모바일 사용자 인증을 위한 티켓기반 AAA 프로토콜에 관한 연구

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

A Study on Ticket-Based AAA Protocol for Mobile User Authentication

Jong-Sik Moon*, Im-Yeong Lee
Division of Computer, Soonchunhyang University

요 약

AAA(Authentication, Authorization, Accounting) 프로토콜은 기존의 유선망 뿐만 아니라 비약적으로 발전하고 있는 무선망에서 VoIP, Mobile IP 등과 같은 다양한 서비스 및 프로토콜 상에서 안전하고 신뢰성 있는 사용자 인증, 인가, 과금 기능을 체계적으로 제공하는 정보보호 기술이다. 그러나 현재 무선망은 유선망에 비해 외부로부터의 공격에 매우 취약하고 통신에 있어서 많은 제약사항이 뒤따르고 있다. 현재 IETF AAA 워킹그룹에서도 무선망에서의 안전한 AAA 프로토콜에 관하여 중요하게 다루고 있으며, 모바일 노드의 이동성에 따른 안전한 인증을 제공하는 방안에 대해서 활발히 연구 중이다. 따라서 본 연구에서는 모바일 노드가 홈 인증 서버로부터 인증을 받고 난 후에 외부 네트워크로 이동하더라도 홈 인증 서버로부터 발급받은 티켓을 이용하여 홈 인증 서버로 접근을 하지 않고 외부 네트워크에서의 인증을 제공하여 서비스를 받을 수 있게 한다. 본 방식은 티켓을 사용함으로써 교환되는 메시지 및 지연을 줄이고 지속적인 서비스를 제공받을 수 있어 효율성을 높일 수 있다.

1. 서론

컴퓨터 및 네트워크의 발전은 사용자들에게 다양한 서비스를 제공하고 있으며, 유선망에서 무선망으로 기술이 발전하면서 모바일 디바이스의 이용 또한 증가하게 되었다. 그러나 현재 무선망은 유선망에 비해 외부로부터의 공격에 매우 취약하고 통신에 있어서 많은 제약사항이 뒤따르고 있다. 이러한 문제점들을 해결하는 방안으로 무선망에서의 모바일 사용자의 인증 및 인가 기술로 IETF 표준안으로 삼고 있는 AAA기술이 있다. AAA는 유/무선 이동 및 인터넷 환경에서 사용자에 대한 안전하고, 신뢰성 있는 인증(Authentication), 인가(Authorization), 과금(Accounting) 기능을 체계적으로 제공하는 정보보호 기술이다. 현재 무선망에서의 모바일 사용자를 위한 인증, 인가, 과금 표준화를 목표로 다양한 응용 서비스에 대한 표준화 작업을 진행하고 있으며, 이 기종망간의 로밍 서비스 및 모바일 IPv6 네트워크망에서의 AAA를 이용한 다양한 연구가 진행 중 이다. AAA기술은 현재 보안의 심각한 문제를 일으키는 IPv4/IPv6기반 유/무선에서의 안전한 인증을 제공하고 이동에 따른 사용자에 대한 인증에서도 적용 가능함으로 인해 사용자의 편의성 및 보안 측면에서의 해결책을 가져다주고 있다. 모바일 디바이스를 이용하여 네트워크의 서비스를 제공받고자 접근하는 사용자를 인증, 인가, 과금 하는 방법으로는 여러 방식이 있으나, 본 연구에서는 사용자 인증과 인가에 초점을 맞추어 모바일 사용자가 다른 외부 네트워크로 이동하였더라도 서비스 이용 시에 편의성을 증대시키고 안전하고 효율적인 방식을 제안한다. 2장에서는 인증 및 인가의 보안요구사항에 대하여 알아보고 3장에서는 티켓을 이용한 기존 방식을 알아본다. 4장에서는 제안 방식에 대하여 설명하고 5장에서는 2장의 요구사항으로 제안 방식을 분석한다. 마지막으로 6장에서는 결론으로 마치도록 한다.

