2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

전자상거래 사이트 구축 시 정보보안 및 관리 방안 연구

이 상연, 김 지영, 윤 동식 °
안동과학대학 사무자동화과
e-mail:yundos@mail.andong-c.ac.kr

A Study of Information and management method when Construction E-business site

Lee sang-youn, kim ji-young, Yun dong-sic
**Dept of office automation, Andong science college

요약

인터넷(Internet) 이란 거대한 네트웍들이 모인 것이다. 인터넷 속의 산업구조는 1:1 대면 방식의 구조에서 네트워크 상의 On-line 구조로 변화되어 가고 있다. 인터넷 상에서의 전자상거래를 통하여 우리 농촌의 농산물 판매 구조가 변화를 가져와야 할 것이다. 생산지에서 소비자에게 직송할 수 있는 상거래 시스템이 필요한 것이다. 이에 본 연구에서는 "웹 상의 농산물 전자상거래 사이트 구축 시 정보보안 및 관리 방안"을 SSL/ TLS를 이용한 쇼핑 시나리오를 이용하여 개선된 암호화 및 사용자 인증 전자결재시 사용되는 전자서명 키를 연구하여 구현하고자 한다. 또한 비대칭적 암호화 기법 및 SET을 이용한 암호화 거래 방법을 제시하였으며, 호스트의 비대칭적인 스위칭 시스템으로 사용자가 웹 사이트에 접속시에는 데이터 서버는 닫혀있는 상태이고 비동기적으로 사용자가 웹 사이트에서 인증을 득한 후에 데이터 서버로 접속이 가능하며 데이터의 액세스가 끝난 후에는 웹사이트의 접속을 재게 시키고 데이터 서버의 액세스는 무효화시킴으로써 서버의 정보 보안 및 관리를 효율적으로 수행한다.

1. 연구 개요

인터넷(Internet) 이란 거대한 네트웍들이 모인 것이다. 즉, 네트웍들의 네트웍이다. 인터넷은 몇 가지 특징을 가지고 있고 그에 따라 여러 가지 문제점을 가지게 되었다.

첫째, 개방성이다. 원래 인터넷은 학술 연구의 목적으로 만들어진 네트웍이기 때문에, 모든 사람에게 개방되어 있다.

둘째, UNIX, TCP/IP 등의 소스 코드가 개방되어 있다. IBM의 SNA 등의 프로토콜은 업체만이 보유하고 있으므로, 보안이 큰 문제가 없지만, TCP/IP 프로토콜이나 UNIX 시스템은 많은 학교나 연구소 등에서 소스 코드를 보유하고 있고, 서점에서도 교재로 판매하고 있을 뿐만 아니라, 인터넷에서 이러한 문서들을 무료로 배포하고 있다.

셋째, 상호 정보 교환이 쉽다. 인터넷에서는 검열이라는 것이 불가능할 정도로 많은 게시판(BBS)과 온라인 정보 교환을 위한 방법들이 제공되므로, 새로운 침입 방법들이 침입자들간에 손쉽고 은밀하게 서로 교환되어 사용되는 것이다.

이러한 인터넷의 취약점을 이용하는 침입자들을 보통 해커 (Hacker) 라고 부르는데, 실제로 해커란 네트웍이나 시스템에 대한 전문가를 가리키는 말이었지만, 이 의미와는 다르게 해석되고 있으므로, 보통 악의를 가진 침입자들을 불법 침입자 (Intruder, Cracker) 라고 부르기도 한다.

침입을 방지하기 위한 인터넷에서의 보안의 목표로는 정보의 비밀성(Information Confidentiality), 정보의 무결성(Information Integrity), 정보의 가용성(Information Availability), 부인 봉쇄(Non-Reputation)등을 들을 수 있다.

불법 침입자라고 알려진 해커들은 이 중에서 주로 첫번째인 비밀성을 위반하는 경우이다.

비밀성이나 무결성을 보장하려면 가용성이 낮아지게 된다. 그 반대도 마찬가지이다. 이들을 위반한 가장 잘 알려진 해킹 사건은 스파이 해킹 사건, 인터넷 웜 사건, 쫀 메카트닉 사건, 씨티은행 침입 사건 등이다. 이러한 해킹 사례를 외국뿐만이 아니라, 최근 국내에서도 급격히 증가하

본 연구는 한국정보보호센터 지원과제임

고 있는 추세이다. 이는 국내의 환경이 열악하기도 하지만, 아직은 관리자들의 인식이 부족하고 보안 시스템에 대한 투자가 적어서 제대로 된 보안 시스템을 갖춘 곳이 거의 없기 때문이기도 하다. 하지만, 이러한 보안 시스템을 아무리 잘 갖춘다고 해도 관리자의 인식이 부족하다면 무용지물이 되고 만다.

