“IoT 보안, 시스템·애플리케이션 개발 초기단계에 적용해야”

스테판 스카린 IAR시스템즈 CEO, “IoT 단말 중 4%만이 보안 적용”

스테판 스카린(Stefan Skarin) IAR시스템즈(IAR Systems) CEO

IT자원의 클라우드화(化), 차세대 이동통신망 구축, 다변화돼 출시되고 있는 사용자 서비스로 사물(Thing) 간 연결이 빠르게 증가하고 있다. 가트너는 2025년 전세계 IoT로 연결된 커넥티드 디바이스가 70억개에 달할 것으로 전망한다. 이는 단순 전망치로 실제 연결되는 단말은 클 것으로 관련 시장에서는 예상하고 있다.

연결성이 가속화되면서 보안 이슈도 등장했다. 통계에 따르면 전세계 기업 20%가 최근 3년간 1회 이상의 IoT 타깃 사이버공격을 당한 것으로 알려졌다. 2018년 기준, 관련된 보안 지출규모도 전년비 28%가 늘었다.

시스템·애플리케이션을 구동하는 소스코드(Source Code)가 복잡해지면서 개발자들도 고민이 많아졌다. 소비자시장(B2C) 대비 기업시장(B2B)에서의 가능성을 더 크게 인정받고 있는 5G 통신망이 상용화되면 잘못된 코드 하나가 시스템 장애로 이어질 수 있어 고수준의 검증도 필요하다. 메모리·전력 사용을 줄이기 위해 코드수도 줄여야 한다.

노드 취약점을 타고 들어오는 해킹 방지와 같은 보안 이슈에도 대응해야 한다. 다수의 기업들이 엔드포인트/게이트웨이 단에서의 사이버공격 이슈에 중점을 두고 있으나 수억개의 노드에서 취약점을 타고 침입한 공격자를 100% 방어할 수는 없다.

그간 코드의 오류검증에 집중해왔던 개발자들도 IoT 디바이스를 기획하고, 설계하는 초기단계에서부터 배포로 이어지는 체인 안에서 유기적으로 확장·구성 가능한 보안환경 구축, 개발된 코드에 대한 지적재산권(IP)을 보호할 수 있는 장치에 관심을 두고 있다.

IT비즈뉴스(ITBizNews)는 컴파일러 툴 글로벌 기업인 IAR시스템즈(IAR Systems)의 스테판 스카린(Stefan Skarin) CEO와 만나 엣지투클라우드 연결성 가속화로 인한 개발자들이 도전한 직면과제와 향후 전망에 대해 들어봤다.

Q. IoT 보안 이슈가 전세계적으로 늘고 있다. 올해 전망은 어떻게 보는가?
A. 보안은 올해에도 IoT 디바이스를 개발사에게 있어 중요한 초점이 될 것이다. 모든 회사는 제품이 성공하기를 원한다. 허나 시스템, 프로세스·애플리케이션의 약점은 재공정을 통해 IP를 도용하거나 제3자 제조사가 원하지 않는 생산배치를 실행하면서 악용될 가능성이 높다. 이는 기업 입장에서는 아주 큰 손실이다.

실제로 시스템 손상은 요즘의 현실이다. 사소한 실수라도 중대한 결과를 초래할 수 있다. 보안을 구현하는 것은 종종 어려운 것으로 간주된다. 고려해야할 매개 변수가 많기 때문이다.

출발점은 디바이스·하드웨어 자체에 있다. 강력한 보안을 구현하는 유일한 방법은 개인 키, 제품 인증서, 보안 부트 기능을 보유한 신뢰할 수 있는 컴퓨팅 기반을 제공하면서 인증·증명과 같은 서비스를 수행 할 수 있는 보안 초기 단계인 RoT(Root of Trust)를 사용하는 것이다. 최근에는 프로세서 제조사가 다양한 보안 하드웨어 모듈을 출시하고 있다. 앞으로도 많은 보안 MCU가 출시 될 것으로 예상된다.

