“IoT에 최적화된 강력한 임베디드 보안 솔루션 필요하다”

▶▶ **스테판 스카린(Stefan Skarin)** IAR시스템즈 CEO

임베디드 시스템 애플리케이션 개발을 위한 소프트웨어툴을 제공하는 스웨덴 기업 IAR시스템즈(IAR Systems)가 커넥티드 디바이스(Connected Device)에 최적화된 새로운 보안 솔루션 ‘임베디드 트러스트(Embedded Trust)’를 전세계 공식 출시했다. 지난 4월 11일 서울 여의도에서 진행된 ‘IAR 개발자 포럼 2018’을 위해 한국에 방안한 스테판 스카린(Stefan Skarin) IAR시스템즈 CEO를 직접 만나 IAR시스템즈가 지향하는 보안 솔루션과 향후 계획에 대해 들어봤다.

이나리 기자 (eled@hellot.net)

여러 시장조사기관에서 발표했듯이 향후 몇 년 안에 모든 사물이 네트워크로 연결되는 본격적인 IoT(사물인터넷) 시대를 앞두고 있다. 2025년이 되면 IoT로 연결되는 커넥티드 디바이스가 70억개가 되고, IoT 매출은 3조 달러가 될 전망이다.

그러나 현재 임베디드 보안 기능을 갖춘 IoT 디바이스는 4% 미만으로, 아직까지 기술 발전에 비해 보안에 대한 대비가 부족하다는 것을 알 수 있다. 2022년까지 보안 디바이스는 새로운 IoT 디바이스가 차지하는 비중이 20%에 달할 것이다. 이는 IoT 디바이스 뿐만 아니라 커넥티드 카로 구현되는 자율주행차에도 보안 문제가 당연히 대두된다.

스테판 스카린 CEO는 "보안은 더 이상 선택 사항이 아닌 필수이며, 신뢰의 문제다. 지적 재산 보호, 중요 인프라 보장, 제품 라이프 사이클 관리 등에 있어서 개발 초기부터 보안을 고려해서 설계해야 한다"며 "우리는 고객사에게 보안에 대한 중요성을 알리고, 그들이 직면한 보안 문제를 이해하고 솔루션을 제시해야 할 책임이 있다"고 강조했다.

IAR시스템즈는 보안 기술을 강화하기 위한 전략으로 2017년 IoT 보안 솔루션 강자인 시큐어씽스(Secure Thingz)를 인수 했다. 시큐어씽스는 영국 캠브리지에 2016년 설립된 기업이며, 22년의 보안 기술 경력을 갖춘 Arm IoT 시큐리티 파운데이션의 창립 멤버가 설립한 기업이다.

이를 시작으로 IAR시스템즈는 2018년 2월 독일에서 개최된 '임베디드 월드'에서 IoT 보안 솔루션 '임베디드 트러스트'를 첫 공개했고, 지난 4월 '임베디드 트러스트 1.2'를 공식 출시했다. 내년 2월에는 2.0 버전을 공개할 예정이다.

임베디드 트러스트는 IAR의 기존 솔루션인 임베디드 워크벤치(Embedded Workbench)에서 보안 코드 단계를 더 추가해서 보안 코드가 유출되지 않게 강화시켰다. 따라서 임베디드 트러스트는 최적화된 C/C++ 컴파일러와 다양한 기능의 C-CPY 디버거를 포함하는 임베디드 워크벤치의 개발 툴 체인과 완벽하게 통합된다. 이런 개발환경은 차세대 MCU에 내장된 보안 아키텍처를 활용해 신뢰성 높은 IoT 솔루션 개발을 가능하게 한다.

임베디드 트러스트의 핵심 기능은 최적화된 보안 개발 환경이다. 따라서 고유한 디바이스 ID 생성, 안전한 애플리케이션 개발, 제조 마스터링을 포함해 모든 보안 기능을 개발하기 위한 환경을 제공한다. 또 보안 부팅매니저를 사용자 정의에 따라 제품에 적합한 보안 레벨을 얻을 수 있다. 이런 확장성 덕분에 여러 공급업체의 다양한 디바이스에 대한 표준화된 워크플로우를 얻을 수 있다.

"보안은 더 이상 선택 사항이 아닌 필수이며, 신뢰의 문제다. 지적 재산 보호, 중요 인프라 보장, 제품 라이프 사이클 관리 등에 있어서 개발 초기부터 보안을 고려해서 설계해야 한다"

보안에 있어서 인증, 승인, 부안 방지, 기밀통신을 제공하는 ID는 시스템의 핵심이다. 임베디드 트러스트는 간소한 보안 관리를 위해 ID와 인증서 구성자를 통합함으로써 인증서 계층 구조가 여러 제품 범위에 걸쳐 있는 방식을 시각화 할 수 있다. 또 보안 부팅 관리자 기능은 디바이스 하드웨어를 보호하고, 코어에서부터 RTOS 또는 애플리케이션 상에서 작동하는 실행, 관리, 업데이트 기능까지 손쉽게 구성할 수 있게 한다. 무엇보다도 마스터링 절차를 통해 개발자 인증서를 공식 제조 인증서로 전환할 수 있어 펌웨어 누출을 사전에 방지할 수 있다. 코드는 대상 디바이스에 대해 서명되고, 암호화돼 악성코드를 추가할 수 없고, 대상 디바이스에서만 코드가 실행된다. 또 버전 관리와 업데이트 인프라를 이용한 제품 출시를 관리할 수 있다.

스테판 스카린 CEO는 "실제로 최근 중국의 제조 공장에서 IP와 코드를 훔쳐서 주문생산량에 큰 피해를 입힌 사건이 있었다. 기업은 코드와 데이터 보호뿐 아니라 지적 재산 보호를 위해 보안의 중요성을 인지해야 한다"며 "IAR 시스템즈는 개발에서부터 제조까지 강력한 보안 솔루션을 제공하겠다"고 전했다. EE