2. 보안 요구사항

모바일 사용자에게 서비스를 제공하는데 있어 접근하는 사용자가 정당한 사용자이며 서비스를 이용할 수 있다는 것을 확인 할 수 있어야 한다. 그러나 모바일 디바이스의 특성으로 인해 사용자는 다양한 외부의 네트워크를 통해서 접근할 수 있다. 또한 서비스를 이용하는 방안에 있어 접근시마다 인증을 제공하는 방안을 제시하고 있으나 이러한 방식은 매번 외부의 네트워크에서 홈 네트워크의 홈 인증 서버에게 까지 인증을 요청하는 문제가 발생할 수 있다. 이에 따라 한번 홈 인증 서버로부터 인증을 받은 후에는 외부의 인증 서버를 이용하여 서비스를 제공받는 방안에 대해서 논의가 되어져 왔다. 우선 외부의 지역 네트워크에서 홈 인증 서버에 접근하는 데이터는 일반적으로 다음과 같은 보안 사항이 제공되어야 한다.

- ❖ 기밀성 : 모바일 단말기에서 전송한 메시지는 인증 서버만이 알 수 있어야 한다.
- ❖ 무결성 : 전송되는 메시지는 중간에 위조, 삭제 그리고 변조할 수 없어야 하며, 만약 위조, 삭제 및 변조되었다면 그 사실을 알 수 있어야 한다.
- ❖ 인증 : 접근하는 사용자가 정당한 사용자라는 것을 검증할 수 있어야 한다.
- ❖ 접근제어 : 정당하지 않은 개체는 서비스를 이용할 수 없어야 한다.

위의 보안 요구사항 외에도 제 3자가 다음과 같은 공격을 할 수 있다.

- ❖ 재전송 공격 : 제 3자가 메시지를 재전송하여 인증 받는 것을 막을 수 있어야 한다.
- ❖ 위장 : 제 3자가 정당한 사용자처럼 접근하는 것을 막아야 한다.
- ❖ 위조 및 변조 : 제 3자가 메시지를 변경하거나 새로 생성하여 인증을 받을 수 없어야 한다.

그러므로 제안하는 방식은 위의 요구사항에 대해 만족해야 한다.

3. 기존 연구

기존에 티켓을 이용한 AAA 프로토콜은 사용자의 인증, 인가 및 빠른 핸드오프를 제안한 다음과 같은 방식이 있다.

3.1 실시간 Secondary Market 서비스를 위해 티켓에 기반한 AAA 프로토콜에 관한 방식

무선 통신 서비스의 수요가 급격히 증가함에 따라 무선 주파수의 부족이 무선 네트워크 발전의 걸림돌이 되고 있다[2]. 그러나 최근 주파수 대역이 충분히 활용되고 있지 않음을 보여주고 있으며, 이 문제에 대해서 주 사용자가 사용하지 않는 주파수를 일시적으로 이차 사용자에게 허가를 해주는 실시간 Secondary Market 개념을 소개하였다. 본 방식에서는 AAA 시스템 구조를 제안하고 이차 사용자를 인증, 인가하는 메커니즘과 다중의 이차 장치 간 동기화를 제공하면서 Secondary Market 서비스를 관리하는 방식을 제안하였다. 본 방식에서는 공개키를 이용하여 티켓을 브로드캐스트 하여 모든 단말기들이 자신의 티켓인지 확인하는 과정이 필요하며, 특히 티켓에 대한 안전성은 난수에 의존하고 있다.

3.2 Mobile IP 네트워크에서 티켓 기반한 AAA 보안 메커니즘에 관한 방식

본 방식은 IP기반 이동성을 가지는 AAA에 대해서 제안하였다[1]. 특히 ISP(Inter Service Provider)와 모바일 무선 사용자들을 위해 보안 문제와 효과적인 이동성 서비스에 대해 제안하였다. 본 방식에서는 MIPv6(Mobile IPv6)에서 모바일 노드를 인증하는데 지연 및 위험을 줄이고 모바일 노드를 인증하고 인가를 제공 할 수 있는 티켓방식의 새로운 AAA 서비스 메커니즘을 제안하였다. 또한 바인딩 업데이트에서 지연을 줄이기 위해 확장된 AAA 구조와 AAA 브로커 모델을 제안하였다.

