Application Note

支持 Wi-Fi® 的电子智能锁

Michelle Tate – SimpleLink™ Product Marketing Engineer
Benjamin Moore – SimpleLink™ Wi-Fi® Applications Manager
Bhargavi Nisarga – SimpleLink™ Systems Engineer

SimpleLink

摘要

本安全应用简报提供了一个对支持 Wi-Fi 的电子智能锁进行安全分析的示例，旨在重点介绍各种潜在威胁情景以及有助于应对这些威胁的相应步骤。不仅包括识别潜在威胁并对其进行排名，还探索了相关的 TI 信息安全机制。

本简报涉及使用 first.org CVSS 3.1 计算器，其中所有评分均基于 TI 的评估。读者应根据其目标应用和系统设计调整每个参数。

内容

商标

English Document: SWRA655

1 引言

数千年来，人们使用传统锁作为安全系统的第一道防线，来控制对住宅和楼宇的访问。随着锁具演变成具有集成电子控制和无线接口的更复杂系统，它们获得了一个新的名称：电子智能锁（电子锁）。在当今世界，徽章、钥匙扣、个人密码、移动设备甚至指纹都是对锁具进行身份验证的常用媒介，在许多情况下不再需要实体钥匙。

人们通过远程监测和控制入口通道来保护资产的需求日益增长，也促使市场上互联电子锁的数量上升。

远程访问和控制电子锁的常见用例包括：

- 向住宅业主的客人授予临时进入权限
- 向送货服务人员授予临时进入设施的权限，以便其投递包裹
- 对于具有多个进入点和权限级别的设施，集中管理进入设施的权限

将 Wi-Fi 等连接添加到电子锁中，可以方便地在任何时间、任何地点创建和管理进入密钥，同时还可以直接连接到互联网，而无需网关或集线器。互联电子锁除了具有上述所有优势之外，其连接也增加了易受安全攻击的暴露点的数量。

电子锁的设计必须考虑安全性，要阻止未经授权的用户，同时保持可供经授权用户使用，以此来控制资产的访问权限。执行威胁和风险评估并确定必需的信息安全机制，有助于降低遭受电子锁攻击的风险。具体而言，本安全应用简报旨在指导您在电子锁系统设计过程中执行安全威胁和风险评估。

2 住宅和商业电子锁

住宅电子锁系统设计通常将电子锁安装在楼宇外部，以打造第一道防线。这些外部电子锁以无线方式往回连接到家庭网关，家庭网关将电子锁连接到远程互联网接入点，如图 2-1 所示。

