Attribute Certificate를 이용한 Web Access Control 연구

박재영*, 김동수*, 박세현*, 송오영*

*중앙대학교, 전자전기공학부

A Study of Web Access Control Based on Attribute Certificate

Jae Young Park*, Dong Su Kim*, Se Hyun Park*, Oh Young Song*,

School of Electrical & Electronics Engineering Chung Ang Univ.

요 약

본 논문에서는 제안하는 AC(Attribute Certificate)를 이용하여 Web 상에서의 권한을 제어하는 방식은 기존의 아이디/패스워드 방식의 사용자 인증보다 좀더 안전하게 사용자에 대한 권한을 관리할 수 있다. 기존의 방식은 ACL(Access Control List)를 사용하여 권한 인증을 하기 때문에 서버의 자원을 낭비하게 된다. 본 논문에서 제한하는 방식은 Web상에서의 활동 시 AC를 이용하여 사용자를 인증하게 된다. 이러한 인증을 각 서비스 제공자 사이의 AC에 대한 양식을 공유하고 권한 정보를 공유함으로써 많은 서비스 제공자 사이의 DB 문제를 해결하고 제휴된 어느 서비스 제공자에게나 사용자가 자신의 AC를 제공하여 권한을 획득할 수 있다.

I. 서론

일반적으로 보안(Security)라고 하는 말은, 아마도 누군가가 다른 사람의 컴퓨터에 침입해서 악의적인 목적으로 데이터를 훼손시키거나 빼내어 가는 과정을 의미하는 것으로 인식되고 있다.[1] 이러한 악의적인 제 3자로 인한 데이터의 손실이나 변조를 방지하기 위해 비밀키를 이용한 보안을 사용하였다. 하지만 기존의 대칭키 암호화 방식에서는 사용자가 많아질수록 키의 분배에 문제가 생기고 현재와 같은 온라인 상에서 물리적으로 멀리 떨어진 상대방에게 비밀키를 전달하는데 어려움을 느끼게 된다. 이러한 문제를 해결하고자 Diffie와 Hellman은 1976년에 Diffie - Hellman Key Exchange 알고리즘을 선보였는데 이것은 안전한 통신을 위해 오늘날의 공개키 암호화 시스템의 발전을 가져온 정교한 방법이다.[2] 공개키 암호화 방식에서는 기존의 방식과는 다르게 통신하고자하는 두 사용자 혹은 서비스 제공자와 사용자가 각각 자신의 공개키와 개인키를 가지고 공개키는 다른 사용자가 접근할 수 있는 공개된 디렉토리에 저장하게 된다. 암호문을 작성할 때는 수신자의 공개키로 암호화하여 보내게 되면 메시지를 받은 수신측은 자신만이 알고 있는 개인키로 메시지를 복호화 하여 메시지가 전달되는 동안변조가 없었다는 것을 확인할 수가 있다. 하지만 여기서는 메시지를 송신자가 누구인지 알 수 없으므로 송신자의 신분을 인증할 만한 방법을 고안하게 되는데 이는 전자서명을 이용한 방식이다.[3] 메시지를 공동의 해쉬 함수로 해쉬한 다음 자신만이 알고 있는 개인키로 암호화 하여 원문과 개인키로 암호화된값(메시지 다이제스트)보내게 되면 수신측은 이 메시지 다이제스트를 송신측의 공개키를 구하여 복호화 한 값과 원문을 해쉬한 값을 비교하여 같으면 송신자를 인증하게 된다. 전자서명에 있는 공개키에 대한 인증으로 인증서를 사용하는데 이러한 시스템을 PKI(Public Key Infrastructure)라 한다.[4] 이러한 강한 인증이 많은 분야에서 시행되고 있는데 Web상의 컨텐츠를 제공하는 업체에서도 기존의 아이디/패스워드 인증방식에서 공개키를 이용한 인증이 요구되고 있는 실정이다. 많은 서비스 제공자들은 각 사용자에게 알맞은 컨텐츠 사용 권한을 부여하게 되는데 여기에 공개키를 이용한 PMI(Privilege Management Infrastructure)를 사용하면 좀더 강한 인증을 할 수 있으리라 예상된다. PMI에서는 각 사용자들의 권한을 AC(Attribute Certificate)를 이용하여 권한에 대한 인증 서비스를 제공하고 있다. 본 논문에서는 현재 Web 서비스 제공자들이 제공하는 컨텐츠에 대한 권한 인증으로 PMI에서 사용하고 있는 AC를 이용한 Web Access Control을 제안한다.

