WAP기반 무선 인터넷 전사상거래 시스템에서 신용카드 결재를 위한 보안 프로토콜 설계

최애라*, 유성진**,김성열***, 정일용****
* ** ****조선대학교 전자계산학과
***울산과학대학 컴퓨터정보학부
e-mail:wwwpda@korea.com
tiger@stmail.chosun.ac.kr,

Secure Protocol for Credit card Approval Process in the Domain of M-Commerce Based on WAP

Ae-ra Choi*, Seong-Jin You**, Seong-Yeol Kim***,
Il-Yong Chung****
* ** ****Dept. of computer science, Chosun University
***School of Computer Information, Ulsan College

요약

유선인터넷의 공간제약성을 극복하고, 더 빠르고 이동성을 요구하는 사용자들에 의해 M-Commerce가 등장하였다. M-Commerce에서 상품이나 서비스를 제공받기 위하여 고객과 판매자는 이동컴퓨팅 단말을 통하여 정보를 교환한다. 그러나 무선통신 환경에서는 정보 누출의 위험이 항상 잠재적으로 내포되어 있으므로 데이터 서비스가 원활하게 제공되기 위해서는 정보보호가 반드시 선결되어야 한다. 이를 위하여 본 연구에서는 무선인터넷 환경 솔루션을 기반으로 하여 데이터 서비스를 원활하게 제공하면서 데이터의 비밀성, 무결성, 인증 메카니즘, 부인봉쇄 서비스 등 기본적인 정보보호 서비스를 갖춘 안전한 M-Commerce 시스템을 설계하고자 한다.

1. 서 론

개인의 정보통신에 대한 수요가 증가하면서 음성 위주의 무선통신은 인터넷 지원이 가능한 데이터 중심의 무선통신으로 빠르게 전환하고 있어 무선통신 환경에서 전자상거래를 비롯한 데이터 서비스의 제공이 미래 정보통신산업의 핵심이 될 것으로 예측된다. 이와 같이 무선 데이터 서비스에 대한 중요성이 강조되고 있는 가운데, 여러 가지 다양한 무선인터넷 솔루션이 개발되고 있으며 무선인터넷 솔루션은 WAP 기반과 HTTP 기반 구조로 구분되고 있다. 이러한 환경 속에서 여러 매체나 보도를 통해 쉽게 접하는 용어 중의 하나가 바로 무선인터넷 전자상거래(M-Commerce)이다. 이런 M-Commerce는 휴대용 무선기기를 사용한 모든 인터넷 비즈니스를 통칭하는 말로써 구매자와 판매자의 정보를 통하여 각각이 필요로 하는 상품이나 서비스를 이동 컴퓨팅 단말을 통하여 연결시켜 주는 서비스이다. 유선 인터넷의 공간 제약성이라는 한계를 극복하고 나날이 다양하게 변화하는 소비자들의 욕구를 반영하며, 더 빠르고 이동성까지 요구하는 것에 의해 M-Commerce가 등장하게 된 것이다.

이에 본 연구에서는 무선인터넷의 전반적인 기술 동향과 무선 인터넷에서 정보보호 서비스를 제공하기 위해서 기존 유선 인터넷에서 가장 많이 사용되고 있는 보안 프로토콜인 SSL에 대해서 살펴보고, 현재 전자상거래 시스템에서 가장 많은 결재 방법으로 사용되고 있는 신용카드 결재 방법은 당분간 M-commerce 에서도 이용되어 질 것으로 보인다. 따라서 본 논문에서는 M-commerce환경에서 결재 기반 시스템의 보호를 위한 연구를 진행하였다.

2. 모바일 컴퓨팅과 무선인터넷

2.1 모바일 컴퓨팅

우리나라의 경우 현재, 무선통신 서비스의 가입자 수는 1500만명, PCS의 가입자수는 1200만명 정도이다. 이것은 국민 2명중 1명이 무선통신 서비스를 이용하고 있는 것으로 이동전화나 PCS를 포함한 모바일 데이터통신 서비스 시장 규모도 크게 늘어날 것이다. 앞으로 무선데이터통신 구매자들은 이동 전화만으로도 사이버쇼핑, 주식매매, 각종 생활정보를 접할 수 있게 되고 나아가 무선 전자상거래, 무선 인트라넷도 쉽게 사용할 수 있게 된다.

