IoT安全之攻击面分析与主要漏洞

根据《牛津字典》，“物联网（Internet of Things）”定义为：“在 Internet 的发展上，将日常物品用网络相联并允许彼此之间收发数据的一种网络概念。”

OWASP Internet of Things （IoT）物联网项目，旨在帮助制造商、开发商和消费者更好地了解与物联网相关的安全问题，并使任何环境中的用户在构建、部署或评估 IoT 技术时能做出更好的安全决策。本项目包含了攻击面分析和高危漏洞方面的关键信息。

注：

1、有关 OWASP IoT 项目的更多信息，可直接在访问本 OWASP 项目的网站：

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main

2、本文由 OWASP 中文项目工作组提供。参与本文的 OWASP 中文项目工作组成员包括：王厚奎、李康伟、王颉。

1. IoT 攻击面分析

攻击面	漏洞
生态系统	• 互操作性标准 • 数据治理 • 系统故障 • 个人利益相关者风险 • 组件之间的隐式信任 • 注册安全 • 退役系统 • 丢失的访问过程
设备内存	• 敏感数据 ○ 明文用户名

	○ 明文密码 ○ 第三方凭证 ○ 加密密钥
设备物理接口	• 固件提取 • 用户 CLI • 管理员 CLI • 特权升级 • 重置为不安全状态 • 删除存储介质 • 防篡改 ○ 调试端口 ○ UART(串口) ○ JTAG/SWD • 设备 ID、序列号曝光
设备 Web 界面	• 标准的 web 应用程序漏洞集, 请参见： ○ 《OWASP Top 10》 ○ 《OWASP ASVS》 ○ 《OWASP 测试指南》 • 凭证管理漏洞： ○ 用户名枚举 ○ 弱密码 ○ 帐户锁定 ○ 已知的默认凭证 ○ 不安全的密码恢复机制
设备固件	• 敏感数据暴露 (见 2013 年版或 2017 年版《OWASP Top 10》中“A6 敏感数据暴露”部分内容)： ○ 后门帐户 ○ 硬编码凭据 ○ 加密密钥 ○ 加密 (对称、不对称) ○ 敏感信息 ○ 敏感的 URL 泄漏 • 固件版本和最近更新日期显示 • 易受攻击的服务 (如：Web、SSH、TFTP 等)

	○ 验证旧的 SW 版本和可能的攻击 (Heartbleed、Shellshock、旧的 PHP 版本等) • 与安全相关功能的 API 暴露 • 固件降级
设备网络服务	• 信息泄露 • 用户 CLI • 管理 CLI • 注入 • 拒绝服务 • 非加密服务 • 弱加密 • 测试、开发服务 • 缓冲区溢出 • UPnP • 易受攻击的 UDP 服务 • DoS 攻击 • 设备固件 OTA 更新阻止 • 通过不安全通道加载的固件（无 TLS） • 攻击重演 • 缺乏有效载荷验证 • 缺乏信息完整性检查 • 证书管理漏洞 ○ 用户名枚举 ○ 弱密码 ○ 账户锁定 ○ 已知的默认凭据 ○ 不安全的密码恢复机制
管理界面	• 标准的 Web 应用程序漏洞，请参阅： ○ 《OWASP Top 10》 ○ 《OWASP ASVS》 ○ 《OWASP 测试指南》 • 证书管理漏洞： ○ 用户名枚举 ○ 弱密码 ○ 账户锁定

	○ 已知的默认凭据 ○ 不安全的密码恢复机制 • 安全/加密选项 • 记录选项 • 双因素身份验证 • 检查不安全的直接对象引用 • 无法擦拭设备
本地数据存储	• 未加密数据 • 使用发现的密钥来加密数据 • 缺少数据完整性检查 • 使用静态相同的 enc / dec 键
云 Web 界面	• 标准的 Web 应用程序漏洞，请参阅： ○ 《OWASP Top 10》 ○ 《OWASP ASVS》 ○ 《OWASP 测试指南》 • 证书管理漏洞： ○ 用户名枚举 ○ 弱密码 ○ 账户锁定 ○ 已知的默认凭据 ○ 不安全的密码恢复机制 • 传输加密 • 双因素身份验证
第三方后端 APIs	• 未加密 PII 发送 • 加密 PII 发送 • 设备信息泄露 • 位置泄漏
更新机制	• 未加密更新发送 • 未签名更新 • 更新位置为可写 • 更新验证 • 更新认证 • 恶意更新 • 缺乏更新机制 • 不支持手动更新机制
移动应用程序	• 设备或云端的隐性信任

