参考文献

保护基于 Arm 的应用处理器

Texas Instruments

Amrit Mundra
Security Architect and Systems Engineer

简介

计算机安全曾一度意味着电脑中恼人的病毒。后来，计算机安全的范围不断扩大。对企业和政府系统的黑客攻击使个人和财务信息暴露在欺诈、盗窃和挪用的风险之下。但现在，嵌入式系统的安全，或者更准确地说，嵌入式系统的不安全，对非常关键的数据构成了威胁。

如今，世界依靠数据运转，每个比特或字节都应被视为潜在的攻击目标。与此同时，软件和硬件系统都变得更加复杂、相互连接和相互依存。随着复杂性而来的是脆弱性。数十亿行或数万亿行代码以及相互关联的硬件模块、子系统和分区全都挤在极小的硅片上，这让黑客不亦乐乎。

当然，黑客也不会停滞不前。有关嵌入式系统漏洞的报道不绝于耳：卫星通信系统、无线基站、住宅和企业中的激光打印机、智能电网、除颤器等医疗设备以及许多其他系统都存在风险。随着时间的推移，对多核嵌入式片上系统 (SoC) 安全的需求越来越高。心脏设备、智能手机和汽车控制单元等嵌入式设备依靠包括嵌入式 SoC 在内的多个元件来保护控制中心。

首先，我们来介绍一下帮助确保嵌入式系统中基于 Arm® 的多核应用处理器安全的必备要素。其次，我们将详细探讨这些处理器的基础安全层，即安全启动，因为有了安全启动，系统从“开机”起就受到了保护。如果没有安全启动，系统从“开机”到使用就会有一段空白。随着威胁的不断变化，安全始终是一个移动的目标。

保护系统不受黑客攻击，防止黑客窃取数据或接管系统另作他用，是系统安全方面的目标。这与功能安全的相关概念不同。安全则更侧重于确保系统有条不紊地应对各种情况，并在必要时从容应对。这些概念的结合意味着系统将在现实世界中按照预期运行（在现实世界中会发生故障，也会有坏人存在）。

风险管理

安全威胁始终存在，并且随着物联网 (IoT) 的快速普及，这些威胁可能来自任何地方，甚至是不显眼且低成本的终端节点设备。基本的安全问题不是系统是否会受到攻击，而是何时会受到攻击。由此得出的结论是，安全既是保护，也是风险管理。

考虑到系统可能会受到攻击，系统设计人员如何尽可能降低安全漏洞的风险？

该保护什么内容？

任何有价值的东西都可能受到攻击。当然，根据黑客的视角和意图，几乎所有东西都可能被认为是有价值的。从最原始的层面上讲，对大部分黑客来说，仅仅是入侵系统的快感就具有价值。大多数黑客都不是无害的寻求刺激者。许多黑客会毫不犹豫地撬开电子钱包或窃取信用卡和银行账号等财务信息用于欺诈。IP 可能被窃取用于销售或获取竞争优势，而政府机密则可能被盗用于破坏、损害或摧毁运输系统、供水系统、能源分配网络、核电站和国家公共基础设施的其他方面。

当然，所有这些有价值的东西都必须受到保护，但在此之前，安全系统本身必须安全。对于嵌入式系统来说，系统内的安全要素及其保护的内容必须得到保障。在最基本的层面上，这意味着要确保用于验证软件、用户和连接链接的加密密钥和身份的安全。这也意味着要确保网络中每个系统或节点上运行的软件的完整性。这就要求即使是网络或互联网中最不起眼的节点上的启动和运行时软件也要具有可见性和可控性。

有多安全？

安全和其他一切事物一样，都是有代价的。系统开发人员的安全成本包括设计安全措施并将其集成到系统中的成本，以及这些安全措施对系统性能的影响。鉴于安全威胁的性质不断变化，以及嵌入式系统通过 IoT 等举措不断普及，新系统的设计应包括制定一套衡量标准，衡量安全成本与安全效益。嵌入式器件可以被接管并用作对可能拥有更有价值资源的其他系统进行攻击的发射台。例如，入侵打印机/复印机可能不会给黑客带来太多价值，但如果打印机打印或复印的每个文档都被捕获并发送给黑客，那么损失可能是巨大的。

