Jacinto™ 7 프로세서의 보안 구현 도구

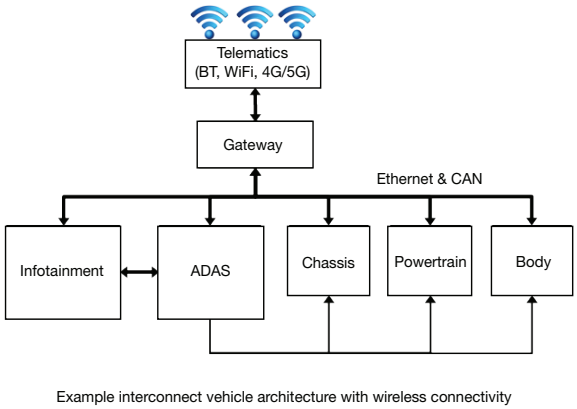
Steve Reis
시스템 애플리케이션 및 아키텍처
Jacinto 프로세서

더욱 강력한 임베디드 프로세서와 시스템온칩(SoC) 솔루션을 통해 설계자는 더욱 유능하고 강력한 시스템을 만들 수 있습니다. 원격 제어 및 관리 기능과 상호 작용하고 공장, 자동차 또는 가정에서 더욱 복잡하고 유능한 시스템에 통합하기 위해 유무선이 모두 가능한 연결성은 이제 대부분의 임베디드 시스템에 필요한 요구 사항이 되었습니다.

또한 기능을 추가하고 오류를 수정하는 원격 업데이트를 지원하는 기능도 표준 요구 사항이 되었습니다. 따라서 이러한 기능을 사용하려면 이러한 시스템에서 상호 호환이 중단되거나 시스템이 잘못 사용되거나 위험해지지 않도록 보안을 강화해야 합니다.

그림 1은 모두 전자 제어 유닛 간의 데이터 공유를 허용하는 네트워크 게이트웨이를 통해 네트워크로 연결된 섀시, 파워트레인 및 차체 시스템과 함께 인포테인먼트 시스템 및 첨단 운전자 보조 시스템(ADAS)이 장착된 오토모티브 시스템을 보여줍니다. 일반적인 오토모티브 임베디드 시스템을 통해 ADAS는 무인 주차, 차선 이탈 방지 및 기타 자동 주행 기능과 같은 일부 차량 이동을 제어할 수 있습니다. 텔레매틱스 게이트웨이는 소프트웨어 업데이트 및 기타 데이터를 위해 차량에서 클라우드에 액세스할 수 있도록 지원합니다.

외부 인터페이스, 특히 무선 인터페이스는 원격 액세스에 취약합니다. 이러한 취약성은 이러한 시스템의 네트워크 특성이 점점 더 강화됨에 따라 보안 위반이 광범위한 영향을 미칠 수 있으며 따라서 반드시 높은 수준의 보호를 제공해야 합니다.



Example interconnect vehicle architecture with wireless connectivity

그림 1. 상호 연결된 차량용 아키텍처.

본 기술백서에서는 TDA4x 및 DRA8x 프로세서가 탑재된 Jacinto 7 프로세서 제품군에 대해 논의하고, 시스템 설계자가 보안 목표를 달성하는 데 도움이 될 수 있는 TI의 Jacinto 7 SoC 제품군의 보안 기능에 대한 개요를 제공합니다. 이것을 보안 구현 도구라고 부릅니다. 보안 구현 도구에 대한 더 자세한 내용은 TI.com/security에서 확인할 수 있습니다.

보안 프레임워크

애플리케이션 수준에서 시작하여 보안 조치를 구현하면 위협으로부터 자산을 보호하는 데 도움이 됩니다. 반도체 수준에서 보호가 필요한 시스템의 주요 자산으로는 데이터, 코드, 디바이스, ID, 키가 있습니다. 시스템의 노출 지점(흔히 공격 표면이라고 함)은 애플리케이션과 시스템 수명 주기 및 운영의 각 부분에서 자산의 취약성을 증가시킬 수 있습니다.

보호가 필요한 자산과 노출 지점을 기준으로 적절한 보호를 설계하려면 적절한 보안 구현 도구를 모두 고려하고 디바이스 수준에서 보안 기능을 선택해야 합니다. 그림 2는 보안 프레임워크의 예시를 보여줍니다.

