추적성이 제공된 속성기반서명 기법에 관한 연구

황용운[1], 신재정[2], 이임영[3]
[1]순천향대학교 컴퓨터소프트웨어공학과 박사후연구원
[2]순천향대학교 소프트웨어융합학과 석사과정
[3]순천향대학교 컴퓨터소프트웨어공학과 교수
hyw0123@sch.ac.kr, jaejeongshin@sch.ac.kr, imylee@sch.ac.kr

A Study on Attribute-Based Signature Schemes Provided with Traceability

Yong-Woon Hwang[1], JaeJeong Shin[2], Im-Yeong Lee[3]
[1,3]Dept. of Software Computer Software Engineering, Soonchunhyang University
[2]Dept. of Software Convergence, Soonchunhyang University

요 약

최근 네트워크 환경에서 통신되는 데이터의 신뢰성을 제공하기 위해 서명기술이 필요하다. 다양한 서명기술들 중 속성기반서명은 사용자들이 가지고 있는 속성을 기반으로 서명을 수행하기 때문에, 각 서명자들의 익명성을 보장할 수 있는 서명기술이다. 하지만 속성기반서명을 수행시 익명성을 악용하는 사용자들이 존재하는데, 이들은 잡히는 위험이 없이 일부 목적(금전, 이익)을 위해 의도적으로 자신의 서명비밀키와 속성을 공개할 수 있다. 서명권한이 없는 제 3자는 이를 이용해 서명을 수행할 수 있다. 본 논문에서는 적절한 수준의 익명성과 추적성이 제공되는 속성기반서명 기법을 제안한다. 본 제안방식은 검증자가 서명 검증시 문제가 생긴 서명에 관해 AA에게 서명을 보낸 서명자의 신원을 요청하여 확인할 수 있다.

1. 서론

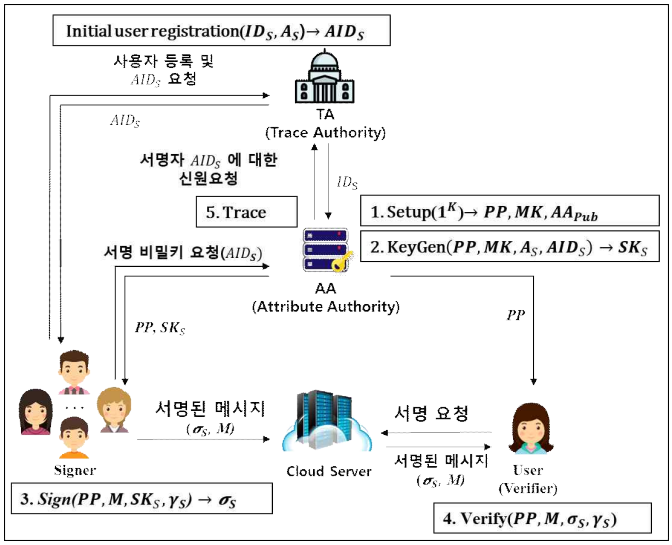
최근 네트워크 환경에서 통신되는 데이터의 중요도에 따라 공격자들의 타켓이 될 수 있으며, 이는 다양한 보안위협을 발생시킬 수 있다. 이를 해결하기 위해 데이터의 신뢰성을 제공할 수 있는 서명기술이 필요하다. 다양한 서명기술들이 존재하는데, 그 중 서명자들의 프라이버시를 보호하기 위한 서명 기술로 속성기반서명이 연구되고 있다[1]. 속성기반서명은 서명자가 가지고 있는 속성들을 기반으로 트리 형태의 접근구조를 만들어 메시지 서명을 수행하는 암호기법이다. 이에, 메시지를 익명으로 올리면서도, 자격증명에 대한 적절한 주장을 할 수 있다. 하지만 속성기반서명에서 제공되는 익명성을 악용하는 사용자들이 몇몇 존재한다. 이러한 사용자들은 잡히는 위험이 없기 때문에 일부 목적(금전, 이익)을 위해 의도적으로 자신의 서명비밀키와 속성을 다른 사용자에게 공개할 수 있다. 서명권한이 없는 제 3자는 이를 이용해 서명을 수행할 수 있기 때문에 이에 대한 대응방안이 필요하다[2].

본 논문에서는 적절한 익명성과 추적성이 제공되는 속성기반서명 기법을 제안한다. 본 제안방식은 검증자가 서명 검증시 문제가 생긴 서명에 관해 AA(Attribute Authority)에게 서명을 보낸 서명자의 신원을 요청할 수 있으며, AA는 TA(Trace Authority),와 협력하여 서명을 보낸 서명자 또는 속성 유출자의 신원을 확인할 수 있다. 따라서 사전에 서명자가 속성이나 서명 비밀키를 유출하는 것을 방지할 수 있다.

2. 제안방식

[그림 1]은 본 제안방식의 전체 시나리오이며, 각 단계에 대한 설명은 다음과 같다.

