갱신 아이디를 이용한 AAA지역 인증 방안에 관한 연구

강서일° 이임영
순천향대학교 정보기술공학부
{kop98°, imylee}@sch.ac.kr

A study on the AAA Regional Authentication using renewal ID

Seo-Il Kang° Im-Yeong Lee
Division of Information Technology Engineering Soonchunyang University

요 약

AAA의 프레임워크를 이용한 모바일 단말 노드에 대한 인증 방식이 연구 진행되어지고 있다. AAA의구조에서는 홈인증서버가 다른 네트워크망을 이용하는 사용자를 인증한다. 이때 모바일 노드가 인증을 받고 나서 또 다른 네트워크로 이동하면, 다시 홈 인증 서버로부터 인증을 받아야 한다. 그러므로 본 연구에서는 단 하나의 ID와 패스워드를 통해 홈 인증 서버로부터 인증을 받고 난 후에는 다른 서버로 이동하더라도 인증 서비스를 제공받을 수 있도록 한다. 본 제안 방식은 외부 네트워크에서 홈 네트워크의 인증을 받아 오면 다른 외부 네트워크로 이동시 홈네트워크 인증 및 이전의 외부 네트워크의 인증을 제공하여 다시 홈네트워크로 접근하지 않도록 한다. 이와 같은 방식은 갱신 아이디를 사용함으로 인해 서비스가 제공된다.

1. 서 론

AAA는 Authentication(인증), Authorization(권한) 그리고 Accounting(과금)으로 이루어진다. 네트워크의 서비스를 이용하고자 접근하는 사용자를 인증하는 방법으로는 여러 방식이 있다. 아이디와 패스워드를 이용하는 가장 일반적인 방식 외에도 원타임 패스워드, 랜덤 수를 이용한 방식 등 다양한 방식이 있다. 모바일 기기를 이용하는 현 시점에서는 모바일 기기를 이용해서 서비스에 접근해야 한다. 그러나 모바일 기기는 이동성을 가지고 있고, 또한 네트워크의 서비스가 제공되는 위치가 꼭 자기가 속해있는 네트워크가 아닌 외부 네트워크 일 수도 있다. 그로인해, 서비스를 제공하고, 과금을 하기 위해서는 모바일 단말기를 정확히 인증할 수 있는 서비스가 제공되어야 한다. 그로 인해 모바일 단말기가 서비스를 제공받기 위해 접근하는 경우 외부 지역 네트워크에서 홈 네트워크로 접근하여 인증을 받고 나서 서비스를 제공받다. 이때 홈네트워크에서는 외부의 접근한 단말기가 정당한 단말기인지를 확인하여 인증하여 한다. 이러한 서비스가 앞으로의 홈네트워크 서비스나 다가올 유비쿼터스 사회에서는 중요한 기술로 이용될 것이다. 본 논문에서는 2장에서 보안 요구 사항을 도출하고 3장에서는 기존의 방식을 알아본다. 4장에서는 제안하는 방식에 대해 설명하고, 5장에서는 제안 방식을 보안 요구사항에 따라 분석한다. 6장에서는 결론을 도출한다.[1]

[1] 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성지원사업의 연구결과로 수행되었음

2. 보안 요구 사항

모바일 단말기를 이용한 서비스를 제공하는데 있어 접근하는 사용자가 정당한 사용자이며 서비스를 이용할 수 있다는 것을 확인 할 수 있어야 한다. 그러나 모바일 단말기의 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 인증 서버가 있는 홈 서버에게 까지 인증을 요청하는 문제가 발생할 수 있다. 이에 따라 한번 내부의 인증 서버로부터 인증을 받은 후에는 외부의 인증 서버를 이용하여 서비스를 제공받는 방안에 대해서 논의가 되어져 왔다. 우선 외부의 지역 네트워크에서 홈의 인증서버에 접근하는 데이터는 일반적으로 다음과 같은 보안 사항이 제공되어야 한다.

