패스워드 기반의 인증 및 키 교환에 관한 연구+

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

A Study on the Password-based Authenticated and Key Exchange

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

요 약

현대 사회에서는 다양한 모바일 단말기를 이용하여 서비스를 제공받고 있다. 그러나 현재 서비스를 제공받기 위해서는 서비스마다 자신의 정보를 등록하여야 하며, 다양한 네트워크를 통해서 접근함으로 인해 사용자가 이용하는 단말기와 안전한 통신을 하기 어려운 점이 있다. 본 연구는 홈 인증 서버를 이용하여 인증을 받은 이후에 외부 서비스 인증 서버와 세션키를 이용하여 안전한 서비스를 제공하는 방안을 제시한다. 모바일 단말기를 사용하는 사용자들은 하나의 인증 서비스를 통해 다양한 서비스를 제공 받을 수 있으므로 효율성을 높일 수 있다.

1. 서 론

현대 사회는 정보화 시대로써 다양한 기기를 이용하여 서비스를 제공받는다. 현재의 네트워크는 홈 네트워크를 구성하여 외부 네트워크를 통해서 홈 네트워크의 기기들을 통제 할 수 있으며, 단말기에 서비스를 제공하기 위해서는 사용자가 정당하다는 인증과 서비스를 받을 수 있는 권한 즉 인가 및 서비스에 대한 과금이 필요하게 된다. AAA는 인증, 인가와 과금을 동시에 제공하는 방안이다. 본 연구에 있어서 사용자가 등록되어 있는 홈 네트워크의 인증 서버로부터 인증을 받은 이후 외부의 인증 서버에 인증을 통보하여 서비스를 제공받을 수 있게 한다. 이때 외부 인증 서버와 사용자가 안전한 통신을 위해 세션키를 설립하도록 인자를 제공한다. 그로인해 사용자는 자신의 등록정보를 홈 인증 서버에만 등록하고 외부 인증 서버는 홈 인증 서버에서 제공하는 인증 정보와 설립한 세션키를 이용하여 서비스 제공와 안전한 통신을 하도록 한다.

본 논문에서는 인증과 세션키 교환을 제안한는 방식으로 2절에서 보안 요구 사항을 알아보고, 3절에서 기존의 아이디와 패스워드를 이용한 방식에 대하여 분석하며, 4절에서 제안 방식을 설명한다. 그리고 5절에서 제안 방식을 분석하며 6절에서 본 연구의 결과와 향후 연구 방안에 대하여 제시 한다.

2. 보안 요구 사항

본 논문에서 제공하는 인증과 서비스를 제공한기 위해서는 인증에 대한 보안 요구 사항 및 서비스에 대한 보안 요구 사항이 필요하다. 인증은 이용자가 정당한 이용자인지를 확인하는 과정으로써 사용자가 사전에 등록한 정보로 확인하는 방안 및 사용자가 증명할 수 있는 인자를 제공함으로 확인 할 수 있다. 그러므로 본 논문에서의 보안 요구 사항으로는 인증과 세션키에 대하여 다음과 같은 보안 요구 사항을 갖추어야 한다.

- 위장 : 정당하지 않은 사용자가 위장을 하여 인증을 받는 경우
- 재전송 공격 : 제 3자가 인증 메시지를 재전송하여 인증을 받는 경우
- 서버 위장 : 사용자에게 서버 위장을 통해 인증을 받을 수 있는 정보를 얻는 것
- 노출 : 인증의 정보 메시지가 노출되어 다른 제 3자가 메시지를 이용하는 경우
- Man in the middle 공격 : 제 3자가 중간에 끼어들어 세션키를 중간에 바꿔치기 하는 공격
- 위조 및 변조 : 인증 정보나 세션키에 대한 메시지를 위조하거나 변조하는 경우
- 기밀성 : 통신에서 정당한 객체만이 메시지를 확인 할 수 있음
- 무결성 : 전송되는 메시지가 변경되지 않은 것을 검증할 수 있음

위와 같은 보안 사항은 인증 서버 및 사용자 그리고 네트워크 전송 메시지에 대하여 제공되어야하는 보안 사항이다.

3. 기존 연구

기존의 ID와 패스워드를 이용하여 인증을 하는 경우 취약성으로 제시되는 것은 고정된 패스워드가 재전송이나 메시지의 위조 및 변경에 노출되어 있다는 것이다. 또한 패스워드의 경우 사용자가 일반적으로 자주 사용하는 단어나 숫자 영문자로 이루어져 사전 공격이나 추측 공격에 취약하며, 이와 같은 것을 보안하기 위하여 원타임 패스워드, 변형 패스워드 방식 등을 이용하고 있다.

3.1 패스워드 기반의 키 동의 기술에 대한 보안

+ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성지원사업의 연구결과로 수행되었음

사용자가 웹 서비스에 등록한 패스워드를 이용하여 사용자를 인증하고 세션키를 생성하여 이용한다[2]. 이와 같은 방법에 있어 기존에 사용자가 동일한 패스워드를 사용하는 취약점을 보강할 수 있는 방안을 제시하였다. 제시한 방안은 사용자가 이용하는 메시지 서버의 아이디를 추가하는 방안이다.

