무선인터넷에서의 안전한 신용카드 지불 프로토콜 설계

임수철[0] 김정범 이윤정 김태윤
고려대학교 컴퓨터학과
{causal[0], qston, genuine, tykim}@netlab.korea.ac.kr

A Design Secure Credit Card Payment Protocol of Wireless Internet

Soo-Chul Lim[0] Jeong-Beom Kim Yoon-Jung Rhee Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

요 약

WPP 지불 프로토콜[3]은 WAP 프로토콜을 이용하여 무선인터넷에서 신용카드 지불을 수행한다. 그러나 WPP 지불 프로토콜은 WAP의 보안 프로토콜인 WTLS를 사용함으로써 종단간 보안을 제공하지 못하는 문제점을 가지고 있다. 본 논문에서는 공개키 암호 시스템과 Mobile Gateway를 사용하여 특정 무선인터넷 플랫폼과 독립적인, 종단간 보안이 제공되는 안전한 신용카드 지불 프로토콜을 제안한다.

1. 서 론

무선인터넷의 발달로 전자상거래 시장이 급속하게 커지고 있다. 무선인터넷 전자상거래에서 상품 구입이나 서비스를 받기 위해서는 안전한 지불 프로토콜이 필요하다. 이러한 필요성으로 인해 많은 무선인터넷에서 안전한 지불 프로토콜이 연구되고 있다. WPP[1] 지불프로토콜은 대표적인 무선인터넷 플랫폼인 WAP(Wireless Application Protocol)[3]을 사용하여 제안한 신용카드 지불 프로토콜이다.

WPP 지불 프로토콜은 WAP의 WTLS(Wireless Transport Layer Security)[2]를 사용하여 무선구간의 보안을 제공한다. WTLS를 사용하는 WAP 프로토콜 스택은 인터넷 프로토콜과 서로 다르기 때문에 변화해주는 WG(WAP Gateway)가 필요하다. 그러나 WG에서 WTLS-SSL 프로토콜 변화시 암호화된 메시지가 복호화 되어 메시지가 노출되어 종단간 보안을 제공하지 못한다[6]. 따라서 WPP는 안전한 지불 수행에 어려움이 있다.

본 논문에서는 종단간 보안이 제공되는 안전한 신용카드 지불 프로토콜을 제안한다. 제안한 지불 프로토콜은 공개키 암호 시스템을 사용하여 안전성을 제공한다. 공개키 암호 시스템은 무선이동 통신에 적합하지 않았으나, 적은 비트 수와 빠른 계산 속도를 보장하는 타원 곡선 공개키 암호 시스템으로 인하여 무선 이동 통신에 공개키 암호 시스템을 사용할 수 있게 되었다[4,7]. 또한 제안한 지불 프로토콜은 WAP의 WG 문제점을 극복하기 위해 무선구간과 유선구간의 연결 기능만을 수행하는 MG(Mobile Gateway)를 사용한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로써 WPP 지불 프로토콜을 기술하고 문제점을 알아본다. 3장에서는 제안한 지불 프로토콜을 기술하고 안전성을 알아본다. 4장에서는 제안한 지불 프로토콜의 성능을 분석하고 마지막 5장에서는 결론을 기술한다.

2. WPP 지불 프로토콜

WPP[1] 지불 프로토콜은 무선인터넷에서 신용카드 지불을 수행 할 수 있도록 제안된 지불 프로토콜이다. WPP는 신용카드 정보를 보호하기 위해 스마트카드 기술을 사용하였고, 무선환경에서 보안성을 제공하기 위해 WAP의 WTLS를 사용하였다.

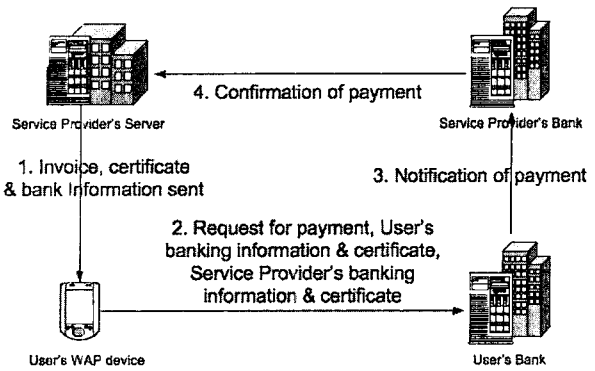

그림 1. WPP 지불 프로토콜

그림 1과 같이 WPP 지불 프로토콜은 사용자와 사용자의 은행, 서비스 제공자, 서비스 제공자의 은행으로 구성된다. 사용자의 WAP 단말기는 사용자의 은행 정보와 지불에 필요한 사용자의 정보를 스마트카드에 저장한다. 무선구간의 사용자 유선구간의 참여자들과 연결하기 위해서는 WG가 필요하다. 그림 1에서는 WPP 지불 프로토콜 시스템의 구성과 지불 흐름도를 나타낸 것으로 WG는 생략하였다(WPP 지불 프로토콜에 대한 자세한 내용은 [1]을 참조하라).

