위장공격을 방지하는 무인증서 기반 인증 및 키 합의에 관한 연구

임혜민, 이임영
순천향대학교 소프트웨어융합학과
renchn1127@sch.ac.kr, *imylee@sch.ac.kr

Certificateless Authentication and Key Agreement to Prevent an Impersonation Attack

Ren Huimin Im-Yeong Lee
Department of Software Convergence, Soonchunhyang University

요 약

인증 및 키 합의 프로토콜은 안전한 통신에 사용자의 세션키를 생성하는 프로토콜이다. 기존에 공개키 인프라 기반 인증 및 키 합의 방식은 인증서와 키의 관리 문제가 존재하며, 신원 기반 인증 및 키 합의 방식은 키 에스크로 문제가 있다. 이러한 문제들 해결할 수 있는 무인증서 암호시스템을 기반으로 하는 무인증서 기반 인증 및 키 합의 프로토콜에 대해서 활발히 연구가 진행 중이다. 하지만, 무인증서 암호시스템에서 사용자의 공개키 인증서를 사용하지 않기 때문에 사용자 식별자에 대한 인증을 할 수 없다. 따라서 무인증서기반 인증 및 키 합의 방식에서 공격자가 사용자의 공개키를 대체하여 위장공격이 가능하다. 본 논문에서는 기존에 있는 위장공격을 해결하고 효율적인 방법에 대해 제안한다.

Ⅰ. 서 론

키 합의 프로토콜은 통신하고자 하는 양방향 또는 다방면의 세션키를 합의하여 안전한 통신을 제공한다. 통신하는 사용자들을 인증을 할 수 있는 키 합의 프로토콜을 인증 및 키 합의(Authentication and Key Agreement, AKA) 프로토콜이라고 한다.

무인증서 기반 인증 및 키 합의(Certificateless Authentication and Key Agreement, CL-AKA) 프로토콜은 무인증서 암호시스템(Certificateless Public Key Cryptography, CL-PKC)기반으로 하는 인증 및 키 합의 프로토콜이다[1].

CL-AKA는 기존에 공개키 인프라(Public Key Infrastructure, PKI)를 사용하는 공개키 인프라 기반 인증 및 키 합의 방식(Public Key Infrastructure Authentication and Key Agreement, PKI-AKA)에 준재하는 인증서와 키의 관리 문제를 해결할 수 있다. 또한, CL-AKA는 신원 기반 암호시스템(Identity-based Cryptography, IBC)를 사용하는 신원기반 인증 및 키 합의 방식(Identity-based Authentication and Key Agreement, ID-AKA)에 준재하는 키 에스크로 문제가를 해결할 수 있다. 이러한 문제들 해결할 수 있는 CL-AKA 프로토콜에 대해서 활발히 연구가 진행 중이다.

하지만 CL-AKA에서는 사용자의 공개키 인증서를 사용하지 않기 때문에 사용자의 식별자 및 공개키에 대한 인증을 할 수 없다. 따라서 CL-AKA에서 공격자가 사용자의 공개키를 대체하여 위장공격을 가능하다[2, 3].

본 논문에서 이 문제 해결하기 위해 KGC(Key Generation Center)의 공개키를 이용하여 서로의 공개키 검증할 수 있는 방식을 제안한다. 또한, 세션키 합의할 때 사용자의 식별자, 임의의 키와 비밀키 등을 바인딩하여 공격자가 사용자의 공개키를 대체해도 같은 세션키를 생성할 수 없도록 위장공격 방지 기능을 설계한다.

본 논문은 기존에 있는 CL-AKA 프로토콜에 발생 가능한 위장공격을 방지할 수 있는 효율적이고 안전한 CL-AKA 프로토콜을 제안한다.

Ⅱ. 관련 연구

공개키 암호시스템에 따라 AKA는 PKI, IBC, 또는 CL-PKC을 이용하는 방식으로 나눌 수 있다.