II. 기존 권한 관리의 문제점

기존의 Web상에서의 권한 인증 방식은 ACL을 이용하여 권한을 획득하였다. ACL은 개개의 사용자들이 디렉토리나 파일과 같은 특정 시스템 개체에 접근할 수 있는 권한을 컴퓨터의 운영체계에 알리기 위해 설정해 놓은 표라고 할 수 있다. 각 개체는 접근제어목록을 식별할 수 있는 보안 속성을 가지며, 그 목록은 접근권한을 가진 각

시스템 사용자들을 위한 엔트리를 가진다. 가장 일반적인 권한은 1개의 파일이나 또는 한 개의 디렉토리 안에 있는 모든 파일들을 읽을 수 있고(Read), 기록할 수 있으며(Write), 그리고 만약 그것이 실행가능한 파일이나 프로그램인 경우라면 실행시킬 수 있는(Execute) 권한 등을 포함한다.

각 ACL은 사용자의 이름이나 사용자 그룹으로 이루어지는 하나 또는 그 이상의 접근통제엔트리(ACE)를 가진다. 사용자는 프로그래머, 테스터 등과 같이 그 역할을 지칭하는 이름이 될 수도 있다. 이렇게, 사용자들이나 그룹 또는 각자의 역할에 따라 액세스 마스크(access mask)라고 불리우는 비트 스트링에 접근권한이 적히게 있다. 일반적으로 시스템관리자나 해당 개체의 소유자가 그 개체에 대한 ACL을 생성한다.

한 예로서, 한명은 프로그래머, 다른 한명은 프로그램 테스터, 그리고 세 번째는 시스템 그 자체로 3명의 사용자를 가지는 운영체계를 가정해 보자. 이때, 주어진 프로그램 개체에 대한 ACL은 다음과 같이 될수 있다.

표 1: ACL

권한 / 사용자	Read	Write	Execute
Programer	O	O	O
Tester	O	×	O
System	×	×	O

이렇게 3개의 엔트리를 갖는 ACL에서 이 프로그램 개체를 읽거나, 쓰거나 또는 실행하기 전에 시스템은 접근제어목록을 참조하여 사용자에게 부여된 접근권한에 따라 작업을 허용할 것인지의 여부를 결정하게 된다. [5] 서비스 제공자는 이러한 ACL을 자신의 서버에 저장하여 사용자가 권한을 요청할 때마다 자신의 ACL을 검색하여 권한을 부여하게 되는데 사용자가 많아지거나 컨텐츠에 대한 정보가 많아질수록 ACL의 크기가 커지고 검색하는데 많은 시간을 허비하게 된다. 또한 아이디/패스워드 방식으로 사용자를 인증하기 때문에 악의적인 제 3자에 의해 불법적인 서비스 사용이 용이하다.

본 논문에서는 Web 상에서의 권한 인증을 받을 때 PMI(Privilege Management Infrastructure)에서 사용하는 AC(Attribute Certificate)를 이용한 기존 방식보다 좀 더 강력한 권한 인증을 제안한다.

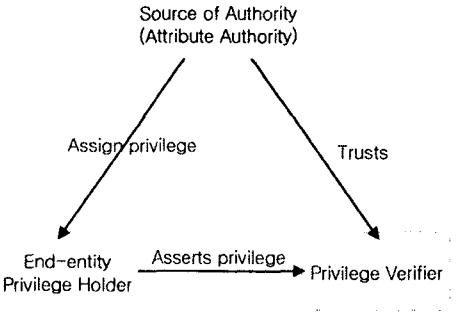
III. PMI

기존 공개키 인증서는 사용자의 신원 확인용으로만 사용되어 지므로 일반적인 환경에서의 접근권한, 역할, 임무, 직위에 대한 정보의 필요성이 존재하게 된다. 이러한 요구로 인하여 인증서와 유사한 AC를 이용하여 사용자의 권한 등을 인증하게 되는데 이를 PMI 라고 한다. PMI는 AC를 발급, 저장, 유통을 제어하는 권한관리 기반구조로서 공개키 기반구조와 유사한 형태를 지니고 있다. AC 정보 제공을 위해서는 기존 신원 확인용 공개키 인증서의 확장 필드를 이용하며 신원 확인용과 별도의 속성 인증서를 발급한다. PMI의 구성요소로는 PKI의 최상위 인증기관(Root CA)와 대응되는 개념으로 최상위 권한 기관인 SOA(Source of Authority), 하위 CA와 대응되는 하위 권한 기관으로 AA(Attribute Authority) 그리고 속성 인증서 발급 서버인 ACS(Attribute Certificate Server)가 있다. PMI의 기본 구성은 그림1과 같이 구성되어 있다.[6]

