사물인터넷 환경에서 단기 인증서 기반 기기 간 TLS 연결에 관한 연구

함초롬, 송정환, 김현수, 정경헌, 권태경*
서울대학교
choromh@snu.ac.kr, jhsong@mmlab.snu.ac.kr, hskim@mmlab.snu.ac.kr,
ghjeong@mmlab.snu.ac.kr, tkkwon@snu.ac.kr

A Study on the device-to-device TLS connection based on Short-lived Certificate in IoT

Chorom Hamm, Junghwan Song, Hyunsoo Kim, Gyeongheon Jeong, Ted Taekyoung Kwon*
Seoul National Univ.

요 약

수 시간에서 수일 동안 유효한 단기 인증서는 인증서 폐기 관리 오버헤드가 없고 짧은 유효 기간을 가지므로 Private key가 탈취되어도 영향이 적다. 사물인터넷 환경에서 안전한 저 지연 연결을 위해 기기 간 직접 TLS 연결이 필요한데, 경량화된 사물인터넷 기기에 단기 인증서를 적용하면 효율적인 관리가 가능할 것이다. 본 논문은 단기 인증서 기반 TLS 연결에 대한 표준화된 프로토콜을 조사하고 이를 응용하여 사물인터넷 환경에서 기기 간 연결에 적용하는 것을 제안한다.

Ⅰ. 서 론

사물인터넷이 급속도로 성장함에 따라 우리 생활과 밀접한 다양한 분야에서 사물인터넷 기술이 사용되고 있다. 사물인터넷 서비스는 몇 가지 특징을 가지는데, 첫째로 다양한 형태의 사물인터넷 기기가 여러 제조사에서 만들어지기 때문에 연결 방식이 다양하며 베터리, 스토리지, 메모리 등이 경량화된 하드웨어 사양을 가지는 경우가 많다. 둘째로, 스마트 홈이나 스마트 오피스와 같이, 사물인터넷 기기와 서비스를 받는 사용자 단말이 근거리에 위치하는 경우가 많다. 또한, 여러 가지 센서를 통해 수집된 데이터에는 사용자의 민감 정보가 포함되어 있을 수 있다. 따라서, 근거리에 있는 사물인터넷 기기와 사용자 단말 간 직접 연결을 통해 데이터를 전송하는 것이 저 지연 서비스 제공 및 프라이버시 보존 측면에도 유리할 수 있다. 이때 데이터가 안전하게 전송되어야 하며 경량화된 사물인터넷 기기에 적합하게 효율적인 인증 방식을 취해야 한다. 기존의 사물인터넷이 구글이나 아마존 등의 클라우드 기반 연결 방식을 사용했기 때문에 사물인터넷 기기와 사용자 단말이 클라우드 서버를 경유 하여 TLS (Transport Layer Security) 연결을 맺고 데이터를 전송했던 반면, 기기 간 직접 연결을 위해서는 사물인터넷 기기가 각각 인증서를 가지고 TLS 연결을 맺는 과정이 필요하다. 사물인터넷 기기에서 웹 기반의 인증서를 그대로 사용할 경우 인증서 발급 및 폐기에 대한 부담이 증가하며 스토리지나 데이터 전송 속도 측면에서도 불리할 수 있다. 따라서, 본 논문에서는 단기 인증서 기반 TLS 연결의 표준화된 프로토콜을 조사하고 이를 응용하여 사물인터넷 기기와 사용자 단말 간 직접 연결 방법에 적용하는 방법을 제안하고자 한다.

Ⅱ. 본론

사물인터넷 기기가 웹 기반의 PKI 인증서를 사용하여 TLS 연결할 경우 인증서 폐기 목록(Certificate Revocation List, CRL)을 관리해야 하는데 이는 경량화된 사물인터넷 기기에서는 부담이 될 수 있다. CRL 관리 오버헤드에는 CRL 분배 및 동기화, 스토리지 및 쿼리 오버헤드가 포함되며 이는 지연 시간을 늘린다. 인증서 유효성 확인에 사용되는 OCSP (Online Certificate Status Protocol)의 경우에도 쿼리로 인한 지연이 발생한다. 따라서 사물인터넷 환경에 적합하도록 오버헤드를 줄이기 위한 관련 연구들이 진행 중이다. Shi(2021)[1]은 다양한 프로토콜의 인증서 폐기 오버헤드에 대해 비교하고 이러한 오버헤드를 줄이는 기법(TinyCR)을 제안하였다. 하지만 수 시간에서 수일 내의 유효 기간을 가지는 단기 인증서를 사용하여 TLS 연결을 하게 되면 인증서 폐기 여부를 확인할 필요가 없으므로 폐기 관리 오버헤드 측면에서 효율적이다.

단기 인증서를 TLS 연결에 활용하는 프로토콜 연구도 진행 중인데, 특히 IETF(Internet Engineering Task Force)에서 표준을 제정한 ACME STAR(Short term, Automatically-Renewed Certificates in Automated Certificate Management Environment)[2]와 Delegated Credential[3]을 들 수 있다. 단기 인증서를 사용하면 폐기 관리에 대한 부담이 없어지는 대신 자주 재발급해야 하는데 ACME는 도메인 유효성 검사, 인증서의 설치와 관리를 자동화하기 위한 프로토콜이다. 인증서 신청자에 대한 검증을 위하여 CA(Certificate Authority)가 요청한 Challenge를 수행하고 검증이 완료되면 URL을 통해 인증서를 발급받을 수 있다. 이러한 ACME 프로토콜에 단기간 유효한 인증서를 자동으로 갱신하는 기능을 추가한 것이 ACME STAR 기법으로, CA와 인증서 신청자 간의 인증서 발급을 위한 절차를 줄이고 발급 시간이 줄어들게 된다. 프로토콜은 STAR 인증서 발급을 CA에게 요청하는 Bootstrap, 발급받은 인증서를 자동으로 갱신하여 URL로 전송하는 Auto-renewal, 인증서의 자동갱신 요청을 취소하는 Termination의 과정으로 이루어진다.