- 기밀성 : 모바일 단말기에서 전송되는 데이터는 홈 네트워크의 인증 서버에서만 알 수 있어야 한다.
- 무결성 : 모바일 단말기에서 전송되는 데이터가 변경되지 않았음을 보여야한다.
- 인증 : 접근하는 모바일 단말기가 정당한 단말기라는 것을 검증할 수 있어야 한다.

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

- 재전송 공격 : 제 3자가 이미 사용한 데이터를 다시

전송하여 인증 받는 것을 막을 수 있어야 한다.
• 위장 : 제 3자가 정당한 사용자 처럼 접근하는 것을 막아야 한다.
• 변조 및 위조 : 제 3자가 데이터를 변경하거나 새로 생성하여 인증을 받을 수 없어야 한다.

그럼으로 제공하는 방식은 위의 공격사항에 대해 안전해야 한다.

3. 기존 연구

기존 연구로는 다음과 같은 방식이 제안되어져 있다.

가. Mobile 환경에서의 AAA지역 등록 인증 개선 방안

본 방식은 지역 AAA서버에서 홈 AAA서버와 연동하여 AEM 메시지를 제공하고 모바일 노드가 접근하였을 때 해쉬값을 확인 절차를 거쳐 인증하게 되어 있다. 하지만 동일 외부 네트워크에서 서비스를 제공하며, 다른 외부 네트워크로 이동한다면 동일하게 홈AAA서버로부터 AEM 메시지를 발부 받아야 한다. 동일 외부 네트워크상에서는 인증에 대한 효율성을 제공하고 있다.

나. IEEE802.11 무선랜 기반의 Mobile IPv6 AAA환경에서 핸드오버 최적화 방안 연구

본 방식은 모바일 단말노드가 두개의 외부 네트워크를 걸쳐가는 경우 핸드 오프 방안으로 데이터를 줄이는 효율성을 나타내었다. 홈 인증서버로부터 인증 받는 방식은 기존의 기술을 기대로 이용하면서, 외부 네트워크에서의 다른 외부 네트워크로 이동하는 방안에 대해서 제시를 하였으나 역시 다른 외부 네트워크로 이동에 따른 홈 인증 서버의 인증을 받아오는 것이 필요하다.

다. authentic : Through Incremental Authentication Models to Secure Interconnected WI-FI WLANs

본 방식은 무선랜에서 인증을 통한 안전한 연결방식에 대해서 제안 하였다. 무선랜의 인증 기술로 WEP, AAA의 인증 서버로 RADIUS를 이용하는 방식을 설명하였다. 결론으로는 AAA의 중계자를 두어 AAA서버를 이용하는 방식에 효율성을 제공하는 방안을 제시하였다. 이때 활용하는 기술로는 DIAMETER/USIM을 적용하여 사용자에 대한 인증을 빠르게 제공하는 방안에 대하여 제시하였다. AAA의 중계자 역할은 초기 홈 인증서버로부터 단말 노드를 인증할 수 있는 값을 전송 받아 활용하는 방안을 이용하였다. 이런 경우 중계 인증 서버가 존재하는 네트워크에서만 서비스를 제공할 수 있으며, 중계 서버가 없는 네트워크에 모바일 노드가 접근하면 다시 홈 인증 서버로부터 인증을 받아야 하는 단점을 가지고 있다.

4. 제안 방식

제안 방식은 모바일 노드가 서로 다른 네트워크을 이동시에 홈 인증 서버로부터 지역 인증서버가 인증을 받고나서, 다른 지역 서버에 이동으로 인한 인증을 제공할 수 있게 되는 것이다. 이와 같은 방식을 이용하면 서로 다른 외부 네트워크를 이동하더라도 따로 홈 인증 서버로부터 인증을 받을 필요성이 없다. 이후 인증에 대한 검증을 제공함으로 인해 모바일 노드가 이동해온 경로로부터 인증을 제공 받았다는 것을 홈 인증서버가 검증할 수 있다.

