특 집

전자상거래 보안

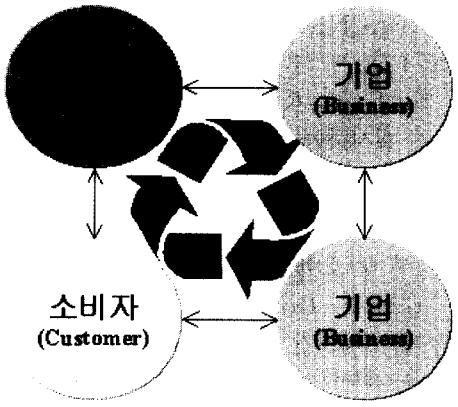
송 상 헌, 이 종 후, 류 재 철
충남대학교 정보통신공학부

I. 서 론

인터넷에 기반을 둔 전자상거래(Electronic Commerce)가 사이버스페이스(CyberSpace) 시대의 새로운 비지니스 개념으로 급부상하고 있다. 전자상거래(Electronic Commerce)의 정의[1]는 관련 기관마다 조금씩 다르지만, 그 근본적인 개념은 전자적 수단을 이용한 상거래라는 점이다. 즉, 인터넷이라는 가상공간에서 물건이나 서비스를 사고 파는 일련의 상거래 활동이라고 할 수 있다. 이러한 전자상거래의 거래 주체는 크게 소비자, 기업, 정부 세 부분으로 나뉜다. 이들 거래 주체별로 전자상거래의 유형을 분류해 보면 〈그림 1〉과 같이 '기업 대 소비자(B to C)', '기업 대 기업(B to B),' '기업 대 정부(B to G)', '정부 대 소비자(G to C)' 등으로 나눌 수 있다. 먼저 이러한 전자상거래 유형을 살펴보면 다음과 같다.

① 기업 대 소비자 전자상거래
(B to C : Business to Customer)

인터넷 비즈니스의 가장 일반적인 형태로 기업이 개인 소비자에게 제품을 판매하는 거래 유형이다. 유형(물리적) 상품 또는 디지털 상품의 생산자나 판매자들이 소비자들을 상대로 가상의 공간인 인터넷에서 쇼핑몰을 개설하고, 상품을 판매하는 형태에 해당하는 것으로 WWW(World Wide Web)의 보급과 더불어 급속도로 성장한 가장 대표적인 전자상거래 형태이다. 주요 취급 상품으로는 서적과 같은 지적 저작물이나 브랜드 등 확실한 소비재 상품들이며, 대금 결제는 전자지불시스템을 통하여 이루어진다.



〈그림 1〉 전자상거래 주체

② 기업 대 기업 전자상거래
(B to B : Business-to-Business)

기업과 기업이 판매와 구매의 주체가 되며, 기업과 기업 사이의 부품의 상호 조달, 유통망 공유 등을 인터넷을 통하여 처리하는 형태이다. 인터넷을 통한 거래 이전에도 EDI(Electronic Data Interchange)나 CALS(Commerce At Light Speed)로 주문, 공급자 관리, 재고 관리 등이 이루어져 왔다.

1) "일반적으로 문자, 음성, 이미지를 포함한 디지털 데이터의 전송과 처리에 기반을 두고, 조직과 개인의 상거래 행위와 관련한 모든 형태의 거래를 말한다(OECD, 1998)", "개방 네트워크를 통하여 기업과 기업, 최종소비자 및 공공 단체 사이에 발생하는 상거래 행위를 말한다(Anderson Consulting, 1999)", "재화나 용역의 거래에 있어 전부 또는 일부가 전자문서교환 등 전자적 방식에 의해 처리되는 거래(전자거래기본법, 1999)"

③ 기업 대 정부 전자상거래

(B to G : Business-to-Government)

현재 많이 이용되는 정부의 전자거래 유형은 조달업무 분야이다. 정부가 조달예상 상품을 인터넷 상에서 공시하고, 기업들은 상품공급을 하는 것을 말한다. 물론 조달업무만이 "B to G"에 속하는 것은 아니고, 기업과 정부간의 전자적 거래를 모두 포함한다. 정부에서 보면 막대한 비용절감을 할 수 있다. 미국은 오래 전부터 연방조달전산망(FACNET)을 구축한 바 있다. 국내의 경우도 EDI 시스템을 기반으로 구매, 계약과 관련한 기반을 구성하여 지방자치단체, 정부투자기관 등이 실시하는 입찰과정에 자격을 가진 기업을 중심으로 인터넷을 통한 조달업무 시스템을 구축하고 있다.

