PKI 기반에서 X.509 인증서를 사용한 권한위임

유정각*, 이건희*, 이상하**, 김동규*

*아주대학교 정보통신공학과, **동서울대 정보통신공학과

Delegation using X.509 Certificates in PKI Based

Jeong-Gak Lyu*, Gun-Hee Lee*, **Sang-Ha Yi, *Dong-Kyoo Kim

*Department of Information Communication Engineering, Ajou Univ.
**Department of Information Communication Engineering, Dong Seoul College

요 약

분산 시스템에서 사용자가 시스템에 로그인 상태에서 자신의 시스템에 존재하지 않는 자원을 이용하기 위한 방안으로 권한위임이 필수적이다. 이러한 권한위임은 다양하게 요구되는 정보보호 응용 서비스의 가용성을 증대시킨다. 본 논문에서는 권한위임을 처리하기 위해서 권한위임 인증서를 생성하여 안전하게 인증서를 중개자에게 전달해야한다. 개시자와 중개자 최종 목적지까지 다단계 권한위임이 발생하는 연결고리에서 PKI 기반 X.509의 공개키를 이용한 효율적이고 추적 및 검증이 가능한 프로토콜을 제안한다.

I. 서론

분산 시스템에서 사용자가 시스템에 로그인한 상태에서 자신의 시스템 내에 위치하지 않는 작업을 권한위임으로 처리하는 것이 필수적이다. 또한 권한위임은 다양하게 요구되는 정보보호 응용 서비스의 가용성을 증대시킨다[6]. 권한위임은 분산 환경에서 한 개시자(delegator)가 다른 중개자(delegate)에게 자신의 편에서 행동하도록 권한부여를 하는 일련의 과정이다. 최종 목적지(final) 사용자는 권한위임을 부여받은 권한인가를 처리한다.

개시자A에서 중개자B로 권한위임은 다음과 같이 $A \Rightarrow B$ 표현한다. 권한위임 경로는 권한위임에 참여하고 있는 사용자의 순서로 개시자로부터 목적지까지 순차적 시간을 의미한다. 다단계 권한위임은 위임을 받은 중간 중개자 다시 다른 중개자에게 권한위임을 주는 관계를 말한다. 권한위임 개시자는 자신의 제한된 권리만 포함한 권한위임 인증서(*DC : delegation certificate*)을 생성하여 중개자에게 넘겨주어 접근권한을 처리하도록 한다. 권한위임 인증서는 개시자의 ID, 권한속성 $Pr_A(B)$을 포함하여 중개자에게 허용하도록 한다. 예를 들어 권한위임 유효기간, 중개자의 ID, 타임스탬프(TS : Timestamp)를 포함한다.

본 논문에서 다단계 권한위임이 요구되는 분산 응용 환경에서 PKI(Public Key Infrastructure) 기반의 계층적 권한위임 인증서의 개념을 도입한다. 이 개념은 개시자로부터 권한위임을 시작하여 중개자에게 안전한 권한부여를 보장하는 것이다. 권한위임의 감사 및 접근통제 신뢰성은 X.509 인증서의 공개키 기반 방법에 의해서 지원이 된다. 이 방법에서 개시자는 중개자의 고의적 수정이나 공격자의 위장 공격을 방지한다. 본 논문에서 다단계 권한위임이 발생할 시 추적이 가능하고, 사용된 권한위임 경로를 따라 목적지는 모든 중개자가 부여받은 권한을 검증할 수 있다.

본 논문의 구성은 2장에서 권한위임에 관련된 연구를 살펴보고, 3장에서 접근방법의 동기를 제시하고, 4장에서 X.509을 이용한 새로운 권한위임 프로토콜 제안하고, 5장에서 결론을 맺는다.