이에 본 연구에서는 "웹 상의 농수산물 전자상거래 정보보안 및 관리 방안"에 대하여 현재의 기술과 개선된 새로운 기술을 연구하고자 한다.

2. 본론

현재의 산업구조는 1:1 대면 방식의 구조에서 네트워크 상의 On-line 구조로 변화되어 가고 있다. 이에 우리 농촌의 농수산물 판매 구조가 변화를 가져와야 할 것이다. 생산지에서 소비자에게 직송할 수 있는 상거래 시스템이 필요한 것이다.

이 농산물 전자상거래를 구축하다보니 장보 보안 및 관리에 필요한 결재 수단이 대두되기 시작한다. 현재 전자상거래 상에서 이루어지는 결재 방식 중 가장 많이 사용되어지는 신용카드 결재이다. 또한 은행을 이용한 온라인 계좌 입금, 지로를 통한 결재 시스템이다.

2.1 전자결재

컴퓨터 네트워크를 이용한 결재에 대하여 살펴보면 인터넷 전자상거래 결제 방법의 발전을 들을 수 있다.

1단계 : 네트워크 외부 결제 또는 보안이 없는 신용카드와 재무정보 송 수신
2단계 : 암호기법을 이용한 신용카드에 의한 결제
3단계 : 전자현금/스마트카드에 의한 결제

본 연구에서는 사이버 머니를 결재 시스템으로 구축하고자 한다. 사이버 머니의 장점을 살펴보면 나만이 활용할 수 있다는 점과 신용카드 결재와 같이 정보의 누출을 막을 수 있다는 것이다.

사이버 머니 지불 시스템을 살펴보면

첫째, 지불 브로커 시스템 둘째, 전자 화폐 시스템 셋째, 소액 전자 지불 시스템 넷째, 전자 수표 시스템 등을 들 수 있다.

사이버 머니는 1995년 4월 CyberCash, Inc.에서 개발되었으며 장범으로는 고도 암호화 기법으로 신용카드정보유출 방지, 판매자가 고개의 신용카드 정보 해독 불가능, FV(First Virtual)의 E-mail 방식보다 처리시간이 적게 소요된다는 것이다. 단점으로는 고객, 판매자 모두 CyberCash 암호화 프로그램을 설치하여야 한다. 또한 판매자는 CyberCash사와 제휴한 은행의 계좌를 보유하여야 한다. 우리나라 현실을 볼 때 이 두 번째 단점은 장점으로 전환 시킬 수가 있다. 현재 우리 농촌 지역의 농민들은 농협이라는 금융기관을 이용하여 농산물 판매를 하며 은행 업무를 수행하고 있다. 그러므로 특정된 은행을 지정하지 않고 현재 사용중인 농협을 활용하면 쉽게 구축될 것으로 사료된다.

또한 농산물 전자상거래 망은 소액 지불 방법으로 이루어지므로 이에 적당한 방법을 고안해 내야 할 것이다. 현재 이에 사용되는 제품으로 Digital Equipment Corp. 사의 Millicent가 존재한다. 이 제품의 특징은 Scrip이라는 소액 전자화폐를 판매자가 발행하며 브로커를 통하여 고객에게 판매하면 고객은 Scrip을 판매자에게 제시한다. 이 시스템의 장점으로는 Scrip은 발행자인 판매자가 진위 및 이중 사용 여부를 즉시 체크할 수 있어, 통신비용을 절감할 수 있으며, Scrip은 소액이기 때문에 Internet상에서 제3자가 가로챌 가능성이 낮아 고도의 보안이 필요치 않다. 단점으로는 Scrip은 특정 가상점포에서만 사용할 수 있어 사용처가 제한된다. 또한 구매절차가 복잡하다는 단점을 가지고 있다. 우리는 이 문제점들을 해결하고자 한다.

2.2 보안 시스템의 종류

보안 시스템에는 여러 가지 종류가 있다. 가장 간단한 예가 라우터(Router)인데, 라우터의 패킷 필터링(Packet Filtering) 기술을 이용하는 것이다. 이를 이용해서 Router를 통과하는 패킷들의 헤더(Header) 내용을 보고 이 패킷들을 통과시킬 것인지 아닌지를 결정하는 것이다. 하지만, 라우터만으로는 제약점이 많고, 패킷 필터링 규칙이 매우 복잡하므로 라우터만으로 보안 시스템을 구현하는 경유는 매우 드물다.

