ID 기반 자기 위임 기법과 응용

이정연*, 천정희*, 조상래**, 진승헌**

*한국정보통신대학원대학교 공학부

**한국전자통신연구원 정보보호연구본부

ID-based Self-Delegation and its Applications

Jung-Yeun Lee*, Jung Hee Cheon*, Sangrae Cho**, Seung-hun Jin**

*Engineering School, Information and Communications Univ.(ICU)

**Electronics and Telecommunications Research Institute(ETRI)

요 약

자기 위임 기법은 사용자의 공인된 하나의 키 쌍을 이용하여 특정 기간이나 목적을 위한 세션키를 생성하여 사용하는 기법이다. 이는 공인키의 사용을 줄임으로서 공인키의 안전성을 향상시킬 수 있을 뿐만 아니라 키의 노출로 인한 손실을 줄일 수 있다. 본 논문에서는 ID 기반 인증 모델에서의 자기 위임 기법을 소개한다. 이 기법을 통한 세션키의 생성 및 사용은 CRL 관리가 없는 ID 기반 인증 모델에서 개인키의 유효기간을 충분히 길게 할 수 있게 한다. 따라서 주기적으로 모든 사용자의 개인키를 갱신하여야 하는 시스템의 부하를 줄일 수 있을 것이다.

I. 서론

한 기업의 직원이 보안에 취약한 노트북을 휴대하고 출장을 가는 경우를 고려해보자. 만약 자신의 공개키 인증서와 개인키가 저장된 노트북을 분실하였다면 그에게 발생되는 손실은 대단히 클 것이다. 이런 문제에 대한 대응책으로 직원이 특정 기간이나 목적을 위한 키를 생성하여 사용하는 방법이 있을 것이다. 하지만 이 경우 새로 생성된 키에 대한 인증을 어떻게 할 것인가 하는 문제가 다시 등장한다. 만약 인증기관을 이용할 경우 한 사용자에 대해 여러 개의 키를 인증해야 하기 때문에 인증기관에 너무 많은 부하가 걸릴 것이다.

이 문제는 다음과 같이 해결될 수 있다. 먼저 사용자는 공인된 공개키와 개인키를 입력 값으로 하는 computably unforgeable 함수를 이용하여 사용목적에 따라 여러 개의 세션 키를 생성하고 사용하고 검증자는 동일한 것들을 입력 값으로 가지는 공개된 함수를 이용해 각 세션키에 대응하는 공개키를 생성하여 검증함으로서 각 세션키를 인증할 수 있을 것이다. 이와 같은 방법의 상용은 공인키의 직접사용을 최소화하기 때문에 공인키의 안전성을 확보할 수 있을 뿐만 아니라 키 쌍의 사용목적을 제한 할 수 있기 때문에 노출 시 사용자가 입게 되는 손실을 막을 수 있을 것이다. 이처럼 하나의 공인 키 쌍을 이용하여 여러 개의 키 쌍을 생성하여 사용하는 기법을 자기 위임 기법이라 한다. 이 기법의 핵심 기술은 각 키 쌍에 사용자 자신의 권한을 삽입하는 기술이다.

자기 위임 기법에 대한 연구 방향은 크게 두가지가 있다. 첫 번째 방법은 대화형 영지식 증명을 이용하여 공인키에 대한 정보를 소유하고 있음을 증명하는 방법으로 [3]에 자세한 기법이 정리되어 있다. 이 방법은 생성된 세션키의 권한을 명시적으로 확인하지 못하는 단점이 있다. 두 번째 방법은 대리서명 기법을 이용하는 방법이다. 원서명자가 대리인에게 서명 능력을 부여하고 대신 서명하게 하는 기술인데 대리인이 자신인 경우 자기 위임 기법이 된다.

