[ITS] 차세대 지능형 교통시스템(C-ITS) 보안 기술 표준화 동향

개요

차세대 지능형 교통시스템(C-ITS: Cooperative Intelligent Transport Systems)이란 도로, 차량, 신호시스템 등 기존 교통체계의 구성요소에 전자, 제어, 통신 등 첨단기술을 접목시켜 교통시설의 효율을 높이고, 안전을 증진하기 위한 차세대 교통 시스템을 의미한다. 즉, 지능형교통시스템은 사람이 두뇌의 조절과 제어 기능에 의해 신체가 움직이듯이 기존의 교통시스템에 인공지능을 갖추어 정보를 제공하고, 그 정보를 통하여 교통시설이 상황에 따라 자동 제어되어 이용자에게 최대한 편의를 제공하는 시스템이다. 하지만 이러한 지능형 교통시스템의 경우 보안에 대한 준비가 제대로 갖춰지지 않을 경우 일시적으로 교통마비 및 대형 교통사고를 유발할 수 있고, 이에 따라 운전자의 생명에도 직접적인 영향을 미칠 수 있기 때문에 그 중요성이 더 증가하고 있다. 지능형 교통시스템(ITS)의 경우 ISO TC204 WG9에서 주로 국제표준화를 추진 중에 있으며, 최근 ITU-T에서도 SG16 Question27에서 지능형 교통시스템 관련 응용/서비스 및 기능 요구사항들에 대한 표준을 개발 중에 있다. 또한, ETSI Technical Committee, Car2Car Communication Consortium(C2C-CC), CAMP(Crash Avoidance Metrics Partnership) 등의 표준화 단체에서도 C-ITS 및 스마트 카 관련 표준을 개발 중에 있으며, ITU-T SG12의 경우 ITS 서비스 성능 향상 방법 및 성능 레벨에 대한 표준을 개발하고 있다. SG17에서는 지능형 교통시스템(ITS) 보안 분야 표준화를 담당하고 있으며, 본 표준화 보고서는 지난 2015년 4월 8일부터 4월 17일까지 스위스 제네바에서 개최된 ITU-T SG17 정기회의에서 논의된 지능형 교통시스템 보안(V2V communication 보안) 관련한 동향을 소개하고자 한다.

차세대 지능형 교통시스템(C-ITS) 보안 기술의 필요성

최근 CES 2015 및 MWC 2015 등을 통해 IoT에 대한 관심과 다양한 IoT 기반 융합서비스들이 소개됨에 따라 이용자들의 기대심리도 더욱 증가되고 있다. 특히, 스마트 카를 중심으로 하는 차세대 지능형 교통시스템 관련한 관심이 지속적으로 확대되고 있다. 이에 따라, 자동차제조사, 이동통신사, 칩제조사 등의 산업체 위주로 구성된 협의체뿐만 아니라 ITU-T, ISO, ETSI, oneM2M

등 다양한 기구에서 관련 기술에 대한 표준화 연구가 활발히 진행되고 있으며, 차세대 지능형 교통시스템의 경우 운전자에게 직접적인 인명피해를 줄 수 있는 분야이기 때문에 보안 분야에 더욱 관심을 기울이고 있는 실정이다. 더욱이 차량과 연계된 교통망 서비스의 경우 한번의 해킹으로 국가차원의 대규모 피해를 입힐 수가 있어 해커들의 공격 목표가 되기 쉽다. 따라서, 교통대란, 자동차 사고 유발 등 사람에게 직접적인 피해가 갈 수 있는 지능형 교통 시스템의 경우 특별히 해킹 사고를 방지하기 위한 다양한 기술 개발 및 이에 대한 표준화 연구가 시급하다 할 수 있다. 지능형 교통시스템 보안과 관련한 표준 기술은 차량과 차량, 차량과 인프라, 차량과 단말기 간의 보안 통신 기술이 필요하며, 스마트 카의 안전성 보장을 위한 소프트웨어 업그레이드 절차 및 방법에 대한 기술, 정보를 상호 전송하는 차량(Vehicle)에 대한 인증 기술, 교통신호제어기에 대한 해킹 방지 기술 등이 있다. 이러한 보안 기술들이 보장이 되지 않을 경우, 운전자에게 악의적인 정보로 인한 사고가 유발될 수 있고, 대형 교통사고로도 확산이 될 수 있기 때문에 본 기술들에 대한 개발 및 표준화가 중요하다고 할 수 있다.

