AAA 서비스 망에서 MN 인증을 위한 MN-AAA 키 재발급 메커니즘

이해동[0], 최두호, 김현곤
한국전자통신연구원, AAA정보보호연구팀
(haenamu[0], dhchoi, hyungon)@etri.re.kr

MN-AAA Key Refreshing Mechanism for MN Authentication at AAA Infrastructure

HaeDong Lee[0], DooHo Choi, HyungGon Kim
AAA Security Information Research Team, Electronics and Telecommunications Research Institute

요 약

현재, IETF AAA 워킹 그룹에서는 기존 AAA 프로토콜인 RADIUS를 보완 및 확장하여 새로운 프로토콜인 Diameter의 표준화를 진행중이다. Diameter는 기존 전화망에서의 PPP 접속 서비스 뿐만아니라 이동 패킷 서비스를 지원하는 Mobile IP 접속 서비스를 지원하도록 설계되고 있다. AAA 서버는 인증(Authentication), 인가 (Authorization) 및 과금(Accounting) 서비스를 사용자에게 제공한다. 이때 홈 Diameter 서버는 MN이 제공하는 credential을 검증함으로써, MN에 대한 인증을 수행한다. MN은 credential을 생성하기 위해서, 홈 Diameter 서버와 MN간에 공유하는 MN-AAA 비밀키와 MAC 알고리즘을 사용한다. 상기 키는 이동 가입자가 AAA 서비스를 초기에 요청할 때 발급되는 비밀키이며, Diameter 프로토콜은 상기 비밀키의 재발급 메커니즘을 제공하지 않는다. 메커니즘 부재는 키의 누출로 인한 서비스 도용이 발생할 수 있는 취약점이 있다. 본 논문에서는 키의 누출에 대비한 MN-AAA 키의 재생성 및 재분배 메커니즘을 제안한다. 이를 위해서, Mobile IP 프로토콜 및 Diameter 프로토콜을 확장 및 보완한다.

1. 서 론

패킷 데이터 서비스의 진화는 복수의 네트워크 사업자에 의해서 관리되고, 유무선이 통합되는 환경을 지향하고 있다. 이러한 이질적인 복수의 데이터 네트워크상에서는 투명한 사용자 로밍 서비스 제공이 필수적이다.

Mobile IP는 사용자가 이동중에도 서비스 단절없이 동일한 IP 주소를 유지하면서 인터넷에 대한 접속점을 변경할 수 있게 한다. 그러나 Mobile IP는 타 네트워크 사업자에 의해 관리되는 네트워크상에서 사용자에게 이동성을 제공하지 못하며, 상업망에서 필수적인 과금에 대한 방법을 지원하지 않는다. 또한 Mobile IP는 고정된 홈 주소와 HA를 유지하기를 권고하였다. 상기 제약 조건은 특정 네트워크에서 Mobile IP의 동작이 불가능하게 할 수 있다. 그래서 현재의 설계 방향은 고정된 홈 주소와 HA를 유지하지 않고도 Mobile IP가 동작할 수 있도록 진행중이다.

Mobile IP가 이질적인 관리 도메인상에서 이동성을 제공할 수 있도록 확장하기 위해서는, Mobile IP 프로토콜이 AAA(Authentication, Authorization, Accounting) 인프라와 정합되는 방향으로 진행중이다.

기존의 AAA 프로코콜인 RADIUS[1]는 전화망 상에서 PPP 접속을 위한 AAA 서비스를 제공하기 위해서 사용되어 왔다. 그러나 프로토콜의 제약 조건으로, RAIDUS 기반 AAA 서버는 라우터 및 NAS(Network Access Server)의 증가된 기능을 수용하기 에 어렵게 되었다. RADIUS의 단점을 극복하고, 기존의 PPP뿐만 아니라 Mobile IP, SIP 등을 포함하는 다양한 접속 기술을 수용하기 위해서, Diameter 프로토콜이 등장하게 되었다.

Diameter 프로토콜의 기본 구조는 새로운 접속 기술에 AAA 서비스를 제공하기 위한 확장 가능한 기본(base) 프로토콜[2]과 각각의 접속 기술을 지원하는 Diameter 응용으로 구성된다. 기본 프로토콜은 모든 응용에 동일한 기능을 제공하게 된다. 현재 Diameter 응용으로는 NASREQ 응용[3], Mobile IPv4 응용[4], CMS 응용[5]이 있다. 추가적인 Diameter 응용이 향후 정의될 수 있다. 아래 그림은 현재 표준화중인 Diameter 프로토콜의 문서 구조를 보여주고 있다.

