SoK Security Evaluation of Home-Based IoT Deployments

基于家庭的物联网部署的 SOK 安全评估

目录

摘要：.....1
背景：.....1
亟待解决的问题：.....1
问题的意义：.....2
主要贡献：.....2
基本概念.....2
主要工作：.....3
可拓展点.....9
总结.....9
心得.....9

摘要：

由于基于家庭的物联网设备在安全性实践方面有很不好的声誉。从表面来说是由于整体的问题引起的不安全性，可以通过简单的措施以解决这些问题，但这项工作发现，事实上很多安全问题的产生是由于传统的计算机安全问题产生的，提出一种方法去帮助从业者对 IOT 设备环境进行安全评估，方法以门户网站的方式呈现。

背景：

1. 物联网面临的安全威胁的场景愈发常见
2. 一些组织和供应商尝试对物联网设备标准化，但未实现

亟待解决的问题：

针对物联网设备所面临的各种安全问题，没有系统性的对各种攻击类别的划分和统计

问题的意义：

帮助物联网设备的各方对所面临的安全问题提出措施时给予参考

主要贡献：

1. 理解攻击技术、提出的缓解措施和利益相关者的责任
2. 评估 45 种设备并概述他们在物联网组件上的安全性
3. 建立门户网站 方便信息获取

基本概念

1. 硬编码：是将数据直接嵌入到程序或其他可执行对象的源代码中的软件开发实践，通常各种应用程序都需要频繁访问数据库和其他应用程序，来查询与业务相关的信息。一般通过在配置文件和脚本中明文嵌入应用程序凭据（用户身份认证的口令），实现这种通信过程自动化。对于管理员而言，识别、更改和管理这些密码非常困难。因此，这些凭证一般都会长期保持不变，进而导致一些敏感系统受到未经授权的访问）
2. 固件：固件是指设备内部保存的设备“驱动程序”，通过固件，操作系统才能按照标准的设备驱动实现特定机器的运行动作，比如光驱、刻录机等都有内部固件。类似 BIOS
3. Fuzzing：一种通过向目标系统提供非预期的输入并监视异常结果来发现软件漏洞的方法
4. 触发性编程操作：一种规定设备使用规则的简单编程 if xx 则 启动的形式
5. OAuth：协议为用户资源的授权提供了一个安全的、开放而又简易的标准。与以往的授权方式不同之处是 OAuth 的授权不会使第三方触及到用户的帐号信息（如用户名与密码），即第三方无需使用用户的用户名与密码就可以申请获得该用户资源的授权，因此 OAUTH 是安全的）
6. UPnP：通用即插即用网络协议该协议的目标是使家庭网络（数据共享、通

信和娱乐）和公司网络中的各种设备能够相互无缝连接，并简化相关网络的实现）

7. NTP:网络时间协议：使得计算机时间同步化的一种协议
8. SSDP：简单服务发现协议，是构成通用即插即用(UPnP)技术的核心协议之一。简单服务发现协议提供了在局部网络里面发现设备的机制，简单服务发现协议是在 HTTPU 和 HTTPMU 的基础上实现的协议。当一个控制点（客户端）接入网络的时候，它可以向一个特定的多播地址的 SSDP 端口使用 M-SEARCH 方法发送“ssdp:discover”消息，当设备监听到这个保留的多播地址上由控制点发送的消息的时候，设备会分析控制点请求的服务，如果自身提供了控制点请求的服务，设备将通过单播的方式直接响应控制点的请求。当一个设备接入网络的时候，它应当向一个特定的多播地址的 SSDP 端口使用 NOTIFY 方法发送“ssdp:alive”消息

主要工作：

提出一种基于组件分析的基于家庭的物联网设备建模方法论，并评估其安全状态，即物联网设备、及其伴随的移动应用程序、云端节点和相关的通信通道。

1.建立抽象模型

抽象模型有四个主要组件:**一组设备(D)、一组云端点(C)、一组移动应用程序(a)和一组通信通道(E)。**

$$where\ A,C,D\ \subset V;$$

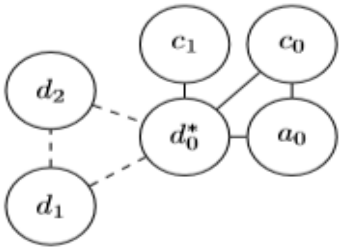
$$D{:}\{d_i\ ,i\in Z\}$$

$$C{:}\{c_j\ ,j\in Z\}$$

$$A{:}\{a_k\ ,k\in Z\}$$

$$E{:}\{e_l\ ,l\in Z\}$$

Fig. 3: IoT graph model.



