전자상거래에서의 보안 암호기술 연구

Study on the Preservation Technology and a Secret-Sign Technology

김 윤상*, 정진용, 김형석, 신 정길, 최 성
남서울대학교 전자계산학과

youn sang Kim,JinYong Jung, Hyungsuk Kim, JungGil Shin, Sung Choi
Dep. of Computer Science, Nam Seoul University

요 약

본 논문은 인터넷과 통신매체의 확산과 더불어 최근에는 기업간, 기업과 정부간에 주로 정형적인 문서교환에 활용되던 초기의 EDI(Electronic Data Interchange)가 멀티미디어 정보교환이 가능한 인터넷의 보급, 확산과 함께 소비자를 대상으로 하는 전자상거래(EC : Electronic Commerce)로 급속히 확산되고 있으며, 이를 지원하기 위해 기업의 정보화 기반을 구현하는 ERP(Enterprise Resource Planning)도 요구되고 있다. 그러나, 전자상거래는 네트워크를 통하여 형성되므로 사용자들은 서로 만나지 않고 거래하게 된다. 이는 전자상거래의 장점이기도 하지만, 반대로 상호간의 신분에 대한 인증이 쉽지 않다는 단점이 된다. 본 논문에서는 이러한 위험을 방지하기 위한 보안기술 및 암호기술에 대해 연구하였다.

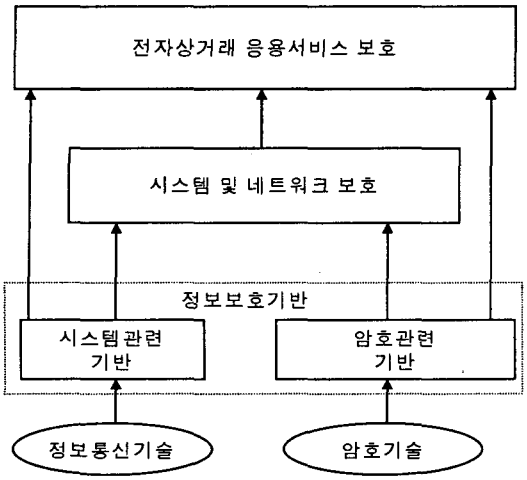
1. 전자상거래의 개념

인터넷에서는 개방형 온라인 네트워크라는 특성 때문에 정보의 효율적인 관리 및 보안 문제 등이 해결해야 할 매우 중요한 과제로 부각되어지고 있다. 특히 인터넷뿐만 아니라 전세계적으로 초고속 정보통신망의 구축이 각 나라의 중요한 하부구조 건설 차원에서 활발히 진행되어지고 있고 또한 이를 기반으로 한 전자상거래, 홈쇼핑 등에서 거래에 수반된 당사자들의 개인정보 보호와 안전한 거래를 보장하는 기술적인 요구사항들을 수용해야 할 시급한 상황에 처해 있다. 따라서, 현재 전세계적으로 개방형 네트워크라는 가상공간에서 요구되는 거래의 안전성을 현실 세계에서의 그것과 동일한 수준으로 보장하는 보안 프로토콜의 연구와 그 실제 구현에 소요되는 요소 기술의 개발이 활발히 진행되어지고 있다. 그러나 국내에서는 아직 보안 프로토콜에 대한 개발이 이론적인 측면에서 진행되고 있으며 암호 알고리즘의 법적인 제약 문제로 인하여 프로토콜 구현에 어려움을 안고 있다.

본 논문에서는 이러한 위험을 방지하기 위해 전자상거래에 대한 개념을 정리하고, 전자상거래에서 정보보호를 위해 제안된 보안기술 및 암호기술에 대하여 연구하였다.