두 번째로, UNIX나 Windows NT, Intranet ware같은 네트웍 운영 체제에서도 일부 보안 기능을 제공하고 있다.

세 번째로, 단순한 패스워드 인식 기법을 사용하는 UNIX 시스템 같은 인증 방법이 아니라, 보다 강력한 사용자 인증을 위한 사용자 인증 시스템이 있다. 주로 일회용 패스워드(One-Time Password)가 이에 해당된다.

마지막으로 가장 안전하고, 효과적인 방화벽 시스템이 있다. 물론 위에서 언급한 시스템들은 보통 개발적으로 사용되지 않고 방화벽과 함께 사용되므로, 방화벽 시스템의 한 구성 요소로 간주하기도 한다.

도 구 명	기 능
COPS	일반적인 시스템 보안 점검 및 보고
Tripwire	파일 시스템 무결성 검사
ISS	Internet Security Scanner. 네트워크 호스트 공격 대상 분석
SATAN	네트워크 취약점 공격
Tcpwrapper	네트워크에서의 접근 제어
Crack	패스워드를 알아내는 도구
Sniffer	네트워크상의 패킷 감청/보고
CPM	LAN 모니터링
Swatch	시스템 로그 분석 및 보고 시스템

3. 전자상거래 정보보안 및 관리 방안 연구

인터넷 상에서 가장 많은 사용자들이 이용하고 있는 전자우편이나 최근들어 대두되기 시작한 전자상거래 서비스 측면에서 보면 파이어월은 그 보안성에 여러 가지 허점을 가지고 있다. 왜냐하면 전자우편의 경우는 내부망에서 작성한 데이터가 파이어월을 거쳐 외부망으로 전송되는데, 파이어월을 거칠 때까지는 안전하지만 외부망에서의 안전을 보장할 수 없게 된다. 또한 전자상거래도 마찬가지로 실제 제품을 구입하고 지불하는 과정에 대한 안전 보장을 해줄 수 없다.

전자우편이나 전자상거래를 포함해 일반적으로 정보를 보안하기 위한 가장 안전한 방식은 정보를 암호화하는 방법이다. 최근들어 정보를 암호화하기 위한 여러 가지 방법들이 나오고 있다.

3.1 암호화

분산 컴퓨팅 환경에서 정보 누출에 대한 위협요소들은 매우 다양하다. 정보 보호에 대한 권한을 가진 권한자의 특권을 대신 도용하는 경우와 같이 권리를 위장하는 경우가 있다. 또한 도청이나 불법접근에 의한 정보노출, 데이터 변경에 따른 무결성 파괴, 사용자 특권을 변경하는 권한 침해와 메시지 송신과 수신을 부정하는 부인 등이 있을 수 있다. 위협 행위들을 해결할 수 있는 방법은 현재로서는 암호화가 가장 강력한 방법으로 떠오르고 있다.

암호화 기술은 모든 정보통신 분야에서 적용할 수 있다. 즉, 디지털 정보를 다루는 모든 분야에서 보안이 필요하다면 암호화를 응용할 수 있다는 것이다. 네트웍상에서 주고받는 정보 혹은 컴퓨터에 저장된 정보를 보호하는 암호화시스템에서 중심적으로 고려하는 내용은 다음과 같다.

첫째, 비밀보장(Confidentiality) 기능이다. 정보를 보호하는데 있어 비밀을 보장하는 것은 가장 기본이 되는 사항이다.

두 번째, 무결성(Integrity)의 보장 기능이다.

세 번째, 부인방지(Non-Repudiation) 기능이다.

암호화(Encryption)는 자료의 기밀성을 보장하는 방법을 말하는 것이다. 기밀을 보장하기 위한 암호화에는 대칭형 방식(비밀키 암호화)과 비대칭형 방식(공개키 암호화) 등 두가지로 나누어 볼 수 있다.

대칭형 암호화 방식은 자료를 암호화하는 키와 암호화된 자료를 복호화 시키는 키가 동일한 방식이다. 암호화의 또 다른 방법은 비대칭 암호화 방식이다. 일반적으로 암호화 정보를 네트웍상의 상대편에게 보낼 때는 암호키까지 보내게 된다. 이러한 경우 이 암호키를 보호할 방법이 없게 되는데, 이러한 문제를 해결하기 위해 개발된 기술이 비대칭 암호화 방식이다.

