Jacinto™ 7 处理器上的信息安全机制

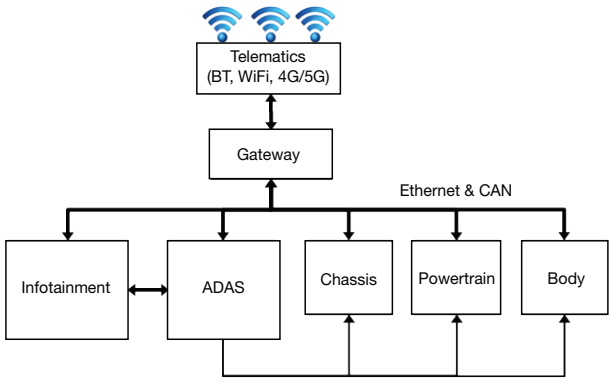
Steve Reis
系统应用和架构
Jacinto 处理器

借助更加强大的嵌入式处理器和片上系统 (SoC) 解决方案，设计人员可以创建功能更强大的系统。为了在工厂、汽车或家居领域实现远程控制和管理功能，以及集成更复杂、更强大的系统，有线和无线连接现在对于大部分嵌入式系统而言都必不可少。

此外，支持通过远程更新添加功能和纠错的能力也成为一种通用需求。这些特性进而需要更全面的信息安全机制，从而防止系统被指定、误用甚至受到安全攻击。

图 1 显示了一个汽车系统，其中机箱、动力总成、车身系统以及信息娱乐系统和高级驾驶辅助系统 (ADAS) 均通过网络网关联网，从而在各电子控制单元之间实现数据共享。典型的汽车嵌入式系统支持 ADAS 控制车辆的部分操作，如自动泊车、车道保持辅助和其他自动驾驶功能。远程信息处理 (Telematics)网关支持汽车访问云端，进行软件更新和获取其他数据。

外部接口，尤其是无线接口，易受黑客远程访问的攻击。再加上联网的系统不断增加，一旦发生任何安全漏洞，多个系统都会受到影响。因此，提供较高网络安全等级的保护势在必行。



Example interconnect vehicle architecture with wireless connectivity

图 1.互联的汽车架构。

在本白皮书中，我们将介绍 Jacinto 7 处理器系列（其中包括 TDA4x 和 DRA8x 处理器），并概述 TI Jacinto 7 系列 SoC 中可帮助系统设计人员满足安全要求的安全特性。我们将上述特性称为信息安全机制需了解有关信息安全机制的更多信息，请访问 TI.com/security。

安全框架

从应用层面实施安全措施，有助于保护数据抵御威胁。从半导体角度而言，系统中需要保护的主要资产有数据、代码、器件身份和密钥。在应用的各个部分以及系统生命周期和运行期间，系统中的众多暴露点（通常称为攻击面）会使数据更容易受到威胁。

根据需要保护的数据和暴露点情况，您需要考虑所有合适的信息安全机制，并从器件层面选择信息安全特性并用于设计对应的保护。**图 2** 展示了一个安全架构示例。

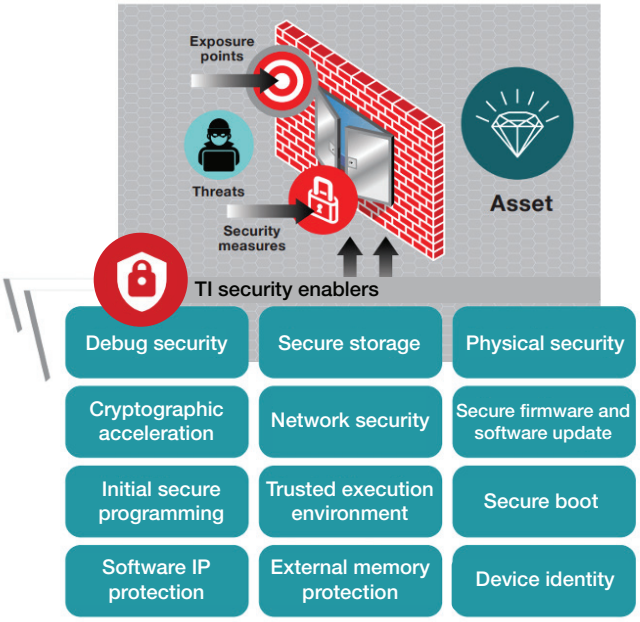


图 2.安全架构。

Jacinto 7 SoC 系列支持许多信息安全机制，可帮助用户实现为其系统量身定制的有效安全措施，从而抵御会通过系统暴露点限制或阻止存在潜在危险的访问，这些安全驱动工具包括：

