사용자 익명성과 프라이버시 제공을 위한 블라인드 티켓 기반 AAA 서비스 모델에 관한 연구+

문종식*, 이임영

순천향대학교, 컴퓨터학부

A Study on Blind Ticket-Based AAA Service Model for User Anonymity and Privacy offer

Jong-Sik Moon*, Im-Yeong Lee

Division of computer, Soonchunhyang University

요 약

컴퓨터 및 네트워크의 발전은 사용자들에게 다양하고 풍부한 서비스를 제공하고 있다. 그러나 최근 사용자의 익명성, 프라이버시 측면에서 많은 문제점을 드러내고 있다. 따라서 본 연구에서는 사용자가 서비스를 이용하는데 안전하고 효율적이면서 사용자의 프라이버시 및 익명성을 제공할 수 있으며, 이동성을 고려하여 홈 네트워크에서 외부 네트워크로 이동하더라도 티켓을 사용하여 안전하고 빠른 인증을 제공할 수 있게 한다.

I. 서론

인터넷의 발전으로 인해 사용자들은 다양한 서비스를 제공받고 있으며, 휴대용 디바이스의 발전으로 이동하면서도 서비스를 제공 받기를 원한다. 그러나 현재 다양한 서비스와는 반대로 보안에는 많은 취약점을 드러내고 있다. 이러한 문제점들을 해결하는 방안으로 안전하고 효율적으로 사용자를 인증하고 인가 할 수 있는 기술로 IETF 표준안으로 삼고 있는 AAA(Authentication, Authorization, Accounting) 기술이 있다. AAA 프로토콜은 기존의 유선망뿐만 아니라 비약적으로 발전하고 있는 무선망에서 다양한 서비스 및 프로토콜 상에서 안전하고 신뢰성 있는 인증, 인가, 과금 기능을 체계적으로 제공하는 정보보호 기술이다. 네트워크 서비스를 제공받고자 접근하는 사용자를 인증, 인가, 과금 하는 기술로는 여러 방식이 있으나, 본 연구에서는 티켓을 기반으로 사용자 익명성과 프라이버시에 초점을 맞추어 편의성을 증대시키고 안전하고 효율적인 방식을 제안한다. 2장에서는 보안 요구사항에 대하여 알아보고 3장에서는 티켓을 이용한 기존 방식을 알아본다. 4장에서는 제안 방식에 대하여 설명하고 5장에서는 2장의 보안 요구사항으로 제안 방식을 분석한다. 마지막으로 6장에서는 결론으로 마치도록 한다.

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

II. 보안 요구사항

다양한 서비스를 제공하는데 있어 접근하는 사용자가 정당한 사용자이며 서비스를 이용할 수 있다는 것을 확인할 수 있어야 한다. 그러나 네트워크의 특성으로 인해 사용자는 다양한 외부의 네트워크를 통해 접근할 수 있다. 또한 서비스를 이용하는 방안에 있어 접근 시 마다 인증을 제공하는 방안을 제시하고 있으나 이러한 방식은 매번 외부의 네트워크에서 홈 네트워크의 인증 서버에 인증을 요청하여 오버헤드가 발생하는 문제가 있다.

이에 따라 초기 인증을 받은 사용자는 홈 인증 서버로부터 티켓을 발급받아 외부 네트워크로 이동하였을 때, 티켓을 이용하여 인증을 수행하는 방안에 대해서 논의가 되어져 왔다. 우선 외부의 네트워크에서 홈 인증 서버에 접근하는 데이터는

다음과 같은 보안 사항이 제공되어야 한다.

- 기밀성 : 사용자가 전송한 메시지는 통신 객체들만이 알 수 있다.
- 무결성 : 전송되는 메시지는 중간에 위조, 삭제 그리고 변조되지 않았음을 보여야 한다.
- 인증 : 접근하는 사용자가 정당한 사용자라는 것을 검증할 수 있어야 한다.
- 접근제어 : 정당하지 않은 사용자는 서비스를 이용할 수 없어야 한다.
- 익명성 : 사용자가 이용한 서비스에 대해서 제 3자가 알 수 없어야 한다.
- 프라이버시 : 사용자의 사적인 정보는 공개되지 않고 간섭 받지 않아야 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/변조 : 제 3자가 메시지를 변경하거나 생성하여 인증을 받을 수 없어야 한다.

또한 티켓을 이용함으로써 티켓의 요구사항은 다음과 같다.

- 위조 : 검증된 티켓으로 받아들일 수 있는 티켓의 생성이 불가능해야 한다.
- 복제 : 티켓은 하나만 존재하여야 하며 복사본이 존재해서는 안 된다.
- 변경 : 티켓의 내용을 변경할 수 없어야 한다.
- 재판매 : 다른 사용자에게 티켓이 양도될 수 있는가의 여부를 판단해야 한다.

