□특집□

전자상거래를 위한 지불방법

김 기 병† 김 수 홍††

◈ 목 차 ◈

1. 서 론
2. 전자 지불의 분류
3. 전자 지불을 위한 보안 기법
4. SET에 기반한 전자상거래 절차
5. 결 론

1. 서 론

인류는 물물교환과 같은 비효율적인 상거래로부터 가치의 추상적인 표현 즉 화폐를 발명함으로써, 보다 효율적이고 편리한 거래가 가능한 세상을 열었으며, 현대에 와서는 다양한 종류의 화폐 및 이를 대용할 수 있는 수단들이 많아져, 보다 다양한 상거래를 가능하도록 하고 있다[1].

화폐의 발전이 지불수단의 다양화를 가져온 반면 네트워크는 상거래의 때와 장소를 다양화 시키고 있다. 미국방성에서 메인 프레임 컴퓨터를 연동하기 위해 처음 구축된 ARPANET으로부터 태동한 인터넷은 90년대에 들어 World Wide Web (WWW) 및 멀티미디어 데이터를 지원하는 탐색기(browser)의 출현으로 다양한 서비스가 개발되고 있으며, 급속히 성장하고 있다. HTML을 기반으로 하는 WWW의 단순성과 이식성은 HTML을 통한 다양한 미디어의 지원을 가능하게 하여 인터넷 서비스제공자와 인터넷 사용자는 폭발적으로 증가하게 되었고, 수많은 어플리케이션들이 인터넷을 기반으로 하여 개발되거나 재개발 되어지고 있다.

이러한 방대한 사용자 층을 기반으로 인터넷을 기반으로 하는 가상의 쇼핑공간이 등장하게 되었고 전세계의 인터넷 사용자를 대상으로 실시간으로 물건을 거래할 수 있는 세계적 시장(global market)이 생겨났다 [2, 6].

상거래는 물건이나 서비스를 제공하고 이에 대한 대금의 지불이나, 결제를 통해 이루어진다. 실거래에서 대금의 결제수단으로 가장 많이 사용하는 것은 현금, 수표, 신용 카드 등이다. 현금이나 수표는 직접 주고 받아야 한다는 제약조건이 따르므로, 인터넷과 같은 가상 공간에서 대금의 결제 수단으로 가장 많이 사용되는 것은 신용 카드이다. 그러나 기존의 인터넷 상에서 신용카드를 이용한 거래는 개인의 정보를 완전하게 보호하지 못함에 따라 여러 가지 문제점들을 야기하였다. 이에 따라, 전자상거래에서의 지불 방법은 소비자(customer)와 상인(merchant), 그리고 중계자(bank, issuer)들이 상호 개입되어 거래를 진행할 때, 적절한 보안과 암호화가 유지되는 한편, 정보의 교환 및 고객의 신원을 확인할 수 있는 인증(authentication) 기능을 필요하다.

또한, 네트워크의 발전에 따라, 컴퓨터 네트워크를 통한 국제적 접속의 증가, 특히 상거래에 있어서의 컴퓨터 네트워크 활용의 급속한 증가에 의해 새로운 지불 수단에 대한 요구가 커지고 있

† 정 회 원 · 한국휴렛팩커드(주) 컨설팅시업부 선임연구원
†† 종신회원 : 상명대학교 전자계산학과 교수

으며, 새로운 지불 수단은 소비자와 상인이 동시에 만족할 수 있는 강력한 보안 및 개인 정보의 보호가 요구되고 있다.

국내에서는 전자상거래 및 지불의 기능 정의 및 구현을 위해 정보통신부, 국제전자상거래연구센터(ICEC), 정보보호센터, Korea Cyber Payment, Commerce Net Korea 등 여러 기관 및 업체에서 관련 표준 및 솔루션을 제공하여 가상공간 내에서 원활한 전자 상거래가 이루어질 수 있도록 노력하고 있다 [7].

한편, 금융계에서도 국내외적으로 급변하는 금융 환경과 보다 폭 넓은 서비스를 기대하는 고객의 요구, 외환 위기로부터 시작된 범국가적 경제 위기 및 금융 개방화 정책으로 다양한 금융 시장과 금융 서비스의 등장이 예고되고 있다. 이러한 흐름으로 인하여 국내의 금융회사들도 금융 환경을 기존의 단순 계정 처리, 통계 처리 및 활용 차원에서 정보의 효율적 관리 및 분석, 그리고 대고객 종합 서비스를 중심으로 하는 정보 집약적인 전자상거래 시스템의 시스템을 구축하여야 할 필요가 매우 커지고 있다. 이에 따라 80년대 후반부터 구성되어진 CD 공동망, BOK-WIRE(한국은행), ARS, 홈뱅킹, 폰뱅킹, EDI, 직불카드 및 신용카드 등의 컴퓨터 네트워크를 이용한 고객 서비스 업무는 더욱 다양하고 복잡해 질 것으로 보이며, 향후 가상의 쇼핑 공간에서 적절한 역할을 수행하기 위해서 외부 네트워크와 연동하기 위한 대외계의 구축 및 기존의 시스템과의 종합적인 관리 체계를 구축을 위한 노력을 기울이고 있다 [8].

