□ 기술해설 □

전자 상거래 보안

시스템공학연구소 임신영
데이콤 권도균

1. 전자 상거래의 정의

전자 상거래 혹은 전자적 상거래는 전자, 정보기술의 발달의 힘을 입은 전자적인 커뮤니케이션의 연장선상에서 상거래적인 커뮤니케이션을 이루는 것을 말한다. 상거래적인 커뮤니케이션은 단순한 커뮤니케이션이 아니라 경제적인 의미를 강하게 포함한 커뮤니케이션이다. 경제적인 의미란 법적인 의미 역시 강하게 포함한다.

오늘날 전자적 상거래가 주목을 받는 주된 이유는 두 가지로 들 수 있다. 하나는 기술적인 측면에서의 진보와 또 하나는 경제적인 측면에서이다.

기술적인 측면에서 전자적 상거래가 활성화되는 요인으로는 컴퓨터와 네트웍기술 그리고 멀티미디어 기술의 발달로 전자적 커뮤니케이션이 실생활의 여러 활동들을 모방할 수 있는 가능성을 열었기 때문이다. 경제적인 측면에서는 전자적 상거래가 비용이 절감되며 효율적이며 새로운 시장의 가능성을 보여주기 때문이다.

특히 인터넷은 전세계적인 연결을 보장하고 수천만이상의 사용자들이 있다는 점에서 전자적 상거래의 주요 장으로 인식되고 있다. 전자적 상거래의 기반환경으로 중요한 요소는 바로 보안(Security)의 문제이다.

본 고에서는 전자적 상거래가 가능하기 위한 안전요소 즉 전자적 상거래의 보안(Security)에 대해 논의하고자 한다. 이를 위해서는 먼저 전자적 상거래의 특징과 거기에 따른 위험요소를 도출해 내어 이를 방지하는 요소를 제안해 보고자 한다. 그리고 전자적 상거래에 있어서 가장 중요한 요소인 전자적인 지불에 대해 이야기와 국내외 프로토콜 및 개발사례 등을 중심으로 살펴보고자 한다.

2. 전자 상거래의 특징

전자적 상거래의 보안을 고려하기위해서는 먼저 전자적 상거래의 환경과 특징을 알아야 할 것 같다. 전자 상거래 특히 인터넷상의 전자적 상거래의 특징은 다음 네 가지로 요약할 수 있다.

2.1 컴퓨터 네트웍

전자적 상거래는 사람이 직접 만나지 않고 컴퓨터와 네트웍을 통해 거래를 이루는 것이므로 네트웍상의 컴퓨터시스템에 대한 확인이 필요하게 된다. 네트웍을 이용한 거래이기 때문에 특별히 기밀성(Confidentiality)에 대한 고려가 필요하다. 기밀성을 얻기위해 암호화 기술을 사용한다[1].

2.2 디지탈

모든 거래에 대한 기록이 디지탈 형태이기 때문에 완벽하게 똑같이 복제가 가능하며 위조가 매우 쉽다. 그리고 디지탈 자료를 거래에 대한 증거로서 사용하기 위해 보조적인 보안요소들이 필요하다.

2.3 익명성

현재 컴퓨터 네트웍 특히 인터넷을 사용하는 사람들의 신분을 인증할 수 있는 인프라가 없

다. 전자우편주소 혹은 IP어드레스 등은 어떤 사용자의 신분을 믿을만하게 대변할 수 있는 도구가 되지 못한다. 그러므로 안전한 전자 상거래를 위해서는 거래 당사자의 신분을 인증할 수 있는 인프라가 필요하게 된다.비자와 마스터 카드사가 공동으로 만든 인터넷전자지불 프로토콜인 SET(Secure Electronic Transaction)의 근본 구조가 CA(Certificate Authority)를 근간으로 한 점도 바로 이런 이유 때문이다[2]. 전자 상거래환경에서의 사용자인증을 위한 키의 분배에는 X.509프로토콜이 광범위하게 확산되고 있다[3].

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[4].

SDSI는 X.509의 복잡성과 최상위CA가 없이도 구성할 수 있는 새로운 공개키인증 프로토콜이다.

