NXP, 혁신적인 엣지락™ 보안 엔클레이브로 수십억 IoT 디바이스에 대한 보안 관리 단순화

2021년 3월 2일 – NXP 반도체는 사물 인터넷(IoT) 엣지 디바이스를 공격이나 위협으로부터 지능적으로 보호할 수 있는 사전 구성된 자율 관리형 온다이(on-die) 보안 서브시스템인 엣지락(EdgeLock)™ 보안 엔클레이브(enclave)를 발표했다. NXP의 신규 i.MX 8ULP, i.MX 8ULP-CS 및 i.MX 9 애플리케이션 프로세서에 내장된 보안 서브시스템으로 완벽 통합된 제품으로, IoT 애플리케이션에 대한 강력한 시스템 차원의 보안 인텔리전스 구현의 복잡성을 줄일 수 있다.

개발자는 이 보안 엔클레이브를 통해 보안 목표를 보다 쉽게 달성할 수 있으며, 엣지 애플리케이션을 차별화하는 새로운 방법에 더 집중할 수 있다. 보안 엔클레이브를 엣지버스 프로세서 제품군에 통합함으로써 NXP는 스마트 홈 디바이스, 웨어러블, 휴대용 의료 기기, 스마트 어플라이언스, 임베디드 제어 및 산업용 IoT 시스템을 포함한 수천 개의 엣지 애플리케이션에 최첨단 보안을 쉽게 구현할 수 있는 광범위한 확장성 옵션을 개발자에 제공한다.

울프강 스타인바우어(Wolfgang Steinbauer), NXP 부사장 겸 암호화 및 보안 부문 총괄은 "엣지에 배치된 수십억 개의 IoT 제품이 사이버 공격의 매력적인 표적이 되고 있다. 강력한 격리를 기반으로 하는 보안 프레임 워크를 제공함으로써 디바이스 제조업체는 기능성에 집중하고, 보안에 대해서는 NXP의 검증된 보안을 활용할 수 있다. NXP는 엔드 투 엔드(end-to-end) 보안 솔루션을 제공해 온 강력한 경험을 토대로, 강력한 보안 메커니즘의 배포를 단순화하며 확장 가능하고 구현하기 쉬운 IoT 보안에 대한 끊임없이 증가하는 수요를 충족하기 위해 엣지락 보안 엔클레이브를 설계했다. 이로써 엣지락 임베디드 개발자는 애플리케이션 및 시장 출시 기간 단축에 집중할 수 있게 되었으며 보안 엔클레이브 기술이 IoT 보안의 근본적인 복잡성을 처리하도록 할 수 있다"고 말했다.

'보안 HQ,' 칩 안의 요새

자체 내장형 온-다이(on-die) 하드웨어 보안 서브시스템은 전용 보안 코어, 내부 ROM, 보안 RAM을 갖추고 있으며, 첨단 사이드 채널 공격 복원 대칭(side channel attack resilient symmetric) 및 비대칭 암호화 가속기(asymmetric crypto accelerators) 와 해싱(hashing) 기능을 지원하며, SoC 내에서 사용자 프로그래밍 가능 코어에 대한 다양한 보안 서비스를 제공한다. 본질적으로, 보안 엔클레이브는 SoC(시스템 온 칩) 내의 요새와도 같은 '보안 헤드쿼터' 역할을 하며 RoT 및 암호화 키를 포함한 주요 자산을 저장 및 보호하여 물리적 및 네트워크 공격으로부터 시스템을 보호한다.

보안 엔클레이브는 애플리케이션 및 실시간 프로세싱 기능을 처리하는 다른 프로세서 코어와 분리되어 있다. 물리적으로 격리된 아키텍처는 SoC 내에서 잘 정의된 보안 경계를 지원하고, 안전한 IoT 제품 개발을 단순화하고, 보안 키 저장소 관리, 암호화 및 기타 중요한 보안 기능을 격리하여 SoC 및 애플리케이션 보안을 강화한다.