WPP 지불 프로토콜은 WAP의 WTLS를 사용하여 무선구간의 보안을 제공한다. 이 때문에 WAP에서는 WAP 단말기와 유선환경에 존재하는 서버를 연결해 줄 수 있는 다리로서 WG를 사용한다. WG에서는 WTLS-SSL 프로토콜 변환 시 암호화된 메시지가 복호화되어 원본 메시지가 노출될 위험성을 가지고 있어 종단간 보안성을 제공하지 못한다[6]. 따라서 WPP 지불 프로토콜은 무선인터넷 전자상거래에서 안전한 지불을 수행하기에는 문제점이 있다.

본 논문에는 공개키 암호 시스템과 MG(Mobile Gateway)를

사용하여 안전한 신용카드 지불 프로토콜을 제안한다.

3. 제안하는 안전한 신용카드 지불 프로토콜

본 장에서는 안전한 신용카드 지불 프로토콜을 제안하고 제안한 지불 프로토콜의 안전성을 분석한다.

3.1 제안한 신용카드 지불 프로토콜

제안한 지불 프로토콜은 공개키 암호 시스템을 사용하여 무선인터넷에서 안전한 신용카드 지불을 수행한다. 공개키 암호 시스템은 무선 이동 통신에 적합하지 않았으나, 적은 비트 수와 빠른 계산 속도를 보장하는 타원 곡선 공개키 암호 시스템으로 인하여 무선 이동 통신에 공개키 암호 시스템을 사용할 수 있게 되었다[4,7]. 제안한 지불 프로토콜의 안전성은 유한체(finite field)의 곱셈군(multiplicative group) 또는 타원 곡선의 부분군(subgroup)과 같은 유한군 G와 생성원 g에서 이산 대수 문제(discrete logarithm problem)[5]가 어렵다는 가정을 근거로 한다. 또한 각 참여자와의 세션키(session key) 설정은 Diffie-Hellman 키 설정[13] 방식을 사용한다. 제안한 프로토콜에서 U는 사용자, V는 상품/서비스 제공자(VASP), MG는 Mobile Gateway, PG는 Payment Gateway를 의미한다. $h(\cdots)$은 일방향 해쉬함수이고, $Sig_X(\cdots)$은 X의 개인키를 사용하여 메시지를 서명한 것이다. $\{\cdots\}_K$은 X와 Y가 공유하는 세션키(K)를 사용하여 암호화한 것이다. 사용한 데이터 요소는 표1과 같다.

표 1. 제안한 지불 프로토콜에서 사용한 데이터 요소

데이터 요소	설 명
id_X	X의 신원
x	X의 개인키
g^x	X의 공개키
K_{XY}	X와 Y가 공유하는 세션키
TX	X에 의해 생성된 타임스탬프
ch_{data}	지불정보를 의미하며, 상품이나 서비스 명칭과 수량이 포함된다.
$card_{data}$	신용카드 정보를 의미한다.

각 참여자는 프로토콜에서 사용되는 알고리즘을 알고 있어야 하며, U는 PG와 공유하는 세션키를 가지고 있어야 한다. 또한 무선단말기의 스마트카드에 저장되어 있는 신용카드 정보는 무선환경에서 사용할 수 있도록 신용카드사와 미리 협정한 정보이다.

제안한 지불 프로토콜은 그림 2에 나타나 있다.

프로토콜의 수행은 U가 V의 서버에 접속하면서 시작한다. U는 난수 u를 생성하여 키 설정용 임시 공개키 g^u를 계산하여 V의 신원과 선택한 상품이나 서비스의 정보 $data$를 V에게 전송한다.

