속성 인증서 기반의 AAA 프로토콜에 관한 연구

정 구 완[0], 송 주 석, 유 희 종, 김 현 곤
연세대학교 컴퓨터과학과, 한국전자통신연구원 AAA정보보호연구팀
{gwjung[0], jssong}@emerald.yonsei.ac.kr {anny5, hyungon}@etri.re.kr

A Study on Attribute Certificate Based AAA Protocol

Gu-Wan Jung[0], Joo-Seok Song, Hee-Jong Ryu, Hyun-Gon Kim
Dept. of Computer Science, Yonsei University
AAA Security Information Research Team, Electronics and Telecommunications Research Institute

요 약

AAA(Authentication, Authorization, Accounting) 프로토콜은 기존의 PPP 뿐만 아니라 VoIP 및 Mobile IP 등과 같은 차세대의 다양한 네트워크와 프로토콜 상에서 안전하고 신뢰성 있는 사용자의 인증, 권한관리 및 과금을 제공하는 정보보호 메커니즘이다. 그러나 이러한 AAA 프로토콜에서는 사용자의 권한관리에 대한 표준화된 메커니즘을 제공하지 않고 있어, 도메인간의 로밍 및 새로이 출현하는 서비스 상의 권한관리에 대해 확장성 및 호환성이 결여될 수 있다. 따라서 본 논문에서는 IETF에서 권한관리 기반구조의 표준으로 제시하고 있는 속성 인증서(Attribute Certificate)를 통해 Diameter 프로토콜에서의 효과적이고 표준화된 권한관리 메커니즘을 제안하고, 관련 Diameter 메시지 등을 정의하였다.

1. 서 론

최근 들어 이동통신 환경의 비약적인 발전으로 로밍(Roaming) 서비스 등에 대한 사용자의 요구가 높아지고 있으며, Mobile IP, VoIP 및 VPN 등의 새로운 서비스가 등장하여 조만간 상용화가 이루어질 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, 그의 서비스 사용 내역에 따른 과금을 부여하는 메커니즘이 필수적으로 구축이 되어야 한다.[1]

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 IP 등의 관련 응용 프로토콜의 표준화를 진행하고 있다.[2]

그러나 기존의 AAA 프로토콜에서는 사용자의 권한관리에 대한 특정한 메커니즘을 제공하지 않고 있으며, 대부분의 권한관리 및 검증 메커니즘이 AAA 서버에 위치한 DB 및 Policy 서버의 수동적인 설정에 의하거나, 사용자의 공개키 인증서를 확장하여 권한 속성을 정의하고 있는 실정이다.

이러한 AAA 서버에 의존적인 사용자 권한관리 메커니즘은 향후 도메인간 로밍이 잦은 환경에서 확장성 및 호환성이 결여될 수 있다. 또한 공개키를 통한 사용자 권한관리 메커니즘의 경우, 실시간 애플리케이션과 같이 사용자의 권한정보가 수시로 변경되는 환경에서는 매우 부적합하게 된다. 따라서 사용자의 인증정보와 권한정보는 분리되어 관리되는 것이 바람직하다.

본 논문에서는 IETF에서 권한관리 기반구조(Privilege Management Infrastructure, PMI)의 표준으로 제시하고 있는 속성 인증서(Attribute Certificate)를 통해 Diameter에서의 효과적이고 표준화된 권한관리 메커니즘을 제안하고, 관련 Diameter 메시지와 AVP 등을 정의하고자 한다.

2. 권한 관리 기반구조

공개키 기반구조(Public Key Infrastructure, PKI)에서 사용되는 공개키 인증서는 상대방의 신원 확인의 기능을 지원하지만, 임무, 지위, 역할 등에 따른 다양한 권한 속성 정보 제공에는 많은 한계를 지니고 있다.[3]

PMI(Privilege Management Infrastructure), 즉 권한관리 기반구조는 속성 인증서를 통해 이러한 사용자의 권한 속성을 체계적으로 생성, 관리 및 검증해주는 기반구조로써, 최근 들어 다양한 분야에 활발히 응용되고 있다.

