Application Note

SimpleLink CC33xx 安全特性

Shlomi Itzhak

摘要

CC33xx 系列器件是新一代 Simplelink™ 嵌入式解决方案。这些器件的主要作用是满足新兴物联网 (IoT) 用例的要求，同时与新兴的尖端技术（如 Wi-Fi™ 6 和低功耗 *Bluetooth*® 5.4）兼容。

在主机处理器运行 Linux® 或 MCU 主机运行 RTOS 的嵌入式应用中，这些新一代器件可实现经济、可靠且安全的连接。CC33xx 系列器件提供广泛的内置安全特性，可帮助开发人员满足各种安全需求。

内容

插图清单

表格清单

商标

1 引言

物联网 (IoT) 产品和系统保存的信息可能是敏感和隐私信息，因此需强调保护数据安全的重要性。此类数据可能包括密码、密钥、凭据、配置、个人信息、供应商知识产权 (IP) 等。由于发布的遭到利用的安全弱点越来越多以及政府和标准组织不断提出要求，我们必须为每个新的物联网设备制定稳健的网络安全措施。

本文档将介绍这些安全相关特性；供应商可以通过一个包含简洁 API、工具和文档的生态系统来利用这些特性。本文档不涉及网络层或应用层上的安全相关特性，仅涵盖 Wi-Fi 和低功耗蓝牙外设中的特性。

1.1 术语和缩写

表 1-1. 术语和缩写

缩写	含义
资产	资产是指对所有者有价值的任何信息（安全相关元素）。因此，必须通过目标系统的各种措施（机密性、完整性、真实性）来保护资产。资产可以是专有信息、个人数据或知识产权。
真实性	确认资产或实体是真实的，且已获得执行某一任务的授权，或者可按预期使用。验证过程通常涉及加密算法，该算法用于检查实体的真实身份与宣称的身份是否相符。某些预定义的信任机制始终属于验证机制的一部分。
证书	证书是标准格式文件。证书通常包含使用者的公钥，以及头文件和公钥的 CA 签名。可提供 CA 公共密钥（若是证书链，则为子 CA）的任何人都能够验证使用者的身份。
证书颁发机构 (CA)	受信任的实体，颁发用于验证身份的证书。
证书链、信任链	证书链包含形成层级结构的多个证书，支持任何人验证一直到根证书的任何证书颁发者的身份。
机密性	机密性可确保资产不会供未获授权的实体使用，也不会向此类实体披露。在大多数情况下，机密性涉及加密，而在其他情况下，则使用混淆技术来保持机密性。
完整性	用于描述对象与原始版本相比完全保持不变的属性。
根 CA	证书颁发机构对照最终验证的证书链提供的最高级别的证书。证书始终自签名且公开可用。

2 物联网 (IoT) 产品和安全性

物联网设备本质上是一种联网设备，因此可充当网关来阻止恶意访问敏感数据（如监控视频），或控制执行器（如门锁）。为确保支持互联网的产品实现良好的安全性，必须对具体产品及系统级要求执行安全评估。这种评估可确定涉及的资产，分析环境以及产品可能按预期和未按预期使用的情况，从而检测产品可能存在的漏洞。

