NXP, 엣지 보안을 위한 업계 최초의 멀티코어 솔루션 2종 출시

- 보안 서브시스템과 소프트웨어 생태계 통합하는 신규 플랫폼… 보안 실행 환경(SEE)을 통해 개발자에게 보안 기능에 대한 액세스 제공
- 광범위한 산업용 및 IoT 엣지 애플리케이션을 위한 40nm 플래시 기술 기반의 LPC5500 싱글 및 듀얼 코어 100MHz Cortex-M33 마이크로컨트롤러
- i.MX RT600 크로스오버 프로세서: 초저전력 엣지 프로세싱 애플리케이션에서 고성능 음성 및 오디오 기능 구현. 28nm FD-SOI 기술에 기반한 최대 300/600MHz Cortex-M33/디지털 시그널 프로세서(DSP) 코어 탑재

2018년 10월 11일 –NXP 반도체(NXP Semiconductors)는 엣지 보안을 위한 업계 최초의 멀티코어 솔루션 2종을 출시했다. 이 솔루션은 강화된 보안 서브시스템과 소프트웨어를 안전 실행 환경(SEE; secure execution environment)에 통합해 신뢰성과 개인정보보호, 기밀성 기준을 한층 향상시킨다. 새롭게 선보이는Cortex-M33 기반 솔루션인 LPC5500 마이크로컨트롤러와i.MX RT600 크로스오버 프로세서는 새로운 보안 기능과 여러가지 특징적인 기능을 제공한다.

임베디드 시스템 보안에 대한 멀티레이어드 방식

NXP는 자사의 보안 전문성에 기반해 구축한, 업계 유일의 멀티레이어드(multi-layered) 하드웨어 지원 보호 체계를 선보인다. 물리적 및 런타임(run-time) 보호에 필수적인 레이어드 보안 방식은 다음과 같은 기능으로 임베디드 시스템을 보호한다.

- 하드웨어 기반의 변경 불가한 RoT(root-of-trust) 용 보안 부팅
- 인증 기반 보안 디버그 인증
- 지연시간 없는 실시간 해독 기능을 갖춘 암호화된 온칩 펌웨어 스토리지

Armv8-M 및 메모리 보호 장치(MPU)용 Arm 트러스트존(TrustZone)의 향상된 Arm Cortex-M33을 활용한 이들 기능은 리소스 및 데이터에 대한 권한 기반 액세스를 위해 하드웨어에 기반한 메모리 매핑된 격리를 제공하며, 물리적 및 런타임 보호를 보장한다.

제프 리즈(Geoff Lees) NXP 마이크로컨트롤러 수석 부사장 겸 총괄은 "사물인터넷을 통해 연결된 세상을 구현하겠다는 약속은 대단한 것"이라며, "NXP의 심도 있는 보안·프로세싱 전문성과 소프트웨어 생태계, 폭 넓은 포트폴리오를 통해 NXP는 모든 개발자들에 IoT 보안에 혁신적이며 액세스 가능한 발전 사항을 제공할 수 있는 독보적 입지와 역량을 갖추었다"고 말했다.

고유한 보안 개선

변경 불가한 하드웨어 'RoT'를 형성하기 위해 디바이스 고유 키를 사용하는NXP의 ROM 기반 보안 부팅 프로세스는 디바이스 신뢰성을 구축하기 위한 초석이다. 이 키는 SRAM 비트셀 본래의 자연적 변형을 사용하는 SRAM 기반 PUF(Physically Unclonable Function)를 활용해, 필요할 때 로컬에서 생성할 수 있다. 이는 최종 사용자와 OEM 간 폐루프(closed-loop) 거래를 가능케 해, 보안이 취약할 수 있는 환경에서 타사 키를 처리해야 하는 필요성이 없다. 기존 퓨즈 기반 방법을 통한 키 주입은 선택 사항이다.

또한 NXP의 SEE는 SRAM PUF의 혁신적인 사용으로 디바이스 고유의 비밀 키를 생성해 엣지-투-엣지, 클라우드-투-엣지 통신을 위한 대칭 및 비대칭 암호화를 향상시킨다. 공개 키 인프라(PKI) 또는 비대칭 암호화를 위한 보안은 TCG(Trusted Computing Group)가 정의한 DICE(Device Identity Composition Engine) 보안 표준을 통해 향상되었다. SRAM PUF는 DICE에서 요구하는 UDS(Unique Device Secret)의 기밀성을 보장한다. 새로이 발표된 솔루션은 mbedTLS 최적화 라이브러리로, 비대칭 암호화(RSA 1024 ~4096-비트 길이, ECC)와 최대 256 비트 대칭 암호화, 해싱(AES-256 및SHA2-256)을 위한 가속을 지원한다.