嵌入式系统在安全成本方面具有优势，因为许多基于嵌入式系统的产品已大量生产。因此，为这些产品开发的安全子系统的成本可以在大规模生产运行中摊销，从而降低单位安全成本。此外，为新设计开发的多功能、可扩展和可移植的安全架构通常可以转移到紧密相关的系统中，或者可以稍微修改该架构以适应其他产品的需求。

架构注意事项

许多安全子系统都采用分层架构，并充分利用了分区的优势。分层部署安全措施会对系统的安全产生累积效应，因为每一层都可以在采取任何行动之前对其下层或上层的安全进行认证。分区对于确保系统上运行的软件的运行时安全非常重要，它使设计人员能够根据受保护资源或进程的相对价值来定制安全措施。

嵌入式安全可以从硬件开始着手。 将软件和硬件安全功能结合在一起，能提供比单独使用任何一种解决方案都更安全的保护层。此外，供应商提供的工具可以简化安全子系统的开发，并确保最终的架构满足开发人员的要求。例如，基于硬件的安全加速器可以降低安全子系统的性能成本。

当然，安全架构的强度取决于其构建的基础。基础层的三个方面至关重要：安全启动过程、基于硬件的器件 ID/密钥和加密加速。

安全金字塔

安全金字塔（参阅**图 1**）展示了多核 SoC 嵌入式处理器的综合安全子系统的各个层和组成部分。

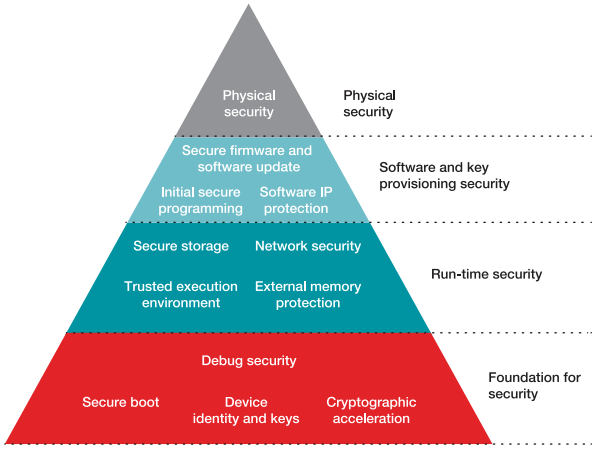

图 1. 安全金字塔。

安全引导

安全启动过程会为嵌入式系统建立信任根。即使从外部闪存存储器初始化启动，安全启动过程也会通过多种机制（包括嵌入式加密密钥等）验证启动固件的完整性。安全启动层可防止恶意软件接管系统、任何可能的系统内 IP 克隆、无意中执行不需要的应用以及其他安全风险。

安全启动还通过加密 IP 和安全复制 IP 来保护内部存储器，从而提供额外的保护。加密功能还能为代码库提供额外的安全，因为它能禁止进行定向探索攻击。

总之，安全启动有助于为嵌入式系统安全奠定基础。

加密加速

加密处理涉及各种公钥和私钥的生成、验证和认证，可能会影响嵌入式系统的性能和吞吐量。一些多核应用处理器配备了基于硬件的加速器或协处理器，可以极大地加快编码/解码过程。基于软件的加速也可用，但作为软件，它本质上不如基于硬件的加密加速安全。

常见加密元素	
随机数发生器 (RNG)	由加密算法和哈希函数使用。硬件生成的随机数比软件生成的 RNG 更安全。
加密算法	
三重数据加密标准 (3DES)	3DES 执行三次 DES 加密，以加强对加密数据的保护，并克服 DES 算法的一些漏洞。
公钥算法 (PKA)	使用 RSA 的加速 PKA 或使用公钥/私钥的 ECC 非对称加密。有助于安全启动中使用的身份验证。
高级加密标准 (AES)	AES 是当今广泛使用的先进加密算法之一。
哈希函数（用于签名、身份验证等）	
消息摘要算法 (MD5)	尽管这种哈希函数已被广泛部署，但它在某些应用中存在一定的漏洞。
安全哈希算法 2 (SHA2)	处理大的哈希，因此比 SHA1 更安全。

