PGP에서 신규 키 생성을 통한 신뢰 관계 취소 기법

이정범, 김현수, 권태경

서울대학교

jblee@mmlab.snu.ac.kr, hskim@mmlab.snu.ac.kr, tkkwon@snu.ac.kr

Revocation of Trust on PGP using New Key Generation

Jungbum Lee, Hyunsoo Kim, Ted “Taekyoung” Kwon

Seoul National Univ.

요 약

중앙 집중형 구조 때문에 발생하는 여러 문제를 해결하기 위한 분산형 PKI구조를 가지는 PGP는 중앙 기관이 키를 관리해 주지 않고, 각 대상이 키의 생성, 해지 등과 다른 키에 대한 신뢰를 관리한다. PGP에서 각 대상은 자신이 직접적으로 신뢰하지 않은 대상들까지 신뢰 영역을 확장하기 위해 자신이 신뢰하는 대상이 신뢰하는 대상을 신뢰하는 방식을 주로 택한다. 이 방식 때문에 중간에 어떤 대상이 공격받아 외부의 악의적인 키를 신뢰하는 보안 문제가 발생하면, 공격받은 대상을 신뢰하는 대상들은 자동으로 악의적인 키를 신뢰하게 되는 문제가 발생한다. 이를 막기 위해 PGP에는 신뢰 관계를 취소할 수 있는 메커니즘이 존재한다. 하지만 이 방식의 문제는 신뢰를 제공받는 측은 손쉽게 신뢰 관계를 취소할 수 있으나, 신뢰를 제공하는 측은 신뢰 관계를 취소하기 어렵다는 점이다. 본 논문에서는 이 취소의 불균등성 문제를 해결하기 위해 신뢰를 제공하는 측에서 신뢰 관계만을 위한 키 페어를 생성해 표준을 크게 변화시키지 않고 기존 시스템에서 존재하는 시스템을 활용해 신뢰를 제공하는 측에서도 신뢰 관계를 취소할 수 있는 기법을 제안한다.

Ⅰ. 서 론

올바른 공개 키의 소유자를 감별하여 상호 간의 신뢰 관계를 구축하는 것은 공개 키 기반 구조(PKI)의 가장 중요한 역할 중 하나다[1]. PKI 는 전자 인증서를 통해 개인 혹은 기관이 소유한 공개 키를 관리, 감독한다. 이러한 구조는 네트워크상의 통신을 보호하고, 데이터의 무결성을 보장하기에 현재 웹 사이트 연결부터 이메일 보안까지 폭 넓은 분야에서 사용되고 있다. 현재 PKI는 대부분 대형 기관들이 중심이 되는 중앙 집중형으로 관리된다[2]. 인증 기관(CA)는 각각의 키 소유자와 신원 사이의 관계를 검증하고 그 사실에 대한 인증서를 관리한다. 하지만 이러한 중앙 집중형 구조는 single point of failure 문제를 야기시켰으며, 잠재적인 보안 이슈들을 발생시켰다[2]. 대표적으로 2011년에 DigiNotar사에서 발생한 대규모의 위조 인증서 발급 사례는 DigiNotar를 신뢰하는 일반 개인뿐만 아니라 거대 기업에도 피해를 주었다[3].

중앙 집중형 구조로 인한 발생하는 문제를 해결하기 위한 다른 접근 방법은 분산형 구조를 택하는 것이다[4]. Web-of-Trust(WoT)구조는 중심 기관이 없어도 신뢰할 수 있는 보안 관계를 수립할 수 있는 구조로, PGP에 기반을 두었다. WoT구조는 키 소유자가 직접 다른 키 소유자의 공개키에 서명하고 인증하는 방식으로 신뢰 구조를 구축한다. 키 소유자는 자신이 신뢰한 대상이 신뢰한 대상들을 신뢰하는 방식으로 자기가 직접 신뢰 관계를 구축한 대상이 아니더라도 신뢰 구조를 넓힐 수 있다. 또 PGP 프로토콜 상에서 암호화와 복호화에 대한 표준도 존재하기 때문에, PGP를 이용해 신뢰 관계가 구축된 대상들끼리는 신뢰할 수 있는 암호화 통신할 수 있다.

