상호 인증을 보장하는 이동단말기를 이용한 지불 모델

임수철° 이병래 김태윤
고려대학교 컴퓨터학과
{causal, brlee, tykim}@netlab.korea.ac.kr

Secure Payment model using Mobile device assuring mutual entity authentication

Soo-Chul Lim°, Byung-Rae Lee, Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University.

요 약

이동단말기의 보급률이 높아짐에 따라 이를 이용한 지불 시스템이 제시되었고, 현재 서비스를 제공중에 있다. 이동단말기를 이용한 지불 시스템은 폭넓은 이동통신 보급률, 편리함, 간편함, 후불결제와 같은 장점들을 가지고 있다. 그러나 사용자는 서비스 제공자가 신뢰할 수 있는 서비스/물품 제공자인지 알 수 없다는 단점을 가지고 있다. 본 문에서는 이러한 단점을 극복하기 위해서 Diffie-Hellman 키 합의 프로토콜을 이용하여 상호 인증을 보장하는 지불 시스템을 제안한다.

1. 서 론

인터넷의 급속한 성장과 이를 바탕으로 한 전자상거래가 급속하게 발전하고 시장이 커짐에 따라, 전자상거래에서 이슈가 되고 있는 지불과 보안에 많은 연구가 진행 중에 있다.

이런 연구를 바탕으로 하여 제안된 지불 시스템에는 전자현금, 신용카드-기반, 전자수표 및 소액 지불 시스템이 있다[1].

이러한 지불 시스템 중에서 최근에 이슈화되고 있는 지불 시스템이 이동단말기를 이용한 지불 시스템이다. 이 시스템은 지불의 매체로 이동단말기를 사용한 것이다. 이 시스템의 장점은 폭 넓은 이동 통신 보급률로 인해 시스템을 이용할 수 있는 잠재적인 사용자들이 많다는 것과 후불제 방식으로 인해 사용자의 부담감을 줄일 수 있다는 것이다.

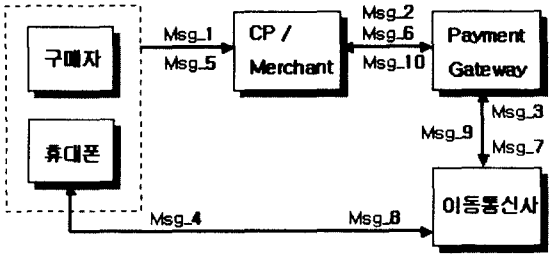
하지만, 무선이라는 환경으로 인해 유선 환경보다 보안에 많은 허점을 가지고 있다. 이러한 문제를 해결하기 위한 방법으로 암호학을 이용한 해결 방법들이 제시되고 있다.

현재 제공되고 있는 이동단말기를 이용한 지불 시스템은 보안에 많은 관심을 기울였으나, 서비스 받으려는 사용자가 서비스제공자가 진실한 제공자인지를 확인 할 수 없다는 단점을 가지고 있다. 이런 단점은 사용자와 제공자사이의 상호 인증을 제공하는 것으로 극복할 수가 있다.

따라서 본 논문에서는 상호 인증을 제공하는 안전한 이동단말기를 이용한 지불 시스템을 제안하고자 한다.

2. 휴대폰을 이용한 지불 모델

휴대폰을 이용하여 제안한 지불모델은 <그림 1>과 같다. 위 모델은 현재 Impay와 Teledit과 같은 컨텐츠 제공 Site에서 사용중인 지불 모델이다[2, 3, 4].



<그림 1>휴대폰을 이용한 지불시스템 모델

이 모델에서 사용한 메시지는 아래와 같다.

Msg_1 - 구매고객이 인터넷을 통해 CP/Merchant에 접속하여 구매의사 표시.

Msg_2 - CP/Merchant는 이동전화번호와 주민번호 및 거래내역을 Payment Gateway(PG)에 전송.

Msg_3 - PG는 이동통신사에 고객 인증 요청과 함께 거래암호를 생성하여 전송.

Msg_4 - 이동전화사가 고객 인증 후 구매고객에게 거래암호 전송.

Msg_5,6 - 구매고객이 거래암호를 입력하면 CP/Merchant는 PG의 거래승인을 받은 후 과금 정보를 생성하여 전송.

Msg_7 - PG는 CP/Merchant로부터 전송 받은 과금 정보를 저

장한 후 이동통신사에 전송.

Msg_8,9 - 이동전화는 구매고객의 이동전화 요금청구서에 결제대금을 통합하여 청구 수납한 후 CP/Merchant에게 대금 정산.

위의 모델은 CP/Merchant가 구매자에게 이동전화번호와 주민번호를 제시받는 방법을 통해서 지불능력이 없는 구매자나 거래에 부적합한 구매자를 CP/Merchant가 PG를 통해서 선별할 수 있게 이동통신사에 확인을 한다. 이로써 CP/Merchant는 구매자를 신뢰할 수 있게된다. 구매자는 이동통신사에서 거래 암호를 전송 받는 것으로 거래승인을 받는다.