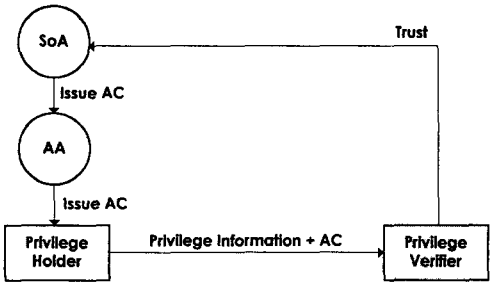

그림 1. PMI의 구조

(그림 1)은 PMI의 전반적인 구조이다. SoA(Source o Authority)는 권한 검증자로부터 무조건적으로 신뢰되는

개체로써, PKI에서의 Root CA와 같은 역할을 하는 최상위의 권한 인증기관이다. 이러한 SoA는 AA(Attribute Authority)에게 권한을 위임할 수 있으며, AA는 조직내의 권한 인증기관으로써 내부의 자원에 대해 권한을 관리하고 사용자 속성 인증서를 발급하는 역할을 한다.[4]

앞으로 PMI 체계는 다양한 네트워크 상의 자원과 사용자간의 체계적인 권한 관리를 제공하여, 향후 권한 관리 메커니즘으로써 중요한 역할을 할 것으로 보인다. 따라서 AAA 환경에서 이러한 PMI를 통한 사용자의 권한 관리 메커니즘은 다양한 네트워크와 프로토콜 상에서 표준화된 방법을 제공할 수 있다.

3. 속성 인증서 기반의 Diameter 프로토콜

3.1 PMI 체계와 AAA Framework의 연동 모델

본 논문에서 제시하는 PMI와 AAA 개체가 연동되는 기본 모델은 (그림 2)와 같으며, ITU-T의 X.509 PM Framework에서 제시하는 일반, 제어, 위임 및 역할 모델 또한 적용이 가능하다.

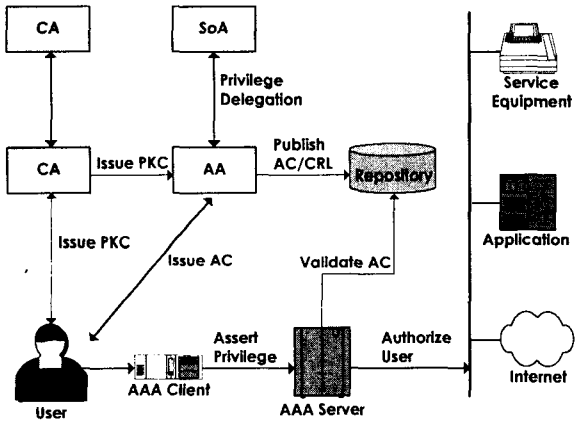

그림 2. PMI 체계와 AAA Framework의 연동

AAA 클라이언트는 일반적으로 NAS 또는 Mobile IP의 FA(Foreign Agent)와 같은 Access Device의 모듈에 포함되며, 사용자의 접속 시, 이의 인증 및 권한 검증 등을 AAA 서버에게 요청하는 개체이다.

기본적으로 사용자와 권한 인증기관은 인증기관, 즉 CA(Certificate Authority)로부터 공개키 인증서를 발급받아 신원을 보증 받아야 한다. 그리고 AA는 사용자의 임무, 지위, 역할 등에 따라 권한이 정의된 속성 인증서를 사용자에게 발급하고, 이를 저장소(Repository)에 공개한다. 이후 사용자가 AAA 서버를 통해 조직내의 주요 자원이나 서비스에 접근 요청 시, AAA 서버는 사용자의 속성 인증서를 획득한 후, 이의 유효성을 검증한다.

3.2 PMI와 AAA 연동을 위한 요구사항

AAA 개체와 AA 및 CA 등의 PMI 개체가 상호 운영되기 위한 각 개체의 요구 사항은 다음과 같다.

(1) AA는 AAA 서버의 권한 관리 모듈에 포함되어 구현될 수 있다. 이 경우 AAA는 인증기관으로부터 공개키 인증서를 발급 받아야 한다.

(2) Diameter 프로토콜은 username@realm의 형식으로 이루어진 NAI(Network Access Identifier)를 가입자에게 부여하며, 이를 통해 사용자 식별 및 홈 네트워크로의 메시지 라우팅을 수행한다. 따라서 속성 인증서의 소유자 필드, 즉 Holder 필드는 이러한 NAI를 rfc822Name 형식에 따라 entityName으로 지녀야 한다. 또한 공개키 인증서는 subjectAltName 확장 필드로 이러한 NAI를 포함하여 NAI를 통해 공개키 인증서가 참조될 수 있어야 한다.