2. 전자 지불의 분류

직접적인 상거래에서 가장 많이 사용되는 지불 수단은 현금, 수표, 신용 카드 등이 대표적이다. 전자상거래에서 사용되는 지불 방법은 그 형태에나 거래 방식에 따라 (그림 1)과 같이 분류할 수 있다 [1, 3].

1. 직접적인 상거래 방식에 기반한 분류
   - 1.1 전자 자금 이체
   - 1.2 디지털 현금
   - 1.3 전자 화폐

2. 자금의 흐름에 따른 분류
   - 2.1 현금방식 지불
   - 2.2 수표방식 지불

3. 거래 방식에 따른 분류
   - 3.1 직접 지불
   - 3.2 간접 지불

4. 처리 방식에 따른 분류
   - 4.1 Online 지불
   - 4.2 Offline 지불

5. 추적가능 여부에 따른 분류
   - 5.1 추적 가능 지불
   - 5.2 추적 불가능 지불

(그림 1) 지불 방법의 분류

전자상거래에서의 대금의 지불에는 현금의 발행자(issuer), 구매자, 상인, 및 취득자(acquirer)가 관여한다. 화폐는 발행자에 의해 발행되고, 이는 구매자의 필요에 의해 은행으로부터 인출이 된다. 인출된 화폐는 다시 상인에게 지불되고 지불된 현금은 상인이 은행(acquirer)에 입금함으로써 최종적으로 취득자에게 전달된다. 즉 실제 현금의 흐름은 현금의 발행자로부터 취득자(acquirer)로 전달되게 되나, 이의 지불은 구매자가 상인에게 지불하는 형태를 가진다.

이에 비해, 수표와 같은 신용 지불 수단은 구매자가 상인에게 현금을 직접 지불하는 대신, 지불을 요구하는 지불요구서(수표)을 제시하는 것으로서 지불을 대신하게 된다. 즉, 구매자는 발행자(issuer)로부터 현금을 인출하는 대신, 지불을 요구할 수 있는 인증서를 얻게 된다. 얻어진 인증서를

통해 구매자는 물건을 구매할 때, 상인에게 지불 요구서를 제시할 수 있게 된다. 상인은 이러한 지불요구서가 합당한지를 취득자(acquirer)에게 확인하고, 지불요구서가 합당할 경우, 지불이 정당한 것으로 인정하게 된다.

(그림 2)에서는 대표적인 전자 지불 시스템들을 보여주고 있다.

신용 카드 지불 시스템
- First Virtual, CyberCash, iKP, SET

전자 지갑
- Danmont, CLIP, Mondex,
- CEN Intersector electronic Purse,
- EMV electronic purse

전자 수표
- FSTC Electronic Check

전자 화폐
- E-cash, CAFÉ

(그림 2) 대표적인 전자지불 시스템

2.1 직접적인 상거래 방식에 기반한 분류

현재 인터넷을 기반으로 한 전자상거래 시스템에서 전자 거래를 위한 다양한 지불 방식들이 제시되고 있으며, 이중 직접적인 상거래 방식에 기반한 분류로는 전송형 지불 방식인 전자 대금 이체, 가치 저장형 지불 방식인 디지털 캐시, 지불 지시형 지불 방식인E-cash가 있다 [3].

2.1.1 전자 대금 이체

전자 대금 이체는 수표나 어음 거래의 전산화된 형태로도 볼 수 있는데, 미국의 경우 60년대부터 사용되어진 대금의 결제방법으로서 국내에서는 자동 이체라는 이름으로도 잘 알려져 있다. 자동이체 거래는 물품이나 서비스에 대한 구매자, 판매자 그리고 중개자(은행, 신용카드사, 금융결제원 등)의 3자간의 거래로 이루어진다. 이러한 거래를 위해서 먼저 구매자는 자동 이체 계약을 설정한다. 이에 따라 판매자는 고객에게 대금의 지불을 요구하게 되고, 다시 고객은 중개자로부터 증명을 얻는다. 이 증명을 이용하여 고객은 자신의 계좌로부터 지불해야 할 금액을 출금하고 이를 증명을 통해 판매자에게 전달한다. 판매자는 고객으로부터 받은 증명을 거래 은행에 제출하게 되고, 은행은 증명이 확인되면 증명과 함께 표시된 대금을 판매자의 계좌에 입금시켜준다.

이러한 전자 대금 결제는 오래된 전자 지불의 한 형태로서, 개념적으로는 수표나 어음을 통한 거래와 유사하나, 대금의 지불에 따른 수표와 같은 문서의 흐름이 전자 문서로 대체된 것으로 볼 수 있으며 그 처리 시간도 출금, 전송, 입금이 순간적으로 발생하므로 거래에 따른 대금의 이체의 지연이 없어진다.