본 연구에서 제시한 시스템은 비대칭 암호화 방식이다. 즉, 공개키 암호화 방식은 정보의 철저한 보호가 가능하지만 알고리즘이 복잡해 처리시간이 많이 걸린다는 단점을 가지고 있다.

3.3 인증 및 전자서명

중간에 데이터가 변조되는 것을 막는 보안 기능이 바로 메시지 인증기능이다. 메시지 인증기능은 메시지를 송수신하는 A가 B외에 제 3자인 C가 메시지 내용을 수정하지 못하게 하는 것에 초점을 맞추고 있다. 메시지 인증기능을 토해 메시지가 수정되지 않았는지, 메시지의 순서가 바뀌었는지에 대한 확인을 할 수 있다.

인증의 방식에는 퍼블릭 키를 이용해 메시지를 암호화하는 방법과 암호화 체크섬 이용, 해쉬함수 이용 등이 있다.

본 시스템은 암호의 체크 섬을 이용하는 방법은 MAC(Message Authentication Code)를 구해 사용한다.

메시지를 주고받는 A ,B가 동일한 키를 가지고 있다면 A는 메시지의 체크섬, 즉 MAC를 구한 후 그 내용을 암호화해서 메시지에 붙여 보내면 B는 그 값을 해독해서 메시지의 체크섬을 새로이 계산해 보고 동일하면 메시지의 변경이 없었음을 증명하는 방법이다.

3.3 전자상거래 보안

전자상거래라고 하는 것은 실재 생활에서 나타나고 있는 모든 거래, 즉 쇼핑, 금융거래, 기업간거래, 보험, 법률 등이 모든 것을 컴퓨터 네트웍 상에서 시뮬레이션을 통해 거래가 가능하도록 하는 것을 말하는 것이다.

전자상거래에서 보안이란 실제 거래를 통해 돈이 오고 간다는 점에서 그 중요성을 찾을 수 있다. 실제로 제품을 구입하고 그 대가를 지불하기 위해서 현재는 신용카드를 이용하는 경우가 가장 많은데 신용카드 번호가 외부 망에 개방돼 버리기 때문에 보안에 취약성을 가질 수 있다. 또한 신용카드 번호를 접수하게 되는 제품 판매자의 불순한 의도에 의해 개인의 정보가 나쁘게 이용될 수도 있다.

본 연구에서 제시한 농산물 전자상거래 사이트는 개인의 손익과 직결되는 사항들로 이루어져 있기 때문에 보안과는 별개로 생각할 수 없는 분야이다. 바꾸어 말하면 전자상거래에 관련한 특별한 보안 조치가 있는 것이 아니라 전자상거래 시스템 자체가 보안 기능을 수행해야만 하는 것이다. 다양한 유형들을 가지고 있지만 실제 인터넷상의 비즈니스나 전자상거래가 활성화되기 위해서는 선결돼야 하는 여러 가지 문제들이 있다. 네트웍 접속, 소프트웨어, 하드웨어 플랫폼, 물품의 배달, 멀티미디어 정보, 지불방식, 법률적 제약 등이 그 문제들로 이것들의 해결을 통해 인터넷상의 거래가 실제 활성화될 수 있을 것이다.

제시한 전자상거래 사이트 보안에서 특징적인 부분이라 하면 거래를 하면서 돈을 지불해야 하는 관계로 지불 방법에 대한 프로그램들 자체가 보안에 대한 기능을 수행하게 된다. 즉, 지불 방법에 따라 거래의 안정성을 보장하게 되는 것이다.

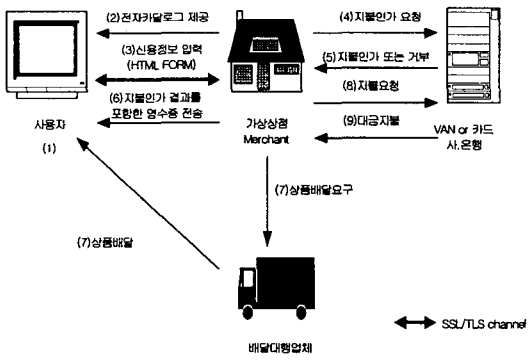
3.4 전자지불

전자지불 방법은 크게 두가지로 나누어질 수 있다. 그 하나가 지불 브로커 시스템이고, 또 다른 하나는 전자화폐를 이용하는 것이다. 지불 브로커 시스템은 우리가 일반적으로 알고 있는 방법으로 신용카드나 은행의 계좌번호를 이용해 네트웍 상에서 대금을 지불하는 방법을 말한다. 이런 시스템은 신용카드를 이용하는 거래에 익숙해져 있고, 사용이 편리하기 때문에 현실적으로 구현 가능한 전자지불 시스템이다.

