PGP를 이용한 WWW 기반에서의 전자지불 프로토콜 설계 및 구현

박 현동*, 강 신각**, 박 성열**, 류 재철*
* 충남대학교 컴퓨터 과학과
** 한국전자통신연구소 정보기술개발단

Design and Implementation of WWW-based Electronic Payment Protocol using PGP

Hyun-Dong Park*, Shin-Gak Kang**, Sung-Yul Park**, Jae-Cheol Ryou*
* Departement of Computer Science, Chungnam National Univ.
** Information Technology Division, ETRI

요 약

WWW(World Wide Web)은 미래의 쇼핑수단으로 자리를 잡아가고 있다. 하지만, 현재 사용하고 있는 지불형태는 구매자의 신용카드 정보가 평문으로 네트워크를 통해 전송되는 것과 같은 보안상의 문제점을 가지고 있다. 이러한 문제점들은 개인정보에 대한 침해 뿐만 아니라 경제범죄 등의 사회적 문제를 야기할 수 있다. 이러한 문제점을 해결하기 위하여 본 논문에서는 신용카드를 사용하는 새로운 전자지불 프로토콜인 SCCP(Secure Credit Card Payment)를 소개한다. SCCP의 적합성을 확인하기 위하여 IBM에서 제시한 기준에 따라 수행한 결과, 본 논문에서 제시하는 방법은 안전한 전자지불 프로토콜로 판단된다.

1 서 론

미국 국방성에서 개발한 TCP/IP 프로토콜을 기반으로 한 인터넷은 현재 수백만 대의 컴퓨터가 연결되어 있는 거대한 네트워크로 발전하였으며, 이러한 규모는 93년 이후부터 매년 2배씩 증가하는 추세이다. 이러한 증가를 발생시킨 이유 중에는 인터넷에서 제공해 주는 여러가지 서비스들의 역할이 크지만 그 중에서도 WWW의 역할이 가장 주도적이라 할 수 있다. WWW은 1990년 Berners-Lee에 의해 처음으로 제안되었으나 제안 초기에는 많은 관심을 받지 못하다가 Mosaic과 Netscape 등 브라우저(Browser)의 출현으로 인하여 널리 퍼져 나가기 시작하였다. 인터넷은 초기에는 전문가들이 주로 교육, 연구용으로 사용하였고, 그 결과로 인터넷에는 수많은 정보들이 저장되게 되었다. 이러한 정보를 이용하고자 사람들이 인터넷에 모이게 되었고, 이제는 WWW을 도구로 삼아 인터넷을 상업적으로 사용하려는 단계로 접어들고 있다[1].

WWW은 FTP(File Transfer Protocol), Telnet, Archie 등 기존의 인터넷 서비스와는 구별되는 편리한 사용자 인터페이스를 제공해 주고, 다양한 형태의 자료를 처리해 줄 수 있기 때문에 상업적 사용이 유리하다. 상점을 운영하는 입장에서 보면 WWW은 매우 매력적인 상점 운영 방식이다. 실세계에서 상점을 운영할

때에 필수적인 상점 건물 등이 필요하지 않고, 네트워크 기능을 갖춘 서버 컴퓨터만 있으면 상점을 개장할 수 있다. 또한 구매자의 입장에서도 쇼핑의 시간적 제약이나, 공간적 제약이 없다는 점에서 사용이 늘어날 것으로 보이고 있다. 이미 인터넷에는 많은 수의 상점이 개장되어 운영 중에 있다. 이러한 이유들로 인해 앞으로 인터넷의 가상 상점의 수는 그 수가 기하급수적으로 늘어날 것이라는 예측을 하고 있다.

하지만, 현재 운영 중에 있는 대부분의 가상 상점들이 전자화폐보다는 사용에 있어 편리하고 구현이 용이한 신용카드를 이용하여 지불을 처리하고 있는 데, 신용카드의 번호, 비밀번호 등과 같이 비밀리에 처리되어야 할 정보들이 평문으로 네트워크를 통해 전송되고 있다. Yahoo 디렉토리에 등록되어 있는 약 300 여 개의 가상상점들을 표본으로 조사한 통계의 결과를 보면 <표 1>과 같다.

<표 1> 인터넷 상점의 운영 형태

운 영 형 태	비 율
제품의 광고만을 인터넷을 사용하고 주문과 대금지불은 구입자가 직접 상점에 가는 하는 방법	16%
광고와 주문은 인터넷을 사용하고 대금지불은 구입자가 상점에 직접 가서 하는 방법	10%
광고, 주문, 지불이 모두 인터넷을 사용. 회원ID를 얻기 위해 신용카드 정보를 전송하고 대금지불 때에는 발급 받은 회원ID를 전송하는 형태	16%
광고, 주문, 지불이 모두 인터넷을 사용. 대금지불 때마다 신용카드 정보를 전송하는 형태	58%