- 器件身份（唯一 ID）。
- 安全启动信任根公钥）。

- 初始安全编程。
- 加解密加速。
- 外部存储器保护（防火墙）。
- 调试安全性（带密码的JTAG 锁）。
- 软件知识产权 (IP) 保护（调试锁定）。

TI 基础安全处理器和固件

Jacinto 7 SoC 安全驱动工具的核心是专用的 Arm® Cortex®-M 处理器和安全随机存取存储器，它们运行有可提供基础安全功能的固件。这些特性包括安全启动和加密OTA 功能、基于 eFuse 的安全密钥管理、器件防火墙管理、JTAG 访问 授权和固件回滚保护。根据器件型号的不同，也可能提供其他特性。

器件身份、密钥和安全启动

Jacinto 7 平台信息安全机制的一项重要作用是，为安全启动和安全信任根密钥提供支持。上述特性共同保护引导过程，并防止加载和执行不可信软件。

此安全基准是基于 Jacinto 7 SoC 中嵌入的安全信任根或密钥集构建。这些密钥包括非对称公私钥对、共享密钥和器件独有密钥。在硬件制作流程中，公钥写入一次性可编程 eFuse 存储器中。此公钥用于对启动系统的初始软件映像进行身份验证，还通过验证软件中嵌入的数字证书和签名，对器件安全初始配置组件进行身份验证。此过程可用于扩展，在其他密钥中建立信任；还可通过对其他软件组件（如适用于 Jacinto 7 SoC 上多个内核的其他引导加载程序和操作系统内核）进行身份验证，扩展信任链。

系统制造商在安全的计算环境中对根密钥进行维护，从而确保系统完整性和授权用户的合法访问，这样授权用户只能间接访问根密钥来签名和加密其系统上的软件。软件通过标准格式的 X.509 证书进行身份验证，该证书不需要自定义证书生成或签名工具，通过常用工具即可创建。因此，可直接在用户的安全计算环境中实现，并保护用户私钥的安全。

Jacinto 7 SoC 的安全启动特性确保设备上运行的软件一定被身份验证过，从而防止在关键的初始引导阶段加载未授权软件。初始安全引导过程通过安全引导只读存储器执行，该存储器可基于器件的信任根对软件组件进行强制身份验证。引导身份验证选项支持 Rivest-Shamir-Adleman (RSA)（高达 4,096 位密钥）或高达 521 位密钥的椭圆曲线数字签名算法 (ECDSA) 椭圆曲线加密 (ECC)，以及用于软件和证书签名的强大 SHA2-512 哈希算法。此外，还支持引导加载程序的 AES-256 加密（可选）。

初始安全编程

对密钥进行编程时，器件密钥的配置过程必须安全进行。为实现密钥编程的安全性、简易性和充分灵活性，系统制造商在其工厂内使用 TI 的安全配置工具，对器件的密钥配置过程进行全方位控制。加密保护可防止在配置过程中暴露对称密钥，并允许在不可信的工厂环境中进行密钥配置和制作。

加解密加速

根据灵活性和吞吐量要求，可在通用计算内核或专用硬件加速器上计算加密运算。Jacinto 7 SoC 包含一组可加速常见加密运算的内核，并对以下算法提供支持：

- 非对称加密：RSA 和 ECC 函数。
- 哈希函数：消息摘要算法 (MD5)、SHA1 和 SHA2-224/256/384/512。
- 对称加密函数：AES-128/192/256。
- 硬件 TRNG 模块具有确定性随机比特生成器 (DRBG) 后处理功能。