2. 전자상거래 보안기술 체계

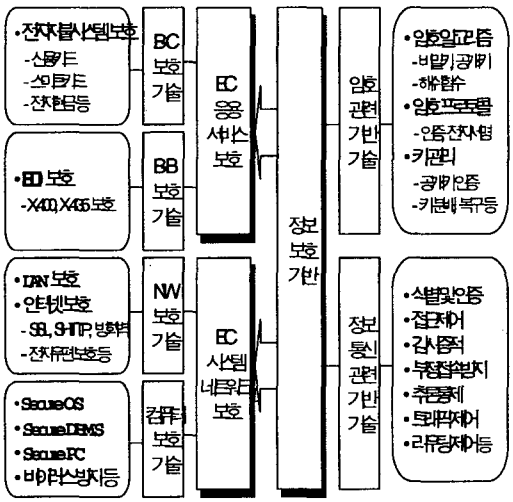
전자상거래 보안기술에 대한 전반적인 이해를 위해서는 전자상거래 정보보호 기술에 관한 분류가 필요하다. 전자상거래 보호를 위한 기술은 <그림 2-1>과 같이 정보보호 기반기술, 시스템 및 네트워크 보호 기술, 전자상거래 응용서비스 보호 기술로 분류할 수 있다. 정보보호 기반기술은 이론적 암호학이나 정수론 등 암호기술에 정보처리 기술이 가미되어 암호 알고리즘, 암호 프로토콜 기술을 형성하고 있는 암호 관련 기술과 감사기록, 접근제어 등 정보처리 기술 및 라우팅 제어, 트래픽 제어 등 정보전송 기술에 기반을 둔 순수 시스템 관련 기술로 구분된다.



<그림 2-1> 전자상거래 보호를 위한 계층

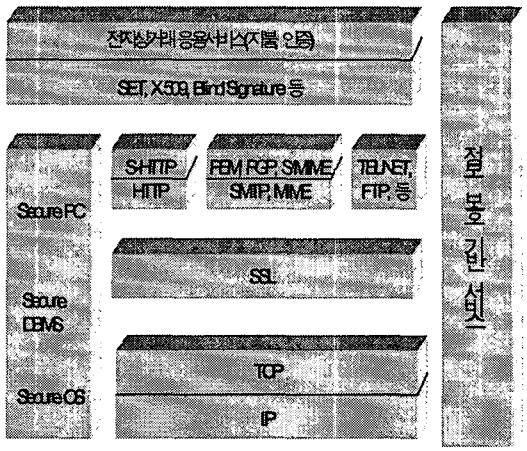
전자상거래는 웹 기술을 근간으로 클라이언트-서버 기술, 분산처리 기술, 실시간 DB기술이 요구된다. 사용자와 상점은 웹이 제공하는 환경에서 거래 행위를 하므로 웹 기술의 보안 취약성은 전자상거래의 미래를 결정짓는 중요한 해결요소이다.

EC 응용서비스 보호기술은 정보보호 기반 및 EC 시스템/네트워크 보호기술들을 활용하여 EC 서비스에 정보보호 기능을 제공하는 기술로 크게 B-C 서비스 보호와 B-B 서비스 보호로 구분할 수 있다. <그림 2-2>는 위와 같은 전자상거래 보호 기술의 분류체계를 보여주고 있다.



<그림 2-2> 전자상거래 보호기술 분류 요약

이와 같은 전자상거래 보호기술의 분류체계에서 대표적인 기술들을 도식화하면 다음 그림과 같다.



<그림 2-3> 전자상거래의 대표적 보호기술

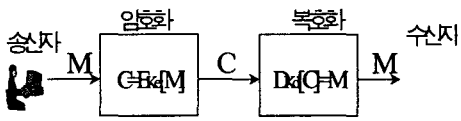
3. 전자상거래 암호기술 체계

3.1 암호 시스템 및 분류체계

넓은 의미에서의 암호학(cryptology)은 평문(plain text)을 보호하기 위한 암호화 알고리즘을 연구하는 암호학(cryptography)과 평문을 해독하기 위하여 암호화 과정과 암호문(cipher text)을 연구하는 암호해독학(cryptoanalysis)으로 구분된다.

