白皮书

互联世界的安全

Kimberly Dinsmore，物联网基础设施业务部门高级工程师，瑞萨电子株式会社

2019 年 9 月

摘要

“安全”这个词总是能引发人们的各种反应，但它的含义却因语境的不同而大相径庭，即使将范围缩小到电子设备领域亦不例外。对消费者而言，“安全”通常意味着个人数据不会被特定目标接收者之外的任何人获取；但对于使用微控制器作为主控的产品，往往并没有多少最终客户数据需要被保护。还是让我们来看“安全”一词的其他解读。对于软件开发者，“安全”可能意味着代码不能被任何人窃取。对于 OEM 厂商，“安全”可能意味着任何人都不能克隆其设备。对于服务提供商，他们会通过电子设备提供服务，“安全”通常意味着如果未经正确授权或付款，任何人都不能使用他们的服务。而对于政府，“安全”可能意味着设备不能被渗透并用作 DDoS 攻击的武器。无论何种市场领域，上述所有定义都绝对适用于微控制器以及基于微控制器的产品。

一旦涉及到安全领域，大家通常就会面对数不清的新术语和缩写词，多得令人生无可恋。让我们一步一步来，先避开艰涩的词汇，看看如何将安全功能集成到基于 MCU 的设计中？

第 1 步：从一开始就致力于安全设计。

在开始新设计时，高层管理者会追求进度，对他们而言，就是尽快有一个原型机，但原型不必追求安全，而且安全性无法成为一个华丽的演示亮点来打动管理层和投资者。将安全性放到设计最后阶段再考虑这一想法的确令人心动，但还是应当抵御这种诱惑。如果换种做法，前期确实需要花费一些时间，而且往往需要说服管理层，但事实已多次证明：安全性无法半途植入到设计中。安全不是一种插件，它是最基本的架构基础。试图后期添加安全性几乎都会导致系统的完全重新设计 ——逐字节生成和传输的数据流无法转换成加密数据块，硬编码的明文私钥无法神奇地变成安全存储的设备唯一密钥，等等等等。

第 2 步：您的产品是否符合行业或政府法规要求？

这项要求往往会推翻关于安全的任何其他想法。如果您所在行业要求使用特定的加密功能套件，即使有能够提供相同级别保护的其他替代方案可以选择，您也必须采用规定的套件。例如，金融交易和电能表，就是存在特定法规而且必须要遵守的两个示例。因此，务必要研究和了解适用于您的产品的所有法规要求，确保您的产品符合最终使用地域的一般政府法规。

第 3 步：您要保护什么？

大多数公司会按照成本要求来确定这个列表，这也是 GDPR 罚款如此之高的原因。政府发现，如果没有利润驱动，公司更愿意事后修补安全漏洞，而不是主动努力预防安全漏洞。创建这个列表时，首先往往会关注设备本身和数据：固件、密钥和客户信息，而不是超越设备本身，将系统作为一个整体来考虑。您可能认为某些数据并非敏感信息，但是否会有人在正常运行期间操控您的设备而造成不利影响（例如 DDoS 攻击）？如果您的设备负责某项关键功能，那么您需要保护该功能，防止任何不当修改。如果需要使用密钥来启用某个服务，那么该服务本身就需要获得保护。

第 4 步：您的薄弱点是什么？

再则，来看设备及其部署的基础设施。在考虑设备时，一个明显的技术漏洞是互联网连接。基于 MCU 的产品通常并不重视这一点，因为非 Linux 的 IP 连接一般不会成为攻击者的目标，而且传输的数据的价值也有待商榷。但是，如果您的设备通过互联网执行固件更新，并且您希望保护自己的代码，那么 IP 连接就会成为漏洞。即使您的设备并非采用 IP 连接方式，也要考虑与外部世界的所有连接。在考虑产品运行环境的同时，也不要忘记考虑人为因素。令人悲哀的一点是，先进的安全技术有时会被一场精心安排的诱骗完全避开，您可以想象恶毒或者只是怀有恶意的演员所能做的事情。

第 5 步：您信赖谁？

有句话说“不要相信任何人”，但安全解决方案会增加成本，这是无法回避的事实。所以，不要将金钱浪费在预防一些不存在的威胁之上。如果您的产品是在工厂现场制造的，那您可能不必再投资购买安全编程解决方案；不过，如果设备编程并非在现场进行，或需要对包含密钥或其他敏感数据的设备进行编程，则您可能需要安全的编程解决方案。

第 6 步：确定您产品的限制范围。

如果有充足的时间和资源，那么任何保护都可以被攻破。所以，您必须确定自己需要保护的范围。一方面，要限制不必要的调试器访问；另一方面，要阻止别人解封 MCU 并使用电子显微镜分析芯片。有时，这些限制由产品的监管机构决定，但它们往往只是按常理判断。例如，如果您的主要目标是保护固件 IP，那么则无需采用能抵御边信道分析攻击的 MCU。