2.4 범세계적

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. 전자 상거래에서 예상되는 보안 침해

3.1 시스템 공격

일반적인 컴퓨터 시스템 특히 네트웍에 연결된 컴퓨터는 외부의 특정인이 이 시스템을 침입하여 부당하게 컴퓨터시스템을 사용하거나, 정보를 유출하거나, 정보를 파괴할 위험이 있다. 일반적으로 이런 위험을 방지하기위해 방화벽과 같은 시스템을 사용하기도 한다. 그러나 전자 상거래는 불특정 다수인의 접근을 허용하는 응용시스템으로서 방화벽을 사용하는데 있어서 제약을 받을수도 있다. 특히 시스템을 불법적으로 사용하는 통계를 보면 외부에서의 침입보다는 내부사용자의 불법적 사용이 더 많기 때문에 적절한 시스템의 운영지침과 내부사용자에 대한 보안대책이 중요한 요소가 된다.

3.2 데이타 공격

전자 상거래에 있어서 데이타의 공격은 두가지로 구분해 볼수 있다. 하나는 시스템내에 저장된 데이타, 또 하나는 네트웍상에 흘러 다니는 데이타에 대한 공격이 있을 수 있다. 시스템에 저장된 데이타의 경우는 앞의 시스템 공격에서 언급되었고, 특히 데이타를 시스템에 저장할 때도 암호화를 해서 저장하는 것이 필요하다. 네트웍상에 흘러 다니는 데이타에 대한 공격을 막기위해 기밀성(Confidentialty), 자료의 통합성(Integrity) 등에 대한 보증이 필요하게 된다.

3.3 Business 공격

앞에서 언급한 두 가지 공격은 모두 일반적인 컴퓨터 시스템의 보안침해와 동일하다. 그러나 전자 상거래에 있어서는 상거래라는 특징 때문에 발생하는 제 3의 공격이 있을 수 있다. 이것을 통칭해 비즈니스공격이라 부른다. 상거래에만 일어날 수 있는 사기가 전자적 상거래에도 일어날 가능성이 있다. 이런 요소들을 전자적으로 막기위한 보안·고려사항들이 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[5].

4. 전자 상거래에서의 지불 환경

전자 상거래 시스템은 일반적인 컴퓨터시스템과 동일한 보안위협에 처하게 된다. 그러나 전자 상거래에 있어서 가장 중요한 보안요소는 바로 전자적인 지불과 관련된 보안요소들이다. 상거래에 있어서 가장 중요한 행위는 바로 대금(돈)을 지불하는 과정이다. 전자 상거래를 구성하기 위해서는 바로 이런 안전한 전자적 지불이 가능하도록 하는 전자지불인프라구조를 가지는 것이 필요로 한다. 오늘날 인터넷상의 전자 상거래서비스를 제공하는 시스템들의 지불환경을 살펴보면 첫째 WWW폼 입력기반 시스템(WWW Form-CGI system)이 있다. 이는 WWW의 HTML문법가운데 폼(form)문법을 이용해 사용자의 신용카드번호, 배달주소 등의 정보를 입력받아 서버측에 전달받아 CGI로 처리하는 방식이 있다. 두번째는 가입자 기반 시스템(Subscribe Base system)이 있다. 이는 미리 해당 서버에 사용자가 등록을 하고 등록시 사용자의 지불정보 등을 등록해 둔후 지불시에는 자신의 ID와 패스워드를 이용해 지불하는 방식이 있다. 세번째는 인터넷상의 전자지불 시스템을 이용해 지불을 처리하는 방식이 있다.

위의 첫번째와 두번째 방식은 해당 정보(지불정보, 사용자ID, 패스워드)가 네트워상에서 전달될 때 안전을 보장받지 못한다. 물론 SSL(Secure Socket Layer) 보안 프로토콜을 이용해 채널보안을 얻을수 있다. 그러나 사용자들의 거래에 대한 부인봉쇄, 상거래서버의 사기 등에 대한 안전장치가 없다.