이와 같은 전자 대금 이체 시스템의 장점으로는 거래에 따른 시간의 지연이 없어지므로, 대금의 결제에 따른 시간의 지체를 없앨 수 있으며, 문서화된 수표나 어음의 발행이 생략되므로 문서의 발행 및 처리에 따른 추가적인 비용을 줄일 수 있다. 또한 그 처리가 전산화되어 있으므로 기존의 ATM 시스템이나 POS단말기 등과도 쉽게 연동될 수 있다는 유연성을 들 수 있다. 그러나 이러한 전자 자금 이체 시스템은 지불에 은행과 같은 중개자가 개입하게 되며 이에 따른 자금의 흐름이 추적될 수 있으므로, 개인의 물품 구매 행위와 같은 개인적인 행동이 추적되어 사생활의 침해에 대한 우려가 존재한다. 즉 현금을 사용했을 때의 익명성이 보장되지 않는다 이에 따라 가상의 시장에서도 구매자의 사생활이 보호될 수 있도록 전자 상거래시스템에서 기존의 문서화된 화폐(지폐)와 같은 익명성을 보장할 수 있는 지불의 수단이 필요하다.

2.1.2 디지털 캐시

디지털 캐시는 문자 그대로 기존의 문서화된

화폐나 동전과 같은 지불 수단을 전자적으로 표현한 것으로서, 익명성과 유동성, 환금성이 반드시 보장되어야 하는 지불 수단이다. 디지털 캐시는 익명성을 보장하므로 디지털 캐시의 사용자가 어떤 물건을 구매하였는지, 또는 얼마를 지불하였는지에 대한 정보는 물건을 판매한 판매자만이 알 수 있다. 그리고 디지털 캐시에 의해 물건을 판매한 경우 어떤 물건이 누구에게 팔렸는지에 대한 기록이 디지털 캐시에 의해서는 기록될 수 없다. 또한, 디지털 캐시는 모든 판매자들에게 통용되어야 한다. 즉 진정한 의미의 디지털 캐시라면 인터넷 상의 상인이나 실제의 상점에서 광범위하게 통용되어야 한다.

이와 같은 디지털 캐시가 실현된다면 이로부터 우리는 여러 가지의 장점을 얻을 수 있게 된다. 현금은 그 익명성과 환금성으로 인해 도난의 소지가 높으며, 제작이나 유지에 많은 비용이 들게 되고, 현금의 이전이나 수송 시에도 많은 비용이 소요된다. 디지털 캐시는 그 형태가 전자적이므로 도난의 우려가 없다. 암호화된 전자 화폐는 위조의 우려가 매우 낮으며 이전이나 수송도 간편하게 행할 수 있다. 디지털 캐시는 현금과 동일하므로 익명성과 환금성이 보장되는 디지털 캐시의 발행은 현금의 발행과 같은 의미를 가질 수 있다.

디지털 캐시는 현재 매우 제한적인 형태로 여러 국가에서 사용되고 있는데 선불카드가 이의 대표적인 예가 될 수 있다. 그러나 선불 카드는 익명성은 보장되나 환금성이 약하며, 거래 금액이 작고, 제한적인 서비스에 대해서만 지불 능력이 있으며, 개인 간의 현금의 이전은 보장되지 않는다.

2.1.3 전자 화폐

인터넷 상의 전자상거래와 이를 이용한 가상의 시장에서 가장 관심을 끄는 지불 방법이 바로 전자 화폐이다. 전자 화폐는 현재 인터넷 상의 거래에 가장 많이 이용되고 있는 신용카드 거래의 문제점을 해결하고 구매자를 보호하기 위해 제시된 지불 방법이다. 인터넷 상에서 신용카드를 이용하여 지불을 할 경우, 신용카드에 관련된 정보가 인터넷 상으로 전송되게 되며, 이는 다시 상인에게 전달된다. 구매자의 신용카드 정보는 상인에게 노출되며 인터넷 상의 해커에 의해 악용될 소지를 가지고 있다. 이러한 인터넷의 보안과 프로토콜 상의 문제로 제안된 것이 전자 화폐이며, 대표적인 전자 화폐의 예는 (표 1)과 같다.

전자 화폐의 한 예로서 E-cash는 네덜란드의 DigiCash사에 의해 개발되었으며 1996년 미국의 Mark Twain은행에 의해 실험적 버전이 구현되었다. 이 시스템에 의하면 구매자와 판매자는 모두 은행에 계좌를 가지고 있어야 하며, 구매자는 반드시 은행에 전자 이체 신청을 해야 한다. 은행에는 전자화폐를 발행하는 Mint가 존재하여 고객은 언제든지 자신의 컴퓨터를 이용하여 자신의 계좌로부터 출금하여 전자 화폐를 자신의 컴퓨터에 저장할 수 있다. 이러한 전자 화폐는 적절하게 암호화되어 있으며, 구매자가 대금을 지불하고자 할 때, 원하는 금액만큼을 다시 암호화하여 상인에게 전달한다. 판매자는 받은 전자화폐로부터 다시 정보를 복원한 후, 자신의 컴퓨터에 이를 저장하거나 Mint에 보내 이를 판매자의 계좌에 입금할 수 있다. 이러한 E-cash는 은행에 의해 관리되지만, 비대칭적 암호화 알고리즘인 RSA암호화 기법을 사용하므로, E-cash의 흐름을 은행이 추적하거나 조사할 수 없으며, 개인 정보를 보호할 수 있다.

