白皮书

保护 IP 和敏感数据

Markus Vomfelde，物联网和基础设施业务部门高级经理，瑞萨电子株式会社

Brad Rex，物联网和基础设施业务部门高级产品营销经理，瑞萨电子株式会社

Zachary Ellis，物联网基础设施业务部门高级营销专员，瑞萨电子株式会社

2020 年 1 月

摘要

本系列第一份白皮书中，瑞萨电子介绍了互联世界的安全。本白皮书将更详细地说明为何以及如何保护 MCU 或应用中存储的数据，即保护数据的需求和技术。我们将借助虚拟示例，引导读者思考根据应用和潜在攻击情景的需求实施不同级别的安全方案。这样可以帮助您针对设备中存储的数据准备安全方案，并根据您的需求寻找最合适的安全级别。

为什么要保护本地存储的数据？

本地存储的数据分为两类，一类是将在运行时执行的应用程序，一类是运行期间使用的本地数据。应用程序包含制造商的知识或 IP，因此设备制造商需要防范其知识被窃取、再利用或抄袭。数据通常存储在设备上。数据可以传输到另一个相同的设备上并在其中进行更新，因为所有设备都有相同的属性。本地数据在最终环境中设置设备或在设备运行期间进行存储。不同设备包含不同的数据，更新频率通常高于应用代码。保护这类数据的原因更多的是考虑到设备用户，因为数据可能包含用户环境的敏感信息。尽管保护数据的动机不同，但保护数据免遭外部访问是这种数据的强制要求。

您的设备是否会联网？

这对于安全实施方案的级别是一个非常重要的问题。对于没有任何连接、独立运行的设备，可能发生的攻击或许仅来自于直接物理访问。对于制造商保护设备内部的 IP 而言，这仍旧是一个问题，但对于用户数据则不然，因为攻击者通常无法直接接触设备。下一级连接是在本地封闭网络中运行的设备，它们不会连接到互联网。攻击者必须先访问封闭网络，然后才能攻击设备，但设备同样需要抵御外部访问，避免成为进入封闭网络的入口。最后是直接连接到互联网的设备，它们需要最高级别的安全实施方案，因为潜在攻击者不再局限于本地连接，而是遍及全球，计算能力无法估量。此外，这一类攻击会越来越多地访问设备内部存储的数据。

应用和安全需求示例

为了更具体地阐述整个主题，我们假设一个完全虚构但足够真实的示例应用，反映真实应用的安全需求。

我们以装有指纹传感器的门锁为例，通过刷指纹可以进入公司大楼的限制区域。这个传感器采用非常聪明的算法，能够在设备中存储 50 个最常用用户的指纹，而占用的内存极低。这是最能吸引市场客户的特色。对于其他用户，设备通过公司 Wi-Fi 网络连接到服务器，对比已存储指纹，这样就需要更多时间才能准许进入，由此可见，内部存储的数据是强大优势。Wi-Fi 网络还需要访问互联网才能接受制造商对设备进行无线更新。

作为设备制造商，必须设计一个确保应用安全的方案。在本白皮书中，我们仅围绕着设备中存储的数据展开说明，忽略通过运行或程序更新交换的数据（动态数据）。

第一类要保护的数据是指纹算法的 IP。这是设备本身的价值所在，应防止任何攻击者通过直接连接或数据连接访问设备。设备接入网络时，仅保护设备中的 MCU 免遭读出、复制或重新编程是不够的。此外，您必须保护 IP，以免攻击者连接后内存转储 IP。

第二类必须注意的数据是用户数据，即本例中的已存储指纹和网络访问数据。如上所述，如果只能通过物理方式访问设备，攻击者会更难获取用户数据。通过互联网连接访问则更容易获取数据，因此需要加强针对攻击的安全防护。一部分因素在于用户及其网络保护；但是，设备内部必须实施安全方案才能形成完整的安全设置。