<표 1>에서 보면 대금지불을 처리해 주기 위해 인터넷을 사용하는 상점은 전체 상점들 중에서 74%를 차지하고 있다. 그리고, 이 74%중에서 약 절반 이상이 안전하지 않은 방법으로 소비자의 신용카드 정보를 전송받고 있다. 보안을 고려하지 않았을 경우에 발생할 수 있는 문제점을 살펴 보면 첫째, 개인의 신용카드 번호와 같은 비밀 정보가 노출될 수 있다. 이는 개인정보의 노출에서 그치지 않고 이를 이용한 경제범죄 행위를 유발시킬 수 있다. 둘째, 구매자가 구매 사실을 부인하거나, 상점이 대금을 받지 못했다고 주장할 경우의 대비책이 전무하다. 셋째, 개인의 구매 정보가 노출됨으로 인해서 프라이버시 보장이 어렵다. 넷째, 불법적인 구매자 및 쇼핑 서버의 난립을 방지하기 어렵다.

본 논문에서는 이러한 WWW에서의 전자지불 처리에 예상되는 문제점들을 해결하기 위해 신용카드를 이용하는 새로운 전자지불 프로토콜인 SCCP을 제안한다. SCCP는 NCSA(National Center for Supercomputing Applications)에서 설계한 WWW 암호통신 프로토콜인 PGP-CCI(Common Client Interface)를 기반으로 구현되었다. 본 논문의 2장에서는 현재까지 이루어진 전자지불 프로토콜 들을 살펴 보고, 3장에서는 본 논문에서 제안하는 SCCP 프로토콜을 설명한다. 마지막으로 4장에서 결론을 맺기로 한다.

2 기존의 연구

WWW에서의 전자지불을 위하여 선진국에서는 암호 메카니즘을 이용한 지불 시스템 개발을 서두르고 있으며, 그 결과로 전자화폐, 전자수표, 신용카드 및 지불 브로커 등의 방식이 소개되고 있다. 전자화

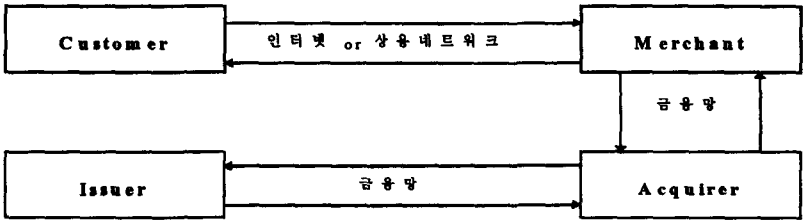
페나 전자수표를 사용하는 방법은 고도의 암호화 기술이 필요하며, 아직은 시기상조라는 견해가 지배적이다. 또 하나의 방법인 신용카드를 이용하는 방법은 이미 우리 사회에 신용카드의 사용이 대중화되어 있기 때문에 이를 이용하는 방법이 가장 현실성 있다고 할 수 있다.

아직 공인된 표준이나 산업계 표준이 존재하지 않은 상태에서 여러 종류의 전자지불 시스템이 발표되어지고 있다. 이 중 몇 가지는 이미 구현이 되어 사용되고 있지만, 그 보다 많은 수가 아직 스펙(spec)이나 계획만 발표하고 서비스는 시작하지 않고 있는 상태이다. 현재 실제로 상품을 구입할 수 있는 전자지불 시스템에는 CyberCash, First Virtual Internet Payment System 등이 있다. iKP(Internet Keyed Payment)는 프로토콜만 발표해 놓은 채 아직 구현은 되지 않은 기술이다. 이들을 중심으로 전자지불 시스템의 종류와 상품구매 방법에 대하여 알아 보도록 한다.

- iKP[2]

iKP는 IBM에서 개발한 인터넷 전자지불 프로토콜로써 공개용으로 발표해 사람들의 의견을 듣고 있는 전자지불 프로토콜이다. iKP라는 이름에서 i는 공개키를 소유하고 있는 당사자의 수를 나타낸다. 전체적인 프로토콜의 참여자는 4부분이다. 서비스를 사려는 사람(Customer), 서비스를 팔려는 사람(Merchant), 서비스를 팔려는 사람이 거래하는 은행(지불되는 금액이 입금되는 은행, Acquirer), 서비스를 사려는 사람이 거래하는 은행(지불되는 금액이 출금되는 은행, Issuer)이 그 당사자들이다. 이들 4부분의 참여자들 중에서 Acquire만이 공개키를 소유하고 있는 형태를 1KP라 하고, Acquirer와 Merchant가 공개키를 소유하고 있는 형태를 2KP, Acquirer, Merchant, Customer가 모두 공개키를 가지고 있는 형태를 3KP라 한다. 공개키를 소유하고 있다는 것은 전자서명을 발행할 수 있다는 것을 의미하며, 보안상의 측면에서는 3KP의 안전성이 가장 우수하다.

iKP의 특징은 구매자와 판매자는 인터넷이나 다른 상용 네트워크를 사용하고 있지만, 은행 사이의 거래는 이와 다른 금융망을 사용하고 있는 것이다. 이를 그림으로 표현하면 (그림 1)의 형태가 된다.