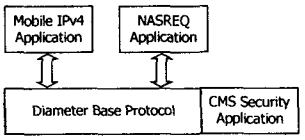

그림 1 : Diameter 프로토콜 표준 구조

인증 및 인가 기능을 수행하는 표준은 개별 접속 기술마다 Diameter 응용이 정의된다. Diameter Mobile IPv4 응용은 Mobile IP 망에서 홈 Diameter 서버가 MN에 대한 인증 및 인가 기능, MN에 대한 HA 및 홈 주소의 할당, KDC의 역할 등을 정의하고 있다.

홈 Diameter 서버는 MN이 제공하는 인증 값을 검증함으로써, MN에 대한 인증을 수행한다. MN이 인증 값을 생성하기 위해서 MN-AAA 비밀키와 MAC 알고리즘을 사용한다. MN-AAA 비밀키는 홈 Diameter 서버와 MN간에 공유하는 키이다. 이러한 키는 이동 가입자가 AAA 서비스를 초기에 요청할 때 발급되는 비밀키이며, Diameter 프로토콜은 명시된 시간이 초과했을 때 상기 비밀키를 재생성하고 분배하는 메커니즘을 제공하지 않는다. 메커니즘 부재는 키 누출로 인한 서비스 도용이 발생할 수 있는 취약점이 있다.

본 논문에서는 키 누출에 대비한 MN-AAA 키의 재생성 및 재분배 메커니즘을 제안한다. 이를 위해서, Mobile IP 프로토콜 및 Diameter 프로토콜을 확장 및 보완이 필요하다. 본 논문의 구성은 다음과 같다. 제 2장에서는 Mobile IP와 Diameter 정합 시나리오를 소개하며, 제 3장에서는 Diameter 프로토콜의 인증 메커니즘을 설명하며, 제 4장에서는 MN-AAA 비밀키에 대한 키 재발급 방법을 제안하며, 마지막으로 제 5장에서는 결론을 맺는다.

2. Mobile IP와 Diameter 정합 시나리오

본 절에서는 Mobile IP와 Diameter 기반 AAA 인프라가 정합될 때 네트워크 구성 및 정합 시나리오를 설명한다.

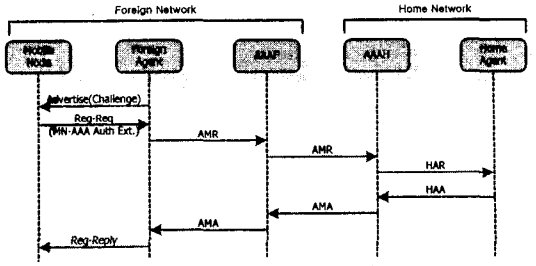

그림 2 : Mobile IP AAA 정합 시나리오

- FA: Mobile IP와 Diameter 모두 이해할 수 있는 Diameter 클라이언트
- AAAF: Diameter 서버로서, 방문 망에 있는 로컬 인증 서버
- AAAH: Diameter 서버로서, 홈 망에 있는 홈 인증 서버
- HA: Mobile IP와 Diameter 모두 이해할 수 있는 Diameter 클라이언트

MN 동작 : 방문 네트워크 상에서 AAA 인프라를 통한 인증 및 세션 키 발급을 요구할 때, MN은 MN-AAA 인증 확장을 등록 요청(registration request) 메시지에 추가하여 FA에게 상기 등록 요청 메시지를 보낸다.

FA 동작 : 이동 노드가 방문 에이전트에게 등록 요청 메시지를 보내어 서비스를 요청하면, 방문 에이전트는 Diameter에서 정의한 AMR(AA-Mobile-Node-Request) 메시지를 생성한다. AMR 메시지는 등록 요청 메시지에서 홈 주소, 홈 에이전트, 이동 노드의 NAI(network access identifier) 그리고 다른 중요한 정보들을 추출하여 생성된다. 방문 에이전트는 생성한 AMR 메시지를 AAAF(AAA-Foreign)로 알려진 로컬 Diameter 서버에 전달한다.

AAAF 동작 : AAAF가 AMR 메시지를 수신하면, AAAF는 수신한 AMR 메시지를 로컬에서 처리할지 AAAH (AAA-Home)로 알려 진 다른 Diameter 서버에 전달하지를 판단하기 위해서 Diameter 기본 프로토콜[2]에 명시된 절차를 수행한다.

AAAH 동작 : 만약 이동 노드가 성공적으로 인증되었으면, AAAH는 등록 요청 메시지를 포함하는 HAR (Home-Agent-MIP-Request) 메시지를 HA에게 보낸다.