Mambo, Usuda와 Okamoto등에 의해 처음 소개된 대리서명 기법은 김승주, 박상준, 원동호가 위임장의 내용을 직접 대리서명에 삽입시킴으로서 대리인에 의한 서명 능력의 오남용을 방지하는 기술까지 발전되었다[5,4]. 기본적인 대리서명 생성 방법은 다음과 같다. 먼저 원서명자가 대리인의 신상정보(ID등)를 포함한 대리서명 권한을 규정한 위임장에 공개키 시스템에서 사용하는 개인키를 이용하여 서명을 생성하고 위임장과 서명값을 대리인에게 전달한다. 그러면 대리인은 서명값과 자신의 개인키를 이용하여 대리서명에 사용될 대리서명 키 쌍을 생성하고 그 중 개인키를 이용하여 대리서명을 생성한다. 검증자는 원서명

자와 대리인의 공개키를 이용하여 대리서명을 검증한다. 여기에서 검증자는 위임장의 내용과 대리서명된 문서의 내용을 검토하여 대리인의 위임된 권한의 행사에 대한 유효성을 확인한다. 만약 이 두 가지 검증 절차가 모두 유효하면 검증자는 검증과정에서 사용된 원서명자의 공개키를 통해 대리서명에 대한 원서명자의 동의를 확인할 수 있고, 또한 위임된 권한의 오남용도 막을 수 있다. 여기에서 알 수 있듯이 대리서명 기법을 이용한 자기 위임 기법은 생성된 각 키의 권한을 쉽게 제한 할 수 있는 장점이 있다.

기존의 여러 가지 자기 위임 기법이 인증서 기반 인증모델에서의 기법임에 반해 본 논문에서 제안되는 기법은 ID 기반 인증 모델에서의 기법이다.

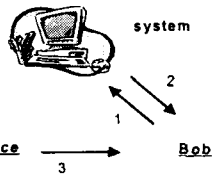
공개키 암호 기술에서는 개인키와 공개키를 이용하는데 공개키를 공개하는 문제는 개인키를 소유자만이 알도록 하는 것보다 매우 단순한 것 같지만 실제 구현 시 공개키를 공개하는 데에 사용되는 간단한 메커니즘(공개키 디렉토리, 게시판 등)들이 자체적으로 안전하지 않아 정보의 변경이 가능하므로 공개키의 위·변조 문제를 야기시킨다. 이런 문제를 해결하기 위해 인증서를 사용하여 공개키를 인증하는 방법이 널리 사용되고 있으며, 최근에는 높은 효율성을 요구하는 분야에 적합한 ID 기반 인증모델이 많이 연구되고 있다.

인증서 기반 인증 모델에서는 사용자가 개인키와 공개키를 생성하여 이중에서 공개키를 공개하는 대신 공개키와 그 소유자를 연결하여 주는 인증서(certificate)를 공개한다. 인증서는 신뢰할 수 있는 제 3자(인증기관)의 서명문이므로 신뢰 객체가 아닌 사람은 그 문서의 내용을 변경할 수 없도록 한다.

반면에, ID 기반 인증 모델에서는 각 사용자의 ID(이메일 주소 등)를 공개키로 직접 사용한다. 따라서 각 사용자의 공개키에 대한 인증기관이 발행

하는 인증서의 필요성은 없어진다. 이 인증 모델은 1984년 A. Shamir에 의해 그 개념이 처음 소개된 이래로 이와 관련한 연구들이 계속되어 D. Boneh 와 M. Franklin에 의해 이 시스템에서의 암호화과정이 만들어 졌다[7,1]. 그 암호화 과정은 [그림 1]과 같다.

ID 기반 인증 모델에서는 각 ID에 대하여 하나씩의 개인키를 생성할 수 있기 때문에 개인키의 노출은 ID를 변경하던지 시스템의 마스터 키를 갱신해야 하는 어려움이 있다. 하지만 자기 위임 기법을 이용하면 하나의 ID에 대하여 여러 개의 키를 생성하여 사용할 수 있는 장점이 있다.



1. Bob은 시스템에 ID를 등록한다.
2. 시스템은 마스터키를 사용하여 Bob의 ID에 대응하는 개인키를 생성하고 발급한다.
3. Alice는 Bob의 ID를 그의 공개키로 이용하여 암호화한다.
4. Bob은 개인키를 이용하여 복호화한다.