这种评估可帮助开发人员使用可用的安全功能制定最佳保护机制。

每种产品的环境、资产和工艺都各不相同，但 IoT 设备通常都有一些相同的暴露点：

- 物理访问（无论是否能够操作硬件接口）
- 局域网连接
- 互联网（或内联网）网络连接 — **本文档未涉及**

图 2-1 所示为连入物联网的产品通常具有的暴露点。

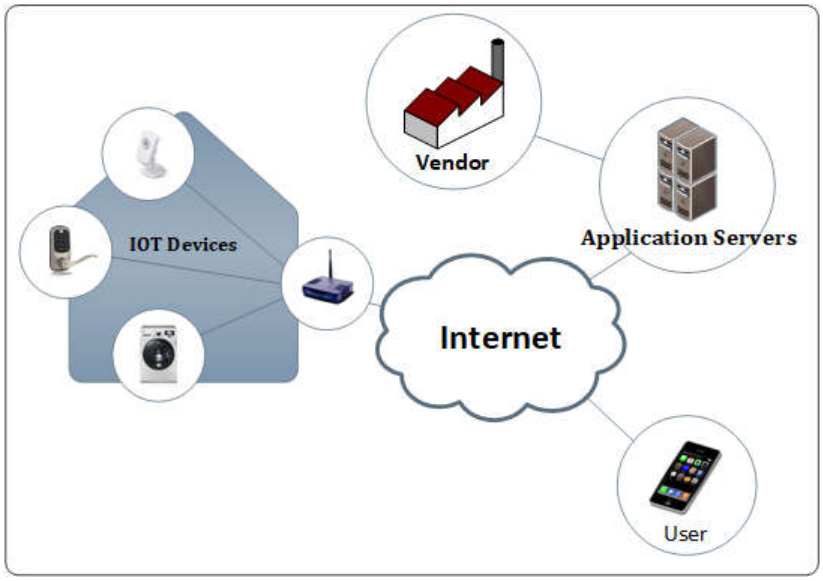

图 2-1. 物联网器件暴露点

2.1 物理访问

若遇到物理访问攻击，暴露点位于产品级，因此需要考虑多种因素。物理访问会引发产品级篡改和印刷电路板 (PCB) 篡改等攻击向量。产品级篡改攻击向量是指在攻击过程中，攻击者可使用最终产品的外部接口（比如电力线、按钮等）来控制设备的运行方式。另一个攻击向量与攻击者能够接触实际电路板 (PCB) 并监听线路或硬件接口相关。在更为严重的情况下，攻击者甚至会尝试篡改导线，替换 PCB 上的器件，连接到主控制器，以及注入信号来触发某些操作。

2.2 局域网连接

局域网的一般性质使其容易受到一组特定的攻击向量攻击。例如，监视无线网络，或者在 Wi-Fi 或局域网 (LAN) 上注入恶意或滥用的流量。

其中一个向量基于攻击者未连接时对无线网络通信的被动监视。无线网络可能会遭到被动监视，因为即便在安全无线网络中，其中一些通信数据包标头也不会进行加密。这些标头会泄露该网络中设备的 MAC 地址或所生成流量的时间特性等信息。

Wi-Fi 联盟在相关标准中规定了安全和合规性测试。CC33xx 配套 IC 经过 Wi-Fi Alliance 测试平台的测试，符合所有相关安全要求。

第二个攻击向量与局域网 (LAN) 中另一设备产生的攻击相关。这为执行涉及网络访问的攻击向量提供了额外的机会，导致能够为网络通信合理注入流量，滥用目标设备上的端口和可用协议。

3 主要特性

CC33xx 配套 IC 提供广泛的内置安全特性。这些安全功能可支持并帮助设计人员解决各种安全需求，降低目标应用中的安全风险。

表 3-1 列出了主要安全功能的概要说明。

表 3-1. 主要安全功能

功能	说明
个人和企业 Wi-Fi 安全	符合 802.11 标准的安全支持（WPA、WPA2-PSK、WPA2-EAP、WPA3、PMF、WPA3-EAP）。
加速器	片上加密引擎（硬件加速器）可减轻数据加密/解密负担。
TI 信任根公开密钥	基于硬件的机制，支持使用非对称密钥将德州仪器 (TI) 验证为特定内容（例如固件二进制文件、RAM 引导加载程序二进制文件或其他容器）的真正来源。
安全引导	在引导期间验证运行时二进制文件的完整性和真实性，以确认下载的固件经过德州仪器 (TI) 签名且未被篡改。
安全主机接口	防止物理嗅探 SDIO/SPI，从而维持数据完整性。
回滚保护	内置硬件机制，可确保不会重新安装和恶意使用早期版本的固件。