V는 난수 r을 생성한 후 첫 번째 메시지에서 받은 U의 키 설정용 임시 공개키를 사용하여 U와 공유하는 세션키 $K_{UV}=h((g^u)^v \| r)$을 생성한다. 그리고 해쉬값을 계산하여 지불 데이터 ch_{data}를 전송한다.

두 번째 메시지를 받은 U는 V와의 세션키를 생성한 후 해쉬값을 계산하여 전송받은 해쉬값 $h(K_{UV} \| r \| id_V)$과 동일한 지를 비교한다. 비교한 값이 동일하면 인증확인 메시지와 $Cert_U$를 전송한다. 또한 지불을 위해 신용카드 정보 $card_{data}$가 들어있는 메시지를 PG와의 세션키를 사용하여 암호화하여 V에게 전송한다.

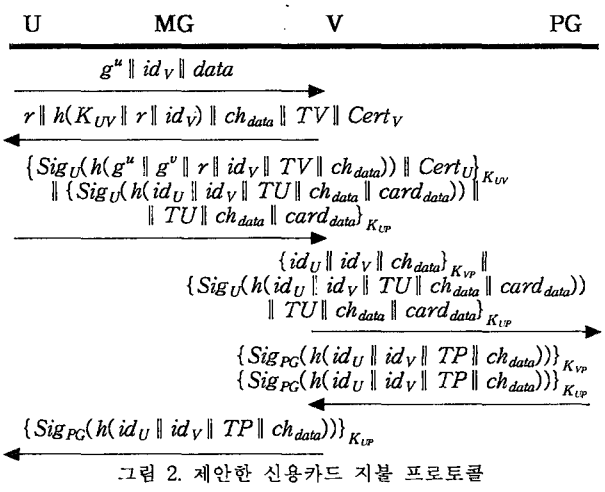

그림 2. 제안한 신용카드 지불 프로토콜

V는 U가 보낸 메시지의 $Cert_U$를 사용하여 해쉬값을 확인한다. V는 PG에게 지불승인 요청을 하기 위해 U가 생성한 지불정보와 함께 id_U, id_V, ch_{data}를 암호화하여 전송한다.

PG는 U와 V가 보낸 메시지를 확인하여 거래정보 ch_{data}를 비교하여 동일하면 신용카드 정보 $card_{data}$를 사용하여 지불처리를 행한다. U가 보낸 신용카드 정보로 성공적으로 지불이 처리되면 거래에 참여한 참여자 id_U, id_V와 지불처리가 수행된 시간 TP, 거래정보 ch_{data}의 해쉬값에 서명하여 암호화한 메시지를 V에게 전송하고, V를 통하여 U에게도 전송된다. 이 과정이 수행되면 V는 U가 선택한 상품이나 서비스를 제공하게 된다.

3.2 안전성 분석

- V에 대한 키 확인과 인증 : 그림 2의 지불 프로토콜 메시지 중 두 번째 메시지에 $h(K_{UV} \| r \| id_V)$를 첨가하는 것은 V가 U에게 키 확인과 V의 함축적 키 인증성과 개체 인증을 제공하기 위함이다.
- U에 대한 키 확인과 인증 : 세 번째 메시지의 인증서 $Cert_U$를 세션키 K_{UV}로 암호화하는 것은 키 확인을 제공한다. 또한 해쉬함수에 $g^u \| g^v \| r$을 첨가하는 것은 U에서 V에게 함축적 키 인증성을 제공하기 위함이다. 난수 r의 첨가는 U에 대한 개체인증을 제공한다.
- 재전송 방지 : V로부터 생성된 난수 r은 K_{UV}의 생성에

필요한 하나의 요소이다. 이는 이전에 사용되었던 K_{UV}가 재 사용되는 것을 방지하기 위함이다. 난수 r과 U로부터 생성된 난수 u는 세션키가 새로운 키(key freshness)임을 증명한다.

- 부인 방지 : U의 전자 서명은 서명된 데이터의 부인 방지를 제공한다. 또한 제안한 프로토콜의 맨 마지막 메시지는 거래와 지불에 대한 부인 방지를 제공한다.

4. 성능 평가 및 분석

본 장에서는 WPP 프로토콜과 제안한 지불 프로토콜을 비교한다. 또한 지불수행에 필요한 전송량과 계산량을 조사하여 성능을 분석한다.

표 2는 제안한 지불 프로토콜과 WPP 프로토콜의 특성을 비교한 것이다.

