익명성 제거의 공개 검증이 가능한 신원 위탁 방식

이용호, 이임영

순천향대학교 정보기술공학부

A Identity Escrow scheme for public proof of anonymity removing

Yong-ho Lee, Im-yeong Lee

Division of Information Technology Engineering Soonchunhyang Univ.

요 약

사용자와 서비스 제공자가 인증을 수행할 경우 사용자의 신원이 노출되는 문제가 사회의 큰 이슈로 떠오르고 있으며, 이러한 문제점을 해결하기 위해서 신원 위탁 방식이 제시되었다. 신원 위탁 방식에서는 사용자의 정확한 신원을 가지고 있는 발행자가 사용자에게 인증 정보를 전달하고, 사용자는 이것을 이용해 익명성을 유지한 채로 서비스 제공자와 인증 단계를 수행하게 된다. 본 논문에서는 신원 위탁 방식의 안전성과 신뢰성을 위한 새로운 요구사항을 제시하고 이를 만족할 수 있는 새로운 신원 위탁 방식을 제안한다.

I. 서론

사용자들은 서비스를 제공받기 위해서 자신이 정당한 사용자임을 증명해야 하는데 이 같은 개인 식별은 사용자들의 프라이버시가 침해될 위험성을 가지고 있다. 따라서 인증 수행 시 사용자는 신원에 대해 익명성을 원하며, 서비스 제공자는 사용자의 정당성을 확인하기 원한다. 이와 같이 상이한 두 가지 조건을 충족시켜 줄 수 있는 것이 신원 위탁 방식(Identity escrow scheme)이다. 신원 위탁 방식에서는 사용자와 서비스 제공자간의 인증 수행 시 사용자는 서비스 제공자에게 자신의 신원을 제공하지 않고, 발행자에게 발급 받은 인증정보를 제공함으로써 사용자에게 익명성을 유지시킨다. 그리고 서비스 제공자는 인증정보를 통해서 사용자의 신원을 알 수는 없지만 정당한 사용자라는 것을 확인할 수는 있다. 그리고, 만약 사용자가 불법적인 행위를 하였을 경우에 사용자의 익명성을 제거하기 위해서 사용자로부터 제공받은 인증정보를 법기관에게 제공하면 법기관과 발행자는 협력하여 그 인증정보에 대응되는 사용자의 정확한 신원을 확보할 수 있다.[1]

본 고의 2장에서는 신원 위탁 방식의 구성요소와 기본단계 그리고 요구사항을 분석한다. 그리고 3장에서는 기존방식들에 대해 간략히 설명한다. 4장에서는 새로운 방식을 제안하고 다른 방식들과 비교/분석한다. 마지막으로 5장에서 결론을 맺도록 한다.

본 논문은 2001년도 순천향대학교 대학자체 학술연구비에 의해 연구되었음.

II. 신원 위탁의 이해

1. 신원 위탁 방식의 구성요소

신원 위탁 방식은 기본적으로 다음과 같은 4개의 구성요소를 가지고 있다.[2][3][4]

- 사용자 (A) : 일반적인 사용자로써 서비스 제공자에게 익명으로 서비스를 제공받기 위해서 발행자에게 자신의 정확한 신원을 제공하고, 서비스 제공자에게 익명으로 인증받을 수 있는 인증정보를 제공받는다.
- 발행자 (ISS) : 익명으로 서비스 제공자에게 서비스를 제공받길 원하는 사용자의 정확한 신원을 저장하고 인증정보를 제공한다. 유사시 법기관의 요청에 의해 사용자의 정확한 신원을 드러낸다.

- 서비스 제공자 (SP) : 사용자의 인증정보를 검증하고 이상이 없으면, 서비스를 제공한다. 만약 사용자가 불법적 행동을 했을 경우에는 법기관에게 사용자의 신원에 대한 익명성 제거를 요구한다.
- 법기관 (LEA) : 유사시 서비스 제공자의 요구를 받아 발행자와 협력해 사용자의 정확한 신원를 드러낸다.