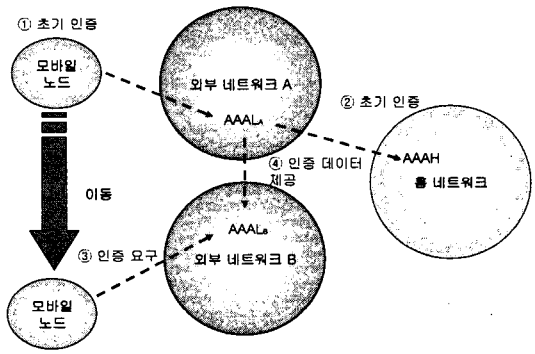

그림 1 제안 방식 흐름도

가. 제안 방식 시스템 계수

• MN : 모바일 노드
• FA : 외부 에이전트
• AAAL* : 외부 네트워크 인증 서버(* : 각각의 외부 네트워크)
• AAAH : 홈 인증 서버
• K_S : 모바일 노드와 홈 인증 서버과 비밀리에 공유한 대칭키
• R* : 의사 난수 발생기에서 생성한 랜덤 수(* : 객체로 모바일 노드, 홈 인증서버, 외부 네트워크)
• No : 외부 네트워크의 일련 번호
• ID_{MN} : 단말기 노드의 ID로써 홈 인증서버에 사전 등록되어 있다.
• Pk : 공개키로 각각의 인증 서버의 공개키가 된다.
• Sk : 개인키로 각각의 인증 서버의 개인키가 된다.

나. 제안 방식

제안 방식은 다음과 같이 진행된다.

1) 사전 등록

사용자는 자신의 모바일 단말기를 홈 인증 서버에 ID_{MN}과 K_S를 등록한다.

2) 외부 네트워크에서 접근

ㄱ. 외부 네트워크에서 사용자는 FA를 통해서 외부 인증 서버에 접근한다. 초기 데이터는 홈 인증 서버와 비밀리에 공유한 키를 이용하여 암호화 하여 전송한다. 이로 인해 홈 인증 서버에 까지 무결성과 기밀성이 제공

된다. 전송되는 데이터는 다음과 같다.

$ID_{MN}, K_S[R, h(ID_{MN}||R)]$

ㄴ. 전송되는 데이터는 외부 네트워크인 $AAAL_A$에서 인증이 되지 않으므로 홈 인증서버로 전송한다. 홈 인증서버는 전송된 데이터의 아이디를 보고 대칭키를 찾아 h 값을 검증하여 R의 값이 변경되지 않은 것을 확인한다. 이후 홈 인증서버는 다음과 같은 아이디와 대칭키를 생성하여 외부 인증서버의 공개키로 암호화하여 전송한다.

$$ID_{MN2} = ID \oplus R, K_{S2} = K_S \oplus R$$

$$PK_{AAALA}[ID_{MN2}, K_{S2}, sig(ID_{MN2})]$$

ㄷ. 전송된 데이터를 받은 외부 인증서버는 모바일 노드로 다음과 같이 인증에 부여하는 일련번호를 전송하여 모바일 노드와 사용할 아이디와 키를 생성하게 된다.

$$ID_{MNA} = ID_{MN2} \oplus No, K_{SA} = K_{S2} \oplus No$$

$$K_{S2}[No]$$

ㄹ. 모바일 노드는 전송받은 내용을 복호화하여 외부 네트워크에서 이용할 아이디와 키를 생성하여 이용하게 된다.

