정보학연구 제5권 제4호 2002년 12월(pp.81-88)
The Journal of Information Technology, Vol.5, No.4

속성인증서와 신분인증서 사이의 바인딩 메카니즘에 관한 연구

박종화*

요 약

신분인증서는 신분확인을 위한 인증서로서 인증기관(Certificate Authority)에서 전자적으로 서명되어 진다. 또 속성인증서는 사용자의 속성정보를 저장 관리하는 인증서로서 속성인증기관(Attribute Certificate Authority)에 의해 전자적으로 서명된다. 웹 상의 많은 응용에서 이들이 사용되기 위해서는 속성인증서를 적절한 신분인증서에 결합하는 바인딩 메카니즘이 필요하다. 이 논문에서 우리는 잘 알려진 바인딩 메카니즘인 선택적 철회 방식[5]과 암호적 바인딩 방식[3]을 분석하고, 위의 방식들이 갖고 있는 문제점을 해결하기 위한 하나의 새로운 방식을 제안한다.

Ⅰ. 서론

최근 인터넷의 급격한 성장에 따라 전자상거래는 기존의 상거래를 보안하거나 대체하면서 급속한 성장을 보이고 있다. 그러나 인터넷은 공개네트워크(Open Network)라는 특성으로 인해 정보의 변조, 위조, 누설 등의 위협에 노출되어 있다. 따라서 인터넷상의 정보보호는 전자상거래의 활성화를 위해 필수적인 요소로 자리잡고 있다. 이러한 정보보호를 제공하기 위해 많은 연구가 진행되고 있으며 특히 최근에는 사용자에 대한 인증 정보를 제공하는 PKI(Public Key Infrastructure)[1]에 대한 연구 및 개발이 활발이 진행되고 있다.

PKI는 사용자에 대한 공개키 소유여부에 대한 인증 정보를 제공하며 정보에 대한 인증(Authentication), 무결성(Integrity), 비밀성(Confidentiality), 부인봉쇄(Non-repudiation) 기능을 제공하며 정보보호 기반구조로 활용되고 있다. 그러나 일반 응용 환경에서는 이와 같은 정보보호 기능뿐만 아니라 사용자에 대한 권한관리를 요구한다. 즉 일반적인 전자상거래에서 사용자가 어떤 물품을 주문했을 때, 서버 시스템에서 물품을 배달할 것인지 결정하는 과정은 물품을 주문한 사용자에 대한 신원확인을 수행하는 인증(Authentication)정보뿐만 아니라 사용자가 주문한 물품의 대금을 지불할 능력이 있는지를 확인하는 인가(Authorization)정보가 매우 중요하다. 따라서, 물품을 구입하기 위해서는 두 가지의 정보, 즉 인증정보와 인가정보가 물품을 배달할 서버 시스템에 제공되어야 한다.

초기에 사용자의 권한과 같은 인가정보는 인증정보와 함께 공개키인증서(Public Key Certificate, PKC)를 통해 제공하려는 연구가 수행되었다. 그러나 공개키에 대한 발급주체가 사용자의 속성을 발급하는 주체와 다르고 공개키의 유효기간과 사용자 속성의 유효기간이 서로 다르기 때문

* 세명대학교 소프트웨어학과 조교수

에 실제 활용되지 못하고 있다. 따라서 최근에 사용자의 임무, 지위, 역할, 접근권한 등과 같은 속성 정보를 별도의 속성인증서(Attribute Certificate, AC)[2,7]에 저장 관리하며 유통하는 속성인증서에 대한 연구가 활발히 진행되고 있다.

이와 같이 인증정보는 공개키인증서를 통해서, 그리고 사용자의 임무, 지위, 역할, 접근권한 등과 같은 속성 정보는 속성인증서를 통해 제공할 때에, 이 들 사이에 적절한 바인딩 메카니즘이 제공되어야한다. 이 논문은 그와 같은 바인딩 메카니즘을 제공하는 것을 그 목적으로 하고 있다.

이 논문에서 우리는 하나의 네트워크 베이스 바인딩 메카니즘을 제공함과 동시에 잘 알려져 있는 암호적 인증서 바인딩 방식(cryptographic certificate-binding methods)[3,4]와 선택적 철회 방식(selective revocation methods)[5]와 우리의 방법을 비교 분석한다.