5. 전자지불 모델

전자지불시스템들의 모델은 크게 세 가지로 구분해 볼수 있다. 첫번째는 지불브로커형 전자지불시스템으로서 전자지불서버 자신이 결재을 위한 방법을 제공하지 못한다. 다만 신용카드 혹은 은행계좌이체 등의 지불방식을 인터넷상에서 안전하게 연결시켜주는 역할을 하는 전자지불모델이다. 현재 많이 알려져 있는 CyberCash전자지불시스템[6]이나 SET(Secure Electronic Transaction)[2] 등과 같은 프로토콜들은 지불브로커형 전자지불시스템이다. 두번째 모델은 전자화폐 모델이다. 전자화폐모델은 지불서비스를 제공하는 지불서버가 스스로 결재를 처리할 수 있는 역할을 할 수 있으며 지불형태역시 화폐의 발행, 유통, 확인, 지불 등 금융기관이 하는 모든 기능을 지불서버가 처리한다. 전자화폐형 전자지불시스템은 법제도적인 준비, 통화정책, 화폐의 익명성 등에 대한 보완이 필요하다. 전자화폐형 전자지불시스템으로는 네덜란드의 DigiCash전자지불시스템 등이 이 모델에 속한다. 세번째 모델은 소액전자지불시스템모델이다. 소액전자지불모델은 전자화폐모델의 일종으로서 주로 한번의 지불트렌젝션에 이루어지는 지불의 규모가 1달라 이하의 소액을 전문적으로 처리하는 전자지불시스템모델이다. 일상적인 상거래에 있어서 소액지불의 규모가 매우 크다는 점과 인터넷 전자상거래분야가운데 전자출판, DB서비스, 온라인게임 등 거래당 소액의 비용을 지불하는 서비스의 잠재력이 크다는 점에서 소액전자지불시스템 모델이 관심을 모으고 있다. 소액전자지불시스템모델에서 주로 고려할 점은 보안보다는 효율성과 비용의 절감이다. 특히 일반적인 전자지불시스템에서는 공개키 암호화방식을 이용하는데 공개키 암호화방식은 매우 비싼 컴퓨팅자원을 필요로하기 때문에 주로 단방향해쉬함수를 이용한 소액전자화폐, 소액전자지불 프로토콜들이 제안되고 있다.

6. 전자 거래 보안 프로토콜

인터넷 기반 전자 상거래 보안 기술을 전자 상거래와 관련된 직접 기술과 이러한 전자 상거래 보안 기술을 구성하는 주요 보안 기반 기술을 간접 기술로 분류할 경우, 추후 구현할 플랫폼(예 : 전자 현금, 지불 브로커 등)과 무관하게 공통적으로 적용해야 할 기술에 대한 분류를 하면 다음과 같다.

직접 기술 : 전자 상거래 전용 프로토콜, 구매자/판매자 인증, 전자 거래 내용 공증, 은닉 전자 서명(Blind Digital Signature) 알고리즘, 전자 화폐 이중 사용 방지 알고리즘

간접 기술 : 공개키 기반 암호화 알고리즘, 국제 표준 암호화 알고리즘

전자 상거래 특히, 대중적으로 가장 많이 사용하는 인터넷을 기반으로 하는 전자 상거래 서비스가 실현 가능성이 가장 높아짐에 따라 이 부분에 대한 선진국의 움직임으로 대표되는 IETF(Internet Engineering Task Force)의 관련 메일링 리스트를 통하여 업체(80% 이상), 연구소(10%) 및 학교(10%)의 전문가들이 기술적 사양의 표준화 및 상용화를 목적으로 의견을 나누고 있다.

IETF의 보안 분야(Security Area)의 일부 작업반(Working Group)에서는 인터넷 전자 상거래 보안 기술 사양과 적용에 대한 작업이 진행 중이며 현재 주로 거론되고 있는 기술 분야들을 작업반별로 분류하면 다음과 같다[7].