(그림 1) iKP의 네트워크 형태

(그림 1)에서 보면, Customer와 Merchant 사이의 통신은 인터넷이나 상용 네트워크를 사용한다. 그러나, Merchant와 Acquirer사이의 통신, Acquirer와 Issuer 사이의 통신은 금융기관에서 사용하는 통신망을 사용하고 있다.

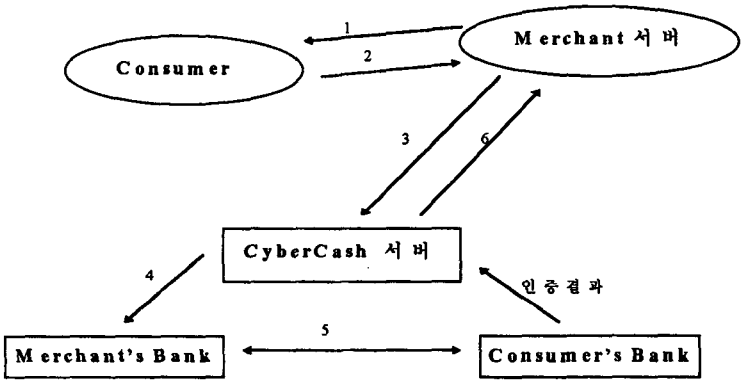
- CyberCash[3]

현재 인터넷상에서 이루어지는 전자 거래에서 가장 일반적으로 사용되는 방법이 신용카드를 이용하는 것이다. 하지만 신용카드를 이용할 경우 신용카드 번호를 네트워크를 통해 상점으로 안전하게 보내는

방법, 불순한 의도를 가진 상점에 의해 신용카드 정보가 악용될 소지, 트랜잭션(Transaction)이 발생할 때마다 신용카드의 번호와 수신자 주소 등의 정보를 입력해야 하는 불편 등이 문제점으로 남는다.

CyberCash를 이용한 전자거래는 구매자, 상인, CyberCash Inc. 사이에서 이루어진다. 구매자는 CyberCash가 무료로 제공하는 CyberCash Wallet이라는 프로그램을 이용하여 CyberCash에 계정을 등록하고, 이 프로그램에 자신의 신용카드 정보를 기록한 후 이용한다. 상인은 CyberCash로부터 상인 자격을 인증받고, 인터넷의 WWW사이트에 자신의 상품을 선전하는 상점을 구축한다. 현재 CyberCash를 이용하는 크고 작은 상점은 약 25개 정도가 존재하는 데 CyberCash 홈 페이지에서 'Cool Places Shop' 을 선택하면 이들의 목록을 볼 수 있다. CyberCash Inc.는 구매자와 상인을 서로에게 인증하고, 소비자의 신용카드 정보를 불순한 의도로부터 보호하며, 신용카드회사에게 상품 대금을 인출하여 상인에게 전달한다.

CyberCash가 동작하는 6단계는 (그림 2)와 같으며 각 단계별 설명은 아래와 같다.



(그림 2) CyberCash의 6단계

1. Consumer는 Merchant서버에 접속하여 구입할 물건의 종류, 갯수, 배달될 주소 등을 지정한다. Merchant서버는 Consumer가 입력한 것을 종합하여, 다시 Consumer에게 보내준다.
2. Consumer는 Merchant가 보낸 값을 보고, 거래를 하기로 결정하면 화면에서 "Pay"버튼을 누른다. "Pay"버튼을 누르면 Checkfree, Compuserver wallet 등이 구동되고, 거기서 지불에 사용할 신용카드를 선택한다. 그 후에 "OK"버튼을 누르면 지불정보가 Merchant에게 암호화되어 전송된다.
3. Merchant는 수신한 암호문에 자신의 전자서명을 붙여 CyberCash서버로 전송한다. 이 때 Merchant는 Consumer의 신용카드 정보 등을 알아낼 수 없어야 한다.
4. CyberCash는 암호문을 복호화하여 지정된 라인을 통해 Merchant의 은행으로 지불내용을 전송한다.
5. Merchant의 은행은 Consumer의 은행으로 Consumer에 대한 인증을 요청한다. 인증 요청에 대한 결과는 CyberCash서버로 전송된다.
6. CyberCash서버는 인증결과를 Merchant에게 전송하고, Merchant는 이를 Consumer에게 전송한다.