본 논문의 구성은 다음과 같다. 2장에서 우리의 방법에 관련된 기술들을 설명하고, 3장에서 하나의 도메인 내에서의 접근 권한에 대하여 다루고, 4장에서는 inter-domain에서의 접근 권한에 대하여 설명하며, 5장에서 잘 알려져 있는 방법들과 우리의 방법과 비교하고, 논의한다. 그리고 마지막으로 6장에서 결론을 맺는다.

II. 관련 기술

2.1 공개키 인증서(Public Key Certificate)

공개키 인증서는 인증기관이 발행하는 디지털 정보로, 특정 공개키가 특정 사용자에게 연관되어 있음을 증명한다. 일반적으로 공개키를 신뢰성 있게 사용하기 위해서는 특정 공개키가 특정 사용자에게 정확히 결합되어 있다는 것을 증명할 필요가 있다. 따라서 사용자 신분 정보와 사용자 공개키가 암호학적으로 안전하게 결합될 필요가 있다. 이렇게 하기 위해서는 공개키와 신분 정보를 포함하는 데이터에 대한 무결성, 결합 증거가 제삼의 기관에 의해서 이루어 졌음을 나타내는 인증성, 부인 방지성의 특성을 요구한다. 이를 제공하기 위한 암호학적 메카니즘이 디지털 서명이다. 즉 사용자의 신분 정보와 사용자의 공개키를 포함하는 문서에 대하여 서명이 요구된다.

ITU(International Telecommunication Union)과 ISO(International Organization for Standardization)은 1988년 X.509 표준[1]을 발표하였고, IETF(International Engineering Task Force)에 의해 채택되었다. X.509는 현재 가장 널리 사용되는 공개키 인증서에 대한 데이터 포맷이며, 인증기관(CA : Certification Authority) 사용을 기초로 한다.

X.509 인증서는 공개키를 특정 개인에게 연결하기 위해 사용되며, 공개키가 이 인증서의 소유자(주체)에 연결되어 있음을 확인하기 위하여 인증서 제공자(인증기관)에 의한 디지털 서명이 이루어진다.

2.2 속성 인증서

속성인증서는 사용자의 속성정보를 저장 관리하는 인증서로서 기존 공개키인증서가 사용자의 공개키 정보를 통해 인증 정보를 제공하는 것과는 달리 사용자의 지위, 권한, 임무 등과 같은 다양한 권한 정보를 제공한다.

속성인증서에 대한 표준화 작업은 ANSI[2],

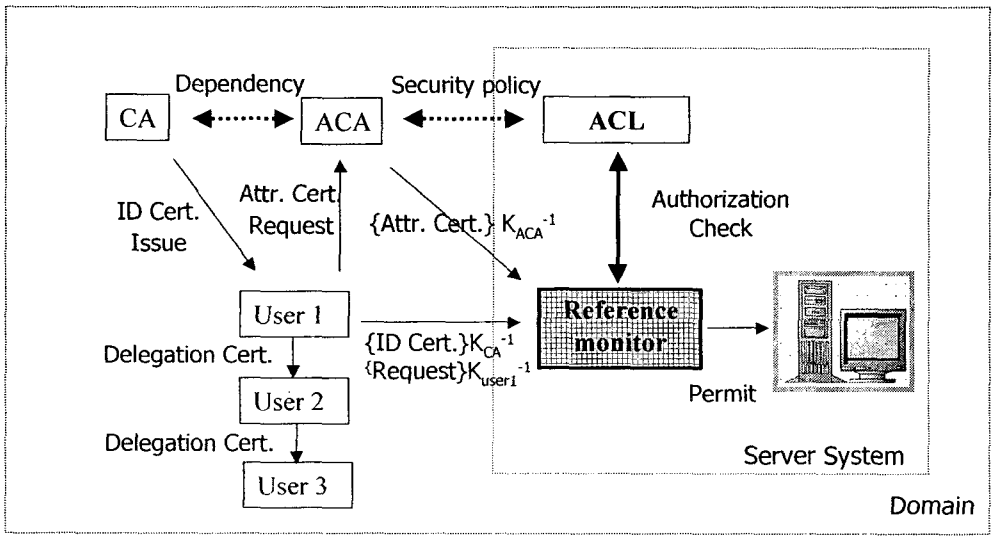
Open Group, ITU-T, IETF 등과 같은 국제 단체에서 진행되고 있다. 이 중 ITU-T는 X.509 Version 4에서 속성인증서와 이를 이용한 권한 관리기반구조인 PMI(Privilege Management Infrastructure)에 대하여 기술하고 있다. 또한 IETF에서는 Attribute Certificate Profile에 대하여 표준을 제정하고 있으며 현재 Version 9 드래프트가 발표되었다. 인터넷상의 전자상거래 정보보호를 위해 일반적으로 복잡한 ITU-T 표준보다 IETF의 RFC나 드래프트가 활용되고 있는 것이 현실이다.

