SET 지불프로토콜을 이용한 효율적인 지불시스템에 관한 연구

A Study for Payment System Efficiently on SET Payment Protocol

°함정훈, 오상훈 한국데이터베이스진흥센터

Hahm jung-hoon, Oh sang-hoon, Korea Database Promotion Center

전자상거래의 급격한 성장에 따라 인터넷이라는 공용 네트워크에서 보다 안전한 지불수단을 필요로 하게 되었다. 현재 SSL을 이용한 정보보호 방법과 SET를 이용한 지불 프로토콜이 표준화 및 상용화되어 있다. 그러나 SSL은 신용카드나 직불카드 번호와 같은 중요한 정보들이 사용자의 의지와 상관없이 여러 통로로 노출될 수 있으며 거래 당사자들의 인증수단이 취약하다는 단점이 있고, SET 역시 프로세스들이 복잡하고 비용 등에 부담을 주고 있다. 새로운 대안으로 SSL기반에 특정한 상황에 SET으로 대체하는 것과 SSL에 인증기능을 강화하는 등의 새로운 연구들이 이루어지고 있다. 본 연구에서는 SET 프로토콜 기반의 새로운 지불 시스템을 제안한다.

1. 서 론

국내에서 인터넷 쇼핑몰 등을 포함한 전자상거래 규모는 해마다 급격한 성장을 보이고 있다. 이러한 추세는 최근 디지털기술이 발달하고, 인터넷의 활성화 및 멀티미디어 중심의 정보서비스가 가상의 공간에서 주요 서비스로 등장하면서 그 속도는 더욱 빠르게 증가하고 있다.

이러한 전자상거래의 급격한 성장은 새로운 지불수단을 필요로 하게 되었다. 전통적으로 지불은 사설, 보안 네트워크를 통해 정보들이 전송되었으나 인터넷을 이용한 전자상거래는 공용의 비보안 네트워크를 이용해야 한다는 문제가 있다. 이런 문제를 해결하기 위해 많은 방법이 도입되고 있는데, 최근에 널리 쓰이는 지불방식은 SSL(Secure Socket Layer)을 이용해 지불 정보를 보호하는 것이다. 그러나 SSL 방식은 몇 가지 단점이 있다. 신용 카드나 직불 카드 번호와 같은 중요 정보들이 사용자의 의지와 상관없이 여러 통로로 노출될 수 있으며, 거래 당사자들의 인증수단이 취약하다는 점이다. 이러한 단점을 보완하기 위해 등장한 것이 SET(Secure Electronic Transaction) 프로토콜을 이용한 지불시스템이다. 하지만 우리나라에서는 사용자들의 인지도, 거래행태, 관습, 비용 등으로 인해 SET보다 SSL을 통한 지불시스템을 선호하고 있다.

본 연구에서는 전자상거래를 위한 지불 프로토콜 개발 현황과 주요프로토콜의 장단점을 비교하고 SET 프로토콜 기반의 새로운 지불 시스템을 제안한다.

2. 지불프로토콜

지불은 단체 혹은 개인 사이의 가치 이전으로써 전자상거래를 위해 꼭 필요한 기술이다. 지불을 위해서 지불을 위한 보안 프로토콜이 필요하며 다음의 기능을 기본적으로 구현되어야 한다.

① 기밀성(Confidentiality): 전달내용을 제3자가 획득하지 못하도록 하는 것이다.
② 인증(Authentication): 정보를 보내오는 사람의 신원을 확인하는 것이다.
③ 무결성(Integrity): 정보전달 도중에 정보가 훼손되지 않았는지 확인하는 것이다.
④ 부인성(Nonrepudiation): 정보제공자, 이용자가 정보제공 사실을 부인하는 것을 방지하는 것이다.

또한 지불 프로토콜은 내부 매커니즘에 따라 지불 브로커 시스템과 전자 현금 시스템으로 구분할 수 있다.

지불 브로커 시스템(Payment Broker System)은 그 자체가 독립적인 신용 구조를 가지고 있지 않고 신용카드나 은행의 계좌를 이용하여 지불을 할 수 있도록 연계 시켜주는 시스템이다. 현재 실제 구매형태가 신용카드를 이용한 거래가 확산되고 있어 인터넷상의 많은 지불 프로토콜이 이 형태를 띠고 있다. First Virtual, CyberCash, SET 등이 여기에 속한다.

