무선인터넷 환경에서 PDA기반 신용카드 결제 프로토콜 설계

이여진, 정일용
조선대학교 컴퓨터공학과

A Design of PDA-based Protocol for Credit Card Transaction on Wireless Internet

Yeijin Lee, Ilyong Chung
Dept. of Computer Science, Chosun University

요 약

M-Commerce에서 안전한 서비스를 제공하기 위해서는 보안 기능을 갖춘 결제 솔루션이 필수적이다. M-Commerce를 이용하기 위한 사용자의 이동 단말기는 핸드폰, PDA, 스마트폰 등으로 다양화 되어가고 있으며, 이 중에서도 PDA의 인터페이스와 이동 접속은 기존 핸드폰의 유선 인터넷의 정보 의존도가 높은 단점을 극복할 수 있다. 본 논문에서는 타원곡선 암호를 이용하여 PDA 기반의 신용카드 결제 시스템을 설계하였다. 제안된 시스템의 SECURE CARD 모듈은 PDA 단말기 자체에 개인정보, 배송정보, 카드정보를 암호화하여 안전하게 저장함으로써 단말기의 정보입력시에 필요한 불편함을 제거하였다. 또한 프로토콜은 M-Commerce에서 인증, 기밀성, 무결성, 부인봉쇄 서비스 등의 보안기능을 제공하도록 설계되었다.

1. 서 론

최근 이동통신망의 급속한 발전과 더불어 PDA 등 소형 정보 단말기의 보급 확대 및 고속데이터전송을 근간으로 하는 IMT-2000의 상용화가 국내뿐 아니라 세계적으로 확대되고 있다. 이러한 흐름에 따라 기존 개인용 컴퓨터 등의 고정 단말기를 기반으로 한 E-Commerce 형태를 벗어나 이제는 이동성(mobility), 휴대성(portability)를 제공하는 새로운 형태의 M-Commerce[1-3]가 보편화되고 있다. 이러한 M-Commerce에서 안전한 서비스를 위해서는 서비스의 특성에 알맞은 무선 결제서비스(Mobile Payment Service)[4]의 연구가 활발하게 진행되고 있다. 현재 무선결제 서비스는 이동통신사를 중심으로 소액결제 서비스가 주로 이루어지고 있으며, 현재 핸드폰 중심의 상거래는 무선 서비스 독자적인 경우보다는 사용자가 유선 상에서 자료를 보고 구매를 결정하는 유선 의존도가 높은 결제방식[5]이다. 이에 반하여 신용카드 기반의 결제구조는 고액결제가 가능하다는 강점을 가지고 있다. 그러나 신용카드 기반 결제구조는 무선 인터넷 인프라가 부족하여 무선결제 시스템에 취약하다는 문제점을 내포하고 있다. 따라서 무선기반 정보제공능력, 고액결제 서비스가 가능한 시스템이 요구된다.

현재 보안측면에서 RSA와 같은 공개키 암호 시스템은 유선상에서 우수한 보안도구로 여겨지고 있으나, 키 사이즈가 너무 크고 처리속도가 느리다는 단점이 있다[7]. 따라서 무선 환경의 낮은 CPU, 적은 메모리의 무선단말기에 적합하지 않은 것으로 판단되고 있다. 이를 보완하기 위해서 무선 단말기에 적합한 무선 공개키 기반구조(WPKI)[8-11]의 방향으로 연구가 진행되고 있고 적은 비트수와 빠른 계산 속도를 지원하는 ECC 공개키 암호 시스템[7, 12, 13]에 대한 관심이 증가되고 있다. ECC 공개키 암호 알고리즘의 장점은 첫째로, 다른 공개키 암호 시스템에 비해 가진 큰 장점은 키의 크기가 작다. 둘째로, 전형적인 RSA 시스템에서 사용되는 키의 크기는 1024비트이지만, 같은 보안 수준을 제공하는 ECC 시스템을 구현하기 위해서는 키의 크기가 160비트만 되더라도 충분하다. 셋째로, 계산적인 측면에서도 RSA에 비해 보다 낮은 비용을 요구함으로 많은 비용을 요구하는 소수의 분석과 같은 과정이 ECC에서는 필요치 않다. 넷째로, 소형기기나, 무선기기와 같은 제한된 성능의 시스템에서도 효율적으로 운용이 가능하다는 것이다[14].