[그림 1] ID 기반 인증 모델

이 논문의 나머지 부분은 다음과 같이 구성되어 있다: 본문의 첫 번째 장에서는 ID 기반 자기 위임 기법을 소개하고 두 번째 장에서는 자기 위임 기법의 응용에 대하여 정리한다. 마지막으로 결론을 정리한다.

II. 본문

1. ID 기반 자기 위임 기법

이 장에서 우리는 ID 기반 인증 모델에서의 자기 위임 기법을 소개한다. 기본적인 설계방법은 대리서명 생성과정과 같다. 먼저 사용자는 새로 생성되는 자기 위임키의 사용 권한 범위가 정리된 m_w에 ID 기반 서명 기법을 이용하여 서명을 생성한다. 여기에서 그 서명 값을 자신의 새로운 키로 정의하여 사용한다. 이 방법은 인증서 기반 인증모델에서 [6]의 대리서명 기법과 유사하다. 하지만 이들은 원서명자과 대리인이 다른 대리서명 기법을 소개한 것이나 이미 약점으로 대리인에 의한 부인방지 기능을 제공하지 못한다는 것이 지적되었다. 그러나 자기 위임 기법에서는 원서명자와 대리인이 동일인이기 때문에 이 기법의 의 사용만으로도 서명자의 부인 방지 기능을 제공할 수 있다.

우리는 ID 기반 자기 위임 기법을 설계하기 위해 [2]의 ID 기반 서명 기법을 사용한다. 차재춘과 천정희가 제안한 ID 기반 서명 기법은 결정적 Diffie- Hellman 문제(DDHP)의 해결은 다항식 시간 내에 쉽게 해결되나 계산적 Diffie-Hellman 문제(CDHP)는 해결하기 어려운 임의의 군 위에서 서명 생성과 검증이 이루어진다. 그러한 군을 gap Diffie-Hellman Group(GDH군)이라 부른다. 여기에서 CDHP의 어려움은 existential forgery 공격을 막기 위해 사용되며 DDHP의 쉬운 해결은 서명의 검증에 사용된다. 타원곡선 중 pairing 계산이 쉬운 타원곡선 군은 GDH 군에 속한다.

위수가 l인 GDH 군 $(G,+)$의 생성원을 P라

하고 그 위에서의 bilinear 함수를 e라 하자. 우리의 자기 위임 기법은 다음과 같다.

[1단계] 시스템 파라미터와 마스터키 생성

(1) 난수 $s \in Z/l$을 생성하고 $P_{pub} = s \cdot P$를 계산한다.

(2) 두 개의 충돌 회피 해쉬 함수를 사용한다.

$$H_1: \{0,1\}^* \rightarrow Z/l \text{과 } H_2: \{0,1\}^* \rightarrow G.$$

(3) 시스템 파라미터 (P, P_{pub}, H_1, H_2)를 공개하고 s를 마스터키로 사용한다.

[2단계] ID에 대응하는 개인키 생성

시스템은 각 사용자가 생성한 ID에 대하여 $D_{ID} = s \cdot H_2(ID)$를 계산하고 그것을 그 ID에 대응하는 개인키로 발급한다. 사용자들은 H_2를 이용하여 ID로부터 쉽게 공개키 역할을 하는 $Q_{ID} = H_2(ID)$를 생성하여 사용할 수 있다.

[3단계] 서명 생성

먼저 사용자는 세션키에 위임되는 권한을 명시한 메시지 m_w를 정리한다. 그리고 자신의 개인키 D_{ID}를 이용하여 m_w에 서명한다. 먼저 난수 $r \in Z/l$을 선택하고 다음을 계산한다.

$$U = r \cdot Q_{ID}$$

$$V = (r + H_1(m_w, U)) \cdot D_{ID}$$

그리고 $\sigma = (U, V)$를 m_w에 대한 서명으로 정의한다.

[5단계] ID 기반 자기 위임키 정의

사용자는 서명 값 $\sigma = (U, V)$ 중 V를 자신의 새로운 세션키 (D_{new})로 정의한다. 이 키는 m_w에 대한 서명이므로 이 메시지에서 규정하고 있는 범위 내에서 특정 기간동안 사용 가능한 세션키이다.