그러므로 제안하는 방식은 티켓을 이용하여 인증을 수행함으로 위에서 언급한 모든 보안 요구사항을 고려해야 한다.

III. 기존 연구

티켓을 이용한 기존 연구로는 다음과 같은 방식이 있다.

1. Kerberos

가장 대표적으로 사용자에게 서비스를 안전하게 이용할 수 있도록 중앙 집중식 인증 서비스를 제공하는 Kerberos가 있다[1]. 사용자가 서비스를 제공받기 위해서는 인증 서버에서 티켓-승인 티켓을 발급 받고, 티켓 발행 서버에서 서비스-승인 티켓을 발행 받아 서비스를 이용하게 된다. Kerberos 프로토콜의 경우 패스워드의 취약점을 안고 있으며, 티켓 발행 서버가 세션키를 분배해주기 때문에 전송되는 메시지 정보를 알 수가 있어 익명성과 프라이버시를 제공하지 않는다. 또한 인증 서버와 티켓 발행 서버로 분리되어 있어 인증 시 지연이 발생할 수 있는 문제점을 안고 있다.

2. 익명성과 프라이버시 보장을 위한 인증 방식

본 방식에서는 다양한 서비스를 편리하게 이용할 수 있도록 EAP-TLS 인증 방식과 Symmetric-Key Key Establishment 방식을 이용하여 보다 효율적인 인증 메커니즘을 설계하였다[3]. 제안하는 메커니즘에서는 사용자가 인증서 방식을 통해 AAA 서버로부터 인증을 받으면 인증 서버와 가맹 관계에 있는 콘텐츠 제공자에는 별도의 로그인 과정 없이 서비스를 이용할 수 있는 SSO 서비스, 사용자 익명성, 프라이버시를 제공한다. 그러나 사용자 이동성 측면에 대한 고려사항은 논의 되지 않았다.

IV. 제안 방식

제안 방식은 사용자가 홈 인증 서버로부터 인증을 받고 나서 티켓을 발급 받은 후, 서비스를 이용하고자 할 때, 서비스 제공자에게 티켓을 제공함으로서 서비스를 이용할 수 있다. 또한 사용자가 이동하더라도 티켓을 이용하여 인증을 받을 수 있으며, 외부 인증 서버를 통해 티켓을 갱신 할 수 있다. 이와 같은 방식을 이용하면 인증 절차에서 발생하는 지연을 감소시킬 수 있으며, 사용자가 이동하더라도 티켓을 이용하여 빠른 인증을 수행할 수 있다. 또한 랜덤 아이디와 세션키 설립으로 익명성과 프라이버시를 제공받을 수 있다. 제안 방식은 총 3단계로 이뤄지는데 사용자 패스워드와 통신에 사용되는 대칭키는 사전에 분배되었다고 가정하며, 인증, 서비스 요청, 티켓 갱신 단계에 대하여 설명한다.

1. 시스템 계수

다음은 본 제안 방식에서 사용되는 시스템 계수이다.

- $*$: 각각의 개체(U:사용자, $AAAF$:외부인증서버, $AAAH$:홈인증서버, SP:서비스제공자)
- ID_* : 각각의 개체 아이디
- ID_R : 사용자의 랜덤 아이디 ($ID \oplus n$)
- $h()$: 충돌성이 없는 안전한 일방향 해쉬함수
- $H^n(PWD)$: $One-Time\ Password$

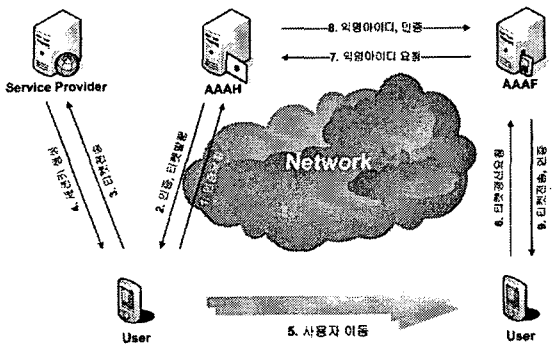

그림 1: 제안 방식 전체 흐름도.

- $E_*[]$: *의 키로 암호화
- K_S : 사용자와 홈 인증 서버 사이의 대칭키
- KU_* : *의 공개키
- KR_* : *의 개인키
- g^{R_*} : *이 선택한 랜덤수를 곱셈군에 연산 값
- $Sign_*$: *의 개인키로 서명
- MAV : *Mtual Authentication Value*
- $Lifetime$: 티켓의 유효시간
- T_* : *이 발행한 *Timestamp*

2. 인증 단계

초기 인증 및 티켓 발행 단계는 사전에 공유된 대칭키를 이용하여 사용자를 인증하며, 정당한 사용자에게 티켓을 발행한다.