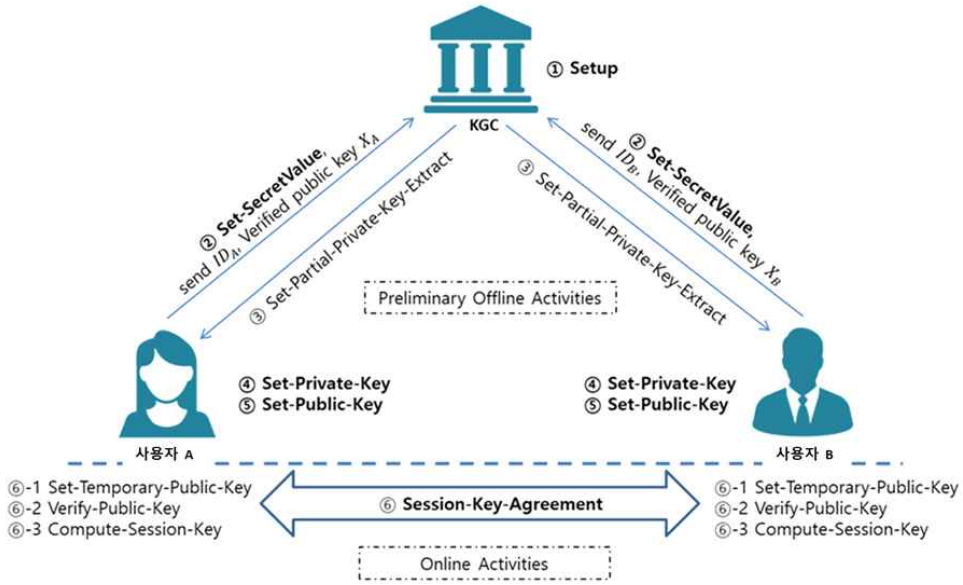
기존의 PKI는 키와 서명, 인증서에 대한 저장소 문제와 배포, 검증 및 폐기 등 관리에 대한 오버헤드가 매우 큰 문제가 있다. 이를 해결하기 위해서 1984년 A. Shamir가 IBC[4]을 제안했다. IBC는 인증서 필요 없고 사용자의 미메일, IP주소와 같은 사용자의 신원정보로부터 해당 사용자의 공개키를 유도한다. 하지만, 각 사용자의 비밀키는 KGC으로부터 생성해하므로 발생하는 키 에스크로로 문제를 해결하기 위하여 KGC에서 사용자들의 키를 전부 생성하지 않고, 일부만 생성하는 형태로 부분 비밀키를 생성하여 전달해 준다.

PKI의 인증서 관리 문제 및 IBC의 키 에스크로 문제를 해결할 수 있기 때문에 현재 CL-AKA의 연구가 많이 나와 있다[5, 6].

Ⅲ. 제안방식

본 장에서는 기준에 있는 CL-AKA 프로토콜의 발생 가능한 위장공격을 방지할 수 있는 효율적이고 보안성 높은 CL-AKA프로토콜을 제안한다. 본 제안방식의 전체 시나리오는 그림 1에 나타낸 Setup, Set-Secret-Value, Set-Partial-Private-Key-Extract, Set-Private-Key, Set-Public-Key, Session-Key-Agreement 총 6단계로 구성된다.

① Setup : KGC는 마스터 공개키 및 KGC의 마스터 비밀키를 생성하고 보안 파라미터를 공개한다.
② Set-Secret-Value : 사용자 자신의 공개키와 비밀키를 생성하고 공개키를 KGC한테 보낸다.
③ Set-Partial-Private-Key-Extract : KGC가 사용자한테 받은 공개키 및 사용자의 식별자를 이용해서 부분 공개키 및 검증용 공개키를 생성한다.



〔그림 1〕 전체 시나리오

④ Set-Private-Key : 사용자가 생성한 비밀값 및 KGC가 생성한 부분 비밀키로 사용자의 비밀키 쌍을 생성한다.

⑤ Set-Public-Key : 사용자가 생성한 공개키 및 KGC가 생성한 부분 공개키와 검증용 공개키로 공개키 쌍을 생성한다.

