안전한 전자상거래 모델

한근희*, 박영종**, 소우영**
* 한국전자통신 연구원, ** 한남대학교 컴퓨터공학과

A Secure Electronic Commerce Model

Gunhee Han*, Young-jong Park**, Woo-young, Soh**
* ETRI, ** Dept. of Computer Engineering, Hannam University

요 약

전자상거래는 기존의 상거래와는 달리 가상공간에서의 거래가 이루어지기 때문에 통신망에서의 발생하는 거래 정보의 기밀성, 무결성이 보장되어야 하며 거래자 상호간의 인증이 해결되어야 한다. 현재 이러한 문제를 해결하기 위하여 암호화, 전자서명 및 인증기관 등을 사용하고 있다. 전자상거래의 정보보호는 네트워크 계층, 기반 서비스 계층 및 응용계층으로 구분하여 이루어져야 한다. 본 논문에서는 정보보호 위협요소를 분석하고 정보보호 서비스 및 메커니즘을 구성 계층에 체계적으로 적용한 안전한 전자상거래 모델을 제시하고자 한다.

1. 서 론

최근 정보통신의 발달과 인터넷의 보급으로 전자상거래가 급속히 확산되고 있는 추세다. 전자상거래는 상거래에서 발생하는 문서의 전자적 교환을 위한 초기의 EDI(Electronic Data Interchange)를 시작으로 기업과 기업간의 거래 및 기업과 소비자간의 거래 형태로 다양하게 확대 발전되고 있다[1].

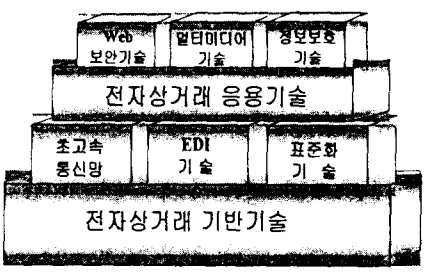
전자상거래는 가상 공간상에 대용량의 기억장치에 멀티미디어 기술을 이용한 다양한 거래를 할 수 있어 경제적이며, 거래 자료의 분석 및 통계처리가 용이하여 업무의 능률화를 기할 수 있고, 기업과 관련 기관간의 직접 접촉을 피할 수 있어 기존의 거래 방식보다 시간적, 경제적 손실을 줄일 수 있는 장점이 있다. 그러나, 전자상거래는 거래 주체간의 인증 문제, 인터넷과 같이 정보보호가 취약한 통신망에서의 거래정보 및 개인정보의 위조, 변조 및 노출 문제, 그리고, 과다한 시스템 구축비

용 부담 등의 역기능이 존재한다[2]. 따라서, 안전한 전자 상거래가 이루어지기 위해서는 이러한 역기능 문제가 해결되어야 한다.

본 논문에서는 전자상거래의 역기능중 정보 전송 시에 발생하는 문제를 해결하기 위하여 필요한 핵심 요소 기술을 분석하고 정보보호 위협요소를 계층적으로 접근하여 정보보호 서비스 및 메커니즘을 각 계층별로 적용시킨 안전한 전자상거래 개념 모델을 제시하고자 한다.

2. 전자상거래 요소 기술

전자상거래는 가상 공간상에서 불특정 다수의 소비자가 Web을 통한 가상 상점을 방문하여 원하는 물건을 선택하여 구매할 수 있으며, 판매자는 별도의 판매공간 없이 가상 공간에서 24시간 영업활동을 할 수 있다는 장점을 가지고 있다. 전자상거래가 성립되기 위해서는 다음 <그림 1>과 같은 핵심 요소기술이 요구된다.



<그림 1> 전자상거래 핵심 기술

전자상거래 핵심 기술은 기반 기술과 응용 기술로 분류할 수 있으며 기반기술로서 초고속 통신망 기술, EDI 기술 및 표준화 기술 등이 있으며, 응용기술로서는 Web 보안 기술, 멀티미디어 기술 및 정보보호 기술 등이 있다.

인터넷상에서 가상상점을 개설하고 통신망을 이용하여 상품을 판매하기 때문에 상품정보를 포함한 각종 정보는 멀티미디어 형태로 제공되어 진다. 따라서, 정보 전송 양이 방대하기 때문에 초고속 정보통신망 기술이 요구된다.

