主題

전자상거래의 보안

한국항공대학교 통신정보공학과 권 용 진
한국항공대학교 항공전자공학과 김 정 선

차 례

1. 서론
2. 전자상거래의 개념
3. 전자상거래 보안
4. 전자상거래 보안 기술 동향
5. 전자상거래 시스템의 사후보안
6. 결론

I. 서 론

최근 정보통신 기술의 발달과 전세계적인 규모의 통신 기반인 인터넷은 전자상거래(Electronic Commerce)라는 새로운 경제 패러다임을 창출하고 있다. 이를 기반으로 사이버 기업(Cyber Company), 사이버 마켓(Cyber Market), 사이버 거래사회(Cyber Trading Community) 등과 같은 신종 기업/비지니스 문화가 탄생하고 있으며, 시간과 장소의 제약에서 탈피하여, 국경의 한계를 초월한 새로운 경제 질서와 문화를 바탕으로 전자적인 비지니스를 실현할 수 있는 환경이 마련되었다.

오늘날 전자상거래가 황금알을 낳는 경제활동으로 주목을 받고 있는 주된 이유는, 기술적인 측면에서 웹(WWW)과 브라우저(Browser)의 등장으로 대변되는 컴퓨터와 네트워크의 기술 그리고 멀티미디어 기술 등의 정보통신 기술의 발달로 인해 실생활의 여러 활동을 모방할 수 있는 가능성이 열렸기 때문이다. 또한 경제적인 측면에서는 전자상거래를 경제활동에 도입하면 상거래 비용이 절감되는 등의 탄력성있는 기업/경제활동이 가능하여 새로운 시장의 개척이 용이하기 때문이다.

통신망을 이용한 전자상거래는 대부분 웹을 기반으로 이루어 지고 있다. 이는 인터넷은 전세계적인 연결을 보장하고 수천만이상의 사용자들이 있다는 점에서 전자상거래의 주요 무대로 인식되고 있기 때문이다. 그러나 시간과 장소의 제약을 탈피시킬 수 있다는 인터넷의 동작적 및 구조적 특성은 거래 내역의 유출 용이, 거래 내역의 부인 용이 등으로 인해, 경제활동의 일환인 전자상거래에는 부적합한 것 또한 사실이다. 아니 전자상거래의 특성과 장점을 활용할 수 있는 어떠한 인프라도 인터넷과 같은 약점을 노출시킬 수 밖에 없을 것이다. 따라서 전자상

거래의 기반환경으로 가장 중요한 요소는 바로 보안(Security)문제이다.

본 고에서는 전자상거래가 가능하기 위한 안전 요소 즉 전자상거래의 보안에 대해 정리하고자 한다. 이를 위해서는 먼저 전자상거래의 개념 및 기술적인 요소, 전자상거래에 예상되는 보안 문제점, 그리고 정보보안 기술 동향에 대해서 살펴보고자 한다. 특히, 실제적으로 구현된 전자상거래 시스템이 현실 사회 구조의 일원으로써 가동되어 많은 사람들이 사용하고 있는 가운데, 어떠한 요인으로 인해 심각한 보안상의 문제가 발생했다고 해서 이 시스템을 정지 가능 할 것인가에 대해서 언급하고자 한다.

2. 전자상거래의 개념

2.1 전자상거래의 정의

전자상거래는 일반적으로 컴퓨터를 통해 전자적인 방식으로 상품, 정보 등의 구매, 조달, 지불행위를 수행하는 것을 의미한다. 전자상거래의 정의는 학자들의 주관적인 관점 등 여러 가지 관점에서 다양하게 내릴 수 있겠지만, 광의의 전자상거래는 사이버 공간에서 수행되는 모든 상거래 행위와 이를 지원하는 활동들을 포함하는 일련의 행위을 말하고 있는 듯하고, 협의의 전자상거래는 인터넷을 통해 상거래 행위에 관련된 문자뿐만 아니라 멀티미디어 정보 등을 쉽게 교환하는 절차를 말하고 있는 듯하다.

전자상거래는 개념적으로 전자상거래를 위한 기반구조와 응용시스템으로 구분할 수 있다.[1] 전자상점, 전자조달, 전자경매, 인터넷 뱅킹, 가상대학, 온라인 관광, 인터넷 무역 등과 같은 다양한 형태의 비즈니스 모델로의 응용시스템과 이러한 응용시스템이 구현되기 위한 전자상거래 기반구조인 기술적(네트워크와 정보기술), 기능적(표준), 제도적(법·제도), 사회적(인식, 교육) 기반이 그것이다.

2.2 전자상거래의 구현

전자상거래는 실물상거래 과정을 전자적으로 구현한 것으로서, 실물상거래 환경에서는 건물(사무실, 공장, 매장 등)과 도로망으로 구성된 도시에서 사람이 각종 교통규칙에 따라 이동하게 된다. 이를 기반으로 구매자와 판매자간의 거래행위가 이루어지고, 유통된 화폐는 은행을 통해 재 유통되며, 상품은 판매자간의 요구에 따라 제조에서 유통단계를 거쳐 판매점으로 공급된다.

전자상거래 환경에서는 컴퓨터와 통신망으로 구성된 사이버도시(Cyber City)를 기반으로 고객, 판매점, 은행이 암호화된 전자상거래 체계와 프로토콜을 통해 온라인으로 연결되며, 제조, 유통과정 등도 전자적으로 실현된다. 이와 같은 전자상거래가 실현되기 위해서는 기본적으로 다음과 같은 기본요건이 만족되어야 한다.[3]

첫째, 전달 정보의 보안대책이 강구되어야 한다. 인터넷과 웹 프로토콜은 정보전달의 안전성이 없다. 따라서, 거래내용의 노출을 방지하기 위한 기밀성(Confidentiality), 거래전문의 변조와 위조 그리고 승인되지 않은 거래전문의 생성을 방지하기 위한 무결성(Integrity) 보장대책이 마련되어야 한다.

둘째, 거래의 확인 및 인증체계가 정립되어야 한다. 네트워 거래에서는 당사자를 서로 확인할 수 없으므로 거래에 따른 부인(Repudiation), 위조(Counterfeit), 복제(Replication)등을 방지하기 위한 상대방 확인체제가 정립되어야 한다.

셋째, 전자적인 지불수단 및 체계가 정립되어야 한다. 인터넷에서는 국경 없는 거래행위가 가능하므로 세계적으로 통용될 수 있는 전자적인 지불수단이 확보되어야 하며, 고객의 편의를 위해 선불, 직불, 후불은 물론 고액, 중규모액, 소액 지불 등 다양한 지불수단이 확보되어야 한다.

넷째, 전자적인 거래에 따른 각 국의 정책과 제도가 정립되어야 한다. 인터넷 상거래를 위해서는 암호화, 전자서명 및 전자영수증 등에 대한 법적효력, 운송, 과세 및 관세, 소비자 보호 등과 관련된 법제도 등 제도적인 기반이 정비되어야 한다.

2.3 전자상거래의 기술체계

전자상거래가 구현되기 위해서는 다양한 정보통신기술이 복합적으로 연계되어야 하며, 이는 전자상거래 시스템을 구축하기 위해서 이용되는 기술과 이러한 기술간의 상관관계가 복잡하다는 것을 의미한다. 따라서 전자상거래와 관련된 기술을 체계적으로 정립하기는 쉽지 않다. 우리나라의 경우, 한국전산원에서 전자상거래의 기술적 구조를 아래의 표 1과 같이 구성하고 있다.[10,11] 한국전산원의 전자상거래 기술체계에 대한 모델링 작업은 다음과 같이 2가지 접근방법으로 시도되었다.

첫째, 기술 분류는 전자상거래에 관련된 모든 정보기술을 망라하지 않고 현재 활용되는 주요 기술을 대상으로 한정하였으며, 기술 발전 동향을 감안하여 인터넷 관련 기술에 초점을 두었다.

둘째, 전자상거래 시스템이 수행하는 기능을 세부 기술간의 상관관계를 고려하여 논리적인 관점에서 계층화하여 분류하였다. 이러한 세부 기술간의 상관관계를 나타내는 전자상거래의 기술구조는 전자상거래 시스템의 참조모델과 같은 성격을 가지며, 상거래 행위를 직접적으로 지원하는 시장 특화된 응용(Market Specific Application)계층에서부터, 일반적인 응용(Generic Application)계층, 미들웨어 계층, 기반서비스 계층, 통신 서비스 계층, 통신 네트워크 계층에 이르는 수직적인 구조와 이러한 6개의 계층에 공통적으로 적용되는 보안/인증 서비스 계층으로 구성된다.