III. 도메인 내에서의 접근 권한

(그림 1)은 PKI 인증서에 의한 접근권한의 전형적인 예를 보이고 있다. 여기서 접근권한은 User1이 자신의 개인키로 서명한 접근요청서를 자신이 접근하고자 하는 객체를 가진 서버에 제출할 것을 요구한다. 또한 User1은 CA(Certificate Authority)에 의해서 서명된 자신의 신분정보를 갖고 있는 신분인증서(Identity Certificate)를 위의 요청서와 함께 제출함과 동시에 ACA(Attribute Certificate Authority)에게 자신의 속성인증서를 서버에게 직접 보낼 것을 요청한다.

객체에 대한 접근은 서버에서 유지되는 ACL (Access Control List)에 의해서 관리된다. 일반적으로 신분인증서는 사용자의 이름과 개인키에 의해 서명된 요청서의 그 개인키와 조화된 공개키와 연관된다. 속성인증서는 사용자가 어느 단체에 소속된 회원임을 정의하며, 사용자가 그 단체에 연관되었음을 나타낸다. 신분인증서는 CA에 의해서 부여되고, 속성인증서는 ACA에 의해서 부여된다. 이때 ACA는 속성인증서를 서버에게 부여하기 전에 CA를 통해 사용자의 신분인증서가 정당한 것인지를 확인한다.

접근요청서를 받은 서버는 그 요청서에 대하여 그 사용자의 신분인증서와 속성인증서의 정



(그림 1) 속성인증서를 이용한 접근권한

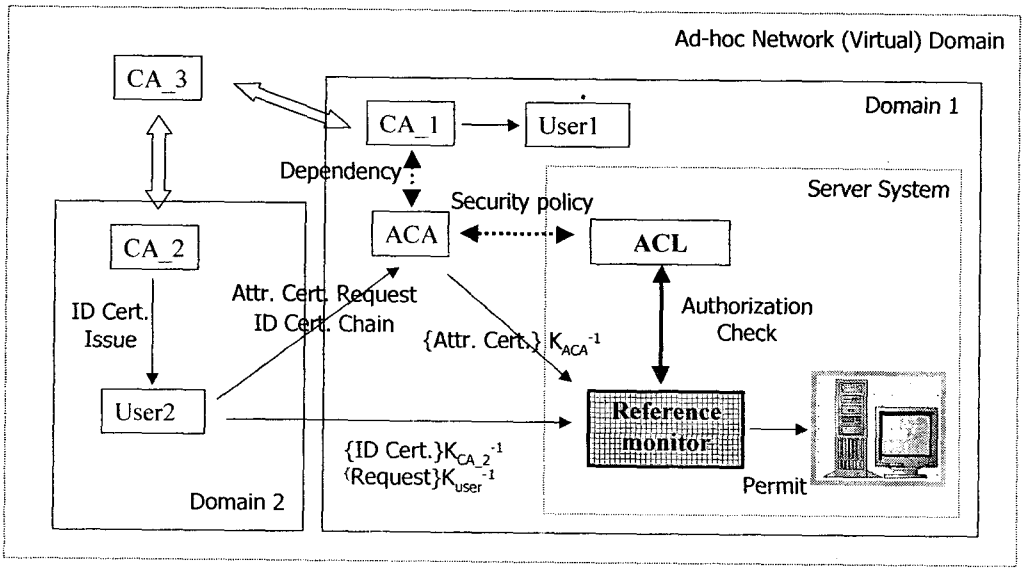
당성을 확인하고, 또 사용자의 그 요청서에 표시된 접근하고자 하는 객체의 ACL에서 사용자가 요청한 특권과 ACL이 허가한 그룹과 연관되는지를 확인하는 것에 의해 권한을 부여한다. 모든 확인 과정을 끝낸 후에 서버는 객체에 대한 사용자의 요청을 수행한다. 이 전형적인 프로토콜로부터 사용자의 속성인증서가 신분인증서에 바인딩 되어지는 것을 알 수 있다. 그것은 접근요청이 서버에 의해서 접근의 특권(속성인증서)이 등록된 사용자(신분인증서)에게 분배됐다고 확인될 때만 승인되어지기 때문이다.