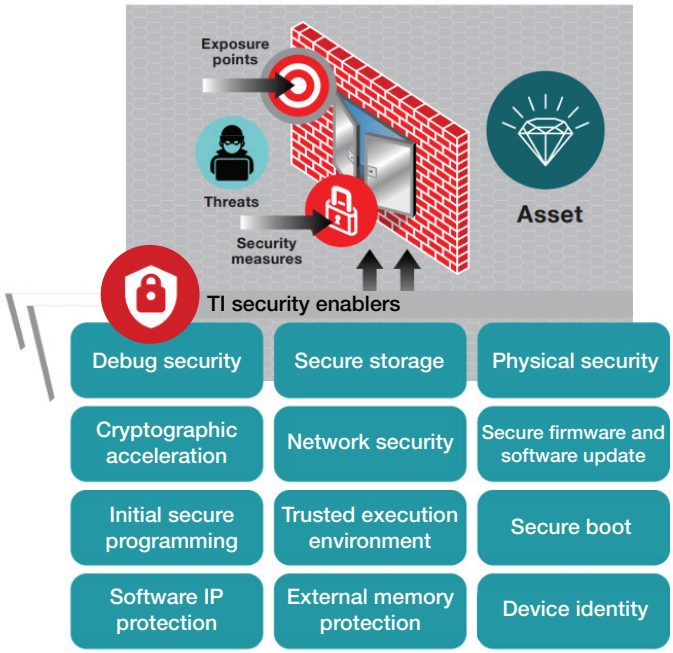


그림 2. 보안 프레임워크.

Jacinto 7 SoC 제품군은 사용자가 시스템에 맞는 강력한 보안 조치를 구현하여, 다음과 같은 시스템 노출 지점을 통한 액세스를 제한하거나 차단할 잠재적 위협에 대응할 수 있도록 많은 보안 구현 도구를 지원합니다.

- 디바이스 ID(고유 ID).
- 보안 부팅(RoT 공개 키).
- 초기 보안 프로그래밍.
- 암호화 가속.
- 외부 메모리 보호(방화벽).
- 디버깅 보안(암호를 사용한 Joint Test Action Group[JTAG] 잠금).
- 소프트웨어 지식재산권(IP) 보호(디버깅 잠금).

TI 기반 보안 프로세서 및 펌웨어

Jacinto 7 SoC의 보안 구현 도구의 핵심은 기본 보안 기능을 제공하는 펌웨어를 호스팅하는 전용 Arm® Cortex®-M 프로세서와 보안 랜덤 액세스 메모리입니다. 이러한 기능에는 보안 부팅 및 보안 기능, 보안 eFuse 키 관리, 디바이스 방화벽 관리, JTAG 액세스 인증 및 펌웨어 롤백 보호 등이 포함됩니다. 디바이스 모델에 따라 추가 기능을 사용할 수도 있습니다.

디바이스 ID, 키 및 보안 부팅

Jacinto 7 플랫폼의 보안 구현 도구 중 중요한 요소는 보안 부팅과 보안 RoT(root of trust) 키를 지원하는 것입니다. 이 두 가지 기능을 함께 사용하면 부팅 프로세스를 보호하고 신뢰할 수 없는 소프트웨어의 로드와 실행을 방지할 수 있습니다.

이 보안 앵커는 Jacinto 7 SoC에 내장된 보안 RoT 또는 키 세트를 중심으로 만들어집니다. 이러한 키는 비대칭 공개 키 및 개인 키 쌍, 공유 암호 키, 디바이스 고유 암호 키로 구성됩니다. 공개 키는 하드웨어 제조 흐름 중에 일회성 프로그램 eFuse 메모리에 통합됩니다. 이 공개 키는 소프트웨어에 내장된 디지털 인증서와 서명을 검증하여 시스템을 시작하는 초기 소프트웨어 이미지와 초기 디바이스 보안 구성의 구성 요소를 인증하는 데 사용됩니다. 이 프로세스는 Jacinto 7 SoC의 다중 코어에 대한 추가 부트로더 및 운영 체제 커널 등의 추가 소프트웨어 구성 요소를 인증함으로써 신뢰 체인을 확장하는 것은 물론 추가 키에 대한 신뢰를 설정하는 것까지 넓게 포함할 수 있습니다.