Authenticated Firewall Traversal(AFT) Working Group :
- SOCKS Protocol Version 5(RFC1928)
- Username/Password Authentication for SOCKS V5(RFC1929) (참조 : http : //www.socks.nec.com/ftp/socks5)

Common Authentication Technology(CAT) Working Group :
- GSSv2 C-Binding
- Extended Generic Security Service-Application Program Interface(XGSS-API)
- Public Key Utilizing Tickets for Application Servers(PKTAPP)

IP Security Protocol(IPSEC) Working Group :
- SEPP(Secure Electronic Payment Protocol)
- SET(Secure Electronic Transaction) [2]

Public-Key Infrastructure(X.509)(PKIX) Working Group :
- Internet PKI(IPK) (참조 : http : //ietf.org/internetdrafts)

Web Transaction Security(WTS) Working Group :
- S-HTTP
- Secure Socket Layer(SSL)

7. 국내 사례

7.1 국내 전자 상거래 관련 활동

국내의 전자 상거래 보안 기술에 대한 가시적인 움직임은 1995년 후반기부터 본격적으로 나타나기 시작하였으며 다음과 같은 연구회 및 모임을 가동하여 금융계, 관계 및 기술계의 융합된 모임을 추진하고 있다.

1996년 4월에 전국 은행 관계자 모임에서 전자 지갑 표준화 실무 작업반을 구성하여 전자 상거래에 필요한 전자 지갑의 표준 규격에 대한 실무를 진행하는 작업반을 구성하여, 금융결재원을 중심으로 IC카드구조에 대한 표준화 작업을 96년 말에 완료하였다. 또한 1996년 11월에는 한국 정보 통신 진흥 협회에서 전자 화폐 연구회를 결성하여 전자 화폐에 대한 전반적인 기술 사항을 다루는 연구회를 가동하였으며 여기서는 3개 분과 위원회를 가동하여 제도/법, 기술 및 서비스에 대한 연구를 진행하고 있다. 이 중 기술 부분에서 전자 상거래 보안 기술을 다루고 있다. 96년 11월에 국제전자 상거래연구센타(ICEC)라는 협회와 관련 기술을 개발하는 기술전담회사가 KAIST를 중심으로 발족되어 전자 상거래와 관련된 연구활동을 추진하고 있다. 역시 1996년 말에 데이콤의 주도로 미국의 커머스넷 컨소시움의 한국판인 한국 커머스넷 컨소시움이 구성되어 연구활동을 시작하였다. 이외에도 개방형컴퓨터연구회(OSIA) 산하 인터넷 KIG 내에 Security 워킹그룹내에도 전자 상거래를 연구하는 활동이 있으며, 웹 코리아(WWW-KR)의 WSP(Web Security & Payment) 워킹그룹내에도 전자지불, 전자 상거래를 연구하는 활동이 있다. 이가운데 WSP 워킹그룹은 96년 4월 국내 17개 기업들로 한국 전자 상거래협의회(KIECA)[8]를 구성 전자 상거래관련 활동을 하고 있다.

은행계의 움직임으로 작년에 동남 은행에서 하나로 전자 지갑 카드를 시험 운용하였으며, 관련 전문 업체인 동성 정보 통신에서는 1996년 11월에 웹 서버와 IC 카드 인터페이스 기술

을 보유하고 있다고 발표된 바 있다.

국내에서는 1996년 10월에 SoftCash전자지불시스템이 데이콤연구소에서 개발되었다. SoftCash전자지불시스템은 지불브로커형 전자지불시스템으로서 대금결재방식으로 신용카드를 통한 결재와 은행 계좌이체를 통한 대금 결재가 가능하도록 인터넷 WWW기반의 전자지불을 구현한 시스템이다[9].

7.2 SoftCash전자지불시스템

7.2.1 시스템 구성

SoftCash전자지불시스템은 앞에서 이야기했듯이 지불브로커시스템의 구조를 가진다. 지불브로커시스템의 구성요소는 사용자 전자지갑(Wallet), 전자 상거래 지불서버, 지불 브로커 서버, 뱅킹 서버 네 가지로 구성된다.

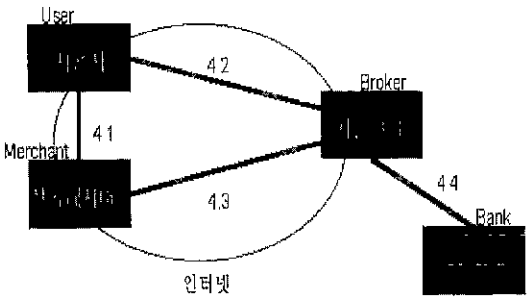

그림 1 SoftCash전자지불 프로토콜 구조

7.2.2 SoftCash전자지불 프로토콜

SoftCash전자지불 프로토콜은 초기화(사용자의 등록), 지불요구, 지불, 지불확인요청, 지불정보확인 요청, 지불정보확인, 영수증발행 등으로 구성된다.