암호화 이상의 성능

또한 보안 관행을 주류 암호화 이상으로 확장하는 유연한 정책 및 제어 기능을 제공한다. 실리콘 RoT(root of trust), 실행 시간 증명, 트러스트 프로비저닝, SoC 보안 부팅 시행, 고급 공격 저항 기능을 위한 광범위한 암호화 서비스로 강화된 세분화된 키 관리와 같은 주요 보안 기능을 자율적으로 관리하는 동시에 보안 인증 경로를 단순화한다.

고급 변조 감지 기술

고급 변조 감지 및 대응 기술은 전체 RoT를 보호하여 보안 프로세서의 작동 중 기능 무결성을 보장한다. 공격이 탐지되면 보안 엔클레이브 시스템이 공격을 차단할 수 있도록 설계되었다.

지능형 전력 관리

엣지락 보안 엔클레이브는 최종 사용자 애플리케이션이 프로세서에서 실행 중일 때 전력 전환을 지능적으로 추적하도록 설계되었다. 이 고유한 '전력 인식' 기능은 애플리케이션 프로세서의 이기종 코어가 서로 다른 전원 모드로 전환될 때 보안 정책을 시행함으로써 저항을 강화하고 새로운 공격 발생을 방지한다.

관리형 에이전트

관리형 에이전트를 사용하여 보안 HQ 외부의 SoC 도메인까지 보안을 확장한다. 이러한 자율 에이전트는 시스템 전체의 보안 기능을 설정 및 유지하고, 키를 관리하며, 도메인 전체에 걸쳐 정책을 시행한다. 에이전트는 SoC 내부의 개별 전송 회로를 통해 독립적으로 작동하여 리눅스(Linux) 또는 RTOS를 실행하는 시스템 도메인과 같은 다른 시스템 도메인이, 특히 전원 모드 전환 중에 항상 보호되도록 한다.

사전 구성 완료

사전 구성된 보안 정책을 통해 개발자는 보안 구현의 복잡성을 줄이고 비용이 많이 드는 통합 오류를 방지하여 시장 출시 기간을 단축할 수 있다. 엣지락 보안 엔클레이브는 엔클레이브 외부의 프로비저닝 서비스를 지원하며, 보안 인증을 위한 간단한 경로를 제공한다. 이러한 온 다이 보안 기술은 공공 혹은 개인 클라우드로의 보안 연결, 디바이스 간 인증, 센서 데이터 보호와 같은 최신 IoT 사용 사례도 지원한다.

이용 정보

엣지락 보안 엔클레이브는 i.MX 8ULP와 i.MX 8ULP-CS, i.MX 9 애플리케이션 프로세서 제품군 및 향후 출시 예정인 엣지버스 제품 전반에 걸쳐 표준 보안 기능으로 완전히 통합된다. nxp.com/secureenclave을 방문하거나 전 세계 NXP 영업팀에 문의하여 자세한 내용을 확인할 수 있다.

NXP 반도체 소개

NXP® 반도체(나스닥: NXPI)는 더욱 편리하고 안전하며 더 나은 삶을 위한 첨단 솔루션을 개발하여, 안전하게 연결되는 스마트 월드를 만들고 있다. NXP는 임베디드 애플리케이션용 보안 연결 솔루션의 선도 기업으로서, 자동차, 산업 및 IoT, 모바일, 통신 인프라 시장의 혁신을 주도하고 있다. NXP는 60년 이상의 전문성과 경험을 바탕으로, 전 세계 30개 이상의 국가에서 29,000명의 직원을 고용하고 있다. 2020년 매출은 미화 86억 1천만 불이다. NXP 관련 뉴스는 www.nxp.com에서 찾아볼 수 있으며, NXP 반도체 블로그 (http://blog.naver.com/nxpkor)에서도 NXP 관련 정보를 확인할 수 있다.