HA 동작 : 홈 에이전트가 HAR 메시지를 수신했을 때, 홈 에이전트는 먼저 Diameter 메시지를 처리한다. 그리고 홈 에이전트는 *MIP-Reg-Request AVP*의 등록 요청 메시지를 판독하고 이에 대한 등록 응답 메시지를 생성한다. 홈 에이전트는 생성한 등록 응답(registration reply) 메시지를 MIP-Reg-Reply AVP에 인코딩한다.

3. Diameter 프로토콜의 인증 메커니즘

본 절에서는 홈 Diameter 서버가 MN을 인증하기 위한 메커니즘을 설명한다. MN은 RFC3012에 정의되어 있는 범용 Mobile IP 인증 확장(Generalized Mobile IP Authentication Extension)을 사용하여 인증 데이터(authenticator)를 제시하며, Diameter 클라이언트인 FA는 상기 인증 확장을 파싱하여(parsing), 홈 Diameter 서버가 이해할 수 있는 형식인 AVP[2]로 인코딩한다. 홈 Diameter 서버는 MN이 수행한 과정과 동일하게 인증 데이터를 생성하고, 제시된 MAC 값과 자신이 계산한 MAC 값의 비교를 통하여 인증에 대한 실패 성공을 결정 짓는다.

Type(36)	Subtype	Length
SPI		
authenticator . . .		

* Subtype(1) : MN-AAA Authentication

그림 3 : 범용 Mobile IP 인증 확장 형식

범용 Mobile IP 인증 확장은 MN이 Mobile IP에서 정의한 HA/FA이외의 노드에게 인증을 요청할 때 사용된다. Subtype이 1인 경우, 범용 Mobile IP 인증 확장은 MN-AAA 인증 확장으로 사용됨을 지시한다. MN이 상기 인증 확장을 사용하여 홈 Diameter 서버에게 인증 데이터를 제시하면, 홈 인증 서버는 MN과 공유하는 동일한 MN-AAA 비밀키와 알고리즘으로 인증 데이터를 검증한다.

인증 데이터 생성은 아래와 같다. 기본 알고리즘은 HMAC-MD5이다. 다른 알고리즘이 사용될 수 있다.

data =
Preceding Mobile IP data // Type, Subtype, Length, SPI

hmac_md5 (data, data_length, MN-AAA- Key, Key_Length, Mac)

본 절에서 언급한 MN-AAA 비밀키는 Diameter 프로토콜 상에서 분배되는 것이 아니며, MN과 Diameter 서버는 제 3의 방법에 의해 키를 발급받는다. 만약 Diameter 프로토콜 상에서 키의 재생성 및 재분배가 안전하게 이루어 질 수 있다면, 사용자는 키의 재발급 편의성, 키의 안정성 보장 등의 장점을 가진다. 다음 절에서 본 논문에서 제안 하는 키 재발급 메커니즘을 설명한다.

4. MN-AAA 비밀키 재발급 메커니즘 제안

현재, Diameter 프로토콜 에서는 MN-AAA 비밀키의 재발급 메커니즘이 정의되어 있지 않으며, 제 3의 방법으로 상기 기능 지원의 필요성을 권고하고 있다. 그러나 Diameter 프로토콜에서 지원하지 않으면, AAA 서비스 가입자는 사업자에게 직접 방문하여, 새로운 키를 발급받는 번거로움이 있다. 본 논문에서는, Diameter 프로토콜과 Mobile IP 프로토콜을 확장하여, 비밀키 재발급 메커니즘을 제안한다.이러한 제안은 새로운 Mobile IP 확장, 홈 Diameter 서버의 기능 확장 등이 따른다. 또한 재발급되는 비밀키의 안정성이 보장되어야 한다.

본 제안의 핵심은 [6]에 명시된 세션키의 분배 및 추출 방법을 MN-AAA 비밀키에 적용하고, Mobile IP 및 Diameter 노드가 상기 방법을 수용하기 위해서, 각각의 프로토콜 데이터 인코딩 방식인 Mobile IP 확장(extension)과 Diameter AVP를 추가하는 것이다.

발급되는 MN-AAA 비밀키의 보안을 위해서, Diameter 서버는 최소 길이 64 비트의 랜덤값(random value)을 생성하여 표 1에서 정의한 AVP로 인코딩하여 HA에게 보낸다. HA는 MN-AAA 비밀키 정보를 표 2에서 제시한 Mobile IP 확장을 사용하여 등록 응답 메시지에 추가한다. MN은 상기 랜덤값을 이용하여 비밀키를 추출한다[6]. 다음은 HMAC-MD5를 이용한 비밀키 추출 방법이다. 다른 알고리즘이 사용될 수 있다.

hmac_md5 (Old MN-AAA-Key, key material, node-address, Mac)
New MN-AAA-Key = Mac

- Old MN-AAA-Key는 재발급 이전에 MN와 AAAH 사이에 공유되는 비밀키.
- key material는 최소 길이 64 비트의 랜덤값.
- node-address는 이동 노드의 identity. MN의 홈 주소와 같다. MN의 홈 주소가 0.0.0.0 혹은 255.255.255.255이면, 대신 NAI를 사용된다.