EDI는 거래 당사자간에 발생되는 문서를 약속된 형식으로 전용회선을 통하여 교환하는 방식이다. EDI의 표준으로는 ITU에서 권고한 X.400 계열의 통신표준을 적용한 MHS와 EDIFACT와 같은 문서표준이 사용된다. 최근에는 전자상거래로 확대 적용할 수 있는 인터넷 기반의 EDI에 대한 연구가 IETF(Internet Engineering Task Force)의 워킹 그룹을 중심으로 진행중이다.

국내 또는 국가간으로 이루어질 수 있는 전자상거래에서 필요한 각종 정보의 표현을 위한 표준 기술, 정보교환 표준 기술 및 정보보호를 위한 표준화 기술 등이 요구된다.

전자상거래는 인터넷의 근본적인 보안상의 취약성 때문에 웹 보안 기술이 요구된다. 현재 웹 브라우저는 간단한 인증 기술만 제공되기 때문에 IP Spoofing이나 Packet Sniffing 등의 위협에 노출될 우려가 있다. 대표적인 웹 보안 기술은 SSL(Secure Socket Layer)이나 SHTTP(Secure HTTP) 등이 있다.

인터넷상의 전자상점 또는 전자상점 대행기관의 서버 내에서 소비자의 취향에 맞는 상품을 전시하기 위해서는 상품정보 및 전자카탈로그 등을 전자적으로 표현하는 멀티미디어 기술이 요구된다

전자상거래는 소비자와 전자상점간의 사이버 공간상에서 이루어지기 때문에 거래와 지불 정보의 노출, 소비자와 기업간의 상호인증 및 지불의 투명성이 제공되어야 하는 정보보호 기술이 요구되어진다[3].

본 논문에서는 전자상거래의 핵심 요소 기술을 분석하고 각 요소 기술 중 정보보호와 관련한 기술의 분석을 통하여 거래의 안전성을 확보할 수 있는 전자상거래 개념 모델을 제시하고자 한다.

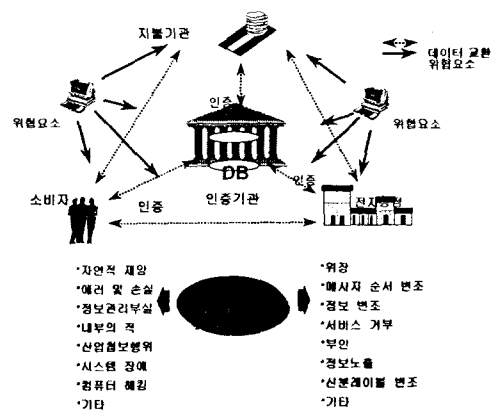
3. 정보보호 서비스 및 메커니즘

정보보호 문제를 해결하기 위하여 정보보호 위협요소를 분석한 뒤 요구되는 정보보호 서비스를 제시하고 해결할 수 있는 정보보호 메커니즘을 제시한다.

3-1. 정보보호 위협요소

전자상거래는 인터넷 EDI의 확장의 개념이기 때문에 EDI 위협요소와 인터넷에서의 정보 전송시 발생하는 위협요소가 존재한다.

아래 <그림 2>는 정보보호 위협요소를 일반적 요소와 자연적 요소로 나타낸 것이다.



<그림 2> 정보보호 위협요소

전자상거래 위협요소는 인터넷과 같은 공중망을 이용하기 때문에 정보의 노출, 변조 등의 위협 요소를 가지고 있다. 소비자와 생산자간의 거래정보는 개인정보를 포함하여 노출 시 재산상의 피해를 입을 수 있다.

전자상점 서버나 인증기관의 인증서버시스템에 대한 위협은 전자상거래 자체를 마비시킬 수도 있다. 거래에 관련정보 및 상품정보 등을 저장하고 있는 상점 시스템에 대한 서버의 공격을 통하여 중요한 기업의 자원 및 개인에 관련된 정보의 손실이 있을 수 있다. 인증기관의 인증서버 시스템에 대한 공격으로 인증관련 정보가 노출되었을 경우 전자상거래 자체가 마비될 수도 있다[3].

