무선 인터넷의 로밍 서비스 보안 기술

한국전자통신연구원 김현곤 · 손승원
충남대학교 김대영*

1. 서 론

최근 무선 근거리 통신망(WLAN)의 부상과 함께 공항 및 컨벤션 센터와 같은 핫 스팟 지역 위주로 무선 인터넷 서비스가 제공되기 시작하였다. 즉, 유선망을 이용한 공중망 무선 인터넷 서비스가 본격화 된 것이다. 한편, 사회 경제적으로 막대한 영향을 끼칠 유무선 인터넷 서비스 및 망 통합도 점진적으로 진행되고 있으며, 이와 더불어 유무선 인프라에 걸친 로밍 서비스에 대해서도 관심이 증대되고 있다. 이와 관련하여 본 고에서는 최근 이슈화가 되고 있는 무선 인터넷 로밍 서비스 제공을 위한 로밍 서비스 보안 기술을 기술적인 측면에서 다루었다.

이동통신 망을 통한 무선 인터넷 사용의 최대 강점은 사용자에게 로밍이나 핸드오프 기술을 통해 언제 어디서나 누구와도 통신을 가능하게 한다는 점이다. 이에 비해 인터넷 망을 통해 무선 인터넷(802.11 또는 Bluetooth 등)을 사용하는 경우에는 제한적인 로밍 서비스만을 제공한다. 미래의 무선 인터넷은 이동통신 망을 이용하든지 또는, 인터넷 망을 이용하든지 하부 인프라와 무관하게 사용자의 입장에서는 하나의 단일 망을 이용하는 것처럼 느껴지도록 발전되어야 한다. 즉, 다수의 사업자가 운영하는 무선랜 공중망간 로밍 서비스 그리고 무선랜 공중망과 이동통신 망의 조합인 이종 망간 로밍 서비스, 더 나아가 이러한 로밍 서비스들의 국제적인 확장이 이루어져야 한다. 이를 위해서는 다양한 액세스 망들에 대해 단일화된 라우팅 프로토콜이 적용되어야 한다. 하나의 후보로서 네트워크 계층에서 IP 이동성을 제공하는 IETF의 Mobile IP(MIP) 프로토콜을 들 수 있다. MIP 프로토콜은 현재 IETF SeaMoby WG에서 빠른 핸드오프 지원, 컨텍스트 전송 등 많은 문제점들을 해결하고 있는 중이다.

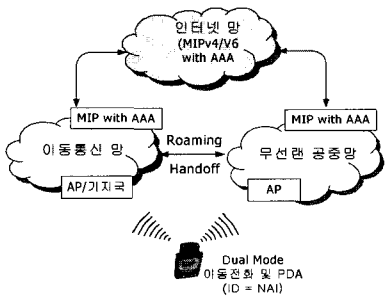


그림 1 이종 망간 무선인터넷 로밍 서비스 제공 예

그림 1에 무선랜 공중망과 이동통신 망간 무선 인터넷 로밍 서비스 제공 예를 보였다. 사용자는 로밍 시 듀얼모드 이동전화 또는, PDA를 가지고 무선랜 공중망 또는, 이동통신 망을 자동으로 선택.접속하여 로밍 서비스를 제공 받는다. 망간에는 MIP를 적용하고, 로밍을 위한 보안 기술은 AAA(Authentication, Authorization, and Accounting) 기술을 적용한다. 사용자 또는, 이동 단말을 구분하는 ID는 user@relam의 형태로 표현되는 NAI(Network Access Identifier)를 적용한다. 이종 망들은 NAI를 분석하여 사용자의 홈 망을 식별하고, 사용자 식별, 인증, 권한 검증, 과금 기능을 수행한다. 무선랜 공중망간 로밍 서비스를 지원하는 관련 업체로서, GRIC communication, HereYouAre communication, I-Pass 등이 있다. 이종 망간 로밍 서비스를 지원하기 위한 관련 업체의 연구 동향으로서, 일본 J-Phone의 3G W-CDMA 망과 무선랜 망간 연동 기술 개발, 핀란드

* 종신회원

WNS사의 400개 기지국을 이용한 GPRS와 WLAN 통합 서비스 준비, 미국 AT&T Wireless 및 Cingulare Wireless사에서 적용성 검토, 퀄컴의 듀얼 모드 칩셋(cdma2000 1xEV-DO/WLAN) 개발 예정 등을 들 수 있다. 국내에서도 최근 한국통신사업자연합회내 무선랜 사업자 협의체가 구성되어 무선랜 공중망 서비스 사업자간 주파수 혼신 방지와 공용 서버 구축에 대한 논의가 시작되고 있다.

그러나 MIP 서비스는 공개된 다수의 망간에 걸쳐 이루어지므로, 많은 보안 취약점을 가질 수 있다. 특히, 무선 인터넷 사용자의 로밍으로 인해 사업자간 망간 연동이 빈번하게 이루어지기 때문에 망간에 걸친 가입자 인증, 권한 검증, 과금, 사업자 망간에 걸쳐 있는 망 노드들간 인증을 제공하는 안전한 로밍 서비스 기술 즉, AAA 기술이 기본적으로 요구된다. 이러한 로밍 서비스는 통신 서비스 사업자 망간에 걸쳐있으므로 제도적인 측면, 정책적인 측면, 기술적인 측면에서 다양한 요구 사항들이 반영되어야 하며, 표준화도 중요 고려 사항이 되어야 한다. 본 고에서는 로밍 서비스를 위해 MIP 프로토콜을 적용하고, 이를 위한 보안 기술로서 AAA 기술을 적용한다고 가정하고[1] 관련 기술들을 소개하고자 한다. 2장에서는 Portability와 Mobility 보안에 대한 개념 소개, 3장에서는 Mobility 기반의 로밍 서비스 보안 기술, 4장에서는 망간 접속에 따른 Scalability 고려 사항을 기술하고, 5장에서 결론을 맺는다.