초기화시에는 사용자에 대한 기본정보와 사용자가 생성한 RSA공개키를 지불서버에 등록한다. 사용자가 쇼핑과정 중에 물건을 주문하면 상거래서버는 지불요구서메시지를 만들어 지불을 요구하며, 사용자의 전자지갑은 상거래서버의 지불요구서를 해석해 상거래서버가 받을수 있는 지불방식(은행계좌, 신용카드)을 이용해 지불을 하며 상거래서버는 사용자가 제시한 지불메시지속에 중요한 정보는 해독할 수 없는 상태로 지불서버에게 지불확인요청을 하게 된다. 상거래서버는 사용자의 지불메시지를 해독해 지불정보를 얻어 뱅킹서버에게 지불허가요청을 한다. 뱅킹서버와 지불서버는 인터넷을 통해 통신을 하는 것이 아니라 안전한 별도의 네트웍을 확보하고 있다고 전제한다. 뱅킹서버는 지불서버가 보내온 지불정보를 확인하고(실제는 지불처리를 한 후에) 지불정보확인 메시지를 지불서버에게 보낸다. 지불서버는 상거래서버에게 지불이 되었음을 지불확인 메시지로 알려주고 상거래서버는 사용자에게 지불받았음을 증명하는 영수증을 전달하면 하나의 거래와 지불이 완료된 것이다.

프로토콜	사용자	상거래서버	지불서버	뱅킹서버
초기화	→			
지불요구	←			
지불	→			
지불확인요청		→		
지불정보확인요청			→	
지불정보확인			←	
지불확인		←		
영수증발행	←			

그림 2 SoftCash전자지불 프로토콜 트랜잭션흐름도

SoftCash전자지불 프로토콜에서 사용되는 각종 메시지는 RFC822의 이름 : 값 쌍형식의 메시지 형식을 따른다. 다음은 SoftCash전자지불메시지의 예이다.

7.2.3 SoftCash보안

자료의 기밀성보장을 위해 SoftCash전자지불시스템에 사용되는 모든 자료 즉 네트웍상에 전송되는 자료나 컴퓨터시스템에 저장되는 모든 자료가 암호화되어 저장한다. 자료의 암호화는 DES와 Triple-DES, 128bit Blowfish 등의 대칭형 암호화기법을 사용하며 세션키는 매 트랜잭션마다 랜덤함수를 통해 생성되며 세션키는 1024bit RSA암호화기법을 이용해 암호화한다.

자료의 통합성은 MD5, SHA 두 가지 단방향 해쉬함수를 이용해 보장받는다. 거래 부인 방지(Non-Repudiation)를 위해 SoftCash지불 프로토콜은 RSA-MD5, RSA-SHA전자서명기술을 이용해 모든 트랜잭션때 생성되는 모든 메시지를 서명하여 거래부인방지를 한다. 사용자의 RSA키는 사용자가 자신을 지불서버에 등록할 때 전자지갑이 1024bit RSA키쌍을 생

성해 공개키를 함께 등록한다.

8. 해외 사례

전자 상거래가 시도된 사례로는 1995. 7~1996. 7까지 영국의 Mondex에서 미래 전자 결재 표준형을 제시한바 있으며, 이 은행은 1996년 7월에는 호주 4개 은행 및 뉴질랜드 6개 은행 그리고 미국과 캐나다에 영업권을 판매하여 현재 전세계 15개국에 전자 결재 표준 사양을 판매하였으며 아시아 권에서는 일본 흥업 은행과 홍콩 및 싱가포르의 은행에서 이를 구매하였다.

특히, 주목할 점은 1995년 12월부터 1997년 초반까지 VISA 및 Master Card사가 공동으로 사양을 설정한 SET(Secure Electronic Transaction)에 의하여 카드 한 장으로 현금, 신용카드, 개인 정보가 포함되는 다기능 전자 화폐 기술 사양을 제시하였다. 그리고 1996년 7월18부터 2주간 애틀란타 올림픽에서 VisaCash를 시험적으로 운영하였으며 이를 바탕으로 이 기술 사양에 대한 세계 표준화를 추진하고 있다. 여기에는 전용 단말기 및 주변기기에 대한 표준화 제정과 동시에 엄청난 수요가 예상되며 이러한 형태의 거래 매출액 규모는 연간 8조 달러로 예상하고 있으며, 이중 약 20% 정도는 10달러 미만의 소액 거래를 하는 사용자가 사용할 것으로 예측하고 있다.

