안전한 사용자 인증을 위한 패스워드 등록에 관한 연구

강서일*, 이임영
순천향대학교 정보기술공학부
e-mail : kop98@sch.ac.kr, imylee@sch.ac.kr

A Study on Secure Password Registration for User Authentication

Seo-Il Kang*, Im-Yeong Lee
Division of Information Technology Eng. Soonchunhyang Unoversity

요 약

휴대 단말기의 높은 보급률 및 무선 인터넷 망의 발달로 인해 휴대 단말기를 이용한 서비스가 증가하고 있는 추세이다. 이와 같은 서비스는 서비스를 받는 사용자의 인증을 필요로 한다. 다양한 서비스의 가입에 따른 사용자의 인증은 가입사가 인증하는 방안을 제시하고 있지만 접속하는 휴대 단말기를 사용하는 사용자에 대한 인증은 제공하지 않는다. 이로 인해 휴대 단말기의 도난이나 제삼자의 활용으로 휴대 단말기의 실질적 소유자가 피해를 입을 수 있다. 이에 휴대 단말기의 사용자 인증 서비스를 제공하고자 한다. 휴대 단말기의 사용자 인증은 휴대 단말기를 소지하고 있는 사용자, 또는 휴대 단말기를 활용하는 사용자가 실제 당사자인지를 확인하는 것이다. 본 논문에서는 사용자가 휴대 단말기의 서비스 제공업자(이동 통신회사)에 사용자의 패스워드를 등록하고 이를 활용하여 사용자 인증을 제공하는 방식에 대한 연구를 진행하였다.

1. 서론

최근의 휴대 단말기(휴대폰, PDA, 등)의 발달로 인해 많은 무선 서비스가 제공되고 있다. 이러한 서비스는 휴대 단말기를 가지고 있는 사용자에게 제공되는 것으로써 휴대 단말기를 사용자의 신뢰할 수 있는 기기로 활용하는 것이다. 이러한 서비스 중 휴대폰의 위치추적 서비스는 사용자의 위치를 알려주는 것으로 위급한 사항이나 위험한 사항을 사용자의 가족 혹은 친구들에게 알려주어 그 사항을 대처해 나가는 것이다. 또한 휴대폰을 이용한 소액의 결제 경우 휴대폰에 인증 메시지를 전송함으로 휴대폰의 사용자에 인증을 제공할 수 있다고 한다.

그러나 휴대폰을 이용한 서비스의 경우 사용자의 인증을 제공하지 못함으로 인해 휴대폰이나 PDA를 빌리거나 도난 당했을 때 다른 제 3자가 자신의 서비스를 활용하거나 서비스를 받을 수 있다. 특히 소액의 경우 적은 금액이지만 다른 인원의 결제를 대리적으로 해줄 수 있다. 이에 따라 결제에 대한 취소나 환불의 서비스가 제공될 수 없는 단점을 가지고 있다.

그 사유는 다음과 같다. 휴대폰의 소액 결제의 경우 지불 대행업체의 인증 메시지를 받아서 온라인 쇼핑몰의 결제창에 입력을 하면, 휴대폰의 요금에 통합되어 부과되는 서비스로써, 발급된 인증 메시지를 통해 휴대폰 인증 및 사용자 인증을 동시에 제공한다.

그러나 휴대폰의 인증 메시지의 경우 사용자의 인증보다는 휴대폰의 인증이 가깝고 휴대폰의 인증이 필요한 이유로는 휴대폰 요금에 통합 과금됨으로 꼭 필요한 사항이다. 이와 같은 이유로 소액 지불의 경우 거래 이후 거래 취소로 인한 환불받기가 매우 어려운 사항이다. 이와 같은 사항이 발생하는 이유로는 거래 당시의 휴대폰 사용자와 환불을 요구하는 사용자가 동일한지를 확인하기 어려운점을 가지고 있다.

본 논문은 사용자가 초기 인증정보를 가지고 이동통신 회사와 사용자 인증의 패스워드를 등록하기 위한 방안을 제시한다.

