Technical Article

使用低功耗无线 MCU 克服主要的无线连接网络安全挑战

Sainandan Reddy Reddy、Benjamin Moore 和 Bhargavi Nisarga

随着无线连接技术的创新，连接设备的能力现已扩展到日常电子产品，使住所和汽车实现智能化（请参阅图 1）。智能化程度越高意味着功能和特性越多：远程监视和控制设备的功能、云计算的增强功能以及更快的软件更新。

然而，随着世界的互联程度越来越高，保护这些产品免遭入侵变得至关重要。从确保存储的个人或敏感应用数据的安全，到保护传输中的数据和物理设备的安全，在设计中实施无线连接的工程师都需要在设计过程中尽早解决系统级安全功能问题，同时还要满足网络安全标准和法规的相关要求。

同样，帮助扩展连接性的无线微控制器 (MCU) 也需要应对不断变化的安全挑战以及网络安全标准和法规。

本文探讨了互联汽车和智能家居应用（特别是汽车门禁、智能恒温器以及智能传感器和电子锁）中不断发展的无线连接安全挑战，以及为应对这些挑战而设计的 MCU。

图 1. 使用智能手机进入汽车

汽车门禁的网络安全挑战

低功耗 *Bluetooth*® (BLE) 无线连接可用于汽车门禁解决方案，以确定车钥匙的距离和位置。安全威胁会导致汽车门禁安全性受损，从而可能导致车辆或财物失窃。

OEM 需要从多个层面考虑门禁安全，包括：

- **无线信号的测距安全性：**操纵测距信号会改变距离估计结果，使车钥匙看起来比实际距离更接近车辆。这些威胁与无线技术有关，无线物理层和介质访问控制规范中的安全功能通常都能解决此类威胁。例如，在最新的蓝牙信道探测规范中，通过使用往返计时 (RTT) 数据包交换和基于归一化攻击检测器度量 (NADM) 的缓解措施，解决了对基于相位的测距距离估计操作的威胁。
- **为设置测距程序所传输的数据提供协议级安全性：**协议级和应用级的威胁包括无线操作过程中的嗅探、中间人和重放攻击。规定相关的加密措施，对所传输的数据进行加密，并将车辆密钥验证为有效实体，可缓解这些攻击。不过，加密安全性取决于用于加密或认证的密钥。
- **终端应用操作（打开车门、启动发动机）的应用级安全性：**在无线连接设备中，通过无线或远程接收的经篡改数据可能会危及设备操作或用于数据通信安全的加密密钥（例如通过恶意软件注入）。因此，低功耗蓝牙无线 MCU 以可靠的方式支持协议级和应用级加密操作以保护密钥，这一点非常重要。通过安全启动、安全固件更新和安全调试访问，确保设备固件操作的安全，所有这些都是必需的。

此外，许多地区还制定了汽车网络安全法规，如国际标准化组织 21434 等标准，要求在设备开发和维护过程中遵守相关的网络安全流程。

智能恒温器面临的网络安全挑战

智能恒温器（请参阅图 2）是一个很好的例子，说明了智能家居技术的优势和面临的威胁。这些设备可让房主随时随地调节室内温度，并通过集成的 Wi-Fi® 连接优化能源使用。

图 2. 客厅中的蓝牙智能恒温器

遗憾的是，连接选项的增加可能会使恒温器面临威胁。例如，黑客可能会通过无线网络传播恶意制作的帧，中断恒温器的运行或迫使其退出网络。故意将设备踢出网络，并在重新连接后监控传输，这样就有可能使用暴力或字典攻击来捕获和解密数据，从而导致用户或供应商的数据和凭证暴露。通过互联网向恒温器发送恶意数据或代码（如恶意软件），或在恒温器和远程云服务器之间传输数据，可以通过远程中间人攻击捕获数据。

为减轻风险，设计人员必须遵循最新的 Wi-Fi 安全标准，这些标准概述了用于身份验证、密钥协议和加密的成熟加密算法，并规定了用于保护管理帧的协议，如 Wi-Fi Protected Access 3。这些设备需要支持最新的网络安全协

议（如传输层安全性协议 v1.3），以保护通过互联网传输的数据。此外，设备需要高效安全地运行这些协议，以存储在执行期间使用的密钥。

智能传感器和电子锁面临的网络安全挑战

智能传感器（如运动、门、窗传感器）和电子锁等（如图 3 所示）电池供电设备越来越多地使用 Zigbee®、Thread 和 Matter 等网状网络技术，来满足低功耗要求，同时仍通过智能家居中心连接到云。嗅探、中间人攻击和设备接管等安全威胁可能会损害设备数据或安全操作（例如，向不良分子授予电子锁访问权限）。在极端情况下，受损的设备可能会影响智能家居网络或生态系统。

图 3. 含有电子锁和智能传感器的智能家居

要保护这些网络的安全，需要保护传感器和集线器之间的通信通道的安全，以便只有可信设备可以加入网络。

Matter 旨在简化开发，并为智能家居产品提供更好的协议级安全性。除了通过强大的加密套件（如用于保密的高级加密标准、用于实现完整性的安全散列算法以及用于密钥交换和数字签名的椭圆曲线加密算法）确保通信渠道的安全外，Matter 还使用证书和基于密码的协议来验证智能家居设备，确保只有正版产品才能加入生态系统。

使用无线 MCU 降低安全威胁

为了降低安全风险，无线 MCU 应支持安全数据通信、安全密钥交换、相互认证、安全密钥存储、安全固件更新和安全启动操作。

CC2745P10-Q1、CC2755R10 和 CC3551E 等无线 MCU 提供集成安全功能，以降低恶意软件和设备接管攻击导致的风险。它们支持基本的安全功能，例如安全启动和带回滚保护的安全固件更新。这些 MCU 具有集成的硬件安全模块 (HSM)，带有专用控制器，用于处理硬件加速加密操作、安全密钥存储和随机数生成。HSM 为加密和密钥处理操作提供可信任的环境，从而有助于降低数据隐私和高级恶意软件风险。这些 MCU 中的 Arm® Cortex®-M33 内核支持 TrustZone-M，可进一步构建可信执行环境以确保软件安全运行。

商标

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