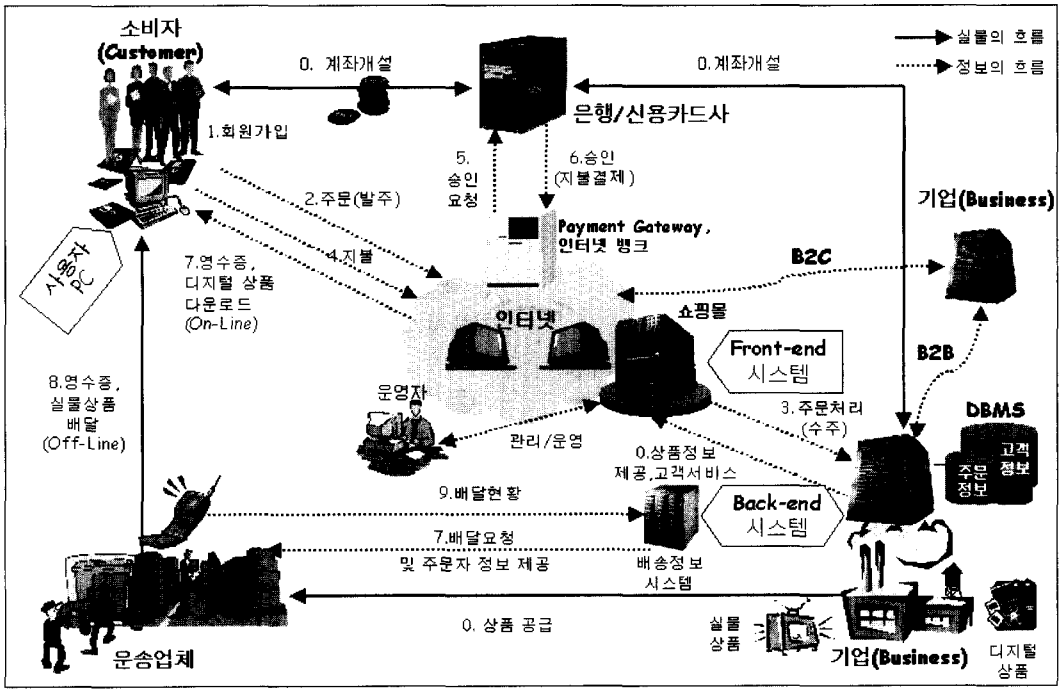
④ 정부 대 소비자 전자상거래

(G to C : Government-to-Customer)

정부와 소비자간 전자상거래는 정부가 정보통신기술을 활용하여 행정활동의 모든 과정을 혁신함으로써, 정부의 고객인 국민에게 질 높은 행정서비스를 제공하는 것에서 출발한다. 아직은 민원서비스 정도를 제공하는 초기 단계이지만, 점차 기업-소비자간 및 기업-정부간 전자상거래가 성장함에 따라 정부는 복지급여의 지급·세금환급, 의료보험, 국민연금 등과 같은 분야에 확대 적용할 것으로 보인다.

인터넷 및 네트워크를 활용하여 전자적으로 행해지는 전자상거래 행위의 기본 구성요소는 크게 주문(발주&수주), 계약, 대금청구&지불, 전송(배달) 등 4단계로 이루어지는데, 〈그림 2〉는 기업과 소비자간 전자상거래의 대표적인 모델로 손꼽히는 웹 기반의 인터넷 쇼핑몰 환경을 나타낸 것이다.

서비스 및 상품 판매자 측의 기업은 전자상거래를 위해 먼저 쇼핑몰이나 거래를 위한 홈페이지를 운영하기 위한 시스템을 구축해야 한다.이러한 시스템은 일반적으로 쇼핑몰 운영 및 고객서비스에 필요한 사용자 인터페이스 및 어플리케



〈그림 2〉 전자상거래 개념 모델

이션을 제공하는 Front-end 시스템과 데이터베이스를 기반으로 한 컨텐츠(Contents), 주문정보, 고객 정보 등을 생성/처리/저장/관리 등을 위한 Back-end 시스템을 네트워크로 연결하여 구축된다. 물론 여기에는 전자지불시스템이 필수적으로 연동되어야 한다.

소비자는 자신의 PC(Personal Computer)를 인터넷과 같은 통신망에 연결할 수 있는 환경을 갖추고, 넷스케입(Netscape), 인터넷 익스플로어(Internet Explorer) 등과 같은 웹 브라우저를 이용해 인터넷 쇼핑몰에 연결하면 된다. 이와 함께 대금지불을 위해 필요한 전자지갑 S/W 또는 신용카드를 가지고 있어야 한다.

이와 같은 전자상거래의 구현은 정보시스템(전자상거래 시스템)을 어떻게 안전하게 구축하고, 운용하는가가 핵심이라 할 수 있다. 특히, 전자상거래의 기반이 되는 인터넷은 본래 개방된 네트워크로 저장·처리·전송되는 정보는 적절한 보호 조치가 없으면 불법 도청 및 변조 등의 위험에 노출되기 쉽다. 따라서 이러한 불법적 행위에 따른 사고로 인해 개인 정보침해 뿐만 아니라 막대한 경제적 손실을 당할 위험이 있다.

이에 따라 본 고에서는 인터넷을 기반으로 하는 전자상거래 환경에서 필요한 보안 요구 사항을 살펴보고, 전자상거래에 필요한 보안 기술을 소개하고자 한다.

II. 전자상거래 보안 요구사항

전자상거래가 안전하게 전개되기 위해서 우선 고객정보 보호, 소비자와 판매자의 신뢰성 확보, 지적재산권 보호, 안전한 대금결제 등과 같은 여러 가지 제반 문제를 해결해야 한다. 이와 관련하여 요구되는 보안 요구 사항을 크게 6가지로 구분하여 정리해보면 다음과 같다.