EDI는 비교적 안전성이 높은 전용망을 사용하기 때문에 정보보호가 비교적 안전하게 이루어지고 있으나, 전자상거래는 인터넷과 같은 공중망을 이용하여 상거래 주체간의 거래 정보를 교환하기 때문에 정보보호 문제가 가장 시급한 문제다. 정보보호 서비스를 세 가지 측면에서 분석하였다.

3-2. 정보보호 서비스

전자상거래의 정보보호 서비스를 시스템 정보보호, 네트워크 정보보호, 및 결제 시스템 정보보호 등의 세 가지 측면에서 분석하고자 한다.

가. 시스템 정보보호

시스템 정보보호는 상인 시스템 서버의 보안과 지불 대행기관 시스템 보안, 및 인증기관의 시스템의 보안으로 구분할 수 있다. 시스템 정보보호는 내부보안과 외부보안을 고려하여 제공되어야 한다.

내부보안은 시스템 관리자나 내부사용자의 의도적인 정보 유출이나 변조 등으로부터 시스템을 지키는 것이며, 비밀번호 관리 및 사후 감사용 자료를 생성하여 사후 보안방안을 마련하는 것이다.

외부보안은 시스템 외부에서 의도적으로 침입하여 정보의 파괴, 유출 등을 시도하려는 해커들의 소행으로부터 시스템을 보호하는 것이다. 시스템 보안은 접근통제기법이나 방화벽에 의하여 이루어지고 있으나, 내부보안은 해결할 수 없으므로 좀 더 능동적이고 지능적인 침입탐지 시스템과 같은 보안 시스템이 요구된다.

나. 네트워크 정보보호

인터넷은 구조적으로 취약성을 지니고 있으며, 취약성을 이용하여 Packet Sniffing과 IP Spoofing과 같은 해킹이 시도되고 있다. 따라서, 네트워크상의 정보의 위·변조를 방지할 수 있는 보안 서비스가 제공되어야 한다.

네트워크 정보보호 서비스는 다음과 같다. 인증은 거래 당사자간의 상호 신분확인을 해주는 서비스며, 전자서명 및 전자인증서를 통하여 이루어진다. 기밀성은 지불정보에 대한 비밀성이 제공되는 것을 의미한다. 또한, 주문정보 및 지불정보에 대한 무결성이 제공되어야 한다. 무결성은 전자서명 방식에 의하여 제공되어질 수 있다[5]. 암호화(encryption)는 위에서 논한 인증, 기밀성, 무결성 등을 제공하기 위하여 사용하는 기법이다.

다. 결제 시스템 정보보호

전자상점이 소비자로부터 결제정보를 받아 결제 기관에 전달하는 상인이 그 내용을 볼 수 없도록 해야 한다. 위와 같은 결제 정보보호 문제도 암호화 알고리듬으로 해결하고 있다. 결제 정보 보호를 위하여 안전성이 확보된 전자결제 시스템을 제공하여야 한다.

3-3. 정보보호 메커니즘

정보보호 서비스를 위하여 제공되고 있는 대표적인 정보보호 메커니즘은 Web 보안 메커니즘, 암호화 알고리듬, 전자서명 방법, 인증기관 및 전자 지불시스템 등이다.

가. Web 보안 메커니즘

웹 보안 메커니즘은 응용계층에서의 보안기술과 네트워크 계층에서의 보안 기술로 분류한다.

응용 계층에서의 보안기술로써 NCSA의 Mosaic/ httpd에서의 PGP/PEM을 이용한 인증 및 암호화, EIT (Enterprise Integration Technologies)에서 개발한 HTTP 프로토콜을 확장한 SHTTP, 일 방향 해시 함수를 이용한 Message Digest Authentication 및 Kerberize Mosaic/httpd 등이 있다[4].

네트워크 계층에서의 보안 기술은 웹 브라우저가 상주하는 응용계층에서 메시지를 암호화하여 불안전한 채널로 전송하는 대신에 응용 계층을 안전한 채널을 설정하는 특수한 소켓만을 설정하도록 하는 Netscape사의 SSL (Secure Socket Layer)이 대표적이다[1, 4].