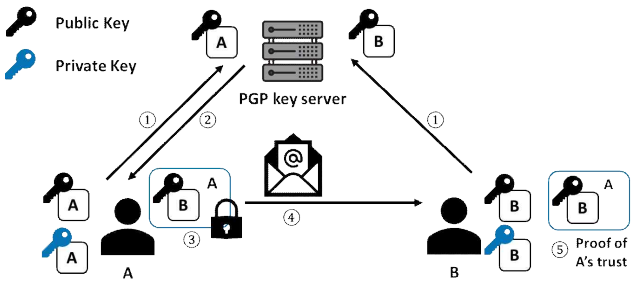

그림 1. PGP에서 다른 개체를 신뢰하는 방법. ① 두 키 소유자 A, B 모두 자신의 공개 키를 키 서버에 올려둔다. ② A가 B를 신뢰하고 싶을 때 A는 B의 공개 키를 키 서버로부터 받는다. ③ 받은 B의 공개 키에 A자신의 개인 키로 서명하고, B의 공개 키를 통해 그 내용을 암호화한다. ④ A는 여러 수단을 통해 B에게 그 내용을 전달한다. ⑤ B는 자신의 개인키로 내용을 복호화하고 해당 내용을 키 서버에 등록해 알린다.

그러나 WoT의 신뢰 구조에는 구조상 문제가 있다. 자신이 신뢰한 대상이 문제가 생겨 그 신뢰를 취소해야 할 때, 취소할 방법이 없다. 이 문제는 자신이 소유한 개인 키로 모든 신뢰 관계에 대한 서명을 했기 때문에 발생한다. 즉 자신의 서명을 무효화 시키기 위해서는 자신이 가진 개인 키를 폐기해야 한다. 이 문제는 만약 신뢰한 대상이 보안 사고에 의해 개인 키가 유출되었을 때 신뢰하면 안 되는 공개 키를 신뢰하게 되는 등 대규모 보안 사고로 이어질 수 있다.

본 논문에서는 OpenPGP 구현을 따르는 GNU Privacy Guard(GPG)를 통해 PGP에 구현된 공개 키 데이터 구조를 이용해 신뢰 관계에 대한 새로운 key를 생성해 신뢰 관계에서 양측 모두 신뢰 관계를 취소할 수 있는

방법을 소개한다.

Ⅱ. 본론

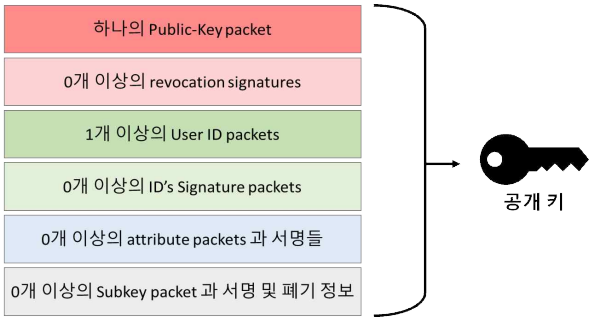

그림 2 PGP에서 사용되는 공개 키 구조

본 논문에서는 PGP에 기본적으로 구현되어있는 공개 키, 개인 키들의 기능을 확장한다. PGP에서 공개 키 혹은 개인 키는 단순히 공개 키 암호화 방식(PKC)에서의 암호학적 키만을 의미하지 않고, 그림 1과 같이 안에 다양한 메타데이터를 넣을 수 있는 구조를 가진다[RFC]. PGP의 공개 키 구조에서 위와 같이 서로 다른 의미를 가진 데이터 단위를 packet이라고 부른다. PGP에서 신뢰의 관리는 외부로 공개된 공개 키에 다른 사람의 신원 정보와 서명을 추가하는 방식으로 관리된다. 만약 받은 서명을 취소하고자 하는 경우 취소하고자 하는 서명의 데이터 일부와 서명 폐기를 의미하는 types number를 메타데이터로 집어넣고 사유와 주석 등을 같이 첨부해 자신의 키로 서명한 후 그 packet을 자신이 소유중인 공개 키 중 해당 서명이 있는 위치 아래에 첨부한다. 그 후 자신의 공개 키를 키 서버 등에 등록하는 방법 등을 통해 공개하면, 다른 사람들은 해당 서명이 과거에는 유효하였으나, 현재는 어떤 이유때문에 유효하지 않다는 것을 알 수 있다. 이 기능은 PGP message format이 처음 정의되고 나서부터 별로 변하지 않고 확장되어 현재까지 사용될 정도로 정교하나, PGP의 구조상 신뢰 관계에서 독립적인 키가 사용되지 않고, 각 대상들의 개인 키가 사용되기 때문에 신뢰 관계에서는 사용되지 않는다.