시뮬레이션 결과 티켓을 사용함으로 인해 교환되는 메시지를 줄임으로써 AAA 브로커 모델의 응답속도를 최소화 하고 보안의 효율성을 높이며, AAA 모델의 응답속도가 줄어듦을 보여준다. 티켓은 안전성을 개선하기 위해 사용자 정보의 노출을 최소화하고 티켓의 유효시간 내에 서비스의 재인증이 요구되지 않기 때문에 효율성을 제공한다.

4. 제안 방식

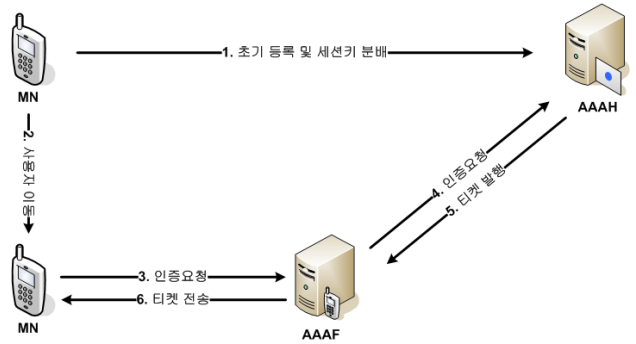
제안 방식은 모바일 디바이스 사용자가 홈 인증 서버로부터 인증 받고나서, 외부 네트워크로 이동하더라도 홈 인증 서버로부터 발급받은 티켓을 이용하여 서비스를 제공 받을 수 있다. 이와 같은 방식을 이용하면 모바일 디바이스 사용자가 외부 네트워크로 이동하더라도 홈 인증 서버로부터 재인증 없이 서비스를 지속적으로 받을 수 있다. 제안 방식은 총 4 단계로 이뤄지는데 사용자 패스워드와 통신에 사용되는 대칭키는 사전에 분배되었다고 가정하며, 등

록, 인증, 인가, 티켓 갱신 단계에 대하여 설명한다.

4.1 시스템 계수

다음은 본 제안 방식에서 사용되는 시스템 계수이다.

- ❖ $*$: 각각의 개체(U : 사용자, $AAAH$: 홈 인증 서버, $AAAF$: 외부 인증 서버)
- ❖ UID : 사용자의 아이디
- ❖ PWD : 사용자의 패스워드
- ❖ $h()$: 충돌성이 없는 안전한 일방향 해쉬 함수
- ❖ $H^n(PWD)$: 사용자의 패스워드를 n회 해쉬한 원 타임 패스워드
- ❖ r_* : $*$이 선택한 랜덤 수
- ❖ g^{r_*} : $*$이 선택한 랜덤 수를 곱셈군에 연산한 값
- ❖ E_*: $*$의 키로 암호화
- ❖ K_S : 사용자와 홈 인증 서버 사이의 대칭키
- ❖ $g^{r_* \cdot r_*}$: $*$와 $*$ 사이의 세션키
- ❖ $Sign_*$: $*$의 개인키로 서명
- ❖ P_* : $*$의 공개키
- ❖ $Lifetime$: 티켓의 유효시간
- ❖ T : Timestamp



(그림 1) 제안 방식 전체 흐름도

4.2 등록 단계

등록 단계는 사용자가 사전에 분배된 대칭키를 이용하여 원 타임 패스워드를 확인하는 절차이며, 세션키를 설립한다.

1단계 : 사용자는 홈 인증 서버에 자신의 아이디와 무결성을 제공하기 위한 해쉬 값 그리고 세션키를 설립할 값과 패스워드를 n회 해쉬한 값을 사전에 공유한 대칭키로 암호화 하여 전송한다.

$$UID,\ h(UID \| H^n(PWD) \| g^{r_U}),\ E_{K_S}[g^{r_U}, n]$$

2단계 : 홈 인증 서버는 사전에 등록된 사용자의 패스워드 값에 n회 해쉬 하여 전송된 값을 확인 하고 세션키를 생성한다. 이 후에 세션키를 설립할 값과 원 타임 패스워드를 대칭키로 암호화한 값을 해쉬 값과 전송한다.

$$h(H^{n-1}(PWD) \| g^{r_{AAAH}}),\ E_{K_S}[g^{r_{AAAH}}, H^{n-1}(PWD)]$$

4.3 인증 단계

사용자는 모바일 디바이스를 이용하여 외부 네트워크로 이동 하였을 때 홈 인증 서버로부터 정당한 사용자임을 인증 받아야 한다. 홈 인증 서버는 사용자 인증 후 외부 네트워크 인증 서버에 티켓을 전송하여 사용자가 세션이 끝난 후에 접근 하였을 때 재인증 절차 없이 서비스를 제공 받을 수 있게 한다.