2. Portability 및 Mobility 보안 기술

인터넷 사용자가 자신이 가입한 서비스 망(홈 망)에서 이동하여 새로운 망(방문 망)에 접속하였을 때, 망에서 제공할 수 있는 IP 서비스는 두 가지로 구분할 수 있다. 하나는 방문 망에서 DHCP를 통해 새로운 동적 IP를 할당 받는 서비스이고, 다른 하나는 가입자가 홈 망에서 할당 받은 고유한 IP를 그대로 사용 가능하게 하면서 동적 IP를 할당 받는 IP 이동성 보장 서비스 즉, MIP 서비스이다. 전자는 한정된 이동성만을 제공하는 Portability 서비스이며, 후자는 Portability를 포함해서 이동성까지 제공하는 Mobility 서비스라 할 수 있다. 이 장에서는 각 서비스에 대한 보안 기술에 대해서 기술한다.

2.1 Portability 보안 기술

초기 인터넷 사용자는 다이얼 업 모뎀 포트(또는 ISDN)를 통해 ISP 망 또는 통신 사업자 망에 접속하여 PPP기반 인터넷 서비스를 제공 받았다. 그러나 점진적으로 다이얼 업 연결 수가 많아짐에 따라 사업자들은 대규모의 복잡하고 다수의 포트를 제공하는 망 접근 장치(NAS; Network Access Server)를 설치하기에 이르렀다. 이와 더불어 노트북 컴퓨터의 등장으로 인해 Portability 서비스 즉, 사용자가 이동하여 유선 포트를 할당 받아 방문 망에 접속하는 서비스가 등장하게 되었다. 이로써 호텔, 공항 그리고 가상 사무실에서 e-mail이나 웹 사용이 자유스러워졌으나, 안전성과 신뢰성 보장이라는 추가적인 요구 사항이 발생하게 되었다. 즉, 불법적인 망 자원 사용을 방지해야 하고, 가입자의 권한 레벨을 부여하고 검증해야 하며, 과금 및 자원 계획을 수립하기 위해 망 자원 사용에 대한 측정이 필요하게 되었다. 또한 망 사업자들이 보유한 다양한 관리 시스템들간 상호 연동이 필요하게 되었다.

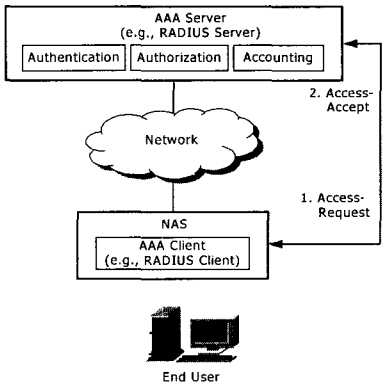


그림 2 AAA 프레임워크(Architecture)

그림 2는 유선상에서 사용되는 RADIUS 기반 AAA 프레임워크를 나타내었다[2]. 프레임워크는 분산된 다양한 망 기술과 플랫폼들에 대한 개별 규칙들을 조화시키며, 체계적인 인증, 권한 검증, 과금 서비스를 가능하게 해준다. 인증은 망 접근을 허용하기 전에 사용자의 신원을 검증하는 것이다. AAA 서버는 사용자가 제공한 인증 데이터와 자신의 보유한 사용자 데이터를 비교하여, 인증서가 일치하면 망에 대한 접근을 허락하고, 일치하지 않으면 망 접근을 제한한다. 권한 검증은 인증에 성공한 사용자에게 어떤 권한과 서비스를 허용할 것인지를 결정하는 것이다.

여기에는 IP 주소, 제공될 응용 및 프로토콜을 결정하기 위한 필터 등이 포함된다. 인증과 권한 검증은 AAA 동작 환경에서 일반적으로 함께 수행된다. 과금은 사용자의 자원 사용에 관한 정보를 모으는 방법을 제공한다. 이 정보는 사용 요금, 회계 그리고 용량 증설 등의 자료로 사용된다.

그림 2에서는 설명의 편의를 위해 단일 AAA 서버의 예를 보였다. 망측의 첫번째 관문인 NAS는 라우터, 터미널 서버, 호스트 등이 될 수 있으며, AAA 클라이언트 기능을 갖는 장치이다. AAA 동작 절차를 순서대로 간략히 기술하면 다음과 같다.

(1) 사용자(End User)는 NAS에 연결하여 망에 대한 접근을 요청한다.
(2) NAS의 AAA 클라이언트는 사용자의 인증 정보를 받아서 AAA 서버로 전달한다.
(3) AAA 서버는 사용자를 인증하고, AAA 클라이언트에게 사용자의 인증 성공 또는 실패 사유와 관련 데이터를 전달한다.
(4) NAS의 AAA 클라이언트는 사용자에게 요청한 자원에 대한 접근이 허용되었는지 또는, 거절되었는지를 통지한다.
(5) 만약 허용되었다면, 사용자는 망에서 제공하는 서비스를 받는다.

2.2 Mobility 보안 기술의 출현 배경

AAA 기술의 표준은 IETF AAA WG에서 주도하고 있으며, NASreq, ROAMOPS, Mobile IP, SeaMoby, Manet WG으로부터 그리고 IMT-2000 표준화 단체인 3GPP 및 3GPP2로부터 요구사항을 수집하여 반영한다. 그림 3에 제안된 주요 AAA 프로토콜의 특징을 비교하였다. AAA WG에서는 이들 3개의 프로토콜과 COPS(Common Open Policy Service) 프로토콜 포함해 4개의 후보를 선정.검토하였으며, 최종적으로 Diameter를 AAA 프로토콜로 선정하고 표준화를 진행 중이다.

TACCS+(Terminal Access Controller Access Control Systems+)는 1993년 RFC1492로 완성된 프로토콜이며, 시스코에 의해 지속적으로 개선되어 왔다. 오픈 소스는 ftp://ftp-eng.cisco.com/pub/tacacs/에 공개되어 있다. 클라이언트-서버 구조이며, RADIUS(Remote Access Dial-In User Service)와 유사한 기능들을 제공한다.