1) SOA 혹은 AA

SOA는 PMI 체계에서 최상위의 권한을 가진 관리자이다. 모든 사용자와 하위 관리자들에 대해 모든 서비스와 모든 역할을 할당하거나 폐지할

그림 1 PMI 기본 구성도



수 있다. 또한 SOA는 하위 관리자인 AA(Attribute Authority)들을 생성해 각 AA에게 일정 권한을 위임하거나 폐지한다. PAC을 사용해 모든 서비스와 역할의 권한 정보를 직접 관리한다.

2) Privilege Verifier

Privilege Verifier는 사용자의 인증서와 SOA 혹은 AA가 발행한 사용자의 AC를 검증하는 역할을 한다.

3) End-entity Privilege Holder

AC를 사용하며 권한을 인증 받는 최종 사용자이다. [7]

AC는 Version, Holder, Issuer, Signature, serial Number, Validity, Attributes, IssuerUniqueID, extensions 필드로 구성되어 있다.

IV. AC를 이용한 Web Access Control

본 논문에서 제안하는 방식은 기존의 아이디/패스워드 방식의 단순한 인증에서 공개키를 이용한 좀더 강력한 인증을 위해 PMI에서 사용하는 AC를 이용한다.

AC를 이용하여 Web Access Control을 하기 위해서는 AC를 발급하게될 SOA 혹은 AA와 SOA혹은 AA가 발행한 AC에 대한 검증 그리고 사용자의 인증서에 대한 검증을 제공하는 AV 그리고 권한에 맞는 서비스를 제공하는 서비스 제공자 그리고 권한을 사용할 사용자로 구성되어 있다. 다음은 AC 발급절차에 대한 설명이다.

① 먼저 사용자는 서비스 제공자에게 사용자 등록을 하며 어떠한 서비스를 사용할 것인지에 대해 요청을 한다.

② 서비스 제공자는 사용자에게 권한과 그에 따른 비용과 같은 사항을 전달한다.

③ 서비스 제공자는 사용자에게서 받은 정보(role, 권한, 사용자의 인증서 등)을 SOA에게 전달하고 그에 대한 AC를 요청한다.

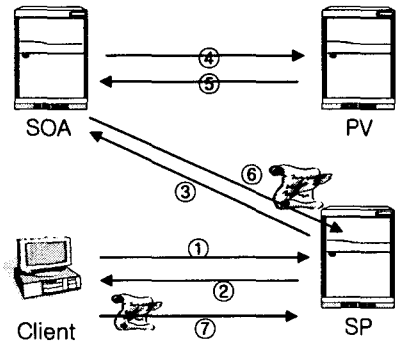
④ SOA는 사용자의 인증서가 유효한지를 AV에게 의뢰한다

⑤ AV는 사용자의 인증서를 가지고 검증을 하여 그 결과 값을 SOA에게 통보한다.

⑥ 사용자의 인증서가 유효하다는 결과를 통보받으면 SOA는 SP가 요청한 권한에 맞는 AC를 발급하여 SP에게 전달한다.

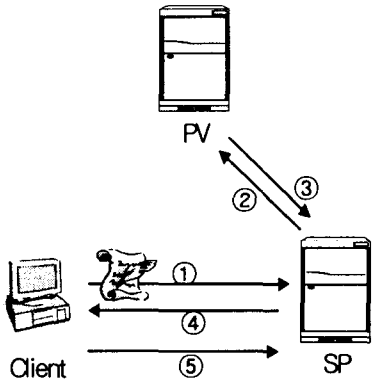
⑦ 최종적으로 사용자는 SP에게 AC를 전달받아서 서비스를 사용할 때 권한에 대한 인증을 얻을 수 있다.

그림 2 AC 발급 절차



본 논문에서 제안한 방식에서는 기존의 방식보다 좀더 강한 인증을 할 수 있다. 공개키를 이용함으로써 사용자에 대한 권한 정보에 사인을 함으로써 악의적인 제 3자가 사용자의 권한을 임의적으로 사용할 수 없게 하며 권한정보 위조, 훼손에 대처할 수 있다.