본 논문의 구성은 2절에서 휴대 단말기의 사용자 인증에 대한 보안 요구 사항을 논의하고, 3절에서

관련 연구에 대해 설명한다. 4절에서는 제안 방식에 논의하고 5절은 2절에서 언급한 보안 요구 사항에 따라 제안 방식을 분석한다. 6절에서는 결론 및 향후 연구 방향에 대해서 논의한다.

2. 휴대 단말기의 메시지 보안 요구 사항

휴대 단말기에서 전송되는 메시지는 다음과 같은 보안 요구사항은 다음과 같이 논의 될 수 있다.

- 접근 제어 : 휴대 단말기를 이용하는 사용자에 대해서 정당한 사용자가 아니면 이용할 수 없어야 한다.
- 인증 : 휴대 단말기의 경우 인증은 두 가지로 분류하여 사용자 인증과 휴대 단말기 인증이 있다.
- 기밀성 : 휴대 단말기의 메시지를 제 삼자가 가로채더라도 메시지의 내용을 알 수 없어야 한다.
- 무결성 : 메시지의 내용에 불법적인 수정 및 삭제가 되어서는 안된다.
- 재전송공격 : 인증의 패스워드 데이터를 가로채어 재전송 하더라도 정당한 사용자가 아닌 경우 인증되어서는 안된다.
- 위장 공격 : 제삼자가 사용자로 위장하거나 이동통신회사로 위장하여 정당한 사용자처럼 인증을 받아서는 안된다.

이와 같은 사항 외에도 다른 보안 요구사항을 논의 할 수 있으며, 본 논문에서는 사용자의 인증을 위해 패스워드를 등록하는 부분과 등록한 패스워드의 활용에 관해서 논의하겠다.

3. 관련 연구

패스워드를 활용하는 논문으로 다음과 같은 관련 연구를 알아본다. 패스워드는 사용자의 인증으로 활용되고 있다.

3.1 해쉬함수를 이용한 안전한 일회용 패스워드 인증 스킴

해쉬함수를 이용한 방식은 인터넷상에서 사용하는 사용자의 인증에서 서비스 거부 공격에 대한 대응방안으로 제시된 방식이다. 프로토콜에서 해쉬함수와 배타적 논리합을 활용 이용하여 사용자의 패스워드 등록 및 인증을 확인한다. 넌스값을 활용하여 매회 다른 패스워드를 생성하고 등록한다. 이를 위해 스마트 카드를 활용하고 있다.[1]

등록 단계에서 비밀값을 저장하여 스마트 카드를 발행하고 인증 시마다 스마트 카드를 활용하여 인증한다. 스마트 카드를 이용하여 사용자 인증을 하는 방식으로써 초기 제 삼자가 스마트 카드에 대한 접근 제어에 대한 언급이 생략되어 있다.

또한 안전성은 해쉬와 배타적 논리합에 의존되어 있다.

3.2 기밀성을 제공하는 상호 인증 일회용 패스워드 메커니즘 설계

기밀성을 제공하는 상호 인증 일회용 패스워드 방안은 상호 인증과 기밀성을 제공하기 위해 암호화 방식을 활용하고 있다. 제안 방식으로는 대칭키 암호화를 활용하며, 랜덤 수를 활용한다. 사용자는 다음의 사용되는 패스워드에 대해서 처음 활용되는 값에 다음 값의 의존된다. 대칭키를 활용함에 있어 패스워드의 안전성은 암호화 알고리즘에 의존하다. 패스워드의 제안 방식 및 키 분배에 대해 상호 인증을 제공한다.[2]

4. 제안 방식

본 제안 방식은 다음과 같이 초기 인증과 패스워드 등록 과정, 패스워드 사용과정으로 이루어져 있다. 초기 인증은 사용자가 이동통신회사와 가지고 있는 정보로 초기 휴대 단말기와 사용자를 인증하고 이후 초기 인증으로 등록된 패스워드를 이용하여 휴대 단말기 인증 및 사용자 인증을 제공할 수 있다. 각 메시지의 무결성을 위해 해쉬함수를 활용한다.