	TACACS+	RADIUS	Diameter
Authentication & Authorization	Separated	Combined	Separated
Packet Encryption	Encryped the entire packet payload	Encryped only the user passwd	Encryped the entire packet payload
Transport	TCP	UDP	TLS/SCTP
End-to-End Security with PKI	Not support	Not support	Support
Global Secure Roaming	Limited	Limited	Support

그림 3 제안된 주요 AAA 프로토콜의 특징

가장 널리 알려지고 많이 사용되는 AAA 프로토콜은RADIUS이다. RADIUS 클라이언트 역할을 수행하는 NAS와 중앙의 RADIUS 서버간 통신을 통해 다이얼 업 모뎀 사용자들을 인증하고, 인증이 성공하면 망 자원에 대한 액세스 권한을 부여하는 기능을 제공한다. 이 프로토콜은 회사가 중앙의 데이터 베이스 내에 사용자 프로파일을 유지하고, 모든 원격지 서버가 공유할 수 있게 해 준다. 그리고 보안 기능을 제공하며, 사용자의 망 자원의 사용량이나 네트워크 통계, 이러한 자료를 통한 망 관리 정책 수립 등을 가능하게 해 준다. 1990년 중반에 Livingston에 의해 만들어진 RADIUS는 Ascend와 같은 다른 네트워크 장비들에 의해 사용되는 사실상의 산업계 표준이며, 이후 IETF에 의해 표준화 되었다.

RADIUS의 특징은 다음과 같다. 첫째, 클라이언트-서버 기반의 동작을 한다. RADIUS 클라이언트 기능은 NAS의 일부 기능으로 존재하며, RADIUS 서버 기능은 망의 중앙에 위치한 별도의 서버로 존재한다. 다수의 NAS가 한 개의 서버와 접속되며, 이들간에는 서버와 클라이언트 모델에 따라 동작을 한다. 한편, RADIUS 서버는 다른 RADIUS 서버나 인증 서버에 대해 프락시 클라이언트로 동작할 수 있다. 둘째, 네트워크 보안 기능을 제공한다. RADIUS 클라이언트와 서버 사이의 모든 통신은 네트워크를 통해 전달되지 않은 공유 비밀키에 의해 인증된다. RADIUS 메시지 안에 포함되어 있는 사용자 비밀번호는 해커의 공격으로부터 보호하기 위해 암호화된다. 셋째, 유연한 인증 메커니즘을 제공한다. RADIUS는 PAP, CHAP 등 다양한 인증 기법들을 수용한다. 넷째, 다른 인터넷 프로토콜과 같이 AVP (Attribute/Value Pair)라 불리는 Type-Length-Value 필드를 따른다.

그러나 RADIUS 프로토콜은 (1)유선에서 출발함으로 인해 무선의 로밍과 로밍 보안 개념이 반영되지 않음, (2)Attribute Value가 255 바이트를 넘지 못함, (3)동시에 처리할 수 있는 메시지 갯수가 255로 제한, (4)서버 제어 불가능, (5)재전송 절차의 부재, (6)End-to-End(이하 E2E) 메시지의 확인 불가, (7)서버 실패 검출의 한계, (8)묵시적인 패킷 폐기, (9)불충분한 서버 Fail-Over, (10)프락시 환경에서 RADIUS 서버의 비효율성, (11)단방향성(unsolicited) 메시지 부재 등의 프로토콜 한계를 가지고 있다. 이러한 한계점들을 극복하고, 무선의 로밍과 로밍 보안 개념을 반영한 새로운 Diameter 프로토콜을 제정하기에 이르렀다.

2.3 Mobility 보안 기술

로밍 서비스 제공을 위한 Mobility 보안 기술은 Diameter 프로토콜 적용을 통해 완성된다. Diameter 프로토콜은 (1)기존RADIUS 프로토콜의 한계점 극복, (2)기존보다 강화된 보안 제공(E2E Security with PKI), (3)각 응용 서비스에 적합한 AAA 기술 제공(MIPv4, MIPv6, and SIP), (4)미래 보안 서비스를 수용할 수 있는 유용한 확장성, (5)다수의 망들을 유연하게 접속할 수 있는 peer-to-peer 구조, (6)로밍에 필요한 도메인간 이동성 보안 기능 제공, (7)로밍 컨소시엄 구성 기능, (8)보안 및 신뢰성을 기반으로 하는 하부 프로토콜의 수용을 특징으로 한다.

그림 4에 Diameter 서버의 프로토콜의 구조를 나타내었다. Diameter 프로토콜은 크게 과금 기능을 포함한 기본 프로토콜(Base Protocol)[3]과 응용(application)으로 분류된다. 현재까지 정의된 응용은 라우터에서 액세스를 위해 사용될 확장된 RADIUS응용(NASREQ 응용)[4], MIPv4 응용[5], E2E Security 및 PKI(Public Key Infra-Structure) 기능을 제공하는 CMS(Cryptographic Message Syntax) 보안 응용[6][7]이 있다. 현재 태동되고 있는 응용으로는 MIPv6에서 AAA 서비스 제공을 위한 MIPv6 응용[8]과, SIP(Session Initiation Protocol)에서 AAA 서비스 제공을 위한 멀티미디어 응용[9]이 있다. 또한, 미래 서비스에 대한 AAA 기능은 기본 프로토콜 상위에 새로운 Diameter 보안 응용으로 추가될 수 있다. 그 동안 많은 변화를 가져온 Diameter 프로토콜의 표준은 아직까지 드래프트 상태에 있지만, 2002년 중 Proposed Standard RFC로 채택될 것이다.

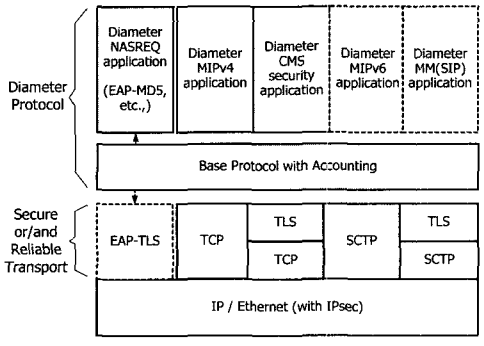


그림 4 Diameter 서버의 프로토콜 구조

3. Mobility 기반의 로밍 서비스 보안 기술

Diameter 프로토콜 기반 AAA는 공개된 네트워크 환경에서 로밍하는 가입자의 정보, Diameter 메시지, 관련 데이터에 대해서 기밀성(confidentiality), 무결성(integrity), 인증(authentication), 부인 봉쇄(non-repudiation) 등의 보안 기능을 제공한다. 이 장에서는 Diameter 프로토콜에서 정의된 각 응용들을 위주로 로밍 서비스 보안 기술을 설명한다. 각 응용들은 독립적으로 운용되나, 경우에 따라 결합되어 운용될 수 있다. 결합되어 운용되는 예를 들면, 중요한 MIP 보안 연관 키나, 서비스 사업자들간에 상호 신뢰가 중요시 되는 가입자의 과금 데이터들은 CMS 응용을 적용하여 보안성을 유지한다. 즉, 강화된 보안 기능을 제공하기 위해 MIPv4 응용과 CMS 응용은 결합되어 운용된다. 이를 위해 Diameter 서버들은 자신이 처리할 수 있는 응용들의 정보를 초기에 상호 교환한다.