아래의 표 2에는 전자상거래 기술체계의 각 계층 분류에 따른 관련 기술 및 특징을 나타내고 있다.

2.4. 전자상거래 시스템의 구성

전자상거래를 위해서는 앞에서 언급한 기본요건을 만족하는 필수 요소시스템들이 구현되어 거래 인프라가 형성되어야 하며, 기업들의 정보 및 거래 서버들이 거래 인프라와 결합됨으로써 고객과 기업간, 기업과 기업간에 안전한 거래 및 지불환경이 구현된다.

전자상거래 시스템은 그림 1과 같이 인증기관(Certificate Authority), 전자지갑(Digital wallet)을 장착한 고객시스템, 지불시스템(Payment system), 상점시스템(Merchant system)으로 구성되며, 안전한 상거래는 사전 인

<table>
<tr><th>계층구조</th><th colspan="3">기술구조</th></tr>
<tr><td rowspan="2">Market Specific Application</td><td colspan="2">광고, 검색, 주문, 지불</td><td rowspan="7">인증/보안</td></tr>
<tr><td>E-Catalog, E-mail</td><td rowspan="4">Directory Service</td></tr>
<tr><td>General Application</td><td>BBS, E-Form, EDI</td></tr>
<tr><td>미들웨어</td><td>RDA, ORB</td></tr>
<tr><td>기반서비스</td><td>E-mail, FTP</td></tr>
<tr><td>Communication Service</td><td>X.400, SMTP/MINE</td><td>X.500, LDAP</td></tr>
<tr><td>Communication Network</td><td colspan="2">PSTN, PSDN, ISDN</td></tr>
</table>

표 1. 전자상거래의 기술적 구조(1998, 한국전산원)

계층분류	관련 기술 및 특징
시장특화된 응용계층	전자 카탈로그(E-Catalog), 전자상점(E-Mail), 전자지불시스템과 같은 단일 시스템과 거래단계별 상행위를 지원하는 사람과 시스템간의 인터페이스 분야로 다른 계층에 비해 기술 진화속도가 빠름
일반적인 응용계층	BBS, E-Form(전자양식), EDI 등과 같이 제반 거래 단계를 지원하는 시스템 컴포넌트에 보편적으로 활용되는 기술로 구성.
미들웨어 계층	정보기술이 분산객체지향으로 발전되면서 효율적인 정보시스템 구축을 위해 활용하는 기술로서 데이터베이스 미들웨어인 RDA(Remote DataBase Access), 분산객체간 통신 미들웨어인 ORB(Object Request Broker) 등
기반서비스 계층	전자메일, FTP 등과 같이 하위계층의 통신 프로토콜을 기능적으로 구현한 응용시스템으로 독립적인 시스템 컴포넌트이면서, 상위계층의 비즈니스 응용 시스템의 중요 기능 요소로 활용
통신서비스 계층	통신 프로토콜로 X.400, SMTP/MINE(Simple Mail Transport Protocol/Multi-purpose Internet Mail Extensions), X.500, LDPA (Lightweight Directory Access Protocol) 등과 같이 응용계층에서 활용하는 메시징 프로토콜.
통신네트워크 계층	ISDN, PSTN, PSDN 등과 같이 트랜스포트 및 하위 통신에 관한 프로토콜로 물리적인 네트워크에 해당
보안/인증	개방형 네트워크인 인터넷상에서 거래의 안전성과 신뢰성을 보장하고 위협으로부터 노출을 방지하기 위한 암호기술, 전자서명, 인증, Firewall 등 여러가지 보안 기술로 6개 계층에 포괄적으로 적용

표 2. 전자상거래 기술체계의 각 계층 분류

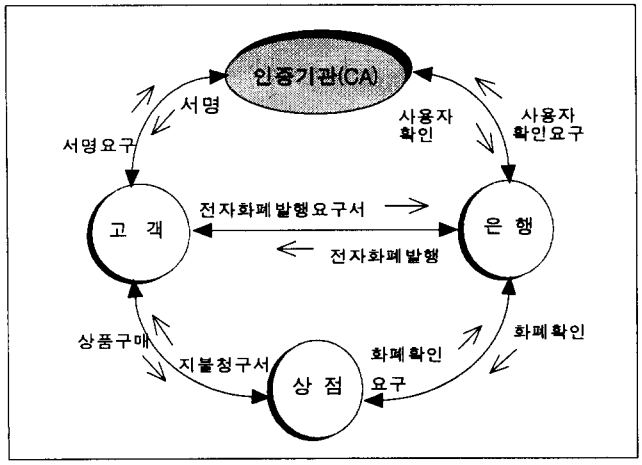

그림 1. 전자상거래시스템의 구성

증 절차를 통해 인증기관으로부터 발급된 전자인증서(Certificate) 또는 여타 인증수단을 토대로 고객과 상점시스템, 지불시스템간에 규정된 암호화 프로토콜 체계를 통해 이루어진다.[3]

첫째, 인증기관은 거래 당사자간을 확인하고 입증해주기 위해 전자인증서를 발행, 개정, 취소하는 기관으로서 거래당사자가 사용하게 될 공개키(암호키 교환용 공개키 및 전자서명용 공개키)를 인증해 준다.

둘째, 고객시스템은 웹 브라우저와 지불을 위한 전자지갑을 장착한 PC로서 지불수단으로는 신용카드, 직불카드, 계좌이체, 전자화폐 등이 이용될 수 있다. 그러나 지금까지는 대부분 신용카드를 기반으로 하고 있다.

셋째, 지불시스템은 상점시스템이 요구하는 대금지불 정보를 처리하는 시스템으로서 지불수단과 처리방식에 따라 지불 브로커, 지불 게이트웨이라고 하기도 한다. 현재는 대부분이 신용카드를 기반으로 한 지불시스템이 개발되어 있으나, 앞으로는 직불카드, 전자화폐 등 다양한 지불시스템이 개발될 것으로 판단된다.

넷째, 상점시스템은 고객들에게 전자적으로 상품(유, 무형)을 판매하는 쇼핑몰(Cyber Shopping Mall)로서 상품정보 DB를 기반으로 실제 쇼핑몰에서 처리하는 상품관리, 매출관리, 고객관리, 매장관리, 상품 수발주 처리, 주문처리, 배송처리, 재고관리 등의 각종 기능을 그대로 수행할 수 있어야 한다.

2.5 전자 지불 방식

네트워크 상에서의 전자상거래가 활발해지면서 전자지불 종류가 다양해지고 있으며, 현재 전 세계적으로 약 30여종이 존재하고 있다. 전자지불시스템들의 방식은 크게 지불브로커형(지불지시형), 전자화폐형(가치저장형)의 2가지로 분류할 수 있다.

첫째, 지불브로커형 전자지불 시스템은 신용카드나 직불카드 기반의 지불 시스템으로, 전자지불서버 자신이 결재를 위한 방법을 제공하지 못하고, 신용카드나 은행계좌이체 등의 지불방식을 인터넷 상에서 안전하게 연결시켜주는 역할을 하는 전자 지불방식이다. 사이버캐시(CyberCash)사가 개발한 전자지불시스템 사이버캐시(CyberCash)와 퍼스트버추얼홀딩스(First Virtual Holdings)사의 퍼스트버추얼(First Virtual)이 대표적이다. 또한 SET(Secure Electronic Transaction) 등과 같은 프로토콜들도 동일한 전자 지불방식을 사용하고 있다.