표 2. 지불 프로토콜의 특성 비교

	WPP 프로토콜	제안한 지불 프로토콜
종단간 보안성 제공	×	○
인증과 지불 통합	×	○
사용 기법	WAP	독립적

(○ : High △ : Low × : None)

제안한 지불 프로토콜은 종단간 보안성을 제공하기 위해 공개키 암호 시스템을 사용하였고, 무선과 유선을 연결해주는 MG를 지불 시스템에 추가하였다. MG는 WG가 프로토콜 변환에 참여하는 것과는 달리 무선과 유선의 연결기능만을 가지고 있다. 또한 인증을 수행한 후 지불과정을 수행하는 WPP 프로토콜과는 달리 인증과 지불과정을 통합하였다. WPP 프로토콜은 특정 무선 프로토콜인 WAP에 제한적이지만, 제안한 지불 프로토콜은 특정 프로토콜에 독립적으로 사용할 수 있는 장점이 있다.

무선환경에서는 유선환경과 달리 제한적인 요소를 많이 가지고 있다. 제한적인 요소 중 통신량과 계산량은 특히 고려해야 한다. 따라서 제안한 지불 프로토콜과 WPP 프로토콜의 통신량과 계산량을 비교해본다. 통신량으로는 전송되는 메시지 횟수로 계산량으로는 암호학적 연산인 멱승(exponentiation)으로 한다.

표 3. 사용자 측면에서의 통신량과 계산량 비교

	WPP 프로토콜	제안한 지불 프로토콜
메시지 교환 횟수	10	4
멱승 횟수	3	4

WPP 프로토콜은 지불을 수행하기 위해 WAP 단말기와 서버가 안전하게 메시지를 전송하기 위해 암호 매개 변수를 교환해야 한다. 암호 매개 변수를 교환할 때 4번의 메시지 교환 횟수가 필요하다. 멱승은 공개키와 pre_master_secret을 생성할 때 사용된다[2]. WAP의 WTLS는 암호 매개 변수를 교환할 때 많은 선택사항을 가지고 있다. 따라서 표 3와 4에서 계산한 멱승 횟수는 선택사항에서 추가되는 횟수는 제외하였다.

제안한 지불 프로토콜에서 메시지 교환 횟수는 지불 수행에 필요한 메시지의 횟수를 계산하였고, 멱승은 공개키 생성과 세션키 생성에 사용되는 횟수를 계산하였다.

표 5. 서비스 제공자 측면에서의 통신량과 계산량 비교

	WPP 프로토콜	제안한 지불 프로토콜
메시지 교환 횟수	10	8
멱승 횟수	3	3

제안한 지불 프로토콜과 WPP 프로토콜을 비교한 표 4와 5를 보면 계산량에서는 두 프로토콜이 비슷하나, 통신량에서는 제안한 지불 프로토콜이 향상된 성능을 보인다.

5. 결 론

WPP 지불 프로토콜은 WAP 프로토콜을 이용하여 무선인터넷에서 신용카드 지불을 수행하기에는 종단간 보안이라는 문제점이 있어 안전상 큰 문제점이 있다. 이러한 문제점을 극복하기 위해 본 논문에서는 공개키 암호 시스템과 Mobile Gateway를 사용하여 특정 프로토콜과 독립적인, 종단간 보안이 제공되는 지불 프로토콜을 제안하였다. 제안한 지불 프로토콜은 WPP 지불 프로토콜보다 향상된 성능을 갖는다.

참고문헌

[1] J. Hall, S. Kilbank, M. Barbeau, and E. Kranakis, "WPP: A Secure Payment Protocol for Supporting Credit- and Debit-card Transactions Over Wireless Networks", IEEE International Conference on Telecommunications (ICT), Bucharest, June, 2001.

[2] WAP Fourm, "Wireless Application Protocol Wireless Transport Layer Security Spectification version 18-FEB-2000", 2000.

[3] WAP Forum, "WAP White Paper", http://www.wapforum.org

[4] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems", ESORICS, LNCS 1485, pp.277-293, 1998.

[5] A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, 1997.

[6] Saarinen, Markku-Juhani. "Attacks against the WAP WTLS Protocol." Communications and Multimedia Security, Belgium, Sep. 1999.

[7] K. M. Martin, B. Preneel, C. J. Mitchell, H. J. Hitz, G. Horn, A. Polickova, P. Howard, "Secure Billing for Mobile Information Services in UMTS", LNCS 1430, Springer-Verlag, IS&N May. 1998.