2.2 자금의 흐름에 따른 분류

2.2.1 현금방식 지불

자금의 흐름에 따른 지불 방식으로는 현금과 같이 화폐의 발행자로부터 구매자가 화폐를 취득하여, 이를 상인에게 직접 지불하는 현금 방식 지

(표 1) 주요 전자 화폐

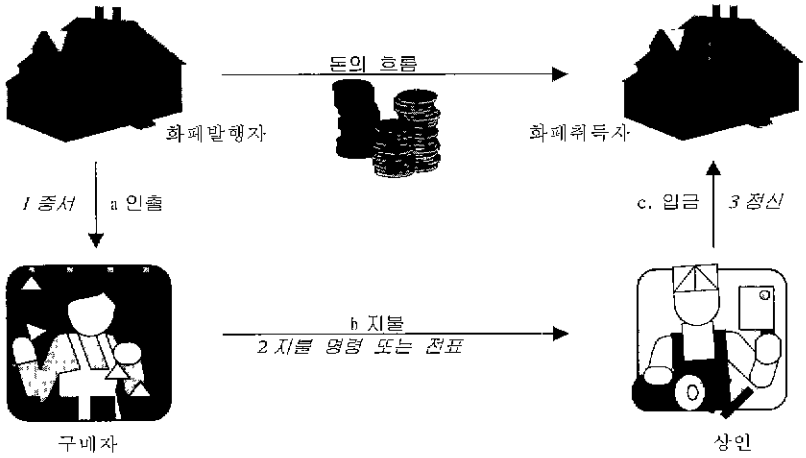
전자화폐	특 징	이 용 분 야
Mondex	-'95년 영국 Swindon 지역에서 시험운영 -전화기로 개인 대 개인 전자화폐 이체 (통화의 흐름관리가 안됨) -월렛으로 개인간 이체 -'96년 마스터카드사에 인수되어 전세계적인 계획 설립 중	-몬덱스 인터네셔널 설립 -영국전역,미국,홍콩,캐나다,호주 등으로 확대 중
Chip	-'96년 Europay사가 발표 -세계 최초의 범용 전자지갑 -EMV 규격을 만족 -유럽 전지역에서 사용할 수 있는 다중통화 방식 전자화폐(복수국가의 전자화폐거래 가능) -RSA 공개키 보안 알고리즘 이용-	-유럽의 여러 나라를 대상으로 발급기관 모집중 -EFT/POS 가맹점
Visa Cash	-'95년 호주에서 처음 시험 -'96년 애틀란타 올림픽에서 시험 운영 (재 충전 사용 불가) -'97년은 영국에서 계획 중	-'96년 11월에 미국 일부지역에서 사용 -EFT/POS 가맹점, 자판기
Ecash	-네덜란드 DishCash사가 미국의 Mark Twain 은행에서 시험 -인터넷 전자상거래 기술 적용 -Blue칩 및 알고리즘 사용 BLIND 서명 소프트웨어	인터넷 전자상거래 : 네트워크형
Proton	-'94년 벨기에 국영 금융기관인 Banksys가 추진 -Visa에 라이센스를 맺음 -'96년 브라질,호주,스위스에서 시험 운영 -'96년 American Express와 라이센스 맺음 -Bull사의 CC-60/100칩 사용- -5천 프랑 한도 내에서 재충전	-벨기에 일부지역 시범운영 -EFT/POS 가맹점, 공중전화, 버스, 지하철

불과, 구매자가 화폐를 직접 취득하지는 않고, 정해진 증서나 문서를 통해 거래를 성립하는 신용방식의 지불로 분류할 수 있다.

현금방식의 지불방식의 지불 방법의 대표적인 예로는 스마트카드를 이용한 전자지갑, 전자화폐 등을 들 수 있다.

2.2.2 신용방식 지불

신용방식의 지불은 구매자가 대금을 직접 지불하지 않고, 대신 지불을 대신할 수 있는 지불명령서를 제시함으로써 지불 행위를 하게 된다. 이의 대표적인 예로는 직불카드와 신용카드를 들 수 있다.



(그림 3) 전자 지불에서의 돈의 흐름과 거래

(그림 3)에서와 같이 화폐의 흐름은 화폐의 발행자로부터 화폐취득자로 흘러가게 된다. 국내의 경우, 화폐의 제공자와 화폐의 취득자는 모두 은행이며, 화폐 제공자 중, 특히 한국은행은 발행자의 성격을 가지는 곳이 된다.

현금 지불의 경우, 현금은 구매자를 통해 상인에게 전달되어, 최종적으로 다시 은행으로 돌아오게 되며(그림3에서 abc), 신용지불의 경우, 자금이 실제로 구매자나 상인에게 전달되지는 않고, 단지, 신용카드나 수표등과 같은 증서의 형태로 전달되어(그림3에서 1→2→3), 거래가 성립하게 된다 [1].

