이기종 네트워크 로밍환경에서 신뢰 관계 서버를 이용한 인증 메커니즘

문종식, 이임영
순천향대학교 컴퓨터학부
e-mail:jsmoon@sch.ac.kr

Authentication Mechanism using Trust Relationship Server in Heterogeneous Network Roaming Environment

Jong-Sik Moon, Im-Yeong Lee
Division of Computer science and Engineering, Soonchunhyang Univ.

요 약

인터넷 및 디바이스의 발달과 유비쿼터스 환경이 도래함에 따라 모바일 디바이스를 이용하여 서비스를 제공받고자 하는 수요는 급속도로 증가하고 있다. 유비쿼터스 환경에서 모바일 디바이스가 이기종 네트워크로 이동하여 언제, 어디서, 누구에게나 끊김없는 서비스를 제공하기 위해서는 이기종 네트워크간의 통신 및 디바이스간의 데이터 통신이 가능해야 한다. 그러나 동종 네트워크에서의 보안 기술 및 통신 기술로는 이기종 네트워크에 적용했을 때 확장성 및 안전성에 많은 문제가 따른다. 따라서 이기종 네트워크 로밍 환경에서 안전하고 효율적인 인증 메커니즘을 제안하였다.

1. 서론

인터넷 및 디바이스의 발달과 유비쿼터스 환경이 도래함에 따라 모바일 디바이스를 이용하여 서비스를 제공받고자 하는 수요는 급속도로 증가하고 있다. 유비쿼터스 환경에서 모바일 디바이스가 이기종 네트워크로 이동하여 언제, 어디서, 누구에게나 끊김없는 서비스를 제공하기 위해서는 이기종 네트워크간의 통신 및 디바이스간의 데이터 통신이 가능해야 한다. 그러나 동종 네트워크에서의 보안 기술 및 통신 기술로는 이기종 네트워크에 적용했을 때 확장성 및 안전성에 많은 문제가 따른다.

따라서 본 연구에서는 이기종 네트워크 로밍 환경에서 신뢰 관계 서버를 이용한 인증 메커니즘을 제안하였으며, ID기반 공개키 방식 및 티켓을 이용하여 안전하고 효율적인 인증을 제공하고자 한다. 본 논문은 2장에서는 보안 요구 사항에 대하여 알아보고 3장에서는 기존에 연구되었던 방식에 대하여 알아본다. 4장에서는 제안 방식을 설명하고 5장에서는 보안 요구 사항에 맞춰 제안 방식을 분석한다. 마지막으로 6장에서는 결론 및 향후 연구 방향에 대하여 논의하고 마치도록 한다.

2. 보안 요구 사항

이기종 네트워크에서는 기본적인 보안 요구 사항 외에 이기종 네트워크에서의 요구사항을 만족해야 한다. 각각의 요구 사항은 다음과 같다.

- 인증(Authentication) : 이기종 네트워크에서 이동하는 디바이스 및 서버의 신원이 정당하다는 것을 검증할 수 있어야 한다.
- 접근 제어(Access Control) : 접근을 얻으려는 각 실체는 각각에 맞는 접근 권한이 주어지도록 우선 식별과 인증 과정을 거쳐야 한다.
- 데이터 기밀성(Data Confidentiality) : 통신에 사용되는 데이터는 정당한 객체만이 확인할 수 있어야 한다. 가장 광범위한 서비스는 일정 기간 동안 두 사용자 사이의 모든 전송 자료를 보호하는 것이다.
- 데이터 무결성(Data Integrity) : 전송되는 데이터는 중간에 위조, 삭제 및 변조 되지 않았음을 확인할 수 있어야 한다.
- 상호 인증(Mutual Authentication) : 이기종 네트워크 및 무선 네트워크에서는 다양한 객체의 개입이 가능하기 때문에 상호인증이 고려되어야 한다.
- 빠른 로밍 인증(Fast Roaming Authentication) : 이기종 네트워크에서는 도메인간의 로밍이 빈번하게 일어나는데, 이때 인증에 소요되는 시간이 길면 부드러운 로밍 서비스를 제공할 수 없게 된다. 따라서 로밍 시 끊김없는 서비스를 제공하기 위해서는 빠른 인증에 대한 고려가 필요하다.
- 홈 인증 서버의 오버헤드(Overhead) : 원격지에서 홈 인증 서버로 전송되는 인증 요청이 빈번하게 일어나면 홈 인증 서버의 오버헤드가 발행할 수 있다.

