2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

사용자 익명성을 보장하는 안전한 휴대폰 지불시스템

임수철*, 이병래*, 강상승**, 김태윤*
*고려대학교 컴퓨터학과
**한국전자통신연구원
e-mail:causal@netlab.korea.ac.kr

Secure Payment System using Mobile Phone assuring User Anonymity

Soo-Chul Lim*, Byung-Rae Lee*, Sang-Seung Kang**,
Tai-Yun Kim*
*Dept of Computer Science & Engineering, Korea University
**Electronics and Telecommunications Research Institute

요약

소액전자지불시스템 중에서 휴대폰을 이용한 지불이 늘어나고 있는 추세인데, 이는 휴대폰의 보편성과 이동통신업체를 통한 통합적인 요금체계, 즉 후불제 방식이라는 장점을 가지고 있기 때문이다. 하지만, 휴대폰을 이용한 지불은 지불 결제시 구매자의 이동통신번호와 주민등록번호를 입력하여 구매자의 신원을 확인하므로 구매자의 정보가 누출될 위험이 있다. 따라서, 본 논문에서는 휴대폰을 이용한 소액지불 결제시 판매자에게 구매자의 신분을 은닉성을 제공하는 안전한 핸드폰 지불시스템을 제안한다.

1. 서론

전자상거래가 발달하면서 최근에 가장 큰 이슈화가 되고 있는 것이 소액전자지불(micropayment)이다. 소액전자지불은 인터넷상에서 상품 혹은 용역의 대가로 부과되는 금액이 일정 기준의 소액인 경우 소액지불을 처리하기 위한 특수한 전자지불시스템을 말한다.

최근 소액전자지불이 주목을 받은 이유는 인터넷 환경이라는 특수성에서 기인한다. 인터넷을 통하여 MP3 파일 다운로드가 폭발적으로 증가하고 있고 최근 음반, 영상 업체들이 자사 콘텐츠의 지적보호를 위해 이의 유료화에 적극 나서고 있기 때문이다. 또 눈으로 직접보고 구입할 수 있는 실물 시장의 강점이 두드러지지 않는 품목들 - 책, CD, 티켓 예매 - 이 대부분 소액인 것도 소액 전자지불 시장 활성화의 한 요인이다.[5]

소액전자지불시스템 중에서 휴대폰을 이용한 지불이 늘어나고 있는 추세인데, 이는 휴대폰의 보편성과 이동통신업체를 통한 통합적인 요금체계, 즉 후불제 방식이라는 장점을 가지고 있기 때문이다. 하지만, 휴대폰을 이용한 지불은 지불 결제시 구매자의 이동통신번호와 주민등록번호를 입력하여 구매자의 신원을 확인하므로 구매자의 정보가 누출될 위험이 있다. 또한 현재의 휴대폰을 이용한 지불은 인터넷에서 구매신청을 하고 지불만 휴대폰을 이용하지만, 휴대폰 서비스의 발달로 휴대폰을 이용하여 구매하는 방법 또한, 고려를 해야 한다.

따라서, 본 논문에서는 휴대폰을 이용한 소액지불 결제시 판매자에게 구매자의 신분을 은닉성을 제공하고, 휴대폰을 이용하여 구매할 수 있는 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 휴대폰 전자 지불시스템에서의 보안 요구 사항과 현재 서비스 중인 지불시스템을 살펴보고, 3장에서는 사용자와 서비스제공자와의 인증과 사용자 익명성을 제공하는 프로토콜을 설계하고 지불시스템을 제안한다. 4장에서는 2장에서의 지불시스템과 제안한 지불

시스템을 비교하고, 마지막으로 5장에서 본 논문의 결론과 향후 연구과제를 논한다.

2. 관련 연구

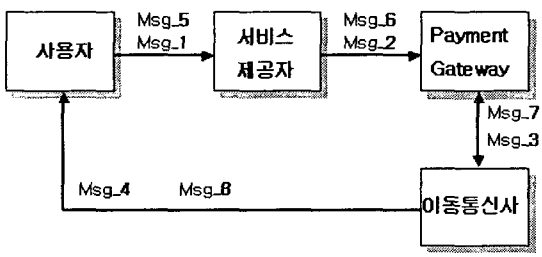
2.1 휴대폰 전자지불시스템에서의 보안 요구 사항

전자지불시스템에서 보안 요구 사항은 개체 인증, 부인방지, 사용자 정보비밀유지이다[3, 4]. 이들 사항은 휴대폰 전자지불시스템에서도 요구되어진다.