본 연구에서는 현재 PDA 시장의 확대에 맞추어 소액결제

방식이 아닌 신용카드 기반의 안전한 고액결제 시스템을 ECC를 기반으로 설계하였다. 또한 모바일 환경을 고려하여 결제 편의성을 갖추도록 하였다.

2. 시스템 설계 및 구현

본 시스템은 무선 단말기 PDA를 이용하여 언제 어디서나 안전하게 농산물 구매가 가능하도록 전자상거래를 구축한다. 이때 개인 단말기라는 특징을 고려하여 보다 안전하고 효율적인 거래가 이루어질 수 있도록 시스템을 구축하였다. [그림 43]과 같이 본 시스템은 m-commerce 실현을 위한 상거래용 서버 역할을 하는 웹사이트, 인증에 관한 기능을 담당하는 인증서버, 실제로 구매를 하는 개인 사용자의 PDA 단말기로 구성되어 있다. 또한 본 시스템은 결재수단을 신용카드로 기본 가정한다. 이때 신용카드사의 지불게이트웨이와의 승인처리를 위한 통신에 대한 구현은 본 시스템에서는 이루어지지 않는다.

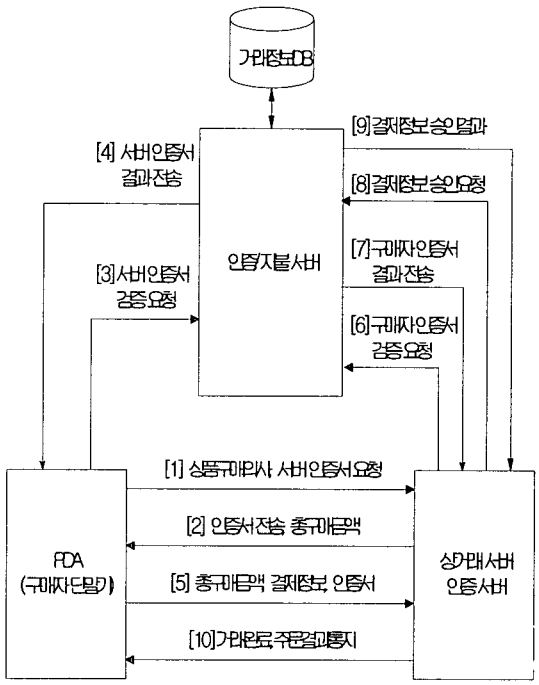
단말기를 이용하여 상거래 서버에 접속한 구매자는 회원가입 및 안전한 구매를 위해 SECURE CARD라는 별도의 프로그램을 다운로드를 받게 된다. SECURE CARD는 구매자에 대한 개인정보와 구매에 필요한 신용카드 정보등을 암호화하여 PDA에 저장함으로써, 개인 단말기라는 특수성을 고려한 시스템 구축이 이루어지게 한다.

SECURE CARD를 이용한 정보저장이 완료된 후 구매자는 원활한 전자상거래를 위해 회원가입을 한다. 회원가입 시 단말기에 저장되어 있던 개인정보를 이용하여 인증서버에 암호화된 형태로 전송되게 되며, 인증서버는 회원가입 절차를 수행한 후 인증서를 생성하여 구매자 단말기로 전송하여 인증서를 이용한 전자상거래 시스템을 구축하게 된다. 구매자는 구매하고자 하는 물품 목록을 선택한 후 지불요청을 수행하게 된다. 구매정보(물품, 가격, 배송정보 등) 등은 상거래 서버에 기록되며, 지불정보(금액, 카드정보)는 인증서버에 암호화된 형태로 전송되게 된다.

아래 그림은 본 연구에서 제안한 시스템의 전체 흐름도를 나타낸 것이다.