II. 관련연구

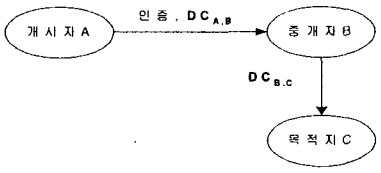
권한위임을 실현하는 다양한 방법들이 연구되어지고 있다. 이들 중에 키 기반과 ID 기반의 대표적인 사례를 보면 다음과 같다. 키 기반 방법의 권한위임 메커니즘은 DDSA(Digital Distributed System Security Architecture)에서 개발되었다[5]. 중개자에서 생성한 비대칭 암호화 키쌍을 이용한다. ECMA 표준는 PAC(Privilege Attribute Certificate)을 보호하기 위해 무결성 키쌍(contol

value, protection value)으로 PAC의 안전성을 보장한다. Neuman은 Kerbros V5을 위한 제한된 프록시 메커니즘을 사용하도록 설계하였다[1]. 사용자는 권한위임 프록시로부터 전달 프록시를 구별하여 사용한다. 프록시는 권한위임 인증서이고, 운반 프록시는 권한위임 키를 사용하고 이를 프록시 키라 한다.

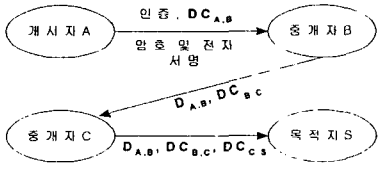
ID 기반 방법으로 Karger는 전자서명대신 일회성 키워드를 사용하여 프록시 로그인 메커니즘을 제안하였다[2]. 일회성 키워드는 사용자의 ID와 관련이 있고 중앙 인증서버에 의해서 제공이 된다. Sollin의 다단계 인증 메커니즘은 전자서명과 nested 토큰을 사용하였다[3]. Varadharajan은 Karger와 Sollin의 메커니즘 방법을 일반화하였다. 이들의 권한위임 방법은 연결고리(chained) 및 nested 토큰을 사용하고, 단순 연결고리 인증서를 가진 문제점을 조사하였다. Neuman의 프록시 권한위임은 ID 기반이고 대부분 ID 기반의 권한위임 방법은 추적이 가능하다. Neuman은 위의 두 가지 조합한 메커니즘을 사용하였다[3].

Ⅲ. 접근방법의 동기

그림1은 권한위임 관계의 개요를 보여주고 있다. 권한위임 개시자A는 위임 중개자B를 선택한다. 개시자는 중재자B를 인증하고, 자신이 서명한 권한위임 인증서 $DC_{A,B}$을 중개자에게 넘겨준다. 단지, 키는 비밀성 보장을 위해 A가 권한위임 키 Kpu_B(B의 공개키)로 암호화하여 B로 전송한다. 그래서 B는 A편에서 행동하고 최종 목적지 S로 접근을 원한다. B는 자신이 전자서명한 권한위임 인증서 $DC_{A,B}$을 보여주고, 부여받은 접근권한을 검증한다.



[그림 1] 권한위임관계



[그림 2]다단계권한위임

그림2은 다단계 권한위임 관계를 보여주고 있다. 명확성을 위해서 인증과 접근권한의 과정을 생략한다. 여기서 세 개의 다른 권한위임 인증서 $DC_{A,B}$, $DC_{B,C}$, $DC_{C,S}$를 가지고 있고, 이들 사이에 상호관계 설정이 필요하다. 이들 중에 한쪽이 다른 권한위임 경로를 구성하기 위해서 공격자에 의해서 대치되거나 위장될 수 있다. A는 B를 신뢰하지만, B는 C를 신뢰하지 못한다. A는 B에게 권한위임을 위해서 전자서명한 권한위임 인증서를 $DC_{A,B}$ 넘겨준다. A의 편에서 행동하는 B는 A의 중개자로서 C에게 권한위임을 하지 못할 것이다. 그래서 권한위임 경로① $A \Rightarrow B \Rightarrow C$는 정당하지 않다. 또 다른 사용자 A는 양쪽 B와 C를 신뢰한다. 그래서 권한위임 경로② $A \Rightarrow B \Rightarrow C$는 정당하다. 만약 공격자가 권한위임 경로 $A \Rightarrow B$로부터 권한위임 인증서 $DC_{A,B}$을 획득한다고 한다면, 안전한 경로②에 해당한다고 하지만, 경로①의 경우 안전하지 못한 결과를 가지게 된다. 다음에 이러한 문제점을 대처하기 위한 다양한 해결책이 존재한다.

1. Varaharajan는 nested 인증서 사용을 제안하였다[7]. 이 인증서 $DC_{A,B}$는 후속 토큰 $DC_{B,C}$를 포함하고 있다는 것을 의미한다. 인증서 $DC_{B,C}$는 B에 의해서 전자서명되고, 그래서 공격자는 위조된 상태로 인증서 $DC_{A,B}$을 대치할 수 없다. 이 해결책은 권한위임 인증서의 크기가 권한위임 경로에 비례하여 증가하는 단점을 가진다.