3.1 安全启动

安全启动的主要目的是在启动期间验证运行时二进制文件的完整性和真实性，以确认下载的 RAM 引导加载程序和固件经过 TI 签名且未被篡改。授权固件是指来自正确实体、具有正确属性（例如正确版本）或适用于特定器件的固件。无论生命周期状态如何，安全启动始终是器件上运行的第一段代码。实施安全启动过程对于器件在整个生命周期中的完整性至关重要。启动过程受到攻击后允许攻击者注入恶意软件、访问资产或完全替换器件上运行的固件。为了通过提供必要的信任度来实现其他安全特性，安全启动过程至关重要。

3.1.1 安全启动容器

为了更好地了解身份认证的实施方式，引入了容器的概念。容器是一个文件，其中包含身份认证、验证和安装更新所需的所有信息和对象。容器包括以下内容：

- 二进制文件 — RAM 引导加载程序、Wi-Fi/低功耗蓝牙的 MAC/PHY 固件
- 证书 — 可以链接起来
- 签名 — 根据信任根公钥进行了测试
  - 版本信息
  - 依赖项

图 3-1 所示为容器的大致结构。

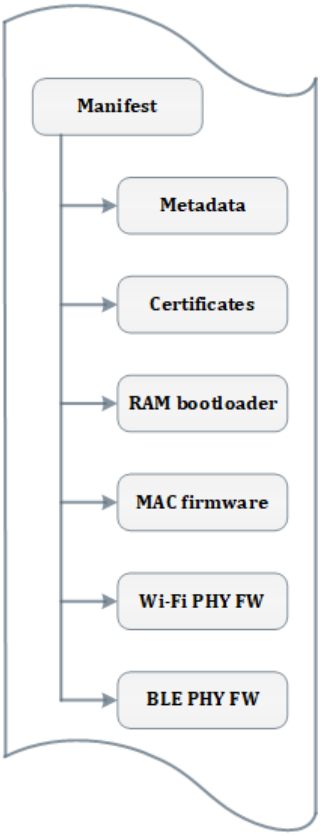

图 3-1. CC33xx 容器

该容器由德州仪器 (TI) 更新可用时进行发布，并在器件初始化期间使用，即从主机通过 SDIO/SPI 在运行模式下使用，或者从工具箱实用程序通过 SWD 线路在调试模式下使用。