또한 무선 네트워크의 취약점으로 인해 위의 보안 요구 사항 외에도 제 3자가 다음과 같은 공격을 할 수 있다.

- 재전송 공격(Replay Attack) : 하나의 데이터 단위를 수동적으로 획득하여 비인가된 결과를 생성하기 위하여 다시 전송하는 것을 막을 수 있어야 한다.
- 패스워드 추측 공격(Password Guessing Attack) : 안전하지 않은 통신로 상에서 악의적인 제 3자가 전송되는 메시지를 분석하여 패스워드를 추측하는 것을 막아야 한다.
- 도청 공격(Eavesdropping) : 통신로 상에서 전송되는 메시지를 악의적인 제 3자에게 노출될 수 있다. 따라서 제 3자가 메시지를 획득 하더라도 중요 값을 유추할 수 없어야 한다.

3. 기존 연구

이기종 네트워크에서 인증 방식과 ID 기반의 연구는 다음과 같다.

3.1 ID기반 패스워드 인증 방식

ID기반 패스워드 인증 방식은 타임스탬프 기반 방식과 난수 기반 방식의 2가지 ID기반 패스워드 인증 방식을 제안 하였으며, 다른 ID기반 방식들과는 달리 사용자들이 그들의 패스워드를 자유롭게 변경할 수 있다. 또한 시간 동기화가 되지 않는 네트워크를 위해 제안된 Nonce 기반 인증 방식은 메시지 재전송 공격에 안전하다[1]. 본 방식은 합법적인 사용자들을 인증 할 수 있고, 패스워드 추측 공격, 메시지 재전송 공격, 위장 공격으로부터 안전하다. 제안된 2가지 방식은 시스템에서 각 사용자의 알고 있는 것, 소유하고 있는 것 그리고 생물학적 측정에 의한 각 사용자를 인증하는 것을 요구한다. 이와 같은 특징은 본 방식의 신뢰성을 높여준다고 하고 있으나, 지문 정보가 없더라도 비밀 값을 알 수 있으며, 소극적 공격에 대한 취약점이 존재한다[3].

3.1 이기종 네트워크에서 ID기반 인증 키 교환 방식

ID 기반 인증 키 교환 방식은 이기종 무선 접속의 안전성을 위해 신원기반 인증과 AKE(Authentication Key Exchange)프로토콜을 제안하였으며, CK(Canetti and Krawczyk)-Model을 사용하여 이상적이고 안전한 키 교환 프로토콜을 처음 제안 하였다[2]. ID 기반 인증 키 교환 방식에서는 1984년 Shamir에 의해 처음 제안된 신원 기반 공개키 암호 시스템을 이용하여 효율적인 AKE 프로토콜을 디자인하였다. 인증서가 필요 없는 신원 기반 공개키 시스템은 공개키 암호의 장점을 그대로 가지면서 전통적인 인증서 기반 공개키 암호 시스템의 복잡성을 감소시켰다. 따라서 ID 기반 인증 키 교환 프로토콜은 사용자 측면에서 계산의 로드를 주로 고려하여 다른 방식들 보다 계산량에서 효율성을 높였다. 또한 안전성을 증명할 수 있는 CK-Model을 적용함으로써, 안전성을 증명하였으며, 메시지에 인증자를 적용하는 대신에 사용자와 네트워크 사이에 명시적인 상호 인증을 제공한다. 그러나 완전한 전방향 안전성을 제공하지 않으며, 부분적인 전방향 안전성만을 제공한다.