- First Virtual[4]

First Virtual Holdings Incorporated사의 First Virtual(이하 FV)은 별도의 전용 프로그램이나 보안이 강화된 프로토콜을 이용하지 않고, 기본적인 WWW브라우저와 전자우편만을 이용하여 전자지불 시스템을 구축

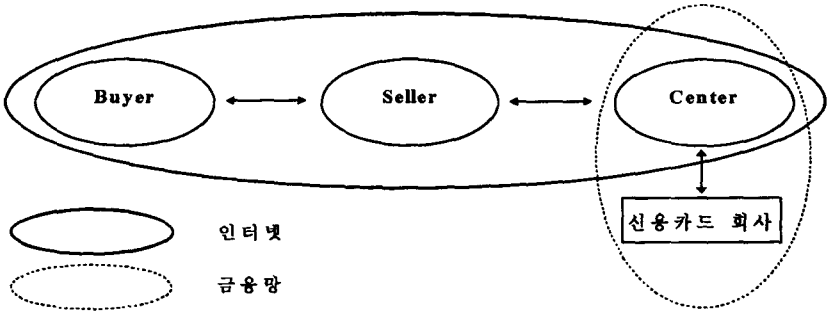
했다는 점에서 다른 시스템과 구별된다. 이는 일반 사용자에게는 지불 전용 프로그램이나 암호화 기법 등은 너무 복잡하고 불편하다는 이유에서 시작되었다. 따라서 이미 익숙한 WWW 브라우저와 전자우편만을 이용한 전자지불 시스템을 구현하였다. 그러나 특별한 암호화 기법을 사용하지 않기 때문에 신용카드 정보의 전달, 상품을 구입할 때 소비자가 계정을 개설한 사람임을 증명하는 방법 등의 보안상의 문제점을 내재하게 된다. FV에서는 이러한 문제를 전화, FAX, 전자우편을 이용하여 안전한 전자거래가 이루어질 수 있도록 한다.

3 Secure Credit Card Payment

Secure Credit Card Payment(SCCP)는 전자우편 보안도구인 PGP를 사용하여 구현한 전자지불 프로토콜이다. PGP와 WWW의 정합을 위해서는 PGP-CCI 기법을 사용하였다. SCCP에서는 지불수단으로 신용카드를 사용하고 있으며, 지불보증 센터라는 기관을 두어 모든 거래에 대한 관리와 책임을 맡기고 있다. 이 프로토콜은 WWW의 암호 통신이라는 문제를 해결한 기반 위에서 출발하므로, 통신되는 HTTP 메세지의 기밀성, 전자서명 등은 기본으로 제공되고 있다. 또한 사용자는 거래에 관한 모든 정보를 브라우저 화면 안에서 얻을 수 있도록 사용자의 인터페이스를 설계하였다.

3.1 SCCP의 지불 프로토콜

SCCP 프로토콜의 참여자는 3부분이다. 상품을 구입하려는 Buyer와 상품을 팔려는 Seller, 그리고 거래를 관리하며, 사용자 인증을 수행하고 신용카드 회사에 명령을 내리는 Center가 각각의 당사자이다. 네트워크의 구성은 iKP에서 제시한 것처럼 Center와 신용카드 회사의 통신은 금융망을 사용하고, Buyer와 Seller 사이의 통신, Seller와 Center 사이의 통신은 인터넷을 사용한다. 이는 (그림 3)과 같다.



(그림 3) SCCP의 전체 네트워크 구성도

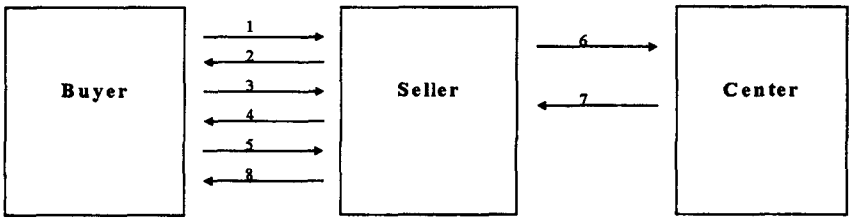
3.2 SCCP의 전제 조건

SCCP에는 몇 가지의 전제조건이 있다. 그 중에서 첫째는 전자지불에 참가하는 모든 당사자들이 상대방의 공개키를 모두 소유하고 있어야 한다. 둘째는 이들 공개키들에 대한 인증이 모두 이루어져 있어야 한다. 이는 Seller와 Buyer의 공개키에 Center의 서명을 붙여 공개한다는 것이다. 셋째는 Buyer와 Seller

가 Center에 회원으로 등록할 때에는 ID로써 PGP 공개키의 user ID를 사용한다. 넷째는 Buyer가 지불수단으로 사용할 카드에 대한 정보 즉, 카드의 회사나 카드번호와 같은 정보들은 이미 Center에 등록이 되어 있어야 한다는 것이다.

3.3 프로토콜의 각 단계별 설명

SCCP 지불 프로토콜을 순서대로 나타내면 (그림 4)와 같으며, 각 단계에 대한 설명은 다음과 같다.



(그림 4) SCCP 지불 프로토콜

1) 지불페이지 요청

(그림 4)의 1번 메세지는 지불페이지를 요청하는 단계로써 Buyer는 쇼핑 도중에 구입하려는 물건을 선택한 후, 지불 페이지를 요청하게 된다.