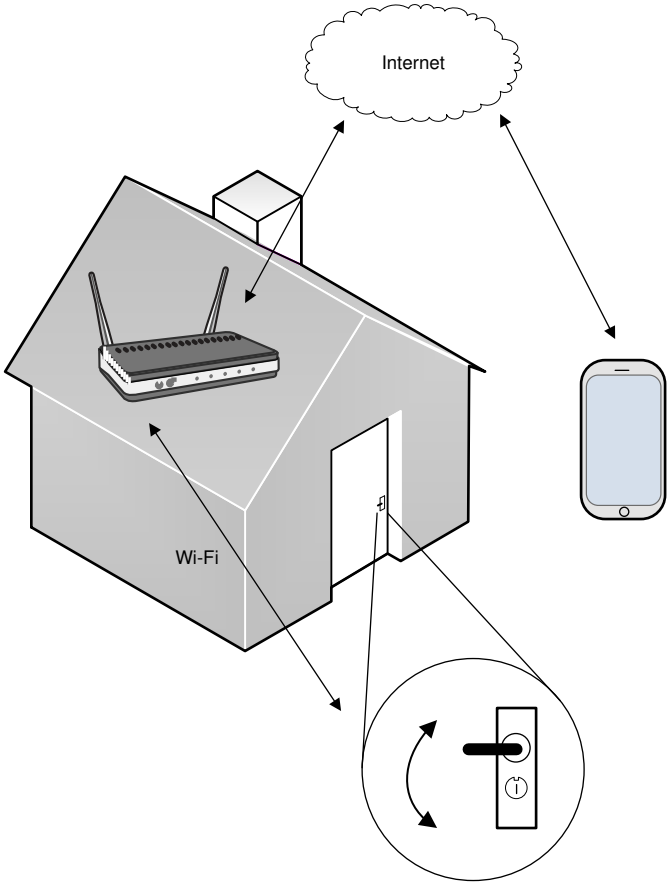

图 2-1. 住宅电子锁系统示例

在商业应用中，通常既在楼宇外部安装锁来作为第一道防线，也在内部安装锁来限制特定人员进入。内部电子锁可能经过多跳才能从初始入口位置连接到中央楼宇安全系统服务器，具体取决于商业楼宇的大小。例如，在较小的酒店中，每个电子锁经过单跳即可以无线方式往回连接到中央服务器。而在大型酒店中，每层都有一个网关，支持无线和有线通信，如 Wi-Fi 和以太网。特定楼层上的电子锁通过无线通信连接到相应的网关，再通过网关往回连接到中央服务器。在商业系统中添加中央服务器，可使楼宇管理员通过无线方式快速、轻松地推送更新，如对电子锁的关键更改。

图 2-2 展示了常见的商业电子锁系统。

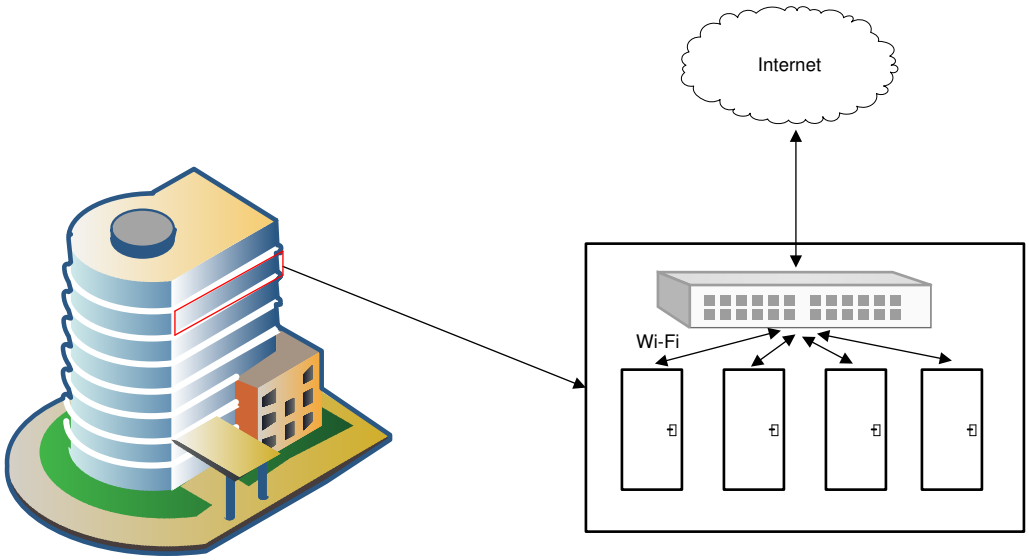

图 2-2. 商业电子锁系统示例

3 为什么电子锁会成为被攻击的目标？

以下是一些典型的示例，说明为什么电子锁会成为被攻击的目标：

- 获取电子锁所保护的资产
- 克隆电子锁产品并在黑市上销售
- 使用勒索软件导致电子锁无法正常工作，除非向攻击者支付了赎金
- 破坏电子锁并将其用作代理来攻击局域网 (LAN) 中的其他节点或中央互联网服务器，例如使用拒绝服务 (DoS) 攻击。
- 根据电子锁使用情况监控客户习惯，并确定何时对房屋或设施实施入室盗窃

在使用联网电子锁的情况下，攻击的动机可能要比仅仅获取被单个锁保护的资产要广泛得多。攻击者的投资回报可能也更高。攻击者可以利用电子锁或网络其他组件中的安全漏洞来破坏现场的多个电子锁。例如，注册到网络上的带有预编程恶意软件（或具有非故意漏洞的软件）的克隆或假冒电子锁产品，可通过使用伪造节点将恶意软件传播到其他设备或在网络中引起 DoS 攻击来执行可扩展的远程攻击。

回顾先前关于攻击者勒索赎金（通常来自公寓、酒店或医院等设施）以让电子锁恢复正常运行的要点，这些类型的攻击通常不仅会造成经济损失，还会使最终用户和产品制造商的声誉受损。与未联网的锁相比，联网产品暴露的攻击面也更大；因此，联网产品同时易受本地和远程攻击。攻击者可能利用电子锁终端节点中的安全漏洞危害本地网络、网关或网络服务器，这可能对所有利益相关者造成更大的影响。例如，如果攻击者可以远程将恶意软件注入多个电子锁（利用电子锁本身或其他网络组件中的漏洞），则他/她可以控制现场的多个电子锁并执行分布式 DoS 攻击（例如，用数据包对服务器进行泛洪攻击）。因此，务必考虑所有网络组件（包括终端节点）的安全性。

