M-Commerce환경의 보안 메커니즘 설계

최애라*, 유성진*, 김성열°, 정일용*
조선대학교 전자계산학과*, 울산과학대학 컴퓨터정보학부°

Design of Secure Mechanism In M-Commerce Environment

Ae-ra Choi*, Seong-Jin You*, Seong-Yeol Kim°, Il-Yong Chung*
*Dept. of computer science, Chosun University
°School of Computer Information, Ulsan College
E-mail : wwwpda@korea.com, tiger@stmail.chosun.ac.kr,
sykim@mina.chosun.ac.kr, iyc@mail.chosun.ac.kr

요 약

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 것이다. 이러한 환경 속에서 주요 이슈가 되고 있다. 그러나 무선통신 환경에서 데이터 서비스가 원활하게 제공되기 위해서는 인터넷에서와 마찬가지로 정보보호 문제가 반드시 선결되어야 한다. 이를 위하여 본 연구에서는 데이터의 비밀성, 무결성, 인증 메카니즘, 부인봉쇄 서비스 등의 정보보호 서비스를 제공하면서 무선인터넷 단말기에 편리한 인터페이스를 제공하는 안전한 M-Commerce 시스템을 제안 하였다.

1. 서론

인터넷이 우리의 생활 속에 자리한 지 7년여가 된 지금, 인터넷은 우리 주변의 모든 것을 바꾸어 놓고 있다. 그중 실생활의 상거래 환경에서 전자적으로 구현한 전자상거래로 기대와 관심이 모아지고 있다. 일반적으로 전자상거래는 기업, 개인, 정부 등 경제 주체들이 인터넷과 같은 네트워크 환경에서 전자매체를 이용하여 수행하는 상품이나 서비스의 거래뿐만 아니라 거래에 수반되는 제반 경제 활동으로 정의된다. 전자상거래는 기업내 또는 기업간 업무의 효율성과 투명성을 높일 뿐만 아니라 시간적, 공간적 제약을 극복할 수 있어 전세계적으로 기업, 개인, 정부 등 모든 경제 주체의 주목을 받고 있다.

또한 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.

어느 쪽이 시장에서 성공을 거둘지는 현재 가늠할 수 없으나 이미 포화 상태에 가까운 유선 인터넷의 한계를 파악하고 새로운 무선 인터넷 시장을 선점하기 위해 전세계 모든 이동통신회사, 단말기 제조회사, 소프트웨어 회사, 컨텐츠 제공회사들이 앞 다투어 무선 인터넷에 투자하고 있다[1].

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. 상거래 시스템의 주체로 떠오른 인터넷 전자상거래가 무선인터넷 시스템으로 진화하고 있는 것이다[2].

그러나 무선통신 환경에서 데이터 서비스가 원활하게 제공되기 위해서는 인터넷에서와 마찬가지로 정보보호 문제가 반드시 선결되어야 할 과제로 여겨지고 있다.

이에 본 연구에서는 무선인터넷의 전반적인 기술동향에 대하여 살펴보고, 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 무선 인터넷

2.1 모바일 컴퓨팅

우리나라의 경우 현재, 무선통신 서비스의 가입자수는 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].

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[3].

2.2 무선 인터넷

무선인터넷 솔루션은 [표 1]과 같이 크게 2가지 분류로 구분할 수 있다. 기존 유선인터넷에서의 프로토콜인 HTTP에 기반해서 무선 데이터 서비스를 제공하는 경우와, 다른 하나는 무선 네트웍 환경에 적합한 새로운 프로토콜을 개발하여 무선 데이터 서비스를 제공하는 방법이다.

[표 1] 주요 무선 인터넷 솔루션

구 분	WAP 기반	HTTP 기반	
		ME	i-mode
개발 주도 업체	WAP forum	Microsoft	NTT Docomo
컨텐츠 기술언어	WML	m-HTML	c-HTML
전송 프로토콜	WSP WTP WDP	HTTP	HTTP
단말기 브라우저	WAP 브라우저	Mobile Explorer	Compact NetFront
보안 메카니즘	WTLS	SSL	SSL

3. 보안 메커니즘

3.1 SSL(Secure Socket Layer)

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.

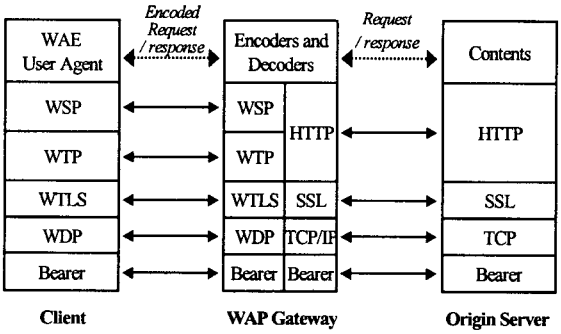
[그림 1] 무선 인터넷에서 SSL

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

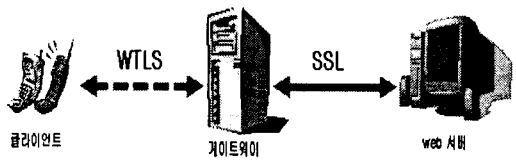
정의하는 작업을 진행중인데, 이 가운데 보안 프로토콜이 WTLS이다[4][5].

