제21회 한국정보처리학회 춘계학술발표대회 논문집 제11권 제1호 (2004. 5)

차세대 보안 네트워크를 위한 인증 인가 서비스

김태성, 조영섭, 진승헌
한국전자통신연구원
email :taesung@etri.re.kr

Authentication and Authorization Service for Network Security System

Taesung Kim, Yeongsub Cho, Seunghun Jin
Electronics and Telecommunications Research Institute

요 약

사용자의 인증 및 자원에 대한 접근 권한을 제어하는 인가는 개별 서버에서 수행되어 왔다. 개별적인 인증과 인가는 서버의 관리 부담을 증가시키며, 서비스의 가입과 반복적인 인증으로 인해 사용자에게 불편을 초래한다. 따라서, 본 논문에서는 중앙집중적으로 인증과 인가를 대행하는 AAS 를 제안한다. AAS 는 ID 관리 기능 외에 단일인증(Single sign on), 멀티티어(multi-tier)인증, 역할기반 접근통제, 인증서 관리 서비스 등을 제공한다.

1. 서론

인증은 시스템을 보호하기 위해 서버가 사용자에게 사전에 약속된 정보를 제시 할 것을 요구함으로써 사용자를 확인하는 것이고, 인가는 인증 절차 후 제공된 토큰을 기반으로 자원의 사용자 접근 권한을 판별하여 허가하는 것이다. 컴퓨터와 인터넷이 급속히 보급되어 모든 분야에 활용됨에 따라 다양한 기능과 형태를 가진 응용이 등장하고 있으며. 무선 네트워크의 활용, 웹 서비스와 같은 새로운 응용 프레임워크의 등장으로 편의성과 안정성을 갖춘 새로운 형태의 인증 인가 기술이 요구 되고 있다.

현재 대부분의 인증과 ID 관리는 개별 서비스에서 수행하고 있다. 정보시스템이 인터넷과 같은 오픈된 네트웍으로 연결되면서 점점 침입이나 공격에 더 많이 노출되고 있다. 따라서 서비스는 이전보다 더 강력한 인증 방식을 도입해야 하고 패스워드나 인증서와 같은 비밀공유정보(credential) 관리에 더 많은 자원을 투자해야 한다. 사용자 입장에서도 접근하는 서비스마다 등록과 인증을 반복해야 하고 기억하고 관리해야 할 비밀공유정보는 점점 더 늘어가고 있다.

역할기반접근통제(RBAC, Role Based Access Control)[3]는 기업 환경뿐만 아니라 데이터베이스, 운영체제 등에 적용될 수 있는 매우 유연한 접근통제 정책으로 임의적 또는 강제적 접근통제 정책보다 정보에 대한 고수준의 접근통제와 효율적인 접근권한 관리를 수행할 수 있는 장점을 가지고 있다.

NSS(Network Security Service)는 보안 라우터, 보안 게이트웨이, VPN, 바이러스월, NIDS, 보안 관리 서버로 구성된 네트워크 보안 시스템으로서, 트래픽 폭주 분석, 네트워크 공격 탐지, 통계 서비스, 취약성 분석 및 보안 패치등을 수행한다. 이 논문에서 제안하는 AAS (Authentication and Authorization System)는 NSS 를 위한 인증 인가 시스템이다. NSS 의 모든 사용자의 ID 관리는 AAS 에서 이루어진다. ID 관리뿐만 아니라 인증도 AAS 가 대행함으로써 개별 서버는 서버 자신과 AAS 서버의 비밀공유정보만을 관리하므로 많은 비용을 절감할 수 있다. 사용자도 개별서버마다 ID 를 등록하고 비밀공유정보를 발급 받을 필요가 없으므로 비밀공유정보의 관리가 편리해지고, SSO 와 같은 고수준의 편리한 인증을 받을 수가 있다.

AAS 는 인가 서비스로 최소권한의 법칙(least privilege principle), 임무분리(SOD: separation of duty), 객체에 대한 고수준의 처리기능 제공이 가능한 역할 기반 접근통제를 제공한다. 서버는 사용자와 객체를 일

일이 인식하여 접근통제 정책을 수립할 필요 없이 역할과 접근객체를 인식함으로써 간단히 접근통제 정책을 수립할 수 있다.

본 논문의 구성은 다음과 같다. 2 장에서는 AAS 에서 사용하는 표준 프로토콜인 SAML 과 XKMS 에 대해 설명하고, 3 장에서는 차세대 보안 네트워크를 위한 인증 인가의 요구사항에 대해 살펴본다. 이 후 4 장에서 AAS 의 구조를 설명하고, 5 장은 AAS 의 인증 서비스, 6 장은 인가 서비스 그리고 7 장은 AAS 의 인증서 관리 서비스를 설명한다. 마지막으로 8 장에서 결론을 맺는다.