4.1 시스템 계수

본 논문에서 활용되는 시스템의 계수는 다음과 같다.

- User : 휴대 단말기를 이용하는 사용자
- Service Provider : 휴대 단말기의 무선 연결을 제공해주는 객체
- hex : 16진수로 휴대 단말기의 고유 일련번호
- M : 사용자의 개인 정보
- M_1 : 휴대 단말기에 부여받은 번호
- PW : 사용자가 입력한 등록 패스워드
- R : 서비스제공업체가 선택한 랜덤 수
- a : 사용자가 선택한 랜덤 수
- H(·) : 128비트의 일방향 해쉬 함수 값
- g : Zp상의 원시 원소
- p : 임의의 소수

4.2 초기 사용자 인증 및 패스워드 등록

초기 인증 및 패스워드 등록은 사용자가 사용하는 휴대단말기의 인증 및 사용자 인증을 수행하고 패스워드를 등록하는 과정이다. .

단계 1

사용자는 이동통신회사에 서비스를 요청하고 이동통신회사는 랜덤 수를 전송한다.

$$g^{R} (\mathrm{mod}\ p)$$

단계 2

사용자는 전송 받은 값에 다음과 같은 연산을 하여 각각의 데이터들을 전송한다.

$$H_1 = H(hex) \qquad H_2 = H(M)$$
$$H_3 = H(PW)$$
$$X = (H_1 + a) \qquad Y = (H_2 - a)$$
$$C = (H_1 + H_2)$$

이동통신회사에 전송하는 데이터는 다음과 같다.

$$g^{RC},\ g^{RX}$$

단계3

이동통신회사는 다음과 같은 연산으로 전송되어 온 데이터를 인증한다.

$$H_1 = H(hex),\ H_2 = H(M)$$
$$g^{RC} \stackrel{?}{=} g^{R(H_1 + H_2)}$$

증명: g^{RC}는 $g^{R(H_1 + H_2)}$임으로 좌변과 우변은 같다. 같으면 g^{RX}저장한다.

단계 4

사용자의 패스워드 등록 단계로 사용자는 다음의 데이터를 전송하고 앞서 인증 받은 데이터로 연산하여 새로운 패스워드를 등록한다.

$$g^{R(Y + H_3)},\ g^{H_3}$$

이동통신회사는 전송받은 데이터로 다음과 같은 연산을 한다.

$$g^{RC} \cdot g^{RH_3} \stackrel{?}{=} g^{R(Y + H_3)} \cdot g^{RX}$$

수식의 증명을 위해 다음과 같이 좌변을 정리한다.

$$g^{RC} \cdot g^{RH_3} = g^{RC + RH_3}$$
$$= g^{R(H_1 + H_2 + H_3)}$$

우변을 정리하여 좌변과 우변의 데이터가 같은 것을 확인한다.

$$g^{R(Y + H_3)} \cdot g^{RX} = g^{R(Y + H_3 + RX)}$$
$$= g^{R(H_2 - a + H_3 + H_1 + a)} = g^{R(H_2 + H_3 + H_1)}$$

좌변과 우변이 같으면, g^{H_3}를 등록한다.