3.1.2 安全启动流程

在启动流程中将解析容器并将其编程到器件中。此过程会对照 ROM 中存在的信任根公钥来检查不同二进制文件的真实性，匹配的私钥位于德州仪器 (TI) 服务器上。

节 3.1.2 展示了启动流程。

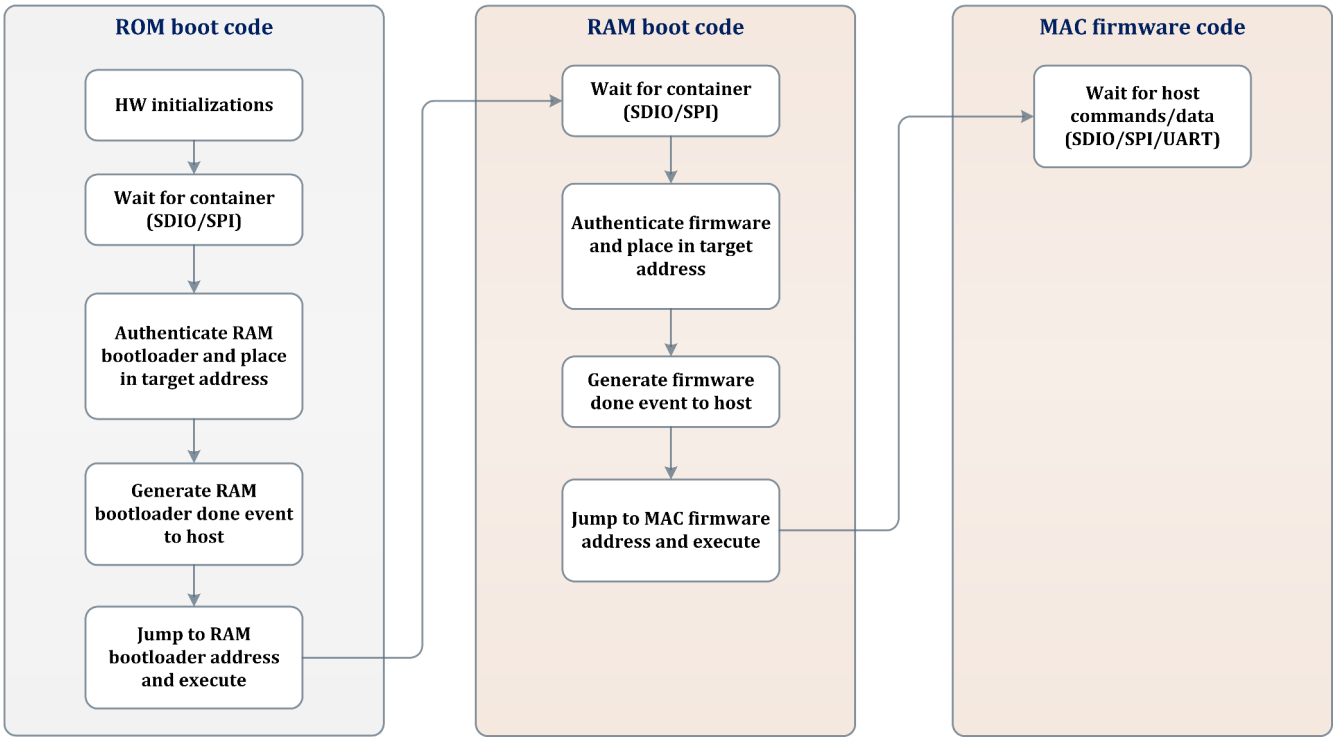

图 3-2. CC33xx 启动流程

启动流程分为两个主要阶段：ROM 启动模式和 RAM 启动模式。背后的逻辑是为了实现灵活性，在检测到错误或添加功能的情况下可以修改引导加载程序阶段，但不会影响安全性。两个引导加载程序分段都被视为在特权安全模式下运行。

在 ROM 引导加载程序阶段会初始化硬件。此步骤包括时钟检测、PLL 锁定、熔丝位验证等。接下来是测试器件的模式或生命周期。在大多数情况下，器件会在功能模式下运行，但在某些情况下，器件处于调试模式、测试模式或某种故障模式。本文档不介绍这些模式。最后在 ROM 引导加载程序分段，RAM 引导加载程序二进制文件以块的形式从主机处理器传出，并置于 RAM 中的目标位置。只有在二进制文件经过解密并根据信任根公钥进行了身份验证后，才会执行此操作。该阶段结束时会生成相应的事件并将其传播到主机处理器。

在 RAM 引导加载程序期间会执行类似的过程，但这次处理的是其余二进制文件，包括 Wi-Fi/低功耗蓝牙 MAC 固件、Wi-Fi PHY 固件和低功耗蓝牙 PHY 固件。该阶段结束时会生成相应的事件并将其传播到主机处理器。此时，固件正在运行并已准备好从主机处理器获取命令和数据。

3.2 Wi-Fi 网络安全性

CC33xx 配套 IC 的 Wi-Fi 层符合 802.11 安全标准，可确保 AP 与 STA 之间或 Wi-Fi 直连模式下两个对等方之间的事务中的帧（L2 数据单元）的完整性和机密性。IEEE 802.11 规范及扩展中描述了这些安全协议。