1. 소비자 정보 보호와 프라이버시

IT 기술은 기업에게는 소비자의 선호에 관한 정보수집을 용이하게 해주며, 동시에 소비자에게는 상품정보를 찾기 쉽게 도와준다. 그러나 이러한 IT기술은 분명히 기업에게 많은 도움이 되는 반면에 개인정보를 누설할 기회를 함께 제공한다. 따라서 전자상거래에 있어서 소비자 개인에 관한 신상정보 및 거래정보의 수집·처리·이용·제공 활동이 적절히 통제되어야 한다. 그렇지 않을 경우 소비자들은 이러한 것들이 사생활을 침해할 수 있는 위협적 요소라고 생각할 수 있고, 이러한 인식은 전자상거래의 확산을 저해하게 된다.

2. 소비자와 기업(판매자)의 신뢰성 확보

인터넷 전자상거래는 그 행위가 인터넷이라는 가상공간에서 서로의 신원을 확인하기 어려운 특성으로 인해 사기 및 거래 부인의 가능성이 높다. 따라서 전자상거래의 안전성과 비대면간의 사용자 신뢰 확보를 위하여 거래 상대방의 신원확인과 의사표시의 진위여부를 확인하고, 신뢰할 수 있는 인증 방법이 필요하다.

3. 데이터 전송을 위한 네트워크(인터넷)의 안전성

인터넷은 본래 보안을 고려하지 않고 설계되어 적절한 보안 장치없이 전자상거래에 이용될 경우 정보의 불법 도청, 변조, 불법 접근과 서비스 거부공격 등의 보안침해 사고가 발생할 수 있다. 전자상거래가 활성화되기 위해서는 네트워크로 전송되는 정보의 기밀성, 무결성, 가용성 등과 같은 보안 서비스 제공이 무엇보다 중요하다.

4. 사용자 PC 및 기업의 서버 시스템 보호 및 안전한 운영

사용자의 PC 또는 기업의 서버 시스템은 정보를 처리/저장/관리하는 중요한 시스템이다. 그러나 이러한 시스템은 컴퓨터 바이러스, 시스템의 불법 침입 및 데이터 파괴 등과 같은 위협에 노출되어 있으며, 최근에는 대부분의 시스템이 인터넷에 연결되는 추세이기 때문에 해킹(크래킹)을 통한 위협이 더욱 가중되고 있는 상황이다. 따

라서 항상 시스템의 정보를 보호하기 위해 사용자 및 관리자는 보안 대책을 세우는데 고심해야 한다.

5. 지적재산권 보호

하루가 다르게 동영상, 이미지 등과 같은 멀티미디어를 활용한 다양한 컨텐츠(Contents)가 만들어지고, 새로운 소프트웨어가 개발되어 배포되고 있다. 이러한 상황에서 사용자들은 아무런 죄의식 없이 컨텐츠나 소프트웨어를 무단복제하고, 이것에 대한 불법 유통이 빈번하게 이루어지고 있는데, 이로 인해 발생하는 피해액은 어마 어마한 규모로 추정되고 있다. 따라서 전자상거래에서 무단복제가 용이한 이러한 멀티미디어 정보, 소프트웨어, 영화 등 디지털 상품에 대한 저작권은 반드시 보호되어야 할 대상이다. 이와 관련 최근 냅스터(Napster)와 미 음반산업협회(RIAA)의 소송, 해커들과 헐리웃 스튜디오 간의 DVD 해독 코드와 관련된 싸움 등 디지털 저작권에 관심이 집중되고 있다.

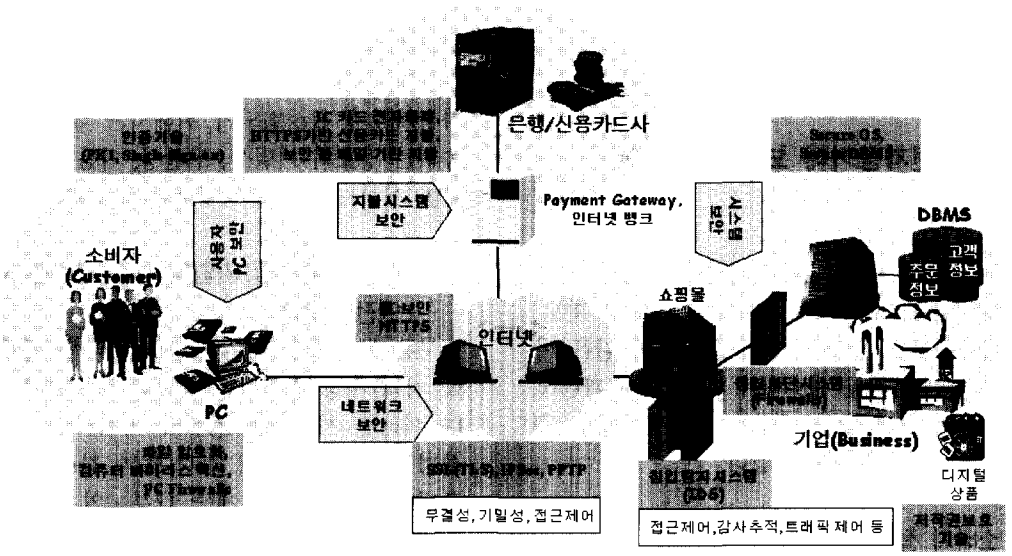
6. 안전한 전자지불 시스템 구축

인터넷을 기반으로 한 전자상거래의 핵심 요건 중 하나는 안전성과 효율성을 고루 갖춘 전자지불 시스템의 개발이다. 인터넷은 그 개방성으로 인하여 표준화된 보안 체계가 부족한 상태로, 거래에 참여하는 고객, 판매자 등이 서비스 및 상품에 대한 댓가를 안전하고 효과적으로 주고 받을 수 있는 정보 전달 및 대금지불 체계를 필요로 한다. 현재 이러한 전자지불 시스템은 전자화폐, 신용카드, 인터넷 뱅킹 등 다양한 솔루션이 개발되고, 이용되고 있지만 표준화를 비롯해 해결해야 할 문제가 적지 않다.