그러나 이 모델에서는 구매자가 정당한 CP/Merchant와 거래를 하고 있음을 신뢰할 수 없다는 단점이 있다. 또한 위 모델은 구매자가 물품/서비스를 구매하기 위해서는 항상 인터넷에 접속해야만 한다는 제약성을 가지고 있다.

3. 종단간 인증을 제공하는 지불 모델 제안

3.1 Diffie-Hellman 기반 종단간 인증

사용자와 서비스제공업체가 상대방의 정당함을 신뢰하게 하기 위해서는 상호 인증을 제공해야 한다.

본 문에서는 Diffie-Hellman 기반 키 합의 프로토콜을 사용하여 상호 인증 프로토콜을 제안한다[6, 7, 8].

아래의 인증 프로토콜은 사용자가 소유하고 있는 이동 단말기와 서비스 제공업체간에 행해진다.

다음은 제안된 인증 프로토콜 구성에 이용한 기호들과 그에 대한 설명이다.

M, V : 사용자와 서비스제공자.

g^m, g^v : M와 V의 공개키.

ID_m, ID_v : M와 V의 ID.

$Cert_M$, $Cert_V$: M와 V의 인증서.

$Sig_m(\ )$, $Sig_v(\ )$: 자신의 비밀키를 사용하여 서명.

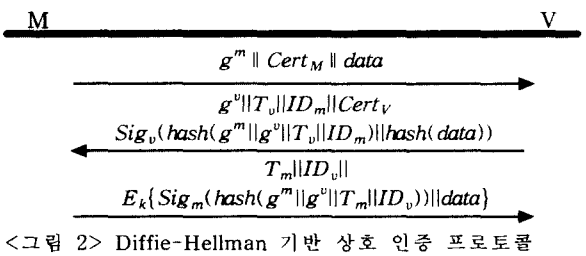
T_m, T_v : Time-stamp.

K : 공유된 비밀키

$data$: 물품/서비스명과 가격

$E_k\{\}$: K를 사용하여 암호화

상호 인증 프로토콜은 <그림 2>와 같다



<그림 2> Diffie-Hellman 기반 상호 인증 프로토콜

M은 V에게 자신의 공개키와 TTP로부터 받은 자신의 인증서와 data를 보낸다. 이를 받은 V는 M의 공개키와 자신의 공개키, Time-stamp, M의 ID를 one-way hash()를 사용하여 나온 값에 자신의 비밀키로 서명을 하고, 자신의 인증서를 함께 M에게 보낸다.

이때 V는 M에게서 받은 data를 one-way hash()를 사용하여 hash()값을 보낸다. M은 V에게 받은 g_v, T_v, ID_m 와 자신의 공개키를 one-way hash()를 사용하여 hash값을 구한다. M은 V의 서명을 확인하기 위해 V의 공개키를 사용하여 확인하고 서명내용과 hash값을 비교하여 같은지를 확인한다.

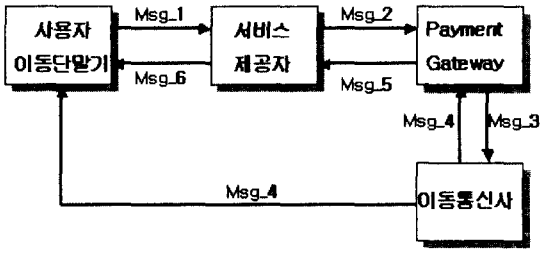
또한 M은 V에게서 받은 hash(data)값과 data를 hash한 값을 비교하여 자신이 보낸 data인지를 확인할 수 있다. M과 V는 공개키를 교환하였으므로 이들은 Diffie-Hellman 기법을 사용하여 공유된 비밀키 K를 구할 수 있다. M은 인증서와 V의 서명으로 인해 V를 신뢰할 수 있다.

세 번째 메시지에서 M은 g^m, g^v, T_m, ID_v 와 이들을 hash함수를 사용한 값에 자신의 비밀키로 서명을 하여 V에게 보낸다. V는 M의 서명으로 인해 M을 신뢰할 수 있다.

이 과정을 수행함으로써 M과 V는 서로를 인증할 수 있다. 더욱이 공유된 비밀키 K를 사용하여 data를 암호화 할 수 있다. 이 data를 공유된 비밀키를 사용하여 암호화함으로써 V는 다시 한번 M을 확인할 수 있으며, M은 V에게 자신이 선택한 목록과 가격을 확실하게 나타낼 수 있다.

3.2 제안한 인증 프로토콜을 사용한 안전한 지불 모델 제안

앞에서 제시한 상호 인증 프로토콜을 사용하여 제안하는 안전한 지불 모델 <그림 3>과 같다.



<그림 3> 이동단말기를 이용한 안전한 지불 모델

제안하는 지불 모델의 메시지는아래와 같다.

Msg_1 - 사용자는 서비스를 선택한 후, 서비스제공자와 상호 인증을 수행한다.

