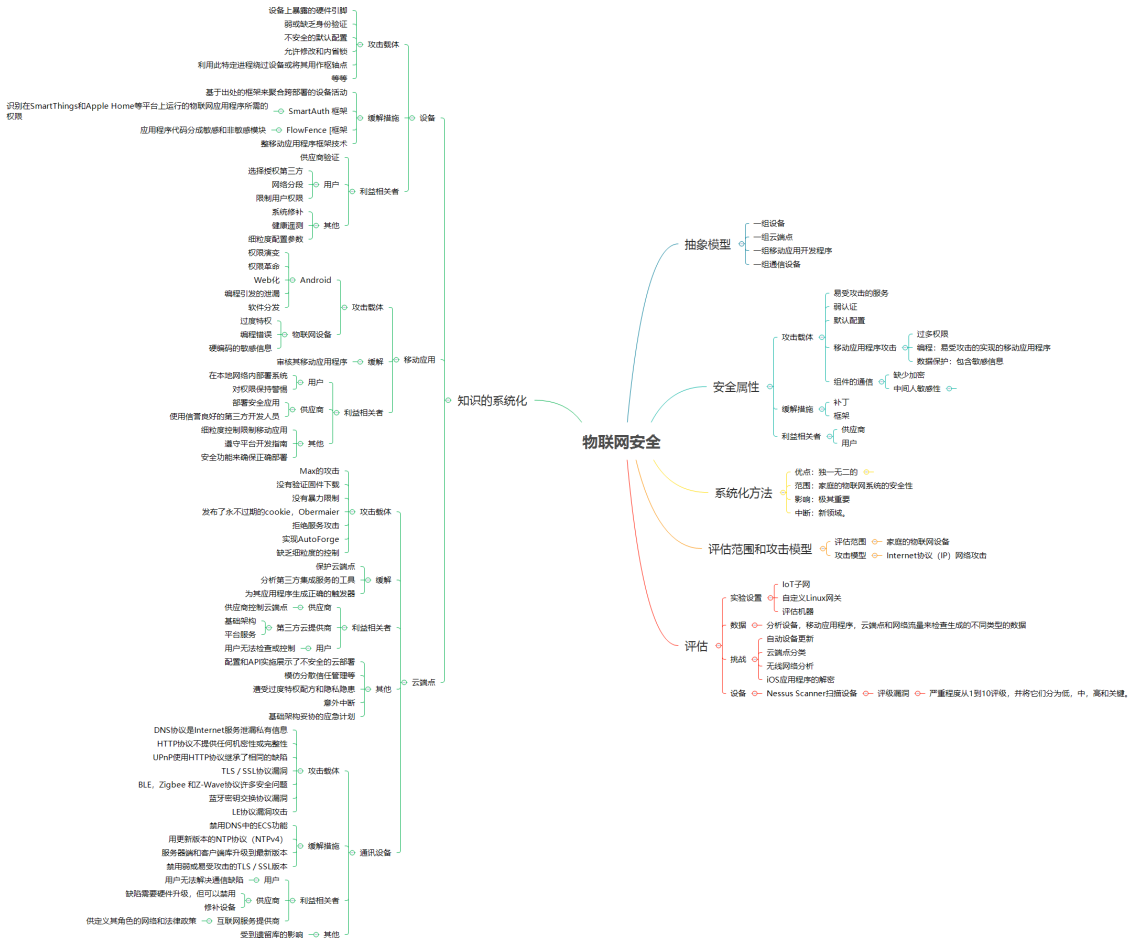
物联网安全



1. 抽象模型

1.1. 一组设备

1.2. 一组云端点

1.3. 一组移动应用开发程序

1.4. 一组通信设备

2. 安全属性

2.1. 攻击载体

2.1.1. 易受攻击的服务

2.1.2. 弱认证

2.1.3. 默认配置

2.1.4. 移动应用程序攻击

过多权限

编程：易受攻击的实现的移动应用程序

数据保护：包含敏感信息

2.1.5. 组件的通信

缺少加密

中间人敏感性

2.2. 缓解措施

2.2.1. 补丁

2.2.2. 框架

2.3. 利益相关者

2.3.1. 供应商

2.3.2. 用户

3. 系统化方法

3.1. 优点：独一无二的

3.1.1.

5.3.3. 无线网络分析

5.3.4. iOS应用程序的解密

5.4. 设备

5.4.1. Nessus Scanner扫描设备

评级漏洞

严重程度从1到10评级，并将它们分为低，中，高和关键。

6. 知识的系统化

6.1. 设备

6.1.1. 攻击载体

设备上暴露的硬件引脚

弱或缺乏身份验证

不安全的默认配置

允许修改和内省锁

利用此特定进程绕过设备或将其用作枢轴点

等等

6.1.2. 缓解措施

基于出处的框架来聚合跨部署的设备活动

SmartAuth 框架

识别在SmartThings和Apple

Home等平台上运行的物联网应用程序所需的权限

FlowFence [框架

应用程序代码分成敏感和非敏感模块

整移动应用程序框架技术

6.1.3. 利益相关者

供应商验证

用户

选择授权第三方

网络分段

限制用户权限

其他

系统修补

健康遥测

细粒度配置参数

6.2. 移动应用

6.2.1. 攻击载体

Android

权限演变

权限革命

Web化

编程引发的泄漏

软件分发

物联网设备

过度特权

编程错误

硬编码的敏感信息

6.2.2. 缓解

审核其移动应用程序

6.2.3. 利益相关者

用户

在本地网络内部署系统

对权限保持警惕

供应商

部署安全应用

使用信誉良好的第三方开发人员

其他

细粒度控制限制移动应用

遵守平台开发指南

安全功能来确保正确部署

6.3. 云端点

6.3.1. 攻击载体

Max的攻击

没有验证固件下载

没有暴力限制

发布了永不过期的cookie，Obermaier

拒绝服务攻击

实现AutoForge

缺乏细粒度的控制

6.3.2. 缓解

保护云端点

分析第三方集成服务的工具

为其应用程序生成正确的触发器

6.3.3. 利益相关者

供应商

供应商控制云端点

第三方云提供商

基础架构

平台服务

用户

用户无法检查或控制

6.3.4. 其他

配置和API实施展示了不安全的云部署

模仿分散信任管理等

遭受过度特权配方和隐私隐患

意外中断

基础架构妥协的应急计划

6.3.5. 通讯设备

攻击载体

DNS协议是Internet服务泄漏私有信息

HTTP协议不提供任何机密性或完整性

UPnP使用HTTP协议继承了相同的缺陷

TLS / SSL协议漏洞

BLE，Zigbee 和Z-Wave协议许多安全问题

蓝牙密钥交换协议漏洞

LE协议漏洞攻击

缓解措施

禁用DNS中的ECS功能

用更新版本的NTP协议（NTPv4）

服务器端和客户端库升级到最新版本

禁用弱或易受攻击的TLS / SSL版本

利益相关者

用户

用户无法解决通信缺陷

供应商

缺陷需要硬件升级，但可以禁用

修补设备

互联网服务提供商

供定义其角色的网络和法律政策

其他

受到遗留库的影响