***表 1.** 常见加密函数的示例。*

器件 ID 和密钥

为了信任通过局域网 (LAN)、广域网 (WAN) 或互联网进行的通信，器件必须具有可共享的唯一身份。然后，通信器件可以决定参与对话的其他器件的真实性或可信度。

应用处理器通常附带某种唯一身份 (ID) 代码。或者，除了 ID 代码之外，器件还可以通过签名或证书密钥以及可通过云服务等访问的相应公钥来识别自己。

图 2. 器件 ID 有助于防盗。

调试安全

在系统开发过程中，设计人员需要访问嵌入式多核应用处理器，以便调试固件和软件，并解决可能的硬件问题。在大多数情况下，提供此访问的端口是 JTAG 端口。在工作环境中，调试端口必须通过某种保险丝密封闭合，或者只能通过经过认证的加密密钥进行访问。否则，调试端口会为黑客提供进入系统的便捷途径（参阅**图 3**）。

图 3. MSP430™ MCU 调试端口。

可信执行环境

运行时安全层由几种不同的功能组成，它们都在启动过程后和系统的操作系统 (OS) 执行过程中起到保护系统的作用。运行时安全的一个重要方面是监控系统的方方面面，以确定何时发生或试图发生入侵。

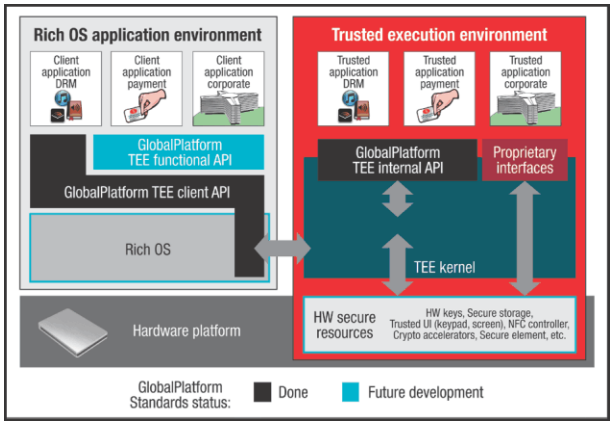

图 4. 可信执行环境 (TEE)。

可信执行环境安全使系统能够同时托管安全和非安全应用，并通过系统维护分区，确保数据不会泄露。运行敏感应用时，必须将应用和相关代码/数据库与其他应用完全隔离。

可信执行环境主要是在多核系统中提供一个安全分区，只有经过认证的安全固件、软件和应用才能在此执行，并存储经过认证的数据。

将可信执行环境与多核/多处理系统的其他部分隔离，可防止可疑代码、应用和数据通过系统传递，污染任务关键型软件、数据和其他 IP。

外接存储器保护

当设计人员必须在系统中添加另一个应用或子系统时，他们通常需要向主处理器添加外接存储器并通过存储器总线进行连接。设计人员必须保护存储在外接存储器中的数据免遭篡改或替换，以确保只有可信数据或应用代码存储在外接存储器中。可以采用多种方法来保护外接存储器的内容，例如：直接从外接存储器进行安全的就地执行，而不将数据加载到处理器的集成存储器中；可以保持机密性，同时允许应用在主处理器上运行的动态解密；以及其他方法。

图 5. 安全存储器。

网络安全

黑客非常擅长拦截无线或有线网络通信。事实上，一些通信协议已经存在已知的安全漏洞，并已被利用。仅部署高度安全的通信协议通常需要大量的处理周期来加密和解密通信流，以及验证发送者或接收者的真实性。设计人员有时面临着平衡通信吞吐量和安全的问题，但一些嵌入式处理器通过集成基于硬件的加密算法加速器（与标准通信协议结合使用）来避免这种困境。

