Application Notes

ZHCAB84 – March 2022

AM2X MCU+系列芯片安全启动方案

Jane Lu

摘要

随着物联网，工业互联网、云计算、大数据等技术的快速普及，网络上所有活动和设施在理论上呈现透明化，一旦遭受攻击，安全和隐私将面临巨大威胁。这些安全威胁可能来自任何地方，甚至是毫不起眼的终端节点设备。万物互联，安全先行，工业界对产品安全性的需求越来越迫切，包括安全启动，安全网络等等。

TI（德州仪器）发布的 SitaraTM AM2x MCU 产品集成了丰富的信息安全特性，可以帮助客户实现灵活的安全功能方案，包括芯片安全启动、加解密硬件加速器、内存 ECC 校验，安全调试、可信运行环境（TEE）等。

本文将介绍 AM2X 系列芯片安全启动相关的密码学方法以及安全启动方案。

Abstract

With the rapid spread of technologies such as IOT, industrial Internet, cloud computing, Big Data, and so on, all activities and facilities on the network are theoretically transparent, security and privacy are at great risk once attacked. These security threats can come from anywhere, even from unobtrusive end-node devices. The need for designers to improve security of products is also increasing in the industrial, including security boot, security network, etc.

Texas instruments SitaraTM AM2x MCU product integrates rich information security features to help customers implement flexible security feature scenarios, including security boot solution, cryptography hardware accelerator, memory ECC features, Safe debugging, Trusted execution environment (TEE), and so on.

This paper presents the cryptography fundamental methods used by AM2X devices and its security boot solution.

Contents

1. 安全启动简介

芯片上运行的代码通常会面临两种风险：代码被恶意更改(攻击)以及代码 IP 被非法读取（被盗）。

防止代码被恶意攻击，需要引入一种安全机制，保证芯片只运行用户指定的程序，防止代码被恶意更改。防止代码被盗则可以对代码进行明文加密存储，启动过程中再通过解密后运行来实现。AM2x 系列芯片集成了安全功能模块 HSM/DMSC，通过对启动代码的数字签名认证、代码加解密等流程保证了芯片代码的信息安全需求。

支持安全启动的 TI 芯片上还集成了一次性编程储存模块，我们称之为 OTP(one time programable)区，它的工作原理跟现实中的保险丝类似：CPU 在出厂后，这块 OTP 空间内所有的比特都是 1，如果向一个比特烧写 0，就会彻底熔断这个比特，再也无法改变它的值，也就是再不能改为 1 了。这个 OTP 区域用来存储用户的密钥信息。

安全芯片在复位后就会进入安全启动流程，安全功能模块开始执行芯片 security ROM 的代码，并用 OTP 区域中的密钥信息对加载的用户代码进行多级安全认证，逐步建立起用户代码的安全信任链。AM2X 的安全启动方案可以实现用户软件版本信息安全的五大特性：

1. 真实性：软件版本未经篡改
2. 完整性：软件版本包含了开发者发布的所有内容，没有内容删减
3. 机密性：软件版本不泄露给未授权的个人、实体、进程，不能被非法盗取
4. 时效性：软件版本是在有效期间内的版本
5. 不可抵赖性：软件发布后，发布者不能否认版本的所有权

2. 安全启动采用的相关密码学方法

2.1. 代码明文加密和对称加密算法

为了保护软件版本 IP，防止被非法盗取，用户可以选择把版本做加密保护。AES 技术是一种对称的分组加密技术，具有应用范围广、等待时间短、相对容易隐藏、吞吐量高等优点，通常被采用做代码加密处理。

所谓对称加密算法，是指用来加密和解密的密钥是相同的密钥。如图 1-1 所示，代码发布者 A 可以将代码明文用加密算法处理成密文作为芯片启动加载的软件版本。安全芯片将加密后的代码读取到内存，再用 OTP 存储模块上事先烧录的密钥进行代码解密，解密过程中用到了加密过程中相同密钥及相同算法的逆算法，从而对密文进行解密，恢复代码明文。 它的最大优势是加/解密速度快，适用于大数据量的加密。

图 1-1. 代码加密图

图 1-2. 代码解密图

2.2. 数字指纹和哈希函数

哈希函数，又称散列算法，是一种从任何一组数据中创建小的数字“指纹”的方法。 如图 2 所示，哈希函数可以把任意长度的消息或数据压缩成固定长度的数字摘要，重新创建一个叫做散列值（或哈希值）的指纹。 哈希变换有两个特点：

1. 加密过程不可逆。这意味着用户无法通过输出的散列数据倒推加密前的明文是什么。
2. 一一对应性。输入的明文和输出的散列数据一一对应，不会存在两个不同明文对应同一个输出的散列数据的情况。

在安全启动中，SHA 哈希函数通常用来对芯片运行的代码版本创建数字“指纹”，以检验代码的完整性。

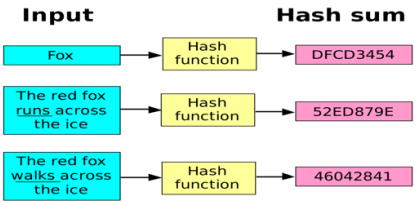

图 2. 哈希变换示意图

2.3. 信任问题和非对称加密

安全芯片加载软件版本的过程中需要解决一个信任问题，即安全芯片如何确定加载的版本是软件发布者 A 授权的软件版本而非其他人的非法版本？ TI 的安全启动方案用 RSA 非对称加密算法来解决这个问题。