2) 지불페이지 전송

지불 페이지를 요청받은 Seller는 지불페이지를 전송해 주는 데, 2번 메세지가 지불페이지의 전송이다. 1번 메세지와 2번 메세지는 암호화 기법이 없는 단계로써 보통의 HTTP와 똑 같이 전송된다. Seller는 2번 메세지에서 Seller의 ID와 자신이 사용하고 있는 Center의 ID를 전송해 주어야 한다.

3) 구입 요청

$EKS1[BuyerID \| 코드 \| 갯수 \| 난수 \| EKR_{Buyer}[H(BuyerID \| 코드 \| 갯수 \| 난수)]] \| EKU_{Seller}[KS1]$

3번 메세지에서 Buyer는 구입하려는 물건의 코드, 갯수, 난수, BuyerID를 Seller로 전송한다. BuyerID는 Seller가 자신에게 문서를 암호화할 수 있도록 하기 위하여 자신의 공개키 ID를 알려 주는 것이고, 난수는 지불처리 후, 영수증을 받을 때에 자신이 신청한 거래에 대한 영수증 인지를 확인할 때 사용된다. 이 메세지에 자신의 서명을 붙임으로써 Buyer에 대한 사용자 인증이 이루어지도록 하고, Seller만이 그 내용을 알아볼 수 있도록 암호화한다. Seller의 공개키 ID는 2번 메세지에서 hidden 태그를 사용하여 전송 받은 내용이다.

4) 가격 동의 요구

$EKS2[가격동의서 \| EKR_{Seller}[H(가격동의서)]] \| EKU_{Buyer}[KS2]$

가격동의서 : SellerID||BuyerID||코드||갯수||난수||가격

3번 메세지를 수신한 Seller는 암호문을 복호화하고, 전자서명을 확인한다. 코드와 갯수를 이용하여 가격을 계산하여 가격동의서를 작성한다. 이 가격동의서에 Seller 자신의 전자서명을 추가한 후, Buyer만

이 알아볼 수 있도록 암호화 하여 Buyer에게 전송한다. 이 메세지에 Seller의 전자서명과 Buyer의 전자서명을 추가함으로써 Center로 하여금 금액에 대해서 두 당사자가 합의를 했다는 증거로 삼는다

5) 가격 동의 확인

EKS3[가격동의서||EKR$_{Seller}$[H(가격동의서)]||EKR$_{Buyer}$[H(EKR$_{Seller}$[H(가격동의서)])]] || EKU$_{Center}$[KS3]

4번 메세지를 수신한 Buyer는 복호화하고, 전자서명을 확인하여 가격동의서의 내용을 본다. 가격을 확인한 Buyer는 Seller가 가격동의서에 붙여 놓은 전자서명에 자신의 전자서명을 추가하여 Seller가 붙인 전자서명과 함께 Center만이 알아볼 수 있도록 암호화하여 Seller에게 전송한다. Seller의 전자서명에 Buyer가 전자서명을 붙인 것은 가격에 대해 Seller와 Buyer가 모두 동의했다는 증거로 활용된다.

6) 지불처리 요구

EKS3[가격동의서||EKR$_{Seller}$[H(가격동의서)]||EKR$_{Buyer}$[H(EKR$_{Seller}$[H(가격동의서)])]] || EKU$_{Center}$[KS3]

Buyer로부터 5번 메세지를 수신한 Seller는 5번 메세지를 그대로 Center에게 전송해 준다.

7) 영수증 발급

EKS4[영수증 || EKR$_{Center}$[H(영수증)]] || EKU$_{Seller}$[KS4]

영수증 : 지불성공여부||CenterID||SellerID||BuyerID||코드||갯수||난수||가격

Center는 6번 메세지를 수신하여 복호화하고 전자서명을 확인하여 Buyer와 Seller에 대해 사용자 인증을 수행한다. 전자서명 확인의 순서는 다음과 같다. EKR$_{Buyer}$[H(EKR$_{Seller}$[H(가격동의서)])]을 복호화하여 구한 H(EKR$_{Seller}$[H(가격동의서)]과 함께 전송된 EKR$_{Seller}$[H(가격동의서)]의 해쉬값을 계산하여 비교한다. 두값이 일치한다는 것은 Buyer와 Seller가 동일한 가격동의서에 서명을 했다는 뜻이 된다. 두값이 일치할 경우에 EKR$_{Seller}$[H(가격동의서)]을 복호화하여 구한 H(가격동의서)와 함께 전송된 가격동의서의 해쉬값을 구하여 비교한다. 두 값이 일치한다는 것은 가격동의서의 내용이 변조되지 않았다는 것을 의미하므로, Center는 지불신청을 처리한다. 지불이 성공했는 지의 여부를 나타내는 메세지와 CenterID, SellerID, BuyerID, 코드, 갯수, 난수, 가격 등을 함께 하나의 메세지로 만들어 자신의 서명을 붙이고, Seller만이 복호화할 수 있도록 암호화 하여 Seller에게 전송한다.