시스템 제조업체는 보안 컴퓨팅 환경에서 루트 키를 유지 관리하여 시스템 무결성을 보장하고 권한 있는 사용자의 액세스를 제한합니다. 권한 있는 사용자는 시스템의 Jacinto 7 프로세서 코어에 대한 소프트웨어를 서명하고 암호화할 목적으로만 간접적으로 루트 키에 액세스할 수 있습니다. 소프트웨어는 표준 X.509 인증서 형식을 통해 인증하며, 사용자 지정 인증서 생성이나 서명 도구가 필요하지 않으므로 공통 도구를 사용하여 생성할 수 있습니다. 그래서 사용자의 안전한 컴퓨팅 환경에 간단한 구현이 가능하고 개인 키의 보안을 유지할 수 있습니다.

Jacinto 7 SoC의 보안 부팅 기능은 디바이스에서 실행 중인 소프트웨어를 항상 인증할 수 있도록 보장하므로 중요한 초기 부팅 단계에서 인증하지 않은 소프트웨어가 로드되는

것을 방지합니다. 초기 보안 부팅 프로세스는 디바이스 RoT와 비교하여 소프트웨어 구성 요소의 인증을 강제 적용하는 보안 부트 읽기 전용 메모리를 사용하여 구현합니다. 부팅 인증 옵션은 소프트웨어와 인증서 서명에 대한 강력한 SHA2-512 해시와 결부하여 최대 521bit 키까지 Rivest-Shamir-Adleman(RSA) (최대 4,096bit 키) 또는 Elliptic Curve Digital Signature Authentication(ECDSA) 타원 곡선 암호화(ECC)를 지원할 수 있습니다. 부트로더의 선택적 AES-256 암호화도 지원됩니다.

초기 보안 프로그래밍

디바이스 키 프로비저닝은 암호 키를 프로그래밍할 때 안전하게 수행해야 하는 프로세스입니다. 디바이스 키 프로비저닝 프로세스는 보안, 단순성 및 키 프로그래밍의 완벽한 유연성을 고려하여 시스템 제조업체가 TI에서 제공하는 보안 프로비저닝 도구를 사용하여 자체 공장에서 완벽하게 제어합니다. 암호화 보호는 프로비저닝 프로세스 중에 대칭 암호 키가 노출되는 것을 방지하므로, 신뢰할 수 없는 공장 환경에서도 키 프로비저닝 및 제조를 허용합니다.

암호화 가속

암호화 기능은 유연성과 처리량 요구 사항에 따라 범용 컴퓨팅 코어 또는 특수 하드웨어 가속기에서 계산할 수 있습니다. Jacinto 7 SoC에는 일반적인 암호화 기능을 가속화하는 코어 세트가 포함되어 있으며 다음 **기능을 지원합니다.**

- 비대칭 암호화: RSA 및 ECC 기능.
- 해싱: MD5(Message Digest Algorithm), SHA1 및 SHA2-224/256/384/512.
- 대칭 암호화 기능: AES-128/192/256.
- 결정론적 난수 발생기(DRBG) 후처리를 지원하는 하드웨어 TRNG 모듈.

또한 Arm Cortex-A CPU는 AES, SHA1 및 SHA2 알고리즘의 실행을 가속화하기 위한 새 명령을 추가하는 ARMv8 암호화 확장을 지원합니다.

소프트웨어 IP 보호(방화벽)

Jacinto 7 SoC에는 TI 디지털 신호 프로세서(DSP) 및 일부 디바이스의 특수 DSP 가속기와 더불어 64bit Arm 코어 및 32bit Arm 마이크로 컨트롤러 코어를 포함하여 다양한 작업에 최적화된 이기종 프로세서 코어 세트가 포함되어 있습니다. 이러한 구성 요소 중 일부는 보안 자산과 연동되다 보니 다른 범용 기능으로부터 보호 및 격리할 필요가 있는 작업에 할당할 수 있습니다. Jacinto 7에는 안전을 위한 격리뿐만 아니라 런타임 보안 보호를 위한 포괄적인 세트의 시스템 방화벽이 포함되어 있습니다. 방화벽을 통해 사용자는 각 프로세서 코어 또는 시스템 초기자가 액세스할 수 있는 하드웨어 요소와 메모리 범위를 정의할 수 있습니다. 이 방화벽 인프라는 기밀 노출을 방지하고, 간섭을 받지 않으며, 가능한 모든 침입의 영향을 제한할 수 있는 핵심적인 구현 도구입니다.