2.3 거래 방식에 따른 분류

지불 방법은 구매자와 상인간의 거래 형태에 따른 프로토콜 방식의 분류가 가능하다. 직접 지불 방식에서는 구매자와 상인간의 거래를 위해 쌍방간의 직접적인 정보의 교환이 일어난다. 이에 비해 간접 지불 방식에서는 거래의 당사자가 지불을 위한 직접적인 정보의 교환이나, 거래 행위를 하지 않는 경우를 말한다. 물건을 사거나 팔 때 행하는 지불은 직접 지불의 형태에 속하며, 지불하는 쪽에서 일방적으로 지불을 수행할 수 있는 현금 이체와 같은 형태의 거래가 간접 지불에 해당한다.

2.4 처리 방식에 따른 분류

지불과 관련한 일련의 처리들이 일어나는 방식의 차이에 따라 전자상거래에서의 지불을 online 지불과 offline 지불로 분류할 수 있다.

2.4.1 Online 지불

Online 지불에는 지불과 관련된 거래의 승인을 위한 인증 서버가 개입된다. 이때 인증서버가 거래에 online으로 개입되므로 이를 online 지불이라고 한다. Online 지불의 경우, 지불과 관련된 거래가 인증서버에 의해 승인되므로 매우 안전한 방식의 지불방법이 된다. 그러므로 online 지불 방법의 경우, internet 상거래 등과 같이 인증서버와의 통신을 보장할 수 있는 경우에는 거래에 쉽게 적용할 수 있으나, 개인이 휴대하고 사용하는 전자지갑과 같은 경우에는 online 지불이 어렵다.

2.4.2 Offline 지불

Offline 지불은 거래 시 상인과 구매자간의 정보 교환만으로 지불이 이루어진다. 즉 인증서버에

의한 인증절차 등이 생략된다. 이에 따라 offline 지불은 구매자의 지불이 정당한가에 대한 검증이 유보되어, 거래 후, 확인하여야 한다. Offline 지불의 대표적인 예로는 Mondex를 들 수 있다.

2.5 추적 가능 여부에 따른 분류

2.5.1 추적 가능 지불

추적가능 지불 방법이란 거래에 따른 지불의 내용이 보존되어, 거래 이후에 누가 얼마만큼의 돈을 누구에게 주었는지에 대한 내용을 추적할 수 있는 지불 방법을 말한다. 상거래에서 수표나 신용카드에 의한 지불이 여기에 해당되며, 전자상거래에서는 신용카드 지불 방법에 기반한 대부분의 지불방법이 여기에 해당한다. 이의 예로는 CyberCash, SET, FirstVirtual등이 있다.

2.5.2 추적 불가능 지불

추적가능 지불에 비해 추적 불가능 지불은 현금지불 방법을 전자 상거래상에 구현한 것이다. 추적 불가능 지불의 경우에는 현금과 마찬가지로 전자 상거래에 의한 거래 이후에도 지불에 따른 거래 정보가 남지 않으므로, 거래 당사자들은 익명성을 보장받게 된다. 이의 대표적인 예로는 NetCash, E-cash, CAFE 등이 있다.

3. 전자 지불을 위한 보안 기법

전자상거래에서의 보안은 그 거래가 디지털화된 정보로 이루어지므로 매우 중요하다. 디지털화된 정보는 그 도용이나 복제가 비교적 간편하고 쉽기 때문이다. 보안의 정도는 거래에 따라 다양한 요구가 발생할 수 있으나, 보편적으로 전자상거래에서의 전자지불은 무결성, 인증, 보안성, 가용성 및 신뢰성이 지켜져야 한다 [1].

무결성이란 전자지불에 관여하는 화폐는 반드시 발행자로부터 획득되어져, 취득자에 돌아올 때까지, 원래 발행된 화폐 이외에는 새로이 생겨나거나 없어지지 않고 유지되어야 한다는 것을 의미한다. 화폐를 이용하여 거래를 할 때에는 상거래의 주체나 당사자 및 지불에 사용되는 화폐가 정당함을 증명하여야 하는데, 이를 인증이라고 한다. 이러한 거래의 당사자는 거래의 내용이 공개되는 것을 꺼려 하는데, 예를 들어 신용카드 거래에서의 신용카드 정보가 이러한 정보의 대표적인 예이다. 이런 경우, 거래에 관련된 정보는 보안이 유지되어야 한다. 이에 따라 전자상거래에도 익명성이나 추적불가를 보장할 수 있어야 한다. 전자지불은 항상 지불이 필요할 때, 지불 수단으로 사용할 수 있어야 하며, 전자 지불의 수단을 손상하였거나, 분실 하였을 때에도 이를 회복할 수 있는 적절한 방법이 제공되어야 한다. 즉 전자 지불 수단은 가용성과 신뢰성을 제공하여야 한다.

전자지불에 요구되어지는 보안의 요구사항은 주로 암호화를 통해 구현된다. 전자상거래에서 사용되는 암호화 방법에는 비암호화 시스템, 패스워드 시스템, 공유키 방식의 암호화(대칭적 암호화) 및 공개키 방식의 암호화(비대칭적 암호화)가 있다.