2. Christianson은 두 인증서를 묶은 전자서명 방법 사용하고, 전체 인증서를 대신하여 후속 인증서에서 단지 전자서명 한 것을 포함한다[4]. 즉, A에 의한 인증서 $DC_{A,B}$의 전자서명은 후속 인증서 $DC_{B,C}$의 일부분이 된다는 것을 의미한다.

3. Neuman은 두 인증서를 묶기 위한 방안으로 권한위임 키를 사용하는 것을 제안하였다[1]. 인증서 $DC_{B,C}$는 개인 권한위임 키로 전자서명이 되고, 그 자체는 대칭키 또는 해당하는 공개 권한위임 키 비대칭 암호 방법으로 선행 인증서 $DC_{A,B}$에 포함되어진다.

이제까지 살펴본 바로 개시자A는 중개자B를 위해 권한위임 인증서 $DC_{A,B}$를 생성하고, 중개자B는 C를 위해 권한위임 인증서 $DC_{B,C}$를 생성한다. 권한위임 인증서 $DC_{A,B}$, $DC_{B,C}$, $DC_{C,S}$은 PKI 기반 X.509 인증서의 비대칭 암호화 방법을 사용하여 계층적인 인증서 기반이 생성된다. 새로운 아이디어는 계층적인 권한위임 인증서를 생성함으로

서 간단하게 연결고리 인증서 문제를 해결한다. 권한위임 키쌍(Kpu_A:개인키, Kpu_A:공개키)는 다음의 관점에서 특징을 가지고 있다.

1. 공개 권한위임 키는 수신자 자신임을 검증하고 비밀성 유지를 위한 인증 공개키로 사용한다.
2. 개인 권한위임 키는 권한위임 인증서의 송신자를 밝히는 전자서명 키로 사용한다.
3. 다단계 권한위임에서 권한위임 키쌍은 계층적으로 구성한다.

이 해결책은 Christianson 및 Neuman의 아이디어의 조합으로 볼 수 있지만, 권한위임 개인키는 전자서명 인수로 사용되어 진다. 이 방법은 생성하는 권한위임 키 및 권한위임 인증서의 단순성을 가지는 장점을 가진다.

계층적 키 생성은 시스템에 많은 사용자를 가지고 있다면, 이들 모두가 동일한 인증당국으로부터 자체로 인증된 공개키를 구하는 것이 아니라 PKI 기반의 공개 인증 디렉토리부터 X.509에서 계층적 순서 당국으로부터 그들의 공개키를 구할 수 있다. 공개키의 연산은 PKI 인증서 구조에서 여러 개의 노드를 따라 역순으로 행해야 한다.

만약 사용자가 이미 임의의 인증 공개키를 알고 있다면, 키 연산은 자신을 위해 쉽게 구할 수 있다. 다단계 권한위임에서 권한위임 인증서는 동일한 방법으로 전자서명 된다. PKI의 계층구조에서 X.509 인증서로부터 권한위임 인증서 키는 획득할 수 있다.

Ⅳ. 새로운 권한위임 프로토콜

시스템에서 모든 사용자는 PKI 계층구조를 가지는 신뢰성 있는 인증 당국으로부터 X.509 인증서를 가진다. 사용자는 자신의 키쌍 (Kpr_A, Kpu_A)은 X.509인증서에 의해서 구해진다. 이들은 신뢰성 있는 키 교환, 인증 및 비밀성을 위해 사용한다. 즉, 개시자A는 권한위임의 요청으로 권한위임 인증서를 안전하게 중개자 및 목적지에 전달하고, 중개자의 고의적인 위조나 수정을 방지할 수 있다. 권한위임 인증서는 비대칭 권한위임 키 또는 사용자 신분 두 가지의 조합에 기반을 두고 있다.

4.1 X.509 키 기반 방법

권한위임에 의한 순서는 다음과 같이 진행이 된다. 권한위임 경로는 $A \Rightarrow B \Rightarrow C \Rightarrow S$로 가정한다면, 3가지 다른 단계로 분할이 된다. 여기서 표기의 편의상 각각의 개시자A, 중재자B, C, 목적지S 사용자 및 프로토콜에 대해서 다음과 같이 기술한다.