WAP 모델에서는 휴대 단말기와 인터넷 서버 사이에 WAP Gateway를 두고 있다. WAP Gateway의 주요 역할은 WAP 프로토콜과 인터넷 TCP/IP 프로토콜을 중간에서 변환해 주는 것이다. 다시 말하면, 모든 휴대 단말기의 인터넷 서비스 요구는 WAP Gateway를 거치도록 되어 있고, WAP Gateway는 프로토콜에 따라 요청 받은 서비스를 기존 인터넷 유선망을 통해 다시 서비스를 요청한다. 이어서 WAP Gateway가 인터넷 서버로부터 응답을 받고 다시 서비스를 최초 요청했던 휴대 단말기에게 WAP 프로토콜로 전송함으로서 모든 과정이 이루어진다. [그림2]는 WAP게이트웨이의 계층 구조를 나타낸 것이다.



[그림 2] WAP 게이트웨이

이러한 WAP 게이트웨이는 웹서버 측에서 전달되는 SSL을 해독하고, 데이터를 WAP 단말기로 전달하기 전에 WTLS를 이용하여 다시 데이터를 암호화한다. 즉, WAP 서비스를 위해서는 중간의 게이트웨이를 거쳐야 하는데 WTLS로 암호화된 데이터는 WAP 게이트웨이에서 복호화된 후 SSL로 암호화되어 서버에 전달되고, 반대로 SSL로 암호화된 데이터는 게이트웨이에서 복호화된 후 WTLS로 다시 암호화되어 단말기에 전달되는 것이다. [그림 3]은 이 구조를 나타낸 것이다.



[그림 3] WAP 보안 구조

4. 보안메커니즘 MoBill(Mobile+Bill) 설계

4.1 MoBill 프로토콜 표기

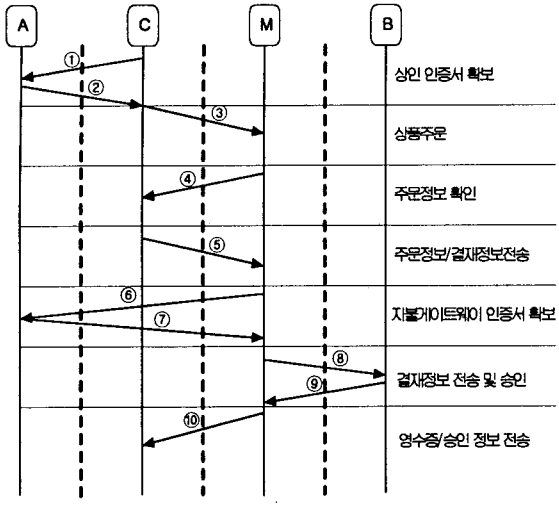
무선인터넷 환경에서 안전하게 신용카드를 이용하여 결재할 수 있는 보안 프로토콜을 제안한다. 제안하는 프로토콜 표기법은 [표 2]와 같다.

[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 4]은 구성요소간 트랜잭션 단계를 나타낸 것이다. 상품을 검색한 구매자는 판매자의 신뢰성을 확인하기 위하여 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)[7][8].



[그림 4] 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 : $E_{M_{pk}}(Inf-M, E_{S_{key}}(Inf-B))$

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

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

PI = MobilePI + 결재금액 + 카드비밀번호

OI = 품명 + 수량 + 가격 + 결제금액

[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, 이동단말기의 번호 등을 등록하고 신용카드를 발급 받는다. 발급된 신용카드에는 카드번호와 유효기간을 포함한다. 이 정보를 자신의 이동단말기(PDA 등)에 등록한다.

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

이때 신용카드의 비밀번호는 저장하지 않도록 한다. 따라서 이동단말기의 분실시 자체적 인증과정에 의해서 이동단말기의 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

무선 인터넷 단말기를 한 사람이 한 대씩 가지게 되는 보급 상황과 항상 휴대한다는 것을 감안할 때, 인터넷 휴대폰은 원투원(One to One) 마케팅을 실현하는 가장 좋은 도구가 될것이다.

그러나 M-commerce에서는 정보 누출의 위험이 항상 잠재적으로 내포되어 있으므로 상황에 맞는 적절

한 보안 시스템을 구축하여야 한다.

본 논문에서는 별도의 추가적인 하드웨어 비용의 소용없이 암호학적 보안 기술을 이용하여 소프트웨어적인 방법으로 구현 가능한 M-Commerce보안 메커니즘을 제안 하였다.

제안된 시스템은 현재 전자상거래 시스템에서 가장 많은 결재방법으로 사용되고 있는 신용카드 방법을 기반으로 하고 있다. 따라서 이동 단말기의 특성을 고려하여 이동 단말기에 개인 데이터를 암호화하여 저장함으로써 전자상거래에서 매번 발생하는 정보 입력의 번거로움을 해결 하였다. 메커니즘은 데이터의 비밀성, 무결성, 인증 메커니즘, 부인봉쇄 서비스 등의 보안 서비스를 만족한다.

[참고문헌]

[1] 남궁정 · 김기천:"이동 인터넷과 무선 액세스 기술 동향" 「한국정보처리학회지」 제7권 제1호, pp.71~78, 2000.

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

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

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

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

[6] 이정은 · 이종렬 · 노강래 · 신동일 · 신동규: "WAP 게이트웨이의 유/무선 프로토콜 변환 기능에 대한 설계 및 구현" 「한국정보처리학회 추계학술발표대회」 제8권 제2호, pp.1549~1552, 2001.

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

[8] 이병래 · 강상승 · 김태윤:"이동 사용자를 위한 인증 및 키교환 프로토콜" 「한국정보처리학회 추계학술발표대회」 제8권 제2호, pp.1237~1240, 2001.