속성인증서를 통해 분배된 특권은 선택적 분배의 형태로 나타난다. 만약 접근에 관한 특권이 위임 인증서를 통해 추이적으로 다른 사용자에게 분배되어 졌다면, 이 위임 인증서가 그 사용자에 의해서 제공되어야 하며, 이 때 서버는 ACL를 통해 그 사용자의 이름이 허가된 그룹에 속한다는 것을 보장하는 것에 의해 정당함을 입증한다.

Ⅳ. 도메인 간의 접근권한

(그림 1)에서 CA와 ACA가 서로 다른 인증서를 부여하는 기능을 갖는 것을 보였다. 이 두 CA와 ACA가 하나의 서버에 존재할 수 있다. 하나의 서버에 두 CA와 ACA를 두고 관리하는 것이 인증 절차를 단순하게 할 수 있다. 그러나, 신분인증기관과 속성인증기관을 분리해서 운영하는 것이 여러 면에서 이점이 있음을 [6]에서 보이고 있다. 그 이점들은 다음과 같다.

(1)인증에 책임이 있는 인증기관과 권한을 부여하는 인증기관 사이의 독립성 유지 (2) 비교적 사용기간이 긴 신분인증서에 영향 없이 속성인증서를 회수하는 것에 의해서 특권 할당을 쉽게 바꿀 수 있는 능력. 특히 여러 도메인 사이에서 자원을 공유하는 도메인간의 네트워크에서는 신분인증기관과 속성인증기관의 분리가 필요하다.



(그림 2) PKI 인증서를 갖는 도메인 간의 접근권한

(그림 2)는 두 개의 자치적인 도메인을 포함하는 네트워크를 보이고 있다. 하나의 자치적인 도메인은 독립적인 인증과 도메인 내의 사용자 등록 및 신분인증서 부여 등을 수행하는 도메인 자체 CA를 소유한다. 자치적인 도메인은 또한 도메인 간의 네트워크의 관리가 자치 도메인 내의 사용자의 등록에 관여하지 않음과 다른 자치 도메인 내의 사용자 등록에도 관여하지 않음을 함축한다. 따라서 자치 도메인들은 독립적으로 그리고 자치적으로 관리되므로, 도메인 간의 네트워크 관리는 자치 도메인 내에 누가 등록된 사용자인지 조차도 알지 못한다.

(그림 2)에서 보이는 네트워크는 새로운 가상의 도메인을 구성하는데, 이 새로운 도메인은 도메인 1과 도메인 2의 사용자와 자원들(즉, 서버들과 객체들)을 포함한다. 예를 들어, 도메인 1은 User1을 그리고 도메인 2는 User2를 등록하고 이들이 구성원으로 전체 가상 도메인을 구성한다. 이 가상 도메인 네트워크에서의 인증은 각 도메인의 인증기관인 CA_1과 CA_2에 의해서 부여하는 신분인증서에 기초하는데, 이 신분인증서는 각 도메인의 인증 정책에 기초한다. 자치적인 도메인은 다른 지역의 사용자 등록과 인증 정책을 지원하므로 지리적으로 멀리 떨어져 있을 수 있으며, 가상 도메인의 네트워크는 사용자 등록과 지역 인증 목적을 위하여 각 자치 도메인 구성원을 믿어야만 한다.