⑥ Session-Key-Agreement

1) Set-Temporary-Public-Key : 사용자가 임시 비밀키를 선택하고, 임시 공개키를 계산한다. 사용자가 통신하는 상대방한테 자신의 식별자, 공개키 및 임시 공개키를 보내준다.

2) Verify-Public-Key : 사용자들이 세션키 합의 하기 전에 상대방에게 받은 임시 공개키 및 검증용 공개키를 검증한다.

3) Compute-Session-key : 사용자가 통신하는 상대방한테 검증용 공개키의 검증이 완료되었다면 키 합의를 진행한다. 사용자가 각각 키 합의 알고리즘을 이용해서 세션키를 계산하고 세션키를 이용해서 안전한 통신을 수행할 수 있다.

Ⅳ. 제안방식 분석

- **위장공격 방지** : 기존 CL-AKA 방식에서 공격자가 사용자의 공개키를 대체하여 위장공격을 가능하다. 본 논문은 사용자가 KGC의 공개키를 이용하여 서로의 공개키를 검증한다. 또한, 세션키 합의할 때 사용자의 식별자, 임의의 키와 비밀키 등을 바인딩하여 공격자가 사용자의 공개키를 대체해도 같은 세션키를 생성할 수 없다. 이를 통해 위장공격을 방지할 수 있다.
- **효율성**: 분 논문은 효율성을 높이기 위한 페어링 연산이 없는 CL-AKA를 제안한다[7]. 또한, 사용자가 키 합의단계에 연산량을 기존의 있는 CL-AKA보다 줄인다. 그러므로 사용자가 키 합의 단계에서 기존의 방식보다 빠르다.

Ⅴ. 결론

본 논문은 기준에 있는 CL-AKA 프로토콜의 발생 가능한 위장공격을 방지할 수 있는 효율적이고 보안성 높은 CL-AKA 프로토콜을 제안한다. 본 제안방식은 공개키 기반 인증 및 키 합의 방식 및 신원 기반 인증 및 키 합의 방식에 발생하는 인증서 관리 문제 및 키 에스크로 문제를 해결할 수 있다. 또한, KGC의 공개키를 이용해 서로의 공개키 검증할 수 있는 방식을 제안한다.

그리고 세션키 합의할 때 사용자의 식별자, 임의의 키와 비밀키 등을 바인딩하여 공격자가 사용자의 공개키를 대체해도 같은 세션키를 생성할 수 없도록 위장공격을 방지할 수 있다. 기존 CL-AKA 프로토콜보다 더욱 효율적이고 빠르다.

ACKNOWLEDGMENT

본 연구는 2019년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2019R1A2C1085718)

참 고 문 헌

[1] S. S. Al-Riyami, K. G. Paterson, “Certificateless Public Key Cryptography”, In International conference on the theory and application of cryptology and information security, pp. 452-473, 2003.

[2] A. Shamir, “Identity-Based Cryptosystems and Signature Schemes”, Advances in Cryptology, pp. 47-53, 1984.

[3] Bala S, Sharma G, Verma A K. “Impersonation attack on CertificateLess key agreement protocol”. International Journal of Ad Hoc and Ubiquitous Computing, pp. 108-120, 2018.

[4] Xie, Yong, et al. "Efficient two-party certificateless authenticated key agreement protocol under GDH assumption." International Journal of Ad Hoc and Ubiquitous Computing 30.1 (2019): 11-25.

[5] Daniel, Renu Mary, Elijah Blessing Rajsingh, and Salaja Silas. "An efficient eCK secure certificateless authenticated key agreement scheme with security against public key replacement attacks." Journal of Information Security and Applications, pp. 156-172, 2019.

[6] Zeng, Runzhi, and Libin Wang. "Cryptanalysis of certificateless authenticated key agreement protocols." International Journal of Ad Hoc and Ubiquitous Computing, pp. 249-257, 2020.

[7] J. BaekReihaneh, “Certificateless Public Key Encryption Without Pairing”, Information Security, pp. 134-148, 2005.