- $E_{Kpr_A}[m]$: 사용자A가 전자서명을 제공하기 위해 메시지 (m)을 A의 개인키 Kpr_A로 전자서명
- $E_{Kpu_B}\{m\}$: 사용자A가 메시지 비밀성을 위해서 메시지 (m)을 B의 공개키 Kpu_B로 암호화
- $k_{A,B}$: 사용자A가 생성한 랜덤넘버(random number)에 해당하는 세션키
- $Pr_A(B)$: $k_{A,B}(A, B, D_t, data)$

  사용자A가 요청한 접근 권한위임 제약속성으로 세션키 $k_{A,B}$로 암호화된 값
- D_t : 권한위임 유효기간
- $cert_A$: 사용자A의 공개키 Kpu_A을 포함한 X.509 인증서
- $h(m)$: 메시지 (m)의 해쉬함수 값

1. $A \Rightarrow B$: $cert_A$, $E_{Kpu_B}\{DC_{A,B}\}$, $Sign_A$

개시자A는 X.509 인증서 $cert_A$을 취득한 상태에서, $cert_A$로부터 개시자A는 권한위임 키쌍 (Kpr_A , Kpu_A)을 획득한다. 또한 A는 권한위임 인증서 $DC_{A,B} := \{A, k_{A,B}, Pr_A(B), TS_{A,B}\}$을 생성한다. A의 권한위임 개인키 Kpr_A는 권한위임 인증서 $DC_{A,B}$의 전자서명용으로 사용하여 다음과 같이 전자서명을 한다. $Sign_A = E_{Kpr_A}[h(DC_{A,B})]$는 부인방지도 함께 이루어진다. 권한위임 인증서 $DC_{A,B}$는 B의 공개키로 비밀성을 위해 암호화하여 $E_{Kpu_B}\{DT_{A,B}\}$ 전송한다.

신뢰성은 인증 방법과 더불어 개시자A의 개인키 Kpr_A을 가지고 있다는 것을 보여줌으로 증명된다. 개시자A, 중개자B는 인증시 또는 권한위임 토큰을 전달하는 과정에서 사용자는 신뢰성 있는 대칭 암호화 세션키 $k_{A,B} := k_A \equiv k_B$를 획득하게 된다.

2. $B \Rightarrow C$: $cert_B$, $E_{Kpu_C}\{DT_{B,C}\}$, $Sign_B$

중개자B는 X.509 인증서 $cert_B$을 취득한 상태에서, $cert_B$로부터 중재자B는 권한위임 키쌍 (Kpr_B , Kpu_B)을 획득한다. B는 권한위임 인증서 $DC_{B,C} := \{B, k_{B,C}, Pr_B(C), TS_{B,C}\}$을 생성하고, B의 권한위임 개인키 Kpr_B로 $Sign_B = E_{Kpr_B}$

$[h(DC_{B,C}), Sign_A]$전자서명 한다. B와 C는 신뢰성 있는 키교환 프로토콜을 사용하여 상호인증을 한다. B는 권한위임 인증서 $DC_{B,C}$를 C의 공개키로 암호화하여 $E_{Kpu_C}\{DC_{B,C}\}$ 전송한다.

신뢰성은 인증 방법과 더불어 중개자B의 개인키 Kpr_B을 가지고 있다는 것을 보여줌으로 증명된다. 중개자B, C는 인증시 또는 권한위임 토큰을 전달하는 과정에서 사용자는 신뢰성 있는 대칭 암호화 세션키 $k_{B,C} := k_B \equiv k_C$를 획득하게 된다.