1단계 : 사용자는 자신의 아이디와 세션키를 이용하여 원 타임 패스워드를 암호화한 값과 해쉬 값을 외부 인증 서버로 전송한다.

$$UID,\ E_{g^{r_U \cdot r_{AAAH}}}[H^{n-1}(PWD)],\ h(UID \| H^{n-1}(PWD))$$

2단계 : 외부 인증 서버는 사용자로부터 전송된 값과 자신이 정당한 외부 인증 서버라는 것을 제공하기 위해 자신의 아이디와 홈 인증 서버의 공개키로 암호화한 랜덤수를 개인키로 서명하여 전송한다.

$$UID,\ E_{g^{r_U \cdot r_{AAAH}}}[H^{n-1}(PWD)],\ h(UID \| H^{n-1}(PWD)),$$
$$Sign_{AAAF}(E_{P_{AAAH}}[r_{AAAF}] \| ID_{AAAF} \| h(r_{AAAF}))$$

3단계 : 홈 인증 서버는 외부 인증 서버의 서명을 확인하고 사용자 인증 후, 외부 인증 서버로 사용자가 사용할 티켓과 사용자와 외부 인증 서버간의 키 설립을 위한 값을 외부 인증 서버의 공개키로 암호화 하여 홈 인증 서버의 서명과 같이 전송한다.

$$E_{P_{AAAF}}[Ticket, H^{n-2}(PWD), g^{r_U}],$$
$$Sign_{AAAH}(ID_{AAAH} \| h(g^{r_U}))$$
$$Ticket = E_{g^{r_U \cdot r_{AAAF}}}[H^{n-2}(PWD), UID, T1, Lifetime]$$

4.3 인가 단계

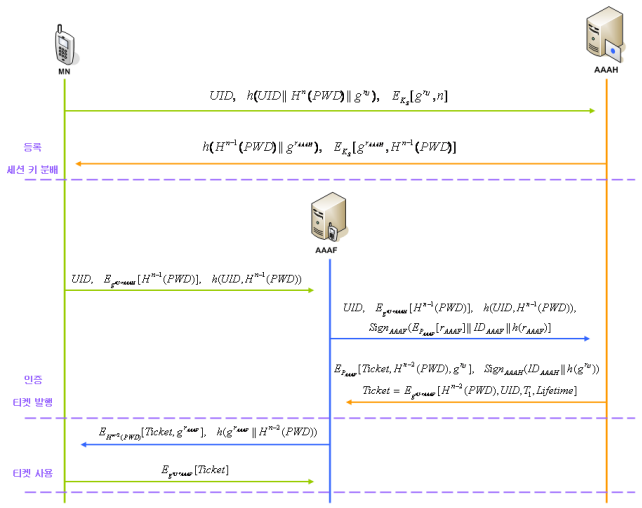
인가 단계는 외부 네트워크의 인증 서버가 사용자에게 티켓을 전송하고 사용자로부터 전송되어온 티켓이 정당한지 검증한다. 사용자는 외부 네트워크 내에서 이동하더라도 티켓을 이용하여 홈 인증 서버로부터 인증을 받지 않더라도 지속적으로 서비스를 제공 받을 수 있다.

1단계 : 외부 인증 서버는 사용자에게 발급한 티켓과 키 설립을 위한 값을 원 타임 패스워드로 암호화하여 해쉬 값과 전송한다.

$$E_{H^{n-2}(PWD)}[Ticket, g^{r_{AAAF}}],\ h(g^{r_{AAAF}} \| H^{n-2}(PWD))$$

2단계 : 사용자는 패스워드 검증 후, 외부 인증 서버와 설립한 세션키로 티켓을 전송하여 인증받고 서비스를 이용한다.