8) 영수증 전송

EKS5[영수증 || EKR$_{Center}$[H(영수증)]] || EKU$_{Buyer}$[KS4]

Center로부터 영수증을 수신한 Seller는 Center의 전자서명을 Buyer만이 복호화할 수 있도록 암호화하여 Buyer에게 전송해 준다. 사용된 CenterID, SellerID, BuyerID, 코드, 갯수, 난수, 가격 등을 모두 비교해 봄으로써 지불처리를 신청한 거래에 대한 영수증임을 확인할 수 있다.

8번 메세지를 수신한 Buyer도 CenterID, SellerID, BuyerID, 코드, 갯수, 난수, 가격 등을 모두 비교해 봄으로써 자신이 구입하려는 상품에 대한 지불 영수증임을 확인할 수 있다.

3.4 SCCP 프로토콜의 안전성

SCCP는 모든 통신에 대해 PGP를 이용하여 전자서명과 암호화를 구현함으로써 통신의 기밀성 및 송신자 부인 방지, 사용자 인증, 메세지 인증 등은 기본적으로 지원해 주고 있다. 그러므로, 이 단락에서는 지불 프로토콜 자체가 가질 수 있는 위험성과 그 위험을 SCCP에서는 어떠한 방법으로 방지하고 있는지를 알아 본다.

- 전자지불 프로토콜의 보안 기준[2]

지불 프로토콜에 문제가 있다면 기밀성과 전자서명이 아무리 잘 구현되어 있다 할지라도, 제대로 지불 업무를 수행해 줄 수가 없다. 앞서 살펴 봤던 iKP에서 주장하는 지불 프로토콜이 가져야 할 보안기준들을 먼저 알아 본다. 각 항목의 머리글로 들어가 있는 알파벳은 프로토콜 각각의 구성원의 입장에서 필요로 하는 요소를 뜻한다. 즉, A는 Acquirer로 Seller가 거래하는 은행의 입장에서 필요한 요소이고, M은 Merchant로 Seller의 입장에서 필요로 하는 요소를 나타낸다. C는 Customer로써 Buyer의 입장에서 필요로 하는 요소를 나타낸다. 앞의 8개는 지불 프로토콜에서 반드시 지켜져야 할 요소들이고, 뒤의 두 가지 요소 C5와 C6은 선택적으로 필요로 하는 요소들이다.

- A1 : Proof of Transaction Authorization by Customer

Seller의 은행 입장에서 보면 Buyer의 신용카드에서 금액을 인출할 때는 이 트랜잭션이 실제로 신용카드의 주인이 허가한 것인 지를 반드시 알아야 한다.

- A2 : Proof of Transaction Authorization by Merchant

Seller의 은행은 금액을 Seller의 계좌에 입금할 때, 이 계좌의 주인이 실제로 거래에 참여하고 있는 Seller인지를 반드시 알아야 한다.

- M1 : Proof of Transaction Authorization by Acquirer

Seller는 자신이 거래하고 있는 은행이 이 트랜잭션에 대해 적합성을 인증해 주기를 원한다. 이렇게 함으로써 나중에 Seller의 은행에서 트랜잭션의 적합성에 대한 의문을 갖지 못하도록 해야 한다.

- M2 : Proof of Transaction Authorization by Customer

Seller는 자신이 거래하는 은행이 트랜잭션에 대해 적합성을 인정해 주었다 하더라도 Buyer에게서도 그러한 인정을 받아야 한다. 즉, 나중에 Buyer가 그 거래에 대한 부정을 할 수 없도록 해야 한다.

- C1 : Unauthorized Payment is Impossible

Buyer가 스스로 트랜잭션을 신청해야 만이 Buyer의 신용카드를 이용하여 출금할 수 있도록 해야 한다. 이는 Buyer의 요청 메세지에 대한 replay 공격을 막아낼 수 있어야 한다는 것이다.

- C2 : Proof of Transaction Authorization by Acquirer

Buyer는 Seller의 은행으로부터 금액을 입금 받았다는 일종의 영수증을 받아 놓아야 한다. 이 영수증을 받아 놓음으로써 나중에 Seller가 금액이 맞지 않는다고 하는 등의 분쟁에서 증거로 활용할 수 있다.

■ C3 : Certification and Authentication of Merchant

Buyer는 지금 거래하려는 Seller가 은행으로부터 인증을 받은 Seller라는 증거를 원한다. 이러한 증거를 확인함으로써 Buyer는 자신의 구매가 위조된 Seller에서 이루어지지 않고 있다는 증거를 확보하게 된다.

■ C4 : Receipt from Merchant

Buyer는 Seller가 돈을 입금 받고 상품을 반드시 배달해 준다는 약속을 받아 놓아야 한다. Seller가 금액을 입금 받고도 상품을 배달해 주지 않을 때에 사용할 수 있는 증거가 필요하다.