第 7 步：制定计划。

决定如何在您设置的限制范围内，利用您信任的元素保护您的资产不受漏洞的影响。有时，这也称为威胁模型、威胁分析、安全评估或安全策略，这项工作需要花费大量时间，以确保合理地关注重点部分并投入预算。这最后一步也十分重要，以防出现任何问题。如果您能证明已通过尽职调查来评估产品的安全需求，则有助于反驳所谓的疏忽之过。

威胁、漏洞和受信任方的组合随嵌入式设备的数量变化而不同，但幸运的是，它们存在一些通用的主题和解决方案。

保护静态数据安全

设备安全的基本要求是能够在设备上安全地存储数据，但就像安全领域的所有事项一样，安全存储包括不同的方面。如果您的设备没有外部连接，那么保护 MCU 则非常简单，禁用或限制所有调试器和编程器访问

即可。如果您需要确保对设备闪存重新编程时不会导致设备本身意外损坏，那么许多 MCU 都具备将部分闪存或全部闪存设定为 OTP 的功能，这样可防止它们被擦除和/或重新编程（即使通过自编程）。不过，如果您的设备具有外部连接，那么您可能需要考虑从逻辑上将代码和数据划分为“受信任”和“不受信任”两类，并做出限制，只有“受信任”代码才能访问“受信任”数据。比较理想的情况下，应通过内存保护单元(MPU)或 Arm® TrustZone®等机制在硬件层面实现强制隔离。尽管这种隔离并非绝对安全，但却能够减小“受信任”数据的攻击面。

设备标识

如果您的设备需要连接基础设施，那么您需要通过某种方式对其进行唯一标识。您可以通过多种方式为每个设备提供唯一标识。有些 MCU 已内置唯一标识，但这些往往只是简单的序列化信息，需要进一步映射，中央控制中心才能识别哪个设备部署在哪里。这种功能可能已经够用了，但加密的唯一标识能更有用，它支持更多安全解决方案，例如保护动态数据的安全。

加密标识利用各种加密方案的特性，设备的标识就是加密密钥。基本选项有两种：

- 对称加密，即加密和解密数据的密钥相同。控制中心需要知道每个设备的对称密钥。
- 非对称加密，这种方案需要使用两个密钥，一个用于加密数据，另一个用于解密数据。功能可以互换，设备可以将一个密钥设为私钥。

难点在于，起初如何获取设备上的密钥，这样控制中心才能知道密钥或知道该密钥可信。这叫做配置。如果您产品的安全评估结果支持由可靠的技术人员执行安装和配置，那么您的解决方案可能包含生产现场进行设定甚至生成密钥。不过，如果您打算由消费者自己来安装产品，则需要安全地配置设备。这可以在安全编程期间完成。

保护动态数据安全

保护动态数据安全需要实现五个目标：保密性、数据完整性、数据源、身份验证和不可否认性。这些已经超出了我们现在讨论的范围。这里首先要考虑什么是通信基础设施？如果您的设备通过封闭式基础设施内的专有总线进行通信，那么满足这些需求的解决方案将与设备通过 Wi-Fi 连接互联网的情形完全不同。后者是最糟的情形，但也是物联网设备最常用的场景。加密标识是保护通过 IP 连接传输的动态数据安全的基本

构建模块。尽管加密标识看起来可能有些大材小用，但如果您的产品采用 IP 连接，就会要求采用加密标识。

安全编程

同大多数安全解决方案一样，安全编程可解决多种问题，并且具有多种选项。安全的部署解决方案可解决 IP 盗用、克隆和过度生产的问题，您可提供只能在特定设备编程器中解密的加密固件映像，并可以收到实际编程设备数量的检查报告。此外，有些安全编程解决方案可以将设备唯一密钥配置到 MCU 中。甚至还有一些高级解决方案，其中 MCU 自身即可生成非对称密钥对、导出公钥并接收和存储包括该公钥的签名证书，进而生成检查报告和一组可用于对最终产品进行身份验证的批准证书。这方面尤其需要获得生态系统合作伙伴对 MCU 的大力支持。

“安全”方案无法做到“一体适用”。因此，在开发初期明确产品的具体要求，选择具备所需硬件功能、软件支持和演示解决方案的 MCU，并由具有强大合作伙伴网络的可靠芯片供应商提供支持，这些都至关重要。安全性问题可能看似令人生畏，但只要正确选择 MCU，并有强大的生态系统支持为后盾，就能打造出适合当今互联世界的安全产品。