

무선 인터넷에서 해쉬체인을 이용한 분할 소액지불시스템에 관한 연구

강서일, 이임영*, 강성우**
*순천향대학교 정보기술공학부
**한국정보보호진흥원 암호인증기술팀

A Study on Divisible Micropayment System using Hash Chain in Wireless Internet

Se-Il Kang*, Im-Yeong Lee*, Sung-Woo Kang**
*Division of Information Technology, Soonchunhyang University

**Electronic Transaction Security Technical Team, Korea Information Security Agency

요 약

오늘날 휴대 단말기의 대중화에 따라 무선 가입자가 유선 가입자를 넘어서고 있다. 이러한 상황에서 유선의 전자상거래 서비스 업체들이 무선의 서비스를 제공하려고 한다. 이에 무선에서 과금 및 금융서비스가 필요하게 되었다. 특히 금융 서비스는 무선에서 제공하는 서비스 중 하나가 될 수 있다. 이에 본 논문에서는 안전하게 지불할 수 있는 시스템으로 해쉬체인을 이용하여 효율성을 높은 소액 지불 시스템을 제안한다. 제안된 방식의 경우 해쉬체인을 이용하므로 분할 지급할 수 있도록 구성하였다.

1. 서론

휴대 단말기의 보급과 무선 인터넷의 서비스의 증가로 인해 무선에서의 과금 및 금융서비스를 제공하게 되었다. 무선에서의 서비스 중 금융의 서비스는 현재 보급 단계에 있으며, 앞으로 활성화될 것으로 예측된다. 현재 많은 이동 통신 업체에서 무선 인터넷 및 근거리 통신 기술을 이용한 지불 시스템을 구성하여 서비스를 제공하고 있다. 이에 본 논문에서는 무선 서비스를 제공받고 과금 및 무선 상거래에 지불할 수 있는 시스템에 대해 연구하였다. 무선 휴대 단말기는 하드웨어의 제약사항이 고려되어야 하나 기술 개발로 인해 제약 사항은 줄어들고 있으며, 현재의 무선 단말기 하드웨어는 인증서를 제공할 수 있도록 개발되어 있다.

본 논문의 구성은 2장에서는 무선에서 전자 지불의 보안 요구사항에 대해 알아보고 3장에서는 무선에서의 지불 시스템에 대한 관련 연구에 대해 논의한다. 4장에 시스템을 제안하고, 5장에서는 보안 요구사항에 따라 제안 시스템을 분석한다. 마지막으로 6장에서는 결론 및 향후 방향에 대해 논의한다.

2. 무선 전자지불 시스템 보안 요구 사항

무선에서의 전자 지불시스템은 무선 통신 및 무선 서비스제공자에게 금액을 제공하는 서비스이다. 이에 무선에서 전자 지불 시스템의 보안 요구 사항은 다음과 같다.

- 안전성 : 전자 화폐를 위조 및 변조를 할 수 없어야 한다.
- 인증 : 사용자가 정당한지 인증을 할 수 있는 방안이 제시되어 있어야 한다.
- 부인 봉쇄 : 사용자의 지불 후에 거래에 대한 부인을 할 수 없도록 한다.

안전성은 지불시스템에서 이용되는 전자 화폐로 위조 및 변조 또한 임의의 생성이 불가능해야 한다. 인증은 서비스에 따른 금액을 지불하는 이용자가 정당한지를 확인할 수 있어야 하고 부인 봉쇄는 거래 후 부인을 막을 수 있는 방안을 제공하여야 한다.

이외에도 지불 시스템의 가지고 있는 보안 요구사항으로 익명성, 분할성, 가치 이전성, 이중 사용방지 등이 제공되어야 한다.

본 연구는 한국정보보호진흥원에서 지원하는 위탁
과제로 수행하였습니다. (과제번호 2003-S-054)

3. 관련 연구

무선 전자 지불시스템으로 AIP(Authentication and Initialisation of Payments)프로토콜로 공개키 암호화 기반의 사용자와 VASP(Value-Added Service Provider)의 사이에서 인증 및 지불 프로토콜이다. 이번 장에서는 AIP 및 기존의 무선 전자 지불시스템에 대해서 논의한다.