- 개체 인증 - 서비스 제공자(물품 판매자)나 사용자(구매자)는 서로를 신뢰할 수 있어야 한다. 인증을 통해서 타인이 사용할 수 없어야 한다. 휴대폰 전자지불시스템에서는 사용자 인증을 이동통신사를 통해서 제공한다.
- 사용자 익명성 보장 - 지불시스템에서는 사용자의 구매행위를 제 3자가 알지 못하게 하거나, 서비스제공자가 사용자의 신분을 알 수 없어야 한다.
- 부인방지 - 사용자는 사용한 서비스에 대한 올바른 대가를 지불해야 하고, 서비스 제공자는 올바른 서비스를 제공해야 한다. 서비스 사용을 부정하거나 바르지 못한 서비스를 제공하지 못하게 해야 한다.

2.2 휴대폰 전자지불시스템

현재 서비스중인 휴대폰 전자지불시스템은 여러 가지가 있으나, 이들 모두가 [2]을 바탕으로 하고 있다. 휴대폰 전자지불시스템은 <그림 1>과 같다.



<그림 1> 휴대폰 전자지불시스템

지불시스템의 구성은 아래와 같다.

- Msg_1 - 구매자는 인터넷을 통해 판매자(컨텐츠 제공자의 site)에 접속하여 구매의사 표시.
- Msg_2 - 판매자는 구매자가 입력한 이동전화번호와 주민등록번호 및 거래내역(컨텐츠명, 가격)을 지불 게이트웨이에 전송.
- Msg_3 - 지불 게이트웨이는 이동통신사에 고객(구매자)인증 요청과 함께 거래암호를 생성하여 전송.
- Msg_4 - 이동통신사는 고객(구매자) 인증 후 구매자에게 거래암호 전송.
- Msg_5 - 구매자가 거래암호를 입력.
- Msg_6 - 판매자는 지불 게이트웨이의 거래승인을 받은 후 과금 정보를 생성하여 전송.
- Msg_7 - 지불 게이트웨이는 판매자로부터 전송받은 과금 정보를 저장한 후 이동통신사에 전송.
- Msg_8 - 이동통신사는 구매자의 이동전화 요금청구서에 결제대금을 통합하여 청구, 수납한 후 판매자에게 대금 지불.

위 지불시스템은 인터넷을 통해 물품/컨텐츠 제공 site에 접속하여 물품/컨텐츠를 제공받고, 대금결제를 휴대폰을 사용하여 결제하고, 지불은 이동통신 요금청구서를 통해서 한다.

후불결제와 결제시 특별한 장비가 필요하지 않다는 장점을 가지고 있으나, 구매자가 물품/컨텐츠를 제공받기 위해서는 자신의 휴대폰번호와 주민등록번호를 노출하여야 한다.

3. 사용자 익명성을 제공하는 지불 시스템 제안

3.1 사용자 익명성을 제공하는 지불 시스템 I

지불시스템에서 사용자 익명성 제공은 사용자 인증과 상반되는 관계를 가진다. 서비스를 받고 지불을 수행하기 위해서는 사용자의 신원을 확인해야 한다. 사용자의 신원을 확인하는 인증단계에서는 사용자의 신분을 나타낼 수 있는 주민등록번호와 같은 것을 드러내야 한다. 이와 같이 사용자 익명성과 인증은 상반되는 관계를 가지고 있는데, 이를 보완하는 방법으로 제안된 것이 일시적인 사용자 아이디를 사용하는 것이다.

사용자가 서비스를 받기전에 이동통신사에서 일회성 아이디를 발급받는다. 사용자는 컨텐츠제공자의 site에 접속하여 이동통신사에서 발급 받은 일회성 아이디를 입력한다. 즉, <그림 1>의 Msg_1과정에서 이동전화번호와 주민등록번호를 입력하는 대신에 이동통신사에서 발급 받은 일회성 아이디를 입력한다. 컨텐츠제공자는 지불 게이트웨이를 통해서 이

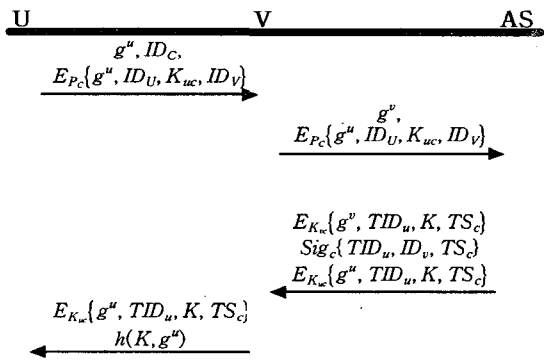
동통신사에게 사용자의 인증을 받을 수 있게 된다. 이 일회성 아이디를 사용하여 단 한번만 서비스를 받을 수 있어야 한다. 만일 일회성 아이디를 사용하여 다수의 서비스를 받게 된다면, 사용자의 익명성을 제공할 수 없게 된다.