암호화되지 않은 상태의 평문을 암호문으로 만드는 암호화 과정(encryption, encoding), 역으로 암호문을 평문으로 변화시키는 복호화 과정(decryption, decoding), 암호화와 복호화 과정에서 사용되는 암호화 키(cryptographic key)와 키 관리 등 정보 보호를 위한 일련의 프로세스를 암호 시스템이라고 한다. 키를 사용하는 암호 시스템은 <그림 3-1>와 같이 표현할 수 있다.

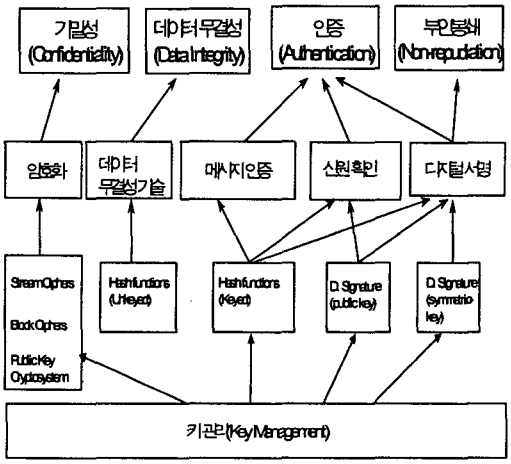
$$Ke(M) = C,\ Kd(C) = M$$



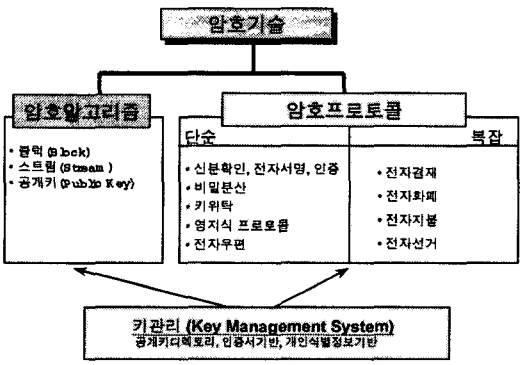
- M: 평문
- E: 암호화알고리즘
- Ke: 암호화키
- C: 암호문
- D: 복호화알고리즘
- Kd: 복호화키

<그림 3-1> 암호화 / 복호화 과정

암호기술은 기밀성, 무결성, 인증 및 부인봉쇄 서비스를 제공하기 위한 기술들로 <그림 3-2>로 분류된다. 초기의 암호기술은 데이터의 기밀성을 보장하는 수단으로 사용되어 발전되어 왔으나, 최근 인터넷과 같은 공중망을 통한 전자거래가 활성화됨에 따라 상대방의 신원 확인, 데이터의 무결성 보장, 전자거래에 대한 분쟁소지를 없앨 수 있는 서비스에 대한 요구에 암호기술의 적용이 활발히 이루어지고 있다.



<그림 3-2> 암호기술간의 상관관계



<그림 3-3> 암호기술의 분류

암호기술은 다시 크게 <그림 3-3>과 같이 암호 알고리즘, 암호 프로토콜과 키관리 기술로 구성되어 있다. 암호 알고리즘은 순수 암호학 및 정수론을 기초로 이를 정보처리기술을 이용하여 데이터의 해독을 어렵게 데이터의 내용을 암호화하거나 복호화하는 방법으로 비밀키 암호, 공개키 암호, 해쉬함수, 난수생성(random number generation)등을 포함한다.

3.2 대칭키와 공개키 암호알고리즘

대칭키 암호 알고리즘은 비밀키 암호 알고리즘 혹은 단일키 암호 알고리즘이라고도 하며, 송·수신자가 동일한 키에 의하여 암호화 및 복호화 과정을 수행하며, 공개키 암호 시스템은 암호화 키와 복호화 키가 서로 다르고, 하나를 알더라도 그에 대칭되는 키를 알기 어려운 암호 시스템을 의미한다.