디버깅 보안

대부분의 프로그램 가능한 디바이스에서 볼 수 있는 유비쿼터스 JTAG 디버깅 포트는 디바이스 레지스터와 메모리에 대한 쉬운 접근성, 쉬운 초기 플래싱 방법 및 프로그램 추적과 같은 많은 접근성 기능을 제공합니다. 이러한 접근성은 이 포트가 시스템에서 가장 취약한 노출 지점일 수도 있음을 의미합니다. 결과적으로, Jacinto 7 SoC의 JTAG 디버깅 포트는 보안 디바이스의 경우 기본적으로 비활성화되어 있으므로 SoC 작업에 액세스하는 데 사용할 수 없습니다. 동시에 Jacinto 7 디바이스 JTAG는 필요한 경우 안전한 방식으로 디버깅 및 분석에 사용할 수 있습니다. JTAG 액세스를 사용하려면 RoT에 연결된 인증서 메커니즘을 통한 인증 또는 승인이 필요합니다. 또한 각 디버깅 인증서는 하나의 디바이스에 연결되며 인증서에 포함된 일부 디바이스 ID에 대해서만 디버깅을 사용할 수 있습니다. 마지막으로, 시스템 보안 프로토콜이 필요한 경우 일회성 프로그램 eFuse 프로그래밍을 통해 JTAG 액세스를 영구적으로 비활성화할 수 있습니다. 이러한 기능은 보호 및 액세스 계층을 제공하고 사용자에게 개발 시 유연한 액세스와 생산 시 보안을 제공합니다.

신뢰실행환경(TEE)

SoC의 Arm Cortex-A72 TrustZone® 기능은 안전한 소프트웨어 구성 요소의 실행을 위한 격리 기능을 제공하며 키, 데이터 및 특수 알고리즘과 같은 중요한 자산을 보호할 수 있습니다. 이러한 보안 환경의 사용을 단순화하기 위한 신뢰실행환경(TEE)은 격리된 보안 애플리케이션에 대한 안전한 소프트웨어 환경을 제공합니다. Jacinto 7 디바이스의 Linux® 소프트웨어 개발 키트는 Linaro OP-TEE 보안 스택의 통합을 지원합니다. 그래서 Arm 플랫폼을 위한 보안 애플리케이션을 개발하기 위해 표준 GlobalPlatform 애플리케이션 프로그래밍 인터페이스를 사용하여 보안 애플리케이션을 구현할 수 있습니다. TEE의 또 다른 이점은 보안 애플리케이션이 Linux 스택의 나머지 부분뿐만 아니라 상호 간에도 분리된다는 점입니다. 따라서 여러 클라이언트가 서로 간에 자산을 노출시키지 않고도 TEE를 안전하게 사용할 수 있습니다.

안전한 펌웨어 및 소프트웨어 업데이트

서비스 기술자나 공장 서비스의 시간과 비용 없이 새롭고 향상된 기능, 버그 수정 및 보안 패치를 신속하게 업데이트할 수 있도록 임베디드 시스템에서 보안 펌웨어 업데이트 기능, 특히 OTA 업데이트의 필요성이 확산되고 있습니다. 그러나 다른 사용자가 이전 버전을 가장하거나 이전 버전으로 롤백하거나 업데이트 메커니즘을 사용하여 손상된 소프트웨어 이미지를 설치할 수 있는 경우에도 이 업데이트 프로세스가 취약점이 될 수 있습니다.

업데이트 이미지의 무결성과 신뢰성을 모두 확인하기 위해 항상 이미지를 해시하고 서명해야 합니다. 무결성 검사를 통해 업데이트가 신뢰할 수 있고 알려진 출처의 것인지 확인하고, 무결성 검사를 통해 전송 및 로드 중에 이미지가 변경 또는 변조되지 않았는지 확인합니다. 보안 부팅 인증에 사용하는 동일한 Jacinto 7 SoC 기능으로도 소프트웨어 및 데이터 업데이트를 인증할 수 있습니다.

마무리

Jacinto 7 디바이스 제품군에서 제공되는 보안 구현 도구는 디자이너와 설계자가 시스템에 필요한 보안 목표를 달성할 수 있도록 하는 포괄적인 임베디드 보안 기능으로 구성되어 있습니다. 이러한 보안 구현 도구는 보통 프로젝트에 대한 특정 보안 목표, 위험 및 조치와 이 보안 목표를 달성하는 데 도움이 될 수 있는 보안 구현 도구를 식별하는 보안 구현 주기의 한 부분으로 평가됩니다. 자세한 내용은 ti.com/security를 참조하십시오.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (https:www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265