3.2 사용자 익명성을 제공하는 지불 시스템 II

사용자 익명성을 제공함과 동시에 사용자 인증을 수행하기 위해서 사용자와 컨텐츠제공자 사이에 인증기관(AS)이 존재한다 가정한다.

사용자와 컨텐츠제공자는 인증기관을 통해서 상호인증과정을 수행하며, 이 과정에서 사용자가 자신의 신분을 나타내는 아이디는 인증기관에게 제공받은 일회성 아이디이다. 사용자는 인증기관에게 일회성 아이디를 제공하고, 컨텐츠제공자는 인증기관을 통해서 인증받는다[1].

아래의 <그림 2>는 서비스를 제공받기위한 인증과정이다.



<그림 2> 사용자 익명성을 제공하는 인증 프로토콜

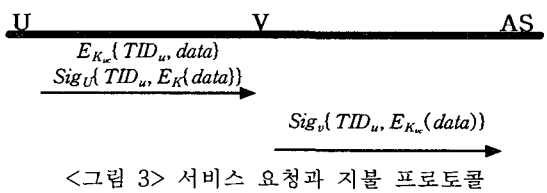
[인증과정]

사용자와 서비스제공자는 인증기관을 통해서 인증을 받는다. 처음 메시지에서 사용자는 자신의 공개키(g^u), 인증기관의 아이디(ID_C)와 인증기관의 공개키를 사용하여 자신의 공개키, 자신의 아이디(사용자의 아이디는 자신의 소유하고 있는 이동전화번호), 인증기관과의 비밀키, 서비스제공자의 아이디를 암호화하여 서비스제공자에게 전송한다. 사용자의 아이디를 암호화하였으므로 서비스제공자는 사용자의 신분을 확인할 수 없게된다. 서비스제공자는 사용자에게 처음 메시지를 받으면 인증기관의 아이디를 확인한 후, 자신의 공개키(g^v)와 사용자가 보낸 암호화된 메시지를 같이 인증기관에게 전송한다. 인증기관은 서비스제공자에게 두 번째 메시지를 받은 후, 자신의 비밀키를 사용하여 암호 메시지를 복호화하여 메시지의 내용을 확인 할 수 있다. 사용자의 아이디를 확인 한 후에 임시적인 일회성 아이디 TID_U를 생성한다. $E_{K_{uc}}\{g^v, TID_u, K, TS_c\}$ 세 번째 메시지 중 이 암호 메시지는 서비스제공자에게 사용자의 신분을 인증해주고, 사용자와 공유하여 사용할 수 있는 비밀키를 암호화하여 전송한다. 또한 인증기관은 사용자의 임시적 일회성 아이디와 서비스제공자의 아이디, time-stamp를 자신의 개인키를 사용하여 서명을 한다. 또한 $E_{K_{uc}}\{g^u, TID_u, K, TS_c\}$ 이 암호 메시지는 사용자와의 세션키를 사용하여 사용자에게 일회성 아이디와 서비스제공자와의 세션키를 암호화한 후에 전송한다.

세 번째 메시지를 받은 서비스제공자는 암호 메시지를 인증기관의 세션키를 사용하여 내용을 확인할 수 있다. 여기서 서비스제공자는 인증기관이 인증한 사용자의 일회성 아이디를 확인 할 수 있다. 인증기관이 서명한 메시지로 인증기관을 더욱 신뢰할 수 있으며, 이를 통해 사용자의 신분을 신뢰할 수 있게된다. 서비스제공자는 사용자에게 인증기관이 전송한 암호 메시지 $E_{K_{uc}}\{g^u, TID_u, K, TS_c\}$와 사용자의 공개키, 세션키를 해쉬함수를 사용한 해쉬값을 전송한다. 사용자는 인증기관이 암호화한 메시지를 통해서 자신의 임시적 일회성 아이디를 가질 수 있게되었다. 또한 서비스제공자와의 세션키를 획득하였다.

위의 인증 프로토콜로 인해 사용자와 서비스제공자는 서로를 신뢰할 수 있게 되었으며, 사용자는 서비스를 제공받기 위해서 자신의 신분을 노출시키지 않아도 된다.