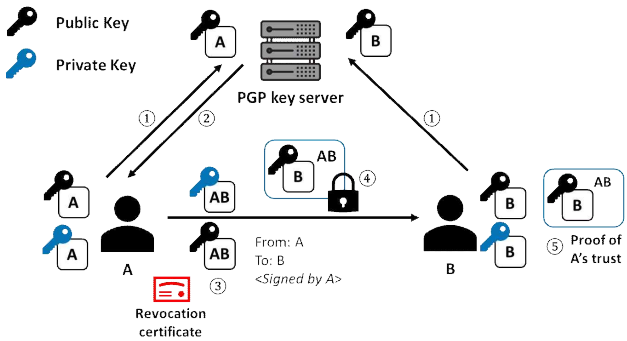

그림 3 양측에서 모두 신뢰를 취소할 수 있는 구조를 위해 새로운 키 페어를 생성하는 과정

본 논문에서는 신뢰를 제공하고 싶은 측에서 PGP에서 정의된 방식대로 새로운 키 페어를 생성한다. 그림 3은 새로운 공개 키의 대략적인 flow를 나타낸 것이다. ①, ②는 그림 1과 같다. ③ A는 새로운 키 페어를 생성한다. 키를 생성할 때 기존 공개 키와 유사하게 구성하되 user ID packet에 신뢰를 하는 측과 받는 측을 명시한다. 그 후 signature packet에 새로운 타입 넘버를 넣어서 이 공개 키과 다른 공개 키와 다른 형식의 공개 키라는 것을 알리고, 신뢰를 제공하고 싶은 측의 개인 키로 서명한다. 키 페어와 함께 함께 표준에 정의된 키 폐기 인증서도 같이 생성한다. 그 후 ④⑤에서 그림 1과 같이 B의 공개 키로 암호화 후 B에게 전송한 후 키 서버에 등록한다.

이 방식을 통해 신뢰를 제공하는 측과 제공받는 측 모두 상황에 따라 신뢰의 제공을 취소하거나 신뢰를 제공받는 것을 취소할 수 있다. 신뢰를 제공하는 것을 취소하기 위해서는 신뢰를 제공하기 위해 생성한 신규 키 페어를 활용해 신뢰를 제공받는 측에서는 모르는 개인 키로 키 폐기 선언을 한 후 신뢰를 제공받는 측의 공개 키를 업데이트하면 된다. 혹은 키 페어 생성 시 같이 만들었던 키 폐기 인증서를 신뢰를 제공받는 측의 공개 키에 첨부하면 해당 키 페어 자체가 폐기되기 때문에 신뢰가 취소된다. 신뢰를 제공받는 것을 취소하기 위해서는 기존 표준에서 지원하는 그대로 자신의 공개 키에 자신의 개인 키로 서명한 키 폐기 선언을 서명 아래에 첨부하면 된다.

Ⅲ. 결론

본 논문에서는 PGP의 키 페어 구조를 활용해 각 대상이 소유한 개인 키를 활용하지 않고 신뢰 관계를 구축하는 방법에 대해 소개한다. WoT를 형성하는 PGP에서 구축한 신뢰 구조는 자신이 과거에 어떤 대상을 신뢰하겠다고 한 선언을 취소할 수 없다는 문제가 있다. 이러한 특성은 WoT 구조에서 한 대상이 개인 키가 탈취당하는 등의 보안 공격을 받았을 때 그 대상을 신뢰한 대상은 신뢰 관계를 취소할 수 없어 악의적인 키를 자동으로 신뢰하게 되는 등 문제가 발생할 여지가 크다. 따라서 본 논문에서는 신뢰 관계에 대한 새로운 키 페어를 생성하는 방법을 제시하여 양측 모두 상대방에 대한 신뢰를 판단하에 취소할 수 있고 WoT구조에서 어떤 대상이 공격당해 신뢰 구조가 위협받아도 각 대상의 책임하에 신뢰 관계를 재구축할 수 있는 방법을 제안한다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2024-2021-0-02048)

참 고 문 헌

[1] H. Finney, L. Donnerhacke, J. Callas, R. L. Thayer, and D. Shaw, "OpenPGP Message Format," Internet Engineering Task Force, Request for Comments RFC 4880, Nov. 2007. doi: 10.17487/RFC4880.

[2] T. Sermpinis, G. Vlahavas, K. Karasavvas, and A. Vakali, "DeTRACT: a decentralized, transparent, immutable and open PKI certificate framework," Int. J. Inf. Secur., vol. 20, no. 4, pp. 553 - 570, Aug. 2021, doi: 10.1007/s10207-020-00518-3.

[3] N. van der Meulen, "DigiNotar: Dissecting the First Dutch Digital Disaster" Journal of Strategic Security, vol. 6, no. 2, pp.46-58, 2013, doi:10.5038/1944-0472.6.2.4

[4] M. Toorani and C. Gehrmann, "A Decentralized Dynamic PKI based on Blockchain." arXiv, Dec. 30, 2020. doi: 10.48550/arXiv.2012.15351.

[5] H. Finney, L. Donnerhacke, J. Callas, R. L. Thayer, and D. Shaw, "OpenPGP Message Format," Internet Engineering Task Force, Request for Comments RFC 4880, Nov. 2007. doi: 10.17487/RFC4880.