(3) 사용자는 AAA 서버에게 인증 요청 메시지를 전송하면서, 속성 인증서 및 공개키 인증서를 직접 전달할 수 있다. 또한 참조를 통해 AAA 서버에게 인증을 요청할 수 있으며, 이 경우 AAA 서버는 LDAP, HTTP 및 FTP 등의 프로토콜을 통해 사용자의 속성 인증서 및 공개키 인증서를 획득할 수 있어야 한다.

(4) AAA 서버는 검증 정책에 따라 속성 인증서와 공개키 인증서의 유효성을 검증할 수 있어야 한다. 검증 정책은 인증서 유효성 검증에 적용될 규칙들을 말하며, 신뢰되는 AA 및 CA 등의 인증기관들을 명시하거나 인증 경로 생성 및 경로 위임 처리에 대한 규칙이나 인증서의 폐지 상태 정보 처리에 대한 규칙 등을 제공한다.

(5) AAA 서버는 요청된 인증서에 대한 폐지 상태를 확인 할 수 있도록 CRL, OCSP, Delta CRL 등의 다양한 폐지 정보를 조합하거나 또 다른 AAA 서버의 응답을 이용할 수 있어야 한다.

3.3 PMI 연동을 위한 Diameter 확장

Diameter 프로토콜은 유연성 및 확장성이 뛰어나, 새로운 메시지 및 관련 AVP의 정의가 용이하다. PMI 체계와 AAA의 연동을 위해 Diameter 프로토콜에서 요구되는 관련 메시지와 AVP는 다음과 같다.

(1) 속성 인증서를 위한 Diameter 메시지

PMI 체계와 연동되기 위해 정의된 새로운 Diameter 메시지는 ACAR과 ACAA이다. 현재 이러한 메시지의 코드값은 IANA(Internet Assigned Numbers Authority)에서 관리되고 있으므로 이의 정의는 생략한다.

- Attribute-Certificate-Authorization-Request
  ACAR로 축약하며, AAA 클라이언트가 속성 인증서를 통해 권한 검증을 요청하는 메세지이다.
- Attribute-Certificate-Authorization-Answer
  ACAA로 축약하며, 속성 인증서를 통해 권한 검증 요청에 대한 응답 메시지이다. 이 메시지에는 권한 검증 환경에 관련된 AVP를 포함한다

(2) 속성 인증서를 위한 Diameter AVP

- User-Certificate AVP
  OctetString의 형식이며, 사용자의 공개키 인증서를 포함한다. 만약 이 AVP가 제공되지 않는다면, 권한 검증자, 즉 AAA 서버는 사용자의 NAI 또는 제공된

속성 인증서의 Holder 필드를 통해 사용자의 공개키 인증서를 획득한다.

- User-Attribute-Certificate AVP
  OctetString의 형식이며, 사용자의 속성 인증서를 포함한다. 만약 이 AVP가 제공되지 않는다면, AAA 서버는 사용자의 NAI 또는 제공된 공개키 인증서의 subjectAltName 확장 필드를 통해 사용자의 속성 인증서를 획득한다.
- CA-Name AVP
  UTF8String 형식이며, 사용자 공개키 인증서의 인증기관 DN(Distinguished Name)을 포함한다.
- AA-Name AVP
  UTF8String 형식이며, 사용자 속성 인증서의 권한 인증기관 DN(Distinguished Name)을 포함한다.
- Key-Hash AVP
  OctetString 형식이며, CA 또는 AA의 공개키 인증서에 대한 SHA-1 Hash 결과 값을 가진다. 검증자는 공개키 및 속성 인증서 검색 시, 이 Hash 결과 값을 인덱스로 사용하여 신속한 검색을 수행할 수 있다.
- Local-CA-Info AVP
  Group 형식이며, CA-Name AVP와 이의 Key-Hash AVP를 그룹 짓는다.
- Local-AA-Info AVP
  Group 형식이며, AA-Name AVP와 이의 Key-Hash AVP를 그룹 짓는다.
- CA-Chain AVP
  OctetString 형식이며, 사용자의 공개키 인증서를 발급한 상위 CA부터 검증자로부터 신뢰되는 CA, 즉 최상단 CA까지의 검증 체인을 포함한다.
- AA-Chain AVP
  OctetString 형식이며, 사용자의 속성 인증서를 발급한 상위 AA부터 검증자로부터 신뢰되는 AA, 즉 최상단 AA까지의 검증 체인을 포함한다.
- Access-Target AVP
  UTF8String 형식이며, 사용자가 접근하고자 하는 자원이나 서비스의 ID 및 URI 등을 포함한다. 이 AVP에 지정된 접근 대상이 속성 인증서의 Access Identity 속성에 나타나지 않는다면, 추가적인 권한 검증을 수행하지 않고 실패를 반환함으로써 보다 신속한 권한 검증을 제공할 수 있다.
- Validation-Policy AVP
  UTF8String 형식이며, 인증서의 유효성 검증에 적용될 AAA 서버의 검증 정책을 포함한다. 사용자는 AAA 서버의 검증 정책에 따라 효과적인 검증 환경을 제공할 수 있다.
- Result-Code AVP
  기존의 Result Code는 PMI 체계 지원 및 속성 인증서 검증 결과에 대한 응답을 반환하기 위해서, 이와 관련된 결과 코드 값의 확장이 필요하다.