[6단계] 자기 위임키를 이용한 서명생성과 검증

사용자는 D_{new}를 이용하여 m_w에서 명시한 권한 내에서 서명 가능한 문서 m_P에 대해서 서명을 생성한다.

(1) 난수 r_P를 선택하고 다음을 계산한다.

$$U_P = r_P \cdot (U + H_1(m_w, U) \cdot Q_{ID}),$$

$$V_P = (r_P + H_1(m_P, U_P)) \cdot D_{\text{new}}$$

(2) 순서쌍 (U_P, V_P, U, m_w, m_P)를 문서 m_P에 대한 서명으로 정의한다.

[3단계] 서명 검증

검증자는 수신된 서명 (U_P, V_P, U, m_w, m_P)을 검증하기 위해 먼저 서명에 사용된 개인키에 대응하는 공개키를 생성한다.

$$Q_P = U + H_1(m_w, U_{ID}) \cdot Q_{ID}$$

그 후, Q_P를 이용하여

$(P, P_{pub}, U_P + H_1(m_P, U_P) \cdot Q_P, V_P)$가 유효한 결정적 Diffie-Hellman 쌍인지 확인한다. 즉, $e(P_{pub}, U_P + H_1(m_P, U_P) \cdot Q_P) = e(P, V_P)$인지 확인하여 검증한다.

우리의 자기 위임 기법은 서명 기법을 반복하여 사용함으로서 설계되었다. 따라서 이 기법의 안전성은 절대적으로 [2]의 서명 기법의 안전성에 의존한다. 하지만 그들은 자신들의 서명 기법이 existential forgery공격에 대하여 안전함을 증명하였다.

2. 응용

ID 기반 인증 모델의 단점은 사용자의 개인키가 노출되었을 경우 파기될 ID의 관리가 어렵다는 것이다. 인증서 기반 인증 모델에서는 인증기관이 파기된 공개키 목록(CRL)을 관리함으로서 쉽게 해결할 수 있으나 ID 기반 인증모델에서는 시스템의 역할이 사용자의 개인키 발급과 함께 없어지기 때문에 파기된 ID에 대한 관리는 대단히 중요한 문제가 된다. 지금까지 제안된 방법은 다음과 같은 세 가지 방법이 있다.

(1) 시스템의 마스터키 갱신: 시스템이 사용자의개인키 생성을 위해 사용하였던 자신의 개인키를 교체하는 방법이다. 이 방법은 해당 시스템에 ID를 등록한 모든 사용자의 개인키는 시스템에 의해 다시 생성되며 전달되어야한다. 따라서 시스템에 상당한 부하가 걸리며, 각 사용자는 암/복호화를 위해 시스템 파라미터를 다시 확인해야 하는 통신 부하가 생긴다.

(2) 사용자의 ID 변경: 사용자의 ID를 교체할 경우 시스템의 부하나 시스템 파라미터를 확인하는 통신 부하는 줄일 수 있다. 하지만 ID는 평생 동안 거의 교체하지 않는다는 특성과 바뀐 ID를 알리는 과정의 복잡성 때문에 개인키 도난 시 발생할 수 있는 문제점에 대한 해결책으로 받아들여지지 않고 있다.

(3) 개인키 생성 방법 수정: 이 방법은 시스템이 개인키 생성 시 단순히 ID에 대응하는 개인키를 생성하는 것이 아니라 ID와 날짜를 연접시킨 (ID||날짜)에 대응하는 개인키를 생성하여 발급하

는 방법이다. 이렇게 함으로서 주기적으로 ID를 교체하는 방법이 있으나 주기 내에 발생하는 개인키의 도난을 고려할 경우 다시 (1) 또는 (2)의 방법을 다시 사용해야 한다. 따라서 최대한 주기를 짧게 하여 개인키를 갱신하여야 하나 이 방법 역시 (1)의 경우와 마찬가지로 시스템의 부하가 너무 크다.