2. 신원 위탁 방식의 기본 단계

신원 위탁 시스템은 크게 4가지 단계로 이루어져 있다.[3][4]

- 시스템 초기화 단계 : 각 참여 개체는 시스템을 초기화하기 위해 자신의 파라미터(공개키 또는 공개 파라미터)를 공표한다.
- 신원 등록 단계 : 사용자는 자신의 정확한 신원을 발행자에게 전달하고 안전하게 인증정보를 제공받는다.
- 인증 단계 : 사용자는 익명으로 서비스를 제공받기 위해 서비스 제공자에게 자신의 인증정보를 제공한다. 이것이 유효한 인증정보이고 사용자가 이에 대한 비밀정보를 알고 있다면 서비스 제공자는 사용자에게 서비스를 제공한다.
- 익명성 제거 단계 : 유사시 서비스 제공자는 법기관에게 사용자가 인증 단계에서 제공한 인증정보를 제공함으로써 사용자의 익명성을 제거하고 정확한 신원을 드러낸다.

3. 신원 위탁 방식의 요구사항

본 절에서는 기존의 요구사항에 대해 알아보고, 전체 시스템의 안전성과 신뢰성 향상을 위한 새로운 요구사항6을 제시한다. 신원 위탁 시스템에서 가장 중요한 것은 사용자의 신원이 정확히 발행자에게 위탁되었다는 것이 증명 가능해야 하고, 제3자가 사용자의 신분을 도용할 수 없어야 한다는 것이다. 그러나 이것이 법기관이나 발행자에 의해서만 이루어지는 것은 시스템의 안전성과 신뢰성을 저하시키는 요소가 된다. 따라서 참여 개체라면 누구나 위 사실을 공개적으로 검증할 수 있어야 한다.

다음은 신원 위탁 방식의 요구사항을 기술한 것이다.

- 요구사항1 (익명성을 제공하는 인증성) : 사용자와 서비스 제공자간의 인증 수행 시 사용자의 익명성은 제공되어야 하며, 정당한 사용자인지 검증 가능해야 한다.
- 요구사항2 (불법 사용자의 익명성 제거) : 유사시 법기관과 발행자가 협력하면 불법 사용자에 대한 익명성을 제거할 수 있어야 한다.
- 요구사항3 (인증정보에 대한 비밀정보 유지 증명) : 제 3자가 사용자임을 사칭할 수 없어야 한다. 즉, 인증정보가 해당 사용자의 것임을 증명할 수 있는 비밀값은 오직 사용자만이 가지고 있어야 한다.
- 요구사항4 (법기관의 독립성) : 법기관과의 통신은 그 특성상 불법 사용자의 익명성 제거 요청이 있을 경우에만 수행되어야 한다.
- 요구사항5 (불법적인 익명성 제거 방지) : 사용자의 익명성 제거는 법기관의 허가가 있어야만 가능해야 한다. 즉, 발행자나 서비스 제공자는 인증정보와 공개된 정보만을 이용해서 사용자의 신원을 밝힐 수 없어야 한다.
- 요구사항6 (익명성 제거 공개 검증성) : 법기관과 발행자가 협력하면 불법 사용자의 익명성 제거가 가능하다는 것을 참여 개체 누구라도 공개적으로 검증 가능해야 한다.

III. 기존 방식 분석

본 장에서는 1998년도 CRYPTO Conference에서 소개된 2가지 방식과 2000년도 멀티미디어학회 논문지에서 소개된 2가지 방식을 적용기술에 따라 구분하여 간략히 소개한다.[2][3]

1. 방식1 (그룹 서명 적용)

이 방식은 1998년도 CRYPTO Conference에서 Joe Kilian과 Erez Petrank에 의해 제안된 방식으로 그룹 서명의 특징을 이용해 사용자의 익명성을 제공하고 있다. 그러나 이 방식은 발행자와 법기관이 비독립적이고, 익명성 제거의 정당성을 공개적으로 확인할 수 없다는 문제점을 가지고 있다.

2. 방식2 (영지식 증명 적용)

이 방식은 1998년도 CRYPTO Conference에서 Joe Kilian과 Erez Petrank에 의해 제안된 방식으로 그룹 서명을 적용한 방식의 문제점을 지적하고, 이를 해결하기 위해 ZKIP(Zero-Knowledge Interactive Protocol)을 적용한 방식이다. 이 방식은 영지식 증명을 적용하여 시스템 초기화시 법기관의 접촉을 제거하였지만 발행자가 사용자의 모

든 정보를 가지고 있기 때문에 사용자를 사칭할 수 있고, 익명성 제거의 정당성을 공개적으로 확인할 수 없다는 문제점을 가지고 있다.