4. 결 론

오늘날의 네트워크 환경은 여러 서비스와 시스템의 비약적인 확대로 그의 사용 권한에 대한 세부적이고 안전한 제어가 요구되고 있다. 이러한 환경에서 기존의 AAA 서버에 의존된 사용자의 권한 관리는 여러 한계점을 가질 수 있다. 따라서 본 논문에서는 속성 인증서를 통한 AAA 권한 관리 메커니즘을 제안하였고, PMI 개체와 AAA 개체간의 상호 운용을 위한 요구 사항과 관련된 메시지를 정의하였다. 이러한 AAA 권한 관리 모델은 기존의 한계를 벗어나 여러 이점을 제공해 준다.

첫째, 세부적이고 효과적인 권한 관리 메커니즘을 제공할 수 있다. 속성 인증서는 주요 자원에 대한 사용자의 권한에 대해 세부적인 속성을 제공함으로써 강력한 권한 관리가 가능하다, 또한 사용자에게 역할만 부여한 뒤, 역할과 권한의 연결 정보를 이용한 역할기반의 접근 제어 등의 효과적인 권한 관리 기법을 제공할 수 있다.

둘째, 다양한 네트워크와 서비스 상에서의 표준화된 사용자 권한 관리 기법을 제공해 준다. 속성 인증서는 권한 관리 기반구조의 표준인 속성 인증서를 통한 AAA 권한 관리 메커니즘은 상이한 네트워크와 서비스에서도 사용자의 권한 관리에 대해 표준성을 제공해 준다. 결과적으로 사용자의 권한 관리 및 유지비용이 낮아지게 된다.

마지막으로, 사용자의 도메인간의 로밍 시, 권한 검증에 대해 호환성을 제공해줄 수 있다. 기존 AAA의 경우 사용자가 방문한 도메인에서의 권한 검증은 별도의 로밍 협약에 의해 사용자의 홈 도메인에서 이루어지게 된다. 그러나 제안된 모델에서는 두 도메인이 동일한 AA 또는 SoA를 갖는다면 사용자의 속성 인증서 검증이 방문한 도메인에서 이루어질 수 있다.

이와 같이 본 논문에서 제안된 속성 인증서 기반의 AAA 프로토콜은 차세대의 다양한 네트워크와 서비스에서 강력하고 효과적인 권한 관리 모델을 제시하였으며, 동시에 여러 이점들을 제공하였다. 앞으로 이와 관련된 많은 연구가 이루어지기를 기대한다.

참 고 문 헌

[1] C. Rensing, M. Karsten, B. Stiller, "AAA: a surve and a policy-based architecture and framework", IEEE, Volume 16, Issue 6, 22-27, Nov.-Dec. 2002

[2] P. Calhoun, T. Johansson, C. Perkins, "Diameter Mobile IP Application", IETF AAA Internet-Draft Apr. 2003

[3] S. Farrell, R. Housley, "An Internet Attribute Certificate Profile for Authorization", IETF PKIX RFC 3281, April 2002.

[4] ITU-T Recommendation X.509, "Public-Key An Attribute Certificate Frameworks", ISO/IEC 9594-8 May 2001.

[5] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", IETF AAA Internet-Draft, Dec. 2002

[6] P. Calhoun, S. Farrell, W. Bulley, "Diameter CMS Security application", IETF AAA Internet-Draf Mar. 2002

[7] 이승훈, 송주석, "PMI 인증서 검증 위임 및 검증 프로토콜", 정보보호학회논문지, 제13권, 제1호, 59-67, 2003. 2