AAA상에서 위치정보를 이용한 안전하고 빠른 Handoff 기법 설계

이덕규° 이임영
순천향대학교 정보기술공학부
{hbrhcdbr°, imylee}@sch.ac.kr

A Scheme on Secure and Fast Handoff Using Location Information with AAA

Deok Gyu Lee° Im Yeong Lee
Div. of Information Technology Engineering, Soonchunhyang University

요 약

여러 네트워크에서 사용자의 이동이나 인증 결과 처리를 최소하기 위한 서비스가 발전하고 있다. 그러나 인증, 권한 검증, 과금을 지원하는 AAA 기반의 망에서는 매 등록이 발생할 때 마다 새로운 세션 키가 필요하며 이를 위해 홈 망까지 등록 절차가 수행되어야 한다. 이것은 이동 노드 재인증 절차와 방문 홈에서 홈 망까지의 통신으로 인한 지연이 발생할 수 있다. 이같은 지연을 방지하기 위해 본 논문에서는 홈 망의 AAA 서버와 상관없이 이전의 할당된 세션 키를 이용하여 빠른 핸드오프 기법을 제안한다. 본 제안 방식은이전 방문 에이전트와 새로운 방문 에이전트간에 제 3자로 하여금 키를 공유하고 홈망까지의 통신이 필요없고 세션키의 기밀성과 무결성이 보장되도록 수행할 수 있다.

1. 서 론

최근 들어 이동 통신 환경의 비약적인 발전으로 로밍(Roaming) 서비스 등에 대한 사용자의 요구가 높아지고 있으며, Mobile IP, VoIP 및 VPN 등의 새로운 서비스가 등장하여 조만간 상용화가 이뤄질 것이다.

그러나 이러한 사용자의 다양한 요구사항과 새로운 서비스들의 본격적인 전개를 위해서는 무엇보다도 신뢰성 있는 정보보호 인프라의 구축이 선행되어야 한다. 즉 서비스에 대한 불법적인 사용자를 방지하고, 인가된 사용자에 대해 적절한 권한을 부여하며 그외 서비스 사용내역에 따른 과금을 부여하는 메커니즘이 필수적으로 구축되어야 한다.

AAA(Authentication, Authorization, Accounting)프로토콜은 이러한 다양한 네트워크와 프로토콜 상에서 안전하고 신뢰성있는 사용자의 인증, 권한관리 및 과금을 제공하는 정보보호 메커니즘으로써 현재 IETF에서는 차세대 AAA 프로토콜인 DIAMETER에서 로밍, Mobile IP등의 관련 응용 프로토콜의 표준화를 진행하고 있다.

그러나 기존의 AAA 프로토콜에서는 FA(Foreign Agent)가 사용자의 인증, 권한 검증, 과금 등에 수행할 때 FA는 홈 망까지 접근하여 사용자의 인증을 수행하게 되는데 이때 사용자의 빈번한 이동 및 세션키 갱신 시 매법 새롭게 갱신되어야하는 문제점을 가지고 있다. 이러한 문제점을 해결하고자 본 제안 방식에서는 이전에 할당된 세션키를 재사용함으로써 핸드오프로 인해 요구되는 새로운 세션키 할당의 필요성을 제거하고 또한 지역망과 홈망간에 신뢰할 수 있는 제 3자를 두어 제 3자에의해 기존 세션키를 이용하여 새로운 지역망에서 사용할 수 있는 세션키를 분배하는 방식을 제안한다. 이 방식은 기존 홈망까지 접근하여 사용자의 인증과 권한 검증을 수행하지 않고, 신뢰할 수 있는 제 3자로 하여금 사용자에게 새로운 세션키를 할당함으로써 사용자의 인증 및 권한 검증을 실시한다.

본 논문의 구성은 기존 방식에 대한 고찰 후에 제안방식에 대한 설명, 마지막으로 결론을 맺도록 한다.