미국의 경우, Forrester Research Inc.에서 조사한 1995년도 미국의 전자 상거래 사용 현황은 총 규모가 약 5억 1천 8백만 달러로 세부 사항은 다음과 같다.

- 전산 관련 구매 : 140(27%)
- 여행 서비스 : 126(24%)
- 오락 : 85(17%)
- 의류 : 46(9%)
- 선물, 꽃 : 45(9%)
- 음식 및 음료 : 39(7%)
- 기타 : 37(7%)
- 총 518(백만달러)(100%)

1995년 동안 거래한 규모는 2,700만 명이 사용하였으며, 이는 일인당 평균 약 190달러의 상품을 구매한 것으로 분석된다. 또한 거래 형태로는 내부 기관간, 업체간, 업체-소비자간 그리고 소비자간의 네 가지 유형의 정형화된 거래 형태를 보이고 있다.

위의 대표적인 사례 외에 다음의 사례는 지난 수년간 관련 업체가 개발하여 제시한 전자 상거래 시범 사업에 대한 사례이다.

- Astoria : (94, 미국) S/W, 음악, 출판물, 정보 서비스의 직배 구매 서비스 시스템(POS를 기반으로 함)에 대한 상용화를 시도하였다.
- CommerceNet : (93, 미국) Internet-Web Server 근간, Business-to-Business 트랜잭션을 위한 전자 시장 시스템을 주력하며 Pilot program으로는 트랜잭션 보안, 지불 서비스, 전자 catalogs, Internet EDI, EDI Data Transfer 등이 있다.
- CyberCash : (94, 미국) 95.4이후 Internet을 통한 secure credit card 트랜잭션 서비스 제공, 일일 수 천건 트랜잭션 처리 시스템, 40만개의 CyberCash Wallets이 배포되어 사용 중이며, 미국 은행의 80%가 연동되어 사용 중이다.
- DigiCash Ecash : (89, 미국) 미국 내 선도적인 security/privacy를 보장하는 electronic payment mechanism을 제공한 network system 개발(Dr. David Chaum 공개키 암호화 기술 근간의 보안 서비스), 최근 MC가 DigiCash 기술 도입, SmartCard chip mask 기술에 사용하고 있다.
- Globe Online : (95, 미국·프랑스) Merchants & Consumers를 위한 Globe Online Merchant Web Servers(MD5, RSA 기술)를 통하여 secure payment interface 제공한다.
- IBM Electronic Commerce : (미국) Web 서버 근간의 서비스 환경에서 iKP(secure payment protocols with RSA) 기술을 제공한다. Financial(기존 은행 회계망)/commercial(iKP) network으로 이원화하여 구축하고 있다.
- MasterCard와 Netscape : (95, 미국) 95. 1 안전한 credit & debit card TX를 Inte-

rnet에서 제공하기로 발표, Internet의 대중성에 부응하여 POI(Point-of-Interaction) 구매 형태 지원 시스템을 개발하였다.(*MC/Cirrus는 ATM 망을 사용, 1996년 65개국에 19만대의 ATM 교환기로 65개국 36억개의 credit & debit card를 처리, 93년 1년간 1억2천만 가맹점에서 총 3,200억 달러의 매상이 36억 TX를 통하여 처리)

- Mondex : (영국) Smart-card 방식의 전자 거래 서비스 시스템을 제공한다.
- Open market : 실시간 사용자 인증(발신자 인증, 온라인 검증, 재무 관리 등), 신용 카드 조회 및 거래 확인, 분쟁 해결을 위한 온라인 통신 기능을 제공한다.

전자 상거래의 유형이 현재 여러 가지 제시되고 있으나 가장 실현 가능성이 높은 안으로는 신용 카드 기반의 전자 상거래를 예측할 수 있다. 그 원인은 새로운 형태의 카드 문화가 사용자에게 정착되기까지는 오랜 시간이 걸리는 문제와 각국의 제도권에서 새로운 기능에 대한 제도 정비가 각기 입장을 달리하기 때문인 것으로 분석된다.