둘째, 전자화폐형 전자지불 시스템은 신용카드 형태의 카드에 화폐가치를 저장한 다음 필요할 때 꺼내 사용하는 것으로써, 지불 서비스를 제공하는 지불서버가 스스로 결재를 처리할 수 있으며, 화폐의 발행, 유통, 확인, 지불 등의 금융기관의 역할을 지불 서버가 모두 처리하는 전자 지불 방식이다. 즉, 실세계에서 사용되고 있는 화폐 형식을 그대로 모방

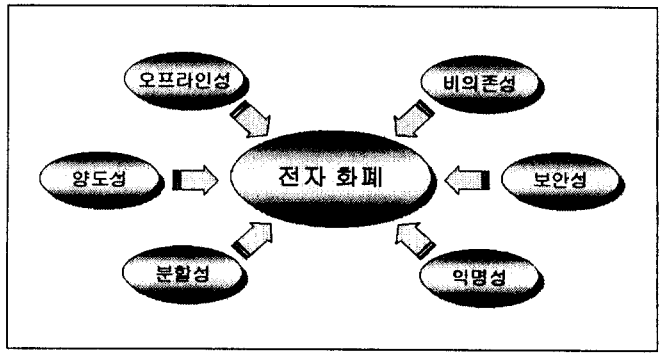

그림 2. 전자화폐의 요구사항

해 실세계의 사용방법과 특성을 같게 만든 방식이라고 할 수 있다. 이러한 화폐의 대표적인 예로써 Mondex사의 Mondex카드, Visa International의 Visa Cash와 같은 IC카드형과 네덜란드의 Digicash사에서 발행하는 Ecash, 캘리포니아 대학에서 개발중인 Netcash 등과 같은 네트워크형이 있다.

전자지불방식을 구현하는 데 있어, 고려해야할 사항으로는 실물 화폐와 동일한 1)소액 지불의 가능성, 2)익명성, 양도성, 추적가능성, 그리고 가상적인 디지털 화폐로써의 3) 보안성 등을 생각할 수 있다.

2.6 인터넷전자상거래의 성장률[4]

전세계 인터넷상거래 시장 성장률은 올해 250%에 다하지만 내년부터는 성장 속도가 둔화될 것으로 보인다. eMarketer(1999/07/22)에 따르면, 인터넷을 매개로 발생하는 상품 매출규모는 1997년 108억 달러에서 1998년에 376억 달러로 증가했고, 금년에는 984억 달러를 기록할 것이라고 밝혔다. 그리고 인터넷상거래 시장이 2000년에 1,972억 달러, 2001년에 3,810억 달러, 2002년에 7,020억 달러, 2003년에는 1조 2,440억 달러로 급증 추세를 지속하겠지만, 전년 대비 성장률에서는 올해에 최고조가 될 것으로 예상했다. eMarketer는 새로운 산업이 생겨날 때 초창기와 같은 높은 성장률이 지속되는 경우가 거의 없을 뿐만 아니라 인터넷 인프라 개발이 진행되는 상태가 앞으로 몇 년 동안 지속될 것이기 때문에 인터넷상거래 시장 성장률이 둔화될 것이라고 설명했다.

한편, 북미주 지역의 온라인 소매시장 규모는 1998년 149억 달러에서 금년에는 360억 달러 이상으로 급증하여 145%의 성장률을 나타낼 것으로 전망하고 있다. Shop.org가 Boston Consulting Group에 의뢰해 실시한 설문 조사 결과에 따르면, 지난해 온라인 소매시장 규모는 북미주 지역 전체 소매시장의 0.5%를 차지하는데 그쳤으나 온라인 인구가 급속히 증가하면서 올해 온라인 매출액은 전체 소매시장의 1.2% 수준으로 높아질 것이라고 한다. Shop.org는 온라인 주문량이 1998년에 200% 증가했고 온라인 쇼핑 인구는 300%나 증가했다고 집계했다.

eMarketer는 새 보고서 "eGlobal Report"에서 전세계 인터넷 사용 인구 중 북미의 비중이 2002년에는 34.8%로 낮아지는 대신, 유럽 사용자의 비중은 29.9%, 아시아 사용자의 비중은 22%로 높아질 것으로 예상했다. 유럽의 경우, 인터넷 보급률이 1998년 말에 6.4%에 그쳤으나 대부분의 서유럽 국가들이 인터넷 인프라 확장에 적극 나서고 있기 때문에 2002년에는 유럽의 인터넷 사용 인구가 8,400만 명에 이르게 될 것이라고 전망했다. 동시에, 아시아의 인터넷 사용자 수는 2002년에 6,100만 명으로 늘어날 것으로 분석했으며 앞으로 아시아의 인터넷 시장은 올해 인터넷 사용 인구가 760만 명에 이르고 있는 일본이 주도해 나갈 것으로 보이나, 중국도 인터넷 시장으로 부상할 것이라고 밝혔다. 한편, 중남미 지역의 인터넷 사용자 수는 2002년에 2,660만 명에 이를 것으로 예상했다.

International Data Corp.(IDC)는 보고서 "The Globalization of eCommerce"에서 세계 전자상거래 시장에서 미국을 제외한 지역이 차지하는 비중이 1998년 26%에서 2003년에는 46%로 크게 높아질 것이라고 전망했다. 이제 서유럽에서는 인터넷이 누구나 사용할 수 있는 일상적 도구로 정착하기 시작했고, 일본을 포함한 아시아-태평양 지역 인터넷 사용자수는 1998년 2,100만 명에서 2003년에는 8,100만 명 이상으로 급증할 것이기 때문이다. 따라서 인터넷을 통해 매출을 올리는 기업들은 여러 언어를 지원하는 전자상거래 사이트를 구축하는 것을 포함한 세계 시장진출 전략을 반드시 마련할 필요가 있다고 강조했다.

Fletcher Research에 따르면, 유럽의 온라인 서비스 시장 규모는 2004년에 180억 달러, 온라인 쇼핑 시장은 180억 달러, 인터넷 광고 시장은 30억 달러에 이를 것으로 예상된다. 특히 유럽 국가들 중에서 독일의 인터넷 인구가 2004년에는 3,000만 명, 영국의 인터넷 사용자 수는 2,500만 명을 기록할 것으로 보인다. 여기에서는 독일, 영국, 프랑스, 이태리 및 스페인이 유럽 인터넷 시장의 75%를 차지하게 될 것이라고 전망하고 있다.

3. 전자상거래 보안

3.1 전자 상거래의 특징

전자 상거래의 보안을 고려하기 위해서는 먼저 전자적 상거래의 환경과 특징을 알아야 할 것 같다. 전자 상거래 특히 인터넷상의 전자적 상거래의 특징은 다음 네 가지로 요약할 수 있다.[5]

첫째, 컴퓨터 네트워크 기반이다. 전자적 상거래는 사람이 직접 만나지 않고 컴퓨터와 네트웍을 통해 거래를 이루는 것이므로 네트워크 상의 컴퓨터시스템에 대한 확인이 필요하게 된다. 네트워크를 이용한 거래이기 때문에 특별히 기밀성(Confidentiality)에 대한 고려가 필요하다. 기밀성을 얻기 위해 암호화 기술을 사용한다.

둘째, 디지털 적이다. 모든 거래에 대한 기록이 디지털 형태이기 때문에 완벽하게 똑같이 복제가 가능하며 위조가 매우 쉽다. 그리고 디지털 자료를 거래에 대한 증거로 사용하기 위해 보조적인 보안요소들이 필요하다.

셋째, 익명성이 존재한다. 현재 컴퓨터 네트워크 특히 인터넷을 사용하는 사람들의 신분을 인증할 수 있는 인프라가 없다. 전자우편주소 혹은 IP어드레스 등은 어떤 사용자의 신분을 믿을만하게 대변할 수 있는 도구가 되지 못한다. 그러므로 안전한 전자상거래를 위해서는 거래 당사자의 신분을 인증할 수 있는 인프라가 필요하게 된다.

넷째, 범세계적 규모이다. 전자 상거래는 일반적인 상거래와는 달리 거래를 일으키는 당사자가 지역적 제약을 받지 않는 특징을 가진다. 즉 지구 반대편에 있는 사람과도 거래를 일으킬 수 있는 특징이다. 이 특징은 전자 상거래의 장점이자 단점이 될 수 있다. 특히 지역적으로 블록화된 세계경제의 구조를 넘어서는 거래이기 때문에 환율, 배달, 지불방식, 거래물품의 품질, 환불, 소비자보호, 문화적 차이 등에 있어서 해결해야 할 과제가 많이 발생한다.

