일회성 패스워드 시스템을 적용한 모바일 결제 프로토콜

지창균°, 정일용, 배용근
조선대학교 전자계산학과

A mobile payment protocol with One-Time Password System

Chang-gyun Chi°, Il-yong Chung, Yong-geun Bae
Dept. of Computer Science, Chosun University
E-mail : ranumm@stmail.chosun..ac.kr, iyc@mail.chosun.ac.kr, ygbae@mail.chosun.ac.kr

요 약

M-Commerce에서 안전한 데이터 서비스를 위해서는 정보보호 및 무선 결제 시스템에 대한 연구가 반드시 선결되어야 한다. 현재 무선 결제 서비스는 이동통신사를 중심으로 한 소액결제 서비스가 주를 이루고 있으며, 신용카드 기반의 결제 서비스는 고액결제가 가능하지만 무선 결제 시스템에 취약한 문제점을 가지고 있다. 본 논문에서는 지불 승인 절차에 병목 현상을 개선하기 위해 일회성 패스워드 시스템을 적용한 PDA 기반 모바일 고액결제 시스템을 제안한다.

1. 서론

정보통신기술 및 무선통신 시스템의 급격한 발전과 더불어 PDA와 같은 소형 단말기의 보급 확대 및 고속데이터를 근간으로 하는 IMT-2000의 상용화가 국내에도 적용되는 시점에서, PC등의 고정 단말기를 이용한 기존의 전자상거래 형태를 벗어나 시간과 장소를 초월해 이동 중에도 무선 단말기를 이용하여 상거래 행위를 할 수 있는 M-Commerce가 보편화되고 있는 실정이다.

E-Commerce가 PC를 이용한 전자적인 모든 거래 형태를 총칭하는 반면, M-Commerce는 PC를 대신하는, "거래가 가능하도록 지원되는 개인화된, 경량화된, 지역 정보 제공이 가능한 개인용 Hand-Held 기기(예를 들면, 핸드폰, PDA 등)를 이용한 전자적인 모든 거래 형태를 총칭"하는 것이다[1].

M-Commerce에서의 정보보호는 데이터의 무결성, 기밀성, 부인방지, 사용자 인증 등의 보안 요소가 충족되도록 구축되어져야 한다. 현재 M-Commerce를 위한 무선 인터넷 보안은 크게 WAP(Wireless Application Protocol), ME(Mobile Explorer), i-mode 방식으로 나뉘어져 있고 각 진영에서 무선 인터넷을 위한 정보보호 서비스 기술 개발에 박차를 가하고 있다[2].

또한 M-Commerce에서 안전한 서비스를 위해 서비스의 특성에 맞는 무선 결제 서비스(Mobile Payment Service)에 대한 연구가 활발히 진행되고 있다.

현재 무선 결제 서비스는 유선 의존도가 높은 핸드폰 중심의 소액결제 서비스가 주를 이루고 있으며, 이에 반하여 신용카드 기반의 결제 서비스는 고액결제가 가능하다는 강점을 가지고 있기는 하지만 무선 인터넷 인프라가 부족하여 무선 결제시스템에는 취약하다는 문제점을 내포하고 있다. 또한 기존의 제안된 방법들도 지불 요청 및 승인 절차에 많은 오버헤드가 발생한다는 문제점을 갖고 있다.

따라서 본 논문에서는 데이터의 무결성, 비밀성, 부인방지 등의 기본적인 정보보호 서비스를 갖추면서 지불 승인 작업에 있어서도 일회성 패스워드 시스템을 적용하여 한층 가벼워진 PDA 기반의 안전한 M-Commerce 고액결제 시스템을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 현재 무선인터넷에서의 결제방식 및 일회성 패스워드 시스템의 개념에 대해서 기술하고 3장에서는 무선 인터넷 환경에 적합한 결제 프로토콜을 제안한다. 마지막으로 4장에서는 결론 및 향후 연구과제를 제시한다.