전자 현금 시스템(Electronic Money System)은 선불카드 혹은 직불카드를 이용하거나 순수한 디지털 현금을 이용하는 방법으로 아직은 실용화보다는 연구단계이며 E-cash가 대표적인 전자 현금 시스템이다.

[표 1] 지불브로커 시스템과 전자화폐 시스템의 장단점

	지불브로커 시스템	전자화폐 시스템
장점	· 기 구축된 금융시스템 사용가능 · 법적, 제도적 문제의 어려움 덜피 · 암호알고리즘의 수출입문제 해결 · 거래방법에 대한 사용자의 친밀감	· 사용자 프라이버시 보호 · 실제 화폐를 대치할 수 있음 · 기밀정보의 노출위험성 제거 · 오프라인방식으로 사용가능
단점	· 사용자의 프라이버시 침해 · 기밀정보의 누출위험성	· 이론적 미해결 문제들 · 효율성 문제 · 법적,행정적 제도의 지원 필요

세부적으로 S-HTTP, SSL, iKP, SET, MPTP, Millcent 등이 지불을 가능하게 하는 프로토콜이다.

2.1 S-HTTP

S-HTTP는 EIT(Enterprise Integration Technologies)에서 HTTP의 보안성이 향상되고 HTTP 통보가 캡슐화된 버전으로 개발한 프로토콜이다. S-HTTP는 HTTP와 마찬가지로 응용부문에서 적용되며, 일반적인 WWW의 보안방법으로 유효하고 지불정보의 안전한 전송에도 이용된다. 상호처리과정 통신을 확실히 증명하며, 통지의 안전성 그리고 출처의 비삭제성을 지원한다.

이 프로토콜은 HTTP세션으로 주고받는 자료를 암호화하고 전자사인을 해서 주고받는 메커니즘이며 RSA 암호문서(암호키 1024비트 내지는 768비트)와 Kerberos[1]에 기초한 보안장치를 지니고 있고 응용시에는 다른 암호문서장치(PGP, PEM)를 선택할 수 있다. HTTP에 대해서는 단지 클라이언트 내지는 서버가 S-HTTP를 지원시에는 비보호적 연결형태에서 통신을 할 수 있는 호환성이 있다.

2.2 SSL(Secure Socket Layer)

SSL은 테리사(Terrisa)가 개발해 Netscape사가 Netscape과 NetSite의 암호화 중심프로토콜로 사용하는 프로토콜이다. 따라서 SSL만으로는 지불 기능을 수행할 수 없다. 전자상거래에서 안전한 지불 기능을 수행하기 위해서 SSL로 서버와 클라이언트간에 인증(Certification) 을 하고 RSA방식과 X.509를 사용하여 실제 암호화된 정보는 새로운 암호화 소켓채널을 통해 전송하는 방식이다.

SSL은 특히 네트워크 레이어(OSI 7 Layer)의 암호화 방식이기 때문에 HTTP뿐아니라 NNTP, FTP등에도 사용할 수 있다. SSL은 모든 데이터가 인터넷상에 전송되기 전 암호화되는 연결을 만든다. SSL를 사용하는 경우에는 구동하기 전 핸드세이크(handshaking: 데이터 전송에 앞서 서로 미리 정한 몇 개의 제어 신호를 교환하는 과정) 과정에서 양측은 서로 신원정보를 공유하고, 여러 가지 암호화 알고리즘 중 하나를 선택하며, 각 SSL 세션 용도에 따라 적절한 암호화 키를 만든다. SSL은 최근에 대부분의 지불 정보 보안에 사용되는 정보보호 방식이다.

[그림 1] SSL기반 지불 프로토콜 쇼핑

2.3 iKP(Internet Keyed Payment Protocols)[2]

iKP는 RSA암호문서에 기초하고, 1995년초 IBM사에서 개발된 지불 프로토콜이다. 이 구조는 한 세션에 셋 또는 그 이상의 참여자가 모여, 지불거래를 직접 은행계좌를 통하거나 다른 금융기관을 통하여 처리한다. iKP는 현재 상황에서는 신용 카드 지불시스템만 지원하지만 구조적으로 보았을 때 다른 유형의 지불시스템으로 확장해 가는데 용이한 메커니즘을 갖고 있다. iKP는 3계층의 프로토콜인 1KP, 2KP, 3KP의 구조로 보안성을 확보한다. 1KP에서는 은행에 대한 인증만을 수행하고, 2KP에서는 상점에 대한 인증만을 수행하며, 3KP에서는 양자 모두에 대한 인증을 수행한다.