3.2 전자상거래 시스템에서 예상되는 보안침해

전자상거래 관련 시스템에서 예상되는 보안침해로는, 1)전자상거래 관련 시스템의 인프라인 컴퓨터 시스템에 대한 공격, 2) 전자상거래의 기본 데이터가 디지털 형태라는 점과, 전자상거래 시스템이 서로 네트워크로 연결되어 있다는 사항 때문에 발생 가능한 데이터에 대한 공격 3) 전자상거래가 경제적인 활동의 일환이라는 측면 때문에 발생하는 비즈니스적인 공격 등을 들 수 있다.

첫째로, 시스템 공격으로는, 일반적인 컴퓨터 시스템 특히 네트워크에 연결된 컴퓨터는 외부의 특정인이 시스템을 침입하여 부당하게 컴퓨터 시스템을 사용하거나, 정보를 유출하거나, 정보를 파괴할 위험이 있다. 일반적으로 이런 위험을 방지하기 위해 방화벽과 같은 시스템을 사용하기도 한다. 그러나 전자 상거래는 불특정 다수인의 접근을 허용하는 응용시스템으로서 방화벽을 사용하는데 있어서 제약을 받을 수도 있다. 특히 시스템을 불법적으로 사용하는 통계를 보면 외부에서의 침입보다는 내부 사용자의 불법적 사용이 더 많기 때문에 적절한 시스템의 운영지침과 내부 사용자에 대한 보안대책이 중요한 요소가 된다.

둘째, 전자 상거래에 있어서 데이터의 공격은 두

가지로 구분해 볼 수 있다. 하나는 시스템내에 저장된 데이터, 또 하나는 네트워크 상에 흘러 다니는 데이터에 대한 공격이 있을 수 있다. 시스템에 저장된 데이터의 경우는 앞의 시스템 공격에서 언급되었고, 특히 데이터를 시스템에 저장할 때도 암호화를 해서 저장하는 것이 필요하다. 네트워크 상에 흘러 다니는 데이터에 대한 공격을 막기 위해 기밀성(Confidentiality), 자료의 통합성(Integrity) 등에 대한 보증이 필요하게 된다.

셋째, 앞에서 언급한 두 가지 공격은 모두 일반적인 컴퓨터 시스템의 보안침해와 동일하다. 그러나 전자상거래에 있어서는 상거래라는 특징 때문에 발생하는 제 3의 공격이 있을 수 있다. 이것을 통칭해 비지니스공격이라 부른다. 상거래에만 일어날 수 있는 사기가 전자적 상거래에도 일어날 수 있는 가능성이 있다. 이런 요소들을 전자적으로 막기 위한 보안고려사항들이 추가적으로 필요하게 된다. 이 분야에서는 암호학 혹은 시스템으로만 모든 것을 다 막을 수는 없다. 제도적인 장치, 법적인 보장, 보험등의 전자적 시스템외적인 보완이 이루어져야 한다. 이런 취지에서 지난 96년 6월에 UN의 국제상거래법 위원회(UNCITRAL, United Nations Commission on International Trade Law)는 "전자 상거래 모델법(Model Law on Electronic Commerce)"이라는 모델법을 통과시켜 공표했다.

본 고에서는 주로 경제 활동적인 측면, 즉 상거래에 직접관련된 공격에 관심을 둔다.

3.3 보안 기술 개요

이렇듯 전자상거래에 있어서 보안은 매우 중요한 핵심 요소로 완벽한 보안 장치가 없다면 전자상거래 자체가 존재하기는 어렵다. 전자상거래 환경에 적용할 수 있는 보안문제는 크게 4가지로 구분할 수 있는데, 제3자의 도청을 방지하는 기밀성, 정보의 훼손을 방지하는 무결성, 정보 제공자의 정보제공 부인을 방지하는 부인방지, 정보를 보내는 사람의 신원을 확인하는 인증 등이다. 이들 요소들을 모두 충족시키는 시스템이 개발되어야 전자상거래 환경에서의 보안 문제가 해결될 수 있다. 이를 해결하기 위한 보안 기술에 대해서 정리해 본다.

3.3.1 암호화 기술

암호화 기술은 정보보호기술의 기반기술이며 인가된 사람만이 보유하고 있는 정보를 이용하여 보호하고자 하는 자료를 임의로 변형하여 인가되지 않은 자에 대하여 아무런 정보도 노출시키지 않는 기술이다. 암호화 기술을 구현하기 위한 방법으로서 키의 형태에 따라 암/복호화 키가 같은 대칭형 암호화(symmetric cryptography)와 암/복호화 키가 서로 다른 비대칭형 암호화(asymmetric cryptography)로 크게 구분할 수 있다.

대칭적 암호화 방식에서는 암호화에 사용하는 키와 복호화에 사용하는 키가 동일하며, 비대칭적 암호화에서는 이 두가지 키가 다르다.

비대칭적 암호화 방식에서는 보통 이중 한가지 키를 공개하고 한가지 키는 개인이 보관하는 방식을 취하는데, 공개하는 키를 공개키(public key), 개인이 보관하는 키를 개인키(private key)라고 한다.

대칭형 암호화 방식의 대표적인 알고리즘으로는 DES(Data Encryption Standard)가 있으며, 비대칭적 암호화 방식에는 RSA(Rivest, Shamir, Adleman)이 있다. 공개키 암호시스템들은 키분배 문제 해결, 디지털 서명 개념 등의 많은 장점과 함께, 긴 암호화/복호화 시간, 넓은 키 공간(Key space) 등과 같은 구현상의 제한을 가지고 있다. 공개키 암호시스템이 가지는 이러한 단점들은 스마트 카드처럼 작은 계산력과 제한된 양의 메모리를 갖는 디바이스에 적합하지 않으므로, 그 사용 분야에 제약을 받게 하는 원인이 되고 있다.

이러한 공개키 암호시스템의 문제점들은 타원곡선(Elliptic Curve)을 이용한 공개키 암호시스템으로 해결 가능하다. 즉, 타원 곡선 위에서의 이산대수문제는 일반적인 그룹에서 정의되는 이산대수문제보다 더욱 어렵고, 키 공간과 계산량의 문제를 어느 정도 해결할 수 있으므로 스마트 카드 등의 제한된 디바이스에도 적용이 가능하다. 하지만, 타원 곡선에 대한 수학적 연구가 오랜 역사를 가지고 있음에도 불구하고, 암호학적인 접근은 최근들어 적극적인 관심과 연구가 시작되었기 때문에 아직은 더욱 많은 연구가 필요할 것으로 보인다.

DES 암호화 방식과 RSA 암호화 방식에 대한 설명은 다른 문헌을 참조하기로 하고, 여기에서는 타원 곡선 암호화 방식에 대해서 소개하고자 한다.

가) 타원곡선

1985년, Neil Koblitz[12]와 Victor Miller[13]는 타원곡선 상의 점들에 대한 이산 대수 문제에 기반을 둔 타원곡선 암호시스템(Elliptic Curve Cryptosystem, ECC)을 각자 독립적으로 제안하였다. 이러한 타원곡선 암호시스템은 암호화 방식뿐만 아니라 디지털 서명 방식으로도 사용될 수 있다.

(1) 타원곡선 이산대수문제 (The Elliptic Curve Discrete Logarithm Problem, ECDLP)

q가 소수의 멱승 형태일 때, F_q는 q개의 원소를 포함하는 유한체(finite field)를 의미한다. 실제 응용에 있어서 q는 일반적으로 2의 멱승(2^m) 또는 홀수인 소수(p)가 된다. 이 때, 타원곡선 이산대수문제는 다음과 같다 : F_q에 대해 정의된 타원곡선 E, order n의 점 $P \in E(F_q)$와 $Q \in E(F_q)$가 주어졌을 때, $Q = dP$를 만족시키는 정수 $d(0 \le d \le n-1)$이 존재한다면 그 값을 구한다.

타원곡선 이산대수문제는 소인수분해 문제나 이산대수문제보다 상당히 어려운 것으로 알려져 있다. 이들을 이용한 암호시스템에서 동일한 암호학적 강도를 가정했을 때 타원곡선 암호시스템의 경우, 다른 시스템들에 비하여 키의 길이가 매우 짧아지는 장점을 갖는다. 예를 들어, 2048-bit의 RSA나 DSA에 비해 300-bit ECC(Elliptic Curve Cryptosystem)의 경우가 더욱 안전한 것으로 알려져 있다[14].