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

2. 핸드오프 시 AAA를 이용한 등록 및 인증과정

사용자 인증은 가입자의 홈 망에 위치한 AAAH(Home AAA server)가 수행한다. 즉, Mobile IP 등록 시, AAAH는 Mobile IP 엔티티들이 사용할 세션 키를 생성하고, 이 키들을 동적으로 분배하는 키 분배 센터 역할을 수행한다. 키의 분배는 사전에 이뤄지지 않고 Mobile IP 등록 시점에 동적으로 분배되며, AAA 메시지내에 세션 키들이 Embedded 되어 전달된다. 사용자 인능 및 동적 SA 키 분배동작을 설명하면 다음과 같다. 매 Moble IP 세션마다 할당되는 세션 키는 lifetime을 가지며, 등록의 효율성을 기하기 위해 lifetime은 Mobile IP 등록 lifetime 보다 길게 지정된다. 즉 , 한번 인증된 결과를 계속된 다수의 Mobile IP 등록에서 활용한다.

2.1 관련된 세션키 교환 기법

본 논문에서와 같이 세션키를 안전하게 전달하기 위해

서는 제안된 다음과 같은 공개키 인증 기법들을 적용할 수 있다. Jacobs는 MIP에 공개키 인증 기법을 도입하였는데 이 기법에서는 등록 메시지들의 안전성을 위하여 MN과 FA 및 HA들간에 인증서를 사용하고, X.509 전자서명을 수행한다. MN, FA, HA 각기 상호간에 공개키 인증 기법에 따른 인증 동작을 수행한다. 메시지를 새로 만들거나 받은 메시지를 전달하는 경우, 메시지 뒤에 전자 서명을 추가함으로써 메시지의 무결성과 부인 봉쇄 기능을 제공한다.

Sufatrio. K. Lam의 MIP를 위한 최소 공개키 인증 기법을 제안하였는데 이 기법에서는 Jacobs의 공개키 인증 기법이 갖는 단점을 개선하기 위해 공개키 암호 연산을 최소화하였다. 그리고 공개키 방식과 비밀키 방식을 조합하여 적용함으로써 Jacobs의 기법에서 생기는 오버헤드를 최소화하였다.

IETF에서는 MOP를 위해 공개키 인증 기법을 적용하는 방안을 표준화하고 있고, 이 기법에서는 MN이 관여되지 않고 MIP 엔티티들과 AAA 엔티티들간의 노드간 상호 인증을 우해 공개키 인증 기법을 적용한다. 하지만 앞에서 언급한 공개키 인증 기법을 적용하여 사용할 수 있지만 공개키 암호 연산에 소요되는 시간은 빠른 핸드오프에 부적하다. 또한 인프라 구축에 많은 비용이 든다는 단점을 가지고 있다. 그리하여 본 논문에서는 공개키 인증 기법을 적용하여 제안하는 것이 아니라 세션키를 분배하고 이전 세션키를 이용함으로써 사용자의 빠른 핸드오프를 실현하도록 제안하였다.

2.2 AAA 인증과정

MIP 상에서는 RADIUS나 DIAMETER같은 AAA 서버가 다이얼 업 컴퓨터의 인증, 허가 서비스를 제공하기 우해 사용되고 있는데 이것은 MN에게 매우 중요하다. MIP는 MN과 HA간에 강력한 인증을 요구하기 때문이다. AAA 서버들은 MN을 식별하기 위해 NAI를 사용하고 이때 항상 홈 주소가 필요하지는 않다. 그래서 MN들은 홈 주소 없이 자신을 인증하고 Foreign Domain에 접속허가를 받는 것이 가능하다. MIP가 동작하려면 MN은 HA와의 SA를 가져와야만 한다. MIP 등록 응답이 MN-AAA 인증확장(MN-AAA Authentication Extension)에 의해 인증되면 MN은 AAA 서버가 만든 키 들을 확장 안에서 확인 할 수 있고 HA나 FA나 FA와의 SA를 생성하는 일을 신뢰할 수 있게 된다.

AAA 서비의 인증과정을 살펴보면 다음과 같다.