非对称加密算法中，有两个密钥：公钥和私钥。它们是一对，如果用公钥进行加密，只有用对应的私钥才能解密；如果用私钥进行加密，只有用对应的公钥才能解密。 密钥的长度越长，算法越安全，破解密钥所需的时间也越长。以目前的算力，破解 RSA 2Kbits 密钥的时间需要十年以上的时间，破解 RSA 4Kbits 密钥长度的时间需要 20 年以上的时间。

在 AM2X 安全启动方案中，如图 3-1 所示，版本发布者 A 可以用 RSA 私钥对代码版本的哈希数字“指纹”进行加密，作为软件版本的数字签名。如图 3-2 所示，芯片侧用配对的公钥对数字签名进行解密，以此验证版本的真实性。一旦验证成功，此版本也具备不可抵赖性，因为只有软件发布者 A 拥有私钥去生成有效的数字签名。

图 3-1. 生成数字签名

图 3-2. 解密哈希指纹

2.4. 公钥信息交互和数字证书

为了保证密钥信息传输的安全性和保密性，需要建立一套信任机制来传递密钥。数字证书是一种权威性的电子文档，是由证书签证机关（CA）签发的对用户的公钥的认证。证书的内容包括：电子签证机关的信息、公钥用户信息、公钥、有效期和数字签名等等。AM2X 系列安全芯片的启动文件证书的格式和验证方法遵循 X.509 国际标准。

3. AM2X 芯片安全启动方案

AM2X 安全启动版本文件包括两部分内容，符合 X.509 格式的数字证书和用户软件版本。

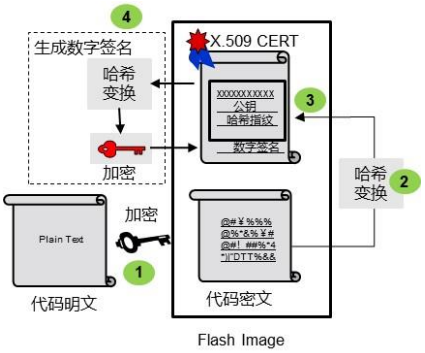

图 4-1. 安全启动镜像

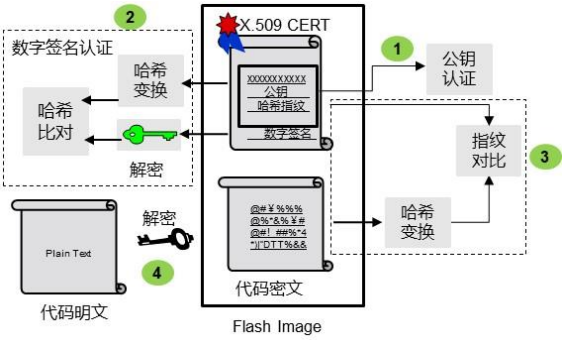

图 4-2. 安全启动流程示意图

图 4-1 是安全启动镜像生成示意图，具体操作流程如下：

1. 用户采用 AES 对称加密算法将代码明文转成密文，用户也需要在 AM2X 加密版本芯片的 OTP 上烧录这个密钥
2. 用户采用 SHA 哈希函数对代码密文计算出一个固定长度的哈希值，即软件代码的哈希指纹
3. 用户生成 X.509 格式的数字证书文件，该文件会包含哈希指纹，以及一个 RSA 公钥
4. 用户采用 SHA 哈希函数对数字证书文件进行哈希计算并得到证书文件的哈希指纹，用户用 RSA 私钥对该数字指纹进行加密，得到用户的数字签名。

图 4-2 是安全启动流程示意图，具体操作流程如下：

1. AM2X 芯片复位后，AM2X 的 HSM 模块先对 Flash 中烧录的 X.509 数字证书上公钥信息进行哈希计算，并与芯片 OTP 区事先存储的公钥哈希值进行比对，确认公钥的合法性。这是信任链的第一环节。
2. 公钥合法性确认后，AM2X 的 HSM 模块再利用 X.509 证书上的数字签名进行用户合法性鉴权。具体方法是用公钥对数字签名进行解密，得到证书的哈希指纹；同时对 Flash 上的 X.509 证书也重新计算哈希指纹，对比两个指纹值是否一致。如果指纹匹配，则鉴权成功。
3. 验证用户软件版本的完整性和合法性，AM2X 的 HSM 模块通过重新计算 Flash 上软件版本的哈希指纹，并与 X.509 证书上的哈希指纹值进行比对，确认是否匹配。匹配成功说明代码没有被恶意篡改。
4. AM2X 的 HSM 模块用 OTP 区上的 AES 密钥对代码进行解密，得到明文代码。

AM2X 系列 MCU+芯片实际安全版本镜像制作过程和安全启动流程会比上述内容更复杂和严密，涉及安全流程机密细节，具体内容不再展开。TI 会给选购 TI 安全芯片方案的客户提供更为详细的文档和工具，以协助客户实现安全启动方案。

4. 总结

本文详细介绍了 AM2X 系列芯片安全启动采用的密码学方法以及安全启动方案。利用这些方法和安全启动方案，用户可以轻松实现代码 IP 知识产权保护、产品安全防黑客攻击等安全需求。除了 AM2X 系列芯片，TI 在其他 EP 产品如 MSP430、Sitara MPU、C2000、CONNECT、DRA7X/8X 等产品都提供安全特性，如需了解更多关于 TI 功能安全产品信息和保护手段，可以访问 TI 网页 www.ti.com/security 获取更多内容。

5. 参考文献

1. Security BOOT on embedded Sitara Processor（spry305a）.
2. Building your application with security in mind (swpb020e)

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