3.1 AIP의 지불시스템

제 3세대 이동통신 시스템에서 요구되는 요금 부과 분야를 지원하는 안전한 과금 프로토콜로 ASPeCT (Advanced Security for Personal Communications Technologies)프로젝트에 의해 수행되었으며, 1997년에 구현된 과금 방식이다.[1]

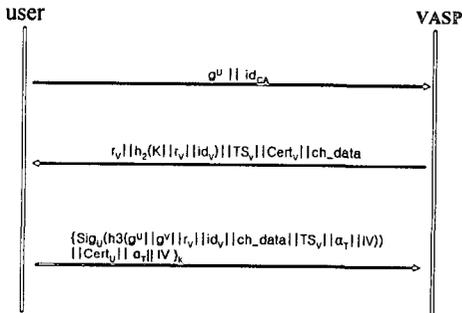


그림 1. API 프로토콜 흐름도

AIP방식은 초기 난수 U를 이용하여, g^u 와 인증기관의 ID_{CA}를 제공한다. 해쉬를 이용하여 비밀키를 생성하여, 지불 정보 및 난수를 사용자에게 보낸다. 사용자는 받은 정보를 확인하여 서명 및 지불의 초기 벡터 IV를 제공하여 티켓을 이용한 지불을 한다.

3.2 이동 통신 시스템에서 종단간 인증 및 지불 프로토콜

이동 통신 시스템에서 종단간 인증 및 지불 프로토콜은 AIP의 프로토콜 및 해쉬체인을 이용하여 지불시스템을 제공한다.[2]

이동 통신 시스템에서의 종단간 인증 및 지불 프로토콜은 인증서 발급 단계와 지불/정보 교환 단계로 두 단계로 되어 있다.

인증서 발급 단계에서는 브로커에서 자신의 공유키를 생성하고 해쉬체인을 이용하여 root 값을 생성한다. root값은 사용자가 해쉬체인에 이용할 값과 난수, 사용자의 아이디, 브로커와 공유키를 해쉬를 취해 저

장한다.

지불의 방식은 사용자와 VASP와 통신으로 PayCert를 전송한다.

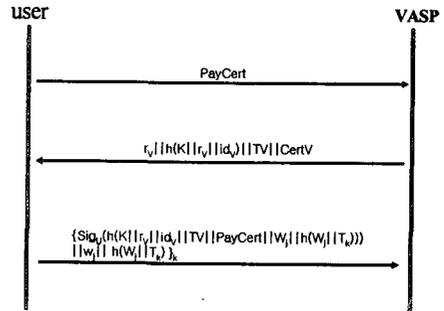


그림 2. 이동 통신 시스템에서의 종단간 인증 및 지불 프로토콜의 흐름도

이와 같은 경우 취약성은 사용자가 root값을 구성할 수 있기 때문에 임의의 값을 생성할 수 있다. 이러한 경우 위조가 가능하다.

4. 제안 방식

무선에서의 지불시스템을 위해 해쉬 체인을 이용하여 소액 지불 시스템을 구성한다.

본 시스템은 세션키 방식의 대칭키를 이용하여 암호화를 제공하며, 세션키 생성으로 인증을 한다.

휴대 단말기의 성능과 메모리의 이용을 최소화하여 효율성을 높인다.

4.1 시스템 계수

본 시스템은 사용자와 은행, VASP의 통신을 통해 인증 및 지불을 한다. 사용자는 통신을 하기 이전에 은행과 VASP와 식별자를 안전하게 나누어 가졌다고 가정한다. 이는 오프라인을 통한 등록이나 단말기의 안전한 등록을 통해 가정할 수 있다.

- U : 사용자
- B : 은행
- V : VASP(Value-Added Service provider)
- Count : 사용자가 선택한 지불 금액
- n : 사용자가 선택한 횟수
- {M}* : *를 이용하여 암호화한 메시지
- S.._key : *와 *의 사이에서 쓰이는 세션키
- g** : *와 *의 사이에 사전에 미리 나누어 가진 식별자

- $h(*)$: 128비트의 안전한 일방향 해쉬 함수
- $Sig(*)$: *의 서명 값
- \oplus : XOR 연산
- R_* : *가 선택한 랜덤 수
- M_data : 지불 금액의 관련된 데이터
- T_data : 금액의 신청한 시간
- $root$: 해쉬 체인의 $root$ 값으로 $h(a^n, T_data)$

은행이 생성하는 메시지

$$B \rightarrow U : \{ \text{count} \oplus R_{B2} \\ \text{root} = h(a^n \parallel T_data) \}$$

$B \rightarrow U : \{ Sig_B(\text{root}), \text{root}, a, T_data \}_{S_{UB_Key}}$

마. 사용자는 위의 전송이 끝나면 다음과 같이 $root$ 값과 a 값을 가질 수 있다.