■ C5 : Privacy

Buyer는 자신의 구매 정보가 거래 당사자들 이외의 사용자들에게는 알려지지 않기를 원한다. 신용카드 정보와 같은 것은 당연히 암호화되어 가지만 그 이외의 정보 즉, Buyer가 어느 물건을 몇 개 신청했는가와 같은 정보도 개인의 취향을 노출시킬 수 있기 때문이다.

■ C6 : Anonymity

Buyer는 자신이 보내는 정보에 대해 기밀성 이외에도 익명성을 보장받으려 할 때가 있다. 익명성은 상품을 판매하는 Seller가 구입하는 사람을 모르게 하는 방법이 있고, 지불을 처리해 주는 쪽에서도 Buyer의 신원을 모르게 해 주는 경우가 있다.

● SCCP의 보안기준 평가

위에서 보인 IBM의 전자지불 프로토콜의 보안기준들 중에서 SCCP는 어느 정도를 만족시켜 주고 있는 지를 알아 본다. SCCP은 iKP와는 달리 Center가 신용카드 회사에 지불명령을 내리면 신용카드 회사는 현재의 금융망에서 사용하고 있는 방법대로 지불을 처리한다.

■ A1 : Proof of Transactión Authorization by Customer

신용카드 회사는 지불보증 센터에서 내려 오는 명령을 근거로 하여 지불처리를 수행하게 되므로 결국, A1에 대한 확인작업은 지불보증 센터에서 이루어진다. (그림 4)에서 Buyer가 보내 주는 5번 메세지가 확인작업을 수행해 준다. EKR_{Buyer}[H(가격동의서)]는 BuyerID에 Buyer가 전자서명을 붙은 것으로 Buyer 본인이 아니면 생성할 수 없는 메세지이므로 Buyer가 신용카드의 주인이라는 것을 확인할 수 있다.

■ A2 : Proof of Transaction Authorization by Merchant

A2는 (그림 4)에서 Seller가 보내 주는 6번 메세지를 이용해 확인할 수 있다. 6번 메세지의 EKR_{Seller}[H(가격동의서)] 부분은 SellerID에 Seller가 전자서명을 붙인 것으로 Seller 이외의 다른 사람은 생성할 수 없다. 그러므로, 지불이 수행되어 금액이 입금되는 통장의 주인이 Seller라는 것을 증명할 수 있다.

■ M1 : Proof of Transaction Authorization by Acquirer

Seller가 신청한 지불처리에 대해 모든 책임은 지불보증 센터가 갖는다. 지불보증 센터는 Buyer와

Seller가 보낸 메세지들을 확인한 후, 신용카드 회사로 명령을 내리므로, 지불보증 센터가 Seller가 보낸 메세지를 확인하여 신용카드 회사로 명령을 내렸다는 것으로 Seller는 자신의 지불 신청이 적합하다는 평가를 받았다는 것을 알 수 있다.

- M2 : Proof of Transaction Authorization by Customer

Seller는 자신이 계산한 금액에 대해 Buyer의 확인을 받기 위해 (그림 4)의 4번 메세지를 전송한다. 4번 메세지의 가격동의서에 Buyer가 전자서명을 붙인다는 것은 Buyer가 이 거래를 인정한다는 의미가 된다. Buyer의 전자서명이 붙은 5번 메세지를 Center에 전송함으로써 Seller는 지불보증 센터에게 자신의 지불요청이 Buyer의 확인을 받은 것이라는 것을 증명할 수 있다.

- C1 : Unauthorized Payment is Impossible

Buyer가 상품을 신청하는 3번 메세지와 가격에 동의한 5번 메세지는 모두 Buyer의 전자서명이 포함되어 있다. Buyer의 전자서명을 Center에서 확인하게 되므로 Buyer 이외의 다른 사람은 정당한 거래를 신청할 수 없게 된다. 또한, 가격동의서에는 난수가 포함되어 Center가 영수증을 발행할 때 포함시키는 난수와 비교하여 Replay 공격을 방지한다.

- C2 : Proof of Transaction Authorization by Acquirer

Buyer는 거래를 신청한 후, 영수증을 받게 된다. 8번 메세지에는 지불보증 센터에서 발행한 전자서명이 붙어 있고, 이는 곧 이 거래가 지불보증 센터의 확인하에 이루어졌다는 증거로 사용될 수 있다.

- C3 : Certification and Authentication of Merchant

Seller가 인증된 서버라는 사실에 대한 여부는 지불보증 센터에서 전자서명의 확인작업으로 확인해 주고, 또한 Buyer가 Seller의 공개키를 입수할 때에 공개키의 인증여부로 확인할 수 있다. Center는 정당한 Seller의 공개키에 자신의 서명을 붙여 공개한다. 만약, Buyer가 어느 Seller의 공개키를 얻었을 때 공개키에 Center의 서명이 붙어 있지 않으면 이는 정당한 서버가 아니라는 사실을 유추할 수 있다. 또한, Buyer가 만약 공개키의 인증여부를 확인하지 않고 사용했다 할지라도, 6번 메세지를 받은 Center가 Seller가 정당하지 않다는 것을 발견할 수 있고, 이 때에는 지불을 처리하지 않게 된다.