III. 전자상거래 보안 기술

전자상거래 환경에 필요한 보안 서비스를 효과적으로 제공하기 위한 전자상거래 보안은 매우 포괄적인 의미를 지니는데, 〈그림 3〉은 전자상거래에 필요한 대표적인 보안 기술을 도식화 한 것이다.

전자상거래 보안은 Secure OS, 침입차단 및 침입탐지 기술 등과 같은 시스템 보안(System Security)과 SSL, IPSec 등과 같은 네트워크



〈그림 3〉 전자상거래 보안

보안(Network Security), 이와 함께 안전한 전자상거래 실현을 위해 사용자 고객정보 보호 및 프라이버시 보호 기술, X.509 공개키 인증서 및 SSO(Single Sign-On) 등과 같은 인증(Authentication) 기술, 안전한 전자결제를 위한 지불시스템 보안, 컨텐트, 소프트웨어 등과 같은 디지털 상품을 보호하기 위한 지적재산권 보호 기술 등 다양한 보안 기술이 포괄적으로 요구되는 분야이다.

1. 컴퓨터 시스템 보안 (Computer System Security)

컴퓨터 시스템 보안(Computer System Security)은 컴퓨터를 이용해 저장되고, 처리되는 정보의 기밀성, 무결성, 가용성을 보장하기 위해 필요한 대책과 통제를 의미한다. 시스템 보안은 인터넷을 구성하고 있는 컴퓨터, 네트워크 장치(라우터 등)에 대한 보안으로 여기에는 운영체제, 클라이언트/서버 어플리케이션, 파일 시스템 등에 대한 보안을 포함하며, Secure OS, 침입차단 및 침입탐지시스템, 바이러스 백신, 파일 암호화 S/W 등 다양한 제품이 개발되고 있다. 최근 대표적인 해킹 툴인 '백오피리스'나 '트로이목마' 등이 인터넷을 통해 널리 퍼지고 있으며, 개인 PC 사용자간에 파일을 공유하는 P2P서비스가 활성화되면서 PC 보안에 대한 관심이 날로 높아지고 있다. 이와 함께 PC용 침입차단시스템과 암호화 솔루션이 계속 등장하고 있으며, 하드웨어 기반의 휴대형 개인정보 보호장치도 다양한 형태로 선보이고 있다.

◆ 침입차단시스템(Firewalls)

외부의 침입으로부터 조직 내의 컴퓨터 시스템 및 정보를 보호하기 위해 가장 널리 사용되고 있는 것이 침입차단시스템이다. 인트라넷과 같은 비공개 네트워크와 인터넷 사이에 위치하여 외부로부터 접근하는 연결을 감시하고, 접근제어를 할 수 있는 시스템이다. 또한 둘 이상의 침입차단시스템 사이에서 VPN(Virtual Private Network) 서비스를 제공할 수 있도록 개발하고 있다.

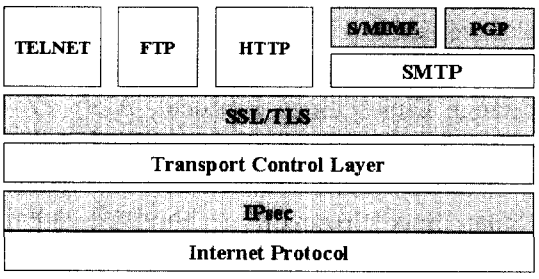
◆ 침입탐지시스템 (Intrusion Detection System ; IDS)

침입탐지 시스템은 침입의 패턴 데이터 베이스와 전문가시스템(Expert System)을 사용하여 네트워크(Network-based IDS)나 시스템(Host-based IDS)사용을 실시간으로 모니터링하고, 불법적인 데이터 접근, 비권한 명령어 수행 등을 검출하여 침입을 조기에 발견하는 시스템으로 침입차단시스템을 통과한 침입자에 대한 제2의 보안대책이라 할 수 있다.

2. 네트워크 보안(Network Security)

네트워크 보안은 시스템과 시스템을 연결하는 통신프로토콜에 대한 보안으로 네트워크를 통해 전송되는 데이터 보호가 가장 중요한 요소이다. 따라서 TELNET, FTP, HTTP, SMTP 등과 같은 모든 통신 프로토콜을 통해 전송되는 데이터 보호를 의미하는데, 네트워크 특성상 상호운용성(Interoperability)이 요구되는 분야이기 때문에 표준화 경향이 뚜렷한 분야이다. 현재 이러한 인터넷에서의 네트워크 보안 기술은 〈그림 4〉와 같이 어플리케이션 또는 TCP/IP 프로토콜 부분에서 보안 서비스를 제공하는 방식을 취하고 있다. 즉, 데이터를 처리하는 어플리케이션 자체를 안전하게 만들거나 또는 어플리케이션 데이터가 전송되는 통신 프로토콜을 안전하게 만드는 것이다.