此外，Arm Cortex-A CPU 支持 ARMv8 加密扩展，后者添加了加速执行 AES、SHA1 和 SHA2 算法的新指令。

软件 IP 保护（防火墙）

Jacinto 7 SoC 包含一组面向各种任务优化的异构处理器内核，包括 64 位 Arm 内核和 32 位 Arm 微控制器内核，以及 TI 的数字信号处理器 (DSP) 和某些器件专用的 DSP 加速器。上述某些元件可能会被分配执行与安全数据相关的任务，因此需要得到保护，并与其他通用元件隔离。Jacinto 7 包含全面的系统防火墙，用于提供运行时安全保护以及安全隔离。防火墙允许用户定义每个处理器内核或系统启动程序可访问的硬件元件和存储器范围。此防火墙基础设施是一项关键要素，可防止保密信息泄露、不受干扰并限制任何潜在的入侵带来的影响。

调试安全性

JTAG 调试端口在大部分可编程器件上随处可见，可提供许多易用特性，如轻松访问器件寄存器和存储器，初始轻松刷写和程序追踪。其易用性也意味着，这种端口在系统中可能很容易受到攻击。因此，为了保护器件，Jacinto 7 SoC 的 JTAG 调试端口是默认禁用的，所以无法用于获取 SoC 的运行情况。当然，可以使用安全的方式启用 Jacinto 7 器件 JTAG，用于调试和分析（如需要）。启用 JTAG 访问需要授权，或通过与信任根相关的证书机制进行身份验证。另外，调试证书与器件都是对应，而且只能根据证书中指定的器件 ID 进行调试。最后，如

果系统安全协议需要，也可以通过一次性可编程 eFuse 编程来永久禁用 JTAG 访问。上述特性提供了层层保护和访问权限，可让用户在开发期间灵活访问，并在量产中实现安全性。

可信执行环境

Jacinto 7 SoC 的 Arm Cortex-A72 TrustZone® 功能可为安全软件组件的执行提供隔离，还能保护密钥、数据和专用算法等重要资源。为了简化这种安全环境的使用体验，可信执行环境 (TEE) 可为隔离的安全应用提供一个安全的软件环境。Jacinto 7 器件的 Linux® 软件开发套件可集成 Linaro OP-TEE 安全堆栈，进而使用标准的 GlobalPlatform 应用程序编程接口启用安全性应用程序，用于开发适用于 Arm 平台的安全应用。TEE 的另一项优势是各安全应用程序之间以及与其他的 Linux 栈相互隔离。这样，可在多个客户端安全使用 TEE，而不会在客户端之间泄露数据。

安全固件和软件更新

为了实现新特性和增强特性的现场更新、快速修复缺陷和安全补丁，同时不增加技术人员或工厂服务的时间和费用，嵌入式系统对安全固件更新（特别是 OTA 更新）功能的需求激增。然而，如果其他固件可能发生仿冒、回滚至之前版本等情况，或利用更新机制安装不可信的软件映像，则此更新过程也易受到攻击。

必须对更新映像进行哈希校验并签名，从而验证其完整性和真实性。真实性检查可验证该更新来自已知的可信来源，而完整性检查可验证该映像在传输和加载过程中未经更改或篡改。Jacinto 7 SoC 的特性不仅可用于安全引导身份验证，也可对软件和数据更新进行身份验证

结束语

Jacinto 7 器件系列中的信息安全机制提供了全面的嵌入式信息安全特性，可让设计人员和架构师满足系统的安全性要求。这些通常可以作为安全实现周期的一部分，即确定每个项目的具体安全要求、风险和措施，以及可帮助满足上述安全要求的信息安全机制。如需更多信息，请参阅 ti.com/security。

重要声明和免责声明

TI 提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他安全、安保或其他要求。这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款 (https:www.ti.com.cn/zh-cn/legal/termsofsale.html) 或 ti.com.cn 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

邮寄地址：上海市浦东新区世纪大道 1568 号中建大厦 32 楼，邮政编码：200122