2.2 무선인터넷

1969년 인터넷이 시작되어, 1992년에 WWW서비스로 인터넷은 유선세계에서 급속히 보급 확산되었다. 인터넷이 무선세계에서 전자메일 등을 이용하여 정보를 엑세스하는 것은 주로 IP(Internet Protocol) 기반의 통신방식에 의해서 이루어지고 있는데, 휴대전화의 디지털화와 PHS의 출현에 의해 이동 중 데이터통신의 가능성이 커졌고 모바일 컴퓨팅 개념의 등장으로 무선통신과 휴대 정보터미널의 유기적인 결합이 더욱 강화되고 있다. 1999년 휴대전화로 인터넷을 통한 web액세스, 전자메일, 온라인 상거래 등이 가능한 서비스가 시작되었고, 2000년 IMT-2000통신에 의해, 고속화와 멀티미디어화, 인터넷을 통한 서비스의 확산과 고도화를 지향하는 새로운 발전이 예견되고 있다.[1][2]

3. 보안 메카니즘

3.1 SSL

SSL은 웹 브라우저 개발로 이미 잘 알려져 있는 Netscape 사에서 1994년에 제안하였으며, 자사의 웹 어플리케이션에 처음으로 구현함으로써 현재 웹 보안의 대명사로 알려져 있는 보안 프로토콜이다. 현재 버전 3.0까지 개발되어 있는 상태이며, Netscape, Internet Explorer와 같은 브라우저에서 널리 사용되고 있다.

3.2 무선 인터넷에서의 SSL

ME나 i-mode와 같이 HTTP를 기반으로 하는 무선 인터넷 솔루션에서 정보보호 서비스를 제공하기 위해서 가장 간단한 방법은 [그림 1]과 같이 SSL을 이용하는 것이다.

[그림 1] 무선 인터넷에서 SSL

3.3 WAP 보안 메카니즘

국제적으로 WAP 정의를 위해 표준화 기구인 WAP포럼이 설립되어 표준화 작업이 진행되고 있다. WAP 포럼은 1997년에 Nokia, Motorola, Ericsson, Unwired Planet (현재의 Phone.com) 등 4개의 단말기 업체를 중심으로 구성되었으며, 현재 약 200여 개의 업체가 참여 중이다. WAP Forum에서는 기존 TCP/IP와는 별도의 무선 환경에 적합한 프로토콜을 정의하는 작업을 진행중인데, 이 가운데 보안 프로토콜이 WTLS이다[3][4].

3.4 SET(Secure Electronic Transaction)

SET은 현실세계의 신용카드 거래를 기반으로 모델링되어 기존의 금융 시스템과 연동이 쉬운 구조로써 구매자(Cardholder), 상인(Merchant), 상인은행(Acquirer), 카드 발행처(Issuer:은행 또는 카드회사), 인증국(CA), 지불 게이트웨이(Payment gateway)로 구성된다[5][6].

4. 보안프로토콜 MoBill(Mobile+Bill)설계

4.1 MoBill 프로토콜 표기

무선인터넷 환경에서 안전하게 신용카드를 이용하여 결재할 수 있는 보안 프로토콜을 제안한다. 제안하는 프로토콜 표기법은 [표 1]와 같다.