이러한 어플리케이션 부분에서 보안을 제공하는 대표적인 기술로 전자우편 보안을 위한 S/MIME과 PGP(Pretty Good Security)가 있



〈그림 4〉 네트워크 보안 기술

다. TCP/IP 부분에서 보안 서비스를 제공하고자 하는 것으로 TCP 계층의 바로 위 계층에 추가된 SSL(Secure Socket Layer) 및 TLS(Transport Layser Security), IP 계층에 통합된 형태로 개발되고 있는 IPSec이 제안되어 있는 상태이며, 이에 대한 표준화가 활발히 진행중에 있다.

◆ SSL(Secure Socket Layer)

SSL은 대표적인 웹 브라우저 개발업체인 넷스케입(Netscape) 사에서 1994년 7월 경에 처음으로 제안한 것으로 자사의 웹 제품에 구현되어 널리 사용되면서 웹 보안의 대명사로 알려진 보안 프로토콜이다. SSL은 1995년 11월에 SSL V3.0가 발표된 이후 1996년 초에 IETF(Internet Engineering Task Force)에서 TLS(Transport Layer Security)라는 W/G이 결성되어 이에 대한 표준화를 진행중이다.

◆ TLS(Transport Layer Security)

TLS는 넷스케입 사에서 제안한 SSL V3.0를 표준화하기 위한 보안 프로토콜이다. 이것은 SSL과 마찬가지로 TCP 계층 바로 위에 위치하여 다양한 응용 프로토콜의 채널 자체를 보호하는 기능을 하며, 클라이언트/서버 인증, 기밀성, 무결성 등과 같은 보안 서비스를 제공하게 된다. 따라서 TLS의 보안 서비스를 이용하고자 하는 어플리케이션은 수정없이 사용할 수 있다. 그러나 TLS는 메시지의 전자서명 기능은 제공되지 않는데, 왜냐하면 클라이언트와 서버의 한 세션 동안 수행되는 모든 송수신 데이터에 대해 전자서명을 하는 것은 비효율적일 뿐 아니라 전자서명은 송수신자(End-to-End)의 인증에 적합한 보안 서비스이기 때문이다. TLS의 기본 구조는 SSL과 마찬가지로 Handshake Protocol, Change Cipher Spec Protocol, Alert Protocol, Record Protocol 등과 같이 네 부분으로 구성된다. Handshake Protocol과 Change Cipher Spec Protocol은 클라이언트가 서버에 연결할 때 X.509 공개키 인증서를 이용해 서버 인증 및 키 교환을 위한 절차를 수행하며, 메시지에 대한 기밀성 및 무결성 서비스는 Record Protocol에서 제공된다.

3. 인증 기술

최근 인터넷 쇼핑몰과 같은 B2C 전자상거래가 활성화되면서 정보 위조 및 유출에 대한 위협 뿐만 아니라 신분 위장에 의한 사기사건이 크게 문제가 되고 있다. 즉 거래 상대방과 직접 대면하지 않는 네트워크 거래의 특성상, 클라이언트(사용자)와 서버(서비스 제공자)는 서로에 대한 신뢰를 확보하기 어려운 점에 기인한 것이다. 따라서 거래 상대방에 대한 신원 확인 작업인 인증의 중요성이 커지고 있다. 이러한 인증 서비스에 이용되는 기술은 기존의 아이디와 패스워드를 이용한 방식, 일회용 패스워드(One Time Password; OTP) 방식, X.509 공개키 인증서를 이용한 방식, 커버로스(Kerberos), SSO(Single Sign On) 등이 있다.

아이디와 패스워드를 이용한 방식은 지금까지 널리 이용되고 있는데, 도청을 통해 쉽게 패스워드가 노출될 수 있는 단점을 가지고 있어 로그인할 때 마다 패스워드를 달리 사용하는 일회용 패스워드 방식으로 대체되기도 한다. 그러나 이러한 패스워드 기반의 인증 기법은 사용자 인증에 국한되는 제약이 따른다.

X.509 공개키 인증서는 인증기관(CA)이 공개키 소유자의 신원확인을 통해 발행하는 것으로서 사용자 인증은 물론 전자서명을 통한 거래내용에 대한 인증 등을 제공할 수 있다. 이러한 X.509 규격은 ITU에서는 표준으로 채택되었으며, IETF에서는 PKIX(Public Key Infrastructure(X.509)) 워킹 그룹을 결성하여 공개키 기반의 인증시스템에 대한 표준화 작업을 추진하고 있다.

이와함께 커버로스(Kerberos), SSO(Single Sign On)는 인증 절차를 매번 거쳐야 하는 불편을 해소하고자, 한번의 인증 절차로 여러 전자상거래 서비스를 함께 이용할 수 있도록 하는 기술로서 최근 각광을 받고 있는 기술이다.

최근 인증 서비스가 본격적인 전자상거래 및

응용 서비스의 성공을 위해 반드시 필요한 요소로 부각되면서, 미국을 중심으로 한 세계 각국에서는 이미 인증 서비스가 실험단계를 거쳐 상용화단계에 이르고 있다. 국내에서도 전자거래기본법, 전자서명법 등의 법률이 이미 제정되었으며, 이를 통해 공인인증체계가 구축되어 본격적인 전자상거래 및 인증 서비스를 위한 환경이 갖추어졌다고 할 수 있다.