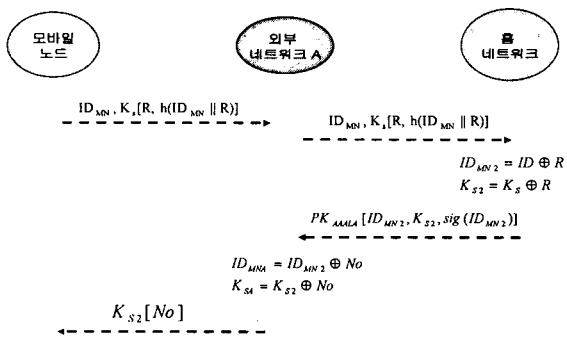

그림 2 인증 프로토콜 흐름도

ㅁ. 외부 네트워크B로 모바일 노드가 이동하면 기존의 방식에서는 다시 홈네트워크에서 인증을 받아왔지만, 외부 네트워크 A에서 B로 인증할 수 있는 정보를 제공한다. 즉 모바일 노드가 외부 네트워크A에서 사용하는 아이디와 비밀키의 정보를 외부 네트워크 B에게 전송하면서 인증을 제공하게 되는 것이다. 전송하는 데이터는 다음과 같다.

• 단말 노드에서 외부 네트워크 B로 전송하는 데이터

$$PK_{AAALB}[ID_{MNA}, No, K_{SA}[R, h(R)]]$$

• 외부 네트워크 B의 서버는 No를 보고 나서 외부 네트워크 A에게 인증을 요구한다. 즉 홈 네트워크 인증서버와 동일한 단계를 거친다.

이와 같은 과정으로 홈 네트워크의 서버를 받을 필요성 없이 외부 네트워크 A에서도 인증을 제공할 수 있게 된다.

5. 제안 방식 분석

제안 방식을 분석하면 다음과 같다. 기밀성은 공개키와 비밀키에 공유한 대칭키를 이용하여 제공된다.

무결성은 각각의 중요 메시지에 대해 해쉬 함수로써 제공된다.

외부 네트워크의 통신은 각각의 일련 번호로 구별을 할 수 있도록 한다.

식별값으로 인해 각각의 네트워크마다 각각의 대칭키를 생성할 수 있고, 아이디를 만들 수 있다. 검증 과정은 각각의 외부 네트워크에서 해줄 수 있게 되어 있다.

재전송의 공격의 경우 각각의 랜덤 수를 요청시 마다 이용함으로 인해 한번 사용한 메시지를 다시 사용할 수 없다.

6. 결론

외부 네트워크에서 갱신 아이디를 확인함으로 인해 홈 네트워크 인증 서버에서 한번만 인증을 받아오면 다시 접근 할 필요성이 없다. 그리고 홈 네트워크의 갱신 아이디는 마지막에 외부 네트워크의 일련 번호를 이용하여 검증 과정을 받아 마지막에 갱신을 하면 된다. 이와 같은 방식을 이용하여 외부 네트워크에서 인증을 받아 사용하는 아이디와 홈네트워크에서 인증 받아 사용하는 아이디를 동일하게 갱신 할 수 있도록 되어 있다.

본 제안 방식에서는 아이디 갱신만을 통해 인증을 각각의 외부 네트워크에서 제공해주는 방식을 이용하고 있다. 유비쿼터스 사회가 이루어 진다면 많은 단말기가 네트워크를 이용하게 될 것이다. 안전한 통신을 하기 위해서는 갱신 아이디 방식뿐만 아니라 키의 관리에 대해서도 염두를 해야 할 것으로 사료 된다.

[참고 문헌]

[1] Artur Hecker, Houda Labiod, Ahmed Serhrouchnei " Authentis : Trhrough Incremental Authentication Models to Secure Interconnected Wi-Fi WLANs, ASWN2002

[2] 이효성, 김기천, 김인수 "Mobile 환경에서의 AAA 지역 등록 인증 개선 방안", 한국정보처리학회 2004년 추계학술대회, pp1267-1270

[3] 진봉재, 허의남, 문영성, "IEEE802.11 무선랜 기반의 Mobile IPv6 AAA환경세서 핸드오버 최적화 방안 연구", 한국정보처리학회 2004년 추계학술대회, pp1201-1204

[4] 이임영, "전자상거래 보안 입문", 생능출판사, 2002년