나. 암호화 알고리듬

암호화 알고리즘은 정보의 기밀성, 무결성을 제공하기 위하여 가장 많이 사용되는 메커니즘이다. 암호화 알고리듬은 암호화키와 복호화키가 같은 경우 대칭형 암호화 알고리듬이라 하며 대표적인 알고리듬으로는 DES가 있으며, 다른 경우는 비대칭형 알고리듬으로써

RSA가 있다[4].

DES는 IBM에서 개발하여 1977년에 미국 표준국에서 표준안으로 채택하였으며 수행시간이 짧지만, 인터넷과 같은 개방 환경에서 키를 안전하게 전달하는 것이 문제가 된다[4].

RSA는 MIT의 Rivest, Shamir, Adleman에 의하여 1978년 개발하였으며, 공개키로 암호화한 메시지는 개인키로만 복호화 할 수 있고, 반대로 개인키로 암호화한 메시지는 공개키로만 복호화가 가능하다. 따라서, 키 전송을 하지 않기 때문에 키 전송 문제가 발생하지 않는다[4].

다. 전자서명(Digital Signature)

전자서명 메커니즘은 무결성, 부인봉쇄 및 인증서비스를 제공하기 위하여 공개키 암호화 알고리듬과 메시지 다이제스트 방식을 이용하는 것으로써 전송할 메시지를 메시지 다이제스트하고 이를 다시 송신자의 개인키로 암호화하는 것을 말한다.

라. 인증기관(Certificate Authority)

거래시 주체 상호간에 발생하는 거래 정보의 인증, 무결성 및 부인방지와 같은 정보보호 서비스를 제공하기 위해서는 거래 주체간의 공개키의 정확성이 보장되어야 한다. 공개키의 정확성을 보장하기 위하여 상거래 주체가 아닌 제 3의 기관이 인증기관이다. 인증기관 체계는 공개키 기반구조를 사용하고 있으며, SET 기반과 미 국방성의 MISSI 기반구조가 대표적이다[4, 5].

마. 전자지불 시스템

전자지불 시스템은 소비자가 전자적인 수단을 통하여 구입물건에 대한 대금을 지불하는 시스템이다. 전자지불 시스템은 크게 기존의 신용카드를 IC 카드로 확장한 개념인 IC 카드 기반 지불시스템과 인터넷 등의 네트워크에서 사용하는 네트워크형 전자지불 시스템으로 구분할 수 있다[6].

IC카드기반의 지불시스템은 IC 카드에 사용자 정보를 기억시킬 수 있는 메모리, 중앙처리장치, 사용자의 신분확인, 상호인증을 위한 암호화 알고리듬이 내장되어 있다. 대표적 IC카드 방식 지불시스템은 Mondex 카드가 있다.

네트워크형의 전자지불시스템은 기존의 신용카드로 온라인 결제하는 것과 같은 시스템, 전자현금시스템, 전자수표시스템, 마이크로 지불시스템 및 전자자금 이체 등이 있다[6]. 네트워크형의 전자지불 시스템 중에서 가장 실생활에 가까운 것은 전자현금시스템이며, 익명성, 보안성, 휴대가능, 양방향성 등을 제공하여야 한다.

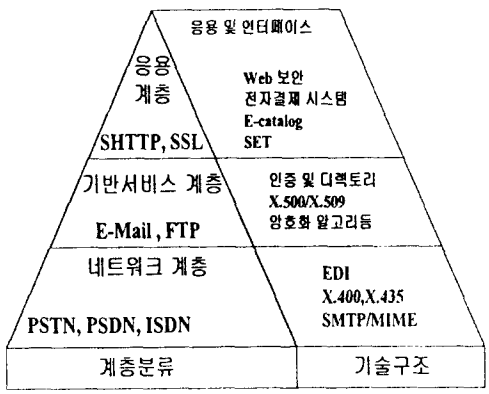
<표 1> 정보보호 기술사례

구분 / 서비스	대 상	사용 기술 사례
Web보안	응용계층	PGP/PEM, EIT, SHTTP
	네트워크	SSL 등
시스템 보안	내부보안	침입탐지시스템
	외부보안	Firewall, 접근제어
인증기관	PKI	SET CA MISSI CA
전자지불	IC 기반	EMV, MULTOS, Mondex, SET 등
	네트워크	DigiCash, ECash,, 전자자금이체 등

위 <표 1>은 안전한 전자상거래를 위하여 각 대상별로 적용한 정보보호 메커니즘 및 사용 기술 사례를 나타낸 것이다.