4. 지불시스템

최근 몇 년 동안 국내외 전자상거래 시장이 급속하게 성장하면서 전자거래의 필수 요소인 전자지불시스템 개발이 활발하게 진행되고 있다. 이러한 전자지불시스템은 크게 지불 브로커 시스템(보통 Payment Gateway ; PG 시스템이라고 함)과 전자화폐 시스템으로 구분할 수 있다. 두 시스템 모두 전자상거래 분야 특히 B-to-C로 대표되는 인터넷 쇼핑몰에서 고객이 상품을 구입할 때 편리하고, 안전하게 대금 결제를 할 수 있도록 개발된 시스템이다. 경우에 따라 인터넷 상에서 거래에 대한 대금결제를 계좌이체로 대신 할 수 있는 인터넷 뱅킹 시스템을 전자지불시스템에 포함시키기도 하지만 기존의 은행거래 일부를 인터넷 서비스의 형태로 제공하기 위해 개발되었다는 점에서 전자지불시스템과 다소 차이가 있다.

지불브로커 시스템과 전자화폐 시스템은 인터넷을 이용한 전자상거래에 사용할 수 있는 지불수단이란 점에서 동일한 시스템으로 보이지만 내부적으로 동작하는 메커니즘은 매우 다르다.

지불브로커(Payment Broker) 시스템은 고객이 신용카드를 이용해 인터넷 상에서 거래에 대한 지불을 할 수 있도록 개발된 것이다. 신용카드를 이용한 거래가 일반화되어 있는 현재, 가장 널리 이용되고 있는 시스템으로 고객과 인터넷 쇼핑몰이 서로를 신뢰할 수 없는 상황에서 지불브로커가 고객과 쇼핑몰 사이에서 신용카드 결재에 대한 중개인 역할을 해 줌으로써 신용카드를 안전하게 이용할 수 있도록 하는 구조로 되어 있다. 그렇지만 이 시스템은 신용카드를 소지하고 있는 고객만 이용할 수 있다는 제약이 따르며, 신용카드 이용에 따른 수수료 지불과 같은 제반 환경상 고액의 거래에 적합한 특성을 지니고 있다.

전자화폐 시스템은 기존의 현금과 동일한 가치를 지니는 디지털 정보 형태의 전자화폐를 고객에게 발행해 줌으로써 전자화폐를 거래에 항시 이용할 수 있도록 한 것으로 선불카드/직불카드를 한 단계 발전시킨 시스템이다. 이러한 전자화폐는 기존의 현금과 동일한 가치를 지니며, 신용카드와 달리 남녀노소 구분 없이 누구나 편리하게 사용할 수 있는 장점을 지닌다. 고객은 은행/신용카드 사로부터 IC카드 형태의 전자지갑을 발급 받고, 자신의 은행계좌의 금액 또는 현금을 전자화폐로 발행 받은 후 인터넷 쇼핑몰에서 물건을 구입하고, 이에 대한 결제를 할 수 있을 뿐 만 아니라 기존의 상점에서 대금결제 수단으로 이용할 수 있다. 즉 기존의 대표적인 지불 수단인 현금의 사용 범위를 실세계는 물론 인터넷까지 확장한 획기적인 전자지불 수단이라 할 수 있다. 또한 거래 금액 면에서 신용카드를 이용한 지불브로커 시스템과 비교해 볼 때 전자화폐 시스템은 현금과 같이 소액의 거래에 적합한 특성을 가지고 있다.

초기에 개발된 전자화폐 시스템은 개인의 PC에 소프트웨어 전자지갑을 설치하여 이용할 수 있는 형태로 개발되었는데, 1994년 경에 네덜란드 DigiCash사에서 개발한 Ecash가 대표적인 전자화폐 시스템이다. 그러나 이러한 소프트웨어 전자지갑 방식을 이용한 시스템은 모든 정보가 PC에 저장되어 관리되기 때문에 이동성이 떨어지는 단점을 지닌다. 또한 전자화폐의 위조 및 이중사용과 같은 보안 위협에 대처할 수 있도록 복잡한 보안 구조 및 프로토콜을 지닌 형태로 개발해야 하는 여러 가지 부담으로 인해 널리 사용되지 못하였다.

최근 전자화폐 시스템은 높은 보안성과 휴대성을 지니고 있는 IC카드를 이용해 전자지갑을 구현하고, 여기에 기존의 현금과 동일한 가치를 지니는 전자화폐를 저장하여 전자거래에 즉시 이용할 수 있도록 한 IC카드 기반 전자화폐 시스템이 각광을 받고 있다.

IC카드는 높은 보안성을 지니고 있음에도 불구하고 초기에 높은 개발비용과 다양한 어플리케이션을 제공하기 어려워 제한적으로 사용되었다. 그러나 최근 IC 카드 개발 기술의 발전과 함께 IC카드와 단말기 가격이 하락하고, Java 기술 등을 접목하면서 다양한 어플리케이션을 수용할 수 있게 되어 전자화폐 시스템은 IC 카드를 기반으로 개발되고 있다.

