모바일 환경에서 ID기반 티켓을 이용한 AAA 메커니즘에 관한 연구+

문종식, 이임영
순천향대학교 컴퓨터학부
e-mail:{comnik528, imylee}@sch.ac.kr

A Study on AAA Mechanism Using ID-based Ticket in Mobile Environment

Jong-Sik Moon, Im-Yeong Lee
Division of Computer Science and Engineering, Soonchunhyang University

요 약

본 연구는 모바일 디바이스가 홈 인증 서버로부터 인증을 받고 난 후에 외부 네트워크로 이동하더라도 홈 인증 서버로부터 발급받은 티켓을 이용하여 홈 인증 서버로 접근 하지 않고 외부 네트워크에서의 인증을 제공하여 서비스를 받을 수 있게 한다. 본 방식은 ID기반 티켓을 사용함으로써 정당한 사용자만이 서비스를 제공받을 수 있고 교환되는 메시지 및 지연을 줄이며 지속적인 서비스를 제공받을 수 있어 안전성과 효율성을 높일 수 있다

1. 서론

유비쿼터스 환경이 도래함에 따라 휴대용 디바이스의 수요는 급속도로 발전하고 있다. 사용자들은 다양한 서비스를 제공받고 있으며, 이동하면서도 동일한 서비스를 지속적으로 제공 받기를 원한다.

모바일 디바이스를 이용하여 네트워크 서비스를 제공받고자 접근하는 사용자를 인증, 인가, 과금하는 기술로는 여러 방식이 있으나, 본 연구에서는 ID기반 티켓으로 사용자 익명성과 프라이버시에 초점을 맞추어 편의성을 증대시키면서 안전하고 효율적인 방식을 제안한다. 2장에서는 보안 요구사항에 대하여 알아보고 3장에서는 기존 방식을 알아본다. 4장에서는 제안 방식에 대하여 설명하고 5장에서는 2장의 보안 요구사항으로 제안 방식을 분석한다. 마지막으로 6장에서는 결론 및 향후 연구방향으로 마치도록 한다.

2. 보안 요구사항

사용자가 서비스를 제공받고자 통신에 사용되는 데이터는 일반적으로 다음과 같은 보안 요구 사항을 만족해야 한다.

- 기밀성(Confidentiality) : 통신에 사용되는 데이터는 정당한 객체만이 확인할 수 있어야 한다.
- 무결성(Integrity) : 데이터는 중간에 위조, 삭제 및 변조 되지 않았음을 확인할 수 있어야 한다.
- 인증(Authentication) : 접근하는 사용자가 전송한 메시지의 출처가 정확히 확인되고, 정당한 사용자라는 것을 검증할 수 있어야 한다.
- 도청 공격(Eavesdropping) : 데이터는 공격자에게 노출될 수 있기 때문에 공격자가 데이터를 획득하더라도 값을 유추할 수 없도록 해야 한다.
- 재전송 공격(Replay Attack) : 통신 중에 전송되는 데이터를 제 3자가 획득하여 메시지를 재전송함으로써 인증 받는 것을 막을 수 있어야 한다.

3. 기존 연구

기존에 연구되었던 ID기반 방식은 다음과 같다.

3.1 ID기반 패스워드 인증 방식

이 방식은 2가지 ID기반 패스워드 인증 방식을 제안 하였다[1]. 그러나 지문 정보가 없더라도 비밀값을 알 수 있으며, 소극적 공격에 대한 취약점이 존재한다[2].

3.2 ID기반의 사용자 인증 방식

스마트카드를 이용한 ID기1반의 사용자 인증 방식은 다양한 공격에 대항할 수 있을 뿐만 아니라 안전성과 효율성을 제공한다. 그러나 시스템클럭의 동기화가 필요하며 스마트카드의 안전성에 절대적으로 의존하고 있다[3].

3.3 ID기반의 키 교환 방식

사용자의 식별 정보를 이용하여 두 시스템 간에 인증과 키 교환을 스마트카드를 이용하여 수행하는 ID 기반의 키 교환 프로토콜을 제안하였다. 그러나 연산량의 증가와 사용자의 편리성에 문제가 있으며 효율성을 떨어진다[4].

+ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음

4. 제안 방식

제안 방식은 모바일 디바이스를 사용하는 사용자가 홈 인증 서버에 접근하여 인증 후 티켓을 발급받고 나서 외부 네트워크로 이동하더라도 티켓을 제시함으로써 인증을 받아 서비스를 지속적으로 제공 받을 수 있다. 이와 같은 방식을 사용하면 인증 절차에서 일어나는 지연을 발생 시킬 수 있으며, 안전성과 효율성을 높일 수 있다.

4.1 제안 프로토콜

제안 프로토콜은 2단계로 이루어진다. 사용자 패스워드와 통신에 사요오디는 대칭키는 사전에 분재되었다고 가정하며, 각 단계는 인증 및 티켓 요청 단계, 외부네트워크에서 인증 단계로 이루어진다.

가. 인증 및 티켓 요청 단계

인증 및 티켓 요청 단계는 사용자가 홈 인증 서버에 인증을 요청하고 정당한 사용자에게 티켓을 발급받는 단계이며 발급받는 티켓은 아이디와 원타임 패스워드를 이용하여 구성한다.