2. 관련연구

2.1 모바일 결제

휴대폰, PDA 등 무선에 특화된 단말기를 이용하여 무선 네트워크 상의 빌링 및 지불 시스템에 접근해 결제 서비스를 제공하는 것을 의미하는 모바일 결제 서비스는 2000년 무렵 국내에 첫선을 보였고, 당시에는 사용자 정보와 함께 SMS 서비스를 이용해 결제 비밀번호를 전송하는 방식이 주로 사용됐었다.

모바일 결제 서비스는 초기 유선인터넷과 무선인터넷이 상호 보완적인 관계를 유지했던 휴대폰 소액 결제 시장에서 출발해 최근에는 휴대폰이 신용카드 등 기존 금융 시스템을 대체하는 모델로까지 변화하고 있다[3].

모바일 결제방식은 크게 소프트웨어 결제방식과 하드웨어 결제방식으로 나뉜다. 소프트웨어 결제방식은 Phonebill, Mobile Wallet 방식이 있으며 Phonebill 방식은 구매대금을 익월 요금 청구서에 통신요금과 합산하여 부과하는 방식이고, Mobile Wallet은 은행 또는 신용카드사 서버에 카드회원 정보를 저장해 두고 가입자가 이동통신 단말기로 서버에 접속하여 결제하는 방식이다.

하드웨어 결제방식에는 Dual Slot 방식, Dual-Chip 방식, One-Chip 방식이 있다. Dual Slot 방식은 모바일 단말기에 스마트 카드 리더 슬롯이 장착되어 있거나 별도로 장착하여 스마트 카드를 이용하여 결제를 하는 방식을 말한다. Dual Chip 방식은 이동통신 사용자의 인증모듈과 금융 어플리케이션을 저장한 칩, 이렇게 두 칩을 지급결제에 사용하는 방식으로, 금융기관이 우위를 가진다. 마지막으로 이동통신사가 주도권을 가지는 One-Chip 방식은 이동통신 가입자 인증모듈 및 금융 어플리케이션을 한 개의 칩에 저장하는 방식이다.

모바일 결제 서비스 현황을 살펴보면 1세대의 경우는 유선 인터넷과 연동될 수 밖에 없다는 한계점을 지니고 있는 반면, 2세대의 경우는 보안 취약성으로 인하여 서비스의 범위에 제한이 생기는 문제점이 나타났다. 3세대에서는 스마트 카드를 도입하면서 보안 취약성을 해결함과 동시에 인프라 측면이 취약한 스마트 카드와의 시너지 효과를 보였지만 스마트 카드가 필요하다는 점 자체가 제한적인 요소로 작용하였다[3]. [표 1]에서 모바일 결제 서비스의 발전 과정을 정리해 보았다.

[표 1] 모바일 결제 서비스의 발전 과정

1세대	·2000 ~, 온라인 결제 솔루션 업체가 주도 ·소액결제 (유료 컨텐트 등) ·온라인 상의 컨텐트 구매를 위한 인증수단, 이동통신 요금에 합산 청구
2세대	·2001 하반기~, 이통사,금융기관이 대등한 구도 ·계좌조회,일부은행권은 자금이체 등의 금융 서비스 제공 ·초기 서비스는 단순 조회만 가능, 금융기관이 모바일 뱅킹 시스템을 갖추지 않고 기존 온라인 뱅킹에 모바일 접속을 가능케 한 수준
3세대	·2002 상반기~ ,이통사,금융기간이 대등한 구도 ·조회,이체,송금 등 금융 서비스 및 결제 서비스 ·스마트 카드 도입을 통한 금융서비스 제공 휴대폰을 이용, 스마트카드의 충전, 이체의 편의성 제공
3.5세대	·2002 하반기~, 휴대폰과 가맹점 단말기간의 근거리 무선통신 전문벤처 기업이 가세 ·오프라인 매장에서의 결제 서비스 추가 (지하철요금, 자판기 이용등) ·적외선,RF,블루투스 등의 근거리통신기술 결합 무선 상의 충전 이외에 오프라인 환경에서의 결제 서비스 제공