此外，大学、研究实验室或其他个人可能希望破解电子锁，以揭露产品漏洞并让物联网 (IoT) 社区意识到互联产品安全的重要性。

攻击联网电子锁的动机多种多样，因此务必了解每种攻击的风险和严重性，以设计必要的安全措施来加强对这些产品的保护。

4 威胁说明和风险评估

风险评估对于确定风险优先级至关重要。表 4-1 列出了采用 Wi-Fi 连接技术的电子智能锁的一些常见威胁。尽管该表很长，但并不详尽，并未列出危害特定安全资产的所有潜在方式。

表 4-1. 威胁分析和 CVSS 评分

威胁	威胁说明	威胁分数	CVSS 链接
电子锁接管	攻击者通过 LAN 或 WAN 攻击使器件感染恶意软件，以从存储器中读取安全凭证，从而访问客户资产或勒索赎金。	9.0	CVSS 计算 - 9.0
现场未经授权的软件更新	攻击者远程发送未经授权的软件更新或对系统执行软件降级/回滚攻击，以操控器件操作	9.0	CVSS 计算 - 9.0
云网络中的未授权器件	攻击者通过恶意软件入口点从存储器中读取器件标识，并欺骗/模拟器件以连接到云网络	9.0	CVSS 计算 - 9.0
在器件编程期间未经授权访问电子锁软件 IP	攻击者在不可信编程设施中窃取未受保护的软件映像，并在器件制造过程中使用它们来克隆电子锁 IP	8.8	CVSS 计算 - 8.8
电子锁软件机密性受损	攻击者直接从器件存储器中读取固件，以便以更复杂的方式利用漏洞/进行攻击，如大规模远程攻击	7.6	CVSS 计算 - 7.6
电子锁用户隐私丢失	攻击者通过本地接口读取存储在电子锁器件上的个人信息或使用情况信息（日志），以了解用户模式	6.2	CVSS 计算 - 6.2
未经授权访问本地网络	攻击者直接从器件存储器（片上/片外）上读取 Wi-Fi 网络认证密钥/密码	5.7	CVSS 计算 - 5.7
未经授权访问本地网络	在配置期间，攻击者通过无线流量进行嗅探，以窃取 Wi-Fi 网络身份验证密钥/密码	5.2	CVSS 计算 - 5.2

NOTE

此表中的威胁分数是使用常见的漏洞评分系统 (CVSS) 3.1 版计算器计算得出的。传输层安全性 (TLS) 是基于互联网协议的联网设备的典型特征，因此威胁分数计算假设 TLS 在所有威胁场景中都受支持，并在电子锁节点与远程服务器之间使用。

5 识别相关的 TI 信息安全机制和功能

德州仪器 (TI) 已于*在构建您的应用时将安全性考虑在内*一文中定义了其安全架构，以概述安全问题的原因、如何评估您需要哪些安全措施以及如何实施这些措施以防范威胁。TI 安全架构还包括 TI 提供的主要信息安全机制，它们可帮助您实现安全目标。