2. 관련 연구

SAML(Security Assertion Markup Language)[1]은 보안 정보를 교환하기 위한 XML 기반의 표준이다. 이 보안 정보는 어떤 보안 도메인에 소속되어 있는 사용자에 대한 보증(assertion)의 형태로 표현된다. 보증은 사용자에 대한 인증, 사용자의 속성, 그리고 자원에 접근 권한에 대한 인가 결정 등에 관한 정보를 담고 있다. SAML 의 주요한 목적은 하나의 도메인에서 인증한 사용자가 재 인증 없이 다른 도메인에서 자원을 접근할 수 있도록 하는 단일 인증(Single Sign On)을 제공함에 있다. SAML 표준을 채택하고 있는 대표적인 프로젝트로는 Liberty Alliance Project[4]와 Shibboleth Project[5]가 있다.

XKMS(XML Key Management Specification)[2]는 W3C 에서 개발한 공개키의 배포와 등록을 위한 공개 표준이다. XKMS 의 주요 목적은 XML 응용 개발자들에게 전통적인 PKI 구현의 복잡성의 부담을 경감시키기 위한 것이다. 신뢰 관계에 관한 처리를 특정 프로세서에게 위임함으로써 XML 에 기반한 시스템은 XML 이 처리되는 클라이언트에 신뢰 관계를 위해 PKI 응용 로직을 구현할 필요가 없다. XKMS 의 주요 기능은 서명 키 쌍의 등록, 공개키의 검색, 검증, 폐기, 갱신 등이다.

3. 요구사항

현재 대부분의 컴퓨터 시스템은 한 개 이상의 서버로 구성된 서비스에서 자체적으로 사용자의 ID 를 관리하고 인증을 수행한다. 네트워크가 고속화되고 시스템에 대한 공격이 지능화되면서 서비스는 강력한 인증 메커니즘을 수용하도록 요구 받고 있고 사용자의 비밀공유정보를 보호하기 위해 많은 비용을 지불하고 있다. 개별적 인증과 ID 관리는 사용자 입장에서도 큰 부담이다. 새로운 서비스를 이용하기 위해서는 사용자는 가입과 인증을 매번 새로이 해야만 한다. 많은 서비스에 가입된 사용자는 모든 서비스의 패스워드를 기억하고 비밀공유정보를 관리하는 것은 불가능하다.

차세대 보안 네트워크를 위한 인증 인가 기술은 개별 서비스에서 수행해 왔던 ID 관리와 인증을 대행해 주는 중앙 집중적인 서버의 도입이 필수적이다.

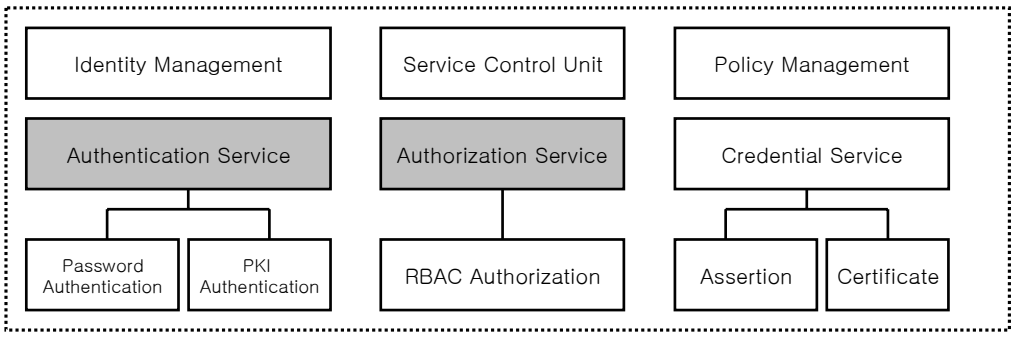
차세대 보안 네트워크의 사용자는 현재의 사용자 디바이스 보다 매우 다양한 모습을 가질 것이다. 현재도 무선 네트워크의 주요 디바이스는 모바일 폰, PDA 등이다. 이러한 장치는 사용자 인터페이스의 제약 때문에 현재의 컴퓨터보다 로그인 과정이 무척 힘들 수 있다. 한 번의 로그인으로 이 후 여러 서비스를 사용할 수 있는 SSO(Single Sign On)는 필수적인 기술이다.

