철도보안인증시스템의 보안인증서 관리에 관한 연구

최현영
한국철도기술연구원
hchoi@krri.re.kr

Study on Certificate Management of Railway Security System

Choi Hyeon Yeong
Korea Railroad Research Institute

요 약

본 논문은 전자인증시 사용되는 보안인증서의 유효성 관리 방법을 분석하고, 철도보안인증시스템의 보안인증서의 유효성을 실시간으로 관리할 수 있는 구조를 제시한다.

Ⅰ. 서 론

열차의 안전한 운행을 위해 열차제어 메시지의 무결하고 안전한 전송이 요구된다. 열차제어를 위한 차상-지상 제어장치 간 주고받는 데이터에 전자인증기술을 적용하여 장치의 인증과 통신 메시지의 신뢰성을 보장하는 철도보안인증시스템이 제안된 바 있다[1]. 이러한 철도보안인증시스템은 철도 운영 및 환경 조건을 반영해야 하며, 특히 열차제어시스템의 가용성을 저해하지 않기 위해 경량화된 보안인증 기술과 이를 위한 인증서 관리 기술이 필수적이다. 본 논문에서는, 전자인증 시 사용되는 보안인증서의 유효성 관리 방법에 대해 고찰하고, 철도보안인증시스템의 보안인증서의 관리 방법을 제시한다.

Ⅱ. 본론

전자인증을 위한 보안인증서는 발급기관(인증기관), 발급자의 전자서명, 소유자, 일련번호, 공개키 정보, 유효기간 등 전자인증에 필요한 주요한 정보를 포함한다. 또한, 보안인증서 생성, 폐지, 갱신 등을 통해 인증서의 관리가 이루어지며, 유효기간 내의 인증서라 하더라도 보안 공격이나 비정상적인 사용이 감지되면 인증서를 폐지하여 인증서의 무결성을 유지한다.

보안인증서 유효성 관리 기술로 인증서폐지목록(CRL: certificate revocation list) 기반의 방법과 온라인 인증서 상태 프로토콜(OCSP: online certificate status protocol)을 이용하는 방법이 있다[2]-[3]. CRL은 유효기간 내의 인증서 중 더 이상 인증서가 유효하지 않을 때 인증기관에서 폐지한 인증서 목록이다. 인증기관에서는 주기적으로 CRL을 생성하고 공지하며, 보안인증서를 사용하는 클라이언트에서는 인증기관이 제공한 URL에서 CRL을 다운로드하여 해당 인증서의 유효성을 확인한다. 그러나 인증기관이 CRL을 갱신하는 주기는 인증기관의 정책을 따르며(일반적으로 24시간 주기), 누적된 CRL의 다운로드 시 부하 발생 및 속도 저하로 인해 실시간으로 보안인증서의 유효성을 검증하는 것은 불가능하다. OCSP는 온라인 인증서 상태 프로토콜이며 인증기관이 OCSP 서버를 운용한다. 클라이언트는 인증서의 유효성 검증을 위해 원하는 인증서 상태 조회 요청을 OCSP 서버로 송신하고, OCSP 서버는 해당 인증서의 상태를 조회하고, 요청에 회신을 준다. 따라서, OCSP는 CRL에 비해 빠르게 응답을 처리할 수 있으나, 다수의 클라이언트가 인증서 상태 요청을 하는 경우 응답지연이 발생할 수 있다.

철도보안인증시스템은 실시간으로 변경되는 열차의 운영 조건에 대응하기 위해 보안인증서의 유효성/무결성 관리에 대한 실시간성이 요구된다. 이를 위해 본 논문에서는 보안인증서의 실시간 유효성 검증 및 관리를 위한 구조를 제시한다. 그림 1은 철도 보안인증시스템의 구성도이며, 보안단말기에서 열차제어 메시지 전자서명/검증, 암복호화 등이 수행되며, 이를 위해 보안 인프라 관리서버와 통신을 통해 보안인증서, 암호화 키 등을 전송받는다. 보안 인프라 관리서버는 보안인증서버와 키관리서버로 구성되며, 통신 보안을 위한 인증서 및 암호화키의 생성, 배포, 삭제, 폐기 등을 관리한다. 이러한 철도보안인증시스템 구조에서, 보안인증서의 실시간 유효성 검증 기능은 CRL 배포관리자에 의해 수행되는 구조를 제시한다. 보안인증서 폐지 이벤트 발생 시, CRL 배포 관리자를 통해 실시간으로 CRL 업데이트를 통지하여 최신의 CRL을 유지하고 인증서 유효성 검증의 실시간성을 확보한다.

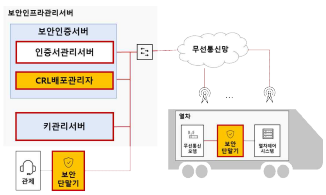

그림 1. 철도보안인증시스템 구조

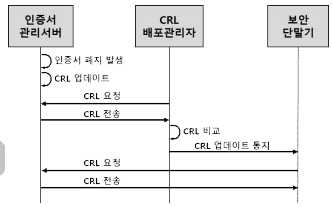

그림 2. CRL 업데이트 절차

그림 2는 실시간 CRL 업데이트를 위한 시퀀스 다이어그램이다. 인증서 폐지 이벤트가 발생하면 인증서관리서버에서 CRL을 업데이트한다. CRL 배포관리자는 인증서 관리서버에 CRL을 요청하여 전송받고, 기존 저장된 CRL과 비교하여 CRL의 업데이트 여부를 확인한다. CRL이 업데이트 되면 보안단말기에 통지를 한다. CRL 업데이트 통지를 받은 보안단말기는 인증서 관리서버에 CRL을 요청하여 CRL을 다운로드한다. 이러한 과정을 통해 실시간으로 CRL 업데이트를 확인하고 최신의 CRL을 유지하여 보안인증서 유효성 검증의 실시간성을 확보할 수 있다.

Ⅲ. 결론

본 논문에서는 CRL 배포관리자를 통해 실시간으로 CRL의 갱신 확인 및 다운로드가 가능한 철도보안인증시스템 구조를 제시하였으며, 이를 통해 실시간으로 보안인증서의 유효성 검증이 가능할 것으로 기대한다.

ACKNOWLEDGMENT

본 연구는 한국철도기술연구원 주요사업의 연구비 지원으로 수행되었습니다.

참 고 문 헌

[1] H. Y. Choi, JKSR, 24(12), pp. 1090-1100 (2021)
[2] RFC 5280, IETF (2008)
[3] RFC 6960, IETF (2013)