Application Brief

*在 **AM26x** 器件上实现更快的安全启动*

Nilabh Anand, Aakash Kedia

为了确保汽车和工业域中的器件安全免受恶意攻击，网络安全法规正得到广泛实施。TI SoC 正在这些领域得到广泛应用。TI AM26x SoC 是一款支持实时功能的器件，具有实时 ARM R 内核、高级检测、精确控制、千兆位连接和专用元件等多种功能，可支持设计具有网络安全和功能安全要求的系统。在本文档中，我们可以查看 AM26x SoC 系列的安全启动增强功能和性能基准测试。

简介

外部闪存器件的优势是具有灵活的 NVM 存储器大小，当面临存储器限制挑战时，无需升级或更改现有 SoC 即可存储应用软件。另一方面，如果没有采取适当的安全措施，则可能会将未经授权的程序加载到存储器中。未经授权的程序可能使系统无法运行，将敏感和机密数据暴露给恶意代理，在某些情况下，可能会造成危及生命的后果、名誉损害和法律责任。

AM26x（AM263x 和 AM263Px）器件系列支持安全启动用户代码，而不会影响代码、数据、密钥等用户信息的真实性和机密性。AM26x 微控制器系列支持 OSPI 和 QSPI 等接口，这些接口支持集成外部闪存器件和提供安全启动特性。这使得用户能够灵活地使用外部闪存技术，同时保持系统的安全性。

AM26 安全启动的加密优势包括：

- RSA-PKCS1-v1_5 和 SHA512 摘要用于验证证书。
- SHA512 用于保持引导加载程序映像的完整性。
- AES-CBC-256 用于解密映像以保持映像的机密性。

快速引导技术

以下各部分包含有关用于提高启动时性能的不同启动优化技术的信息。

闪存时钟、配置和 DMA 集成

AM26x 器件系列没有用于执行代码的内部非易失性存储器，极度依赖内部易失性存储器（TCM 和 SRAM）。与许多其他高级 SOC 一样，AM26x 器件也具有*多级启动*架构。在执行 ROM 引导加载程序 (RBL) 期间，会将二级引导加载程序 (SBL) 映像从外部闪存（通过 SPI）复制到内部存储器中。在 SPI 协议中，数据速度 (bps) 与 SPI 外设计时频率 (Hz) 成正比。根据 *JEDEC xSPI 标准*，将 OSPI 控制器配置为支持更高的模式可以实现更快的数据传输。因此，更高的 SPI 时钟速率和更高的配置可以带来更好的性能。

English Document: SPRADM8
Copyright © 2024 Texas Instruments Incorporated

表 1. AM26x 器件的闪存控制器比较

	AM263x	AM263Px
最大闪存时钟速率	80MHz	133MHz
支持的最大配置	1s-1s-4s	8d-8d-8d
DMA 与闪存控制器集成	是	是

经优化的 OSPI PHY 调优（仅对 AM263Px 有效）

AM263Px SOC 上的 OSPI 控制器集成了专用 PHY 模块，从而可实现灵活且节能的传输。这使我们能够**在单倍传输速率 (STR) 模式下以 50MHz 使用闪存时钟，在双倍传输速率 (DTR) 模式下以 25MHz 使用闪存时钟**。在 OSPI_PHY_CONFIGURATION_REG 中配置 PHY_CONFIG_TX_DLL_DELAY_FLD 和 PHY_CONFIG_RX_DLL_DELAY_FLD 之前，该 PHY 要求对所有有效值进行软件校准。因此优化软件算法可以跨越有限值在 ***不到 2.5ms*** 的时间内完成校准。

请参阅 *AM263Px TRM* (13.3.3.6)，了解有关 OSPI 控制器和 PHY 模块的更多信息。点击*此处* 获取有关经优化的 PHY 调优的应用手册。

映像格式 (MCELF)

与之前采用的专有 RPRC 格式不同，多核 ELF 或 MCELF 是基于 ELF（可执行和可链接格式）标准的应用程序映像格式。使用 ELF 文件格式的可执行文件包含 ELF 标头，后跟程序标头表或段标头表，或同时包含这两者。文件中的程序标头表和段标头表的偏移在 ELF 标头中定义。这两个表描述了文件的其余特性。下表总结了 MCELF 格式相对于 RPRC 格式的优势。

表 2. RPRC 和 MCELF 格式之间的比较

特性	RPRC	多核 ELF
映像生成工具	自定义	开源
可由标准 ELF 工具读取	否	是
可自定义的元数据	否	是
可自定义的数据段大小	否	是
XIP	是	是
安全启动时间	慢	快

安全启动的流支持

由于闪存时钟有限，直接在闪存存储器中验证映像会带来瓶颈，并且缺少暂存区存储器会导致安全启动映像无法复制到存储器中进行验证。验证外部闪存中的安全启动映像也会使软件面临 TOCTOU 攻击的风险，从而增加许多安全限制。因此，流安全启动使用户能够将映像复制到 SBL 中的存储器，然后向 TIFS-MCU 服务发出调用以在流模式下对映像进行身份验证。这利用执行存储器进行放置和身份验证，从而提高了身份验证的速度。