3.1 하부 프로토콜 및 기본 프로토콜 기술

Diameter 하부 프로토콜은 전송 계층 보안 프로토콜인 TLS(Transport Layer Security) 또는 IPsec을 적용하며, TLS 하부에는 TCP 및 UDP가 제공하지 못하고 있는 전송계층에서의 신뢰성을 제공하기 위해 SCTP(Stream Control Transmission Protocol)를 적용한다. Diameter 서버는 반드시 TLS와 IPsec을 지원해야 하는 반면, Diameter 클라이언트는 IPsec을 반드시 지원해야 하나 TLS는 권고(should support) 사항이다. MIPv4에서 Diameter 서버는 방문 망 또는 홈 망의 AAA 서버들이 되며, Diameter

클라이언트는 MIPv4의 FA(Foreign Agent) 또는 HA(Home Agent)가 된다. Diameter 하부 프로토콜의 요구 사항은 AAA Transport Profile[10]에 별도로 정의하고 있다.

기본 프로토콜 기능은 AVP 전달 기능, 자신이 처리 가능한 응용들의 정보인 능력 정보를 교환하는 기능, 오류 신호 처리 기능, 피어 연결 관리 기능, 라우팅 서비스 기능, 사용자 세션 관리 기능, 그리고 E2E security 및 PKI 기능을 적용하는 노드를 위해 보안 연관 설정 기능 등 전반적으로 Diameter 노드들의 운용에 필요한 기본 기능들을 제공한다.

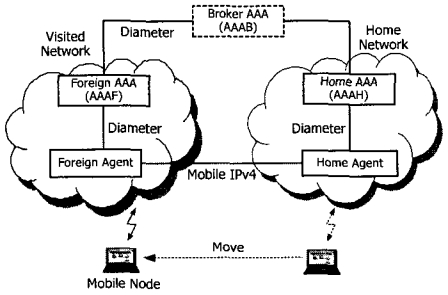


그림 5 MIPv4를 위한 Diameter 기반의 AAA 프레임워크

3.2 MIPv4 응용 기술

MIP 서비스는 데이터 링크 계층 기술과 독립적으로 네트워크 계층에서 IP 이동성을 제공한다. 즉, 홈 망에서 할당 받은 고유한 IP 주소를 방문 망으로 이동해서도 그대로 사용할 수 있다. 그림 5에 MIPv4를 위한 Diameter 기반의 AAA 프레임워크를 나타내었다. AAAF는 방문 망에 위치한 Diameter 서버이다. AAAH는 홈 망에 위치한Diameter 서버로써, 자신의 가입자에 대한 인증, 권한 검증, 과금 기능을 수행하며, 세부적으로는 MN(Mobile Node) 인증을 위한 AAA 신호 처리 기능, MN에 대한 인증 수행, MIP 동적 세션 키 생성 및 분배 기능, HA 동적 할당 신호 처리 기능, MN의 홈 주소 동적 할당 기능 등을 수행한다. AAAB의 역할은 4장에 기술하였다.

MIP를 위한 AAA 기능은 두 가지의 효율적인 아이디어가 내포되어 있다. 첫번째 아이디어로서, 최초의 MIP 등록에는 AAA 프레임크가 적용되나, 이후 계속 발생하는 MIP 등록에는 AAA 인증 lifetime 내에서 AAA 프레임워크가 적용되지 않는다. 즉, MIP 엔티티들인 MN, FA, HA간에만 MIP 등록이 이루어진다. 이는 매 MIP 등록 때마다 지리적으로 떨어져 있는 망간 AAA 오퍼레이션에 따른 지연, 그리고 AAA 서버들에 의해 발생하는 지연을 최소화 시켜주는 장점이 있다. 이로 인해 초기의 MIP 등록은 추가적인 지연(time overhead)이 발생하나, 이후 계속 발생하는 MIP 등록은 기존 MIP 프레임워크만 적용되므로 별도의 지연이 발생하지 않는다. 두번째 아이디어로서, RADIUS에서는 액세스 인증이 완료된 이후에 MIP 등록이 별도로 발생한다. 즉, RADIUS에서는 2회의 왕복 오퍼레이션이 필요하다. 그러나 Diameter에서는 액세스 인증과 MIP 등록을 동시에 처리하므로 1회의 왕복 오퍼레이션만 필요하다. MIP 메시지들은 AAA 메시지 내에 embedded되며, Diameter 프로토콜에서는 이를 동시에 처리한다. 이로 인해 Diameter는 RADIUS보다 두배 가까운 지연 시간을 줄일 수 있다.

이 응용은 아래의 알고리즘을 사용한다.

- ■Prefix+Suffix MD5 [Mobile IP]
- ■HMAC-MD5 [HMAC]
- ■HMAC-SHA-1 [HMAC]

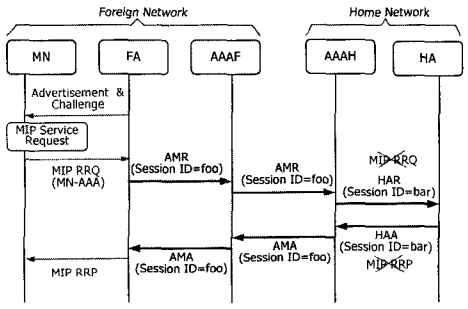


그림 6 MIPv4 등록에 따른 AAA 동작 절차

그림 6에 MIP 등록에 따른 AAA 동작 절차를 보였다.