Step 1. 사용자는 홈 인증 서버에 무결성과 인증을 제공하기 위한 원-타임 패스워드를 아이디와 연접한 값을 패스워드 해쉬 횟수 값을 사전에 공유한 대칭키로 암호화 하여 사용자의 아이디와 전송한다.

$$ID_U,\ E_{KS}[n,\ h(ID_U \| H^n(PWD))]$$

step 2. 홈 인증 서버는 그림 2와 같이 전송된 값을 검증한 후, 랜덤 아이디를 생성한다. 이후에 티켓을 생성하고, 티켓과 원-타임 패스워드를 대칭키로 암호화 하여 사용자에게 전송한다.

$$ID_R = ID \oplus n$$

$$E_{KS}[Ticket,\ n-1,\ H^{n-1}(PWD)]$$

3. 서비스 요청 단계

서비스를 이용하고자할 때, 사용자는 서비스 제공자와 세션키를 설립한 후에 티켓을 전송하여 인증 받고 서비스를 제공받을 수 있다. 이 단계에서 티켓에 포함된 사용자의 랜덤 아이디를 확인함으로써 익명성이 제공되고, 사용자와 서비스 제공자 사이에서 세션키를 설립함으로써 프라이버시를 제공한다.

Step 1. 사용자는 서비스 제공자에게 세션키 설립 인자와 상호 인증을 위한 값을 서비스 제공자의 공개키로 암호화 하여 전송한다.

$$E_{KU_{SP}}[g^{RU},\ MAV,\ h(g^{RU} \| MAV)]$$

Step 2. 서비스 제공자는 메시지의 무결성을 확인한 후, 세션키를 생성한다. 그리고 자신의 세션키 설립 인자를 서명한 값과 세션키로 상호 인증 값을 암호화 하여 전송한다.

$$Sign_{AAAF}[g^{RSP},\ h(g^{RSP})],$$

$$E_{Kg^{RU \cdot RSP}}[MAV-1,\ h(MAV-1)]$$

Step 3. 사용자는 설립된 세션키로 티켓과 상호 인증 값을 암호화하여 전송한다. 외부 인증 서버의 검증 후, 사용자는 서비스를 제공 받을 수 있다. 본 메시지를 통하여 사용자는 익명성과 프라이버시를 제공 받을 수 있다.

$$E_{Kg^{RU \cdot RSP}}[Ticket,\ MAV-2]$$

4. 지역 이동 및 티켓 갱신 단계

사용자가 홈 네트워크에서 외부 네트워크로 이동하였을 경우, 티켓의 유효시간이 만료되면 사용자는 티켓을 갱신할 수 있다.

Step 1. 사용자는 지역을 이동하여 티켓을 갱신하고자 할 경우, 외부 인증 서버에게 기존에 사용하던 티켓과 원-타임 패스워드를 외부 인증 서버의 공개키로 암호화 하여 전송한다.

$$E_{KU_{AAAF}}[Ticket,\ n-2,\ H^{n-2}(PWD)]$$

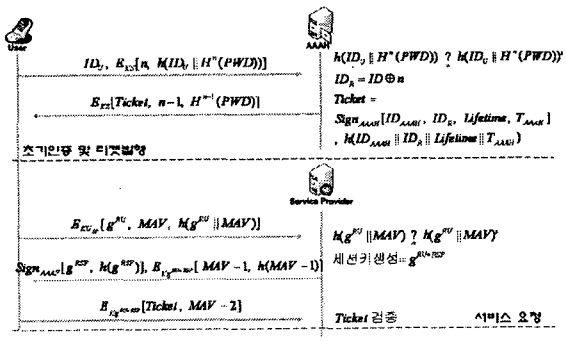

그림 2: 인증 및 서비스 요청 단계 프로토콜.

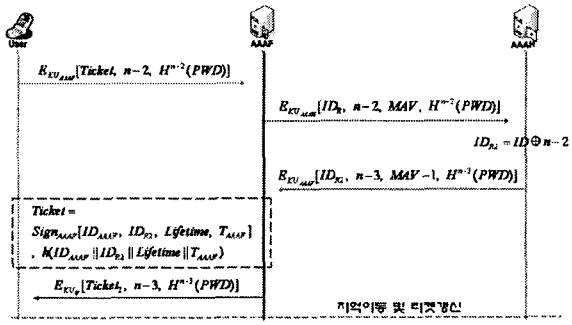

그림 3: 지역 이동 및 티켓 갱신 단계 프로토콜.