- MN이 홈 네트워크에서 떠나면 홈 주소를 가지지 않기 때문에 HA와의 보안 협력을 가지지 않게 된다.
- MN이 처음으로 HA에 등록할 때 등록요청에 MN-AAA 인증확장을 포함한다.
- MN-AAA 인증 확장내의 정보가 AAA 서버에 의해 확인되면 AAA서버는 MN을 위해 키를 생성하고 MN과의 SA에따라 키를 생성한 후 등록응답에 삽입한다.
- 만약 응답이 인증을 통과하고, AAA 확장안에 MN-HA 키가 포함되어 있으면 MN은 AAA와의 SA에 따라 키를 복호한다. 키는 HA와의 보안협력을 생성하고, MN-HA 인증확장을 인증하는데에 사용된다.
- 유사하게 만약 응답이 인증을 통과하고 AAA 확장안에 MN-FA 키가 포함되어 있으면 MN은 AAA와의 SA에 따라 키를 복호한다. 키는 FA와의 SA를 생성하고 MN_FA 인증 확장을 인증하는데에 사용된다.

3. 제안 방식

본 제안 방식은 지역 등록에서 적용하며 이를 위해 최초 발급된 세션키를 재사용한다. 공개키 연산대신 신뢰할 수 있는 제 3자를 두어 키를 공유하는 방법을 제안한다. 제안 방식에서는 TT가 FA들간에 신뢰할 수 있는 제 3자 역할을 수행한다.

지역 등록에서 정의된 것과 같이 TT는 계층산 상위에 존재하며, 다수의 FA들을 하위에서 관리한다. TT는 로컬 망내에 위치하는 AAAF와 사전 SA(Security Association)가 설정되어 있으며, 해당 망내에서 신뢰할수 공간내에 존재한다고 가정한다. 이종망간에 발생하는 핸드오프는 제안한 알고리즘으로 동작하지 않고 홈 망까지의 재 등록, 재 인증 절차가 수행한다.

3.1 시스템 계수

본 제안방식에서는 다음의 시스템 계수를 사용하여 설명한다.

S_* : (* : MN과 FA간, FA-HA간, MN과 HA간 공유되는 세션키)
DK_* : 임시로 연산하는 동적 세션키
$E_K(\ )$: 키 K로 암호화한 값
K_{TT} : TT와 공유되는 공유키
R : 랜덤값
F_{ID} : FA의 Identity
MSG_{req} : 지역 등록 요청 메시지
MSG_{rsp} : 지역 등록 응답 메시지

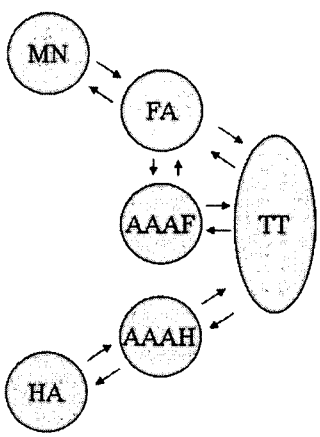

그림 1 제안 방식

3.2 제안 방식

본 제안 방식의 다음의 3가지 단계에 따라 진행된다.

3.2.1 라우터 요청 및 변경

MN은 자신이 이동 노드인 것을 알리기 위해 이동 메시지를 FA에 요구하며 과정은 다음과 같다.

Step 1. MN는 FA에게 자신의 이동을 알리고 자신이 전송할 메시지를 생성하여 전송한다.

$MN \rightarrow FA: R_{msg}$

FA랜덤 넘버 R선택

$FA\ compute\ DK_{MN-FA}$

$MSG = E_{DK}\{S_{MN-FA}, S_{FA-HA}\}$

Step 2. FA는 전송받은 메시지를 다음과 같은 메시지를 생성하고 보관한다.

$Stored\ FA: R, F_{ID}, MSG$

3.2.2 등록 요청

다음은 MN에서 FA를 거쳐 실제적으로 등록 요청하는 단계에 대하여 설명한다.

Step 1. MN는 FA에게 지역 등록 요청 메시지와 함께 랜덤값, FA의 Identity를 전송한다.

$MN \rightarrow FA: MSG_{req}, R, F_{ID}$

Step 2. 전송받은 FA는 사전에 받은 값과 비교하고 보관하고 암호화된 메시지를 복호화한다.