(1) FA는 MN으로부터 받은 MIP RRQ (Registration Request) 메시지내 정보를 이용하여 AMR(AA-MN-Request) 메시지에 포함될 AVP들(MN의 홈 주소, HA 주소, MN의 NAI 등)을 생성하고, 생성된 AVP들을 포함하는 AMR 메시지를 AAAF에게 전송하여 MN에 대한 인증 및 권한 검증을 요청하다.

(2) AAAF는 수신된 AMR 메시지내 User-Name

AVP를 식별하여 AAAH에게 전달한다.

(3) AAAH는 수신된 AMR 메시지내 MIP-MN-AAA-Auth AVP를 이용하여 MN에 대한 인증 및 권한 검증을 수행한다. 이 AVP에는 초기 MN과 AAAH 사이에 사전 공유한 인증 키가 포함되어 있다. 그리고 동적 세션 키들을 생성한다. 세션 키들은 이후 발생하는 연속적인 MIP 등록시에 MN, FA, HA들간 보완 연관 설정에 사용된다. 생성된 세션 키들과 MIP-Reg-Request AVP를 포함하는 HAR(HA-MIP-Request) 메시지를 생성하여 HA에게 전달한다.

(4) HA는 수신된 HAR 메시지내 MIP-Reg-Request AVP를 분석하여 MIP 등록을 수행하고, MIP-Reg-Reply AVP를 포함하는 HAA(HA-MIP-Answer) 메시지를 생성하여 AAAH에게 전송한다.

(5) AAAH는 HAA를 수신하고, AMR 메시지에 대한 응답으로 AMA 메시지를 생성하여 AAAF에게 전송한다.

(6) AAAF는 수신된 AMA 메시지를 해당 FA에게 전송한다.

(7) FA는 수신된 AMA 메시지내 MIP RRP 메시지를 디캡슐레이션 시키고, MIP 등록 절차를 완료한다. 그리고 MIP RRP(Registration Reply)를 MN에게 전송한다.

(8) 정상적인 MIP 등록 절차가 완료되면, MN은 서비스를 개시하며 이와 동시에 과금 정보가 방문 망과 홈 망에 걸쳐 실시간으로 전달된다.

이 외에 본 고에서는 기술하지 않았지만 방문 망에서 HA 할당을 위한 AAA 동작 절차, Co-located MN을 위한 AAA 동작 절차, 세션 종료 절차, 실시간 과금 처리 절차 등이 정의되어 있으며, 빠른 핸드오프를 위한 AAA 동작 절차는 Seamoby WG에서 정의되는 빠른 핸드오프 절차에 따라 추후 정의될 예정이다.

3.3 CMS 응용 기술

초기의 Diameter 기반 AAA 기술은 hop-by-hop security가 적용되었으나 첫째, 중간 노드들에 의한 메시지 변조를 막을 수 있는 무결성을 제공하지 못함으로 인한 보안 취약점 둘째, 메시지 전송을 부인하는 부인 봉쇄를 제공하지 못함으로 인한 보안 취약점 셋째, E2E 노드들의 중간에 위치하는 다수의 Diameter 서버들에 의한 암.복호화 부담 등의 문제점들로 인해 삭제되었다. 이의 해결책으로Diameter 노드들간 상호 인증이 필요하게 되었다. Diameter 노드들간 상호 인증을 위해 E2E Security 및 PKI가 적용되며, 이 두 기술들은 lightweight data object 보안을 지향하고, 기존 정의된 보안 프로토콜 활용 측면에서 기존의 CMS 기술을 적용한다[7][11].

E2E Security는 엄밀하게 따지면 가입자 단말과 망의 인증 주체간에 적용하는 보안 기술이 아니라, 액세스 망의 첫번째 Diameter 서버와 가입자의 홈 망에 위치한 Diameter 서버간에 적용하는 보안이다. 물론 정책에 따라 중간 노드들 사이에도 이 기술들이 적용될 수 있다. E2E Security는 PKI와 더불어 두 종단 Diameter 노드 사이에 다수의 라우터, Diameter 브로커, Diameter 프락시 등이 중간에 존재할 경우, 디지털 서명을 통해 인증, 무결성, 부인 봉쇄 기능을 제공하고 암호화를 통해 기밀성을 제공한다. 이 절에서는 Diameter 노드가 PKI와 관련하여 공개키/비밀키(public key/private key)를 생성 과정, 공개키 인증서를 인증 기관으로부터 발급 받는 과정, 발급 받은 키를 이용해 암호화/복호화(encryption/decryption) 과정, 서명/검증(signature/validation) 과정, CMS 보안 응용에서 사용하는 알고리즘에 대해 기술한다.

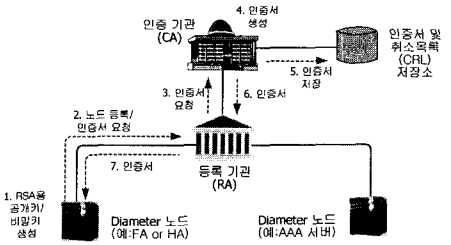


그림 7 공개키/비밀키 생성 및 인증서 발급

가. 공개키/비밀키 생성 및 인증서 발급

E2E를 사용하는 종단의 두 Diameter 노드들은 자신의 공개키/비밀키 쌍을 생성하여 등록 기관에 공개키를 등록하고 인증서를 요청한다. 등록 기관은 각 노드들을 확인한 후, 인증 기관에게 이를 확인시킨다. 인증 기관은 각 노드의 공개키에 대한 인증서를 생성한 후, 이를 인증서 저장소에 저장하고 등록기관

에게 전송한다. 등록 기관은 전송 받은 공개키 인증서를 해당 각 노드에게 보낸다. 이 과정에서 등록 기능을 등록 기관 없이 인증 기관에서 직접 담당할 수 있다.

나. 공개키 검색

두가지 공개키 검색 방법이 있다. 첫째는 초기에 두 노드간 Diameter 보안 연관(DSA; Diameter Security Association) 설정을 위해 송수신되는 DSAR/DSAA(DSA Request/Answer) 메시지 안에 각각의 공개키를 포함시켜 전송하는 방법이다. 이 방법은 LDAP 등의 프로토콜을 이용하지 않고 Diameter 자체적으로 공개키 검색 문제를 해결할 수 있다. 둘째는 두 노드들이 DSAR/DSAA 메시지를 주고 받아 통신하고자 하는 상대방의 인증서 위치를 알아낸 후, LDAP 프로토콜을 이용해 인증서를 받아오는 것이다. 이 두가지 방법을 이용하여 인증서를 받아온 후, 노드들은 RFC2459(Internet X.509 PKI Certificate and CRL Profile)[12]을 통해 인증서를 검증한다.