2. **安全属性**
   - 攻击载荷
     - 设备：
       - 脆弱服务：涉及到运行服务的脆弱性
       - 弱认证：可猜测凭证
       - 默认配置：出厂不安全设置
     - 应用程序：
       - 权限：越权
       - 编程：编程上的不安全
       - 数据保护：硬编码问题
     - 组件通信：
       - 加密：缺乏数据保护
       - 中间人：重放 攻击等
   - 缓解措施
     - 补丁
     - 框架
   - 涉众
     - 供应商
     - 终端用户
3. **评估范围：**家用物联网设备
4. **攻击模型：**简化为一个互联网协议 IP 网络攻击者
5. **系统化知识：**

5.1 设备的攻击向量

不安全的出厂配置与弱认证导致的安全问题，August 智能锁存在弱认证，不安全的默认配置，硬编码凭证；基于云的相机上密码默认配置；缺乏身份认证的设备；对第三方应用的信任导致安全问题；测信道攻击；固件漏洞窃取 WIFI 证书，从而远程控制设备；

5.2 设备的缓解

源于供应商的更新；类似错误或异常检测的框架；对所需权限进行分析；框架更新；

5.3 设备的涉众责任

供应商负责修补和更新设备；将责任分散给用户，给予用户一定的权限使用户可以禁用一部分服务，仅运行部分服务。

5.4 设备的措施

基于传统计算机系统面临的问题

5.5 应用的攻击向量

越权行为，程序错误，数据保护错误；编程错误泄露敏感信息；模糊测试寻找 bug；使用应用收集有关可用家庭设备的信息，重新配置规则；局域网的宽松安全假设暴露敏感信息；

5.6 应用的缓解

访问控制策略；成熟的应用平台提升安全问题；

5.7 应用的涉众责任

用户+供应商，用户确保应用来源安全，供应商确保编程问题。

5.8 措施

滥用应用与设备之间的隐含信任，细粒度的控制限制移动应用程序对设备的访问

5.9 云节点的攻击向量

云端节点上的不安全 API，越权行为；Wifi Barbie doll 面临的 XSS 攻击，永不过期的 cookie；针对于监控摄像头，伪造攻击载荷，DOS 攻击；伪造载荷从而实现密码的破解，密码侦测；针对于物联网集成平台 DOS 攻击；云平台的触发性编程操作；云平台破坏造成令牌暴露； 云集

成服务缺乏细粒度控制，它们会泄漏可能导致入侵的私有和敏感信息。

5.10 云节点的缓解

推荐了正确的配置和安全的认证机制;分析用户定义的错误触发器;可编程平台的去中心化框架;

5.11 云节点涉众

用户没有办法检查或控制他们的设备发送到云端点的内容；托管物联网平台，这些平台将大部分安全责任转移给了公共云提供商，云提供商的意外停机，基础设施崩坏，遭受故意攻击;

5.12 云节点措施

集成云平台为用户提供了一种基于事件的多物联网设备执行任务的方式，而用户会受到过度特权配方和隐私影响的困扰；供应商针对于云平台安全性提出的解决方案将云平台安全性委托给其他的云平台提供商

5.13 通信链路的攻击向量

家庭物联网经常使用的物种流行应用层协议 NDS HTTP UPnP NTP 自定义实现；DNS 引发的泄露隐私；针对于 NTP 协议的中间人攻击；HTTP 协议的不安全;UPnP 滥用以及继承自 HTTP 的不安全性问题;使用 TLS/SSL 可以增强安全性；TLS/SSL 协议旧版本发现了严重问题；BLE/ZigBee/Z-wave 存在不安全隐患；LE 协议缺陷;

5.14 通信链路缓解措施

禁用 DNS 中的 ECS 功能，使用 NTP 协议的更新版本(NTPv4)，以及使用 TLS/SSL 和安全协议(HTTPS);禁用弱的或脆弱的 TLS/SSL 版本会减少暴露，但会失去向后兼容性。对于基于 LE 的通信，第一代 Zigbee 和 Z-Wave 协议有严重的缺陷和有限的缓解选项。供应商可以以牺牲兼容性为代价来禁用这些协议的不安全部分；不安全流量监控并发送报告框架；使用 Z-Wave Plus；使用 ZigBee 的 TC