주목할 부분은 미국을 중심으로 하는 다국적 기업인 Visa 및 MasterCard사가 공동으로 제안한 SET(Secure Electronic Transaction)이 관련 업체에서 긍정적인 평가를 받으면서 지속적인 버전 관리를 하여 1997년 2월 현재 1996년 11월에 최종적으로 발표된 사양을 관련 업체 및 전문가 집단에서 검토 중에 있다.

9. 결 론

지금까지 전자 상거래와 전자 상거래에 필요한 기반 보안기술에 대해 이야기하였고 특별히 전자지불프로토콜에 대해 이야기 하였다. 컴퓨터와 컴퓨터네트웍의 활용은 이제 정보의 전달뿐 아니라 상거래의 영역에까지 확대되어 국가와 사회에 어떤 영향력을 미칠지 예측하기가 힘들게 빠른 속도로 변화하고 있다. 이 현상에 대해 마치 산업혁명과 같다는 표현을 빌리는 사람들도 있을 정도이다. 앞으로 전자 상거래가 경제, 사회, 국제적 교역에 미칠 영향은 다른 분야에서 특별히 연구해야 할 주제라 본다. 그러나 전자 상거래에서 가장 중요한 보안의 요소는 향후 전자 상거래기술의 주도권을 확보할수 있다는 가능성 때문에 세계각국에서 매우 활발하게 연구하고 실용화하고 있는 주제들이다. 특히 보안기술은 국가적인 활용과 국제적인 활용으로 구분해 볼수 있고, 국제적인 활용을 위해서는 국제적인 표준활동과 보조를 맞추어야할 필요성이 있다. 그리고 전자 상거래분야는 일반적인 분야와는 달리 학문적인 가치뿐 아니라 산업계에서의 파급효과가 크므로 산업계와 학계가 밀접하게 연계해 발전시켜야 할 분야이다. 전자 상거래기술과 관련 보안기술의 확보는 다음 세기의 국가경쟁력의 기반기술이 될 것이다.

참고문헌

[1] Taher Elgamal, CREDIT CARD PAYMENT APPLICATIONS OVER THE INTERNET, http : //home.netscape.com/newsref/std/credit.html, July 14. 1995.

[2] VISA, Master Card, SET(Secure Elecronic Transaction) http : //www.visa.com, http : //www.mc.com/.

[3] ITU-T, X.509 The Directory : Authentication Framework, 1993.

[4] Ronald L. Rivest, SDSI(A Simple Distributed Security Infrastructure), http : / / theory.lcs.mit.edu / ~ rivest / sdsi10.html, Sep. 15 1996.

[5] UN. UNCITRAL Model Law on Elecronic Commerce(Report of the United Nations Commission on Internation Trade Law on the work of its twenty-ninth session), 28 May-14 June 1996.

[6] D. Eastlake 3rd, CyberCash Credit Card Protocol Version 0.8, ftp : //ds.internic.net/rfc/rfc1898.txt, Feb 1996.

[7] http : //www.ietf.cnri.reston.va.us.

[8] 권도균, 한국적 전자 상거래 테스트베드 구축 협의회, http : //madang.dacom.

co.kr / dgguen / payment / summary. html, 4 1996.
[9] 권도균, SoftCash전자지불시스템. http : / / madang.dacom.co.kr / ~ dgguen / payment/softcash/2 1997.
[10] Entrust Technologies demo web CA site : http : / / www.entrust.com / new. htm.

임 신 영

1983 건국대학교 공업화학(학사)
1985 건국대학교 화학공학(석사)
1986~현재 시스템공학연구소 (선임연구원)
1992 건국대학교 전자계산학(석사)
1996 고려대학교 전자계산학(박사 수료)
관심분야 : 전산망 보안, 분산 시스템, 차세대 인터넷 기술

권 도 균

1986 경북대학교 전산학과(학사)
1989~현대 데이콤 종합연구소 멀티미디어연구팀
관심분야 : 전자 상거래, 보안프로토콜, 멀티미디어 등