- $Inial\ user\ registration(ID_S, A_S)$: 서명자는 TA에게 등록요청을 TA는 서명자의 가명 ID값(AID_S)을 만들어 보내준다.
- $Setup(k)$: AA에서 보안파라미터 k를 통해 공개파라미터(PP)와 마스터키(MK), 공개키(AA_{Pub})를 생성한다.
- $KeyGen(PP, MK, A_S, AID_S)$: 서명자는 AA에게 가명 ID값($AID_S$)과 속성값을 보내 서명 비밀키($SK_S$)를 발급받는다. 서명 비밀키 값에는 키를 발급받은 서명자의 신원을 확인할 수 있는 값(PSK와 UTR)이 포함되어 있다.



[그림 1]. 본 제안방식의 전체 시나리오.

· $Sign(PP, M, SK_S, Y_S)$: 서명자는 자신의 속성으로 접근구조 Y_S를 생성한다. 그리고, PP와 SK_S를 가지고 메시지(M)을 서명한다. 그리고, 서명된 메시지를 클라우드 서버로 보내 저장한다.

· $Verify(PP, M, \sigma_S, Y_S)$: 사용자는 클라우드 서버로부터 서명문을 요청하여, 수신받고 PP, M, Y_S를 가지고 서명을 검증한다. 올바르게 검증되면, 사용자는 A_S의 속성을 가진 서명자가 메시지를 서명하여 보낸 것을 알 수 있다.

· $Trace(AID_S, T_S)$: 만약 검증된 메시지가 불분명하거나 오류가 날 경우 사용자는 AA에게 서명(σ_S)을 전송한 서명자의 신원을 요청한다. AA는 σ_S에 포함된 PSK와 UTR을 가지고 서명한 서명자의 가명 ID값(AID_S)을 도출하고 TA에게 전송한다. TA는 연산을 수행하여 가명 ID값(AID_S)에 대응되는 사용자의 신원을 확인하여 알려준다.

3. 제안방식 분석

• **서명자의 프라이버시 보호 가능 :** 본 제안방식은 서명자의 가명 ID와 속성값을 활용하여 속성기반서명을 수행하기 때문에, 서명자의 프라이버시를 보호할 수 있다. 세부적으로, 속성(A_S)을 가지고 만든 Y_S으로 메시지에 서명하였으며, 이를 사용자가 검증시, A_S의 속성을 가진 서명자가 서명을 전송한 것을 알 수 있다.

• **서명자 및 속성 유출자를 추적하여 신원확인 가능:** 본 제안방식은 서명 수행시 가명 ID 값이 포함되어 있다. 사용자가 서명된 메시지 검증 후 메시지가 불분명하거나 문제가 있는 경우 AA에게 서명자의 신원을 요청할 수 있으며, AA는 TA와 협력하여 서명자의 신원을 확인할 수 있다. 또한 서명 수행 시 서명 비밀키를 최초로 발급받은 서명자의 신원을 확인할 수 있는(PSK와 UTR)값이 포함되어 있어, 만약 서명자가 누군가로부터 서명 비밀키와 속성을 유출 받아 서명했을 경우 유출자의 신원을 추적하여 확인할 수 있다.

4. 결론

본 논문에서는 추적성이 제공되는 속성기반서명 기법을 제안하여, 통신되는 데이터의 신뢰성을 제공하였다. 제안방식은 속성기반서명에서 제공하는 익명성을 악용하는 사용자들을 추적하여 신원을 확인할 수 있다. 이에, 사전에 서명자가 속성이나 서명 비밀키를 유출하는 것을 방지할 수 있다. 또한 가명 ID 값과 속성값으로 서명을 수행했기 때문에, 서명자의 프라이버시 보호가 가능하며, 검증과정을 통해 메시지에 대한 무결성이 보장된다.

향후, 속성기반서명 기법에서 가명 ID의 보안성을 높이기 위해 가명 프로토콜을 도입할 수 있는 연구가 필요할 것으로 사료된다.

Acknowledgments

본 연구는 한국연구재단 4단계 두뇌 한국21사업(4단계 BK21사업) (과제번호:5199990914048)와 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구(No. 2022R1A2B5B01002490), 문화체육관광부 및 한국콘텐츠진흥원의 2023년도 SW저작권 생태계 조성 기술개발 사업으로 연구가 수행되었음 (과제명 : 클라우드 서비스 활용 구축형태별 대규모 소프트웨어 라이선스 검증 기술개발, 과제번호 : RS-2023-00224818, 기여율: 33%)

참고문헌

[1] Oberko, P. S. K., et al. “A survey on Attribute-Based Signatures”, Journal of Systems Architecture, 102396, 2022.

[2] Wei, J., Huang, X., Liu, W., and Hu, X., “Practical attribute-based signature: Traceability and revocability”, The Computer Journal, Vol. 59, No. 11, pp. 1714-1734, 2016.