SSO 가 가능하다 할지라도 모든 서버가 같은 비밀 강도를 가진 인증을 사용하지는 않을 것이다. 응용 특성에 따라 낮은 인증을 통과한 사용자는 비록 인증이 끝났다 하더라도 더 높은 인증을 수행하기를 바라는 서버는 존재한다. 예를 들어, 네트워크 장비의 중요 설정을 바꾸는 작업을 수행하기 위해서는 패스워드 인증 보다는 인증서 인증이 필요하다고 요구 할 수 있다.

RBAC 은 권한관리를 사용자와 정보 객체간의 관계가 아닌, 역할과 정보 객체간의 관계로 설정할 수 있게 함으로써, 정보 객체의 종류가 많은 환경에서 적합한 인가 모델의 특성을 가진다. 또한, 최소권한의 법칙(least privilege principle), 임무분리(SOD: separation of duty), 객체에 대한 고수준의 처리기능 제공 등과 같은 주요 보안 원칙들 역시 지원 하고 있다.

RBAC 은 여러 접근 제어 모델과 비교해서 많은 우수한 특성을 가지는 것으로 여겨지고 있다. AAS 와 같이 사용자 정보와 사용자가 접근하려는 정보 객체가 떨어져서 존재하는 모델은 사용자와 정보객체 사이에 역할을 두는 RBAC 모델이 적합하다.

.

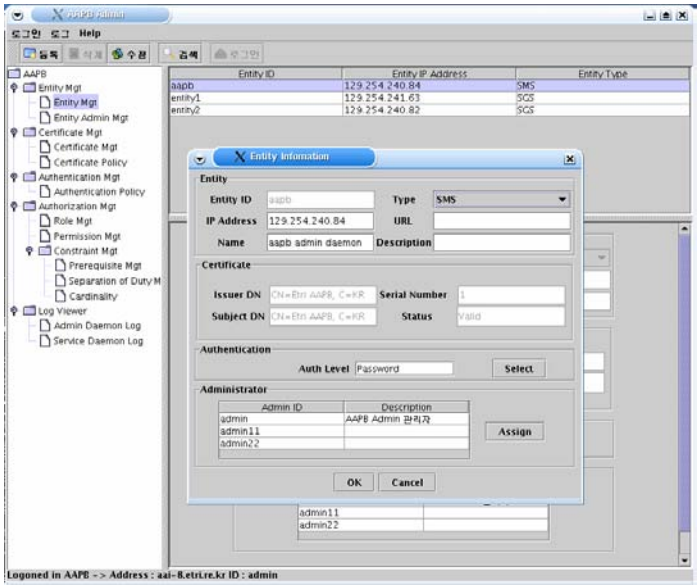


[그림 1] AAS(Authentication and Authorization System)의 구조

PKI 는 키 분배의 용이성과 수학적으로 증명된 해킹의 어려움 때문에 네트워크의 기반 구조 보호에 많이 사용된다. AAS 는 인증과 인가 외에도 인증서의 발급, 검증, 폐기에 이르는 인증서 라이프사이클(life cycle) 관리를 지원할 필요가 있다

4. AAS 의 구조

[그림 1]는 AAS 의 구조도이다. Service Control Unit 은 AAS 로의 요청을 분석하여 적절한 기능을 호출하고 응답하는 기능을 제공한다. Authentication Service 와 Authorization Service 의 실제 구현 서비스는 추가가 가능하도록 설계되었다. 현재 인증은 패스워드와 PKI 에 기반한 인증 기능을 제공하고, 인가는 RBAC 모델에 기반한 접근제어 기능을 제공한다. Credential Service 는 인증서관리와 AAS 에서 발급한 보증관리를 담당한다.



[그림 2] ID 관리창

5. 인증 서비스

AAS 는 NSS 의 모든 엔터티(entity)에 대한 ID 관리를 수행한다. ID 관리를 AAS 에게 일임함으로써 NSS 의 다른 서버는 사용자의 등록 및 비밀공유정보의 관리가 필요 없다. 사용자는 한번의 등록으로 여러 서버에 접속이 가능하고 비밀공유정보의 관리도 간결해진다. [그림 2]는 AAS 의 서버 ID 관리창이다. ID 관리창을 통해 서버에 접근 가능한 사용자, 인증서 관리, 인증 정책의 선택 등을 할 수 있다.

AAS 는 SAML 보증(assertion)을 이용한 SSO 서비스를 제공한다. 사용자는 AAS 에 로그인 하면 SAML 보증을 발급 받는다. 보증의 유효기간은 각 서버의 정책에 의해 결정되며 세션의 유지는 AAS 에 의해 관리된다. 세션 동안은 사용자는 여러 서버들에 인증과정 없이 사용할 수 있다.