5.15 通信链路涉众

供应商可以部分解决通信链路问题修补部分漏洞，终端用户无法；ISP 可以看到通信流量，但无法实施缓解措施，使得 ISP 参与到 IP 协议的部分中；LE 协议部分，供应商可以通过禁用脆弱的配对来减少遗留设

备；用户可以使用具有下一代 LE 协议的设备

5.16 方法

UPnP,在 LAN 中的通信很少加密，弱加密和 MITM 攻击；TLS/SSL 在实现和部署上有缺陷,这些协议依赖于 PKI;

6. 评估

6.1 实验设置

物联网子网、自定义 Linux 网关、评估机器

6.2 数据

设备、移动应用程序、云端点和网络流量生成的不同类型的数据；交互过程产生的网络流量，提取、捕获、并分类于应用层协议中

6.3 面临问题

自动设备更新、云端点分类、无线网络分析和 IOS 应用程序的解密

6.4 针对于设备的评估

- Nessus 扫描器使用 CVSS 评分系统
- 45 台设备、84 个服务、39 个问题相关问题
- 使用 TLS/SSL 配置设备，但配置有问题证书是自签名的，它们支持弱到中等的密码，它们使用短的 TLS/SSL 密钥，它们允许使用脆弱的 SSL 版本(v2、v3 和 CBC 模式)，并且有过期的证书
- 运行 UPNP 的设备没有内置的身份验证或安全性，脆弱版本

6.5 针对于移动应用的评估

- MobSF、Qark 和 Kryptowire 的服务对物联网设备的每个移动应用程序进行静态和动态评估
- 42 设备有配套应用、分析 83 个（android 41,42IOS）、39 个设备有问题，越权 24 个、15 个敏感信息泄露、17 个未加密数据

6.6 针对于云节点的评估

- 使用 Nessus 扫描器来发现、分析和评估云端点上正在运行的服务
- 45 个设备 4000 多云端点域
- 对每个域进行分类分为四类：第一方（基于云的）、第三方（订

阅 CDN）、混合、未知

- 第一方 950、第三方 1287、混合 630、1288 未知
- 18 台设备使用了过时的服务
- 8 台使用云终端的设备容易受到攻击，存在公共漏洞。
- 7 台设备以明文方式通过云端点身份验证
- 26 个使用云端点的设备存在 TLS/SSL 配置问题签名证书、域名不匹配以及对脆弱的 TLS/SSL 协议版本的支持
- 10 台设备使用了配置错误的云端点， 允许文件路径和服务器上运行的进程等敏感信息公开
- 4 台设备使用了运行过时操作

6.7 针对于通信的评估

- 使用 Nessus 扫描器，ntop-ng，Wireshark、sslsplit 来发现
- 手动检查流量，并使用 sslsplit 测试它们的 MITM 攻击
- DNS、HTTP、UPnP、NTP 和定制协议
- 41 台设备使用了 DNS 协议
- 38 台设备使用 HTTP 协议\ 34 台使用 TLS/SSL 会话(HTTPS)
- 21 个使用通用即插即用协议的设备\ SSDP 请求，要么响应一个 SSDP 请求
- 25 个使用 NTP 协议进行时间同步的设备
- 28 个使用特定于设备的自定义协议
- D-C 25 台设备加密了它们所有的通信，15 台设备部分加密了它们的通信，还有 2 台设备没有加密它们与云端点的通信
- A-C 24 个应用程序加密了它们所有的通信，10 个应用程序部分加密了它们的通信，1 个应用程序没有加密它到云端点的通信
- A-D 5 个设备对它们的通信进行了加密，2 个设备对它们的通信进行了部分加密，还有 20 个设备没有对它们的通信进行加密
- MITM 攻击 20 个设备中，有一个或多个易于受到 MITM 攻击的通信边缘

7. 建议

7.1 针对于涉众的建议

- 供应商确保组件安全需求
- 用户配置使用加密，禁用服务，网络分段
- 其他 ISP 补救
- 云提供商保障

可拓展点

- 针对于设备间通信、移动应用到设备交互以及物联网组件间的信任关系额外测量
- 设备间通信在局域网环境下的研究
- 设备未经授权与其他同局域网下设备进行交互
- 物联网标准制定

总结

通过一个抽象模型讲物联网设备现有文献系统化，并针对 45 个设备进行评估

心得

本文是系统性的分析了当前家用物联网环境下的主要安全风险，有助于理解整个家庭物联网的总体安全情况，有引导性和概括性，属于**综述类型**的文献，针对于特定的方向可以根据本文的参考文献进行深入的探索。