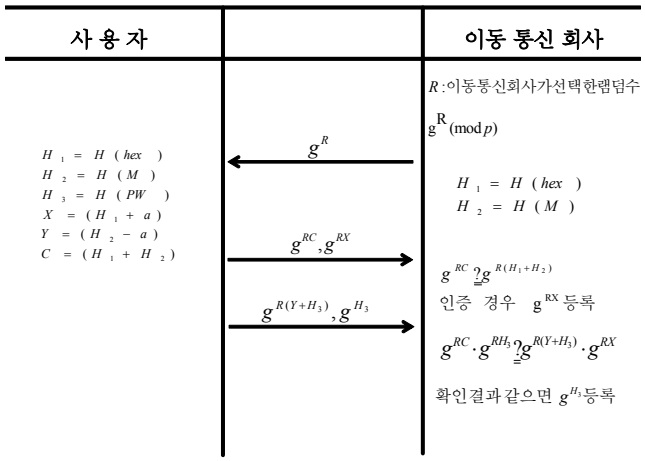

그림 1 사용자 인증 및 패스워드 등록

4.3 사용자 패스워드 인증

사용자는 자신이 초기 인증 당시 등록한 패스워드를 이용하여 사용자 인증을 받는다. 사용자 인증 받는 방법은 다음과 같다.

단계 1

사용자는 서비스를 활용 중에 사용자 인증이 필요하거나, 서비스를 등록하기 위해 다음과 같이 이동통신회사에 사용자 인증을 요청한다. 이동통신회사는 랜덤 수를 선택하여 사용자에게 전송한다.

$$g^{R_2}$$

2단계

사용자는 이동통신회사로부터 받은 데이터와 사용자가 등록한 패스워드를 이용하여 다음과 같은 데이터를 전송한다.

$$X_2 = g^{R_2(H_1 + a_2)}$$
$$Y_2 = g^{(H_3 - a_2)}$$

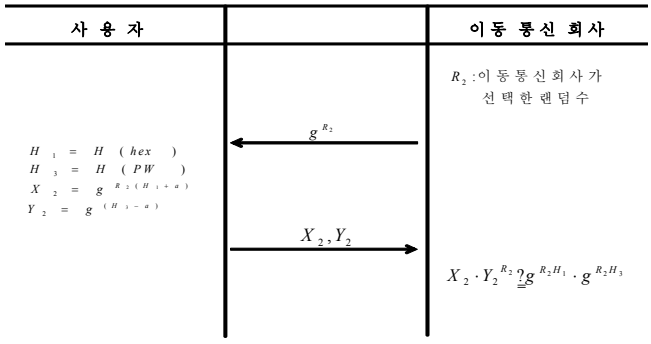

그림 2 패스워드 사용 프로토콜

3단계

이동통신회사는 사용자로부터 받은 데이터와 등록

되어있는 패스워드를 이용하여 사용자를 확인하고 인증한다.

$X \cdot Y^{R_2} = g^{R_2 H_1} \cdot g^{R_2 H_3}$의 좌변을 정리하면

$$X \cdot Y^{R_2} = g^{R_2(H_1 + a_2)} \cdot g^{R_2(H_3 - a_2)} = g^{R_2(H_1 + H_3)}$$

우변을 정리하면 $g^{R_2 H_1} \cdot g^{R_2 H_3} = g^{R_2(H_1 + H_3)}$ 임으로 정당한 사용자라는 것을 검증 할 수 있다.

5. 제안 방식 분석

본 논문에서 제안한 방식이 2절에서 언급한 보안 요구사항과 부합되는지 분석하겠다.

- 사용자 인증 : 초기 인증에서 사용자가 이동통신 회사에 등록한 개인의 정보를 가지고 인증하고 이후에 등록한 패스워드를 가지고 확인하다. 초기 인증에서 제삼자는 C의 값을 생성할 수 없으며, 이동통신회사는 C값을 생성하여 사용자를 인증할 수 있다.
- 휴대 단말기의 인증 : 본 제안 방식의 수식에 있어 H_1은 휴대 단말기의 고유한 값을 해쉬한 것으로 휴대 단말기의 인증을 제공하고 있다.
- 기밀성 : 이산대수의 문제를 활용함에 있어 지수승의 값을 알아내기는 무척 어려우며, 사용자와 이동통신회사는 자신들의 지수승 값을 알고 있기 때문에 각각의 값을 확인하기는 쉽다.
- 무결성 : 데이터의 값들은 해쉬를 취함으로 인해 각각의 값이 변화되는 경우 올바른 데이터 값을 생성할 수 없다.
- 부인 봉쇄 : 초기 인증과정과 패스워드 인증 과정에서 휴대 단말기의 고유번호 H1이 사용되다. 또한 각각의 값을 생성하기 위해서 사용되는 개인정보는 사용자만이 알고 있으므로 사용자는 부인 할 수 없다.
- 위장 공격 : 제 삼자가 이동통신회사로 위장하여 사용자의 전송 데이터를 얻는다 해도 지수승의 값을 모르는 이상 이동통신회사에 등록할 수 없다.
- 수정, 삭제, 변조 공격 : 초기 인증 과정에서 데이터에 등록되는 값을 제 삼자가 수정, 삭제, 변조하였을 경우 $g^{RC} \cdot g^{RH_3} \stackrel{?}{=} g^{R(Y + H_3)} \cdot g^{RX}$의 수식을 만족할 수 없으므로 인해 정당하게 인증되지 않는다. 패스워드 인증에서 임의 값을 전송한 경우는 다음의 수식을 만족시키지 못한다.