중요한 건, 하드웨어가 전부가 아니다. 하드웨어 기능을 활용하려면 소프트웨어가 필요하다. 이를 위해 우리는 개발 초기 단계에서부터 보안이 포함 된 워크플로우 구축을 위해 시큐어씽즈(Secure Thingz)와 협력을 추진해왔다.

Q. 지난해 씨큐어씽즈를 인수하고 '임베디드 트러스트(Embedded Trust)'를 발표했다
A. 우리는 시큐어씽즈의 솔루션과 보안 기술이 연결된 디바이스와 제품에 필요한 보안 기능을 완벽히 제공할 수 있다고 믿는다. 임베디드 트러스트는 개발자 보안 환경을 쉽게 구축할 수 있도록 지원하며 개발 초기단계에서 배포까지 일괄된 체인 안에서 보안환경을 제공하는 툴이다.

이는 임베디드 워크벤치(IAR Embedded Workbench) IDE와 통합된 보안개발환경으로 MCU에 내장된 보안 하드웨어를 활용, 신뢰할 수 있는 IoT 솔루션에 필요한 저수준 트러스트 앵커와 보안 서비스를 제공한다. 지난해 말 파트너사를 대상으로 배포된 상태며 올해 다양한 제품들이 출시될 것으로 예상한다.

Q. 엣지-투-클라우드가 빠르게 전개 중이다. 애플리케이션 디자인에 부문에서는 중요한 이슈로 보이는데

A. 우리는 업계에서 35년 간 파트너사와 같이 해오면서 다양한 과제와 니즈를 적극 반영해왔다. 예상했던 대로, 임베디드 시스템·애플리케이션 개발이 복잡해지면서 개발사는 코드 품질에 대한 우려가 크다.

지난 몇 년간 새로운 기회를 창출 할 수 있는 핵심요소로 연결성, IoT가 부상하면서 이와 관련된 보안 이슈가 발생했다. 커넥티드 환경에서의 보안은 성공의 필수요소다.

현재 전세계 연결된 IoT 디바이스의 4%만이 보안을 내장하고 있다. 자체 보고서를 근간으로, 이 수치는 2022년에 20%로 늘어날 것이다. 보안 이슈의 핵심은, 시스템 개발 시작단계에서부터 통합돼야 한다는 점이다. 개발 프로세스의 후반부에 보안을 추가하는 것은 거의 불가능하기 때문이다.

아울러 IoT 보안은 간단하고 확장 가능해야 한다. 보안을 설계 프로세스에 통합하는 것이 장기적이고 견고하며 확장 가능한 보안을 달성하는 최선의 방법으로 볼 수 있다. 관련 기술을 적용하는 방법도 쉬워야 한다. 이렇게 해야만 고객사가 지적자산을 보호하고 신뢰할 수 있는 제품 개발을 가속화하면서 TCO를 줄일 수 있는 순환구조를 만들 수 있다.

Q. 자체적으로 구상하고 있는 개발자 에코시스템이 있는가?

A. 앞서 언급했듯 우리는 오랫동안 업계에서 고객의 요구를 반영해왔다. 우리는 8비트와 16비트로, 또 32비트로의 전환을 경험해왔다. ARM의 진화와 이것이 전세계의 고객사·개발자는 물론 관련 산업계에 어떤 영향을 끼치는지 봐왔다.

최근에 흥미로운 트렌드를 보자면 RISC-V의 움직임이다. IAR은 지난해 RISC-V 파운데이션에 가입하고 에코시스템 확장 및 아키텍처 툴을 제공하고 있다. 다수의 칩 벤더들과 파트너십도 확대하고 있다.

첨언하자면, 향후 인공지능(AI)/머신러닝(ML)과 같은 기술이 빠르게 고도화되면서 새로운 혁신적인 제품과 서비스가 출시될 것이다. 특히 자동차산업(오토모티브)에서 이러한 신기술이 빠르게 도입되면서, 자동차가 '데이터 플랫폼'으로 자리하면서 중요한 산업시장으로 부상할 것이다. [ITBizNews 최태우 기자]