이상의 본 시스템에서 사용되는 계수이다.

4.2 제안 방식의 프로토콜

제안 방식의 발행과 지불 프로토콜은 두 단계로 나눌 수 있다. 발행 프로토콜은 사용자가 은행으로부터 소액 지불 가능한 체인의 $root$ 값을 발급 받는다. 지불 프로토콜은 사용자와 VASP의 지불 프로토콜로 사용자는 VASP로 지불의 데이터의 필요한 정보를 얻는다. 이후에 은행으로부터 발급 받은 해쉬체인을 소액 지불로 나누어 지불한다.

(1) 발행 프로토콜

사용자와 은행은 앞에서 가정한 것과 같이 식별자를 나누어 가진 상태에서 프로토콜이 진행된다.

가. 은행은 임의의 랜덤수(R_B)를 생성하여 사용자에게 전송한다.

$$B \rightarrow U : R_B$$

나. 사용자와 은행은 다음과 같은 계산으로 공통 세션키를 생성한다.

$$S_{BU_Key} = h(h(gID_B) \oplus R_B)$$

다. 사용자는 생성한 세션키를 이용하여 자신이 선택한 지불 금액과 회수 및 금액의 신청시간을 암호화하여 보낸다.

$$U \rightarrow B : \{ \text{count} \parallel n \parallel T_data \}_{S_{UB_Key}}$$

라. 은행은 사용자가 전송 받은 메시지를 생성한 세션키로 복호화하고 랜덤수를 선택하여 생성한 $root$ 및 메시지를 전송한다. 이때 세션키는 사용자의 식별자를 인증할 수 있는 방안이 된다. 만약 세션키로 복호화가 되지 않는다면 거래를 중단한다.

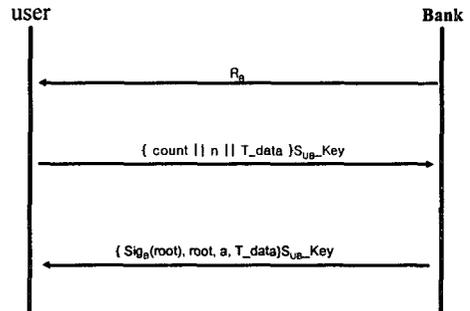


그림 3. 제안 방식의 발행 프로토콜

(2) 지불 프로토콜

지불은 사용자와 VASP와의 거래에서 전송되는 것으로서 사용자와 VASP간의 식별자를 이미 나누어 가진 상태에서 시작된다. 이 또한 세션키 방식을 이용한다.

가. 지불을 위해 VASP는 임의의 수를 선택 및 지불 데이터를 전송한다.

$$V \rightarrow U : R_v, M_data, h(R_v, M_data)$$

나. 사용자는 받은 랜덤수를 이용하여 세션키를 생성하고 지불 데이터를 이용하여 자신의 지불할 j 에 대해 다음과 같이 계산한다.

세션키 생성

$$U : S_{UV_Key} = h((g^{UV}) \oplus R_v) \\ b = a^{n-j}$$

다. 사용자는 생성한 세션키로 지불값을 암호화하여 전송한다.

$U \rightarrow V$

$$\{ \text{root}, T_data, a^{n-j}, j, Sig_B(\text{root}) \}_{S_{UV_Key}}$$

라. VASP는 사용자에게 받은 암호화 메시지를 복호화 하여 값을 확인한다.

