3131100788 · 物联网安全

浅谈你对物联网的理解

胡玉斌 / 2021111054

October 14, 2021

物联网是一个比较广的概念，我们常用的手机可能是物联网中的终端节点，教室里面的摄像头在物联网中负责采集信息，提到物联网，可能涉及我们生活中的方方面面。

物联网中的技术工作是具体而细致的，例如，针对图像识别算法进行设计可以使得轻量级视频传感器节点高效工作、对移动终端安全机制进行设计可以保护用户在使用物联网服务中的个人隐私安全。

认真思考，回答你在这一课程中，会聚焦哪一方面的技术工作呢?

1 什么是物联网？

物联网（IoT，Internet of things）即“万物相连的互联网”，是互联网基础上的延伸和扩展的网络，将各种信息传感设备与网络结合起来而形成的一个巨大网络，实现任何时间、任何地点，人、机、物的互联互通。

诚然，互联网上对物联网的定义有很多，掌握一项技术的关键是要了解其背后的基本思想，这有助于定义您自己的含义和适用性。每个人都可以有自己的定义，对我来说，物联网是这样的：

- 物联网!= 硬件
  这是人们之间普遍的误解，认为物联网仅指硬件，这造成了想象中的障碍，并使大多数安全研究人员不愿涉足物联网安全。随着学习的深入，我们会意识到硬件仅构成 IoT 生态系统的 1/3。最重要的是，如果您可以破坏其他组件（例如，Cloud），则不仅会入侵设备，还会造成更大的破坏。
- 提供虚拟物理接口的硬件设备
- 后端数据存储区，用于存储和计算能力以对数据进行统计分析。
- 一个虚拟界面，供用户查看分析的数据并将命令发送到物理世界

2 物联网在哪里使用？

- 家庭自动化
- 智能基础设施
- 医疗保健
- 工业控制系统
- 运输
- 实用工具
- 还有更多

3 物联网架构以及攻击面

物联网架构以其最简单的形式包括三个组件 [1]

- Mobile
- Cloud
- Device

现在我们可以很容易地将 IoT 的各个组成部分隔离开来，并尝试为每个组件分别定义攻击面，然后将它们组合起来以创建一个整体的概述。

3.1 Mobile

移动是物联网的重要用户界面之一，通过它最终用户可以洞悉物理世界的状态。由于移动应用程序与 IoT 生态系统进行通信以发送命令和读取数据，因此它成为 IoT 生态系统的切入点之一。我们将尝试从物联网的角度列出移动设备的攻击面：

- 存储
- 认证
- 加密
- 通讯

3.2 Cloud

云是物联网的重要组成部分之一，通常来自产品线所有实例的数据都在这里汇聚。这使其成为非常有趣的攻击点。记住，我在上一篇文章中提到物联网不仅与硬件有关。原因是云将保存所有已部署的 IoT 实例的数据，并具有向所有实例发送命令的特权。通常它是由用户启动的，但是如果受到威胁，攻击者将获得对全球部署的设备（及其数据）的控制权，这很危险。总体而言，攻击面专注于它提供的接口，其中包括：

- 存储
- 认证
- 加密
- 通讯
- 蜜蜂

3.3 Device

接下来是设备，它是 IoT 技术的游戏规则改变者：)。它与物理世界进行交互，并与虚拟世界进行通信。这是物理世界数据的第一站。鉴于围绕用户隐私存储的用户敏感数据（例如房屋数据，身体数据，个人信息），围绕用户隐私存在着整个争论。将来，设备可能会直接通过其钱包或单独的临时钱包使用用户的加密货币来购买物品，进行维修等。攻击面看起来如下所示

- 存储
- 认证
- 加密
- 通讯
- 传感器接口
- 外围接口
- 硬件接口
- 人机接口

3.4 通讯

尽管这不是有形的攻击面，但理想情况下，有形的攻击面将是通信接口和负责通信的各个驱动程序/固件。但是，这需要一个单独的部分，因为 IoT 生态系统可以在有线以及无线介质上使用的通信协议列表很多。以下是构成通信攻击面的一些区域。

- 认证
- 加密
- 偏离西医标准
- 协议实施异常

4 聚焦的技术工作

选题的方向是根据当今流行的漏洞选择，在谈论十大漏洞时，我们首先想到的是 OWASP。为什么不呢，毕竟他们是定义 Web 和移动十大漏洞的先锋。

2021 年的十大漏洞 [2]：

1. 2021-Broken Access Control
2. 2021-Cryptographic Failures
3. 2021-Injection
4. 2021-Insecure Design
5. 2021-Security Misconfiguration
6. 2021-Vulnerable and Outdated Components
7. 2021-Identification and Authentication Failures
8. 2021-Software and Data Integrity Failures
9. 2021-Security Logging and Monitoring Failures
10. 2021-Server-Side Request Forgery

我准备关注 Broken Access Control [3] 漏洞，它涉及访问控制强制执行策略，使用户不能在其预期权限之外采取行动。故障通常会导致未经授权的信息泄露、修改或破坏所有数据或执行超出用户限制的业务功能。

在之后的报告中会详细描述漏洞以及如何预防，并且在之后复现 CWE。

References

[1] S. Paper, "物联网安全从入门到入坑." https://paper.seebug.org/1045/, Sep 2019.

[2] OWASP, "A01:2021 –broken access control." https://owasp.org/Top10/A01_2021-Broken_Access_Control/, 2021.

[3] OWASP, "Welcome to the owasp top 10 - 2021." https://owasp.org/Top10/, 2021.