3.2 모바일 IP에서 동적 홈 에이전트에 등록 방안

모바일 IP를 이용하여 홈 네트워크에 접근하는 방법으로 모바일 IP가 매번 주소를 변경하여 서비스를 요청하므로 변경된 주소를 등록하는 방안을 제시하였다[3]. 기존의 갱신된 아이피를 등록하는 것은 홈 에이전트였으나 모바일 에이전트를 제시하여 모바일 노드가 홈 인증 서버에 접근하지 않고도 갱신하는 IP를 등록하여 서비스를 제공하는 방안이 된다.

4. 제안 방식

제안 방식은 모바일 단말기 사용자가 외부의 서비스를 제공받기 위해서 홈 인증 서버를 통해 외부 인증서버에 인증된 내용을 확인 받고 외부 서버와 안전한 통신을 위해 세션키를 설립하도록 한다. 그러므로 자신의 사전 정보는 홈 인증 서버에만 존재하도록 한다.

4.1 시스템 계수

제안 시스템의 시스템 계수는 다음과 같다.

- u : 사용자
- MN : 모바일 노드로써 단말기
- FA : 외부 에이전트
- AAAF : 외부 서비스를 제공하는 외부 인증 서버
- AAAH : 홈 인증 서버
- * : *는 각각의 객체
- ID* : *의 식별 아이디
- E* : 키 *로 암호화한 메시지
- D* : 키 *로 복호화
- h : 충돌성이 없는 일방향 해쉬 함수
- PIN : 패스워드로 사용할 수 있는 개인 식별 코드
- i : 인덱스 번호
- Si : i번호에 해당하는 값
- R* : *가 선택한 임의 랜덤 값
- Ks : 사용자와 홈 인증 서버가 비밀리에 공유한 대칭키
- Sig* : *의 개인키로 서명제공

4.2 인증 및 세션키 분배

외부의 서비스를 이용하기 위해 사용자는 자신의 단말기를 이용하여 홈 인증 서버에 접근한다.

1단계 : 사용자는 자신의 PIN과 Si의 값을 연접하여 해쉬를 하고 공유 대칭키로 암호화하여 외부 인증 서버에 전송한다.

$$E_{K_S}[h(\mathrm{PIN}\|S_i), i]$$

2단계 : 외부 인증 서버는 사용자 단말기를 인증할 정보가 없으므로 홈 인증 서버에 인증을 요청한다. 이때 자신이 정당한 외부 서비스 인증 서버라는 것을 제공하기 위해 개인키로 자신의 서버 ID를 서명하여 다음과 같이 전송한다.

$$E_{K_S}[h(\mathrm{PIN}\|S_i), i], Sig_{AAAF}(ID_{AAAF}\|h(R_{AAAF}))$$

3단계 : 홈 인증 서버는 외부 인증 서버로부터 제공된 메시지에서 공유키로 암호화 되어 있는 부분을 복호화하여 i번째의 Si값을 사용자의 PIN과 해쉬하여 정당한 값이 나오는지를 확인하고 외부 인증서버의 공개키를 가지고 와서 서명을 확인한다.

$$h(\mathrm{PIN}\|S_i) \stackrel{?}{=} h(\mathrm{PIN}'\|S'_i)$$

4단계 : 홈 인증 서버는 사용자를 인증한 다음 인증한 메시지를 외부 인증 서버 및 단말기에 전송하고 외부 인증 서버와 단말기가 활용할 수 있는 세션키를 설립할 수 있게 인자를 제공한다.

공유한 키로 암호화한 메시지 :

외부 인증 서버의 메시지에는 외부 인증 서버의 공개키를 이용하여 메시지를 전송한다.

외부 인증 서버의 공개키로 암호화한 메시지 :

$$E_{K_{AAAF}}[Sig_{AAAH}(ID_{AAAH}\|h(R_{AAAF})), g^a(\mathrm{mod}\, n)]$$

5단계 : 외부 인증 서버는 홈 인증 서버로부터 전송된 메시지를 복호화하고 서명 값을 확인한다. 그리고 자신이 전송한 해쉬 값과 동일한지를 확인한다. 이후 모바일 단말기 사용자와 통신을 위한 세션키 생성한다.

세션키 생성 과정 :

$$S_{K_{AAAF,MN}} = g^{ax_{AAAF}} \bmod n$$

6단계 : 사용자 단말기는 공유한 대칭키로 복호화를 하고 다음과 같이 외부 인증 서버과 공유할 수 있는 세션키를 생성한다. 이후 세션키에 대한 인증을 위해 외부 인증 서버에 메시지를 전송한다.