- C4 : Receipt from Merchant

Seller는 지불보증 센터에서 지불을 처리해 주어 입금을 받은 후에 상품을 Buyer에게 배달하지 않을 수도 있다. 하지만, 지불보증 센터에는 Seller와 Buyer의 전자서명이 붙어 있는 6번 메세지가 저장되어 있으므로, 거래 자체에 대해 부정을 할 수는 없다. 만약 정해진 기간 내에 상품이 배달되지 않을 경우, Buyer는 지불보증 센터의 협조를 얻어 내용을 확인할 수가 있다. 그러므로 Seller가 금액만 입금 받고 상품은 배달해 주지 않는 상황을 방지할 수 있다.

- C5 : Privacy

SCCP에서 네트워크를 통해 전송되는 모든 내용들은 PGP를 이용해 암호화된 상태로 전송된다. 특정인이 어느 상품을 몇 개 신청했는가와 같은 정보도 Seller와 Center만이 알아볼 수 있도록 암호화되기 때문에 모든 메세지들에 대한 기밀성이 보장된다.

■ C6 : Anonymity

Buyer는 Seller에 대해 익명성을 제공받는다. Seller가 알 수 있는 정보는 Buyer가 신청한 상품의 종류와 갯수, 그리고 Buyer의 ID이다. 하지만, ID만 사용해서 Seller가 Buyer에 대한 정보를 알아낸다는 것은 불가능하다. 하지만, 지불보증 센터에서는 Buyer와 Seller의 ID, 신용카드 정보, 통장번호와 같은 정보를 저장하고 있기 때문에 Buyer는 지불보증 센터에 대해서는 익명성을 보장받지 못한다. 그러나, 지불보증 센터에 대해서도 익명성을 지켜주려 할 경우에는 Buyer에 대한 신분확인 작업과 지불처리가 불가능해지므로 지불보증 센터에 대해서도 익명성을 보장받는 프로토콜은 불가능하다고 볼 수 있다. 그러므로, SCCP은 익명성을 보장받는다고 할 수 있다.

SCCP는 IBM에서 평가기준으로 제안한 10가지에 대해서 모두 만족하는 것으로 평가된다. 이는 iKP 프로토콜 중에서도 1KP와 2KP에서는 불가능하고 3KP에서만 가능한 것으로 이 사실은 SCCP이 iKP와 비교해 보안적 측면에서 동등한 프로토콜임을 보여 준다.

4 결 론

WWW이 쇼핑수단으로 본격화되고 있지만 지불수단으로 사용되고 있는 방법들은 보안상의 많은 문제점을 내포하고 있다. 안전하지 않은 전자지불 프로토콜의 사용으로 예상할 수 있는 문제점으로는 개인정보의 유출과 경제범죄 발생을 예상할 수 있다. 이는 더 이상 간과할 수 없는 것으로 인식되어 여러 회사에서 전자지불 프로토콜의 개발을 위해 많은 투자를 하고 있다.

이러한 상황에서 WWW기반의 전자지불 프로토콜로 개발된 SCCP는 신용카드를 이용한 전자지불 방식을 채택하였다. 이는 신용카드를 이용한 방식이 이미 사람들의 생활에 관례화되어 있어 구현과 사용이 편리하기 때문이다. 또한, SCCP는 구매자가 상품의 신청에서부터 거래의 결과까지를 하나의 브라우저 안에서 수행할 수 있는 형태의 편리한 인터페이스를 설계하였다. SCCP는 암호화 모듈로 사용한 PGP의 특성대로 인터넷에서 전송되는 모든 메세지들에 대해서 전자서명과 암호화 작업을 수행해 준다. 전자서명의 사용으로 대금지불 메세지에 대한 송신부인 방지 및 메세지 인증, 사용자 인증이 가능해져 전자지불 프로토콜에서 요구하는 모든 사항들을 만족시켜 주고 있다.

참 고 문 헌

[1] 권도균, "WWW 보안과 전자화폐", http://wsp.nextel.net/seminar/etc/wwwpay.html

[2] Mihir Bellare, "iKP : A family of secure electronic payment protocols", http://www.zurich.ibm.ch/Technology/Security/extern/ecommerce/iKP_overview.html

[3] CyberCash 사, "The Six Steps in a Secure Internet Credit Card Payment", http://www.cybercash.com/cgi-bin/vdkw_cgi/x8eb907a8-4285/Search/4982900/1

[4] FV 사, "First Virtual Overview", http://www.fv.com/info/overview.html