그림 3 권한 검증 절차



이렇게 발급 받은 AC는 사용자가 서비스에 대한 권한을 부여받기 위한 인증절차 시 필요하게 된다. 그림3은 인증절차에 대한 설명이다.

① 먼저 사용자는 권한을 획득하기 위해 서비스 제공자에게 AC, 인증서, 사인값을 전달한다.

② 서비스 제공자는 사용자가 제공한 AC, 인증서, 사인값 등을 AV에게 전달하여 권한에 대한 검증을 요청한다.

③ AV는 SP로부터 전달받은 데이터를 가지고 사용자에 대한 권한을 검증하여 SP에게 결과값을 전송한다.

④ SP는 결과값에 따른 사용자의 권한을 인정한다.

⑤ 사용자는 SP로부터 전달받은 권한에 맞는 서비스를 사용한다.

이러한 검증과정을 거침으로써 서비스 제공자는 자신의 서버에 ACL 형태로 권한정보를 저장함으로써 저장 정보의 크기나 사용자의 수가 늘어남에 따라 DB가 커지는 부담이 있었으나 사용자의 AC에 권한 정보를 담게 됨으로써 서버측의 DB 부담이 감소하게 된다. 또한 서비스 제공자마다 동일한 AC에 대한 약속을 통하여 권한 정보를 공유함으로써 많은 서비스 제공자 사이의 DB 공유문제를 해결하고 제휴된 어느 서비스 제공자에게나 사용자가 자신의 AC를 제시함으로써 권한을 획득할 수 있다.

V. 결론

인터넷 환경이 발전하고 현실 생활에서의 활동

을 Web 상에서 실현하기 위해 노력들이 많아지고 있다. 이러한 인터넷 환경에서는 각자에 대한 정보가 노출될 가능성 또한 크며 악의적인 제 3 자가 신원을 위장하여 불법적인 일들을 할 수 있다. 인터넷의 발달과 더불어 보안 적인 측면도 크게 부각되게 되었다. 현재도 우리는 Web 상에서 많은 정보들을 얻으며 서비스 제공자가 제공하는 많은 컨텐츠들을 사용하고 있다. 본 논문에서 제시한 AC를 이용한 Web Access Control은 기존의 아이디/패스워드를 사용한 방식보다 나은 서비스를 제공하게 된다. 먼저 서비스에 대한 권한을 제공받을 때 공개키 기반 구조에서 사용하는 인증서를 이용한 사용자 인증을 거치므로 사용자에 대한 좀더 신뢰할 수 있는 서비스를 제공할 수 있다.[7]

또한 사용자가 접속하여 권한을 부여받고자 할 때마다 자신의 DB에 있는 ACL을 검색하여 사용자에게 권한을 부여함으로써 권한 인증 시 자원을 낭비하게 된다.

이러한 자원낭비 뿐만 아니라 각 서비스 제공자는 사용자에 대한 권한을 자신만의 DB에 저장하게 되고 다른 서비스 사용자와의 연계성이 떨어진다. Web Access Control시에 AC를 사용시 각 서비스 사업자들간의 약속을 통하여 동일한 양식의 AC를 사용함으로써 사용자는 하나의 AC로 여러 서비스 제공자들이 제공하는 서비스를 사용할 수 있다. 또한 Service Authentication Information, Access Identity, Charging Identity, Group[, Role, Clearance등을 이용하여 다양한 정보를 제공받을 수 있다.

참고문헌

[1] Stuart McClure and Joel Scambra and George Kurtz, "Hacking Exposed", Osborne/McGraw-Hill, 2001.

[2] James F. Kuros and Keith W. Ross "Computer Networking" , Addison Wesley 2002.

[3] W. Polk and D. Solo " Internet X.509 Public Key Infrastructure Certificate and CRL Profile" RFC 2459, 1999.

[4] Russ Housley and Tim Polk, " Planning for PKI, WILEY, 2001.

sDefinition/ 0, sid14_gci213757,00.html ,Nanci Ellen, Jul 24, 2001.

[5] http://searchsecurity.techtarget.com/

sDefinition/ 0, sid14_gci213757,00.html ,Nanci Ellen, Jul 24, 2001.

[6] Andrew Nash and William Duane and Celia Joseph and Derek Brink "PKI:Implementing and Managing E-security" McGraw-Hill, 2001.

[7] S. Farrell and R. Housely " An Internet Attribute Certificate Profile for Authentication" RFC 3281, 2002.