[단계 1,2] 사용자는 상품 검색 및 선택을 하여 인증서와 구매정보등의 내용을 상거래 서버와 공유된 키로 SECURE CARD를 이용하여 암호화하여 전송한다. 상거래 서버는 상품 내역을 복호화하고 상품 내역을 확인한다.
[단계 3,4] 인증서 서버는 사용자의 인증서를 검증한다.
[단계 5,6,7] 인증이 검증되면 상거래 서버와 공유한 키로 SECURE CARD를 이용하여 암호화한 개인정보를 전송한다. 상거래 서버는 키를 이용하여 개인 정보를 복호화하여 저장한다.

[단계 8,9] 상거래 서버는 사용자와 지불 게이트웨이와 공유된 비밀키로 암호화된 카드정보, 타임 스탬프를 상거래 서버와 지불 게이트웨이와 공유된 세션키로 암호화하여 전송한다. 카드 정보는 상거래 서버는 알지 못하고 사용자와 지불 게이트웨이만 볼 수 있도록 하였다. 이 단계는 본 연구에서는 기본 가정으로 설정한다. 지불 게이트웨이는 신용카드 회사등을 생각할 수 있다



가. 전자상거래 웹사이트

개인 무선 단말기를 통해 언제 어디서나 접근 가능한 농산물 전자상거래 구축을 한다. 즉, 유선환경과 무선환경의 조화와 함께 접근 용이성이 탁월한 m-commerce가 구축되게 된다. 이때 사용자 개인 단말기라는 특징을 고려하여 SECURE CARD라는 별도의 어플리케이션을 이용하여 개인 정보의 반복 입력의 불편함을 해소하며, 상거래 진행 시 입력되거나 저장되어 있는 정보들은 별도의 암호화의 과정을 통해 상거래 서버와 통신을 하게 된다.

전자상거래를 위한 홈페이지를 구축함으로써, 무선 단말기를 이용해 언제 어디서나 접근이 가능하게 된다.

나. 인증 서버

회원가입의 경우 가입을 위한 개인정보는 암호화과정을 통해 암호화되어 인증서버로 전송되게 된다. 인증서버는 사용자가 보내준 암호화된 정보를 복호화하여 데이터베이스에 저장한 후 이 정보를 이용하여 인증서를 생성하여 사용자에게 재전송하게 된다. 또한, 추후 이 사용자가 구매를 하고자 할 경우 신용카드 및 구매정보 역시 암호화된 형태로 인증서버로 전송되게 된다.

이 시스템은 신용카드 결재를 기반으로 하기 때문에, 카드회사와의 연계가 필요하지만, 본 연구수행 중에는 카드회사와의 연계의 어려움이 있으므로, 인증서버에서 결재정보를 수신한 후 카드회사의 프로토콜 형식에 맞는 데이터 전송이 이루어져 결재에 대한 승인이 이루어짐을 가정으로 한다.

다. SECURE CARD

PDA는 이동성이 강한 정보기기로 기존 유선상의 정보기기에 비하여 정보입력 작업이 원활하지 않은 입력 구조를 가지고 있다. 따라서 PDA기반의 결제 솔루션을 제공하는데 거론될 수 있는 문제가 사용자와의 인터페이스이다. 이동기기의 정보입력에 대한 불편함을 해결하고 안전한 결제 솔루션을 제공하기 위하여 SECURE CARD를 설계하였다.

SECURE CARD는 사용자가 정보를 입력하면 그 정보를 PDA에 저장하여 모든 상거래 서버와 거래할 때 사용할 수 있도록 구성하였다. 또한 PDA 분실시 개인정보 보호를 위해 입력된 정보는 안전한 블록 암호 알고리즘(대칭키 암호 알고리즘)을 이용하여 암호화하여 저장된다. 일반적으로 인증을 위해 대칭키 암호 알고리즘과 공개키 암호 알고리즘을 사용한다. 대칭키 암호 방식은 비밀키가 공유되었다는 전제를 바탕으로 인증 및 보안 서비스를 제공하지만, 인터넷과 같은 공개 네트워크 상에서는 사전에 안전하게 키를 분배하는 것이 매우 어렵기 때문에 공개키 암호 방식을 이용하기도 한다. 공개키 암호의 경우 대칭키 방식에 비해 시간이 오래 소요되는 단점이 있다.