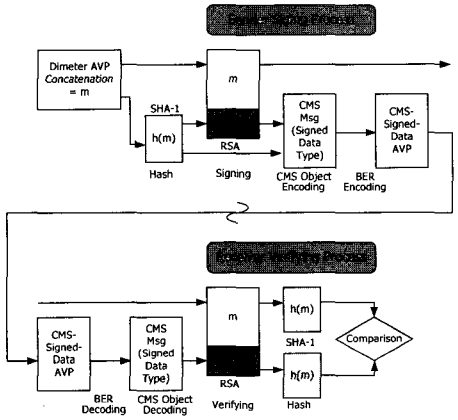


그림 8 Diameter AVP들의 서명 및 검증 과정

다. 서명 및 검증

그림 8에 나타낸 디지털 서명 및 검증은 인증, 무결성, 부인 봉쇄 기능을 제공한다. 두 사업자간 양방향 승인이 필요한 과금 정보와 같은 중요한 데이터들이 서명되며, 서명이 필요한 AVP는 Diameter 헤더에 'P' 비트가 셋팅된다. 서명 절차는 다음과 같다. 송신 노드는 서명할 AVP들을 concatenation시키고, 원문을 해쉬함수SHA-1으로 압축(digest)한다. 그리고 이 결과 값을 RSA로 서명한다. 압축된 값과 서명문을 CMS의 SignedData Type에 포함시키고, BER 엔코딩하여 CMS-Signed-Data AVP를 최종적으로 생성한다. 이 AVP는 다른 AVP들과 동일하게 Diameter 메시지에 패킹되어 수신측에 전달된다.

서명문의 수신자인 수신 노드는 검증을 수행한다. CMS-Signed-Data AVP에서 원래의 SignedData Type을 추출한다. 그리고 RSA 알고리즘을 통해 검증한다. 검증을 통해 나온 값을 SHA-1으로 해쉬하고, 다시 원래의 메시지를 해쉬하여 두 값을 비교한다. 비교한 결과가 같으면 검증은 성공한 것이므로 이후 Diameter 메시지 처리를 계속 수행한다. 비교 결과가 다르면 해당 Diameter 메시지는 폐기한다.

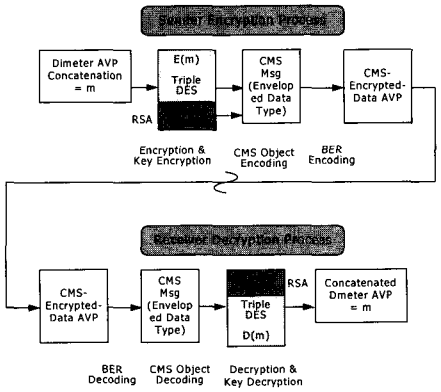


그림 9 Diameter AVP들의 암호화 및 복호화

라. 암호화 및 복호화

그림 9에 나타낸 암호화 및 복호화는 Diameter 메시지의 기밀성을 제공한다. 로컬 정책 및 Diameter 규격에서 암호화를 추천하고 있는 AVP의 예를 들면, MIP의 동적 세션 키들을 들 수 있다. 암호화 절차는 다음과 같다. 암호화할 AVP들을 concatenation시키고, 원문을 Triple DES로 암호화하고 DES Key를 RSA로 암호화 한다. 암호화된 값을 CMS의 EnvelopedData Type에 포함시키고 BER 엔코딩 하여 CMS-Encrypted-Data AVP를 최종적으로 생성한다. 이 AVP는 다른 AVP들과 동일하게 Diameter 메시지에 패킹되어 수신측에 전달된다. Diameter 수신 노드는 복호화를 수행한다. CMS-Encrypted-Data AVP에서 원래의 EnvelopedData Type을 추출한다. 그리고 RSA로 복호화하여 키를 추출한 후, Triple DES로 메시지를 복호화하여 원문을 추출한다. 이의 결과는 concatenated된 AVP이다 어떤

AVP들은 암호화와 복호화가 동시에 이루어질 수 있다. 이 경우, 암호화를 먼저 수행하고, 그 결과 값을 서명한다.

마. 알고리즘

Diameter CMS 보안 응용에서는 아래의 알고리즘을 사용한다. 참고로 Triple DES는 AES로 대치될 것이다.

- Hashing: sha-1
- Signature: rsaEncryption
- Content Encryption: ded-ede3-cbc
- Asymmetric Key Transport: rsaEncryption
- Symmetric Key Encryption: id-alg-CMS3 DESwrap

바. Diameter 보안 연관 설정

Diameter 메시지들은 각 에이전트의 응용에서 처리되기 때문에, 통신하고자 하는 두 Diameter 노드 사이에 한 개 또는, 그 이상의 다른 에이전트들이 존재하는 경우에 hop-by-hop security 메커니즘들 즉, TLS, IPsec으로서는 충분한 보안을 제공할 수 없다. 이를 위해 응용 계층에서 Diameter 메시지들을 보호할 수 있는 새로운 메커니즘이 요구된다. 이를 위해 Diameter에서는 통신하고자 하는 두 노드간 사전에 DSA를 설정한다. 그림 10에 나타낸 DSA는 보호된 AVP가 라우팅 경로에서 변경되었는지 그리고, 중간 에이전트들이 중요한 데이터를 감추었는지를 검출할 수 있게 해 준다.