차세대 지능형 교통시스템(C-ITS) 보안 기술 표준화 진행 상황 및 표준화 회의 결정사항

현재 SG17 Question 6에서 추진하고 있는 차세대 지능형 교통시스템(C-ITS) 보안 기술 표준화는 총 2건이 있으며, 두 건 모두 2014년 9월 회의에서 신규 표준화 과제로 채택되어 개발 중에 있는 권고안이다. 첫 번째 권고안은 “ITS 통신 디바이스를 위한 소프트웨어 업데이트(X.itssec-1)”이며, 해당 권고안은 스마트 카 등 ITS 통신 디바이스에 불법 소프트웨어 업데이트를 방지하기 위한 기술을 정의하는 권고안으로 원격 소프트웨어 업데이트를 위한 기본 모델 제시, 보안 위협 분석, 소프트웨어 업데이트를 위한 보안 기능 요구사항 및 구조 등을 제안하고 있다. 본 권고안은 2015년 4월 회의를 통해 소프트웨어 업데이트를 위한 기본 모델과 위협/취약점 분석 등을 기고하였으며 SG17 회의를 통해 해당 기고 내용을 권고안에 모두 반영하는 것으로 결정되었다. 두 번째 권고안은 “V2X 통신 시스템을 위한 보안 가이드라인(X.itssec-2)”으로써 차량간(V2V), 차량과 인프라간(V2I), 차량과 단말기간(V2N) 등에서 필요한 보안 요구사항을 정의하고 있다. 또한, 본 권고안은 V2V, V2I, V2N 각각에 대한 보안위협 및 취약성 분석, 보안 요구사항, V2X 보안 시스템을 위한 Use Case 등으로 구성되어 있다. 2015년 4월 정기회의에서는

두 개의 레퍼런스 모델에 대해 제시하였으며, SG17 회의를 통해 권고안에 모두 반영하는 것으로 결정되었다. 두 권고안 모두 아직은 개발 시작 단계이기 때문에 완성도 면에서는 많이 부족하지만 차기 회의부터 지속적으로 개발해 나간다면 2017년에는 권고안이 개발 완료될 것으로 예상한다.

차세대 지능형 교통시스템 보안 기술 표준화 관련 시장 전망 및 국내 표준화 활동에의 제언

차세대 지능형 교통시스템 보안 기술의 경우 현재 각국의 정부뿐만 아니라 전세계 자동차 개발 업체들로부터 많은 관심과 개발이 진행되고 있는 기술이기 때문에 국내 자동차 업계에서도 많은 관심이 필요하다. 물론 이미 현대/기아 자동차가 관련 기술 개발에 참여하고는 있지만 해당 기술 이외에도 자동차 지능화 및 교통 정보 지능화 관련 시장은 앞으로 지속적으로 발전할 수 있는 시장이기 때문에 관련 업계의 적극적인 기술 개발 노력이 필요하다.

이미 국내에서도 2012년 6월에 국토해양부(현 국토교통부)에서 도로교통 분야 ITS의 개발·보급 촉진을 통한 저비용·고효율의 미래형 스마트 교통SOC 구축을 위해 '자동차·도로교통 분야 ITS 계획 2020'을 수립하였으며, 2015년 3월에는 국토교통부에서 차세대 ITS 시범 사업을 본격 착수한다고 발표하였다. 이렇듯 차세대 지능형 교통시스템 분야는 현재 정부에서 많은 관심과 지원을 하고 있기 때문에 이를 활용하여 보안 업계에서도 적극적인 차세대 ITS 보안 기술 개발 및 국제 표준화 개발을 통해 국내 우수 기술에 대한 국제 경쟁력 강화뿐 아니라 국내 우수 기업들이 국외에 진출할 수 있는 계기를 마련하여야 할 것이다.

백종현 (KISA 팀장, ITU-T SG17 Q6 라포처, jhbaek@kisa.or.kr)