表 5-1 将客户资产映射到 TI 信息安全机制。

表 5-1. 客户资产到 TI 信息安全机制的映射

威胁	安全资产	措施	器件资产	暴露点	TI 信息安全机制	信息安全机制的使用
电子锁接管	电子锁器件操作	• 发送命令以通过电子锁系统验证用户身份时进行安全传输（控制命令） • 具有加密、身份验证和访问控制功能的非易失性存储器，用于存储已编程的用户访问代码	• 器件标识和密钥 • 代码	运行时、传输	• 安全存储 • 网络安全性 • 安全启动 • 加密加速	• 在与远程网络（云）通信时使用安全套接字，可以增强对中间人攻击（会导致感染恶意软件）的防护。 • 假设可以通过网络接口感染恶意软件，借助文件系统安全性，存储用户文件时可进行加密、签名和设置访问限制，以帮助降低从非易失性存储器中读取关键信息（如凭证）的风险。 • 使用签名存储应用软件可以在器件启动操作期间验证软件，以防止执行无效的软件。 • 加密加速可加快安全套接字连接的速度，以便在与云建立连接和发送/接收命令时减少延迟并节省功耗。加密加速还通过减少验证签名和解密应用软件所需的时间来支持安全启动过程。
现场未经授权的软件和固件更新	电子锁操作和可用性	• 固件更新传输期间的安全通信 • 经过身份验证的固件更新 • 安全启动以防止执行未经授权的映像	代码	传输、存储、运行时	• 网络安全性 • 安全固件和软件更新 • 安全存储 • 安全启动 • 加密加速	• Wi-Fi 网络安全性可增强对无线更新期间的中间人攻击的防护。 • 对下载的固件和软件映像捆绑包进行签名验证，有助于确保更新的完整性并验证更新来源可信。 • 借助文件系统安全性，可以创建通过签名进行加密和身份验证（安全签名）的文件。必须向器件提供安全签名文件的签名，并在每次写入文件时进行验证。 • 软件篡改防护监视旨在访问/写入非易失性存储器中固件的无效尝试，并可以锁定文件系统以防止访问软件 IP。 • 安全启动使器件能够在器件启动操作期间验证软件，以增强对执行无效软件的防护。 加密加速可减少在启动操作期间解密固件和验证签名时所消耗的时间和电力。
云网络中的未授权器件	客户云网络资源（云的可用性和安全性）	• 器件注册到网络时进行客户端身份验证 • 在器件上安全地存储客户端标识	器件标识和密钥	存储、运行时	• 器件标识 • 安全存储	• 使用 128 位唯一器件 ID 和内置的唯一非对称密钥对将器件标识为原装产品。器件标识（唯一器件 ID 和唯一密钥对）可用于生成证书签名请求 (CSR)，该请求可由权威机构签名并用于在云网络中注册器件。 • 借助文件系统安全性，可通过访问控制以加密方式存储私钥。
在器件编程期间未经授权访问电子锁软件 IP	客户软件 IP	在生产线上保护客户软件映像	代码、数据、标识和密钥	传输、存储	• 安全初始编程 • 软件 IP 保护 • 加密加速	• 安全初始编程使开发人员能够在生产线上使用加密的映像，并将系统限制为仅由可信的个人/环境激活。 • 克隆防护（通过使用器件唯一密钥对文件系统加密来启用）有助于降低将软件 IP 从一个器件复制到另一个器件以创建系统其他克隆的风险。 • 加密加速器可减少在生产编程期间加密/解密软件映像所需的时间。
电子锁软件机密性受损	电子锁软件 IP 机密性和完整性	• 阻止在编程后访问调试接口 • 保护器件上的软件 IP •安全启动以防止执行未经授权的映像	代码	运行时、存储	• 调试安全性 • 安全存储 • 软件 IP 保护 • 安全启动	• 在生产线上对系统进行编程时，禁用 JTAG 访问和对文件系统的逐文件访问，可增强对攻击者直接从片上或外部存储器读取软件 IP 的防护。 • 文件加密可提高安全性，以防止攻击者以纯文本形式从非易失性存储器中读取软件。 • 软件篡改防护监视旨在读取非易失性存储器中固件的无效尝试，并可以锁定文件系统以防止访问软件 IP。 • 安全启动使器件能够在器件启动操作期间验证软件，以增强对执行无效软件的防护。
电子锁用户隐私丢失	客户的电子锁使用数据（日志）和一般个人数据。	保护器件上存储的日志和/或个人数据 在本地或通过网络传输时加密敏感的用户数据	数据	存储、传输	• 安全存储 • 网络安全性 • 密钥 • 加密加速	• 文件加密、身份验证和访问控制有助于保护系统上本地存储的敏感数据不被攻击者读取。 • 在通过本地网络传输数据时，可以使用 Wi-Fi 安全性和安全套接字以增强保护。 • 当通过物理接口传输时，可以使用加密实用程序和加速器增强对敏感信息的保护。
未经授权访问本地网络	可保护通过本地网络的通信数据的 Wi-Fi 密码或身份验证密钥	对器件上存储的网络凭证进行安全存储和受限访问控制	密钥	存储、运行时	• 安全存储 • 独立执行环境	• 文件系统安全性（加密和访问控制）有助于防止攻击者直接从非易失性存储器中读取系统上本地存储的网络密码或身份验证密钥。 • 为应用 MCU 和网络处理器提供独立执行环境，以便在配置后将对密钥的访问限于网络处理器子系统。

表 5-1. 客户资产到 TI 信息安全机制的映射 (continued)