Step 1. 사용자는 패스워드와 인증 시간 값을 XOR 연산하여 OTP를 생성한다. 사전에 공유된 대칭키를 이용하여 생성된 OTP와 사용자의 아이디, 인증 시간 값을 암호화 하여 홈 인증 서버에게 전송한다.

$$PW \oplus AT = OTP,\ E_{KS_{U-AAAH}}[ID_U,\ OTP,\ AT]$$

Step 2. 홈 인증 서버는 사용자로부터 전송받은 메시지를 공유된 대칭키로 복호화 한다. 서버에 저장되어 있던 패스워드와 인증 시간 값을 XOR연산 하여 OTP'를 생성한 다음 복호화한 메시지의 OTP와 비교한다. 값이 일치하면 아래와 같은 함수식에 따라 연산을 한 후 티켓을 생성한다. 생성된 티켓을 대칭키로 암호화하여 사용자에게 전송한다.

$$PW \oplus AT = OTP',\ OTP \stackrel{?}{=} OTP'$$

$$S_i = ID_U^{OTP},\ H_i = g^{OTP},\ X_i = g^{AT} \oplus S_i$$

$$Y_i = S_i \bullet H_i^{AT}$$

$$Ticket = ID_{AAAH}, Sign_{AAAH}[ID_U, Lifetime, h(X_i \| Y_i)]$$

$$E_{KS_{U-AAAH}}[Ticket]$$

Step 3. 사용자는 전송받은 메시지를 복호화 하여 티켓이 정당성을 검증 한다.

$$S_i = ID_U^{OTP},\ H_i = g^{OTP},\ X_i = g^{AT} \oplus S_i,$$

$$Y_i = S_i \bullet H_i^{AT},\ h(X_i \| Y_i) \stackrel{?}{=} h(X_i \| Y_i)'$$

나. 외부 네트워크에서 인증 단계

사용자가 홈 네트워크에서 외부 네트워크로 이동하였을 경우, 사용자는 티켓을 제시하여 인증을 받고 서비스를 지속 받을 수 있다.

Step 1. 사용자는 홈 네트워크에서 외부 네트워크로 이동 하였을 경우 사용자의 아이디, OTP, 인증 시간 값과 티켓을 대칭키로 암호화 하여 전송한다.

$$E_{KS_{U-AAAF}}[ID_U,\ OTP,\ AT,\ Ticket]$$

Step 2. 지역 인증 서버는 사용자로부터 전송받은 메시지를 복호화 하여 사용자의 정당성을 검증하여 인증이 완료되면 인증을 수락한다.

$$S_i' = ID_U^{OTP},\ H_i' = g^{OTP},\ X_i' = g^{AT} \oplus S_i$$

$$Y_i' = S_i \bullet H_i^{AT},\ h(X_i \| Y_i) \stackrel{?}{=} h(X_i \| Y_i)'$$

$$Y_i^{OTP^{-1}} = ID_U \bullet (X_i \oplus S_i)$$

5. 제안 방식 분석

제안 방식을 2장의 보안 요구사항에 맞추어 분석하면 다음과 같으며, 각 방식별 통신에 따른 연산량을 비교하면 다음 <표 1>과 같다.

- 기밀성 : 기밀성은 공유한 대칭키로 제공된다.
- 무결성 : 무결성은 통신에서 사용되는 메시지에 해쉬 연산($h(X_i \| Y_i)$)을 함으로써 제공된다.
- 인증 : OTP와 티켓을 검증함으로써 제공된다.
- 도청 공격 : 제 3자가 메시지를 획득하더라도 인증을 위한 값과 비밀 값 등을 유출할 수 없다.
- 재전송 공격 : OTP, AT와 티켓의 $Lifetime$을 사용함으로써 재전송 공격에 안전하다.

<표 1> 통신에 따른 연산량 분석

	2.1	2.2	2.3	**제안방식**
총 통신 횟수	3회	3회	3회	**4회**
초기인증통신 횟수	3회	3회	3회	**2회**
암호화 연산	S : 3회	S : 3회	S : 2회	**S : 3회**
해쉬 연산	1회	1회	1회	**1회**
보유키 갯수	1개	1개	2개	**n+1개**

[S : 대칭키 암호화 연산 n : 증가되는 서버의 수]

<표 2> 제안 방식 분석표

	2.1	2.2	2.3	**제안방식**
기밀성	○	○	○	**○**
무결성	○	○	○	**○**
인증	△	○	○	**○**
도청공격	X	△	△	**○**
재전송공격	X	○	○	**○**
효율성	X	△	△	**△**

[○:제공, 안전함 △:보통 X:제공 못함, 위험]

6. 결론

본 제안 방식은 사용자 인증을 위해 OTP와 ID 기반 티켓을 이용하여 사용자가 홈 네트워크에서 외부 네트워크로 이동하더라도 서비스를 지속 받을 수 있는 방안에 대하여 연구를 진행하였다. ID기반 티켓을 이용함으로써 통신 횟수를 줄이고 안전성과 효율성을 높였다. 그러나 각 서버와 대칭키 공유로 인해 서버가 증가할 시 보유 대칭키가 증가하며, 향후 외부네트워크에서의 티켓 갱신과 세션키 교환에 대한 추가적인 연구가 필요할 것으로 사료된다.

참고문헌

[1] H. S. Kim, S. W. Lee and K. Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," ACM Operating Systems Review, Vol. 37, No. 4, pp.32-41, 2003

[2] Michael Scott, "Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints," ACM Operating Systems Review, Vol. 38, pp.73-75, 2004

[3] 이원진, 김은주, 전일수, "스마트카드를 이용한 ID기반의 사용자 인증 프로토콜," 한국컴퓨터종합학술대회, Vol. 32, No. 1, pp166-168, 2005

[4] 배헌중, 김현성, 유기영, "스마트 카드를 이용한 ID기반의 키 교환 프로토콜," 한국정보과학회학술대회, Vol. 30, No. 1, pp491-493, 2003