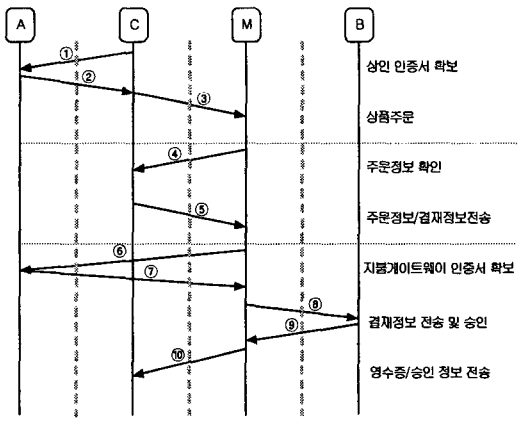
[표 2] 프로토콜 표기

표 기	의 미
A	인증국(Authentication Server)
B	금융기관-지불게이트웨이(Banking organ)
C	구매자 (Customer)
M	판매자 (Merchant)
I_{pk}	I의 공개키
I_{sk}	I의 비밀키
S_{key}	B와 C의 공통키
$E_k(m)$	키 k로 메시지 m을 암호화
CA[I]	I의 인증서, 인증서 유효기간, 아이디, I의 공개 키가 인증기관에 의해 서명된 정보
ToV	유효기간 (a Term of Validity)
Request-M	주문요구메시지
Accept-M	구매지불요구메시지
Inf-M	판매자에 대한 구매지불요구의 이중서명정보
Inf-B	은행에 대한 구매지불요구의 이중서명정보
Recog-M	판매자에게 결재가 승인되었음을 알리는 메시지
Inf-Recog	구매자에게 주는 결재승인정보
Amount	판매자가 발급하는 영수증

4.2 MoBill 프로토콜 수행절차

[그림 2]은 구성요소간 트랜잭션 단계를 나타낸 것이다. 상품을 검색한 구매자는 판매자의 신뢰성을 확인하기 위하

여 ①②단계를 통해 판매자의 인증서를 확인한다. 판매자의 신뢰성이 확인되면 주문요구메시지를 전달한다(③). 주문을 확인한 판매자를 구매자의 인증서를 확인한 후 지불요구메시지를 전송한다(④). 지불요구메시지를 확인한 구매자는 자신의 결재 정보를 전송한다(⑤). ⑥⑦단계에서 지불게이트웨이의 인증서를 확보한 후 결재정보를 전송한다(⑧). 판매자의 인증서를 확인한 지불게이트웨이는 결재승인정보를 전송한다(⑨). 판매자는 거래가 정상적으로 수행되었음을 뜻하는 영수증과 결재승인내역을 구매자에게 전달한다(⑩).



[그림 2] MoBill 프로토콜 수행절차

[1단계] C → A : $E_{A_{pk}}(C, M, E_{C_{sk}}(C, M))$

[2단계] A → C : $E_{C_{pk}}(ToV, ID_M, M_{pk}, CA[M])$

[3단계] C → M : $E_{M_{pk}}(Request-M, CA[C])$

[4단계] M → C : $E_{C_{pk}}(Request-M, Accept-M, E_{M_{sk}}(Request-M, Accept-M))$

[5단계] C → M : $E_{M_{pk}}(Inf-M, E_{S_{key}}(Inf-B))$

$PI = MobilePI + 결재금액 + 카드비밀번호$

$OI = 품명 + 수량 + 가격 + 결제금액$

$Inf-M = (OI, H(PI), E_{C_{sk}}(H(OI)|H(PI))$

$Inf-B = (PI, H(OI), E_{C_{sk}}(H(OI)|H(PI))$

[6단계] M → A : $E_{A_{pk}}(M, B, E_{M_{sk}}(M, B))$

[7단계] A → M : $E_{M_{pk}}(ToV, ID_B, B_{pk}, CA[B])$

[8단계] M → B :

$E_{B_{pk}}(ToV, ID_M, M_{pk}, CA[C], CA[M], E_{S_{key}}(Inf-B))$

[9단계] B → M :

$E_{M_{pk}}(Recog-M, E_{B_{sk}}(Recog-M), E_{S_{key}}(Inf-Recog))$

[10단계] M → C :

$E_{C_{pk}}(Amount, E_{M_{sk}}(Amount), E_{S_{key}}(Inf-Recog))$

4.3 프로토콜 분석

정보의 안전한 송수신을 위하여 구매자는 카드발행처에 자신의 주민번호, 비밀번호, 이동단말의 번호 등을 등록하고 신용카드를 발급 받는다. 발급된 신용카드에는 카드번호와 유효기간을 포함한다. 이 정보를 자신의 이동단말(PDA 등)에 등록한다.

이동단말의 카드등록 프로그램을 실행하여 카드번호, 유효기간, 주민번호를 등록한다. 카드등록 프로그램은 입력된 정보에 단말의 Phone-No를 추가하여 금융기관 지불게이트웨이의 공개키 B_{pk}로 암호화하여 이동단말의 기억장치에 MobilePI를 저장한다.