가상 도메인 네트워크에서 다른 도메인의 자원에 대한 접근은 인증서 체인을 통해 발급 받은 신분인증서와 접근하고자 하는 도메인의 ACA으로부터 서버로의 속성인증서 발급 요청 그리고 개인키에 의해 사인된 요청서(Request)를 접근하고자 하는 도메인의 서버에게 제출함으로서 이루어진다. 예를 들면, (그림 2)에서 도메인2의 User2가 도메인1의 서버시스템에 접근하고자 할 때에, 우선 User2는 도메인1의 CA_1으로부터 신분인증서를 인증서체인(CA_2, CA_3, CA_1)을 통해 받는다. 그리고 User2는 그 신분인증서를 이용하여 도메인1의 ACA에게 속성인증서를 발급하여 도메인2의 서버에게 보낼 것을 요청함과 동시에 CA_1으로 부터의 신분인증서와 자신의 개인키로 사인한 접근요청서를 도메인2의 서버에게 보낸다.

V. 신분인증서와 속성인증서의 바인딩에의 적용

이 절에서, 우리는 신분인증서와 속성인증서와의 바인딩에 대한 여러 가지 방식들을 비교, 검토한다. 그 방식들은 선택적 철회 방식[5]와 암호의 바인딩 방식[3] 그리고 이 논문에서 제안한 방법 등이다. 여기서 우리는 각 방식의 장단점 등을 비교 분석하고, 그들 가온데서 우리가 제안한 방식에 대하여 상대적인 장점이 무엇인지 설명한다.

5.1 선택적 철회 방식

선택적 철회 방식은 권한이 없는 특권유지 문제에 대한 해답으로 Himanshu와 Virgil[5]이 제안하였다. 이 선택적 철회 방식을 지원하기 위해서는 인증서와 연관된 서버들 사이에 동적인 링크의 유지가 요구되는 데, 이 링크들은 분산 시스템에서 선택적 철회를 적용하기 위해 서버들간에 적절한 메시지를 보내기 위해 사용되어진다. 이 방식에서 각각 인증서와 연관된 서버들은 시간이 기록된 기본적인 사건들(즉, 보낸

메시지와 받은 메시지)의 순차적인 기록들을 유지한다. 선택적 철회의 적용은 이 기본적인 사건들에 기초한 보내는 메시지를 포함한다. 하나의 ACA는 사용자에게 속성인증서를 발급할 때는 언제든지 그 사용자의 신분인증서를 발급했던 CA에게 속성인증서 분배 사실을 메시지로 보내야한다. 그 때 이 메시지는 CA의 기록으로 유지될 것이다. 또 CA가 그 사용자의 신분 인증서를 철회하고자 할 때 CA는 그 철회에 대하여 ACA에게 메시지를 보내어 ACA로 하여금 그 사용자의 속성인증서를 선택적으로 철회 할 수 있게 한다. 이 방식은 인증서들의 분배와 철회에 대하여 인증서와 연관된 서버들 간에 동적인 링크들의 유지를 요구하는데, 이 방식은 추가적인 통신비용의 원인이 될 것이다.

5.2 암호의 바인딩 방식

선택적 철회의 다른 방식으로, 암호적 바인딩 방식이 Park과 Sandhu[3]에 의해서 제안되었다. 이 방식은 강결합(strong binding)에 기초하는데, 강결합은 하나의 유일한 신분인증서가 속성인증서에 의해 분배된 접근 특권에 묶여진다는 것이다. 그러므로 만약 그 신분인증서가 철회되었다면, 사용자는 다른 신분인증서를 통해 접근하는 일이 발생하지 않을 것이다. 즉 권한없는 특권유지 문제가 제거되어진다.

이 방식에 의한 결합의 적용에서는 모든 접근 요청에 대하여 서버는 신분 인증서와 접근제어 인증서가 미리 정의된 것과 맞는지를 확인하여야한다. 즉, 서버에서 매 접근 요청에 대해 그의 신분인증서와 속성인증서의 정당성을 확인해야만 한다. 따라서 이 방식은 모든 접근 요청에 대하여 추가적인 computation을 요구하며, 이것이 권한 부여의 추가적인 부담이 될 것이다.