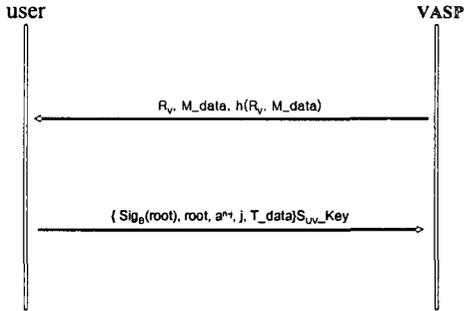


그림 4. 제안 시스템의 지블 프로토콜

(3) 분할 지급

사용자는 자신의 해쉬 체인의 첫 번째로 a^n 부터 a^{n-j} 까지를 이용하였다. 이후에 분할 사용을 위해 사용자는 j 값과 a^{n-j} 값을 저장한다. 두 번째 사용시의 k 만큼 지불한다면 사용자는 다음과 같이 계산하여 지불하여야 한다.

$j+k, a^{n-j+k}$ 의 값을 전송하여 지불한다.

5. 제안시스템 분석

이번 장에서는 제안시스템을 2장에서 논의한 보안 요구사항으로 분석한다.

(1) 안전성

위조 및 변조를 하려면 사용자가 root의 값을 변조하고 은행의 서명을 해야 한다.

root의 값을 변조하려면 R_b 를 알거나 임의의 값을 구해서 작성할 수 있다, 그렇지만 은행의 서명은 복사할 수 없으므로 인해 root의 값을 변경할 수 없다.

(2) 인증

사용자가 정당한 사용자인지 부정 사용자인지를 구별하는 방법으로 세션키를 생성할 수 있는가 없는가로 구별한다. 이는 미리 분배한 식별자를 가지고 있는 지를 확인하는 방법으로 가능하다. 임의의 수를 제 3자가 생성할 수 있으나, 세션키 생성으로 암호문을 확인하지 못함으로 이후의 부정에 대해서 막을 수 있다.

(3) 부인 봉쇄

인증에 사용된 세션키를 생성하기 위해서는 식별자와 자신이 생성한 난수를 이용한다. 이로 인해 자신이

생성한 것을 부인 할 수 없게 된다.

6. 결론 및 향후 방향

무선에서의 휴대 단말기와 서비스의 증가로 무선의 과금 및 금융 서비스를 안전하게 제공할 수 있는 방안에 대해 연구를 하였다. 무선에서의 지불시스템은 무선 휴대 단말기의 하드웨어의 능력 및 계산 능력을 최대한 효율성이 높게 할 수 있는 방안으로 연구를 수행해야 할 것이다.

이에 본 논문에서는 대칭키와 해쉬 함수를 이용하여 분할 지급할 수 있는 방안에 대해 연구를 하였다. 미리 나누어 갖는 식별자가 있으나, 이를 이용하여 무선에서 인증 및 세션키를 생성하여 지불에 이용한다.

그러나 익명성을 제공하지 못하는 단점을 가지고 있다. 향후 연구 방안으로는 익명성을 제공할 수 있는 방안 및 좀더 효율성을 높일 수 있는 방안에 대해 연구하여야 한다.

[참고문헌]

- [1] 장석철, “분할성 및 익명성 제어를 갖는 네트워크형 전자화폐 시스템에 관한 연구”, 석사학위논문, 순천향대학교 정보기술공학부, 2001년
- [2] 김선형, 김태윤, “이동 통신 시스템에서의 종단간 인증 및 지불 프로토콜”, 정보과학회2002, 추계학술대회 VOL 29, No 02, pp 115~117, 2002, 10
- [3] 이만호, 김광조, “이동 컴퓨팅 환경을 위한 소액 지불 시스템”, 2001년, CISC, 한국 정보보호학회 종합 학술 발표회 논문집 VOL.11, NO.01
- [4] UMTS Forum, “A Regulatory Framework for UMTS”, Report No. 01, 1997
- [5] R.Sai Anand, C.E.Veni Madhavan, “An Online, Transferable E-Cash payment system”, INDOCRYPT 2000, LNCS 1977, pp 93~103, 2000
- [6] Markus Stadler, Jean-Marc Piveteau, Jan Camenisch, “Fair Blind signatures”, EUROCRYPT’95, LNCS 921, pp 209~219, 1995
- [7] 이임영, “전자 상거래 보안 입문”, 생능 출판사, 2001년
- [8] 이임영의 3명, “컴퓨터 통신 보안”, 그린 출판사, 2001년