威胁	安全资产	措施	器件资产	暴露点	TI 信息安全机制	信息安全机制的使用
未经授权访问本地网络	可保护通过本地网络的通信数据的 Wi-Fi 密码或身份验证密钥	为系统配置网络凭证以进行安全传输	密钥	传输	网络安全性	• 使用 Wi-Fi 安全性和安全套接字来保护电子锁与用于进行配置的器件之间的本地链路，有助于降低在设置过程中攻击者访问 Wi-Fi 凭证的风险。

6 具有信息安全机制的 TI 器件

SimpleLink™ Wi-Fi CC3235x 和 CC3220x 器件提供了广泛的内置安全特性，以支持并帮助设计人员应对电子锁安全威胁。表 6-1 列出了主要信息安全机制的概要说明。

表 6-1. SimpleLink WiFi CC3235x 和 CC3220x 器件的信息安全机制

信息安全机制	详细的安全特性	TI 器件	
		SimpleLink CC3220S/SF	SimpleLink CC3235S/SF
安全引导	安全引导	✓	✓
器件标识/密钥	器件标识 安全存储 受信任的根证书目录 TI 信任根公钥	✓	✓
加密加速	FIPS 140-2 1 级认证		✓
	AES/DES/TDES/3DES SHA/MD5 PKA (RSA) TRNG	✓	✓
调试安全性	调试安全性 (默认情况下在生产映像上启用)	✓	✓
安全存储	文件加密 文件身份验证 文件访问控制 出厂映像恢复 文件捆绑包保护 文件系统安全性 软件篡改检测	✓	✓
外部存储器保护	请参阅上面的安全存储特性	✓	✓
网络安全	个人和企业 Wi-Fi 安全性 • Wi-Fi 保护接入 (WPA) • WPA2 预共享密钥 (PSK) • WPA2 可扩展的身份验证协议 (EAP) • WPA2 + 受保护管理框架 (PMF) • WPA3 安全套接字 • 安全套接字 (SSL) v3 • TLS 1.0/1.1/1.2 超文本传输协议安全服务器	✓	✓
	在线证书状态验证 (OCSP)		✓
安全固件和软件更新	网络安全性 固件/软件映像身份验证 捆绑包保护 出厂映像恢复	✓	✓
初始安全编程	加密编程映像	✓	✓
软件 IP 保护	文件系统安全性 软件篡改检测	✓	✓

NOTE

加密技术领域不断发展。随着密码分析不断有新的发现，旧的算法将变得不安全。此外，随着计算能力的提高，蛮力破解攻击具有可行性，将使已知的密码系统或使用某些密钥长度变得不安全。应遵循美国国家标准与技术研究院 (NIST) 等标准机构提出的建议。

7 结论

随着市场上互联锁的数量不断增加，遭到更复杂远程安全攻击的风险也变得越来越大。正如我们在本安全应用简报中所示，与利用单个非互联锁的漏洞相比，利用互联电子锁漏洞会带来更严重的安全问题。这种危险比以往任何时候都更需要进行威胁和风险评估，以确定保护终端设备资产所需的安全措施。

根据安全威胁分析，要考虑的最严重的攻击是利用恶意软件实施的攻击或导致未经授权软件更新的攻击，此类攻击可能导致整个系统被接管并可能泄露机密资产，如软件 IP、器件身份和密钥以及个人数据。此外，降低未经授权访问软件 IP 的风险也很重要，因为未经授权访问软件 IP 可能允许系统克隆或对软件执行逆向工程，从而暴露漏洞并在更大范围内执行更复杂的攻击。

CC32xx 器件系列配备了重要的信息安全机制（网络安全、通过文件系统安全性实施安全存储、调试安全性、软件 IP 保护、内置器件身份、TI 信任根、安全启动以及支持安全的软件/固件更新），可帮助您为电子锁应用和系统设计所需的安全解决方案。

8 参考资料和相关文档

- 德州仪器 (TI)：*支持 SimpleLink™ Wi-Fi® 的电子智能锁*
- 德州仪器 (TI)：*了解 SimpleLink™ Wi-Fi® CC32xx MCU 的安全特性*
- 德州仪器 (TI)：*CC3x20、CC3x35 SimpleLink™ Wi-Fi® Internet-on-a Chip™ 解决方案内置安全特性*
- 常见的漏洞评分系统 3.1 版计算器

9 修订历史记录

注：以前版本的页码可能与当前版本的页码不同

Changes from Revision * (September 2019) to Revision A (September 2020)	Page
• 更新了整个文档中的表格、图和交叉参考的编号格式	2
• 更新了表 6-1，*SimpleLink WiFi CC3235x 和 CC3220x 器件的信息安全机制*	8

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