Step 3. FA는 자신이 받은 메시지를 최초 AAAF를 거쳐 TT에 전송한다.

$FA \rightarrow TT: MSG_{req}, R, F_{ID}, E_{DK}\{M\}$

3.2.3 등록 응답

TT로부터 등록 응답 메시지를 수신한 FA는 등록 응답 처리를 수행한 후, DK로 복호화하여 키를 추출하고 이전에 할당한 세션키를 획득한다. 이 키를 핸드오프 이후에 사용할 키로 변경하고 이에 대한 등록 메시지를 MN에게 송신하고 절차를 마감한다.

Step 1. TT는 FA에게 다음의 메시지와 암호화한 값을 전송한다. E내부에는 K_{TT}가 위치해 있으며, DK로 복호할 수 있도록 사전에 DK로 암호화되어 전송된다.

$TT \rightarrow FA: MSG_{rsp}, E$

Step 2. 최종적으로 FA로부터 MN에게 응답 완료메시지가 전송되고 사전에 분배받은 세션키를 이용하여 서비스를 이용할 수 있다.

$FA \rightarrow MN: MSG_{rsp}$

4. 결 론

최근 네트워크 환경은 여러 서비스와 시스템 발전으로 사용권한에 대한 세부적이고 안전한 접근 및 제어가 요구되고 있다. 이와 같은 환경에서 기존의 AAA 서버에 의존한 지역 등록 문제점 및 한계점을 가질 수 있다. 이러한 문제점을 해결하고자 본 논문에서는 신뢰할 수 있는 제 3자를 두어 제안하였고, TT와 FA간의 상호 운영을 위한 요구사항을 정의하고, 이를 바탕으로 프로토콜을 제안하였다. 권한 관리 모델을 이용함으로써 기존의 문제점을 해결할 수 있다.

FA가 이동시에 사용자의 인증 정보 및 인가 정보를 홈 망까지 이동하면서 불법적인 문제나 행동에 대해 문제점을 해결하고자 하였다. 본 제안방식은 사용자의 빈번한 이동이나 세션키의 빈번한 갱신에 따른 홈망의 과부하 발생과 불필요한 통신과정을 해결하고자 하였다.

이와 같이 본 논문에서 제안된 신뢰된 제 3자를 기반으로 한 AAA 프로토콜은 차세대의 다양한 네트워크와 서비스에서 효율적인 모델이 될 수 있다. 앞으로도 이와 관련된 이종망간의 연구가 진행된다면 향후 유비쿼터스 사회에서 많은 발전을 가져올 것이라 사료된다.

[참고문헌]

[1] Jalal Al-Muhtadi, Anand Ranganathan, Roy Campbell, and M. Dennis Mickunas,"A Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments," ICDCSW '02, pp.771-776, 2002

[2] M. Roman, and R. Campbell, "GAIA: Enabling Active Spaces," 9th ACM SIGOPS European Workshop, September 17th-20th, 2000, Kolding, Denmark

[3] 이근호(R&BD), "유비쿼터스 컴퓨팅 환경에서의 정보보호", Symposium on Information Security 2003, pp.629-651. 2003

[4] ITU-T, Draft ITU-T RECOMMANDATION X.509 version4, ITU-T Publications, 2001. 5.

[5] A. Aresenault, S. Tuner, Internet X.509 Public Key Infrastructure, Internet Draft, 2000. 11

[6] S. Farrell, R. Housley, An Internet Attribute Certificate Profile for Authorization, Internet Draft, 2001.

[7] 이성용, 정현수, "Ubiquitous 연구 동향 및 향후 전망", Worldwide IT 제 3권 7호, pp.1-12, 2002

[8] 이윤철,"최근 홈 네트워크 기술동향 및 시장 전망", ITFIND 주간기술동향(TIS-03-20) 1098호, pp22-33. 2003

[9] 김현곤,"AAA기반 Mobile IP 환경에서 안전하고 빠른 핸드오프 기법 설계", 한국정보보호학회논문지, 2004.2