전자화폐 시스템은 금액 정보를 비롯한 모든 거래 정보는 디지털 형태로 저장되고, 금융망 또는 인터넷과 같은 네트워크를 통해 전송되는데, 디지털 정보는 특성상 불법적인 제3자에 의해서 위조되거나 변조될 가능성이 매우 높다. 따라서 전자화폐를 이용하기 위해서는 안전성과 신뢰성은 매우 중요한 요소인데, IC 카드는 디지털 정보 형태의 전자화폐, 거래 내역 등과 같이 중요한 정보를 안전하게 보호하고, 저장하는데 매우 적합한 기술로 평가되고 있다. 이에 최근 몇 년 사이 국내외적으로 IC 카드를 이용한 전자화폐시스템 개발을 서두르고 있다.

5. 저작권 보호 기술

이미지(Image), 오디오(audio), 멀티미디어 데이터(multimedia dat) 등과 같은 디지털 정보로 구성되는 컨텐츠(Contents)는 복사하기 쉽고, 일단 복사하면 원본과 완전히 동일하다. 또한 복사 횟수의 제한마저 없어서 배포가 용이한 특성을 지니고 있다. 이에 대비하여 최근에 등장하게 된 것이 워터마킹(watermarking)이라는 기술이다. 이 기술은 이미지(Image), 오디오(audio), 멀티미디어 데이터(multimedia data) 등의 원 소유주만이 아는 신호를 사람의 육안이나 귀로는 구별할 수 없게 삽입하고 이를 사용자들에게 제공한다. 소유주의 신호가 들어 있는 자료를 구입한 사용자들이 소유주의 허락없이 상업용으로 이용하거나 불법적인 용도로 사용하였을 시 소유주는 그러한 자료에서 자신의 넣었던 신호를 추출하여 자신의 권리를 찾을 수 있다. 또한 사용자들이 자료를 변형시키거나 가공하였어도 소유주는 그런 자료에서도 자신의 신호를 추출할 수 있다.

최근에는 워터마킹 기술에 해쉬, 전자서명 등과 같은 암호기술을 접목하고 있으며, 또한 DRM (Digital Rights Managements) 기술이 등장하고 있다. DRM은 워터마킹 기술과는 달리 과금 체계가 접목된 기술로서 컨텐츠 유통의 안전성을 보장하기 위한 기술이다.

6. 개인정보 보호와 프라이버시

컴퓨터를 이용한 정보처리기술의 발달로 인해 개인에 관한 정보를 대량으로 수집하고, 이를 분석하기 용이함으로써 개인정보에 관한 상업적 이용 가능성이 매우 높아졌다. 그러나 개인정보에 관한 상업적 이용은 개인정보 침해, 유출, 근본적으로는 프라이버시 침해라는 우려를 증폭시키고 있다. 개인정보침해 주요사례를 요약하면 다음과 같다.

1. 회원탈퇴 및 개인정보 열람·정정·삭제요구 불응
2. 이메일주소 유출(이메일주소의 경우에는 인터넷상에서의 공개성이 다소 높은 정보이고, 입수경로가 워낙 다양)
3. 이용자의 동의없는 제3자 제공
4. 개인정보 미파기(회원탈퇴후 개인정보를 계속 보유)
5. ID 도용으로 인한 이용요금 과다 청구
6. 주민등록번호 도용으로 인한 무단회원가입 등

이와 같이 정보시스템 발전에 따른 개인정보유출에 대한 우려를 반영하여 1980년 OECD에서는 프라이버시 보호에 관한 가이드라인을 채택하였다. 이 가이드라인은 특정한 기술을 염두해 두지 않고 작성된 것이기 때문에 급속히 변화하는 환경에서도 적용될 수 있는 큰 원칙을 제시하였다. 가이드라인의 주요원칙은 데이터를 수집할 때에 그 사용목적을 명기하고 이후 목적을 바꿀 때에는 매번 이를 명기할 것, 정보주체의 인지나 동의가 있을 것, 명기된 사용목적 이외에는 정보주체의 동의가 있거나 법원의 요구 없이 전용하지 말 것, 정보주체의 권리보장 등으로 이루어져

있다.

국내에서도 온라인 개인정보보호를 위해 1999년 7월 "정보통신망이용촉진등에관한법률"을 개정하여 정보통신망을 통해 수집·유통되는 개인정보에 관한 보호규정들을 신설하였다. 그리고 2000년 6월, 정보통신서비스이용자의 개인정보를 보다 효과적으로 보호하기 위하여 개인정보보호지침을 제정, 개인정보를 수집하는 서비스제공자가 지켜야 할 구체적인 사항을 정한 개인정보보호지침을 마련하고 있다. 이와 관련하여 W3C컨소시엄에 추진중인 P3P를 소개하면 다음과 같다.

◆ Platform for Privacy Preferences (P3P)

W3C(World Wide Web) 컨소시엄에서 개발 중인 Platform for Privacy Preferences Project (P3P)는 사용자가 방문하는 웹 사이트에서 사용자 자신의 정보 사용을 좀 더 안전하고, 쉽게 제어할 수 있도록 하기 위한 기술이다. 이를 위해 P3P는 프라이버시 정책에 대한 표준을 정의하여 사용자가 웹 사이트에 접근하면 웹 사이트는 먼저 프라이버시 정책을 사용자에게 보냄으로써 프라이버시 정책에 포함된 개인정보에 대한 관리규정을 사용자가 알 수 있게 된다. 사용자가 그 정책에 대해 동의하게 되면 비로서 웹 사이트는 컨텐트를 전송하게 된다. 즉 이러한 P3P 기술을 통해 사용자에게 프라이버시 정책을 제공함으로써 사용자는 개인정보 보호와 프라이버시를 지키는 수단으로 이용할 수 있게 된다.