본 연구에서는 PDA와 같은 무선단말기의 CPU나 밧데리 등의 한계를 고려하여 대칭키 암호 알고리즘을 이용한 암호화 과정을 수행하며, 암호키의 보호와 안전한 인증을 위해 타임 스탬프를 이용한 인증 절차를 수행한다.

본 연구에서 제안하는 SECURE CARD는 설치 모듈, 거래정보 관리 모듈, 암·복호화 모듈로 구성된다.

(1) SECURE CARD 설치 모듈

사용자는 안전한 거래를 위하여 m-commerce를 이용하고자 할 때 전자 상거래 서버로부터 SECURE CARD를 다운받아 설치하여야 한다. 한번 설치가 되면 SECURE CARD는 제휴된 모든 m-commerce 환경에서 사용이 가능하다.

(2) SECURE CARD 거래정보 관리 모듈

거래정보 관리는 온라인상에서 회원가입 또는 상거래 거래시 필요한 정보의 활용을 위해서 개인정보, 배송정보, 카드정보의 필수 항목을 관리한다. 개인정보에는 ID, 인증코드, 이름, 주민등록번호, E-mail 주소, 전화번호를 필수항목으로 하여 사전에 입력받는다. 사용자는 자신이 소유하고 있는 카드정보도 PDA에 미리 저장한다. 카드에 대한 필수항목은 카드번호, 유효기간(년, 월)으로 설정하였다.

SECURE CARD는 사용자로부터 입력받는 개인정보, 배송정보, 카드정보를 암호화하여 PDA에 저장하며 복호화 작업도 수행한다. 암·복호화 모듈은 다른 암·복호화 알고리즘을 추가적으로 확장할 수 있다. 암·복호화 모듈은 입력받은 개인정보, 배송정보, 카드정보를 사용자가 초기에 입력한 인증코드를 이용하여 암·복호화 기능을 수행한다.

라. Active X 모듈

홈페이지에 접속한 사용자는 원활한 물품구매를 위해 관련 모듈을 다운받아 개인 PDA에 등록하게 된다. 이때 등록한 Active X는 회원가입과 지불처리를 위한 모듈로 구성된다.

(1) 회원가입 Active X 모듈

홈페이지에서 회원가입 메뉴를 선택할 경우 Active X 모듈이 실행되게 되는데, 회원가입시 필요한 사용자 정보들은 SECURE CARD를 통해 PDA에 이미 저장되어 있던 개인정보들을 이용하게 되므로, 별도의 중복입력이 필요없게 된다. 이 모듈은 인증서버에 접속하여 가입정보들을 암호화하여 전송하여 주고, 인증 서버를 통해 인증서형식의 인증정보를 다운받게 된다. 추후 이 인증서는 지불처리시 이용되게 된다.

(2) 지불처리 Active X 모듈

사용자가 상품을 구매 요청하는 경우 서비스 제공자는

구매정보를 Active X 컨트롤을 이용하여 PDA 사용자의 SECURE CARD로 전송한다. PDA 사용자는 구매정보를 확인한 다음 자신의 배송정보, 카드정보를 선택하여 Active X 컨트롤을 이용하여 서비스 제공자의 SECURE CARD로 전송한다. 배송정보와 카드정보는 암·복호화 모듈에 의해서 암호화되어 전송된다. 상거래서버도 사용자에게 전달할 데이터가 있을 경우 사용자처럼 Active X 모듈을 이용하여 암호화하여 전송한다.