이때 신용카드의 비밀번호는 저장하지 않도록 한다. 따라서 이동단말의 분실시 자체적 인증과정에 의해서 이동단말의 불법적 사용을 막을 수 있을 뿐만 아니라 신용카드 정보에 대한 사용이 불가능하도록 한다.

공개키 암호화 방식과 공통키 암호화 방식을 사용하여 각 참여자간의 사용자 인증을 위해 인증서버로부터 전자인증서를 발부 받아 정보 송수신시 서로 교환하도록 하였다. 그리고 카드사용자인 구매자의 거래절차를 좀더 단축시키기 위하여 구매 요청시 구매자는 구매요청서에 자신의 전자 인증서를 첨부하여 보내고 판매자는 인증서버에 의존하지 않고도 거래상대자인 구매자를 인증할 수 있게 하였다. 또한 거래시 각 정보는 참여자의 공개키로 암호화하여 보냄으로 전자상거래 분쟁 해결기능으로서 부인봉쇄 서비스를 하고 카드사용자인 구매자가 주문정보 및 지불정보 보안을 위해 은행과 공통키 암호화 방식을 사용하여 이중서명(Dual signature)으로 안전한 정보 전송시 보다 안전하고 거래 절차를 최소화하도록 하였다. 그리고 이중서명은 전송되는 지불정보를 중간에서 악의의 제3자가 대체하거나 바꾸거나 할 수 없도록 하면서 동시에 판매자는 지불에 관한 정보를 모르도록 보안을 유지하고 은행은 구매에 관한 정보를 모르도록 하여 판매자에 대해서는 지불정보의 투명성을 은행에 대해서는 구매정보의 투명성을 제공한다. 결론적으로 전자상거래 문제점인 부인봉쇄, 무결성, 투명성, 기밀성 제공으로 보다 안전한 거래가 될 수 있도록 설계하였으며 전자상거래 각 참여자들의 인증국 조회 횟수 단축으로 트랜잭션 비용이 감소될 수 있도록 하였다.

5. 결론

현재 전자상거래 시스템에서 가장 많은 결재 방법으로 사용되고 있는 신용카드 결재는 당분간 M-commerce에서도 이용되어 질 것으로 보인다. 결국 신용카드 결재 기반 시스템의 보호를 위한 SET

의 사용이 필요할 것이다. 하지만 현재 M-commerce에 적용된 SET은 언급되고 있지 않다. 따라서 본 논문에서는 SET을 적용한 M-commerce에서의 결재시스템을 설계하였다.

무선 인터넷 환경 솔루션을 기반으로 하여 데이터 서비스를 원활하게 제공하면서 정보보호 기술을 만족하는 안전한 전자상거래 시스템 구현이 중요하다. 이를 위하여 본 연구에서는 데이터의 비밀성, 무결성, 인증 메카니즘, 부인봉쇄 서비스 등 기본적인 정보보호 서비스를 갖춘 안전한 M-Commerce 시스템을 설계하였다.

6. 참고문헌

[1] 강철희 · 이재기 · 정제창 · 한치문: 일본 멀티미디어 통신연구회:「모바일 컴퓨팅」 교보문고, pp.2~32. pp.121~144, 2001.

[2] 좌정우 · 박성주:"한국통신 프리텔 n016 persnet 서비스 구축 경험" 「한국정보처리학회지」제7권, 제3호: pp.72~77, 2000.

[3] 탁성우 · 임신영 · 박창순 · 김태윤 : "전자거래 사용자 보안 서비스 요구 사항 사항 분석 및 설계", 「한국정보처리학회 춘계 학술발표 논문집」 제4권 제1호, pp.670~671, 1997.

[4] 서병기 · 김태연:"WAP 환경에서의 안전한 키 분배 프로토콜" 「한국정보처리학회 추계학술발표대회」제8권 제2호, pp.985~988, 2001.

[5] 김대송 · 김화진 · 윤채원 · 정승원 · 이강복: LG-EDS 시스템 아이엔텍팀 「무선 인터넷 어플리케이션 프로그래밍」삼양출판사, pp.24~53, 2000.

[6] 정승용:"전자상거래의 새로운 패러다임"「한국정보처리학회지」제7권, 제1호: pp.45~48, 2000.