비 암호화 시스템은 암호화하지 않은 정보를 교환하는 것으로 실제 시스템에서는 거의 사용되지 않는다. 패스워드 시스템의 경우도 정보 접근을 위해 패스워드를 통한 인증을 제공하는 것으로서 거래 내용을 암호화하는 보안 시스템과 연계하여 사용되어진다. 데이터를 암호화하는 방식으로는 암호화와 복호화에 동일 키를 사용하는 공유키 방식의 암호화와 서로 다른 키를 사용하는 공개키 방식의 암호화가 대표적으로 사용된다.

전자상거래 시스템의 무결성, 보안성, 신뢰성 등을 해치는 공격의 예로는 시스템에 대한 공격, 데이터 공격, 비즈니스에 대한 공격 등이 있다 [5]. 시스템에 대한 공격이나 데이터에 대한 공격

을 막기위한 요소로서 시스템에 대한 방화벽, 디렉토리에 대한 Kerberos 시스템 및 특정 어플리케이션에 대한 접근을 제한할 수 있는 ACL(Access Control List)등이 사용되며, 외부의 네트워크로부터의 시스템에 대한 공격을 차단하기 위해서는 보안 방화벽이 사용된다.

비즈니스 측면에서도 보안은 매우 중요하다. 전자 상거래를 통한 거래를 행할 때, 서로 주고받는 정보는 대금의 지불이나 결제와 관련된 것들이므로, 외부의 공격에 의해 잘못된 정보의 전달이나, 대금 결제와 관련된 정보의 유출은 곧바로 현금의 도난이나 유용과 연결된다. 인터넷에서 널리 사용되는 대금의 결제 방식인 신용 카드는 고객 정보의 유출로 인하여 심각한 문제를 야기할 수 있다. 인터넷은 익명의 사용자가 공유하는 네트워크 공간으로서 네트워크를 통한 다양한 형태의 정보에 대한 침해가 예상된다. 이를 방지하기 위해 전자 상거래에서의 보안 시스템은 필수적이다. 특히 전자 상거래에서의 거래는 사람이 직접 만나지 않고 컴퓨터와 네트워크만을 이용하여 거래를 하는 방식이므로 네트워크상에서의 정보의 보호 뿐만 아니라 거래 상대방을 확인할 수 있는 확인 절차와 더불어 암호화가 필요하게 된다. 즉 전자상거래 시스템에서의 암호화 기술은 개인 정보의 보호와 거래 당사자들의 인증 기능을 동시에 제공하게 된다. 이에 따라 전자상거래를 위한 보안 기술은 인증을 위한 부분과 암호화 부분으로 나뉘어 연구되고 있다.

보안을 위한 암호화 기술은 암호화 방법과 이를 다시 풀어내는 복호화 방법에 사용되는 키의 적용 방식에 따라 대칭적 암호화 알고리즘과 비대칭적 암호화 알고리즘으로 분류한다. 대칭적 암호화 방식에서는 암호화에 사용하는 키와 복호화에 사용하는 키가 동일하며, 비대칭적 암호화 방식에서는 이 두 가지 키가 다르다. 비대칭적 암호 방식에서는 보통 이중 한가지 키를 공개하고 한 가지 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.

보안 기법을 지원하는 전자 지불을 위한 대표적인 절차로는 신용카드 지불을 지원하는 MasterCard 및 VISA에서 제안하고 구현한 SET이 있다.

3.1 DES 암호화 방식

DES 암호화 방식은 대표적인 대칭적 알고리즘으로서 정보의 암호화와 해독에 64bits(56bits의 키 + 8bits의 패리티)의 동일한 키를 사용한다. 정보를 교환하는 양측이 암호화에 사용된 키를 상대방에게 건네주는 방식이다. 그런데 거래의 상대방이 불특정 다수일 경우에는 방대한 고객의 수만큼 키를 만들어 나누어주어야 하고 이를 각각의 고객과 연관하여 유지하여야 하는데 이는 실제적으로 매우 비효율적이다. 또한 공개키 방식을 이용한 암호화 문장은 상당히 쉽게 해독될 수 있음이 입증되었으며, 이에 따라 공개키 방식이 제안되었다 [3].

3.2 RSA 암호화 방식

RSA 암호화 방식은 제안자의 이름을 따서 RSA(Rivest, Shamir, Adoleman)라는 이름이 붙여졌다. RSA 알고리즘에서는 개인이 보관하는 개인키와 공개해 놓는 공개키의 두개의 키를 이용하며, 공개키로 암호화한 문장은 공개키에 대응하는 개인키를 이용하여 해독할 수 있으며, 반대로 개인키로 암호화할 경우, 대응되는 공개키를 이용하여야만 원문을 재생해낼 수 있다.