3. $C \Rightarrow S$: $cert_C$, $E_{Kpu_C}\{DC_{C,S}\ or\ m\}$, $Sign_C$

중개자C는 X.509 인증서 $cert_C$을 취득한 상태에서, $cert_C$로부터 중재자C는 권한위임 키쌍 (Kpr_C, Kpu_C)을 획득한다. C는 권한위임 인증서 $DC_{C,S} := \{C, k_{C,S}, Pr_C(S), TS_{C,S}\}$을 생성하고, C의 권한위임 개인키 Kpr_C로 $Sign_C = E_{Kpr_C}[h(DC_{C,S}), Sign_C]$전자서명 한다. C와 S는 신뢰성 있는 키교환 프로토콜을 사용하여 상호인증을 한다. C는 권한위임 인증서 $DC_{C,S}$를 S의 공개키로 암호화하여 $E_{Kpu_S}\{DC_{C,S}\}$ 전송한다. 또는 중개자C는 메시지 $m = \{(ID_A), (DC_{A,B}), (ID_B), (DC_{B,C})\}$를 최종 목적지 S로 전송할 수도 있다. 신뢰성은 인증 방법과 더불어 중개자C의 개인키 Kpr_C을 가지고 있다는 것을 S에게 보여줌으로 증명된다. 중개자C와 목적지S는 인증시 또는 권한위임 인증서를 전달하는 과정에서 사용자는 신뢰성 있는 대칭 암호화 세션키 $k_{C,S} := k_C \equiv k_S$를 획득하게 된다.

권한위임 키쌍 (Kpr_A, Kpu_A), (Kpr_B, Kpu_B), (Kpr_C, Kpu_C), (Kpr_S, Kpu_S)의 연산은 PKI의 계층구조에 따른 키 생성의 아이디어에 기반 한다. 이 키쌍에서 개인키는 사용자의 이름을 나타낼 수도 있고, 전자서명 및 부인방지를 한다.

권한위임 인증서 $DC_{A,B}$, $DC_{B,C}$ 및 $DC_{C,S}$는 각각의 공개키에 의해서 S로 전달하는 간단한 연결고리를 형성하여 전송한다. 매 단계에서 두 권한위임 인증서를 함께 묶어서, 다음 단계의 전자서명 매개변수로 사용한다. 그래서 공격자는 결코 권한위임 인증서 $DC_{A,B}$, $DC_{B,C}$ 및 $DC_{C,S}$을 변경이 불가능하고 또 다른 권한위임 경로를 구성할 수 없다. 본 논문에서 정보보호의 안전성은 PKI의 X.509 인증서의 전자서명 방법 및 인증키 교환 프로토콜에 의존한다. 또한 ID도 함께 사용하여 권한위임 연결고리의 경로는 추적이 가능하다.

V. 결론

분산 시스템에서 권한위임 발생시 개시자, 중개자 및 목적지 사이에 권한위임 인증서를 안전하게 전달해야 한다. 각각의 사용자는 PKI 기반에서 X.509 인증서를 가지고 있다는 가정하에 이루어진다. 본 논문에서는 공격자의 권한위임 인증서의 위조나 변경을 방지하고, 중개자의 고의적인 수정을 방지하는 프로토콜을 제안하였다. 또한 권한위임 경로 상에 목적지는 모든 중개자를 권한을 검증이 가능하다. 제안한 프로토콜은 사용자의 ID 및 키 기반을 통시에 처리 가능함으로 추적이 가능한 프로토콜을 제시하였다. 향후 PMI(Privilege Management Infrastructure) AC(Attribute Certificate)의 연관성을 고려한 연구가 필요하다.

참고문헌

[1] B. Clifford Neuman, "Proxy-Based Authorization and Accounting for Distributed System," In Proceedings of the 13th International Conference on Distributed Computing Systems, pp.283-291, 1993.

[2] Jonathan T. Trostle, B. clifford Neuman, "A Flexible Distributed Authorization Protocol," Internet Society 1996 Symposium on Network and Distributed System Security, pp.43-52, May 1996.

[3] Karen R. Sollins, "Cascaded Authentication," In Proceedings of th 1988 IEEE Symposium of Research in Security and Privacy, pp.156-163. Apr. 1988.

[4] M. R. Low, B. Christianson, "Self Authenticating Proxies," The Computer Journal Vol.37, No.5 pp.422-428, 1994.

[5] M. Gasser and E. McDermott, "An Architecture for Practical Delegation in a Distributed System," IEEE Symposium on Security and Privacy, pp.20-30, 1990.

[6] Tuomas Aura, "Distributed access-rights management with delegation certificates," In Secure Internet Programming-Security Issues for Distributed and Mobile Objects, volume 1603 of LNCS, pp.211-235. 1999.

[7] V. Varadharajan, P. Allen, S. Black, "An Analysis of the Proxy Problem in Distributed System," Proceeding of the 1991 IEEE Symposium on Research in Security and Privacy, pp.255-275, 1991.