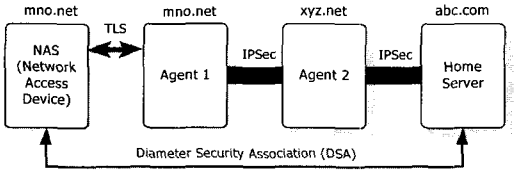


그림 10 Diameter 보안 연관(DSA) 설정

Diameter 프로토콜은 두 Diameter노드 사이에 한 개 이상의 Diameter 브로커를 거쳐 통신하는 것을 허용한다. Diameter 브로커는 중계 에이전트, 프락시 에이전트, 리다이렉트 에이전트가 될 수 있다. 중계 에이전트는 사전 로밍 컨소시엄을 맺은 Diameter 노드들간 메시지를 라우팅하며, 중간에 메시지를 변경하지 않는다. 프락시 에이전트는 정책을 반영하고, 액티브하게 메시지를 변경한다. 리다이렉트 에이전트는 Diameter 메시지의 경로를 재지정하는 역할을 한다. Diameter 프로토콜에서는 네트워크 토폴로지에 따라 그리고 에이전트들의 형태에 따라 (1)중계 에이전트를 거친 보안 연관 설정, (2)프락시 에이전트를 거친 보안 연관 설정, (3)리다이렉트를 거친 보안 연관 설정을 선택할 수 있다.

3.4 NASREQ 응용 기술

Diameter NASREQ 응용은 기존 RADIUS 프로토콜과 역 호환성(Backward Compatibility)을 제공한다. 그리고 무선랜에서 사용하고 있는 PPP-EAP (PPP-Extensible Authentication Protocol) 프로토콜을 지원한다. 이외에 PPP 다이얼 인, 터미널 서버, L2TP(Layer Two Tunneling Protocol) VPN 등 다양한 서비스를 지원한다. 이 응용은 초기에는 기존 RADIUS 기능 제공이 위주가 될 것이나, 점차적으로는 최근 관심을 끌고 있는 무선랜 서비스를 위한 보안 기능을 제공할 것이다.

이 응용이 제공하는 장점들은 다음과 같다. 첫째, 로밍 서비스를 고려한 Diameter 프레임워크를 적용함으로 인해 다수의 사업자 망들의 서버들간 peer-to-peer 형태로 운용하여 서비스 할 수 있다. 둘째, PPP-EAP를 적용하여 다수의 인증 메커니즘 즉, 스마트 카드, 토큰 카드, kerberos, 공개키, OTP(One Time Password) 들을 제공할 수 있다. 셋째, EAP 클라이언트와 홈 Diameter 서버인 AAAH간 E2E 보안을 제공하므로 재생 공격(replay attack) 및 끼어들기(man-in - the-middle attack) 공격과 같은 보안 위협성을 없앨 수 있다. 이러한 상호 인증은 로밍 PPP 환경에서 기존 PPP PAP과 CHAP으로서는 제공할 수 없는 기능이다. 넷째, 또 다른 인증 방식으로서 하위 계층에EAP-TLS를 적용할 수 있다. 이 방식은 상위 응용인 NASREQ와 독립적으로 강화된 보안을 제공할 수 있다.

그림 11에 Diameter NASREQ 기반의 무선랜 EAP 인증 절차를 하나의 예로 보였다. Diameter 서버들간 통신에 있어서 PPP-EAP 메시지 및 AVP들은 EAP-Payload AVP로 엔캡슐레이션되거나 또는 반대로 디캡슐레이션 된다. 즉, PPP-EAP는 NAS REQ 패킷에embedded된다. PPP-EAP는 다수의 인증 메커니즘을 포장하는 틀을 제공한다. PPP-EAP를 위해 정의된 코드는 요청, 응답, 성공, 실패로 4개

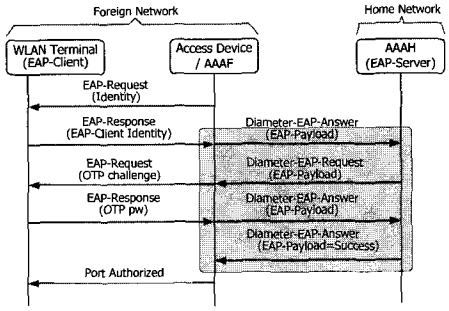


그림 11 Diameter NASREQ 기반의 무선랜 EAP 인증 절차 예

가 존재하며, 타입으로는 Identity, Notification, Nak-Response, MD5-Challenge, OTP, Generic Token Card가 있다. 이 중 전자의 3개는 기본적으로 지원되어야 하며, MD5 Challenge 인증 방식은 무선랜에서 반드시 지원되어야 한다. 지정된 인증 메커니즘에 따라 EAP 클라이언트와 서버간 라운드 트립 횟수가 결정된다. 물론 다수의 메시지를 주고받는 핸드쉐이킹을 할 수 있으며, 이를 나타내기 위해 서버들은 Result-Code에 DIAMETER_MULTI_ROUND_AUTH를 지정한다.

3.5 미래 응용 기술

현재 제안되고 있는 초기 단계의 미래 응용은 Diameter 멀티미디어 응용과 MIPv6 응용을 들 수 있다. 전자는 SIP 서비스에 대한 AAA 기능을 제공하며, 후자의 경우는 MIPv6에 대한 AAAv6 기능을 제공한다. 멀티미디어 응용은 3GPP 규격에서 먼저 제안되었으며, 인증센터와 홈 위치등록기 기능을 제공하는 HSS(Home Subscriber Server)와 SIP 서버 기능을 수행하는 CSCF(Call Session Control function)간 인터페이스에 적용된다[13]. 이 응용은 IETF에 개인 자격의 드래프트로 제안되어 있다. 후자의 MIPv6 응용 또한 개인 자격의 드래프트로 제안되어 있다. 이러한 응용들은 이후 공식적인 드래프트로 상정될 예정이므로 표준화가 단기간에 완성되기는 어려울 것이다.

4. 망간 접속에 따른 Scalability 고려사항

다수의 무선랜 공중망들의 접속 또는 다수의 무선랜 공중망과 이동통신 망을 접속하여 로밍 서비스를 제공하기 위해서는 망간에 걸친 AAA 서버들의 접속에 따른 확장성(scalability)을 우선적으로 고려해야 한다. 더구나 국외 사업자간 AAA 서버들의 접속하는 상황을 고려해볼 때, 그 중요성이 더 커지게 된다. 클라이언트-서버 구조이면서, 수직적인 계층적 구조를 갖는 RADIUS는 확장성을 제공하지 못한다. RADIUS에서 고려해볼 수 있는 사업자간 접속 방법은 두 가지를 들 수 있다. 첫째는 사업자간 망을 직접 접속하는 방법이고, 둘째는 사업자간 상위에 공용서버를 두는 방법을 고려해 볼 수 있다. 그러나 둘 다 메쉬 형태로 접속되므로 확장성에는 한계가 있으며, 사업자들의 망이 상호 개방되기 때문에 새로운 보안 취약성을 가진다.