AAAH는 위의 루틴을 사용하여 MN과 공유하는 MN-AAA 비밀키를 생성한다. 한편, 초기의 MN-AAA 비밀키는 Diameter 프로토콜상에서 발급되지 않고, AAA 서비스 가입시 제 3의 방법으로 발급받는다. 랜덤 값으로부터 MN-AAA 키 추출 방법은 세션키의 추출 방법과 동일하며, [6]에서 상기 방법이 안전함을 설명하였다.

표 1 : Diameter 프로토콜 확장

추가 항목	설명
MN-AAA-Key-Lifetime AVP	MN-AAA 비밀키의 유효기간
MN-AAA-Key AVP	MN-AAA 비밀키 생성을 위한 랜덤 값
MN-AAA-Key-Request Flag	MIP-Feature-Vector AVP의 데이터로 MN-AAA 비밀키의 요청 지시

표 2 :Mobile IP 프로토콜 확장

추가 항목	설명
MN-AAA Key Request Extension	MN-AAA 비밀키 요청을 위한 MIP 등록 메시지 확장
MN-AAA Key Reply Extension	MN-AAA 비밀키 응답을 위한 MIP 등록 메시지 확장

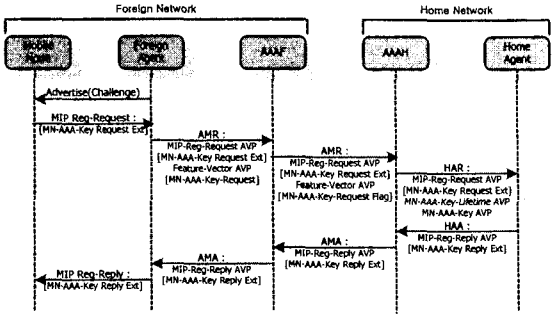

그림 4 : MN-AAA 비밀키 재발급 동작 메커니즘

- MN 동작 요구사항 : MN-AAA 키의 재분배를 요청하기 위해서 등록 요청 메시지에 MN-AAA 인증 확장을 붙인다.
- FA 동작 요구사항 : MIP-Feature-Vector AVP의 MN-AAA-Key-Request 플래그 비트를 설정한다.
- AAAH 동작 요구사항 : MIP-Feature-Vector AVP를 판독하여 MN-AAA 키를 생성하고, HAR 메시지에 MN-AAA-Key-Lifetime AVP와 MN-AAA-Key AVP를 붙인다.
- HA 동작 요구사항 : MN-AAA-Key-Lifetime AVP와 MN-AAA-Key AVP을 이용하여 등록 응답 메시지에 MN-AAA Key 응답 확장을 붙인다. 등록 응답 메시지는 HAA 메시지에 인코딩한다.

5. 결 론

본 논문에서는, MN-AAA 비밀키의 누출 방지를 위해서, Diameter 프로토콜과 Mobile IP 프로토콜을 확장하여 비밀키 재발급 메커니즘을 제안하였다. 본 메커니즘의 핵심은 새로운 Mobile IP 확장, 홈 Diameter 서버의 기능 확장, 프로토콜상에서 발급되는 비밀키의 안전성 보장 방안 등이 핵심이다. Diameter 프로토콜 상에서 키 재발급이 이루어지므로, 사용자는 오프라인(off-line)으로, 즉 사업자의 비밀키 발급장소를 직접 방문하지 않고, 온라인(on-line)상에서 편리하게 키 발급을 제공받을 수 있다.

참고 문헌

[1] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[2] P. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. Rubens, "Diameter Base Protocol", draft-ietf-aaa-diameter-11.txt, *IETF work in progress*, June 2002.

[3] P. Calhoun, W. Bulley, A. Rubens, J. Haag, "Diameter NASREQ Application", IETF work in progress.

[4] P. Calhoun, C. Perkins, "Diameter Mobile IPv4 Application", IETF work in progress.

[5] P. Calhoun, W. Bulley, S. Farrell, "Diameter CMS Security Application", draft-ietf-aaa-diameter-cms-sec-05.txt, IETF work in progress, April 2002.

[6] C. Perkins, P. Calhoun, "AAA Registration Keys for Mobile IP", draft-ietf-mobileip-aaa-key-09.txt, IETF work in progress, July 2001.