保护 IP

根据给出的示例，保护已存储数据有几个安全前提。为了突出数据安全，我们假设所用设备具有安全设备

就 IP 保护而言，可以实施几种保护级别，这取决于您选择的安全方案和定义的保护范围。首先，选择的 MCU 必须能够防范不必要的调试访问和重新编程。实现这种关键保护的方法有多种，您必须对比不同的实施方法做出判断。不同的供应商使用不同的保护方法，这些方法也具备不同的安全能力。您必须确保实施推荐的安全方案，而不仅仅是防止意外的设备改装。下一级是使用能够支持不同访问区域的 MCU，可以是受信任或不受信任的 MCU。这样可避免 MCU 内核直接访问 IP，防止轻松地转储数据。这一级别同样有不同的解决方案。最常见的是可以用于上述目的的内存保护单元 (MPU) 实施方案或基于 ARM® 的微控制器的 TrustZone® 实施方案。最后，以加密方式将 IP 存储在设备上。这样可以加强对物理攻击的防御，因为不存在以可读数据形式存储 IP 的非易失性内存，无法通过封装或电子显微镜分析来读出 IP。因此，存储在 MCU 中的加密密钥也必须防止读出、从 CPU 直接访问，且必须安全存储以避免读出密钥和加密 IP，从而访问机密信息。如果以加密形式存储算法，必须在设备 RAM 中解密和执行。这是存储 IP 的最安全方法，但也须将存储算法的 RAM 部分纳入 MPU 可信部分。

保护静态数据安全

在第二步中，您必须决定最终客户存储在设备中的数据。在我们的示例中，已存储指纹数据以便快速访问相应区域，而且可访问客户网络，以便连接到存储所有指纹数据的服务器。这样制造商也可以进行未来的固件更新。基本上，可以应用相同的安全措施，因为该操作是针对设备中存储的 IP 执行的。我们想深入探讨，决定运行中的强制性安全实施方案级别。设备应防止数据读出或重新编程，哪怕只是部分禁止，避免安装任何通过网络向攻击者提供数据的恶意软件。此外，实施受信任和不受信任内存区域也很有意义，因为这样可以限制 MCU 访问存储数据的可能性，这样会提高攻击难度，通过受限性能降级加强保护。

最后，数据加密是强制性措施，这会对性能产生负面影响。所有已存储指纹必须先解密，算法才能开始运算，因此必须事先考虑插件性能影响。另一方面，直接接触客户大楼内的设备可能很难，如果这种插件是强制性的，则需要考虑物理访问。只要攻击者无法接触对比算法，对已存储指纹数据就无计可施。网络访问数据则不同。性能的负面影响几乎为零，因为一天只需要运行一两次，但如果能直接接触设备，以未加密数据形式读取网络访问代码，就能完全访问客户网络，这样更危险也更无法预测。另外需要强调，存储加密密钥时的安全级别必须高于数据本身，以避免对加密数据进行任何不必要的访问。一种高效做法是每个 MCU 上采用独特封装密钥，本系列的后续白皮书中将探讨“密钥管理”主题。

结论

如何实施安全以及实施何种程度的安全始终取决于应用、预期攻击者以及攻击者对受保护设备或数据的访问形式。这意味着对于每种安全实施方案，开发团队必须在项目初期就通盘考虑，决定哪种 MCU 满足所有安全实施需要。本文示例展示了本地存储数据的不同安全需求，随着动态数据功能的增加或无线安全编程的发展，安全需求会越来越高。本系列其他白皮书将为您提供相关信息，帮助您设计适合互联世界的安全产品。

瑞萨电子提供了多种 MCU[1] 以解决本白皮书中探讨的问题。请访问我们的网站，了解更多信息。

参考资料：

[1] RA 系列 32 位 Arm Cortex-M MCU
RX 系列 32 位 MCU
Synergy 平台 32 位 Arm Cortex-M MCU + 合格软件