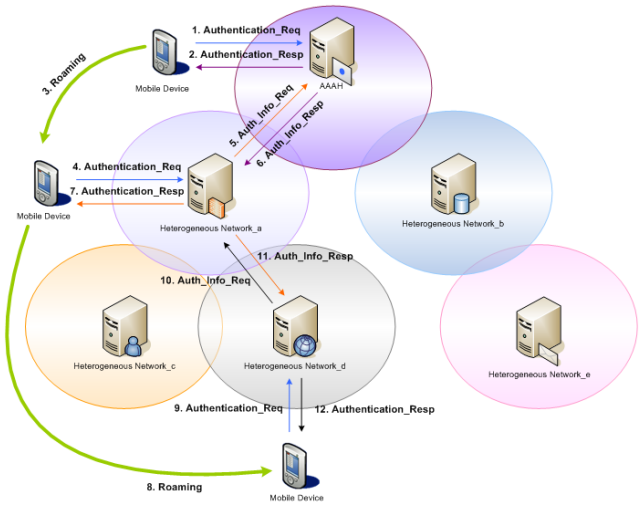
4. 제안 방식

네트워크의 통합으로 인해 모바일 디바이스를 이용하여 이기종 네트워크간의 로밍 서비스 및 인증을 제공받고자 하는 사용자는 지속적으로 증가할 것이다. 그러나 동종 네트워크간의 통신 기술 및 보안 기술로는 이기종 네트워크에 적용 시 많은 취약점이 발생할 수 있다. 따라서 제안 방식은 모바일 디바이스가 홈 네트워크에서 이기종 네트워크로 이동하더라도 홈 네트워크로 접근하지 않고 이기종 네트워크에서 인증을 받아 서비스를 지속 받을 수 있다. 또한 모바일 디바이스가 다른 이기종 네트워크로 이동하더라도 홈 네트워크로 접근하지 않고 신뢰 관계를 가지는 상위 이기종 네트워크로부터 인증 정보를 제공 받아 모바일 디바이스를 인증할 수 있다. 이와 같은 방식을 이용하면 인증 절차에서 일어날 수 있는 지연 및 홈 네트워크 서버의 오버헤드를 줄일 수 있으며, 안전하고 효율적인 서비스를 제공할 수 있다.

4.1 시스템 계수

다음은 본 제안 방식에서 사용되는 시스템 계수 이다.

- $*$: 각각의 개체 (MD : 모바일 디바이스, $AAAH$: 홈 네트워크 인증 서버, HN_* : 이기종 네트워크 인증서버)
- ID_* : $*$의 아이디
- PW : 모바일 다비이스의 패스워드
- g : 곱셈군 Z_n^*의 생성자
- $h()$: 충돌성이 없는 안전한 일방향 해쉬 함수
- OTP : 일회용 패스워드
- AT(Authentication Time) : 인증 시간 값
- α, β : 인증을 위한 인증 값
- MAC_* : $*$의 키로 생성한 MAC
- $Auth$: MAC을 기반으로 생성된 인증 값
- $E_*[\,]$: $*$의 키로 암호화
- $Sign_*$: $*$의 개인키로 서명
- KU_* : $*$의 ID 기반 공개키
- $KUCert_*$: $*$의 인증서 기반 공개키
- KR_* : $*$의 ID 기반 개인키
- KS : MD와 $AAAH$ 사이의 사전 공유키
- TK : 이기종 네트워크에서 설립한 세션키
- $Lifetime$: 티켓의 유효시간



(그림 1) 인증 메커니즘 전체 흐름도

4.2 제안 프로토콜

제안 프로토콜은 초기 인증 단계와 이기종 네트워크에서의 인증 단계, 신뢰 관계 서버를 이용한 인증 단계로 이루어지며, 모바일 디바이스의 패스워드와 초기 인증 단계에서 사용하는 대칭키는 등록 과정에서 분배 되었다고 가정한다. 인증 값 생성의 기본적인 개념은 Bilinear Pairing을 기반으로 한다.

4.2.1. 초기 인증 단계

초기 인증 단계는 모바일 디바이스가 등록 후 홈 네트워크 인증 서버로부터 인증을 받고 이기종 네트워크로 이동하였을 때 인증을 제공받을 수 있는 티켓을 발행 받는다.

step 1. 모바일 디바이스는 OTP를 생성하고 ID 기반 공개키/개인키 쌍을 생성한 다음, OTP와 인증 시간 값을 등록 단계에서 분배된 대칭키로 암호화 하여 아이디와 함께 전송한다.

$$OTP = h(AT_{MD}^{PW})$$
$$KU_{MD} = g^{ID_{MD}}$$
$$KR_{MD} = g^{ID_{MD}} \bullet Auth$$
$$ID_{MD}, E_{KS_{MD-AAAH}}[OTP, AT_{MD}]$$

step 2. 홈 인증 서버는 전송된 메시지를 복호화 하여 OTP'를 생성하여 비교한다. 값이 일치하면 MAC을 기반으로 생성된 인증 값($Auth$)을 생성하고 자신의 ID 기반 공개키/개인키 쌍을 생성한다. 그 후, 사용자 인증 정보 α, β를 생성하여 티켓을 구성한 다음 모바일 디바이스의 ID 기반 공개키로 암호화 하여 전송한다.