제공되는 기능의 중요성, 네트워크 환경, 사용자 환경 등의 요인에 따라 서버가 원하는 사용자 인증의 비밀강도는 다르다. AAS 는 서버가 자신이 원하는 인증 강도를 설정할 수는 있는 방법을 제공하고, 설정된 인증 강도보다 낮은 인증을 수행한 사용자의 경우는 재 인증을 요구한다. AAS 에서 인증 강도는 숫자로 표현된다. 현재 패스워드 방식은 1, 인증서 기반 인증은 2 로 설정되어 있다. 인증 강도는 포함 관계로서 인증 강도 2 로(여기서는 인증서) 인증한 사용자는 이보다 같거나 낮은 인증 강도로 정책이 설정된 서버에서는 재인증이 필요 없다. 패스워드나 인증서 같은 인증 메커니즘을 직접적으로 정책에 세팅하도록 하지 않고 인증의 강도를 숫자로 표현한 이유는 새로운 인증 메커니즘의 수용을 원활히 할 수 있는 장점과 강한 인증이 낮은 인증을 수용하기에 적합하기 때문이다. [그림 3]은 인증 정책의 예를 보여 주고 있다.

[그림 3] 인증 정책

6. 인가 서비스

AAS 는 RBAC 형태의 인가 서비스를 제공한다. 사용자는 하나 이상의 역할(role)을 부여 받고 역할은 권한(permission)을 부여 받는다. 역할은 계층(hierarchy)구조를 갖는데 상위 역할은 하위 역할의 권한을 자동적으로 소유하게 된다.

AAS 는 RBAC 의 정적인 제약조건(constraint)를 지원한다. 선행 제약조건(prerequisite constraint)는 사용자가 정해진 역할을 부여 받기 전에 미리 부여 받아야 할 역할을 명시하는 제약조건이고, SOD 제약조건(separation of duty constraint)은 한 사용자에게 동시에 부여 될 수 없는 역할을 설정하는 것이다. Cardinality 제약조건은 정해진 역할에 부여 될 수 있는 사용자의 개수를 제한 하는 것이다.

사용자가 AAS 에 로그인하면 인가 보증(assertion)은 서버에게 전달된다. AAS 는 사용자에게 할당된 역할을 검사한 후, 각 역할에 부여된 권한을 모아서 인가 보증을 생성한다. 인가 결정은 AAS API 에서 인가 보증을 검사하여 해당하는 권한을 찾아내어 결정한다. 이것은 인가 결정이 로컬에서 수행되도록 함으로써 응답 시간을 줄이는 효과가 있다.

7. 인증서 관리 서비스

AAS 는 사용자 및 서버에게 인증서 관리 서비스를 제공한다. 인증서는 사용자의 인증에 사용될 뿐 아니라, 사용자의 서버 인증, AAS 의 서버 인증에 사용되

고, 사용자, AAS, 서버간의 통신의 비밀성과 무결성을 보장하기 위해 발급된다. AAS 는 인증서의 발급, 갱신, 폐기에 이르는 life cycle 동안의 관리 서비스를 제공하고 서버의 요청에 의해 인증서의 유효성 검증을 수행한다. 인증서에 관련한 모든 서비스는 XKMS 프로토콜을 준수한다.

8. 결론

AAS 는 차세대 네트워크 환경에서 요구되는 중앙집중적인 ID 관리 및 SSO 를 제공하고 인증 정책과 인증 강도의 개념을 통해 multi-tier 인증을 제공한다. 또한, RBAC 모델에 기반한 인가 서비스를 제공하며 인증서 관리 서비스를 제공한다.

향후에는 패스워드와 인증서 방식 외의 인증방법을 제공할 것이며 특히 IC 카드에 의한 인증 방법을 추가할 예정이다. 그리고, 사용자의 경우 XML 의 처리, 인증서의 처리 등 복잡하고 많은 메모리를 요구하는 연산을 수행할 수 없는 light-weight 사용자를 위해 AAS 에이전트를 추가할 것이다.

참고문헌

[1] Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML), OASIS, April 2002.
[2] XML Key Management Specification (XKMS), W3C, http://www.w3c.org/TR/xkms, March, 2001
[3] Role Base Access Control (RBAC), NIST, http://csrc.nist.gov/rbac/, April, 2004
[4] Liberty ID-FF Architecture Overview Version 1.2, http://project-liberty.org,
[5] Shibboleth Overview and Requirements, internet2, http:// http://shibboleth.internet2.edu, February 20, 2001