(2) 타원 곡선의 정의

타원곡선은 일반적으로 임의의 유한체 상에서 정의될 수 있으며, 특히 F_{2^m}의 경우 연산 수행에 있어 더욱 효율적이다. 여기에서는 설명을 단순화하기 위해 Z_p(p는 3보다 큰 소수)상에서의 타원곡선에 대해 설명한다.

Z_p에 대한 타원곡선 E는 다음과 같은 형태로 정의된다.

$$y^2 = x^3 + ax + b \pmod{p}$$

여기서, $a, b \in Z_p$는 $4a^3 + 27b^2 \neq 0$인 상수이며 타원곡선은 무한원점(point at infinity)이라고 하는 원소 O를 포함한다.

타원곡선 E는 적절한 연산을 적용함으로서 abelian 그룹으로 구성할 수 있는데, 일반적인 그룹을 정의하는 것처럼 타원곡선 위의 점에 대해 다음과 같이 덧셈을 정의한다. 단, 모든 연산은 Z_p위에서 정의된다.

1. 모든 점 $P \in E(Z_p)$에 대하여 $P+O = O+P = P$이 성립한다.
2. 만약 $P = (x, y) \in E(Z_p)$이면, $(x, y) + (x, -y) = O$가 된다. (점 $(x, -y)$는 $-P$로 표시하고, P의 negative라고 한

다.)

3. $P=(x_1, y_1)\in E(z_p)$, $Q=(x_2, y_2)\in E(z_p)$라고 할 때, $P+Q=(x_3, y_3)$가 된다.

여기서, $x_3=\lambda^2-x_1-x_2$

$$y_3=\lambda(x_1-x_3)-y_1$$

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & (P\neq Q \text{ 일때})\\ \dfrac{3x_1^2+a}{2y_1} & (P=Q \text{ 일때})\end{cases}$$

위와 같은 덧셈 규칙은 기하학적으로 잘 설명된다[15]. 타원곡선 E상의 서로 다른 두 점 P와 Q의 합 $R=(x_3, y_3)$는 다음과 같이 정의된다. 첫 번째로 P와 Q를 통과하는 선을 그린다; 이 선은 세 번째 점에서 타원곡선과 교차한다. 이 때, R은 이 점의 x축에 대한 투영(reflection)이다(그림 3). 그림에서 타원곡선은 타원(ellipse)과 무한 곡선(infinite curve)의 두 부분으로 구성된다.

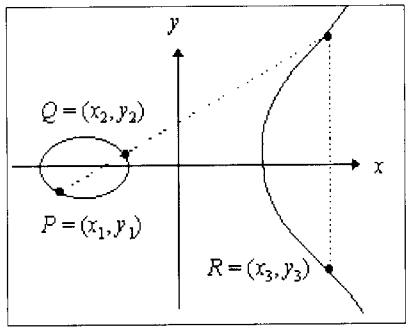

그림 3. 서로 다른 두 점의 덧셈에 대한 기하학적 표시 : P+Q=R

$P=(x_1, y_1)$일 때 P의 doubling, $R=(x_3, y_3)$은 다음과 같이 정의된다. 첫 번째로 타원곡선 상의 점 P에 대한 접선(tangent line)을 그린다. 이 선은 두 번째 점에서 타원곡선과 교차한다. 이 때, R은 이 점의 x축에 대한 투영이다(그림 4).

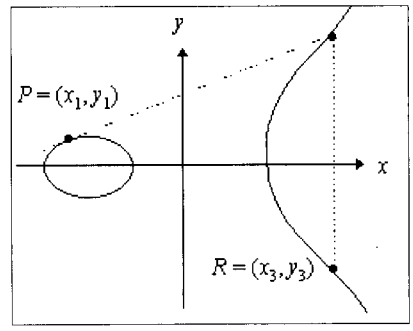

그림 4. 한 점의 doubling에 대한 기하학적 표시 : P+P=R

나) 타원곡선 암호시스템

타원곡선 이산대수문제를 기반으로 하는 타원곡선 암호시스템으로는 암호화 방식인 ECES (Elliptic Curve Encryption Scheme)와 디지털 서명 방식인 ECSS(Elliptic Curve Signature Scheme), ECDSA(Elliptic Curve Digital Signature Algorithm), 그리고 키 설정 프로토콜인 ECKEP(Elliptic Curve Key Establishment Protocol) 등이 있다.

각 프로토콜의 자세한 내용과 타원곡선 암호시스템의 전자화폐 시스템에의 응용에 대해서는 문헌[2]를 참조하기 바란다.

3.3.2 인증기술의 개요

인터넷 전자공간과 같은 사이버 공간의 비대면 특성을 보완하고 상거래 행위의 신뢰성 보장을 위하여 거래 당사자간 신분 확인, 즉 사용자 인증이 필요하다. 또한 전송하고자 하는 메시지를 암호화했다고 해서 메시지의 무결성이 보장되는 것은 아니다. 즉, 전자상거래를 이용한 거래에서는 모든 정보가 전자문서의 흐름에 의해 처리되기 때문에 메시지가 전달되는 과정에 수정되지 않았음을 보장하는 메시지 인증이 필요하다. 그리고 거래사실 부인 및 거래내용 시비 등 제반 분쟁 해결을 위한 디지털 서명이 필요하다. 마지막으로 네트워크 상에서 거래를 하는 각

각의 개체가 실제로 거래를 하여도 안전한 대상인지를 증명하는 것은 쉽지 않다. 이를 정확히 증명해주기 위해 디지털 증명을 이용한다. 디지털 증명서를 이용하면 구매자와 판매자의 신분을 네트워크 상에서 확인할 수 있게 되므로 전자상거래의 신용을 높일 수 있다.

첫째, 사용자 인증은 사용자의 정당성을 식별하는 기술로 키나 카드 등 본인만이 가지고 있는 것을 식별하는 방법, 패스워드나 비밀키 등 본인만이 알고 있는 정보를 이용하여 식별하는 방법 그리고 지문, 음성, 사인, 망막, DNA 정보 등 본인의 신체 특징 정보를 이용하여 식별하는 방법 등으로 크게 나눌 수 있다. 본인만이 가지고 있는 정보나 본인만이 알고 있는 정보는 분실, 도난, 망각 등의 가능성이 있기 때문에 신체 특징 정보를 이용하는 사용자 인증이 이중 가장 안정한 방법으로 알려져 있다. 그러나 이를 직접 구현하여 사용하기에는 많은 양의 데이터베이스 관리 등 실용상의 문제점이 많이 있어 특수한 용도에 한하여 사용되고 있다.

한편, 본인만이 가지고 있는 정보나 본인만이 알고 있는 정보를 이용하여 식별하는 방법은 암호를 이용할 경우 안전하고 실용적인 사용자 인증 방식이 될 수 있다. 널리 알려져 있는 방식들로는 패스워드 이용 방식, 일회용 패스워드 방식(One time password), 시도 응답 방식(Challenge response), 영지식증명을 이용한 방식들이 있다.

둘째, 메시지 인증은, 메시지가 송신 또는 전달 도중에 어떠한 변경이나 위조 없이 수신자에게 전달되었다는 것을 확인하는 절차로 크게 통신문 복원법과 인증자 조회법으로 대별할 수 있다.

통신문 복원법은 수신측에서 복원된 통신문의 의미가 정당한 지를 인증하는 것이다. 메시지 전체의 암호문에 의해서 인증자를 만드는 것으로, 송신자가 통신문 m과 비밀키를 이용하여 암호화하게 된다. 수신자는 서명문을 복호화하여 복호화된 내용이 의미가 있는지의 여부를 인증한다. 만일 의미가 없는 랜덤한 내용이면 원래의 메시지와 다른, 변경이나 위조가 발생하였음을 알 수가 있다. 통신문 복원법은 부속 정보로 일련번호나 시간 정보(time-stamp)를 이용하여 안전성을 높일 수 있으며, 비밀키 암호나 공개키 암호로도 실현될 수 있다.