참여자(이용자, 카드회사 등)을 위한 최대한의 보안성과 장치의 표준화 그리고 다수의 지불거래참여의 의미를 부여하고 기존의 금융기본구조에 연결하는 것이 iKP가 설정한 목표이다. 1996년 전반기에 iKP는 제한된 기본실험으로서 프로토타입이 완성되었으나, 같은 시기에 SET 프로토콜이 개발되었기 때문에 iKP에 대한 지속적인 개발이 없었다.

2.4 SET(Secure Electronic Transaction)

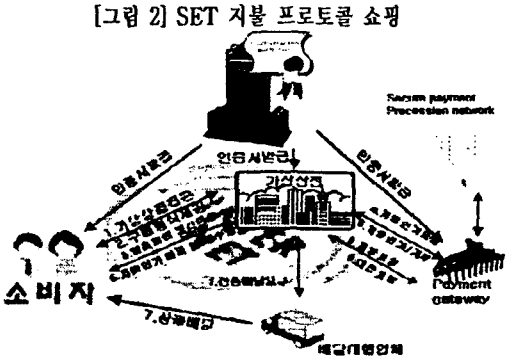
VISA와 MasterCard사가 공동 개발한 인터넷을 통한 신용카드 거래를 주목적으로 하는 프로토콜이다. 기존 신용카드 기반으로한 인터넷 전자상거래 환경을 실현하기 위해 전자상거래 요소, 시스템간의 암호화, 거래 및 지불시스템과 각 참여 개체들 사이의 인증을 위한 프로토콜이다. SET은 안전한 지불을 위해 정보의

1) http://web.mit.edu/kerberos/www/, 네트워크 기반의 인증시스템

2) http://www.ikp.de/

기밀성 유지와 메시지의 무결성 보장, 트랜잭션에 관련된 당사자간의 인증에 초점을 맞추고 있다. 이미 존재하고 있는 많은 인터넷 보안관련 프로토콜에 비하여 SET는 디지털 서명에 대하여 정의하고 있다. 디지털 서명은 지불 트랜잭션이 관련된 모든 당사자들을 인증하는데 사용된다.

[그림 2] SET 지불 프로토콜 쇼핑



SET은 Internet상의 신용카드 결제를 위한 보안 시스템 표준이며, 현재까지 가장 안전한 신용카드 기반의 지불 프로토콜이다.

2.5 MPTP(Micro Payment Transfer Protocol)

MPTP는 잦은 거래가 발생하는 두 상대방간에 소액거래에 적합하도록 최적화된 프로토콜이다. 이 프로토콜은 사기 등 불법행위를 막을 수 있는 높은 등급의 보안을 제공한다. 또 MPTP는 판매자와 소비자가 공통의 브로커를 이용하는 경우에 사용될 수 있다. 소액지불의 보안을 위해 공개키 알고리즘 보안방식을 사용하며, HTTP와 SMTP, MIME(Multipurpose Internet Mail Extentions)을 포함하는 다양한 인터넷 프로토콜을 기반으로 구현된다.

정보의 단위가 상대적으로 작은 소액지불 시스템에서는 정보의 처리속도와 비용이 가장 큰 관건이다. 따라서 소비자들의 구매가 잦을수록 응답하는 시간을 줄이는 것은 필수적이라 할 수 있으며, 브로커와 판매자들에게 부담되는 트랜잭션 처리와 저장에 대한 요구는 소액거래에 맞도록 경제적이어야 한다. MPTP는 수시로 일어나는 구매와 지불 행위를 처리하고, 지불의 흐름이 일방적인 특정 거래를 제외하고는 소비자와 판매자간의 구분이 없는 비동기 프로토콜이며, 대칭적인 프로토콜이다. 그리고 공개키 서명방식을 채택함으로써 소자본가들도 경제적으로 적용할 수 있다.

2.6 Millcent Protocol[3)]

Millcent프로토콜은 Digital Equipment사에서 센트(cent)부분을 위한 소액 계산을 하기 위하여 고안되었다. 중개인은 공급자와 고객으로부터 계좌관리를 담당하고 고객을 위하여 내용증명서를 제공한다. 내용증명서의 중복발급에 대한 검사는 공급자 스스로 한다. 따라서 중앙서버는 필요 없다. 고객은 중개인 수수료를 포함하는 합산된 금액을 전자 지불수단이나 전통적인 방법으로 지불할 수 있다. 중개인은 이로 인하여 고객과 공급자 사이에서 상호조정 계산 담당을 하는데, 이처럼 Digital Equipment사는 VISA나 MaterCard사, 은행들과 같은 금융기관이나 AOL, CompuServe와 같은 대규모 인터넷 내지는 온라인 서비스제공자들에게 중개인 역할을 한다.