이에 반해, peer-to-peer 구조이면서, 수평적인 계층 구조를 갖는 Diameter는 확장성을 기본적으로 제공한다. Diameter에서는 AAA 브로커(AAAB)를 통해 다수 사업자들의 망을 논리적이고 안전하게 분리하므로, 사업자 망간 직접적인 비즈니스 관계와 보안 관계를 가지지 않을 수 있도록 해준다. 또한 (글로벌) 로밍 컨소시엄 구성 및 운용할 수 있도록 해준다. 로밍 컨소시엄 기능은 AAA 브로커를 통해 이루어지며, 모든 사업자 망은 지정된 브로커를 통해 접속된다. 브로커의 주요 기능으로서, Diameter 요청 및 응답 메시지 중계 기능, Diameter 메시지 경로 재설정 기능, 로밍 컨소시엄 관리 기능 등이 있으며, 필요에 따라 프락시 기능을 수행할 수 있다. 이 노드는 별도 제3자의 망에서 운용될 수도 있고, 방문 망 또는 홈 망에서 운용될 수 있다.

5. 맺음말

유무선 통합 서비스라는 패러다임의 변화가 구체화되고 있다. 점진적으로 무선랜 공중망 서비스가 확산됨에 따라 시장이 확대되고, 이로 인해 무선랜 공중망간 로밍 서비스 그리고 무선랜 공중망과 이동통신 망간 로밍 서비스 요구가 증대될 것이다. 이를 위해서는 서비스 사업자간 주파수 혼신 방지, 무선랜 자체의 강화된 보안 기술 개발, 무선 인터넷 서비스를 제공하는 무선랜 공중망과 이동통신 망간 로밍 체계 및 관련 인프라 구축, 망간 로밍 서비스 제공을 위한 정책 수립 및 기술 표준화, 로밍 서비스를 위한 안전한 로밍 서비스 보안 기술 개발 등이 이루어져야 한다. 미래의 무선 인터넷은 다양한 액세스 망간에

걸쳐있는 이동성이 필수적으로 요구될 것이다. 특히, 무선 인터넷 사용자의 로밍 서비스를 위해 필수적으로 제공되어야 할 로밍 서비스 보안 기술 즉, 망간에 걸친 가입자 인증, 권한 검증, 과금, 망 노드들간 상호 인증을 제공하는 AAA 기술은 중요도가 더해 질 것이다. 이러한 AAA 기술은 현재 키워드가 되고 있는 유무선 통합 망에 적용될, 그리고 beyond IMT-2000 망에 적용될 주요 기술 중의 하나로 발전될 것이라 판단된다.

참고문헌

[1] Charles E. Perkins, "Mobile IP Joins Forces with AAA", IEEE Personal Communications, August 2000.

[2] Christopher Metz, "AAA PROTOCOLS: Authentication, Authorization, and Accounting for the Internet", IEEE Internet Computing, December 1999.

[3] Pat R. Calhoun, Jari Arkko, Erik Guttman, "Diameter Base Protocol", draft-ietf-aaa-diameter-10.txt, IETF work in progress, March 2002.

[4] Pat R. Calhoun, Allan C. Rubens, Jeff Haag, Glen Zorn, "Diameter NASREQ Application", draft-ietf-aaa-diameter-nasreq-09.txt, IETF work in progress, March 2002.

[5] Pat R. Calhoun, Charles E. Perkins, "Diameter Mobile IPv4 Application", draft-ietf-aaa-diameter-mobileip-09.txt, IETF work in progress, March 2002.

[6] Pat R. Calhoun, Stephen Farrell, William Bulley, "Diameter CMS Security Application", draft-ietf-aaa-diameter-cms-sec-04.txt, IETF work in progress, March 2002.

[7] R.Housley, "Cryptographic Message Syntax", RFC 2630, June 1999.

[8] Stefano M. Faccin, Franck Le, "Diameter Mobile IPv6 Application", draft-le-aaa-diameter-mobileipv6-01.txt, November 2001.

[9] Tony Johansson, Kevin Purser, "Diameter Multimedia Application", draft-johansson-aaa-diameter-mm-app-01.txt, IETF work in progress, Feb. 2002.

[10] Bernard Aboba, "Authentication, Authorization and Accounting (AAA) Transport Profile", draft-ietf-aaa-transport-05.txt, IETF work in progress, November 2001.

[11] 김현곤, 유희종, 이윤주, "AAA의 Diameter CMS 보안 응용 기술", ETRI 주간 기술 동향 1030호, pp.20-32, January 2002.

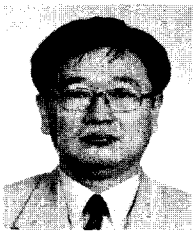
[12] R.Housley, Ford, Polk, Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

[13] 3GPP TS 29.229 v1.0.0, "3GPP TSG Cx Interface based on the Diameter Protocol: Protocol details (Release 5)", December 2001.

김 현 곤

1992 금오공과대학교 전자공학과 학사
1994 금오공과대학교 전자공학과 석사
1997~현재 충남대학교 전자공학과 박사과정
1994~현재 한국전자통신연구원 정보보호연구본부 AAA정보보호연구팀장
관심분야:IP 기반의 이동통신 네트워크 및 정보보호, 무선 인터넷 정보보호
E-mail:hyungon@etri.re.kr

손 승 원



1984 경북대학교 전자공학과 학사
1994 연세대학교 전자공학과 석사
1999 충북대학교 전자공학과 박사
1991~현재 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 부장
관심분야:IC Card, Biometry, Active Network
E-mail:swsohn@etri.re.kr

김 대 영

1975 서울대학교 전자공학과 학사
1977 한국과학기술원 전기 및 전자공학과 석사
1983 한국과학기술원 전기 및 전자공학과 박사
1983~현재 충남대학교 공과대학 정보통신공학부 정교수
관심분야:차세대 컴퓨터 네트워크, 차세대 인터넷 프로토콜
E-mail:dykim@cnu.ac.kr