物联网设备固件漏洞检测与嵌入式系统安全加固

任浩，王晓明

西安浩瀚明景信息科技有限公司，陕西 西安 712000

摘　　要： 随着物联网（IoT）技术的飞速发展，物联网设备已广泛应用于工业、消费类等多个领域，实现了更高的自动化和生产率。然而，这些连网设备的高度依赖也带来了一系列网络安全威胁，特别是 IoT 设备固件漏洞问题，往往在开发和部署过程中被忽视。针对这一问题，亟需制定全面的安全策略，包括对 IoT 设备固件环境进行审计，并评估相关审计工具和技术的有效性。同时，嵌入式系统作为物联网的核心组成部分，其安全性也直接关系到物联网的整体安全。因此，本文旨在探讨物联网设备固件漏洞检测的重要性、方法及工具，并分析嵌入式系统安全加固的策略。

关 键 词： 物联网设备；固件漏洞检测；嵌入式系统；安全加固

Firmware Vulnerability Detection for Iot Devices And Security Reinforcement for Embedded Systems

Ren Hao, Wang Xiaoming

Xi 'an Haohan Mingjing Information Technology Co., LTD. Xi'an, Shaanxi 712000

Abstract: With the rapid development of Internet of Things (IoT) technology, IoT devices have been widely applied in various fields such as industry and consumer sectors, achieving higher levels of automation and productivity. However, the high dependence on these connected devices also brings a series of cybersecurity threats, particularly firmware vulnerabilities in IoT devices, which are often overlooked during development and deployment. To address this issue, it is urgent to establish comprehensive security policies, including auditing the firmware environment of IoT devices and evaluating the effectiveness of relevant audit tools and technologies. At the same time, embedded systems, as a core component of the IoT, directly impact the overall security of the IoT. Therefore, this paper aims to explore the importance, methods, and tools for detecting firmware vulnerabilities in IoT devices, and analyze strategies for enhancing the security of embedded systems.

Keywords: Internet of Things devices; firmware vulnerability detection; embedded systems; security reinforcement

引言

随着物联网（IoT）技术的飞速发展，物联网设备已广泛应用于智能家居、工业自动化、医疗设备等多个领域。然而，物联网设备的安全问题日益凸显，尤其是固件漏洞成为黑客攻击的主要目标。固件作为物联网设备的核心软件系统，负责控制设备的硬件功能，其安全性直接关系到设备的整体安全。因此，对物联网设备固件进行漏洞检测以及加强嵌入式系统的安全加固，对于保障物联网系统的安全运行具有重要意义。

一、固件漏洞检测的重要性

物联网设备固件漏洞检测是网络安全防御体系中不可或缺的关键环节，其重要性体现在多个层面。固件作为设备底层软件，直接控制硬件运行并存储核心逻辑，一旦存在漏洞引发连锁反应。攻击者通过逆向工程或漏洞利用工具可获取设备控制权，窃取敏感数据如用户隐私或企业机密，甚至植入恶意代码形成僵尸网络发起 DDoS 攻击。2016年 Mirai 病毒利用默认密码漏洞感染百万级物联网设备，导致美国东海岸大规模断网，凸显固件安全缺陷的现实危害。专业检测技术能识别缓冲区溢出、硬编码凭证、加密缺陷等漏洞类型，结合静态分析、动态模糊测试等方法覆盖代码逻辑和运行时行为。制造商通过持续检测可避免类似华为路由器后门事件的供应链风险，医疗物联网设备更需严格检测防止患者生命体征数据被篡改[1]。监管部门将固件安全纳入标准体系，如欧盟 EN303645 认证要求漏洞扫描作为准入条件。企业建立固件 SBOM（软件物料清单）并配合自动化检测工具，能在产