Msg_2 - 서비스제공자는 사용자가 전송한 data, ID_V와 ID_M을 Payment Gateway에게 전송한다.

Msg_3 - Payment Gateway는 data, ID_V와 ID_M을 저장한 후, 이동통신사에게 전송한다.

Msg_4 - 이동통신사는 사용자의 지불능력을 확인한 후, Payment Gateway에게 확인 사실을 전송한다. 또한

data와 ID_V을 사용자에게 전송한다. 사용자는 data와 ID_V을 확인한다.

Msg_5 - Payment Gateway는 확인 사실을 서비스제공자에게 전송한다.

Msg_6 - 서비스제공자는 사용자에게 물품/서비스를 제공한다.

제안하는 지불 모델은 인증 프로토콜을 삽입하므로 인해 사용자가 서비스제공자를 신뢰하여 안전하게 거래를 할 수 있게 된다. 서비스제공자 또한 사용자를 신뢰하고, Payment Gateway를 통해서 사용자의 지불능력이나, 거래 불량을 확인할 수 있으므로 보다 안전한 거래를 할 수 있다.

더욱이 사용자가 서비스를 제공받을 때 자신이 선택한 data를 암호화하여 전송한다. 전송된 데이터를 판매자는 공유된 비밀키로 확인할 수 있게 된다. 이는 사용자와 서비스제공자간에 상호 교환한 데이터로서 후에 문제가 생겼을 때, 부인을 방지할 수 있는 증거가 된다.

또한 제안하는 지불 모델은 휴대폰 지불 모델이 서비스를 제공받기 위해서 인터넷을 사용해야만 한다는 위치제약을 제안한 프로토콜을 사용한 지불 모델을 통해서 극복하였다.

4. 성능 평가

관련연구에서 제시한 두 개의 지불 모델과 앞 절에서 제안한 지불 모델과의 비교는 <표 1>과 같다.

<표 1> 이전 모델과 제안한 모델과의 비교

모델 / 비교항목	휴대폰 지불 모델	제안한 지불모델
상호 인증	△	○
부인 방지	×	○
이동단말기 분실시 피해방지	△	△
이동성	×	○

(○:High △:Low ×:None)

휴대폰 지불 모델은 서비스제공자만이 사용자를 인증하는데 반해, 제안한 모델은 사용자와 서비스제공자간의 인증 과정을 통하여 상호인증을 제공한다. 또한 물품이나 서비스를 구입하는 과정에서 사용자가 공유된 비밀키를 사용하여 물품/서비스명을 암호화하여 전송하는 것으로 인해 사용자와 서비스제공자간의 부인방지를 제공한다. 또한 이동단말기를 분실하였을 경우, 휴대폰 지불 모델은 사용자가 사전에 자신의 지불 금액을 결정하는 방법이나 이동통신사에 분실 신고를 하는 것으로 휴대폰 분실시 피해를 최소화하는 방법을 사용하고 있다. 제안한 모델 또한, 분실 신고나 지불 금액 한도액을 정하는 방법으로 이동단말기 분실시 피해를 최소화 할 수 있다.

서비스를 받을 수 있는 장소가 휴대폰 지불 모델은 항상 인터넷에 접속하여 서비스를 받는 반면에 제안한 모델은 이동단말기를 이용하여 서비스를 받으므로 어디에서나 사용할 수 있다는 장점이 있다.

5. 결론 및 향후 연구 과제

제안한 인증 프로토콜로 인해 사용자와 서비스제공자는 상호인증을 할 수 있게 되었다. 이로 인해 이동단말기를 이용한 안전한 지불을 수행할 수 있게 되었다. 또한 이동적인 제약성을 극복하여 어디에서나 서비스를 받을 수 있다. 이전 모델은 휴대폰을 단지 지불의 매개체로 활용을 하였지만, 제안한 모델은 이동통신이 주체가 되어 물품이나 서비스를 구매할 수 있게 되었다.

그러나 사용자의 거래내역이나 사용자의 신분이 드러남으로 인해 개인정보를 보호할 수 없다. 따라서 향후에는 사용자에게 익명성을 제공하는 연구를 할 것이다.

참고 문헌

[1] http://etlars.etri.re.kr/ETLARS/industry/jugidong/994/99401.htm

[2] Impay "http://www.impay.co.kr"

[3] Teledit "http://www.teledit.com"

[4] [특허]휴대폰을 이용한 지불방법 "http://www.wips.co.kr"

[5] Bruce Schneier, "Applied Cryptography, Second Edition", John Wiley & Sons, Inc, 1996

[6] Y. Zheng, "An Authentication and Security Protocol for Mobile Computing", In Proc. of the IFIP World Conference on Mobile Communications, Canberra, 1996.

[7] Michael Peirce and Donal O'Mahony, "Flexible Real Time Payment Methods for Mobile Communications", IEEE Personal Communications, Dec 1999.

[8] G. Horn and B. Preneel, "Authentication and payment in future mobile systems, Computer Security" - ESORICS'98, Lecture Notes in Computer Science, 1485, pp. 277-293, 1998