English Document: SPRADM8
Copyright © 2024 Texas Instruments Incorporated

加密 DMA

DTHE（数据转换和哈希引擎）是与 AM26 器件集成的加密 IP 上的包装器。DTHE 支持 EDMA（增强型 DMA）集成，可减轻突发数据传输的负担。增强型 DMA 可以被编程为事件触发，并可根据配置的突发大小自动传输数据。这允许将 Crypto IP 事件配置为 EDMA 源事件，从而支持完全转移 CPU 的负载。

表 3. 加密硬件性能

数据	不使用 DMA（以 Mbps 为单位）	使用 DMA（以 Mbps 为单位）	改进
SHA512			
4KB	250.41	679.58	2.7x
16KB	265.65	1024.60	3.85x
AES-CBC-256			
4KB	93.61	239.30	2.55x
16KB	94.81	301.54	3.18x

RSA 签名验证不受 DTHE 中 DMA 集成的影响。有关更多信息，请参阅 TIFS-MCU 文档中的 PKE 硬件集成。

通过安全启动服务并行使用闪存

下一个优化途径是在 SBL 中，对顺序闪存读取进行修改，以执行并行读取。在 SBL 中添加并行化以支持 (n+1) 个段的并行闪存读取，同时 TIFS-MCU 正在验证 (n) 个段。通过增加对 HSM 服务器上 SIPC 消息排队的支持并按顺序处理这些消息，实现了进一步的增强，例如，支持发送非阻塞请求和处理来自客户端 (SBL) HSM 的多个响应。下面是 SBL 从闪存进行读取时 TIFS-MCU 占用情况的直观表示。

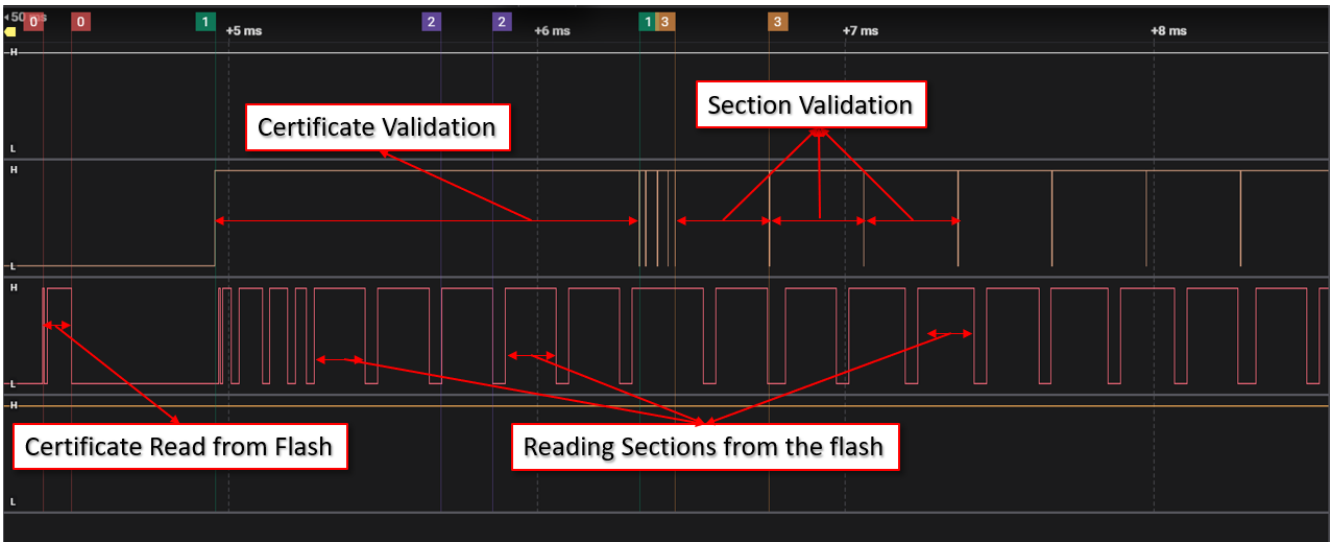

图 1. 启动并行化

安全启动基准测试

通过实施上述技术，启动时间性能显著提高，表 4 显示和总结了该情况。

AM263x

- SBL 大小 - 55KB。SBL 经过加密和身份验证。
- TIFS-MCU 大小 - 70KB。TIFS-MCU 会进行加密和身份验证。

表 4. AM263x 启动时间性能

应用程序大小	仅身份验证	仅加密 + 身份验证
64KB	40.53ms	43.40ms
128KB	41.05ms	44.58ms

Copyright © 2024 Texas Instruments Incorporated

表 4. AM263x 启动时间性能（续）

应用程序大小	仅身份验证	仅加密 + 身份验证
256KB	45.62ms	56.18ms
512KB	60.45ms	76.39ms
1024KB	90.16ms	116.92ms

