嵌入式系统的安全性

为保证密钥的安全性，密钥应永不离开嵌入式系统的边界，否则就为攻击者攻破设备的安全屏障提供了捷径。

嵌入式系统的安全性往往最后才会被考虑到。工程师们在设计产品时往往以迅速上市为目标，而将安全性问题留待将来的版本升级时再行解决。这也并非不合逻辑，因为高级别的安全性会增加产品的成本，并延迟上市时间。

然而，许多系统一开始时就需要高级别的安全性。有些情况下，安全要求出自政府或某些贸易组织。例如，Visa®和MasterCard®信用卡公司制订的PCI要求，对于销售点终端或PIN键盘的安全性要求提供了详细说明。在其他一些情况下，安全性设计被用来保护企业营收。安全应用能够阻止逆向工程设计，防止产品被仿制，或者提供真正的篡改侦测功能。

安全微控制器究竟做了些什么呢，为什么安全微控制器对于敏感应用如此之重要?

只有密钥安全，系统才会安全

安全性不仅仅取决于加密环节。尽管加密算法和密钥管理程序的选择很关键，但它们常常并不是安全应用中的薄弱环节。设想这样一种场景，Alice和Bob各有一部只能彼此通信的安全电话。电话的加密措施牢不可破，即使使用当今世界所有的计算能力，也需要一个世纪才能破解。那么，薄弱环节在哪儿呢？电话！如果攻击者控制了其中的一个电话，他或她就可以伴装Alice或Bob，立刻得到他们的秘密信息。攻击者甚至用不着偷电话，只要趁Alice或Bob不觉，简单地安装一个窃听装置就可以了。

在此场景中，加密措施并未被攻破，而是执行加密的设备，或者“密钥”，安全性被轻而易举地攻破了。在嵌入式系统中，密钥通常是一个很大的密码，被加密程序用来加密信息或认证数据。所以，一个安全嵌入式系统最为重要的工作就是保护该密钥。如果系统遭到攻击，必须清除该密钥，防止其落入攻击者之手。密钥的破坏使设备无法工作，避免攻击者获取敏感信息，例如银行帐号和密码。

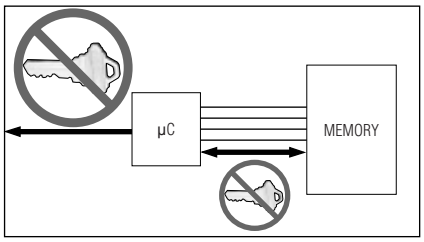

图1. 密钥数据不应离开设备，甚至不应在芯片间传送。

为保证密钥的安全性，密钥应永不离开嵌入式系统的边界，否则就为攻击者攻破设备的安全屏障提供了捷径(见**图1**)。设计专门的存储器保存密钥的做法不可取，因为微控制器和存储器之间的通信是可见的。最安全的做法是使密钥停留在处理器内部，并用它实现数据的加密和认证。这就是说，系统微控制器需要有内部的非易失存储器。

引发线和塑料保护

即使密钥数据只保存在微控制器中，攻击者还是有可能发现安全信息。例如，如果攻击者可以访问微控制器地址和数据总线，他就可以通过插入指令的办法使密钥数据暴露于外部I/O口。更高级的攻击者还可以移除微控制器的塑料封装，使用微探针读取内部存储器的内容。所以，安全系统需要采取措施阻止这种访问，甚至在必要时令微控制器擦除其存储器内容。

应对这一安全挑战的一个简单方法是将整个“敏感区域”(例如微控制器、时钟和存储器)密封在某种足够牢靠的材料内，可能需要将印制板上的一块区域用塑料填充或用金属罩覆盖。感应线装置可以用来感测高温或外壳的移动。然而，如果微控制器处于低功耗状态而不能采取行动，这种感测就没有作用。

DS5250：真正安全的密钥保护方案

DS5250内部的非易失性SRAM (NV SRAM)为敏感信息和密钥提供了理想的存储手段。

DS5250—Dallas Semiconductor精湛的安全微控制器技术的结晶，解决了这些问题，可协助设计者实现高度安全的系统，足以满足政府和金融应用之需。其所有出发点都聚焦于存储器。

NV SRAM

DS5250内部的非易失性SRAM (NV SRAM)为敏感信息和密钥提供了理想的存储手段。这种常规的、低泄漏的SRAM满足两个关键要求：

1) *数据必须是非易失的*。利用一个很小的廉价电池，就可以保持关键数据长达数年。

2) *数据必须易于迅速擦除*。一旦芯片的入侵侦测电路被触发，DS5250的SRAM瞬间即被擦除。

电池供电的入侵侦测及其反应

除了NV SRAM外，一个安全系统还应有一些传感器来侦测攻击行为。DS5250有多个电池供电的入侵传感器。无需微控制器处于活动状态即可对入侵事件作出反应。

利用其片上温度和电压传感器，DS5250可以侦测故障注入攻击手段。

利用其片上温度和电压传感器，DS5250可以侦测故障注入攻击手段。当工作电压或温度超出微控制器工作范围，DS5250立即清除其内部NV SRAM。这种机制消除了攻击者获取任何密钥数据的机会。为阻止对NV SRAM单元的微探针探测，DS5250的硅片顶层设置了一层超细网格。如果网格线被短路，DS5250即触发自毁，清除密钥数据。

DS5250还提供了允许外电路触发自毁的输入。这样系统可以实现多层保护。外部自毁触发电路没有任何限制。一些常见的外部传感器包括：

- 外壳上的侵入侦测开关。
- 印制板上的连线当外罩被移动时断开。
- 利用光传感器检测外壳是否被打开或被窥视。

加密的代码空间

最初装载系统时，DS5250使用一个随机生成的3DES密钥将指令代码加密后再存储到外部存储器中(**图2**)。这可避免攻击者向DS5250加入恶意代码并运行之，也可阻止对应用进行逆向工程。代码里也可以加入完整性检查，以便侦测攻击者改变程序代码的企图。

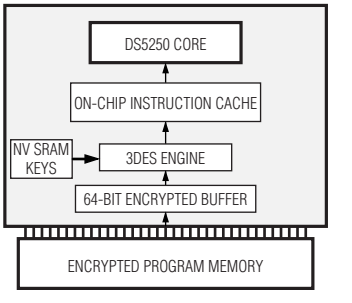

图2. 经过加密的代码空间可保护外部存储空间中的算法和数据。

经过加密的代码空间不仅阻止攻击者对应用进行逆向工程，而且可以阻止设备被非法仿制。因为密钥由每个DS5250随机生成，所以任何两个系统的外部闪存里的数据都不同。只有在攻击者知道密钥后，外部闪存数据才有用，而从上面的叙述中我们已经看到，从DS5250获取密钥并非易事。

安全工程

安全系统设计是一富有挑战性的工作。而要强化已有设计的安全性更难。密钥保护是安全系统设计中最关键的部分。DS5250专门有密钥保护设计，因而可为敏感数据提供最高安全等级的保护。要了解有关DS5250和我们的安全微控制器技术的更多详细情况，请浏览www.maxim-ic.com.cn/securemicro。