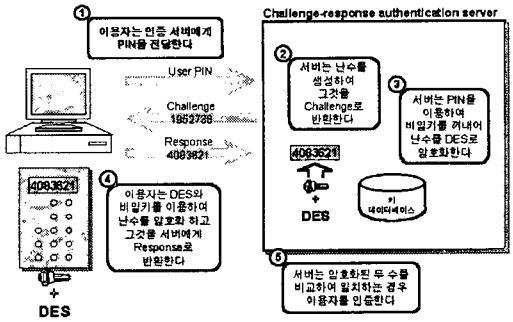
2.2 일회성 패스워드 시스템

현재의 로그인 체계에서는 네트워크 도청을 통하여 사용자 계정과 패스워드를 쉽게 알아낼 수 있다. 하지만 일회성 패스워드는 시스템에 로그인시 매번 다른 패스워드를 입력하게 함으로서 이러한 문제점을 해결할 수 있게 해주며, 한번 사용된 패스워드는 재사용이 불가능하게 되므로 불법 도청을 통해 사용자 계정과 패스워드를 알아냈다 하더라도 시스템에 접근할 수 없게 된다[4].

일회성 패스워드 기술은 S/Key 인증 시스템, Challenge-Response 인증 시스템, 시간을 이용한 일회용 패스워드 인증 시스템 등이 있다[5].

일회성 패스워드 구현 방법 중 Challenge-Response Scheme은 비교적 복잡성이 덜하고 안정성이 높으며 구현 방법이 쉽다. 인증 절차는 다음과 같다. 먼저 사용자가 인증을 요구하게 되면 서버는 임의의 Challenge를 생성하여 사용자에게 전송한다. 사용자는 PIN(사용자 식별 번호)와 Challenge를 이용하여 서버에 전송할 일회성 패스워드를 생성하고, 서버에게 응답 메시지를 전송한다. 서버는 동일한 Challenge와 등록된 사용자 정보를 사용해서 일회성 패스워드를 생성한 후 사용자가 전송한 Response 값을 비교하여 사용자 인증을 하게 되는 방식이다.

아래 [그림 1]은 Challenge-Response 방식의 사용자 인증 절차를 보여준다[5].

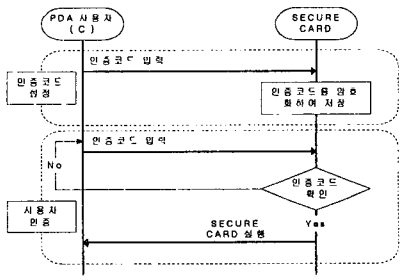


[그림 1] Challenge-Response 방식의 인증 절차

3. PDA 기반 안전한 결제 프로토콜 설계

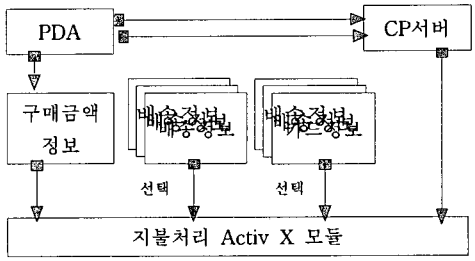
3.1 Secure Card 모듈

PDA는 이동성이 강한 정보기기로 기존 유선상의 정보기기에 비하여 정보 입력 작업이 원활하지 않은 입력 구조를 가진다. 따라서 PDA기반의 결제 솔루션을 제공하는데 거론될 수 있는 문제가 사용자와의 인터페이스이다. 이동기기의 정보입력 불편의성의 문제를 해결하고 안전한 결제 솔루션을 제공하기 위하여 'SECURE CARD'를 설계하였다. SECURE CARD는 사용자가 한번의 정보 입력으로 모든 상거래 서버와 거래를 할 수 있도록 구성 하였다.