대칭적인 암호방식이 사용되며, 익명성을 제공하진 못한다. 고비용의 암호문서장치는 소액을 취급하기 때문에 적용되지 않으며 이 시스템은 현재까지는 상업적으로 이용되지 않고 있다.

현재 전자상거래를 위한 다양한 지불 프로토콜들이 제안되었으나, 아직까지는 국제 표준기구에서의 표준화 움직임은 없다. 다만, 지불시스템을 상용화하려는 현 시점에서 각 지불시스템간의 상호호환성 확보에 대한 문제가 제기되어 업체들끼리의 컨소시엄을 통해 표준화 작업들이 진행 중에 있다. 현재 제안된 대부분의 지불 프로토콜은 서로간의 상호호환성이 전혀 없으며, 그렇다고 각자의 프로토콜을 버리고 단일화할 전망은 거의 없다고 할 수 있다.

3. 주요 지불프로토콜 비교

연구된 여러 지불프로토콜 중에서 사실상 표준으로 인식되고 있는 SSL 프로토콜을 이용한 지불 시스템과 SET 지불프로토콜를 비교하였다.

[표 2] SSL과 SET의 장단점 비교

특 징	SSL	SET
증명서	증명서가 없을 수도 있다.	신뢰받는 제3자에 의해 모두증명
인증	참여자를 인증 없다.	고객과 판매자 모두 인증되었다.
부인 봉쇄	고객의 약속 준수를 확보하는 메커니즘이 없다.	고객이 구매하고 지불한다는 약속에 디지털 서명을 한다.
상인사기의 위험	고객이 핵심 재무자료를 상인에게 준다.	고객이 핵심 재무 자료를 지불게이트웨이에게 준다.
고객사기에 대한 책임	사기일 경우 판매자가 책임진다.	사기일 경우 금융 기관이 책임있다.
인프라	브라우저와 웹서버에 위치한다.	전본 시범에서 입증, 소프트웨어 몰카지나 툴로 시판되었다.
익명성 대 감사 가능성	각 사용자들이 트랜잭션 시작시 자신들을 증명해지만 이에 대한 보증은 약하다.	트랜잭션 내내 모든 참여자들이 증명을 받아야 한다.
표준화	IEFT에 의해 표준화	SETCo에 의해 표준화
범용성	널리 사용된다.	널리 사용되고 있지 않다.

SET과 SSL은 보안을 제공한다는 점을 제외하고는 설계에서부터 근본적으로 다른 프로토콜이다. SSL은 통신상의 정보를 보호하기 위

3) http://www.research.digital.com

한 프로토콜로써 HTTP, FTP, SMTP, Telnet 등 상위 프로토콜의 하위에서 상위 프로토콜의 모든 정보를 암호화하여 통신하고 있는 양자간의 인증 및 데이터의 무결성, 인증, 기밀성을 제공해 준다. SET은 인터넷상에서 신용카드 기반의 전자 지불을 위한 트랜잭션을 제공하며 이때 교환되는 정보를 보호하기 위해 정보보호 기능을 제공하는 보안 프로토콜이다.

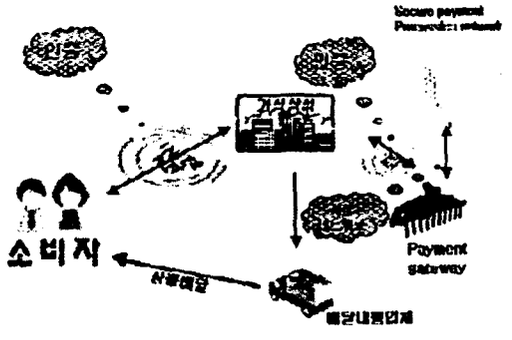
전자상거래 판매 시스템이 성숙되면서, SET로 전환이 더욱 어려워지고 있다. 1997년에 SET을 기다리던 많은 판매자들은 비용과 과도한 트랜잭션으로 인해 이 프로토콜을 포기하고 대신 SSL 암호화 방식을 채택하였다. SSL 방식을 채택하므로써 생기는 문제들을 처리하기 위해서는 사기행위 감시 서비스에 의존하고 있다.

