서 PEM이 널리 사용되고 있지는 못한 형편이다. 일반 사용자들에게는 외면을 당하고 있지만 강력한 보안 기능 덕분에 은행 시스템이나 군사 목적의 시스템에서는 적합한 보안도구로 인식되고 있기도 하다.

PGP는 개인이 만든 응용 프로그램으로서 공개키 인증에 대한 권한을 모든 사용자들에게 공개시켜 놓아 구현이 비교적 용이하다. 사용이 용이하기 때문에 일반 인터넷 사용자들 사이에서 가장 보편적으로 사용되고 있는 보안 프로그램이다. 그러나 보안성만을 따지고 보면 PEM보다는 낮은 보안성을 가지고 있다.

그러나 이것은 보안성이 상대적으로 낮다는 것이지 절대적 기능 자체가 열악하다는 것은 아니다. PGP는 공개용으로 나와 있기 때문에 국내 사용자들도 자유롭게 사용할 수 있지만 그 목적이 비상업용이어야 한다는 전제 조건이 있다. PGP 알고리즘은 국내에서도 한글화 작업이 활발히 진행되고 있다.

PEM과 PGP 제품과는 별도로 PEM을 단순화시킨 RIPEM(Riordan's Internet Privacy Enhanced Mail)이 있고, PEM과 RIPEM의 복잡성을 단순하게 만들기 위해 메일 사양보다는 문서 양식(MINE)만을 정의한 MOSS가 제안되기도 했다. 최근에는 미국 RSA사가 S/MINE이라는 MOSS와 비슷하지만 상호 호환성에 초점을 맞춘 사양을 제안해 구현되고 있으며, 전자우편 보안으로 많이 보급되고 있다.

2.3 전자상거래 보안

전자상거래라고 하는 것은 실제 생활에서 나타나고 있는 모든 거래, 즉 쇼핑, 금융거래, 기업간 거래, 보험, 법률 등 이 모든 것을 컴퓨터 네트웍상에서 시뮬레이션을 통해 거래가 가능하도록 하는 것을 말하는 것이다. SF영화에서나 볼 수 있었던 이와같은 일은 국내에서도 실현하기 위해 전자상거래 연구센타가 설립되는 등 그 준비가 활발히 일어나고 있으며, 미국에서는 이미 오픈된 사이트가 운영되고 있다.

전자상거래에서 보안이란 개념이 그 어느 분야보다 크게 대두되는 것은 실제 거래를 통해 돈이 오고 간다는 점에서 그 중요성을 찾을 수 있다. 실제로 제품을 구입하고 그 대가를 지불하기 위해서 현재는 신용카드를 이용하는 경우가 가장 많은데 신용카드 번호가 외부망에 오픈돼 버리기 때문에 보안에 취약성을 가질 수 있다. 또한 신용카드 번호를 접수하게 되는 제품 판매자의 불순한 의도에 의해 개인의 정보가 나쁘게 이용될 수도 있다.

이와 같이 전자상거래는 개인의 손익과 직결되는 사항들로 이루어져 있기 때문에 보안과는 별개로 생각할 수 없는 분야이다. 바꾸어 말하면 전자상거래에 관련한 특별한 보안 조치가 있는 것이 아니라 전자상거래 시스템 자체가 보안 기능을 수행해야만 하는 것이다. 그렇기 때문에 전자상거래 보안에 대한 얘기는 전자상거래 방법들을 얘기하면서 대체될 수 있을 것이다.

인터넷상에서의 전자상거래는 몇가지 유형으로 구분된다. 대부분 잘 알려져 있거나 접속 횟수가 가장 많은 광고 사이트들로 야후나 넷스케이프, 핫와이어드, 다몰 등이 있다. 다음으로 실제 제품을 구입할 수 있는 쇼핑몰 사이트가 있고, DB서비스, 온라인 출판, 오락 등의 서비스를 제공하는 사이트들이 현재 제공되는 전자상거래 유형들이다.

다양한 유형들을 가지고 있지만 실제 인터넷

상의 비즈니스나 전자상거래가 활성화되기 위해서는 선결돼야 하는 여러가지 문제들이 있다. 네트웍 접속, 소프트웨어, 하드웨어 플랫폼, 물품의 배달, 멀티미디어 정보, 지불방식, 법률적 제약 등이 그 문제들로 이것들의 해결을 통해 인터넷상의 거래가 실제 활성화될 수 있을 것이다.

전자상거래 보안 또한 앞에서 설명한 보안 기능들과 큰 차이가 있는 것은 아니다. 정보의 기밀성을 보호하기 위한 대칭형/비대칭형 암호화와 자료의 통합성을 제공하기 위해 메시지 다이제스트 기능을 제공하여야 한다. 또한 전자서명을 이용한 부인봉쇄, 시간 동기, 인증 등의 보안 기능을 수행해야 한다.