[그림 2] SECURE CARD 인증모듈

Secure Card 설치는 사용자가 처음으로 M-Commerce를 이용할 때 안전한 거래를 위하여 전자 상거래 서버로부터 Secure Card 프로그램을 다운받아 설치한다. 인증모듈은 어플리케이션을 실행할 권한이 있는지를 결정하며 사용자는 설치후 인증코드를 설정하고 암·복호화 모듈에 의해 암호되 되어 저장된다. 거래정보 관리는 온라인 상에서 회원가입 또는 상거래 거래시 필요한 정보의 활용을 위해서 개인정보, 배송정보, 카드정보의 필수 항목을 관리한다. 개인정보에는 ID, 인증코드, 이름, 주민등록번호, E-mail 주소, 전화번호를 필수 항목으로 하여 사전에 입력 받는다.



[그림 3] 지불처리 Active X 모듈

배송정보와 카드정보는 다수의 데이터를 입력 받을 수 있어야 한다. 사용자들은 보통 최소 집, 회사 2개의 배송지를 사용하고 카드도 1개 이상을 사용하는 것이 일반적이다. 그리고 자신이 소유한 카드정보도 PDA에 설치한 Secure Card에 미리 암호화되어 저장한다.

사용자가 상품을 구매 요청하는 경우 서비스 제공자로부터 구매금액에 대한 정보를 전달받고 사용자는 자신의 배송정보, 카드정보를 선택할 수 있다. 구매금액은 Active X 컨트롤을 통해서 온라인 결제시 Secure Card로 전달되며 암·복호화 모듈에 의해서 배송정보와 카드정보가 암호화 된다. 최종적으로 전달되는 데이터는 구매금액, 배송정보, 카드정보이다.

3.2 Secure Card를 이용한 프로토콜

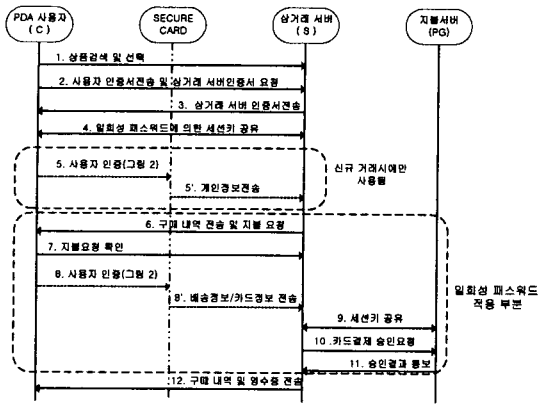
무선인터넷 환경에서 PDA에 기반한 신용카드 결제 시스템을 제안한다.

제안된 프로토콜 수행절차는 [그림 4]와 같고, 사용자는 신용카드를 발급 받을 때 비밀번호를 함께 등록한다. 비밀번호는 M-Commerce를 이용할 때 지불서버와 사용자의 비밀키로 사용되어진다. 사각형 점선 부분은 처음 거래하는 상거래 서버에서만 발생하게 된다.

제안한 프로토콜을 이용하여 전자 상거래를 한다면 종단간 보안, 기밀성, 인증, 무결성, 부인봉쇄 서비스 등을 제공받을 수 있다. 또한 사용자와 지불서버와의 종단간 보안이 가능하고, 무선 환경에 적합하게 정보 입력의 불편함을 해소하기 위하여 거래 정보를 PDA에 암호화하여 저장하였다.

종단간 보안은 [단계 8']와 [단계 10]에서 볼수 있듯이 사용자와 지불서버만이 공유하는 일회성 패스워드 비밀키로 암호화하여 상거래 서버에 전달되기 때문에

상거래 서버에서는 볼 수가 없고 사용자와 지불서버만이 신용카드 정보를 알 수가 있다.



[그림 4] Secure Card를 이용한 프로토콜

기밀성은 안전한 세션키 교환이 필수적인데 세션키 교환은 [단계 4]와 같이 일회성 패스워드를 사용한 세션키를 안전하게 교환한다. 이렇게 교환된 세션키를 이용하여 [단계 5]부터 전송되는 모든 데이터를 안전하게 암호화하여 다른 사용자의 도청으로 보호한다.