$$OTP' = h(AT_{MD}^{PW})$$
$$OTP' \stackrel{?}{=} OTP$$
$$Auth = MAC_{KS}[OTP]$$
$$KU_{AAAH} = g^{ID_{AAAH}}$$
$$KR_{AAAH} = g^{ID_{AAAH}} \bullet Auth$$
$$\alpha = AT_{AAAH} \bullet g^{ID_{AAAH}}$$
$$\beta = e(KR_{AAAH},\ AT_{AAAH} \bullet KU_{MD})$$
$$Ticket = ID_{AAAH},\ Sign_{AAAH}[ID_{MD},\ h(\alpha\|\beta),\ Lifetime]$$
$$E_{KU_{MD}}[Ticket,\ \alpha,\ \beta]$$

step 3. 모바일 디바이스는 전송된 값을 복호화 하고 β'를 생성하여 전송된 값과 비교하여 값이 일치하면 티켓의 정당성을 검증한다.

$$\beta' = e(KR_{MD},\ \alpha)$$
$$\beta' \stackrel{?}{=} \beta$$
$$h(\alpha\|\beta)' \stackrel{?}{=} h(\alpha\|\beta)$$

4.2.2 이기종 네트워크에서의 인증 단계

이기종 네트워크에서의 인증 단계는 모바일 디바이스가 이기종 네트워크로 이동하여 인증을 받고 서비스를 지속적으로 제공받고자 할 때, 이기종 네트워크 인증 서버에게 인증을 요청한다. 이기종 네트워크 서버는 홈 네트워크 인증 서버로부터 인증 정보를 제공받아 사용자를 인증 하고 서비스를 지속적으로 제공한다.

step 1. 모바일 디바이스는 이기종 네트워크로 이동하여 인증을 제공받고자 할 때, 이기종 네트워크 인증 서버에게 인증 요청을 한다. 이기종 네트워크는 홈 네트워크 인증 서버에게 인증 정보를 요청하면 홈 인증 서버는 사용자의 인증 정보를 이기종 네트워크 인증 서버의 인증서 기반 공개키로 암호화 하여 전송한다. 홈 네트워크 인증 서버와 이기종 네트워크 인증 서버는 신뢰 관계를 가지고 있다고 가정한다.

$$Authentication\_Req$$

$$Auth\_Info\_Req$$
$$E_{KU_{HN\_a}}[Auth,\ h(\alpha\|\beta)]$$

step 2. 이기종 네트워크 인증 서버는 자신의 ID 기반 공개키/개인키 싸을 생성하고 모바일 디바이스 에게 티켓 제시를 요청한다.

$$KU_{HN\_a} = g^{ID_{HN\_a}}$$
$$KR_{HN\_a} = g^{ID_{HN\_a}} \bullet Auth$$
$$Authentication\_Resp$$

step 3. 모바일 디바이스는 인증 값을 생성하고 티켓을 이기종 네트워크 인증 서버의 공개키로 암호화하여 전송한다.

$$\alpha_{MD} = AT_{MD} \cdot g^{ID_{MD}}$$
$$\beta_{MD} = e(KR_{MD},\ AT_{MD} \cdot KU_{HN\_a})$$
$$E_{KU_{HN\_a}}[Ticket,\ \alpha,\ \beta]$$

step 4. 이기종 네트워크 인증 서버는 β'의 값을 생성하고 전송된 값과 비교하여 값이 일치하면 임시키를 생성하여 전송한다.

$$\beta_{MD}' = e(KR_{HN\_a},\ \alpha_{MD})$$
$$\beta_{MD}' \stackrel{?}{=} \beta_{MD}$$
$$\alpha_{HN\_a} = AT_{HN\_a} \cdot g^{ID_{HN\_a}}$$
$$TK = e(KR_{HN\_a},\ \alpha_{MD} \cdot \alpha_{HN\_a})$$
$$E_{KU_{MD}}[\alpha_{HN\_a},\ h(TK)]$$

step 5. 모바일 디바이스는 전송된 인증 값을 가지고 임시키를 생성하여 값이 일치하면, 이후의 통신은 임시키를 가지고 안전하게 통신한다.

$$TK' = e(KR_{MD} \cdot \alpha_{HN\_a},\ AT_{MD} \cdot KU_{HN\_a})$$
$$TK' \stackrel{?}{=} TK$$