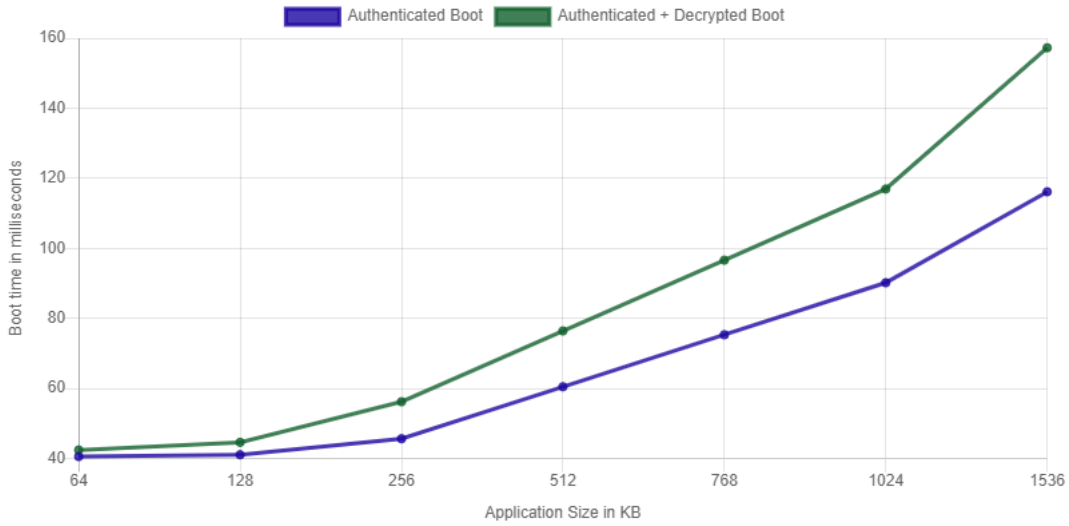

图 2. AM263x 启动性能

AM263Px

- SBL 大小 - 60KB。SBL 经过加密和身份验证。
- TIFS-MCU 大小 - 61KB。TIFS-MCU 会进行加密和身份验证。

表 5. AM263Px 启动时间性能

应用程序大小	仅身份验证	仅加密 + 身份验证
1024KB	37.11ms	64.13ms
512KB	32.61ms	45.85ms
256KB	30.74ms	37.48ms
128KB	29.83ms	33.31ms
64KB	29.35ms	30.26ms

Copyright © 2024 Texas Instruments Incorporated

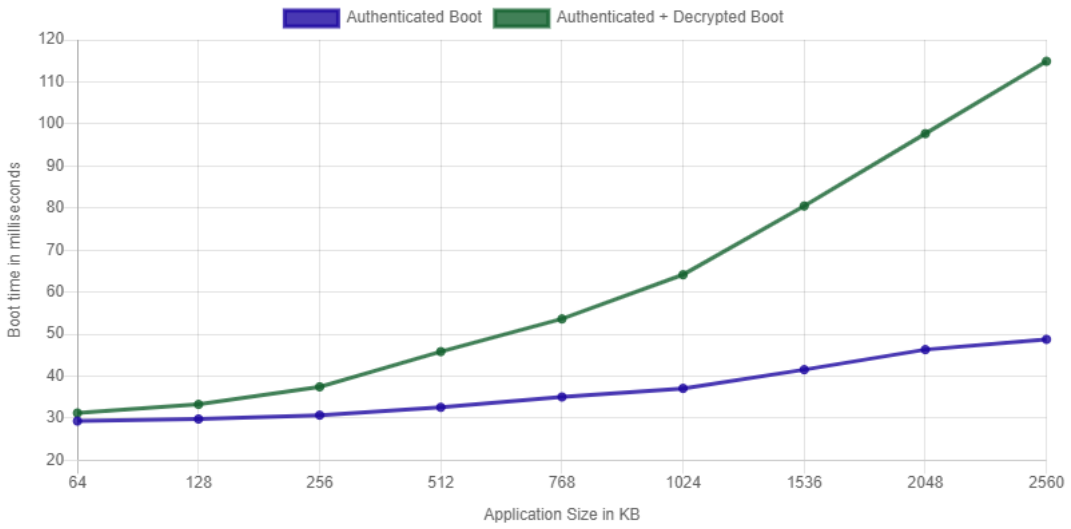

图 3. AM263Px 启动性能

结语

安全启动会由于身份验证和映像完整性验证而产生额外的运行时开销。但是，通过采用软件设计和硬件负载减轻技术，可以缩短安全启动时间，从而提高整体系统性能。在汽车系统中，启动时间目标非常严格，同时几乎不会影响系统的安全性。本文中讨论的适用于 AM26x 系列 SOC 的优化安全启动方法旨在利用高效的硬件架构和软件设计解决相同的难题。

商标

所有商标均为其各自所有者的财产。

English Document: SPRADM8
Copyright © 2024 Texas Instruments Incorporated

重要声明和免责声明

TI“按原样”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功能安全、信息安全、监管或其他要求。

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 的销售条款或 ti.com 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。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2024，德州仪器 (TI) 公司