인증자 조회법은 패리티 검사 부호와 원리적으로 유사하지만 패리티 비트에 해당하는 인증자를 해쉬 함수와 비밀키를 이용하여 발생하는 점이 다르다. 먼저, 송신자가 메시지 m에 비밀키와 일방향 해쉬 함수 h를 이용하여 서명문인 인증자 h(m)을 발행하여 메시지 m과 함께 수신자에게 보낸다. 수신자는 수신된 메시지 m과 자신의 비밀키 그리고 해쉬 함수 h를 이용하여 새로운 인증자 h(m)을 만들어 수신된 송신자의 인증자와 조회하여 본다. 만일 일치하면 송신자의 메시지는 변형없이 정확한 것임을 인증받게 된다.

인증자 조회법의 대표적인 것으로는 DES를 이용하는 MAC(Message Authentication Code)이 있으며 메시지 인증 방식으로 가장 많이 사용되고 있다.

셋째, 디지털 서명은 공개키 암호가 제공할 수 있는 하나의 특징으로, 수신자가 받는 메시지의 변조나 위조를 방지하며, 메시지의 송신자가 추후 부인할 수 없도록 하는 것으로 메시지 인증과 사용자 인증을 동시에 수행하는 것이다. 비밀키 암호를 이용한 메시지 인증에서는 송신자와 수신자 사이의 분쟁 발생시 문제 해결이 곤란하지만, 디지털 서명에서는 제3자의 중재를 통하여 분쟁을 해결할 수 가 있어 전자 상거래 등에 널리 활용될 수 있다.

RSA 공개키 암호를 이용한 디지털 서명 방식을 간략히 소개하면 다음과 같다.

먼저 서명자는 자신의 비밀키 Dk와 메시지 m을 이용하여 서명문 s=Dk(m)을 발생하여 메시지 m과 함께 수신자에게 보낸다. 수신자는 수신한 서명문 s를 서명자의 공개키 Ek를 이여 암호화한 결과와 수신한 메시지를 비교하면 된다. 어느 누구도 서

명자의 비밀키는 알지 못하므로 m에 대한 서명문을 만들 수 없게되며, 서명자가 추후 부인할 수 없는 사유가 되기도 한다. 대표적인 디지털 서명의 표준으로 미국의 DSS가 있다.[7]

4. 전자상거래 보안 기술 동향

4.1 암호화 기술 동향

4.1.1 대칭형 암호화 방식

NIST에서는 1998년을 기점으로 DES의 표준 기한이 만료되므로, 향후 정부와 상업계에서 사용할 수 있는 강한 비밀키 암호화 알고리즘인 미국 차세대 암호 표준(AES : Advanced Encryption Standard)을 개발하기 위해 노력중에 있다. AES로 제안되는 알고리즘은 3-DES보다 더 효율적이어야 하고, 더 안전해야 한다는 설계기준이 제시되었다. 또한 로열티가 없어야 하며, 공개적으로 정의되고 평가될 것을 요구조건으로 하고 있다. NIST는 이미 1998년 8월 20일 전세계 15개 업계 및 단체들이 제안한 암호 알고리즘에 대한 소개를 위한 컨퍼런스 개최를 시작으로 1999년 4월 15일까지 각 암호 알고리즘에 대한 평가 작업을 수행하였다. 특히 우리나라의 보안, 네트워크 전문업체인 ㈜퓨쳐시스템(http://www.future.co.kr/)에서 순수 자체 기술로 개발한 128 bits 블록 암호 알고리즘 'Crypton'이 1차 평가 대상 알고리즘으로 선정이 되어, 일본 NTT에서 제안한 암호 알고리즘 'E2'와 함께아시아 지역의 암호 기술을 인정 받을 수 있는 기회가 되었다.

차세대 암호 표준(AES)을 선정하기 위한 평가기준은 크게 3부분으로 나누어지는데,

첫째, 보안(Security): 평가기준 중 가장 중요한 항목으로 암호 해독에 대한 저항력, 탄탄한 수학적 바탕, 알고리즘 결과에 대한난수성(Randomness), 그리고 다른 후보 알고리즘과의 상대적 보안 평가 등을 종합하여 보안 항목을 평가한다.

둘째, 비용(Cost): 로열티가 없어야 한다는 전제조건에서 출발한 AES이므로, 비용에 대한 평가는 주로 다양한 플랫폼에서의 암호 알고리즘 계산 속도나 능력, 그리고 메모리 요구 수준 등으로 평가한다.

셋째, 알고리즘 및 수행 특성(Algorithm and Implementation Characteristic): 알고리즘의 유연성, 하드웨어/소프트웨어 적합성, 그리고 알고리즘의 단순성 등으로 평가한다.

NIST에서는 이러한 평가 기준으로 15개 후보 알고리즘에 대한 평가 작업을 수행하여, 지난 1999년 8월 9일 AES 최종 후보로 5개 알고리즘(MARS, RC6, RIJNDAEL, SERPENT, TWOFISH)을 선정하였다[4]. 이어 NIST에서는 이들 5개 암호 기술을 앞으로 1, 2개로 더 압축, 오는 2001년 여름까지 표준화 기술로 확립하여 암호 기술을 미국이 주도적으로 이끌 계획이다. 위의 〈표 3〉에는 AES 최종 후보 5개 알고리즘에 대한 설명을 나타내고 있다.

국내에서는 아직까지 국가 표준 비밀키 암호 알고리즘이 없는 상태이지만 한국정보보호센터가 주축이 되어 표준화 작업을 추진하고 있는 상태이다.

4.1.2 비대칭형 암호화 방식

미국 비밀키 암호 알고리즘의 표준인 56 bits DES에 대한 암호해독기술의 발전과 더불어 공개키 암호 알고리즘의 사실 표준인 RSA도 서서히 암호체계가 해독이 되고 있는데, 지난 8월 22일에는 Amsterdam에 근거를 둔 CWI(Centrumvoor Wiskunde en Informatica)의 Herman te Riele가 주도한 6개국의 암호 전문가들에 의해 RSA-155(512 bits RSA 키)가 해독이 되었다. 송신자의 암호문을 수신자가 아닌 타인이 해독하기 위해서는 임의의 개인키를 생성하여 복호화될 때까

알고리즘 명	제안자	제안자 소속국	키 길이 변화에 따른 Key Setup Speed	키 길이 변화에 따른 Encryption Speed	라운드수(Cycle)/설계 (Design Paradigms)	
MARS	IBM	미국	constant	Constant	32(16)	Extended Feistel
RC6	RSA Laboratories	미국	constant	Constant	20(10)	Feistel
RIJNDAEL	Joan Daemen, Vincent Rijmen	벨기에	increasing	128 키:10 rounds 192 키:12 rounds 256 키:16 rounds	10, 12, 16	Square
SERPENT	Ross J. Anderson, Eli Biham, Lars Knudsen	영국 이스라엘 노르웨이	constant	Constant	32	Substitution Permuattion
TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson	미국	increasing	Constant	16	Feistel

표 3. AES최종 후보 5개 알고리즘[9]

지 암호문에 대입하는 작업이 필요한데, RSA-155 코드는 십진 155자리의 수(이는 512 bits에 해당됨)로 해독하기 위해서는 2의 512승에 해당하는 키들을 복호화될 때까지 대입해야 하기 때문에 지금까지는 안전하다고 여겨왔었다. 암호 전문가들은 이번 RSA-155암호 해독을 위해 주로 밤시간과 주말을 이용하여 7개월이 소요되었는데, 만약 대형컴퓨터를 이용한다면 1주일 이내로 암호 해독이 가능할 것으로 지적하고 있다. 현재 컴퓨터 암호체계는 512 bits RSA 보다 더 난해하고 복잡한 것이 개발되어 있기는 하나 미국이 국가안보를 이유로 512bits 이상의 암호체계에 대해서는 수출을 금기하고 있어서, 전자상거래를 위한 인터넷 전자결제의 95% 가량이 기존 RSA-155 암호체계를 이용하고 있다. 위의 표 4에는 각 십진자리 수별로 RSA가 해독된 시점과 사용 알고리즘을 나타내고 있다.