3. 방식3 (블라인드 기술 적용)

이 방식은 2000년도 멀티미디어학회 논문지에서 황보성 등에 의해 제안된 방식으로 Joe Kilian과 Erez Petrank이 제안한 2가지 방식의 문제점을 해결하기 위해 블라인드 기술을 적용하였다. 이 방식은 블라인드 기술을 적용하여 사용자의 익명성을 제공하고 있지만 법기관의 독립성을 제공하지 못하고 있으며, 익명성 제거의 정당성을 공개적으로 확인할 수 없다는 문제점을 가지고 있다.

4. 방식4 (전자화폐 프로토콜 적용)

이 방식은 2000년도 멀티미디어학회 논문지에서 황보성 등에 의해 제안된 방식으로 법기관의 독립성을 만족시키기 위해 전자화폐 프로토콜을 적용하였다. 이 방식은 전자화폐 프로토콜을 적용하여 법기관의 독립성을 제공하고 있지만 익명서 제거의 정당성 증명을 공개적으로 확인할 수 없다는 문제점을 가지고 있다.

IV. 제안 방식

본 장에서는 블라인드 복호와 대리 서명을 기반으로 법기관의 독립성을 제공하면서 익명성 제거의 공개 검증이 가능한 새로운 신원위탁 방식을 제안한다.

1. 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수에 대한 설명이다.

- p, q : 큰 소수(단, q| p-1)
- g : Z_p상의 원시원소
- * : A(사용자), ISS(발행자), SP(서비스 제공자), LEA(법기관)
- ⊙ : 구성 요소들의 비밀키 또는 공개키
- X_* : *의 비밀키
- Y_* : *의 공개키
- $E_{⊙}()$: ⊙를 키로 이용해 암호화한 암호문
- $Sig_{⊙}()$: ⊙를 키로 이용해 서명한 서명문
- S : 사용자 인증정보에 해당하는 비밀값
- f : 블라인드 복호에서 사용되는 인자
- ID_A : 신원 등록자 A의 가명 ID
- σ : 서명자의 대리 서명
- h() : 안전한 일방향 해쉬함수

2. 프로토콜

본 프로토콜은 사용자 신원 등록 및 검증 단계, 대리 서명 정보 생성 및 검증 단계, 서비스 요구 및 검증 단계 그리고 익명성 제거 단계로 구성되고 각각의 단계는 다음과 같다.

1) 사용자의 신원 등록 및 검증 단계

가) 사용자 수행

① 임의의 랜덤값 t와 f를 생성한 후 비밀값 S를 다음과 같이 구성한다.

$$S = X\_A + t \quad (1)$$

② 다음 정보를 구성하고, 발행자의 공개키를 이용해 암호화하여 전송한다.

$$E_{Y\_ISS}(\text{신원}||E_{Y\_LEA}(t||g^S)) \;||\; g^S * E_{Y\_ISS}(f) \quad (2)$$

나) 발행자 수행

③ 신상정보를 저장하고 가명 ID_A를 생성한 후 다음과 같이 블라인드 복호 기술을 이용하여 계산하고 결과값을 안전하게 저장한다.

$$f * Sig_{X\_ISS}(g^S) = E_{X\_ISS}(E_{Y\_ISS}(f) * g^S) \quad (3)$$

④ 다음 정보를 구성하고, 법기관의 공개키를 이용해 암호화하여 전송한다.

$$E_{Y\_LEA}(t||g^S) \;||\; E_{Y\_LEA}(ID\_A) \quad (4)$$

다) 법기관 수행

⑤ 다음 수식을 검증하고, 이상이 없으면 공개 보드에 가명 ID를 등록한다.

$$g^S = Y\_A * g^t \quad (5)$$

2) 대리 서명 정보 생성 및 검증 단계

가. 발행자 수행

⑥ 임의의 랜덤값 d를 생성하고, 이를 이용해 대리 서명 정보를 생성한다.

$$D = g^d \bmod p \quad (6)$$

$$\sigma = (X\_ISS + d*D) \bmod p-1 \quad (7)$$

⑦ 다음 정보를 구성하고, 사용자의 공개키를 이용해 암호화하여 전송한다.

$$E_{Y\_A}(\sigma||D||ID\_A||f * Sig_{X\_ISS}(g^S)) \quad (8)$$

나) 사용자 수행

⑧ 다음 수식을 검증하고 맞으면 계속 진행한다. 그렇지 않으면, 발행자에게 문의하여 대리 서명 정보 생성 과정을 다시 시작한다.