<표 3-1> 대칭키 암호시스템과 공개키 암호시스템 비교

	대칭키 암호 시스템	공개키 암호 시스템
작업을 위한 요구사항	-동일한 키를 가진 동일한 알고리즘이 암호/복호에 사용 -수신자와 송신자는 알고리즘과 키를 나누어야 함	-암호, 복호용 키 두개와 한 개의 알고리즘 -수신자와 송신자는 두개의 키 중 일치하는 키가 한 개 이상
보안성을 위한 요구사항	-키는 비밀을 유지해야 함 -만일 다른 정보를 이용할 수 없다면 메시지를 해독하는 것이 불가능 / 비실용적 -알고리즘과 암호문 샘플만으로는 키를 알 수 없음	-두개의 키 중 하나는 비밀유지 -만일 다른 정보를 이용 불능이면 메시지 해독불능/비실용적 -알고리즘과 암호문 샘플, 한 개의 키만으로는 키를 알 수 없음

3.3 키 관리

키 관리의 목적은 대칭키 암호 시스템 또는 공개키 암호 시스템에서 사용되는 암호학적 키들을 안전하게 다루기 위한 키의 생성, 등록, 확인, 분배, 설치, 저장, 파생, 보관, 취소, 말소 , 폐기 등과 같이 일련의 절차를 제공하는 것이다. <표 3-2>은 키 관리 서비스를 간단히 설명한 것이다.

<표 3-2> 키 관리 서비스

키 관리	내 용
키 생성	강한 안전성을 가진 키를 안전하게 생성할 수 있는 절차를 제공한다.
키 등록	키와 사용자를 연결시키는 서비스로 키 등록기관에 의해 제공된다.
키 확인서 생성	공개키와 사용자의 연관성을 보장하는 것이며, 인증기관에 의해 제공된다.
키 분배	인가된 사용자들에게 키관리 정보 객체들을 안전하게 제공해 주는 일련의 절차를 제공한다.
키 설치	키를 사용하기 전에 항상 필요한 절차로서 키관리 설비 내에서 키가 위험하지 않은 방식으로 배치한다.
키 저장	미래에 사용하거나 백업을 위해 생성된 키들을 안전하게 저장해주는 서비스이다.
키 파생	파생키라고 불리는 비밀 근원키를 이용하여 다른 새로운 세션키들을 생성하는 작업이다.
키 보관	일반적인 사용후에 키를 안전하게 보관하기 위한 일련의 절차를 제공한다.
키 취소	키의 노출, 확인서 사용기간의 만료 등과 같은 경우에 사용자가 키를 취소할 수 있게 한다.
키 말소	키와 사용자의 연결을 단절시켜 주는 서비스로 키 폐기 서비스의 일부분이 된다.
키 폐기	더 이상 사용될 필요가 없는 키들을 안전하게 폐기하기 위한 일련의 절차를 제공한다.

4. 비밀분산방식 알고리즘

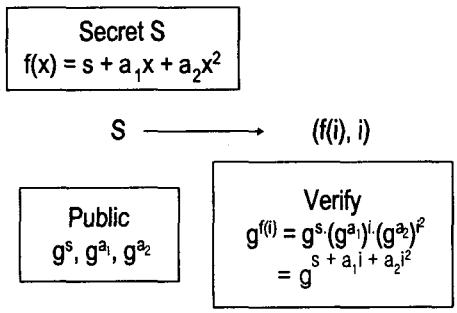
어떤 중요한 비밀(Secret)을 여러 개의 조각(Share)으로 나누어 여러 사람이 관리하도록 하는 것을 비밀분산 방식이라고 한다.