최근에는 국내외 컨소시엄 및 연구를 통해 SSL 및 SET 기반의 새로운 지불프로토콜을 개발하고 있다.

4. SET 프로토콜을 이용한 새로운 지불방식

본 논문에서 제안하는 모델은 특정 커뮤니티 안에 강력하고 신뢰성 있는 '서비스중개자'가 지불에 관한 인증기능과 지불브로커 기능을 수행하는 것이다. 그렇게 함으로써 저비용으로 효율적인 전자상거래를 할 수 있다.

[그림 3] SET 기반의 새로운 지불 프로토콜 쇼핑



① SET 프로토콜을 통해 교환된 정보를 인터넷 서비스 제공업자가 인증한다. 기존의 SET에서는 앞에서 살펴본 것과 같이 별도의 인증기관이 담당하므로써 과도한 트랜잭션과 비용을 초래하였다. 기존의 안전성이 입증된 SET 프로토콜을 이용하고 소비자와 가상상점에 대한 정보를 가지고 있는 서비스 중개자가 인증을 함으로써 지불 인증 비용을 줄일 수 있다.

이런 인증기능을 하는 인터넷 서비스 제공업자들을 통합하여 하나의 인증기관을 이룰 수도 있을 것이다.

② 커뮤니티 브로커가 기존의 금융결제망이나 카드회사 사이에 이루어지는 지불은 기존의 폐쇄형 사설 네트워크를 이용하여 구축비용을 줄일 수 있다.

인증기관은 틀리지만 인증기능 및 부인 봉쇄 기능 그리고 상인 사기의 위험에 대한 기능은 기존의 SET 지불 시스템과 동일하다.

[표 3] SET와 제안된 새로운 지불방식 비교

특 징	SET	새로운 지불방식
증명서	인증기관	신뢰받는 서비스중개자
고객사기에 대한 책임	사기일 경우 금융 기관에 책임 있다.	사기일 경우 서비스중개자가 책임진다.
익명성 대 감시 가능성	트랜잭션 내내 모든 참여자들이 증명을 받아야 한다.	각 트랜잭션에 참여자들만 증명을 받는다.

소비자는 자신의 브라우져를 통해 가상상점에 접근하고 원하는 상품을 발견하여 '거래요청'을 하게되면 소비자와 가상상점은 서비스 중개자로부터 인증을 받아 거래가 이루어지게 된다. 가상상점은 고객으로부터 받은 지불정보를 서비스 중개자에게 전송하여 거래 성사를 알리며 일정한 주기로 거래금액을 상환 받는다. 따라서 커뮤니티 브로커 역할을 하게되는 서비스 중개자의 기능과 책임이 매우 중요하게 될 것이다.

5. 결 론

SSL 프로토콜을 이용한 지불 시스템이 국내에서 사실상 표준으로 인식되고 있지만, B2B 시장이 확대됨에 따라 보다 안전한 지불 시스템의 도입이 시급한 실정이다. 또한 안전한 지불 프로토콜로 SET 지불프로토콜이 개발되어 지불시스템으로 상용화 되어 있긴 하지만 비용 및 많은 트랜잭션으로 인하여 사용자들이 기피하고 있다. 따라서 본 연구에서는 SET 지불시스템의 인증기능을 특정 인증기관이 수행하는 것이 아니라 특정 커뮤니티안에 강력하고 신뢰성 있는 '서비스중개자'를 이용한 지불시스템을 제안한다. 이 시스템이 안정화되면 보다 적은 비용으로 안전한 보안기능 및 인증기능이 있어 고액거래 및 국제시장 거래가 활발하게 이루어질 수 있을 것이다.

< 참 고 문 헌>

1. 채송화. 1999. 「SSL기반 전자 상거래 지불 프로토콜 설계」, 아주대학교, 석사학위논문
2. 정명진. 1999. 「SET기반 한국형 전자상거래 지불결제 시스템에 대한 연구」, 성균관대학교, 석사학위논문
3. 허제도. 1999. 「전자상거래를 위한 전자지불방법 및 보안기술에 대한 사례 연구」, 아주대학교, 석사학위 논문
4. 최년식. 1998. 「인터넷 전자상거래 전자지불 시스템의 평가 분석에 관한 연구」, 고려대학교 석사학위논문
5. 이성렬. 1999. 「인증 기능이 강화된 온라인 전자 지불 시스템」, 부산대학교, 석사학위논문
6. http://www.openssl.org/
7. http://mastercard-visa.com/