$$X \cdot Y^{R_2} = g^{R_2 H_1} \cdot g^{R_2 H_3}$$

그러므로 수정, 삭제, 변조의 공격을 막을 수 있다.

- 재전송공격 : 제 삼자가 데이터를 가로채어 재전송하는 경우 이동통신 회사의 랜덤 수가 각각의 통신마다 사용됨으로 가로챈 데이터는 사용할 수 없다.

본 방식은 관련 연구와 비교하여 일회용으로 사용되는 패스워드의 생성에 차이점이 있다. 관련 연구의 일회용 패스워드는 사용자가 각각의 랜덤 값으로 생성하고 이전의 값과 비교하여 확인하다. 그러나 본 연구의 패스워드는 이동통신회사의 응답으로 서로 패스워드를 확인할 수 있다. 또한 사용자 인증만 제공하는 것이 아니라 휴대 단말기에 대한 인증도 제공함으로 인해 신뢰할 수 있는 기기를 정당한 사용자가 활용하고 있음을 알 수 있다.

6. 결론 및 향후 연구 방향

본 논문에서는 휴대 단말기를 이용함에 있어 사용자 인증을 제공한다. 휴대 단말기 자체가 사용자의 신뢰된 기기로 볼 수 있으나 실제 있어서는 누구나 접근이 가능한 기기이며, 빌려주거나 빌려 사용하는데 있어 제약이 따르지 않는다. 그러나 기본적인 전화의 경우에 서비스에 제약을 두지 않지만, 인터넷을 이용한 서비스나 다른 부가 서비스의 신청 같은 경우 사용자의 인증이 필요하며, 이와 같은 필요성에 의해 패스워드 등록 및 이용에 대해 논의한 것이다. 본 논문에서는 초기 인증 이후 패스워드를 등록할 수 있는 방식을 언급하였다. 앞으로는 휴대 단말기를 활용 및 다양한 모바일 단말기들에서 활용될 것이며, 이와 같은 단말기에서의 카드 사용자의 인증 이외에도 단말기 사용자의 인증은 필요할 것으로 보며, 앞으로 지속적인 연구가 필요할 것으로 생각된다.

참고문헌

[1] 윤은주, 류은경, 유기영, “해쉬함수를 이용한 안전한 일회용 패스워드 인증 스킴”, 한국정보보호학회 동계 정보보호학술대회논문집 Vol.13, No2, pp.221～226

[2] 박희운, 이임영, ‘기밀성을 제공하는 상호 인증 일회용 패스워드 메커니즘 설계“, 2000년 한국정보처리학회 춘계 학술발표 논문집 제 7 권, 제 1 호

[3] 이주화, 설경수, 정민수, “자바카드 기반 무선단말기용 사용자 인증 프로토콜의 설계 및 구현”, 정보처리학회논문지 C, 제 10-C권, 제 5호, pp585~594

[4] 이임영, “전자상거래보안입문”, 생능출판사, 2001년

[5] 한국정보보호진흥원, “무선 전자결제시스템의 보안기술분석”, 2004년