	• 用户名枚举 • 账号锁定 • 已知默认凭据 • 弱密码 • 不安全的数据存储 • 传输加密 • 不安全的密码恢复机制 • 双因素认证
供应商后端 API	• 云或移动应用的内置信任 • 弱认证 • 弱访问控制 • 注入攻击 • 隐藏服务
生态系统通信	• 健康检查 • 心跳 • 生态系统命令 • 取消配置 • 推送更新
网络流量	• LAN • 局域网到互联网 • 短范围 • 非标准 • 无线（WiFi、Z 波、XBee、Zigbee、蓝牙、LoRA） • Fuzzing 协议
认证与授权	• 认证、授权相关值（如：会话密钥、令牌、cookie 等）泄露 • 重新使用会话密钥、令牌等 • 设备到设备的认证 • 设备到移动应用程序的认证 • 设备到云系统的认证 • 移动应用程序到云系统的认证 • Web 应用程序到云系统的认证 • 缺乏动态认证
隐私	• 用户数据泄露 • 用户/设备位置暴露 • 差异化隐私

硬件（传感器）	• 感知环境操作 • 篡改（物理上） • 损害（物理上）

2、IoT 漏洞项目

漏洞	攻击面	概要
用户名枚举	• 管理界面 • 设备 Web 界面 • 云界面 • 移动应用程序	• 能够通过认证交互收集一组有效的用户名。
弱密码	• 管理界面 • 设备 Web 界面 • 云界面 • 移动应用程序	• 如，允许将帐户密码设置为“1234”或“123456”。 • 使用预先编程的默认密码。
账号锁定	• 管理界面 • 设备 Web 界面 • 云界面 • 移动应用程序	• 能够在 3 至 5 次登录尝试失败后，继续发送身份验证尝试。
非加密服务	• 设备网络服务	• 网络服务未作适当加密来防止攻击者窃听或篡改。
双因素认证	• 管理界面 • 云 Web 界面 • 移动应用程序	• 缺少双因素认证机制，如安全令牌或指纹扫描器。
轻度加密	• 设备网络服务	• 虽然已执行加密，但是该配置不正确或未被能准确更新。例如使用 SSL v2 。
非加密更新	• 更新机制	• 更新是在没有使用 TLS 或加密情况下通过网络传输更新文件的。
更新位置为可写	• 更新机制	• 更新文件的存储位置为可写，并允许修改固件并分发给所有用户。
拒绝服务	• 设备网络服务	• 服务能够以拒绝该服务或整个

		设备的服务方式进行攻击。
删除存储介质	• 设备物理接口	• 能够从设备中删除物理存储介质。
无手动更新机制	• 更新机制	• 无法手动强制更新检查设备。
缺乏更新机制	• 更新机制	• 无法更新设备。
固件版本显示及最后更新日期	• 设备固件	• 当前固件版本不显示，或者最后更新日期不显示，也有可能两者都不显示。
固件和存储提取	• JTAG / SWD 接口 • In-Situ dumping • 拦截 OTA 更新 • 从制造商网页进行下载 • eMMC 敲击 • 取消链接 SPI Flash / eMMC 芯片并在适配器中进行读取	• 固件包含许多有用的信息，例如，运行服务的源代码和二进制文件、预设密码、ssh 密钥等。
操纵设备的代码执行流程	• JTAG / SWD 接口 • 侧面渠道攻击，如：Glitching 攻击。	• 借助于 JTAG 适配器和 gdb，我们可以修改设备中固件的执行程序，并绕过几乎所有基于软件的安全控制。 • 侧面通道攻击还可以修改执行流程，或者可以用来获取设备泄漏的有趣信息。
获取控制台访问	• 串行接口（SPI / UART）	• 通过连接到串行接口，我们将获得对设备的完全控制台访问。 • 通常来说，安全措施包括防止攻击者进入单独用户模式的自定义启动程序，但它也可以绕过攻击者。
不安全的第三方组件	• 软件	• 使用过期版本的 busybox、openssl、ssh、web 服务器等。