십진자리 수	Bit 크기	암호해독 년도	사용 알고리즘
RSA-100	330	1991.4.	Quadratic Sieve
RSA-110	364	1992.4.	Quadratic Sieve
RSA-120	397	1993.6.	Quadratic Sieve
RSA-129	425	1994.4.	Quadratic Sieve
RSA-130	430	1996.4.	Number field Sieve
RSA-140	463	1999.2.	Number field Sieve
RSA-155	512	1999.8.	Number field Sieve

표 4. RSA가 해독된 시점과 사용 알고리즘[1]

공개키 알고리즘인 512bits RSA에 대한 비보안성에 대한 인식으로, 상업적인 목적의 단기간의 보안을 위해서는 1,024bits RSA를 중/장기 보안을 위해서는 2,048bits RSA 사용을 권장하고 있다. 그러나 RSA 키의 길이가 늘어날수록 Bandwidth의 한계, 연산 능력, 저장 및 전력 소비 등과 같은 컴퓨터 환경의 제약으로 어플리케이션 성능이 현격하게 감소하게 된다. 한편 소인수분해의 난해성에 기반을 둔 RSA에 비해 Certicom (http://www.certicom.com)사의 타원곡선 암호화(ECC: Elliptic Curve Cryptograph)방식은 타원곡선 이산대수문제에 기반을 두고 있으며, 안전도 및 짧은 키 길이로 인해 빠른 계산 속도가 큰 장점으로, RSA를 중심으로한 미국의 독주에 제동을 걸 수 있는 공개키 암호 방식으로 많은 연구와 개발이 이루어지고 있다. 또한 Certicom사는 다양한 플랫폼상에서의 적용을 위한 연구 개발을 통해 타원곡선 암호 알고리즘의 활용 폭이 점점 넓어지고 있다. 위의 표 5에는 대칭형 암호화 방식의 키 길이와 해당 알고리즘의 예, 그리고 이와 동등한 보안성을 제공하는 공개키 암호 알고리즘 RSA와 ECC의 키 길이를

대칭형 암호화(비밀키 암호 알고리즘)		비대칭형 암호화(공개키 암호 알고리즘)	
키 길이	알고리즘 예	ECC 의 키 길이	RSA 의 키 길이
80bits	SKIP JACK	160	1,024
112bits	Triple-DES	224	2,048
128bits	128bits AES	256	3,072
192bits	192bits AES	384	7,680
256bits	256bits AES	512	15,360

표 5. 대칭형 암호화 방식의 키 길이와 해당 알고리즘의 예[1]

나타내고 있다. 기타 자세한 내용은 문헌[1]를 참조하기 바란다.

4.2 지불보안 기술·동향

전자 지불시스템과 관련된 보안 기술의 표준으로는 SET(Secure Electronic Transaction)이 신용카드 기반의 전자지불시스템에 대한 사실표준(de facto standard)으로 수용되고 있다. 1996년 2월 전세계적으로 가장 큰 신용카드 회사인 VISA International과 Master 카드사는 인터넷 상에서 신용카드를 이용하여 대금의 지불을 함에 있어 개인의 정보와 재산을 보호해 줄 수 있는 안전한 방법을 찾기 위해 공동으로 연구를 시작하였고, 97년 5월 SET (Secure Electronic Transaction) 1.0을 발표하였다. SET 프로토콜은 대칭적 암호화 방법인 DES와 비대칭적 암호화 방법인 RSA 및 디지털 봉투를 이용하여 암호화에 걸리는 시간을 줄이고 해독의 가능성을 더욱 낮추었다. SET 지불 정보 및 주문 정보에 대한 보안, 전송되는 데이터에 대한 기밀성 보장, 판매자에 대한 인증 및 각 구성 요소들 간의 상호 운용성을 보장해 주는 거래 프로토콜이다.

SET을 이용한 데이터의 암호화 및 전송방식은 다음과 같다.

1. 구매자는 전송메시지를 자신의 인증서와 함께 이용하여 RSA방식으로 암호화한다.
2. 원문과 1의 결과를 구매자의 인증서와 함께 DES방식으로 암호화한다.
3. 2에서 사용된 DES 키를 판매자의 공개키를 이용 RSA방식으로 암호화한다.
4. 2의 결과(메시지 내용)와 3의 결과(봉투)를 판매자에게 보낸다.

이 메시지를 수신한 판매자는

1. 수신자의 비밀키를 이용 RSA방식으로 봉투를 해독한다.
2. 이때 봉투에는 송신자의 DES 키가 들어있다.
3. 암호화된 메시지를 2의 DES 키를 이용하여 원문 및 송신자의 디지털 서명과 송신자의 인증서를 얻는다.
4. 3에서 얻은 디지털 서명을 송신자의 공개키로 암호화하면 원문을 얻을 수 있다.

이 방법은 DES방법의 간편성과 빠른 처리속도를 이용하여 본문을 암호화한 후, 여기에 사용된 키와 관련 정보를 속도는 느리지만 보안 성능이 보다 뛰어난 RSA 방법으로 암호화하여 마치 봉투처럼 만들어서 연산의 속도와 암호화의 성능등 두 가지 측면에서의 장점을 수용하는 방법이다[5].

전자지불보안 기술의 최근 동향으로써는, IC CARD의 표준으로 개발된 EMV(Europay, Master, Visa)와 SET을 결합한 형태인 C-SET(Chip SET)이 개발 중에 있다. 또한 W3 컨소시엄과 CommerceNet의 JEPI(Joint Electronic Payment Initiative), OBI(Open Buying on the Internet)컨소시엄

의 OBI, OTP(Open Trading Protocol)컨소시엄의 OTP, Checkfee, Microsoft, Intuit이 공동개발한 OFX(Open Financial Exchange) 등 전자지불에 대한 프로토콜을 포함하는 다양한 표준화 활동(Standard Initiative)이 민간부문에서 추진되고 있다[16].

한국에서는, 전자지불과 관련하여 한국은행과 금융결제원은 국내 독자적인 128비트 대칭키 블록 암호알고리즘(SEED)을 채용한 한국형 전자화폐(KEP) 사업에 대해 올 연말에 시범서비스에 들어갈 예정이다. KEP는 접촉식, 비접촉식(RF) 기능을 통합한 콤비카드시스템을 구축할 예정인데, 공개키 암호 알고리즘을 수용할 수 없어 국제 표준규격인 EMV 등과의 호환이 불가능한 문제점을 가지고 있다는 지적도 있다[17].

4.3 인증기술동향

위에서 설명한 SET은 사용자의 인증을 위해 CA(Certificate Authority)를 근간으로 구조를 채용하고 있다. 인증기관은 인증서를 발급하는 기관으로 다양한 분야에 다수가 존재할 수 있고, 서로 다른 인증기관의 인증서를 가지고 있는 쌍방이 거래를 할 수 있으며, 전자서명의 검증을 위해서는 다수의 인증기관 연계 사슬인 인증체계가 필요하다. 일반적으로 인증체계의 유형은 계층 구조와 네트워크 구조가 있는데, 계층 구조는 하나의 최상위 인증기관을 정점으로 하위 인증기관이 계층구조로 연결되는 트리 구조를 가지며, 네트워크 구조는 독립적인 인증기관들이 상호 보증하는 구조이다.

전자 상거래환경에서의 사용자 인증을 위한 키의 분배에는 ITU에서 인증에 대한 표준으로 제정한 X.509프로토콜이 광범위하게 확산되고 있다. 최근 X.509기술을 이용한 상업적인 공개키 인증서비스 등이 다수 등장하고 있으며 인터넷상의 보안응용시스템들이 X.509기술을 수용하는 추세이다. 그러나 X.509는 구조가 최상위(Root)CA로부터 트리구조로 키의 인증이 이루어지는 전세계적인 구조를 지녀야 하며, 자료 형식의 표현을 ASN.1형식을 사용해서 코딩과 디코딩이 복잡하다는 단점을 가지고 있다. 최근 Rivest는 X.509의 단점을 보완한 SDSI(Simple Distributed Security Infrastructure)프로토콜을 제안했다. SDSI는 X.509의 복잡성의 최상위CA가 없이도 구성할 수 있는 새로운 공개키인증 프로토콜이다.

또한 전자서명 등 공개키 암호화 기술의 활용에 대해서는 RSA사에서 제안한 PKCS(Public-Key Cryptography Standards)가 사실표준으로 수용되고 있다.

국내에서는, 7월 1일부터 '전자서명법' 발효를 시작으로 국내 인증시장도 뜨거워질 전망인데, 인증솔루션은 사용자와 상점이 서로 인증하고 또한 믿을 수 있는 제 3자에 의해 상점도 인증하도록 지원하는 상거래의 안정성 향상 기술이다[1,17].