作者简介：任浩（1987.11－），男，汉族，陕西商洛人，本科，中级工程师，从事计算机科学与技术研究工作。

品生命周期中持续监控 CVE 漏洞库更新，实现从开发到运维的全流程防护[2]。

二、固件漏洞检测方法

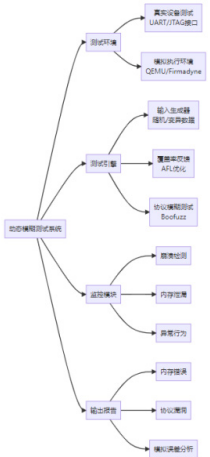
（一）静态分析

静态分析技术通过直接解析固件的二进制文件或固件镜像，在不执行代码的情况下识别潜在漏洞。这种方法适用于缺乏源代码的场景，如第三方闭源设备或老旧系统。自动化工具如 Binwalk、Ghidra 和 IDA Pro 可解包固件，提取文件系统并分析可执行文件，检测缓冲区溢出、格式化字符串漏洞、硬编码密钥等风险。模式匹配技术通过对比已知漏洞特征库（如 CWE、CVE）快速定位高危代码段，而数据流分析则追踪变量传递路径，识别未经验证的用户输入或危险函数调用。例如，检测到 `strcpy` 函数未检查长度可能导致栈溢出，或发现 `system` 函数调用外部命令可能引发命令注入[3]（见图1）。

> 图1 静态分析框架图

（二）动态模糊测试

动态模糊测试通过向运行中的固件注入异常或随机数据，观察其反应以发现漏洞。在物联网环境中，模糊测试分为基于真实设备和模拟执行两种方式。真实设备测试需物理连接目标硬件，通过 UART、JTAG 或网络接口发送畸形数据包，监测设备是否崩溃或内存泄漏，结果更贴近实际运行状态，但受限于硬件资源，难以大规模部署。模拟执行则利用 QEMU、Firmadyne 等工具虚拟化固件运行环境，自动化生成测试用例并监控异常，成本低且可并行测试，但可能因模拟不完整（如缺失外设驱动）导致漏报[4]。高级模糊测试工具如 AFL（American Fuzzy Lop）结合覆盖率反馈，动态调整输入以探索更深层代码路径，有效发现如 Heartbleed 类的内存错误。针对网络协议固件，协议模糊测试（如 Boofuzz）可构造畸形 TCP/UDP 报文，测试路由器或摄像头等设备的协议栈健壮性。模糊测试的随机性可能遗漏逻辑漏洞，需与静态分析互补使用[5]（见图2）。



> 图2 动态模糊测试框架图

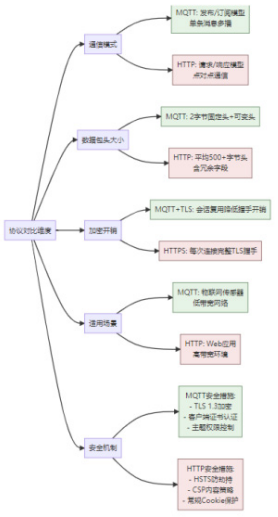
三、嵌入式系统安全加固

（一）物理安全加固

嵌入式设备的物理安全加固是防止硬件攻击的关键环节。攻击者可能通过调试接口（如 JTAG、UART、SWD）提取固件、篡改配置或植入恶意代码，因此设计阶段需禁用或加密这些接口，仅在可信环境中开放。采用防篡改外壳、环氧树脂封装或自毁机制可阻止物理拆解，金融终端和工业控制器常采用此类防护[6]。硬件安全模块（HSM）或可信平台模块（TPM）能保护加密密钥，即使设备被物理窃取也无法提取敏感数据。部分高端设备集成物理入侵检测电路，一旦检测到外壳被破坏立即擦除存储内容。在供应链安全层面，需防范固件被篡改，可通过安全启动（Secure Boot）验证固件签名，确保仅允许授权代码运行[7]。

（二）网络安全保护

嵌入式设备的网络暴露面不断扩大，使其成为攻击者的主要目标。加密通信（如 TLS 1.3或 IPSec）可防止数据窃听和中间人攻击，但需注意避免使用弱加密算法（如 RC4或 DES）。防火墙规则应限制不必要的端口和服务，例如仅允许特定 IP 访问管理接口。网络分段技术（如 VLAN 或零信任架构）能隔离关键设备，防止横向渗透[8]。入侵检测系统（如 Snort 或Suricata）可实时分析流量，识别异常行为（如暴力破解或 DDoS 攻击）。对于资源受限设备，轻量级协议（如 MQTT with TLS）比传统 HTTP 更安全（见图3）。