$$g^{\sigma} = Y\_ISS*D^{D} \bmod p \quad (9)$$

3) 서비스 요구 및 검증 단계

가) 사용자 수행

⑨ 임의의 랜덤값 r과 서비스 요구 메시지 m을 이용하여 사용자 인증정보 $S_{\sigma}(m)$을 다음과 같이 구성한다.

$$R = g^{r} \bmod p \bmod q \ , \ H = h(m) \quad (10)$$

$$S_{\sigma}(m) = S*r - R*\sigma*H \bmod p \quad (11)$$

⑩ 전송된 $f*Sig_{X_ISS}(g^{S})$에서 블라인드 인자 f를 제거한다.

$$Sig_{X\_ISS}(g^{S}) = f*Sig_{X\_ISS}(g^{S})/f \quad (12)$$

⑪ 다음 정보를 구성하고, 서비스 제공자의 공개키를 이용해 암호화하여 전송한다.

$$E_{Y\_SP}(ID\_A||D||R||m||S_{\sigma}(m)||Sig_{X\_ISS}(g^{S})) \quad (13)$$

나) 서비스 제공자 수행

⑫ 다음 수식을 검증하고 맞으면 사용자에게 서비스를 제공한다. 그렇지 않으면, 사용자에게 에러 메시지를 전송한다.

$$H = h(m), \ V = Y\_ISS*D^{D} \bmod p \quad (14)$$

$$R*g^{S} = g^{S\sigma(m)}*V^{RH} \bmod p \bmod q \quad (15)$$

검증 과정은 다음과 같이 이루어진다.

$$\begin{aligned} R*g^{S} &= g^{S\sigma(m)}*V^{RH} \\ &= g^{S*r \ - \ R*\sigma*H} \ * \ g^{\sigma*R*H} \\ &= g^{S*r} \\ &= R*g^{S} \end{aligned} \quad (16)$$

4) 익명성 제거 단계

가) 서비스 제공자 수행

⑬ 만약 사용자의 부정이 발견되면 발행자의 서명이 수행된 $Sig_{X_ISS}(g^{S})$를 법기관에게 전송하고 사용자의 익명성 제거를 요청한다.

나) 법기관과 발행자 수행

⑭ 법기관과 발행자는 전송된 $Sig_{X_ISS}(g^{S})$를 이용하여 사용자의 익명성을 제거한다.

3. 제안 방식 비교/분석

본 절에서는 제시된 요구사항을 중심으로 4가지 기존 방식과 제안 방식을 비교/분석한다.

표 1: 각 방식별 비교/분석표.

방식 / 요구사항	방식1	방식2	방식3	방식4	제안방식
요구사항1	O	O	O	O	O
요구사항2	O	O	O	O	O
요구사항3	O	X	O	O	O
요구사항4	X	O	X	O	O
요구사항5	O	X	O	O	△
요구사항6	X	X	X	X	O

제안 방식은 시스템 초기 설정 시 법기관의 통신을 1-pass로 처리하여 독립성을 유지하고 있으며, 기존 방식에 비해 현저히 적은 통신량을 가지고 있어 가장 효율적인 방식이라 할 수 있다.

V. 결론

사용자가 공개 네트워크 상에서 서비스 제공자와 인증을 수행할 경우 사용자는 자신의 신원에 대해 익명성을 가지기를 원할 것이고, 서비스 제공자는 사용자의 정확한 신원을 확인 후 서비스를 제공하기를 원한다. 이렇게 상반되는 이해관계는 신원 위탁 방식을 사용함으로써 사용자와 서비스 제공자 모두의 요구사항을 만족시킬 수 있을 것이다. 본 논문에서는 기존 신원 위탁 방식들의 문제점들을 알아보았고, 이들의 문제점들을 해결하면서 상기 요구사항을 만족할 수 있는 새로운 신원 위탁 방식을 제안하였다. 향후 좀 더 안전하고 효율적인 신원 위탁 방식의 연구가 진행되어야 할 것이다.

참고문헌

[1] 이임영, *전자상거래보안입문*, 생능출판사, 2001

[2] Joe Kilian and Erez Petrank, "Identity Escrow," Advances in Cryptology-CRYPTO'98, pp. 169-184, 1998

[3] 황보성, 이임영, "사용자의 익명성을 제어하는 신원위탁 방식 제안", 멀티미디어학회 논문지 제 3권 제 6호, pp.617-624. 2000

[4] 황보성, 이임영, "신원위탁 방식의 설계", WISC'2000, pp588-602, 2000