3.3 전자 서명과 디지털 증명

전송하고자 하는 메시지를 암호화했다고 해서 메시지의 무결성이 보장되는 것은 아니다. 즉 전자상거래를 이용한 거래에서는 모든 정보가 전자문서의 흐름에 의해 처리되기 때문에 거래 당사자들이 거래에 참여했다는 것을 기술적으로, 또는 법적으로 보장할 수 있어야 한다. 전자 서명은 메시지가 전달 또는 수정되지 않았음을 보장하는 프로토콜로서 메시지 인증과 암호화기술로 구성된다.

전자 서명은 구매자가 거래 내역을 자신의 개인키로 암호화하여 판매자에게 전송하며, 판매자는 구매자의 공개키로 메시지를 해독하여 정상적인 메시지일 경우에만 거래를 진행한다. 이때 구매자의 공개키는 공개된 정보이므로 누구나 이 메시지를 해독할 수 있다. 이를 막기 위해 구매자가 전송하기 전 자신의 개인키로 암호화한 메시지를 다시 판매자의 공개키로 암호화하여 지정된 상대방만이 최종적으로 자신의 메시지를 해독할 수 있도록 함과 동시에 거래의 주체가 누구인지를 입증하는 기능을 동시에 수행하게 된다.

네트워크 상에서 거래를 하는 각각의 개체가 실제 누구인지를 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.

대칭적, 비대칭적 암호화 방법을 네트워크 상의 socket 계층에 적용한 보안 방법으로 Netscape 등의 WWW 검색기에서 사용하고 있는 SSL (Secured Socket Layer)가 있다 [4].

3.4 SET(Secured Electronic Transaction)

1996년 2월 전세계적으로 가장 큰 신용카드 회사들인 VISA International과 Master 카드사는 인터넷 상에서 신용카드를 이용하여 대금의 지불을 함에 있어 개인의 정보와 재산을 보호해줄 수 있는 안전한 방법을 찾기 위해 공동으로 연구를 시작하였고, 97년 5월 SET 1.0을 발표하였다. SET 프로토콜은 대칭적 암호화 방법인 DES와 비대칭적 암호화 방식인 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, 카드 및 카드 사용자에 대한 인증, 판매자에 대한 인증 및 각 구성 요소들 간의 상호 운용성을 보장해주는 거래 프로토콜이다.

SET을 이용한 데이터의 암호화 및 전송 방식은 다음과 같다.

1. 구매자는 전송메시지를 자신의 개인 키를 이용하여 RSA 방식으로 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.

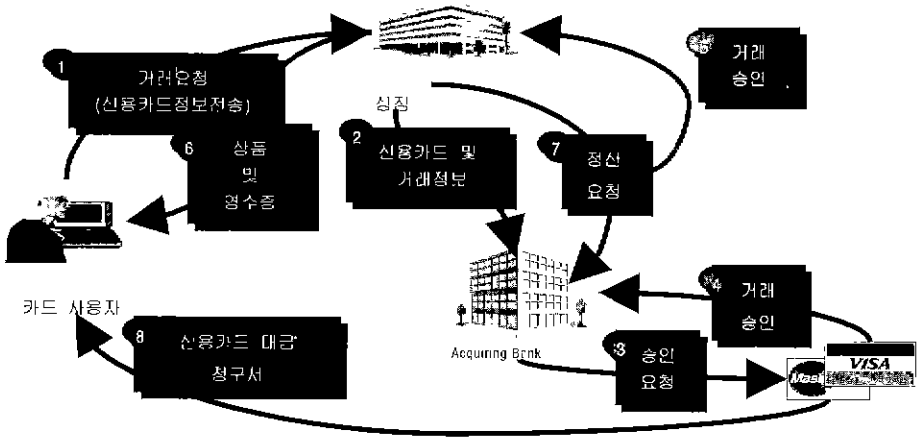
이 메시지를 수신한 판매자는

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 복호화하면 원문을 얻을 수 있다.

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

4. SET에 기반한 전자상거래 절차

전자상거래를 위한 시스템을 구축하기 위해서는 소비자, 상인 및 중계인(은행 또는 카드사등)의 구성요소가 갖추어져야 한다. 현재 Visa와 Master 카드사에 의해 제안되어 신용카드 거래에 의한 전자상거래에서 사실상의 표준(de facto standard)처럼 받아들이고 있는 SET을 기반으로 한 거래의 예는 (그림 4)과 같다.



(그림 4) SET의 거래 절차

SET을 이용한 전자 거래 시스템은 SET의 세가지 구성 요소인 상인, 구매자, 중개인에 해당하는 응용 프로그램을 제공한다. 예를 들어 SET에 기반한 전자상거래 시스템인 VeriFone 시스템의 경우, SET의 세가지 구성요소에 대해 구성 요소인 상인 측에는 거래를 수행하고 구매자로부터 대금을 받기 위한 응용 프로그램으로 vPOS, 구매자 측에는 전자 화폐를 저장하거나 지불에 사용할 수 있는 전자 지갑 형태의 vWallet, 중개자 측에는 대금의 결제나 이체를 지원하는 vGate를 제공하여, 이를 통하여 물품의 구매, 거래 및 대금의 지불, 회수를 가능하게 한다.