图 6. 安全存储。

安全存储

加密密钥和安全数据必须存储在系统存储器中不被意外访问的位置。可使用多种功能来提供安全存储，包括加密密钥块、只能通过主密钥解锁的防篡改保护、非易失性存储器和加密引擎之间的私钥总线等。

初始安全编程

在当今的全球化时代，设计、密钥配置和制造相互脱节，有时甚至相距甚远，这给确保密钥等安全资产的安全带来了挑战。让问题变得更复杂的是，这种商业模式可能涉及到完全不可信的生产设置的 ODM。

初始安全编程等信息安全机制提供了一种方法，客户可以对它们进行评估并选择使用，以加强在不受信任的设施中或在应用首次启动期间编程的初始固件或密钥的保密性、完整性和真实性。

安全固件和软件更新

更新系统的能力是安全架构的重要组成部分，这为客户提供了远程修补或更新软件的机会，以消除系统中已发现的漏洞，但更新过程中的主要挑战是如何防止间谍、冒充和重播。

安全架构提供额外的密钥和机制，如身份验证、加密和完整性检查，可用于确保更新的真实性。

软件知识产权 (IP) 保护

客户为创造知识产权 (IP) 进行了大量投资，而这些知识产权对市场上的最终用户来说可能是至关重要的价值主张，因此，安全架构必须提供加密启动、隔离处理能力和防火墙等机制，让客户能够保护其知识产权。

物理安全

据了解，老练和不太老练的黑客组织都会从系统中取出芯片，或从芯片封装中取出硅片，以访问嵌入式资产。

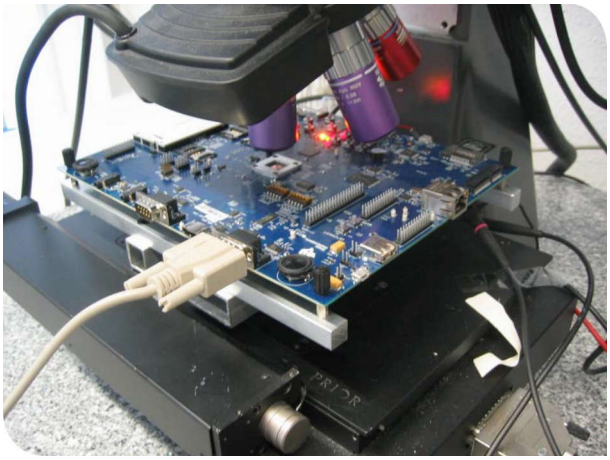

图 7. 受到物理攻击的系统。

一旦器件或芯片被取出，黑客就可以用激光对其进行轰击，将其功率提升到超过规定的功率限值，或采用其他手

段。他们的目标是观察器件对刺激的反应，因为这种反应可能会泄露黑客可以利用来访问器件的漏洞。

一些应用处理器已经集成了硬件和软件功能，以阻止对 SoC 数字和模拟部分的物理入侵。集成到多核应用处理器中的防篡改模块可以包含电源和温度监测器、复位功能、频率监测器和可编程防篡改功能。

外壳保护

外壳保护功能是保护系统外壳的物理措施，包括锁定装置、电子开关、断线跳闸装置等（参阅图 8）。

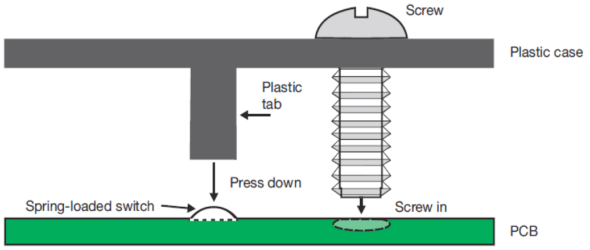

图 8. 外壳保护。

嵌入式安全从何入手？

嵌入式多核应用处理器安全的根本基础始于硬件。如果硬件不安全，再多的安全软件也无济于事。假设硬件内置了安全功能，那么开始构建安全子系统的第一个地方就是开机后执行的第一个软件，即启动代码。如果启动过程无法通过身份验证，那么系统上运行的其他软件也无法通过身份验证。因此，确保启动过程的安全是系统各方面安全所依赖的支点。