4. 안전한 전자상거래 모델

본 논문에서는 안전한 전자상거래 모델을 정보보호 서비스 및 메커니즘을 제시하기 위하여 보안 기술을 계층적 관점에서 제시하였다. 다음 <그림 3>은 전자상거래 기술구조를 계층적으로 나타낸 것이다.



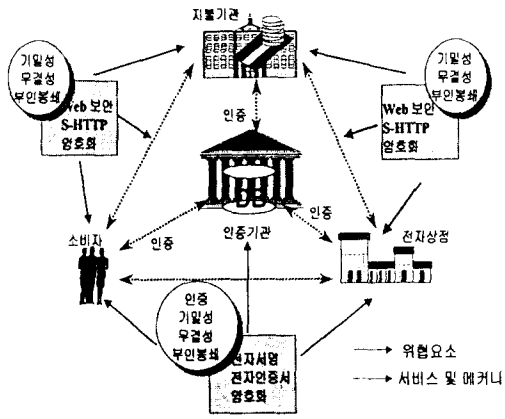
<그림 3> 전자상거래 기술구조

<표 2> 전자상거래 적용 기술

구분 / 대상	서비스	메커니즘 및 적용기술
시스템	접근통제 무결성 기밀성	암호화 알고리듬 방화벽, 침입탐지 시스템
네트워크	무결성 기밀성 인증	암호화 알고리듬 전자서명, SHTTP, SSL
결제정보	익명성 보안성 휴대가능 양방향성	IC 카드 기반 네트워크 기반 SET

<표 2>는 정보보호 대상별로 필요한 정보보호 서비스 및 메커니즘을 나타낸 것이다.

<그림 4>는 전자상거래의 정보보호 위협요소를 제시하고 필요한 정보보호 서비스 및 메커니즘을 적용하여 안전한 전자상거래 개념 모델을 나타낸 것이다.



<그림 4> 안전한 전자상거래 개념 모델

안전한 전자상거래를 위해서는 핵심 요소 기술의 개발과 계층별 보안기술의 적용, 그리고, <그림 4>와 같은 상거래 주체간의 정보보호 서비스 및 메커니즘을 적용하여 역기능 문제를 해결하여야 한다.

5. 결 론

전자상거래는 우리 나라를 비롯하여 대부분의 국가에서 이루어지고 있으며, 전자상거래의 이용 확대는 국제적인 추세에 있다. 본 논문에서는 전자상거래의 핵심기술을 분석하고 그 중 정보보호 기술을 분석하여 안전한 전자상거래 개념 모델을 제시하였다. 전자상거래는 국내의 기업과 소비자간의 문제뿐만 아니라 국가간의 무역에도 커다란 영향이 미치기 때문에 국가간의 법률적 제도적 문제들이 해결되어야 하며 그러기 위해서는 국가 차원의 인증기관의 설립, 암호화 기법의 개발 등이 선행되어야 할 것이다.

*. 참고문헌

1. 임춘성 외 3, "전자상거래 구현을 위한 기술 체계와 적용요인 분석", 한국 CALS/EC 학회지 제2권 제2호, 1997. 12.
2. 고승철, 성맹희, "정보보호 기술 분류", 정보처리지 제4권 제2호, 1997. 3.
3. 김기현 외 3, "정보보호 기술 분류", 통신정보보호학회지 제8권 제1호, 1998. 3.
4. Warwick Ford, Michael S. Baum, "Secure Electronic Commerce", Prentice Hall PTR, 1997.
5. 김종기, "미 국방부의 다수준 정보체계 보안사업(MISSI)", 정보처리지 제4권 제2호, 1997. 3.
6. 정준원 외 3, "전자지불시스템 기술 및 표준동향 분석", 정보처리지 제5권 제2호, 1998, 3.