세션키를 생성하기 위해서는 외부 인증 서버의 공개키를 가지고와서 홈 인증 서버로부터 전송된 랜덤수를 지수승한다.

$$S_{K_{홈,AAAF}} = g^{x_{AAAF}a} \bmod n$$

동일한 세션키를 만들어다는 인증 메시지 전송 :

$$C = mg^{x_{AAAF}a} \bmod n$$
$$h(m)$$

외부 인증 서버에 전송되는 메시지 :

$$E_{K_{AAAF}}[C, h(m)]$$

7단계 : 외부 인증서버는 자신의 개인키를 이용하여 메시지를 복호화하여 획득한 메시지 m을 해쉬하여 같은 동일한 값인지 확인한다. 동일한 값으로 확인되면 사용자와 동일한 세션키를 가지고 있음을 인증하게 된다. 사용자가 외부 인증서버의 키를 확인하기 위해서 외부 인증 서버는 전송 받는 해쉬값을 자신의 아이디와 연접하여 세션키로 암호화 전송한다.

검증 방식 :

$$C = mg^{x_{AAAF}a} / g^{ax_{AAAF}} \bmod n = m'$$
$$h(m) \stackrel{?}{=} h(m')$$

외부 인증 서버에서 사용자에게 전송하는 메시지 :

$$E_{K_{S_{AAA,홈}}}[ID_{AAAF} \| m]$$

5. 제안 방식 분석

제안 방식에서 2장의 보안 요구 사항에 따른 분석을 하기 위해서는 다음과 같은 분석을 할 수 있다.

- 재전송의 공격 : 재전송의 경우 메시지 이전의 Si값을 저장해 두어 같은 값을 요구하지 못하도록 한다. 세션키의 경우 초기 설정에서 홈 인증 서버로부터 인자를 제공 받아 세션키를 생성하고 이후의 설립에서 홈 인증 서버가 매번 새로운 인자를 제공하므로 이미 사용한 키를 다시 사용하는 경우는 매우 작다.
- 위조 및 변조 : 메시지를 위조 및 변조한 경우 검증으로 제공되는 해쉬 값과 동일한 값이 생성되지 않으며, 위조 및 변조를 한 경우 서버들의 개인키로 서명을 제공하거 사용자의 비밀 공유키를 알 수 있어야 한다.
- 서버 위장 및 사용자 위장 : 서버 위장의 경우 아이디와 랜덤 값은 생성할 수 있으나 서버의 서명은 위조할 수 없으며, 홈 서버의 위장의 경우 서명 값에 외부 서버로부터 받은 랜덤 해쉬 값을 포함 시킬 수 없다.
- 제 3자가 중간의 객체로써 공격하기 위해서는 대칭키로 생성된 메시지를 수정할 수 있어야 한다. 동일하게 생성된 대칭키를 이용하여, 인증을 위해서 사용된 메시지가 노출 되지 않으므로 인해 중간에 제 3자가 개입할 수 없다.
- 무결성과 기밀성 : 메시지에 대한 암호화 적용 및 해쉬 함수를 적용하여 메시지에 대한 기밀성과 무결성을 제공한다.

이와 같이 보안 기술을 이용하여 사용자는 홈 인증 서버로부터 인증을 제공 받고, 세션키를 설립할 수 있는 값을 제공 받아 외부 인증 서버와 안전하게 통신하며 서비스를 제공 받을 수 있다.

6. 결론 및 향후 연구 방향

본 연구에서는 무선 네트워크를 이용하는 단말기를 기반으로 하여 서비스를 제공하는 방안에 대하여 연구를 진행하였다. 연구의 진행에 있어 단말기는 이미 홈 인증 서버에서 비밀 공유키와 PIN 그리고 Si값을 가지고 있다. 이와 같은 사전 등록 과정이 없으면 제 3자로부터의 공격으로 취약성을 가지고 있다. 하나의 단말기에 다양한 서비스를 제공하기 위해서는 보안 요청이나 보안 서비스가 간략하게 이루어져야 하며, 사용자에게 등록되어 있는 정보가 노출 되거나 중복 되어서는 안된다. 본 논문의 제안 방식에서는 외부 네트워크에서 홈 네트워크의 인증을 받아서 서비스를 활용하는 부분을 제시하였다. 이와 같은 부분은 외부의 서비스를 활용하는데 있어 인증을 위한 등록정보를 계속 제공하지 않아도 된다는 편리성을 가지고 있다. 그리고 키의 설립도 하나의 대칭키를 활용함으로 인해 효율성을 높였다. 하지만 향후 연구 방향으로는 단말기 하나를 가지고 모든 정보에 접근하기 위한 서비스 개발과 그에 따른 과금 방법 그리고 정당한 당사자끼리의 통신에 대한 안전성에 더욱 관심을 두어야 할 것이다.

[참고 문헌]

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

[2] Qiang Tang, J.Mitchell, "On the security of some password-based key agreement schemes", Cryptology ePrint Archive, 2005.

[3] Yu Chen, Terrance Boult, "Dynamic Home Agent Reassignment in Mobile IP", IEEE-WCNC02, 2002.

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

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

[6] 이임영, "전자상거래 보안 입문", 생능출판사, 2002년