5. 결 론

본 조사연구에서는 전자상거래에서의 지불 방법을 그 거래 유형이나 화폐의 흐름에 따라 (표 1)과 같이 5가지로 분류해보았다. 또한, 전자 상거래에서 사용되는 거래 당사자와 거래 정보의 보안을 위한 방법에 대해 살펴보았다. 전자상거래 시스템의 보안은 비즈니스 측면에서 매우 중요하다. 이를 보장하기 위해 non-SET 기반으로 대칭적 암호화 기법, 비대칭적 암호화 기법 및 SET을 이용한 암호화 거래 방법을 살펴보았다. 전자상거래 시스템의 구성 요소는 구매자, 판매자 및 중개인역할을 하는 화폐발행자, 화폐취득자로 이루어진다.

전자상거래의 지불 방법이나 보안에 관한 요소는 다른 학문적인 요소와는 달리 그 실용적인 성격과 파급 효과로 인하여 세계 각국의 정부 기관이나 연구소에서 주도권 쟁탈을 위한 노력을 기울이고 있다. 이러한 전자상거래의 기법들은 전자상거래의 기술을 연구하고 제시하는 쪽 보다는 현실적인 필요성에 의해 금융기관이나 전자상거

레 서비스를 제공하는 업체들에 의해 주도적으로 개발되는 경우가 많다. 컴퓨터와 네트워크의 급속한 발전 속도와 영역의 확장은 앞으로의 전자상거래가 국가나 사회에 어떤 영향을 미칠지를 예측하기 어렵게 한다. 다시 말하면 앞으로 전자상거래가 사회, 경제적 또는 외교적으로 미칠 영향은 매우 크리라 예상된다. 이러한 전자상거래 분야에서 선도적인 입장을 유지하기 위해서는 이와 관련된 정부부처, 연구소, 각급 기관 및 업체들이 서로 협력하고 조율하여 국제적인 표준과 보조를 맞추고, 국내 기술과의 접목을 가능하도록 하는 협조와 지원에 필요하리라고 본다. 또한 전자상거래 관련 지불 기술과 보안 기술의 원천적 확보는 국내 전자상거래 시장에서의 국가 경쟁력 확보 및 차세대 거래 수단으로서의 전자상거래 시장에서 기회를 확보할 수 있는 초석이 될 것이며, 전자상거래 시장은 국내가 아닌 전세계적 시장이라는 인식하에 국제 표준화 등에도 주도적으로 참여하여 글로벌화 되는 전자상거래 시장에서 확고한 위치를 가질 수 있도록 노력해야 할 것이다.

참고문헌

[1] N. Asokan, Phillipe A. Janson, Michael Steiner, Michael Waidner, "The state of the art in electronic payment systems, IEEE Computer, Sep. 1997.

[2] Nabil Adam, Yelena Yesha, et al. "Strategic Directions in Electronic Commerce and Digital Libraries: Towards a Digital Agora, ACM Computing Survey, Vol. 28, No. 4, Dec. 1996.

[3] Patiwat Panurach, "Money in Electronic Commerce: Digital Cash, Electronic Fund Transfer, and Ecash, Communication of ACM, Vol. 39, No. 6, Jun. 1996.

[4] 권도균, 전자상거래를 위한 보안기술과 전자지불, 기술문서, 1997. (http://www.initech.com)

[5] 임신영, 권도균, 전자상거래 보안, 정보과학회지, 제15권, 제4호, 1997년 4월.

[6] Ravi Kalakota, Andrew B. Whinston, Readings in Electronic Commerce, Addison-Wesley Publishing Company, 1997.

[7] 백은경, 전자대금 결제를 위한 보안기술 현황, 정보통신연구, 제11권, 제2호, 1997년 6월.

[8] Bernard S. Hirsch, Reflections on a System Integration Project for Internet Banking, Technical Report, Hewlett Packard Company, 1997. (http://home.sprynet.com)

김 기 병

1990년 서울대학교 계산통계학과 (이학사)
1992년 서울대학교 계산통계학과 전산과학전공 (이학석사)
1994년 서울대학교 컴퓨터공학과 박사과정 수료
1994년 일본 통산성 정보기술총합연구소(ETL) 방문연구원
1994년-1997년 서울대학교 컴퓨터공학과 연구전문요원
1996년 독일 국립정보연구소(GMD) 방문연구원
1997년-현재 한국 휴렛팩커드㈜ 선임연구원
관심분야 : 데이터베이스, 멀티미디어 데이터베이스, 전자상거래, 디지털 비디오 처리

김 수 홍

1974년 서울대학교 공과대학 응용수학과 (공학사)
1983년 동국대학교 경영대학원 경영학과 정보처리전공 (경영학석사)
1990년 서울대학교 대학원 계산통계학과 전산과학전공 (이학석사)
1992년 서울대학교 대학원 전산과학과 (이학박사)
1992년-현재 상명대학교 산업대학 전자계산학과 부교수
관심분야 : 병렬처리시스템, 프로그래밍언어, S/W 공학, 물류자동화, EC/CALS 등