전자상거래 보안에서 특징적인 부분이라 하면 거래를 하면서 돈을 지불해야 하는 관계로 지불 방법에 대한 프로그램들 자체가 보안에 대한 기능을 수행하게 된다. 즉, 지불 방법에 따라 거래의 안정성을 보장하게 되는 것이다.

전자지불 시스템 구현

전자지불 방법은 크게 두가지로 나누어질 수 있다. 그 하나가 지불 브로커 시스템이고, 또다른 하나는 전자화폐를 이용하는 것이다. 지불 브로커 시스템은 우리가 일반적으로 알고 있는 방법으로 신용카드나 은행의 계좌번호를 이용해 네트웍상에서 대금을 지불하는 방법을 말한다. 이런 시스템은 신용카드를 이용하는 거래에 익숙해져 있고, 사용이 편리하기 때문에 현실적으로 구현 가능한 전자지불 시스템이다.

그러나 이와 같은 시스템은 신용카드의 수수료가 비싸거나 사용자들의 개인정보나 거래정보 등의 자료가 쉽게 노출될 수 있기 때문에 비밀보장이 되지 않는다는 단점이 있다. 이러한 단점 때문에 전자상거래에서 이 방식은 일시적으로 사용될 가능성이 높다고 할 수 있다.

전자화폐의 경우는 아직 실용화되기에 이른 감이 있지만 이론적으로 또는 실험적으로 많이 연구되고 있다. 전자화폐를 이용하는 것은 신용카드를 이용해 발생할 수 있는 단점들을 개선할 목적으로 만들어진 것이다. 그렇기 때문에 전자상거래에서 보안의 또다른 방법이 전자화폐의 사용이다. 대표적인 전자화폐 지불 시스템으로는 사이버캐쉬, E캐쉬, 퍼스트 버추얼 인터넷 지불 시스템, 스마트월넷과 시큐어 패이 등이 있다.

전자화폐의 장점은 사용자 측면에서 현금과 같은 익명성을 보장받을 수 있다는 것이다. 즉, 상점에서 물건을 살 때 구매자가 누구인지가 알려지지 않는 것이다. 또한 사용자와 인가된 상점간의 거래 뿐만 아니라 사용자간 화폐의 이동도 가능하다.

이러한 전자지불 시스템에 있어서도 가장 중요한 요소는 역시 암호화 기법이다.

전자지불 서비스가 인터넷상에서 현실적인 요소로 등장하자 관련 업체에서는 전자지불에 대한 프로토콜을 개발하고 서비스를 개시하고 나섰다.

비자카드사와 마이크로소프트는 공동으로 STT라는 신용카드 응용 전자지불 프로토콜을 지원한다고 밝혔다. 또한 넷스케이프는 마스터카드사와 시큐어 커리어(Secure Courier) 전자지불 서비스를 지원하기로 제휴했다. IBM은 마스터카드에서 출자한 유로피사와 iKP프로토콜을 이용한 전자지불 서비스를 시작하기로 한 바 있다.

이러한 회사들이 서로 다른 방법들을 내놓고 있지만 사실상 거의 같은 모양의 기술을 사용한 것으로 겉포장만 조금씩 다르게 해 놓았다고 볼 수 있다. 또한 최근에는 전자지불 분야에서 활발한 경쟁을 벌이고 있는 비자와 마스타 카드사가 공통으로 SET 프로토콜을 정의하고 함께 활동할 것을 결의하기도 했다.

<표 1> 비밀키 암호화와 공개키 암호화 비교

비밀키 암호화	공개키 암호화
1. 동일한 키와 동일한 알고리즘으로 복호 2. 송신자와 수신자와 알고리즘과 비밀키를 공유해야 함 3. 비밀키가 잘 보호되어야 함 4. 알고리즘과 암호화된 예문으로 키의 추론이 불가능하여야 함	1. 동일한 알고리즘과 한쌍의 키(비밀키, 공개키)로 복호 2. 송신자와 수신자는 각각 한쌍이 되는 키를 하나씩 소유 3. 적어도 공개키 두 개의 키중 하나는 보호되어져야 함 4. 알고리즘과 하나의 키로 다른 키의 추론이 불가능해야 함

<표 2> 정보보호 기술 표준화 현황

· 국내 표준화 연구단체	국제 표준화 연구 단체
· 국립기술표준원 산하 전문위원회 · 한국통신기술협회(TTA) · 국립기술표준원 · 한국통신연구개발원 · 한국전자통신연구소 정보통신표준연구센타 · 개방형컴퓨터통신연구회(OSIA) · 한국통신정보보호학회(KIISC)	· SC27/WG1 · SC27/WG2 · SC27/WG3 · JTC1/SC21 · JTC1/SC6