3. 결 론

M-Commerce 환경에서 데이터 서비스를 원활하게 제공하면서 정보보호 기술을 만족하기 위해서는 안전한 전자상거래 시스템 설계가 중요하다. 기존의 공개키 암호 시스템은 M-Commerce에 적합하지 않았지만, 적은 비트 수와 빠른 계산 속도를 보장하는 타원곡선 공개키 암호 시스템으로 인하여 M-Commerce에서 공개키 암호 시스템이 사용 가능하게 되었다. 제안된 프로토콜에서는 M-Commerce에 적합한 타원곡선 암호 시스템을 이용하여 PDA 기반의 신용카드 결제 시스템을 설계하였다. 세션키 교환에서는 Diffie-Hellman의 키 교환 기법을 이용하였고, 타원곡선 암호 알고리즘과 안전한 블록암호 알고리즘을 이용하여 거래 정보의 기밀성, 무결성, 인증, 부인봉쇄 서비스 등을 갖춘 안전한 M-Commerce 프로토콜을 설계하였다. 제안된 프로토콜의 장점은 종단간 보안이 가능하며, SSL에서 지원하지 않는 부인봉쇄 서비스를 지원한다. 또한 PDA를 이용하여 거래를 할 때 정보 입력의 불편의성을 극복할 수 있게 설계하였고, 단말기 분실시 개인정보를 보호하기 위해여 인증 모듈이 1차 사용자 인증을 하고, M-Commerce시 다시 2차 인증을 한다. 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 극복할 수 있고, 안전한 M-Commerce가 가능하게 설계되었다. 이를 통해 신용카드 결제 서비스의 모바일 전자상거래 활성화에 기여할 수 있을 것으로 기대된다.

참 고 문 헌

[1] 이재규 외 3인, "전자상거래원론", 범영사, 2000.

[2] Nam-Je Park, You-Jin Song, "M-Commerce Security Platform based on WTLS and J2ME," ISIE2001, 2001.

[3] Lyytinen, K., "M-commerce - mobile commerce : a new frontier for E-business," Proceedings of the 34th Annual Hawaii International Conference on System Sciences, 2001.

[4] 김선형 외 2인, "이동 통신 시스템에서의 효율적인 소액 지불 기법", 춘계학술발표논문집, 한국정보과학회, 2002.

[5] 임수철 외 3인, "M-Commerce를 위한 고액 지불 시스템", 춘계학술발표논문집, 한국정보처리학회, 2002.

[6] Forrester Research, "Mobile Payment's Slow Start," May, 2001.

[7] H. X. Nel, Doris Baker, "보안과 암호화 모든 것", 인포북, 2001.

[8] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems," ESORICS, LNCS 1485, 1998.

[9] Wireless Application Protocol Wireless Transport Layer Security, WAP Forum, April, 2001.

[10] Wireless Application Protocol Public Key Infrastructure Definition, WAP Forum, Oct., 2000.

[11] 정여석, 김수진, 서인석, 서상원, 원동호, "무선 PKI 기술 및 서비스 동향에 관한 연구", 한국정보처리학회 추계학술발표대회, 한국정보처리학회, 2002.

[12] 최용락 외 3인 공역, "컴퓨터 통신 보안", 도서출판 그린, 20001.

[13] M. Aydos, B. Sunar and C. K. Koc., "An elliptic curve cryptography based authentication and key agreement protocol for wireless communication," end International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, Texas, October, 1998.

[14] 무선인터넷백서 편찬위원회, "무선인터넷 백서", 소프트뱅크 미디어, 2000.

[15] http://www.kisa.or.kr, 한국정보보호진흥원.

[16] 임수철, 강상승, 이병래, 김태윤, "무선인터넷에서의 종단간 보안을 제공하는 신용카드 기반의 지불 프로토콜", 한국정보과학회논문지, 한국정보과학회, 2002.

[17] Eun-Kyeong Kwon, Yong-Gu Cho, Ki-Joon Chae, "Integrated transport layer security : end-to-end security model between WTLS and TLS," Proceedings of the 15th International Conference on Information Networking, 2001.

[18] A. Freier, P. Karlton, P. Kocher, "The SSL Protocol version 3.0," Internet Draft, Nov., 1996.

[19] 유성진, 김성열, 정일용, "안전한 통신서비스를 제공하는 향상된 SSL기반 정보보호 시스템의 설계", 한국통신학회논문지, 한국통신학회, 2000.

[20] 박지철, 한명진, 이경현, "Session Resume의 기한 연장을 이용한 SSL/TLS Handshake 프로토콜의 성능개선", 한국정보과학회 추계학술발표대회, 한국정보과학회, 2002.

[21] 최진규, 이헌길, "WAP환경에서 안전한 종단간 보안을 제공하는 TLS-Plus 프로토콜", 한국정보과학회 춘계학술발표대회, 한국정보과학회, 2002.