Delegated Credential(DC)은 ACME STAR 인증서와 같이 단기간 유효하며 CA로부터 발급받지 않고 운영자의 역할을 하는 내부 서버로부터 발급받을 수 있다. CDN (Contents Delivery Networks) 등 물리적으로 떨어져 있어 Private key 관리가 어려운 경우, 직접 private key를 보내는 대신 인증서로 생성한 DC를 보내서 TLS 연결에 활용하게 한다. 위임 사용

(DelegationUsage) Extension을 부여한 X.509 인증서를 가지고 있는 내부 서버가 생성하며, 인증서의 Private key로 서명된 신원 보장 자료구조이다. 최대 7일의 유효 기간을 가지므로 폐기 관리가 필요 없고 X.509 인증서보다 경량화된 구조를 가진다. 또한, 인증서 검증에 사용하는 Signature 알고리즘과 DC 검증에 사용하는 Signature 알고리즘을 다르게 정의하는 것이 가능하다. DC 기반 TLS 연결 시, 사용자 단말 등 클라이언트가 DC Extension을 명시한 ClientHello를 보내고 이를 받은 서버가 DC를 지원하는 경우 이를 검증에 활용하여 TLS 연결을 맺을 수 있다.

단기 인증서를 사물인터넷 환경에 적용하면 인증서 폐기 관리의 부담이 없으므로 적합할 수 있으나 이외에 몇 가지 문제점이 발생할 수 있다. ACME STAR 프로토콜을 적용하면 기기가 매번 인증서를 CA로부터 발급받기 때문에, 외부 주체인 CA에 대한 의존도가 여전히 존재하며 네트워크의 오류 등으로 인해 자동갱신되지 않는 경우 안정적인 연결을 저해할 수 있다. 반면, DC 기반 연결을 사물인터넷 환경에 적용할 경우 매번 CA로부터 인증서를 발급받아야 하는 번거로움을 줄이고 내부 운영 서버가 DC 생성 및 관리를 할 수 있는 장점이 있다. 내부 운영 서버가 CA로부터 인증서를 발급받고, 이를 기반으로 DC를 생성하여 사물인터넷 기기 각각에 전달함으로써 인증서의 권한을 위임할 수 있다. 인증서의 Private key 대신 DC를 전송하기 때문에 Private key를 안전하게 보관할 수 있는 장점도 있다. 그러나 DC의 경우에는 최대 7일의 짧은 유효 기간을 가짐에도 자동으로 갱신되지 않기 때문에 운영자가 재발행해야 하는 번거로움이 있을 수 있다. 따라서, ACME STAR의 자동갱신 기능과 Private key를 안전하게 관리하는 DC의 장점을 접목하여 사물인터넷 환경에 적용하면 적합할 것이다.

Ⅲ. 결론

본 논문에서는 수 시간에서 수일간 유효하여 인증서 폐기 관리 오버헤드가 없는 단기 인증서 프로토콜인 ACME STAR와 Delegated Credential 프로토콜을 조사하였다. ACME STAR는 도메인 유효성 검증, 인증서 설치 및 발급을 자동화한 단기 인증서 기법으로 인증서 발급 절차 및 소요시간을 줄이고 자동갱신이 가능하지만, 외부 CA로부터 발급을 받아야 하므로 발급이 부담이 늘게 되고 안정적인 연결이 외부 요인에 영향을 받게 된다. 반면, Delegated Credential은 위임 사용 권한을 부여받은 X.509 인증서를 가진 내부 서버에 의해 생성되고 분배되는 형식으로 외부 CA의 의존도를 줄일 수 있는 장점이 있다. 또한, 인증서의 Private key는 서버에 보관하고 DC를 보내기 때문에 Private key 보관 측면에도 유리하다. 그러나, 단기 유효 기간에도 불구하고 자동갱신되지 않기 때문에 ACME STAR의 자동갱신과 접목하여 사물인터넷 환경에 적용하면, 보다 효율적으로 사용이 가능할 것이다.

ACKNOWLEDGMENT

"This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government(MSIT)." (2022R1A2C2011221)

참 고 문 헌

[1] X. Shi, S. Shi, M. Wang, J. Kaunisto, C. Qian, "On-device IoT Certificate Revocation Checking with Small Memory and Low Latency", ACM SIGSAC Conference on Computer and Communication Security(CCS '21), Nov. 2021. doi:10.1145/3460120.3483580

[2] Y. Sheffer, D. Lopez, O. de Dios, A. Pastor, T. Fossati, "Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME)", RFC 8739, DOI 10.17487/RFC8739, March 2020, <https://www.rfc-editor.org/rfc/rfc8739.pdf>

[3] R. Barnes, S. Iyengar, N. Sullivan, E. Rescorla, "Delegated Credentials for (D)TLS", Nov, 2022, <https://datatracker.ietf.org/doc/draft-rescorla-tls-subcerts>