<표 3> 암호화 제품들의 간단한 특징

종류	입출력크기	키크기	라운드수	특 징
DES	64비트	56비트	16라운드	참고자료 참조
FEAL	64비트	64비트	N라운드	
LOKI	64비트	64비트	16라운드	
GOST	64비트	256비트	32라운드	
IDEA	64비트	128비트	8라운드	
SAFER	64비트	64비트	6라운드	
MISTY	64비트	128비트	8라운드 이상	

<박스기사> 표준화 현황

현재까지 유일하게 표준화된 암호화 알고리즘 : DES

이외에도 RSA, MD5, RC2/RC4/RC5 등 수 많은 암호화 알고리즘이 존재하고 있으며, 각 국가들은 이에 대한 표준을 마련하려는 움직임을 보이고 있다. 하지만 세계 선진국들 간에는 암호화 기술을 하나의 국가경쟁력 제고를 위한 방안으로 고려, 국제적인 표준은 제정하지 않는다는 잠정적인 방침을 세웠다.

이와는 대조적으로 OECD에서는 각 암호 기술의 상호연동성 등을 고려한 표준마련을 추진하고 있다. OECD 가입국들은 오는 97년 5월 회의를 통해 표준에 대한 기본안을 마련할 계획이다. (이번 회의에서 우리나라는 OECD 가입 이후 최초로 승인에 참여)

<박스기사> 세계 각국의 주요 보안 기술

미국 · SkipJack - 64Bit I/O, Keysize 80

미국은 공모를 통해 보안 알고리즘의 민간표준을 제정하려는 움직임을 보이고 있다. 즉, IBM이나 MS, HP 등의 업체들을 위주로 하여 보안 알고리즘 개발을 공모하고 이를 국가에서 평가하여 표준으로 재정하는 방법을 추진하고 있다. 물론 여기서 개발 업체는 채택된 기술에 대한 아무런 권한(ex : 특허권)을 갖지 못한다. (DES도 이러한 공모를 통해 표준으로 추진된 경우)

한편 현재 미국 내의 표준으로 인식되고 있는 기술인 SkipJack은 알고리즘 자체가 기밀사항으로 간주돼, 그와 관련된 자료는 공개되지 않고 있다.

일본 : FEAL32

유럽(EU) : IDEA

러시아 : GOST

한국

현실적으로 그동안 국내에서는 이 분야에 대한 연구가 이루어지지 않았다. 최근 들어 국가적인 차원에서의 연구가 진행되고는 있지만, 관계자들은 이에 대한 내용에 대해 밝히기를 꺼려하고 있다. 특히 현재까지 국내에 도입된 알고리즘은 없으며, 향후 계획도 불투명하다.

<박스기사> 제품 수출 · 입의 제한

• 미국의 수출 제한 : 과거에는 키의 길이가 40Bit 이상일 경우를 군수품으로 간주하여 수출 대상 품목에서 제외시켰다. 하지만 최근 美 상무부 수출관리국(BXA)에서는 민간사용이 증가하면서 이를 2중사용품목(Dual-Uses)으로 지정, 예외조항으로 구분하고 있다. 상무부에서 지난해 12월 30일자로 발표한 내용에 따르면 현재 사용이 크게 줄어든 RC2/RC4, DES 등 40Bit 이하의 제품들의 수출이 가능하다. 또한 64Bit 이하(패리티를 제외한 경우 56Bit)의 DES 및 이와 동급의 성능을 가진 암호화 제품에 대해서는 상무부에서 성능을 검사하여 승인된 경우에 한해 수출할 수 있도록 하고 있다. 참고로 40Bit 이하의 제품들은 현재 해독이 가능하기 때문에 사용되지 않고 있다.

• 한국의 수입 제한 : 국내에서는 공중망에서의 암호화가 불가능하다(안기부에서 관리). 하지만 암호화 알고리즘의 수입에 대한 제한은 없는 실정이다. 이는 현재까지 수입된 알고리즘이 없기 때문에 이에 대한 제한을 가할만한 경우가 없었다는 것이 주요한 이유라고 할 수 있다. 다만 수입에 대한 제한이라고 한다면 수출을 하는 국가의 정책적인 문제에서 파악해야 한다. 즉 대상국이 관련제품에 대한 수출을 어떠한 형태로 제한하고 있는지가 가장 중요한 사항이 되는 것이다. (현재까지 이에 대한 정확한 기준은 없다)

김 형 만

광운대 경영학과 졸업(학사)
월간 컴퓨팅 기자
월간 네트워타임즈 기자
월간 오픈컴퓨팅 취재부 팀장 역임
현재 격주간 네트웍컴퓨팅 취재부 차장

한국컴퓨터 기자클럽(KCRC) 선정
'94년 올해의 기자상' 수상