安全启动过程可建立信任根，这是每个安全子系统的目标。通过安全启动过程建立信任根有助于确保系统的完整性并防止黑客接管系统的任何部分。这还有助于保护系统中的客户软件，并起到防克隆屏障的作用，使系统或其任何部分都无法被复制。

通常，安全启动过程涉及将公共加密密钥编程到系统中某处的非易失性一次性可编程存储器中。然后，必须将该公钥和与启动代码相关的私钥/公钥进行匹配，以便在开始执行前验证加密启动代码的有效性。启动固件既可以加载到嵌入式处理器的 RAM 中，也可以在嵌入式处理器的外接存储器中就地执行，以提高安全性。一些固件映像由各种组件或模块组成。在解密和执行每个模块之前要求进行身份验证可提高启动安全。

TI 应用处理器的信息安全机制

我们基于 Arm 的应用处理器提供了一整套信息安全机制，帮助开发人员部署安全措施，保护他们的资产（数据、代码、身份和密钥）。

信息安全机制	AM335x	AM437x	AM438x	AM570x/ AM574x	AM64x/AM65x	AM62/ AM62L/ AM62P	AM68x/AM69x	DRA821/ DRA829/ TDA4VM
加密加速	✓	✓	✓	✓	✓	✓	✓	✓
器件身份/密钥	✓	✓	✓	✓	✓	✓	✓	✓
安全启动	✓	✓	✓	✓	✓	✓	✓	✓
调试安全	✓	✓	✓	✓	✓	✓	✓	✓
外接存储器保护			✓		✓	✓	✓	✓
可信执行环境 (TEE)		✓	✓	✓	✓	✓	✓	✓
网络安全					✓	✓	✓	✓
安全存储		✓	✓	✓	✓	✓	✓	✓
软件 IP 保护	✓	✓	✓	✓	✓	✓	✓	✓
初始安全编程	✓	✓	✓	✓	✓	✓	✓	✓
安全固件更新	✓	✓	✓	✓	✓	✓	✓	✓
物理安全			✓					
申请访问权	联系 TI 代表	更多信息	更多信息	更多信息	更多信息	更多信息	更多信息	更多信息

表 2. TI 应用处理器的信息安全机制。

结论

嵌入式处理器安全是一个多方面的复杂课题。随着 IoT 的兴起和嵌入式系统的普及，黑客现在比以往拥有更多的主要目标。

当然，硬件中必须已经具备基本的安全功能，但为嵌入式多核 SoC 构建安全子系统应该从安全启动的基础层开始。如果没有来自安全启动过程的信任根，其他任何安全措施都无足轻重。一旦建立了这种信任根，系统安全的其他方面，例如调试安全、运行时安全和网络安全，就有了坚实的基础。否则，一切安全措施都是徒劳。

参考资料

1. 德州仪器 (TI)：*电子书：在构建应用时将考虑安全性考虑在内* (SWPB021)
2. 德州仪器 (TI)：***利用硬件加速加密技术提高安全和芯片性能***
3. 德州仪器 (TI)：***嵌入式 Sitara™ 处理器上的安全启动***
4. 德州仪器 (TI)：***Sitara AM438x 处理器：防篡改***

重要声明: 本文所提及德州仪器 (TI) 及其子公司的产品和服务均依照 TI 标准销售条款和条件进行销售。建议客户在订购之前获取有关 TI 产品和服务的最新和完整信息。TI 对应用帮助、客户的应用或产品设计、软件性能或侵犯专利不负任何责任。有关任何其它公司产品或服务的发布信息均不构成 TI 因此对其的认可、保证或授权。

Arm® is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.
所有商标均为其各自所有者的财产。

© 2025 Texas Instruments Incorporated

重要通知和免责声明

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 产品的相关应用。 严禁以其他方式对这些资源进行复制或展示。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
版权所有 © 2025，德州仪器 (TI) 公司