5.3 우리의 제안된 방식

우리가 위에서 언급한 두 가지 방식, 선택적 철회 방식과 암호적 바인딩 방식을 검토해 볼 때, 선택적 철회 방식은 각 인증서의 서버들, CA와 ACA 사이에 추가의 동적인 링크를 요구하고 있어, 이 방식은 추가적인 통신비용에 대한 부담을 갖게 한다. 또한 암호적 바인딩 방식은 신분 인증서와 속성 인증서 간의 결합이 정당한 것인지를 분석하기 위한 추가적인 처리와 계산이 요구되어 진다.

우리의 제안된 방식에서는 암호적 바인딩 방식에서 발견되는 인증서들 간의 조회에 따른 어려움은 일어나지 않게 된다. 그 이유는 하나의 속성 인증서는 오직 하나의 신분 인증서에 의해서만 참조되기 때문이다. 그리고 이 신분 인증서는 참조된 속성 인증서와 함께 자료를 갖고있는 서버에 제출될 것이다. 또한 이 방식은 권한없는 특권 유지 문제를 제거할 수 있는데, 그 이유는 속성 인증서에 의해서 분배된 접근 특권이 유일한 신분 인증서에 만 묶여 있기 때문이다. 따라서 만약에 그 신분 인증서가 철회된다면 사용자가 다른 신분 인증서를 이용하여 자료를 갖고 있는 그 서버에 대한 접근은 사실상 어렵게 되는 것이다.

VI. 결론

이 논문에서, 우리는 PKI 인증서를 이용한 접근 권한이 인증서 간의 상호 의존성 유지에 영향을 받음을 보았고, 의존성이 유지되지 않을 때는 접근이 허가되어서는 안 된다는 원칙에서, 기존에 제안된 방식인 선택적 철회 방식과 암호

결합 방식의 문제점을 제시하였다. 그 문제점들은 선택적 철회 방식에서는 각 인증서의 서버들 즉 CA와 ACA 사이에 추가의 동적인 링크의 요구가, 그리고 암호 결합 방식에서는 신분 인증서와 속성 인증서 간의 결합이 정당한 것인지를 분석하기 위한 추가적인 처리와 계산 등이다. 우리는 이 논문에서 인증서간의 의존성 유지를 위한 네트워크에 기반 한 하나의 해결책을 제시하였고, 이 해결책이 선택적 철회 방식이나 암호 결합 방식보다 통신비용의 측면에서나 또는 추가적인 처리 계산등에서 더 효과적임을 보였다.

참고문헌

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

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

[3] Joon S. Park and Ravi Sandhu,"Binding Identities and Attributes Using Digitally Signed Certificates", 16th Annual Computer Security Applications Conference (ACSAC), New Orleans, Louisiana, December 11-15, 2000.

[4] Joon S. Park and Ravi Sandhu, "Smart Certificate : Extending X.509 for Secure Attribute Services on the Web", NISSC, 1999.

[5] Himanshu Khurana and Virgil D. Gligor, "Enforcing Dependencies between PKI certificates in ad-hoc Networks, IEEE International Conference on Telecommunications, Buchartest, Romania, pp. 293-298, June 2001.

[6] J. Lim, M. Nystrom, "Atribute Certification : On enabling technology for delegation and role-based controls in distributed environments", Proceedings Fourth ACM Workshop on Role-Based Access Control, 1999.

[7] Ravi Sandhu, Edward Coyne, Hal Feinstein and Charles Youman, "Role-Based Access Control Models", IEEE Computer, Volume 29, Number 2, February 1996.

A Method Enforcing Dependencies between ID Certificates and Attribute Certificates in Inter-domain

Chong-Hwa, Park*

Abstract

An ID certificate is digitally signed by a certificate authority for authentication and a attribute certificate is digitally signed by an attribute certificate authority for authorization. In many applications in web, there should be a mechanism to bind attributes to proper identities. So we analyzed some known binding methods, selective revocation methods and cryptographic binding methods and we proposed the new mechanism in order to solve their problems.

* Dept. of software, Semyung University