Step 2. 외부 인증 서버는 티켓에서 랜덤 아이디를 추출하고 원-타임 패스워드, 상호 인증 값, 랜덤 아이디를 홈 인증 서버의 공개키로 암호화하여 전송한다.

$$E_{KU_{AAAH}}[ID_R,\ n-2,\ MAV,\ H^{n-2}(PWD)]$$

Step 3. 홈 인증 서버는 랜덤 아이디와 원-타임 패스워드를 검증 후, 새로운 랜덤 아이디를 생성한다. 그리고 랜덤 아이디와 상호 인증 값, 원-타임 패스워드를 외부 인증 서버의 공개키로 암호화하여 전송한다.

$$E_{KU_{AAAF}}[ID_{R2},\ n-3,\ MAV-1,\ H^{n-3}(PWD)]$$

Step 4. 외부 인증 서버는 홈 인증 서버로부터 받은 랜덤 아이디를 포함하여 티켓을 갱신한 다음 사용자에게 갱신된 티켓과 홈 인증 서버로부터 전송 받은 원-타임 패스워드를 전송한다.

$$E_{KU}[Ticket_2,\ n-3,\ H^{n-3}(PWD)]$$

Step 5. 사용자는 이후 서비스 요청 단계와 동일하게 갱신된 티켓을 이용하여 서비스를 제공 받을 수 있다. 외부 인증 서버가 생성한 티켓의 동기화는 고려하지 않았으나, 외부 인증 서버와 홈 인증서버 간 안전하게 티켓을 전송함으로써 티켓을 동기화 시킬 수 있다.

V. 제안 방식 분석

제안 방식을 2장의 보안 요구사항에 맞추어 분석하면 다음과 같다.

- 기밀성 : 기밀성은 사전에 공유한 대칭키($E_{KS}[n,\ h(ID_U \| H^n(PWD))]$)와 통신에서 설립한 세션키($E_{Kg^{RU \cdot RSP}}[Ticket,\ MAV-2]$)로 제공된다.
- 무결성, 인증 : 해쉬 값($h(ID_U \| H^n(PWD))$)으로 무결성이 제공되며, 인증은 원-타임 패스워드($H^n(PWD)$)로 제공된다.
- 접근제어 : 정당한 사용자만이 티켓을 획득하여 서비스를 이용할 수 있음으로써 제공된다.
- 익명성과 프라이버시 : 티켓에 포함되어 있는 랜덤 아이디($ID_R = ID \oplus n$), 서비스 제공자와 통신에서 설립한 세션키($E_{Kg^{RU \cdot RSP}}$)로 제공한다.
- 효율성 : 티켓의 사용으로 인증 절차 지연 감소 및 효율성을 제공한다.
- 재전송, 위장 및 위/변조 : 제 3자의 공격으로부터의 안전성은 원-타임 패스워드와 홈 인증 서버의 서명($Sign_{AAAH}$)으로 제공된다.
- 복제, 위조, 변경, 재판매 : 티켓의 복제는 암호화 ($E_{KS}[Ticket,\ n-1,\ H^{n-1}(PWD)]$)로, 위조 및 변경은 랜덤 아이디($ID_R$), 티켓의 유효시간($Lifetime$), 서명($Sign_{AAAH}$)으로 티켓의 요구사항에 만족하며, 재판매에 대한 사항은 고려하지 않았다.

VI. 결론

본 제안 방식은 사용자 인증을 위해 티켓을 기반으로 하여 외부 네트워크에서 지속적인 서비스를 제공하는 방안에 대하여 연구를 진행하였다. 또한 티켓의 유효기간이 만료되더라도 티켓의 갱신으로 서비스를 지속할 수 있다. 이와 같은 방식으로 통신 횟수를 줄임으로써 지연을 감소시키고 효율성을 가져다주며, 최근 이슈가 되고 있는 사용자의 프라이버시 및 익명성을 제공 할 수 있다.

향후 유비쿼터스 사회가 도래됨에 따라 디바이스의 경량화, 소형화 및 이동성을 고려하여 보다 안전하고 효율적인 보안 프로토콜에 관한 연구가 필요할 것이다.

참고문헌

[1] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service ," RFC 4120, 2005

[2] Markus Hillenbrand, Joachim G¨otze, Jochen M¨uller, and Paul M¨uller, "Role-based AAA for Service Utilization in Federated Domains," DFN Arbeitstagung Düsseldorf, pp. 205-219, 2005.

[3] 이동명, 최효민, 이옥연, "익명성과 프라이버시 보장을 위한 효율적인 인증 메커니즘 설계," 한국정보처리학회 추계학술발표대회, PP. 941-944, 2005