Ⅳ. 결 론

안전한 전자상거래의 구현은 단순히 몇 개의 보안 프로그램을 설치 및 운용하는 것만으로 이를 수 있는 것이 아니라, 시스템 보안기술, 네트워크 보안기술, 어플리케이션 보안기술 등 다양한 보안기술을 효율적이고 체계적으로 관리/운영함으로써 가능하다. 또한 과거에는 기업과 소비자(B to C) 전자상거래가 대부분이었으나, 최근의 전자상거래는 기업과 기업(B to B), 기업과 정부(B to G) 등으로 범위를 확장해 가고 있으며, 이에 따라 적용되는 전자상거래 보안기술 역시 좀 더 복잡하고 다양해질 수밖에 없다. 따라서 위에서 언급한 보안기술들에 대한 연구와 함께 네트워크의 안전성 및 신뢰성, 사용자 PC 및 기업의 서버 시스템 보호, 보안 관리를 통한 운영, 지적재산권 보호, 안전한 전자지불 시스템 구축, 정보의 적절한 규제 등이 체계적인 연계성을 맺는 가운데 이루어져야 한다.

전자상거래가 보다 더 성숙하기 위해서는 정보통신기술 수준의 향상뿐만 아니라, 이를 안전하고 효율적으로 운용하는 것이 중요하다. 이를 위해서 전자상거래 기술의 표준화, 관련 법·제도적 틀의 정비는 빼놓을 수 없는 중요한 요소이다. 이와 관련하여 전자지불 기술, 암호기술, PKI, 전자우편 등 전자상거래에 필요한 보안기술 분야의 표준화가 ISO, IETF 등의 국제 표준화 기구에 의해서 이루어지고 있으며, 국내에서도 독자적인 기술표준의 개발작업이 진행되고 있다. 또한 미국, 독일을 비롯한 대부분의 국가에서는 전자서명법을 제정하여 시행하고 있으며, 국내에서도 전자거래기본법, 전자서명법 등이 제정되어 시행되면서 전자상거래 운용 환경이 점차 성숙되고 있는 상황이다.

전자상거래는 이제 단순한 인터넷 응용 서비스의 하나가 아니라, 우리의 생활과 밀접한 관계를 갖는 생활수단으로 받아들여지고 있다. 이러한 상황에서 전자상거래를 더욱 활성화시키고, 이를 이용하는 사용자들에게 보다 많은 편익을 주기 위해서는 전자상거래 보안의 중요성을 인식함과 동시에 정부, 기업, 학계의 전자상거래 보안 기술에 대한 지속적인 연구가 이루어져야 할 것이다.

참 고 문 헌

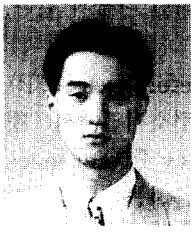
[1] Cryptography and Network Security: Principles and Practice Second Edition, William Stallings, Prentice-Hall, Inc.

〔2〕 Digital Certificates/Applied Internet Security, Jalal Feghhi, Peter Williams, Addison-Wesley, pp. 127-161.
〔3〕 SSL 3.0 SPECIFICATION, http://home.netscape.com/eng/ssl3/3-SPEC.HTM
〔4〕 IP Security Protocol (ipsec), IETF, http://www.ietf.org/html.charters/ipsec-charter.html
〔5〕 Building Internet Firewalls, D. Brent Chapman and Elizabeth Zwicky, O'Reilly & Associates 1995.
〔6〕 전자상거래 통계조사 결과, 통계청, 2001. 4

저 자 소 개

宋 尙 憲

1974년 1월 1일생, 1995년 2월 배재대학교 전자계산학과 학사, 1997년 2월 충남대학교 대학원 컴퓨터과학과 석사, 2001년 2월 충남대학교 대학원 컴퓨터과학과 박사수료, 〈주관심 분야 : 네트워크 보안, 전자지불시스템〉



李 鍾 厚

1973년 2월 6일생, 1997년 2월 충남대학교 자연과학대학 컴퓨터과학과 학사, 1999년 2월 충남대학교 대학원 컴퓨터과학과 석사, 1999년 3월~현재 : 충남대학교 대학원 컴퓨터과학과 박사과정, 〈주관심 분야 : 네트워크 보안, PKI〉

柳 在 哲

1962년 10월 3일생, 1985년 2월 한양대학교 산업공학 학사, 1988년 5월 Iowa State University 전산학 석사, 1990년 12월 Northwestern University 전산학 박사, 1995년 6월~1996년 6월 : 시스템공학연구소 초빙연구원, 1999년 9월~2000년 9월 : 금융결제원 전산고문, 2000년 3월~2001년 3월 : 주택은행 자문위원, 1991년 4월~현재 : 충남대학교 정보통신공학부 부교수, 〈주관심 분야 : 인터넷 보안, 전자지불시스템〉