인증은 1차적으로 무선 단말기의 분실에 대비하여 [그림 2]와 같이 PDA 자체에서 일방향 함수를 이용하여 인증코드를 암호화하여 저장하고, 인증코드가 정확히 입력되었을 때 개인 정보를 볼 수가 있게 된다. 2차적으로 전자상거래시 거래정보를 전송하기 전에 인증코드 확인 절차를 거쳐 상거래 서버로 거래 정보를 전송하게 된다. 그리고 사용자와 상거래 서버간의 인증은 [단계 2]와 [단계 3]에서와 같이 신뢰된 인증기관으로부터 발부 받은 인증서를 서로 교환하여 서로 인증이 가능하다.

무결성은 거래 정보가 변경 되었을때 확인 할 수 있는 방법이다. 제안된 프로토콜에서는 중요 정보에 대하여만 해쉬 함수를 수행하여 불필요한 오버헤드를 줄였다. 즉, 신용카드 정보와 결제에 대한 데이터인 [단계 8], [단계 10], [단계 11], [단계 12]에서 해쉬 함수를 사용하였다.

부인봉쇄는 거래 정보를 개인키로 서명함으로써 이루어지는데 기존의 유선에서 사용하는 공개키 암호 시스템을 M-Commerce에서 사용하면 연산 속도가 오래 걸리는 단점이 있다. 제안된 프로토콜에서는 타원곡선 암호 시스템을 이용하여 M-Commerce에 적합한 서명을 하여 부인봉쇄 서비스를 제공한다. 또한 모든 거래 정보에 서명을 하지 않고 [단계 8], [단계 10], [단계 11], [단계 12]과 같은 중요한 데이터에만 서명을 함으로써 불필요한 오버헤드를 줄였다.

4. 결론

M-Commerce 환경에서 데이터 서비스를 원활하게 제공하면서 정보보호 기술을 만족하기 위해서는 안전한 전자상거래 시스템 설계가 중요하다. 일반 공개키 암호 시스템은 M-Commerce에 적합하지 않지만, 적은 비트 수와 빠른 계산 속도를 보장하는 타원곡선 공개키 암호 시스템으로 인하여 M-Commerce에서 공개키 암호시스템이 사용 가능하게 되었다. 제안된 프로토콜에서는 M-Commerce에 적합한 타원곡선 암호 시스템 및 일회성 패스워드 시스템을 이용하여 PDA 기반의 신용카드 결제 시스템을 설계하였다. 세션키 교환에서는 일회성 패스워드를 이용하였고, 타원곡선과 안전한 블록암호 알고리즘을 이용하여 거래 정보의 기밀성, 무결성, 인증, 부인봉쇄 서비스 등을 갖춘 안전한 M-Commerce 프로토콜을 설계하였다. 제안된 프로토콜의 장점은 PDA를 이용하여 거래를 할 때 정보 입력의 불편의성을 극복할 수 있게 설계 하였다. 또한 중요한 정보만을 선택적으로 전자 서명 및 해쉬 함수를 수행함으로써 불필요한 오버헤드를 줄였고 타임스탬프를 이용하여 재전송 공격으로부터 안전하다.

따라서 본 논문에서 제안된 프로토콜에 의해 PDA의 정보입력 인터페이스의 단점을 극복하고 이를 통해 신용카드 기반의 결제 서비스를 통한 무선 환경에서의 전자상거래 활성화에 기여할 수 있을 것으로 기대된다. 또한 다양한 형태의 지불시스템에서 원타임 패스워드를 적용하여 보다 안전한 시스템으로 발전시켜 나가는 방안에 대한 연구가 필요하다.

[참고문헌]

[1] J Davision 등 저, "Mobile E-Commerce : Market Strategies", Ovum, 2000.

[2] 무선인터넷 백서 편찬위원회, "무선 인터넷 백서 2001", 소프트뱅크 미디어, 2000.

[3] 소프트뱅크 리서치, "국내 모바일 결제 시장 현황 분석", 2002.

[4] "A One-Time Password System", rfc193.

[5] "일회용 패스워드 기술", http://www.kisa.or.kr/technology/sub4/password.htm