우리는 이 문제의 해결책으로 위 ID 기반 자기 인증 기법을 제안한다. 앞장의 기법에서 특히 중요한 부분은 m_w의 내용이다. m_w의 내용을 단순히 날짜로 정의한다면 각 사용자는 직접 자신의 개인키를 매일 갱신할 수 있으며 이렇게 함으로서 시스템이 매일 또는 특정 기간에 한번씩 키를 갱신해야 하는 부하를 제거할 수 있다.

3. 비교

분류		[6]	[3]	제안 기법
효율성	온라인 상태	필요없음	필요	필요없음
	공개키 인증서	필요	필요	필요없음
기능	오남용 방지	제공못함	제공	제공

표 1. 제안 자기 위임 기법과 기존 기법의 비교

이 장에서는 본 논문에서 제안한 자기 위임 기법과 기존에 제안된 두 가지 기법과 효율성과 기능 측면에서 비교한다. [표1]

먼저 효율성 측면에서 살펴보면 우리의 기법이 가지는 장점은 크게 두 가지로 요약된다. 한가지는 ID 기반 인증 모델을 기반 구조로 사용함으로써 자연스럽게 만들어지는 것이며 다른 한가지는 서명 기법 상에서 발생하는 장점이다. 첫 번째 경우는 제안 기법이 ID 인증 모델 위에서 설계되었기 때문에 공개키에 대한 인증서가 필요 없다는 것이다. 이것은 서명 검증 시 공개키 습득 과정을 제거할 수 있게 해준다. 두 번째는 장점은 [3]과의 비교를 통해 찾을 수 있었다. [3]은 검증자가 세션키의 권한을 확인하기 위해 서명자와 대화형 영지식 증명을 사용해야 하는 단점이 있다. 이에 반해 제안 기법은 권한을 서명 내에 직접 삽입함으로서 그 단점을 극복하였다.

제안 기법이 가지는 주요 기능으로는 세션키의 권한을 명시적으로 제시하기 때문에 키의 분실이나 도난 시 그 손실을 최소로 할 수 있는 장점이 있다.

III. 결론

우리는 본 논문에서 공인된 하나의 키로부터 여러 개의 키를 생성하여 사용할 수 있는 자기 위임 기법을 ID 기반 인증모델 위에서 설계하였다. 이 기법을 통한 세션키의 생성 및 사용은 CRL 관리가 없는 ID 기반 인증 모델에서 개인키의 유효기간을 충분히 길게 할 수 있게 한다. 따라서 주기적으로 모든 사용자의 개인키를 갱신하여야 하는 시스템의 부하를 줄일 수 있을 것이다.

논문에서 제시하는 기법은 서명 기법에만 적용되는 것으로 암호화 알고리즘에도 적용되는 자기 위임 기법의 설계는 아직 미해결 문제이다.

참 고 문 헌

[1] D. Boneh and M. Franklin, " Identity-Based Encryption from the Weil Pairing," Springer-Verlag, Advances in Cryptoloy, Proceedings of CRYPTO '01, LNCS 2139, pp. 213-229, 2001.

[2] J. Cha and J. Cheon, "An Identity-based Signature from Gap Diffie-Hellman Groups," *To appear in Proceedings of PKC '03.*

[3] Oded Goldreich, Birgit Pfitzmann, and Ronald L. Rivest, "Self-Delegation with Controlled Propagation - or - What If You Lose Your Laptop," Springer-Verlag, *Advances in Cryptoloy, Proceedings of Crypto '98, LNCS* 1462, pp. 153-168, 1998.

[4] S. Kim, S. Park, and D. Won, "Proxy Signatures, Revisited," Springer-Verlag, *Proceedings of ICICS '97,* LNCS 1334, pp. 223-232, 1997.

[5] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signature: Delegation of the Power to Sign Messages," In *IEICE Trans. Fundamentals,* Vol. E79-A, No. 9, Sep., pp. 1338-1353, 1996.

[6] H. Petersen and P. Horster, "Self-certified keys - Concepts and Applications," Chapman and Hall, *In Proceedings of Communications and Multimedia Security '97,* pp. 102-116, 1997.

[7] A. Shamir, "Identity-based Crypto systems and Signature Schemes," Springer-Verlag, *Advances in Cryptoloy, Proceedings of Crypto '84, LNCS* 196, pp. 47-53, 1985.