존 론코(John Ronco) Arm 임베디드&자동차 사업부 부사장 겸 총괄은 "커넥티드 디바이스의 폭발적 성장을 이어가려면 이들 디바이스에 대한 사용자 신뢰가 향상되어야 한다. 커넥티드 디바이스 보안에 대한 NXP의 노력은 새로이 선보이는 Cortex-M33 기반 제품에 자명하게 드러나 있다. 이 솔루션은 검증된 보안 기반인 트러스트존 기술을 토대로 구축되었다. 또한 Arm의 플랫폼 보안 아키텍처(PSA)의 설계 원칙을 통합했고, Cortex-M 성능 효율의 한계를 뛰어 넘는 것이 특징이다"고 말했다.

머신 러닝 및 DSP 컴퓨팅 성능 가속화

NXP는 Arm v8-M 아키텍처의 전체 기능을 활용하기 위해 전략적으로 Cortex-M33을 선택했다. 이를 통해 보안 플랫폼을 제공하고, 기존 Cortex-M3/M0 MCU에 비해 상당한 성능 향상(각각 15~65% 이상 향상)을 거둘 수 있다. Cortex-M33의 핵심 기능 중 하나는 밀착 결합된 코프로세스의 효율적인 통합을 허용하면서, 전체 생태계와 툴체인 호환성(toolchain compatibility)을 유지하는 CPU의 프로세싱 기능을 확장하는 전용 코프로세서 인터페이스이다. NXP는 이 기능을 사용해 컨볼루션(convolution)과 상관 관계, 행렬 연산, 전달 함수, 필터링 등 핵심 ML 및 DSP 기능을 가속화하기 위한 코프로세스를 구현해 Cortex-M33에서 실행하는 것 대비 최대 10배 성능을 향상시킨다. 또한 이 코프로세서는 널리 사용되는 CMSIS-DSP 라이브러리 콜(API)을 사용해 고객 코드 이식성을 간소화한다.

LPC5500 플랫폼– 산업용 및 IoT 애플리케이션을 위한 멀티 코어 Cortex-M33 MCU

통합 DC-DC를 갖춘 싱글/듀얼 코어 Cortex-M33는 최대 90 밀리암페어당 코어마크(CoreMarks™/mA)에 달하는 일부 전력 예산으로 업계 선도적 성능을 제공한다. 최대 640KB 플래시와 320KB SRA의 고밀도 온칩 메모리로 복잡한 엣지 애플리케이션을 효율적으로 실행할 수 있다. 또한, 사용자 정의 작업

오프로딩 및 실행을 위한 NXP의 자율적이며 프로그래밍 가능한 로직 유닛은 향상된 실시간 병렬 처리 기능을 제공한다. LPC5500 시리즈에 대한 보다 자세한 정보는 여기에서 확인할 수 있다.

i.MX RT600 크로스오버 플랫폼 – 실시간 머신 러닝(ML)과 인공 지능(AI) 애플리케이션을 위해 전력 최적화된 Cortex-M33 / DSP MCUs

최대 300MHz Cortex-M33, 최대 600MHz 카덴스 텐실리카(Cadence® Tensilica®) HiFi 4 DSP 및 최대 4.5MB의 공유 온-칩 SRAM으로 폭넓은 작동 전압과 성능 범위를 갖춘 이 플랫폼을 활용해 효율적인 로컬 오디오 전처리와 몰입형 3D 오디오 재생, 음성 기반 경험을 구현할 수 있다. 4x 32비트 MAC, 벡터 FPU, 256비트 폭의 접근 버스 및 특수 활성화 함수 (예: 시그모이드 전송 함수)를 위한 DSP 확장으로 DSP 내 ML 성능은 한층 강화되었다. i.MX RT600 시리즈에 대한 보다 자세한 정보는 여기에서 확인할 수 있다.

도버 코어가드(Dover CoreGuard) – 하드웨어 기반 방어 보안

NXP는 도버 마이크로시스템(Dover Microsystems)사와 협력해 향후 임베디드 플랫폼에 도버의 코어가드(CoreGuard™) 기술을 도입한다. 코어가드는 사전 설정된 보안 규칙을 위반하는 명령을 즉시 차단하는 하드웨어 기반 액티브 방어 보안 IP로, 임베디드 프로세서가 소프트웨어 취약성과 네트워크 기반 공격으로부터 스스로를 방어할 수 있도록 한다. 이에 대한 자세한 내용은 여기에서 확인할 수 있다.

NXP 반도체 소개

NXP 반도체는 더욱 편리하고 안전하며 더 나은 삶을 위한 첨단 솔루션을 개발하여, 안전하게 연결되는 스마트 월드를 만들고 있다. NXP 는 임베디드 애플리케이션용 보안 연결 솔루션의 선도 기업으로서, 시큐어 커넥티드 카, 엔드 투 엔드 보안 및 프라이버시, 스마트 커넥티드 솔루션 분야의 혁신을 주도하고 있다. NXP 는 60 년 이상의 전문성과 경험을 바탕으로, 전 세계 30 개 이상의 국가에서 30,000 명 이상의 직원을 고용하고 있다. 2017 년 매출은 미화 92 억 6 천만불이다. NXP 관련 뉴스는 www.nxp.com 에서 찾아 볼 수 있으며, NXP 반도체 블로그 (http://blog.naver.com/nxpkor)에서도 NXP 관련 정보를 확인할 수 있다.