"메타버스, NFT, AI, 자동차 등 신기술 대상 신종위협 및 대응" 특집호 발간에 즈음하여

2016년 1월 스위스 다보스에서 열린 세계경제포럼에서 처음으로 4차 산업혁명이 언급된 이후, 현재까지 우리는 정보통신기술이 급속도로 변화하고 발전하고 있는 지식혁명시대를 살아가고 있다. 특히, 인공지능(AI), 사물인터넷(IoT), 자율주행 자동차, 가상현실(VR), 증강현실(AR), 메타버스, 대체불가토큰(NFT) 등 다양한 신기술들이 가져올 변화에 대한 기대가 높은 상황이다. 그리고 모바일, 웨어러블, 드론 등 다양한 스마트 기기의 수와 사용자 수 역시 폭발적으로 증가하고 있는 가운데, 운전자의 미개입이 가능한 자율주행 기술의 일부가 적용된 차량의 상용화를 2024년에 달성할 것으로 예측되고 있어, 결국 자율주행차량 역시 IoT 기기들의 한 종류처럼 다뤄질 것으로 전망된다.

하지만, 새로운 기술들에 대한 기대감과 함께, 다양하고 복잡해지는 정보통신기술들을 대상으로 하는 신종 사이버 보안 문제들에 대한 관심과 걱정도 커지고 있다. 스마트 엣지 기기들과 자율주행 자동차들에서 사용되는 System-on-chip (SoC)의 종류가 다양화되고 있고, 하드웨어의 복잡도도 증가하는 한편, 다양한 프로그래밍 언어로 구현되는 소프트웨어의 종류와 복잡도도 증가하고 있다. 이처럼 빠르게 변화하는 정보통신기술의 발전이 가져올 새로운 컴퓨팅 환경에서는 기존 사이버 보안 위협들을 포함하여, 현재까지는 나타나지 않았던 새로운 보안 문제점들이 충분히 발생할 수 있다. 따라서 신기술들을 대상으로 다각화된 공격모델을 제시해 줄 수 있는 선제적인 연구가 반드시 필요한 상황이다. 그리고 변화하는 환경에 맞는 유연한 보안 솔루션의 확장과 개발을 가져올 수 있는 혁신적인 연구가 필요하다.

본 특집호에서는 인공지능 기술을 이용하는 차량용 침입 탐지 시스템들을 대상으로 차량용 내부 네트워크인 CAN을 이용해 다양한 공격을 진행하고 분석한 내용에 대해 살펴보고, 기계학습 모델을 사용하여 Custom Memory Allocator를 탐지하고 이를 통한 메모리 안정성 강화 연구의 결과를 소개한다. 다음으로, 메타버스 서비스 이용 환경, 가상 환경 및 디지털 트윈 환경에서 발생할 수 있는 보안 위협 요소들에 대해 소개하고, 메타버스의 변화에 따라 다양해지는 ID 관련 보안 위협과 대응 기술의 현황 및 메타버스 범죄 동향과 디지털 포렌식 대응 방안에 대해서 살펴볼 것이다.

끝으로 바쁘신 중에도 소중한 시간을 내시어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회, 그리고 학회 사무국 관계자 여러분께 깊은 감사의 마음을 전합니다.

2022년 8월

숭실대학교 소프트웨어학부 교수 조 해 현