먼저 비밀 분배자는 비밀값 S를 포함하는 다항식 f(x)를 만든다. 또한 각 항의 상수를 공개값 g에 승산해서 g^{s}, g^{a1}, g^{a2}를 만들어서 공개한다. 그리고 나머지 사항은 비밀의 공유자인 각각의 i 에 대해서 비밀 조각인 점(i, f(i))를 전송한다. 이러한 비밀 조각(shadow)을 수신한 사용자는 공개값인 g^{s}, g^{a1}, g^{a2}와 자신이 수신한 (i, f(i))값을 이용해서 다음과 같은 수식을 만들 수 있다.

$$g^{f(i)} = g^{s} \cdot (g^{a1})^{i} \cdot (g^{a2})^{i2}$$

만약 위 수식이 올바르다면 비밀 조각의 수신자는 자신이 수신한 것이 원래 비밀의 조각임을 확신할 수 있다. 또한 비밀 분배자를 제외한 모든 사람은 이산대수 계산의 어려움에 따라 g^{s}, g^{a1}, g^{a2}값을 안다고 하더라도 s, $a1$, $a2$값을 알 수 없기 때문에 비밀은 안전하게 공유된다.

그리고 이 알고리즘을 도식화 하면 다음 그림과 같이 나타낼 수 있다.



<그림4-1 비밀분산 알고리즘>

5. 결 론

전자상거래에는 해결해야 할 문제가 몇 가지 있다.

첫째는 프라이버시 문제다. 우리가 전송하거나 받은 메시지를 중간에 제3자가 가로채거나 몰래 읽거나, 또는 수정하지 않았다는 것을 어떻게 보장하겠는가 하는 것이며, 둘째는 사기행위의 문제다. 어떤 사람이 신용카드의 사용자라고 했을 때 신분 확인 없이 이것을 어떻게 믿을 수 있겠는가 하는 것이다. 소비자의 입장에서 한번도 본적이 없는 인터넷 상인을 과연 믿을 수 있겠는가 하는 것도 여기에 포함된다. EC의 활성화는 이러한 문제가 모두 해결될 때 가능하다.

이상에서 우리는 전자상거래의 보안에 대한 전반적인 내용을 다루고 암호기술에 관하여 조사하였다. 암호기술이 전 세계적으로 가장 널리 사용되고 있는 것은 사실이다. 그러나 점점 암호기술에 대한 신뢰성이 떨어져 가고 있는 실정이다. 이 문제점을 해결하기 위한 앞으로의 연구방향은 웹상에서 쉽고 편리하게 정보를 보호할 수 있는 프로토콜의 개발에 주력하는 것이다. 또한 웹이나 전자메일등을 전적으로 수입에 의존하고 있는 현재의 상황에서 벗어나기 위해 우리 실정에 맞는 적합한 암호화 알고리즘과 비밀키의 보안 및 관리등을 위한 기술 개발에 노력해야 한다.

<참고문헌>

(1) 강명호, 송주석, "전자상거래 관련 기술," 통신정보보호학회지, Vol.7, No.3, 1997.9.
(2) 김광조, "암호이론", 제4회 정보통신망 정보보호 워크숍(NETSEC-KR'98) 특강자료집, 1998. 6.
(3) 김기현 외 3인, "정보보호 기술 분류"
(4) 김지홍, "공개키 기반구조 기술", 제4회 정보통신망 정보보호 워크숍(NETSEC-KR'98) 발표 자료집, 1998. 6.
(5) 김홍근, 최영철, "전자상거래 정보보호기술 현황 및 대응방안, 정보처리학회지 Vol.6, No.1, 1999.1
(6) 한국정보보호센터, 정보보호 총서, 1996.12
(7) 한국정보보호센터, CALS/EC 정보보호기술 표준화에 관한 연구, 1998.6
(8) 한국정보보호센터, CALS/EC 정보보호 표준 교재, 1999.1
(9) 한국정보보호센터, CALS/EC 공개키 인증 시범시스템 개발 보고서, 1998.6
(10) 한국정보보호센터, CALS/EC 키관리 시스템 개발 보고서, 1998.6