5. 전자상거래 시스템의 사후보안

전자상거래 시스템에 포함되어 있는 인증기관의 인증용으로 사용되는 마스터 비밀키가 어떠한 요인으로 기관 밖으로 유출되어 공개되었다고 가정해 보자. 완벽한 시스템은 없다는 전제하에서, 전자상거래 시스템을 구성하는 프로토콜상의 예기치 못한 오류에 의해서 발생할 수 도 있다. 그래서 안전성에 문제가 없는 키 관리문제를 포함한 알고리즘, 프로토콜을 제안하고, 이를 바탕으로 어떠한 경우에도 안전한 전자상거래 시스템을 구현하려고 많은 연구를 하고 있는 것도 사실이다. 이 많은 연구에서 간과되고 있는 내용 중, 중요한 사항 2가지를 설명하고자 한다. 첫째는, 전자상거래 시스템에 있어서의 인적요소의 역할 또는 영향이다. 한마디로 인간은 정말 윤리적인가 하는 점이다.[18] 최근에 일본에서

발생한 방사선 유출관련 사건을 보면, 아무리 완벽한 관리지침과 공정 매뉴얼을 마련해도, 현장에서 작업하는 인적 요소의 근본적인 안일, 소홀이 돌이킬 수 없는 사태를 만들고 말았다. 핵 분열의 임계상황의 발생을 막기위한 모든 조치는 현장 인적요소의 무시로 이론적으로 완벽하게 안전한 핵 관련 시설은 핵폭탄으로 변하고 말았다. 전자상거래의 활성화에 따라, 전자상거래 시스템가 현 사회의 구성 요소의 하나가 될 것은 자명한 상황에서, 전자성거래 시스템의 일시정지는 사회 활동 특히 경제 활동에 막대한 영향을 초래할 수 있으므로, 인적요소의 오류에도 강한 프로토콜의 개발이 시도되어야 할 것을 본다.

둘째로, 프로토콜의 오류, 인적요소의 오류 등으로 현재 운용되고 있는 전자 상거래 시스템의 비밀정보, 예를 들면 인증기관의 인증용 마스터 비밀키 등이 유출됐다고 했을 때, 전자상거래 시스템을 일시정지 가능한가? 사회에 끼치는 영향을 최소화하기 위해서는 운용하면서, 다시 한번 완전하고 안전한 시스템으로의 이행을 시도해야 할 것이다. 이와 같은 시도를 원활히 수행하기 위해서는 전자상거래 시스템의 구축 초기 단계부터, 아니 암호화 알고리즘 및 프로토콜의 연구, 설계, 구현 단계에서 재복구의 효율성과 안전성을 염두에 두어야 할 것이다. 이와 같은 연구는 지금까지 디지털 회로 설계의 분야로부터 컴퓨터 네트워크 시스템 분야에 이르는 분야까지 많은 분야에서 예를 찾을 수 있다.

지금까지 언급한 내용은 일반적으로 사회정보학(Social Informatics)라는 분야에서 많은 관심을 갖고 있으며, 공학적인 연구 결과가 사회의 하나의 구성원으로써 인간사회의 일부가 될 때에는 좀더 포괄적인 관점에서의 연구가 필요하다고 생각한다.

6. 결 론

본 고에서는 전자상거래의 개념과 요소기술을 체계적으로 분류하고, 전자상거래와 관련된 보안기술, 즉 암호화 기술, 지불 보안 기술, 인증기술에 대해서 기본적인 사항들을 설명하고, 이와 관련된 최근 동향에 대해서 살펴 보았다. 이밖에도 전자상거래가 현실적으로 대부분 웹기반으로 이루어지고 있다는 현실을 고려할 때, 웹, TCP/IP 등의 인터넷 관련 보안기술, 침입탐지, 데이터베이스 등의 시스템 관련 보안기술에 대해서 언급할 필요가 있을 것이다.

전자상거래의 보안과 관련된 요소 기술들은 실용적인 성격과 파급효과 등의 현실적인 필요성에 의해 응용적인 내용들이 부각되는 경향도 없지 않으나, 전자상거래 분야에서 실질적인 주도권을 유지하기 위해서는 암호화 기술 등의 이론적인 연구에 대한 지원의 확대와 활성화가 요구되고 있다. 또한 암호화 기술의 현실 응용의 현실을 생각할 때, 인간적인 요소를 고려한 암호화 프로토콜, 나아가 전자상거래 시스템의 구축을 연구하여야 할 것이다. 그리고 전자상거래 시스템의 막대한 사회적 영향을 중시하여, 운용중인 시스템에 보안 문제가 발생했을 때, 일상생활 등의 사회적 악영향을 최소화 하면서 온전하고 안전한 시스템으로 복귀가 가능한 체제에 대한 연구가 사회 정보학(Social informatics)적인 입장에서 진행되어야 할 것이다.

※ 참 고 문 헌

[1] 홍승표, 강회일, 이동일, "전자상거래 정보보호(보안/인증) 기술동향", 주간 기술 동향 제 916호, 한국전자통신연구원, 1999.10.

[2] 전병욱, 권용진, "Blinding ECDSA를 기반으로 한 분할가능 전자화폐 시스템", 한국 통신정보보호학회 논문지, 제9권 1호, pp. 103-114, 1999.

[3] 김춘길, "전자상거래의 개념과 발전방향", 한국정보과학회 학술지, 제16권 제5호, 1998년.

[4] 이경전, "해외 인터넷 상거래 동향과 전망", 통신시장 통권 제26호, 한국통신 경영연구소, 1999년.
[5] 김기병, 지정권, 김형주, "전자상거래를 위한 지불방법 및 보안", 한국정보과학회 학술지, 제16권 제5호, 1998년.
[6] 정철종, 권용진, "추적성을 부여한 전자지불시스템의 구현", 한국통신학회 99년 하계 종합 학술 발표회 논문지, pp.994-997, 1999년.
[7] 이임영, 박춘식, "암호기법", 한국정보과학회 학술지, 제15권 제4호, 1997년.
[8] 임신영, 권도균, "전자상거래 보안", 한국정보과학회 학술지, 제15권 제4호, 1997년.
[9] http://www.counterpane.com/aes-performance.pdf.
[10] 한국전산원, "정부 EC 플랫폼 발전방안에 관한 연구", 연구결과보고서, 1998.6.
[11] 한국전산원, "CALS/EC 표준화 로드맵 연구", 연구결과보고서, 1998.6.
[12] N. Koblitz, "Elliptic curve crypto-systems", Mathematics of Computation, number 48, pp.203-209, 1987.
[13] V. S. Miller, "Use of elliptic curves in cryptography", Advances in Cryptology-Proceedings of CRYPTO '85, Springer Verlag Lecture Notes in Computer Science 218, pp.417-426, 1986.
[14] A Certicom Whitepaper, "Remarks on the security of the elliptic curve crypto-system", September, 1997
[15] D. B. Johnsom, A. J. Menezes, "Elliptic Curve DSA(ECDSA): An Enhanced DSA", A Certicom Whitepaper, 1997.
[16] 김범태, 김은, "전자상거래 표준화 동향 및 이슈", 정보처리학회지 제6권, 1999.1.
[17] 전자신문, 해당 기사들.
[18] J. Kreie, T. P. Cronan, "How Men and Women View Ethics", Communications of the ACM, Vol. 41, No. 9, Sept. 1998.

권 용 진

1986년 한국항공대학교 항공전자공학과 (공학사)
1986년~1988년 일본 京都대학 공학연구과 정보공학전공 연구생
1988년~1990년 일본 京都대학 정보공학과 석사과정 졸업
1990년~1994년 일본 京都대학 정보공학과 박사과정 졸업
정보공학전공 공학박사 취득
1994년~현재 한국항공대학교 통신정보공학과 조교수
※연구분야 : 스위칭이론, 논리회로 합성 및 설계, 부호이론, 암호이론, 정보보안.

김 정 선

1965년 한국항공대학교 항공전자공학과(공학사)
1972년 한양대학교 전자공학과(공학석사)
1983년 경희대학교 전자공학과(공학박사)
1984년~현재 한국항공대학교 항공전자공학과 교수
※연구분야 : 컴퓨터 구조, 네트워크 보안 등