"자동차보안" 특집호 발간에 즈음하여

2010년 Univ. of Washington 연구팀은 자동차의 전장화로 인한 사이버공격 가능성을 IEEE S&P 학회에서 발표하였다. 이후 2013년 Defcon에서 Charilie Miller와 Chris Valasek의 자동차 해킹 시연은 산업계에서도 자동차 보안에 대한 많은 관심을 불러 일으켰다.

운전자의 편의성 및 안정성 (Safety) 향상을 위하여, 최근 자동차에는 전기 및 전자 장비들이 탑재되고 있다. 특히, 높은 수준의 자율주행 레벨을 위해서는 모터, 모듈, 센서, 제어기 등과 같이 많은 수의 전장 장비들이 계속해서 자동차에 탑재될 것으로 예상되며, 이로 인해 자동차에 대한 사이버 공격 위협도 함께 증가될 것이다. 유럽경제위원회 (UNECE) 산하 자동차 기준 국제조화회의 (WP.29)에서는 2020년 자동차 사이버보안에 관한 법규 (UN Regulation No. 155: Cybersecurity Regulation)을 채택하였다. 해당 법규에 따르면, 2022년 7월부터 UNECE 회원국에 등록되는 신형 자동차의 차량 형식승인을 받기 위해서는 자동차 사이버보안 관리체계 (Cybersecurity Management System, CSMS)에 대한 인증을 의무적으로 취득해야 한다. 또한, 기존에 이미 개발되어 있는 자동차의 경우라 할지라도 2024년 7월까지 CSMS 인증을 취득해야 해당 차량들을 판매할 수 있게 된다. 즉, 자동차 제조사와 부품사들은 자동차 Life Cycle 전반에 걸쳐 준수해야 할 사이버보안 요구사항과 증빙 자료를 구체화해야 하는 등 자동차보안에 대하여 적극적이고 선제적인 참여 및 대응 전략이 필요해지고 있다.

본 특집호에서는 자동차 사이버공격 대응을 위한 가상화 사이버훈련 개발환경 구축 사례에 대하여 살펴보았다. 또한, 최근 미국 10대들 사이에서 'Kia Challenge'라 불리면서 이슈가 되었던 자동차 스마트키 시스템 보안 연구 동향에 대해서도 살펴보았다. 앞으로 자율주행자동차의 자율주행 레벨의 고도화되었을 때 운전자 또는 제조사의 책임소재 여부를 판단할 수 있는 디지털운행기록 장치 데이터 보안 및 자동차 포렌식에 대한 연구 동향도 함께 살펴보았다. 게다가, 향후 자동차 내부 네트워크에 사이버 공격이 발생하였을 때, 침입원점에 대한 식별기술 연구동향에 대하여 살펴보았다. 마지막으로, Automotive Ethernet으로 자동차 내부네트워크 통신 프로토콜이 대체됨에 따라 Ethernet 상에서의 Middleware 통신 프로토콜인 ROS의 보안 연구 동향에 대하여 살펴보았다. 본 특집호를 바탕으로 학계뿐만 아니라 산업계에서도 자동차보안에 대한 중요성을 인지하고 관련 기술 개발에 대한 지금보다 더 적극적인 투자 및 관련연구가 진행되었으면 하는 바램이다.

끝으로 바쁘신 중에도 소중한 시간을 내시어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회, 그리고 학회 사무국 관계자 여러분께 감사를 드립니다.

2023년 8월

고려대학교 정보보호대학원 교수 최 원 석

"정보보호 국제표준화 동향" 특집호 발간에 즈음하여

국제표준화 대면 활동이 COVID-19로 인하여 단절되었다가, 점점 회복하는 과정에 있다. COVID-19의 후유증으로 경기가 침체 국면에 접어들면서, 국제활동에 국력의 차이가 표출되고 있다고 생각된다. 그중 하나는 유럽의 공항에 가보면 한국이 자동심사로 구분되어 있어서, 입국심사가 훨씬 자유롭고, 편해졌다. 그리고 한국어로 인사를 하며, 한국어를 할 수 있음을 과시하는 공항 직원들을 만나는 것은 마음속에 잔잔한 미소를 띄우게 하며, 한국민에 대한 자부심과 즐거움이 돋아나는 순간을 경험하게 된다.

정보보호 분야에서 새로운 기술들이 두각을 나타내고 있다. 메타버스, AI/ML, IMT 2030(6G), 블록체인, 자율주행, Zero Trust, Supply chain 등과 연계한 정보보호 표준개발을 위하여 국내의 기술 및 정책에 맞추어 활발하게 구도를 재정비하고 있다. 특히 오픈소스 활용으로 인하여 정보보호의 중요도가 더욱 강화되고 있으며, Supply chain을 중심으로 OpenAI, IMT 2030(6G)의 개방성 등으로 인하여 취약점이 다수 발생될 것이 예측되고 있으며, 이에 대응하는 정보보호 기술 및 표준 개발이 시급한 상황이다. 오픈소스 생태계와 관련하여 취약점 분석과 보안패치 관리, 라이선스 컴플라이언스, 개인정보보호, 지식재산권 보호 그리고 외부업체와의 협업/관리등과 같은 주제들에 대한 표준개발이 요구되고 있다.

본 특집호에서는 국내 정보보호 표준전문가들의 주요 활동무대인 ITU-T SG17 (Security), ISO/IEC JTC 1/SC27 (Information security, cybersecurity and privacy protection), ISO TC307 (Blockchain and Distributed ledger technology), ITU-R WP5D (IMT Systems) 등의 국제표준화 그룹에서 진행되고 있는 표준화 동향을 살펴본다. ITU-T SG17에서는 차기 회기(2025-2028)의 구조에 대한 논의와 함께, 양자암호, 차량통신 보안 관련 표준화 작업이 진행되고 있으며, ISO/IEC JTC1/SC27에서는 암호기술, 적합성평가 및 개인정보보호 표준화와, ISO/TC 307에서는 탈중앙 신원관리, NFT 및 감사 표준, ITU-R WP5D에서는 IMT 2030(6G) 통신시스템에 대한 지능형 보안관제 및 정보보호 표준화가 집중되고 있다.

끝으로 바쁘신 중에도 소중한 시간을 내시어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회, 그리고 학회 사무국 관계자 여러분께 감사를 드립니다.

2023년 8월

ETRI 사이버보안연구본부 전문위원 나 재 훈