아래의 <그림 3>은 서비스를 요청과정과 지불과정이다.



<그림 3> 서비스 요청과 지불 프로토콜

[지불과정]

사용자는 서비스를 선택하여 서비스제공자에게 서비스 요청을 한다. 사용자가 서비스제공자에게 보내는 첫 번째 메시지에서 data는 사용자가 선택한 서비스명과 가격을 나타낸다. 이 메시지에서 사용자는 인증기관에게 전송할 메시지와 서비스제공자에게 전송할 메시지 두 개의 메시지를 생성한다. 서비스제공자에게 전송할 메시지는 $Sig_u\{TID_u, E_K\{data\}\}$으로 data를 암호화하고, 자신의 일회성 아이디를 서명하여 보낸다. 또한 인증기관에게 거래사실을 확실히 하기 위해 자신의 아이디와 거래내역을 암호화하여 전송한다. 이를 받은 서비스제공자는 자신에게 온 메시지를 확인하고 사용자를 확인한 후 자신이 가지고 있던 사용자 일회성 아이디와 일치하면 서비스를 제공한다. 인증기관에게 사용자가 암호화한 메시지를 전송한다. 인증기관은 이 메시지를 확인하고, 사용자의 이동통신사용내역에 첨부하여 이동통신요금과 함께 청구하고, 서비스제공자에게 지불을 한다.

4. 성능 평가

이 장에서는 앞에서 제안한 지불시스템 I, II와 휴대폰 전자지불시스템을 비교한다.

비교한 내용은 <표 1>과 같다.

<표 1> 지불시스템간의 비교

	휴대폰 전자 지불시스템	제안한 지불시스템 I	제안한 지불시스템 II
익명성 제공	×	○	○
상호 인증	△	△	○
부인 방지	×	×	○
참여자 수	4	4	3

(○:High △:Low ×:None)

제안한 지불시스템은 사용자의 아이디를 인증기관이나 이동통신사로부터 임시적인 일회성 아이디를 전송받아 서비스 거래에 사용하기 때문에 제 3자나 서비스제공자는 사용자의 신분을 알 수 없게되었다. 또한 서비스제공자만이 사용자를 인증할 수 있었지만, 제안한 지불시스템 II에서는 인증기관을 통한 인증으로 상호인증이 지원된다. 이를 통해 사용자와 서비스제공자는 서로 신뢰하며 거래를 할 수 있게 되었다. 제안한 지불시스템 II는 사용자와 서비스제공자간의 공유하는 세션키를 사용하여 거래내역을 암호화하여 전송하고 인증기관(이동통신사)에게 거래내역을 전송하므로, 서비스 제공 후에 일어날 지불부인이나 서비스제공을 부인하는 것을 막을 수 있게되었다. 또한 시스템 II에서는 인증기관이 이동통신사와 지불 게이트웨이 역할을 동시에 함으로 인해, 지불시스템을 위해 참여하는 참여자의 수를 3으로 할 수 있게 되었다.

5. 결론

본 논문에서는 사용자가 인터넷을 통하여 서비스제공자의 사이트에 접속하였을 경우 사용자와 서비스제공자가 인증기관을 통해서 사용자의 익명성을 제공하며 인증과정을 수행하여 안전한 지불시스템을 제안하였다. 본 논문에서 제안한 지불시스템으로 인해 서비스를 받고, 제공하는 과정에서 사용자의 신분이 노출되는 것을 인증기관에서 제공한 임시적인 일회성 아이디를 사용하여 사용자 익명성을 제공하였다. 또한 상호 인증과 부인방지 문제를 해결하였다. 그러나 사용자가 인터넷에 접속하여야만 서비스를 제공받을 수 있다는 위치적 제약성 문제는 해결하지 못하였다. 따라서 향후에는 위치 제약성 문제를 해결하는 지불시스템을 연구할 것이다.

참고 문헌

[1] Byung-Rae Lee, Kyung-Ah Chang, Tai-Yun Kim, "Temporary Mobile User Certificate for Mobile Information Services in UMTS" IEICE TRANS. COMMUN. Vol.E83-B, NO.8, 2000

[2] [특허]핸드폰을 이용한 지불모델, "http://www.wips.co.kr

[3] J. Zhou and K-Y. Lam, "Undeniable Billing in Mobile Communication", p284-290, Mobicom, 1998

[4] C. S. Park. "On certificate-based security protocols for wireless mobile communication systems. IEEE Network, 11(5):50-55, 1997

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