> 图3 MQTT with TLS 与传统 HTTP 协议的对比图表

（三）定期软件和固件更新

固件更新机制的安全性是嵌入式设备长期可靠运行的核心。制造商应建立漏洞响应流程，及时发布补丁修复 CVE 漏洞。更新过程需采用端到端加密（如 AES-256）和数字签名（ECDSA 或 RSA-PSS），防止中间人攻击或恶意固件植入。差分更新技术可减少带宽消耗，适用于低功耗设备。回滚保护机制能阻止攻击者降级固件至易受攻击版本。设备应支持远程安全更新（OTA），但需确保更新服务器身份验证严格，避免类似 SolarWinds 的供应链攻击[9]。

（四）强化设备认证和授权

身份认证是防止未授权访问的第一道防线。默认密码必须强制修改，并符合复杂性要求（如长度12位以上，含特殊字符）。双因素认证（2FA）结合密码与硬件令牌或生物特征，大幅提升

安全性。基于角色的访问控制（RBAC）限制用户权限，例如运维人员仅能查看日志，管理员才能修改配置。API 访问需采用 OAuth 2.0或 JWT 令牌，并设置短期有效期。对于高安全场景，设备间认证可使用双向 mTLS，确保通信双方均经过验证。审计日志记录所有登录和操作，便于事后追溯[10]。

（五）使用安全的编码实践

嵌入式开发中的安全编码能从根本上减少漏洞。避免使用危险函数（如`strcpy`、`gets`），改用安全替代方案（`strncpy`、`snprintf`）。静态分析工具（如 Coverity 或 Klocwork）可在编译阶段检测内存泄漏和未初始化变量。动态分析工具（如 Valgrind）帮助发现运行时错误。输入验证需严格过滤特殊字符，防止 SQL 注入或命令注入。内存安全语言（如 Rust）逐渐替代 C/C++，减少缓冲区溢出风险。代码审查和渗透测试应纳入开发周期，工业领域遵循 IEC 62443等安全标准。开发者需持续关注 CWE Top 25漏洞类型，并在设计阶段实施最小权限原则，降低攻击面（见表1）。

表1 CWE Top 25漏洞类型

序号	漏洞类型（CWE编号）	漏洞描述	影响
1	CWE-119	缓冲区错误	可能导致代码执行、数据泄露或程序崩溃
2	CWE-79	跨站脚本（XSS）	可能导致会话劫持和用户数据泄露
3	CWE-89	SQL注入	可能导致数据泄露、数据篡改和应用崩溃
4	CWE-416	释放后使用	可能导致程序崩溃、使用意外值或执行代码
5	CWE-125	越界读取	可能允许攻击者从其它内存位置读取敏感信息或导致崩溃
6	CWE-20	不正确的输入验证	可能导致系统接收部分非正常输入，攻击者可能利用该漏洞修改控制流

四、结束语

物联网设备固件漏洞检测与嵌入式系统安全加固是保障物联网安全的重要环节。通过静态分析、动态模糊测试等方法可以有效发现固件中的安全漏洞，并通过物理安全加固、网络安全保护、定期更新、强化认证授权、安全编码实践等多层面策略提升嵌入式系统的安全性。

参考文献

[1] 张洪源，谢永 . 物联网固件漏洞检测技术综述 [J]. 软件导刊 ,2024,23(05):205-211.

[2] 陈灏 . 面向物联网设备固件命令注入漏洞的智能动态检测技术研究与实现 [D]. 北京邮电大学 ,2023.

[3] 万上锋 . 面向物联网设备的安全检测技术 [D]. 北京交通大学 ,2023.

[4] 蒋奎 . 面向嵌入式系统优化安全加固的程序控制流静态分析关键问题研究 [D]. 西安电子科技大学 ,2023.

[5] 廖志伟 . 面向嵌入式操作系统的安全通信技术研究与实现 [D]. 电子科技大学 ,2019.

[6] 崔亮亮 . 大数据时代背景下计算机信息处理技术的分析 [J]. 现代工业经济和信息化 ,2022(02)：122-123+152.

[7] 祖晓明 . 基于云环境的大数据计算机处理技术分析 [J]. 电子技术 ,2022(02)：156-157.

[8] 孙宇轩 . 基于大数据的计算机信息数据处理技术研究 [J]. 现代工业经济和信息化 ,2022(01)：112-113+118.

[9] 李琳；周庆 . 基于大数据的计算机信息处理技术应用与实践 [J]. 无线互联科技 ,2021(23)：102-103.

[10] 何鹏 . 大数据环境下的计算机信息处理技术研究 [J]. 中国新通信 ,2021(22)：55-56.