CC33xx 配套 IC 的 Wi-Fi 子系统支持个人或企业安全模式，包括基于 RADIUS 的身份验证 (802.1X)。

> CC33xx 配套 IC 中未实施 Wi-Fi 企业版，而是在外部（例如，Wpa_supplicant 和 hostapd）实施。

CC33xx 配套 IC 符合 Wi-Fi Alliance (WFA) 安全标准和测试套件要求。

表 3-2 列出了支持的 Wi-Fi 安全相关功能。

表 3-2. Wi-Fi 安全

类型	Wi-Fi 安全
个人	WPA-PSK (TKIP)
	WPA2-PSK (AES)
	WPS PBC + PIN
	WPA3 (SAE)
	(PMF)，
企业版（对于基站模式，支持 192 位的 GCMP 长密钥）	EAP TLS
	EAP TTLS
	EAP TTLS-MSCHAP
	EAP PEAPv0-MSCHAP
	EAP PEAPv1-TLS

3.3 回滚保护

回滚保护是一种内置的硬件机制，用于确保不会重新安装和恶意使用早期版本的固件。基本假设是存在漏洞（通常是实施问题）并会随着时间的推移而检测到漏洞。因此，安全启动将分区为 ROM 和 RAM 以允许更新安全启动代码本身。实际版本保存在熔丝位中，反映 RAM 引导加载程序、不同固件二进制文件和德州仪器 (TI) 证书吊销列表的版本。初始化时会测试受版本控制的元素，以使版本等于或高于配置的版本。

回滚保护机制最多包含 16 个版本的 RAM 引导加载程序和 32 个版本的固件。

3.4 JTAG 保护

CC33xx 配套 IC 还包括一个两线制串行线调试 (SWD) 接口。SWD 接口与主机接口无关，可以在引导时使用此接口，而不是使用主机接口来进行无线电测试。通常，SWD 接口已锁定，以便对 CC33xx 上部署的软件和硬件进行开发、调试和分析，客户可通过 SimpleLink™ 平台 Wi-Fi 工具箱中的无线电工具实用程序来使用此接口。

3.5 安全主机接口

> 主机接口安全性仍在设计阶段，且必须在后续阶段实现。尽管如此，此处还是介绍了主机接口安全性以供参考。

安全主机接口侧重于处理从主机 MCU/MPU 子系统传输到 CC33xx 配套 IC 的流量。潜在的黑客可能会劫持接口硬件线路，并使用这些线路读取加密密钥、数据单元有效负载等机密信息。黑客还可能会向这些线路写入数据，导致器件出现意外的行为，或向主机控制器发出误导性事件，如图 3-3 所示。

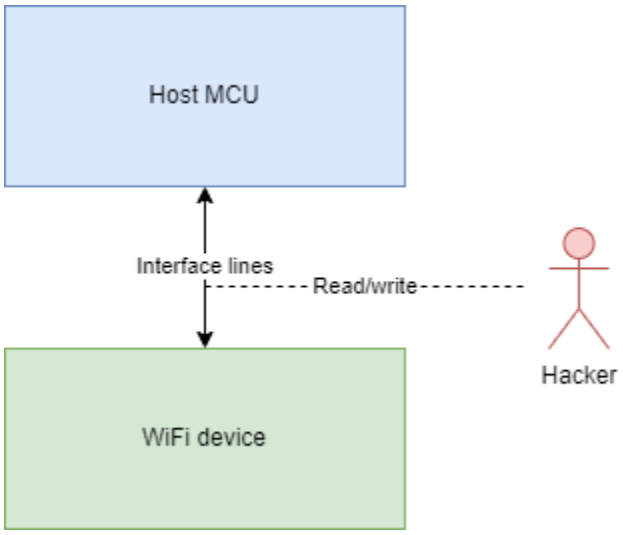

图 3-3. 主机接口威胁

4 修订历史记录

注：以前版本的页码可能与当前版本的页码不同

Changes from Revision * (September 2023) to Revision A (January 2024)	Page
• 在主要特性列表中添加了“JTAG 保护”特性	1
• 按照重要性顺序移动了主要特性	1
• 更新了“安全主机接口”以删除误导性信息	1
• 更新了“CC33xx 引导流程”图以反映当前状态	1
• 更新了 Wi-Fi 安全套件	1
• 删除了“独立执行环境”特性以防混淆	1

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