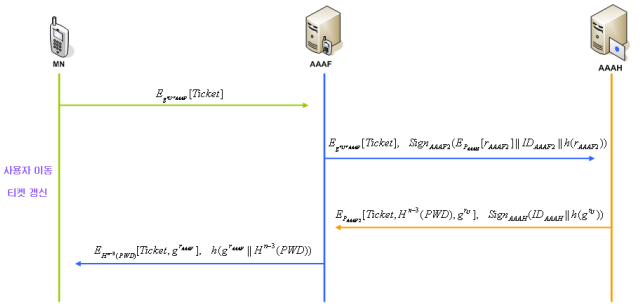
$$E_{g^{r_U \cdot r_{AAAF}}}[Ticket]$$



(그림 2) 등록 및 인증, 인가 단계 흐름도

4.4 티켓 갱신 단계

티켓 갱신 단계는 사용자가 접근한 외부 네트워크에서 다른 외부 네트워크로 이동 하였을 때 홈 인증 서버로부터 티켓을 갱신하여 서비스를 제공 받을 수 있어야 한다. 프로토콜은 (그림 3)과 같이 인증 단계와 인가 단계의 프로토콜과 유사하다.



(그림 3) 티켓 갱신 단계 흐름도

5. 제안 방식 분석

제안 방식을 2장의 보안 요구사항에 맞추어 분석하면 다음과 같다. 기밀성은 비밀리에 공유한 대칭키($E_{K_S}[g^{r_{AAAH}}, H^{n-1}(PWD)]$)와 통신에서 설립한 세션키($E_{g^{r_U \cdot r_{AAAH}}}[H^{n-1}(PWD)]$)를 이용하여 제공되며, 무결성은 해쉬 값($h(UID \| H^{n-1}(PWD))$)으로, 인증은 원 타임 패스워드($H^n(PWD)$)로 제공된다. 접근제어는 티켓을 이용함으로써 정당한 사용자만 서비스를 이용할 수 있다. 제 3자의 공격에 대한 안전성은 원 타임 패스워드를 이용함으로써 재전송 공격에 안전하며 외부 네트워크와 세션키를 설립하고 서버의 개인키로 서명($Sign_{AAAH}(ID_{AAAH} \| h(g^{r_U}))$)을 제공함으로써 위장 및 메시지를 위/변조 할 수 없다.

6. 결론

본 제안 방식은 모바일 사용자 인증을 위해 티켓을 기반으로 하여 외부 네트워크에서 지속적인 서비스를 제공하는 방안에 대하여 연구를 진행하였다. 또한 다른 외부 네트워크로 이동 하였을 경우, 티켓을 갱신하여 지속적으로 서비스를 제공 받을 수 있다. 이와 같은 방식으로 모바일 단말기의 메시지 교환 횟수와 지연을 줄일 수 있으며, 인증 시 마다 홈 인증 서버로 접근 할 필요가 없다. 따라서 홈 인증 서버의 부담을 줄일 수 있으며, 안전하고 효율적인 서비스를 제공할 수 있다. 무선 네트워크의 발전으로 모바일 사용자의 수는 점점 증가하고 있으며, 그에 따른 보안에 대한 요구 역시 증가 하고 있다. 이로 인해 무선 네트워크에서 안전하고 효율적인 AAA에 관한 연구가 활발히 진행 되고 있다. 본 방식에서는 인증 시 원 타임 패스워드를 이용하고 있지만, 향후 모바일 디바이스의 처리 능력의 향상 등을 고려하여 인증서를 이용한 인증방식에 대한 연구가 필요할 것이다.

참고문헌

[1] Jung-Min Park, Eun-Hui Base, Hye-Jin Pyeon, and Kijoon Chae, "A Ticket-Based AAA Security Mechanism in Mobile IP Network," ICCSA 2003

[2] Yihong Zhou, Dapeng Wu, and Scott M. Nettles, "On the Architecture of Authentication, Authorization, and Accounting for Real-Time Secondary Market Service," IJWMC 2005

[3] 서승현, 조태남, 이상호, "OTP-EKE : 원-타임-패스워드 기반의 키 교환 프로토콜," 한국정보과학회논문지 2002