4.2.2 신뢰 관계 서버를 이용한 인증 단계

모바일 디바이스가 이기종 네트워크에서 다른 이기종 네트워크로 이동하였을 때, 홈 네트워크 인증 서버로 접근하지 않고 신뢰 관계에 있는 상위 이기종 네트워크 인증 서버로부터 인증 정보를 전송받아 사용자를 인증하여 서비스를 지속적으로 제공한다. 이는 로밍 시 매번 홈 네트워크 인증 서버로 접근하여 인증 요청을 하면 홈 네트워크 인증 서버의 오버헤드로 인한 효율성이 저하 될 수 있기 때문이다. 이와 같은 방식은 모바일 디바이스가 이동한 모든 인증 서버에 모바일 디바이스의 인증 정보가 남아 위험이 초래될 수 있으나, 티켓의 유효시간을 통해 주기적인 인증 정보 업데이트를 통해 해결할 수 있다.

5. 제안 방식 분석

제안 방식을 앞에서 언급한 요구 사항에 맞추어 분석하면 다음과 같다. 일반적인 보안 요구 사항에 대한 분석은 제외하고 이기종 네트워크의 보안 요구 사항을 초점으로 하여 분석한다.

- 상호 인증(Mutual Authentication) : 상호 인증은 통신하는 객체 간에 양방향으로 각각의 개체를 인증하는 것이다. 제안 방식은 초기 인증 단계에서는 홈 네트워크 인증서버는 모바일 디바이스의 OTP를 이용하여 인증을 확인하며, 모바일 디바이스는 홈 네트워크 인증 서버의 인증 값 α, β을 통해 β'를 계산하여 인증과 티켓의 정당성을 검증 할 수 있다. $\beta' = e(KR_{MD},\ \alpha)$는 $\beta' = e(g^{ID_{MD}} \cdot KR_{MD},\ AT_{AAAH} \cdot g^{ID_{AAAH}})$로 계산될 수 있다. 이는 홈 네트워크가 생성한 β을 풀어서 계산하면 $\beta = e(g^{ID_{AAAH}} \cdot Auth,\ AT_{AAAH} \cdot g^{ID_{MD}})$ 가되기 때문이다. 이기종 네트워크에서의 인증 단계와 이와 같은 방식으로 상호 인증을 제공한다.
- 빠른 로밍 인증(Fast Roaming Authentication) 및 홈 인증 서버의 오버헤드(Overhead) : 이기종 네트워크에서는 도메인간의 로밍이 빈번하게 일어나는데, 이때 인증에 소요되는 시간이 길면 부드러운 로밍 서비스를 제공할 수 없게 된다. 또한 원격지에서 홈 인증 서버로 전송되는 인증 요청이 빈번하게 일어나면 홈 인증 서버의 오버헤드가 발행할 수 있다. 따라서 제안 방식은 티켓을 이용한 빠른 인증을 제공하며, 계층적 신뢰 관계를 가지는 서버로부터 인증 정보를 제공받아 홈 네트워크 인증 서버로 접근하지 않기 때문에 홈 인증 서버의 부담을 줄일 수 있다.

6. 결론 및 향후 연구 방향

본 논문은 이기종 네트워크 로밍 환경에서 신뢰 관계 서버를 이용한 인증 메커니즘을 제안 하였다. 제안 방식은 이기종 네트워크로 로밍 시에 계층적 신뢰 관계를 가지는 상위 인증 서버로 인증 정보를 제공받아 모바일 디바이스를 인증하여, 홈 네트워크 인증 서버의 오버헤드를 줄일 수 있으며, 또한 경량화된 ID 기반 공개키 방식 및 티켓의 사용으로 빠른 인증을 제공하고 안전성을 강화시켰다. 향후 이기종 네트워크에서 티켓과 인증 정보의 갱신에 관한 연구가 필요할 것으로 사료되며, 인증 메커니즘을 기반으로 한 시스템 구성을 위한 데이터 타입 확립과 성능 분석에 대한 연구가 지속적으로 이루어져야 할 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] Jun Jiang, Chen He, Ling-ge Jiang, "On the Design of Provably Secure Identity-Based Authentication and Key Exchange Protocol for Heterogeneous Wireless Access," ICCNMC, pp.972-981, 2005.

[3] 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

[4] 이희진, 송유경, 이명수, 김종권, "계층적 캐싱을 이용해 로밍 확장성을 높인 인증 프레임워크," 정보과학회논문지, 제32권, 제5호, pp.561-573, 2005.