그러나 이와 같은 시스템은 신용카드의 수수료가 비싸거나 사용자들의 개인정보나 거래정보 등의 자료가 쉽게 노출될 수 있기 때문에 비밀보장이 되지 않는다는 단점이 있다. 이러한 단점 때문에 전자상거래에서 이 방식은 일시적으로 사용될 가능성이 높다고 할 수 있다.

전자화폐의 경우는 아직 실용화되기에 이른 감이 있지만 이론적으로 또는 실험적으로 많이 연구되고 있다. 전자화폐를 이용하는 것은 신용카드를 이용해 발생할 수 있는 단점들을 개선할 목적으로 만들어진 것이다. 그렇기 때문에 전자상거래에서 보안의 또 다른 방법이 전자화폐의 사용이다. 대표적인 전자화폐 지불 시스템으로는 사이버캐쉬, E캐쉬, 퍼스트 버추얼 인터넷 지불 시스템, 스마트월넷과 시큐어 페이 등이 있다.

전자화폐의 장점은 사용자 측면에서 현금과 같은 익명성을 보장받을 수 있다는 것이다. 즉, 상점에서 물건을 살 때 구매자가 누구인지가 알려지지 않는 것이다. 또한 사용자와 인가된 상점간의 거래뿐만 아니라 사용자간 화폐의 이동도 가능하다.



위의 그림은 SSL/ TLS를 이용한 쇼핑 시나리오이다.

본 연구에서는 위의 시스템도를 이용하여 농촌형 전자상거래에 맞게 변형을 하고자 한다. 위의 그림에서 가상상점은 웹사이트상의 전자상거래로 구현을 수행하고 배달 대행업체는 기존의 농협 판매망을 활용하며 지불 결제 은행은 농협 내에 사이버 머니를 구축하여 사용하고자 한다.

4. 결론

국내 전자상거래 사이트 상의 정보보호 및 관리 기술 분야는 많은 발전을 가져오고 있다. 정보 보안 프로토콜, 지불 프로토콜, 전자화폐 시스템 등 여러 분야에 걸쳐 연구되어지고 있다. 그런데 대다수의 전자상거래 사이트들은 유통망이 정형화되어 있는 상품 및 정찰된 가격에 대하여 이용되어지고 있는 것이 현실이다. 또한 여러 단계의 유통단계를 거쳐야 하는 품목들에는 아직 미흡하다. 이에 본 연구에서는 유통망이 복잡한 농산물 거래를 전자상거래 사이트 구축을 통한 정보보안 및 관리 방안에 대하여 연구하고 있다. 본 시스템에서는 비대칭적 암호화 기법 및 SET을 이용한 암호화 거래 방법을 제시하였으며, 호스트의 비대칭적인 스위칭 시스템으로 사용자가 웹 사이트에 접속시에는 데이터 서버는 닫혀있는 상태이고 비동기적으로 사용자가 웹 사이트에서 인증을 득한 후에 데이터 서버로 접속이 가능하며 데이터의 액세스가 끝난 후에는 웹 사이트의 접속을 재개 시키고 데이터 서버의 액세스는 무효화시킴으로써 서버의 데이터 보안 및 관리를 효율적으로 수행한다. 이 시스템은 한가지 단점을 가지고 있다. 실시간 접속이 부자연스럽고 사용자의 대기 시간이 부여되므로 처리 시간이 다소 지연되어진다 .이 문제를 해결하는 것이 향후 연구 과제이다.

[참고문헌]

[1] 김병천 "암호기술 및 전자상거래보안", 한국정보보호센터 기술개발부 기반기술팀, 1999년 2

[2] Paul Timmers, " Business Models for Electronic Markets", Electronic Market, Vol.8, No2, April 1998.

[3] Ravi Kalkota, Andrew B. Whinston, readings in Electronic Commerce, Addison-Wesley Publishing Company, 1997.

[4] 개방형 통신망 환경에서의 인증 및 접근 통제 기술, 한국정보보호센터 기술본부 기술응용팀, 1998년 4.

[5] 인터넷 전자상거래의 물결-뉴글로벌시장, 한국 전자통신 연구원 1998.6

[6] 전자상거래를 위한 보안 기술 체계 및 요소 기술에 대한 이해 한국 전산원 1999.6

[7] 김기병, 김수홍, "전자상거래를 위한 지불방법" 한국정보처리학회지, Vol. 6, No.1, January. 1999.