IOT安全

相关资源

IOT 漏洞 top 10

https://xz.aliyun.com/t/2278

https://www.owasp.org/images/8/8e/Infographic-v1.jpg

https://payatu.com/iot-security-part-3-101-iot-top-ten-vulnerabilities/

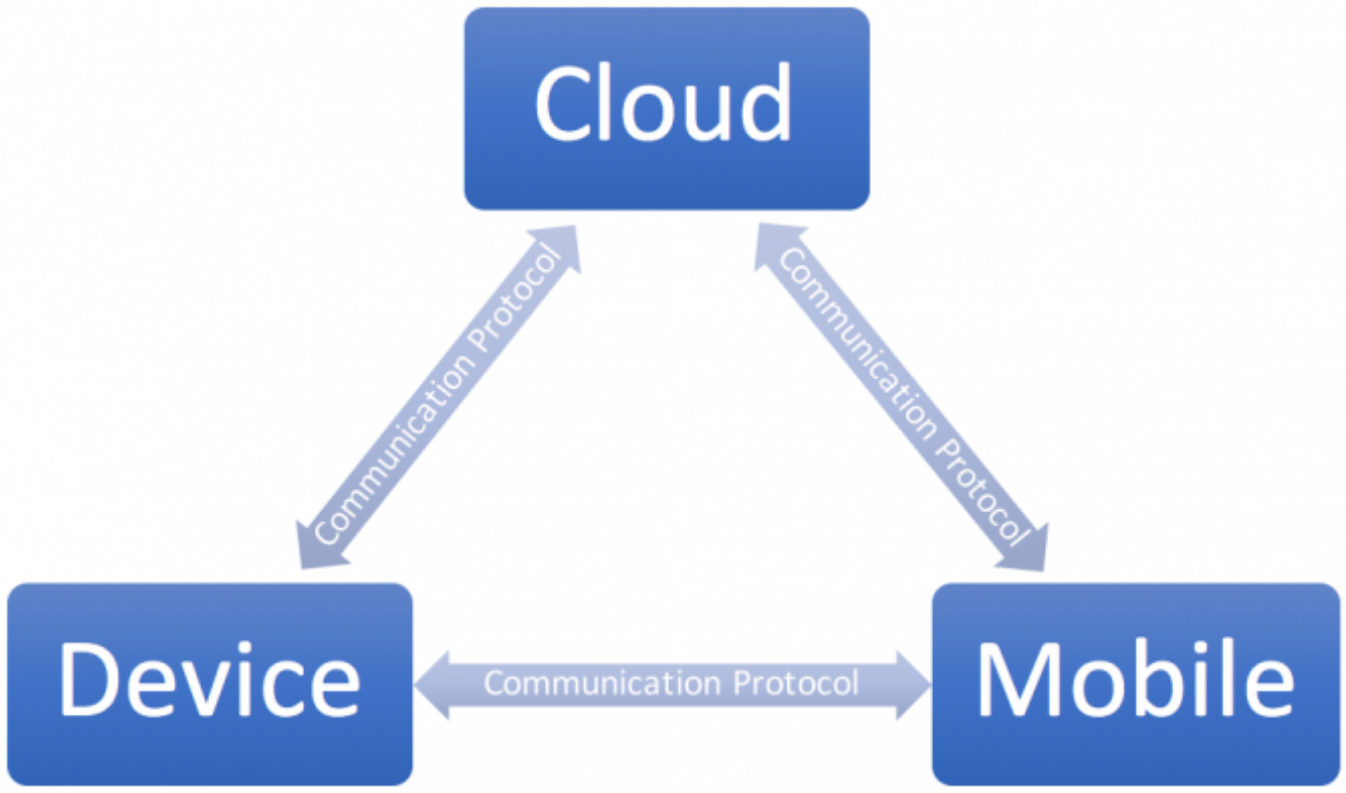
总结性的资源

https://github.com/nebgnahz/awesome-iot-hacks

https://github.com/V33RU/IoTSecurity101

IOT架构

IOT 的整体架构主要就 三部分： 硬件设备，移动终端，云。他们之间的通信都有可能会出现问题。



智能硬件的攻击面也主要在 **协议** 这一块， 比如协议数据的加密问题， 协议的权限问题，认证机制以及对数据的处理问题（堆栈溢出）

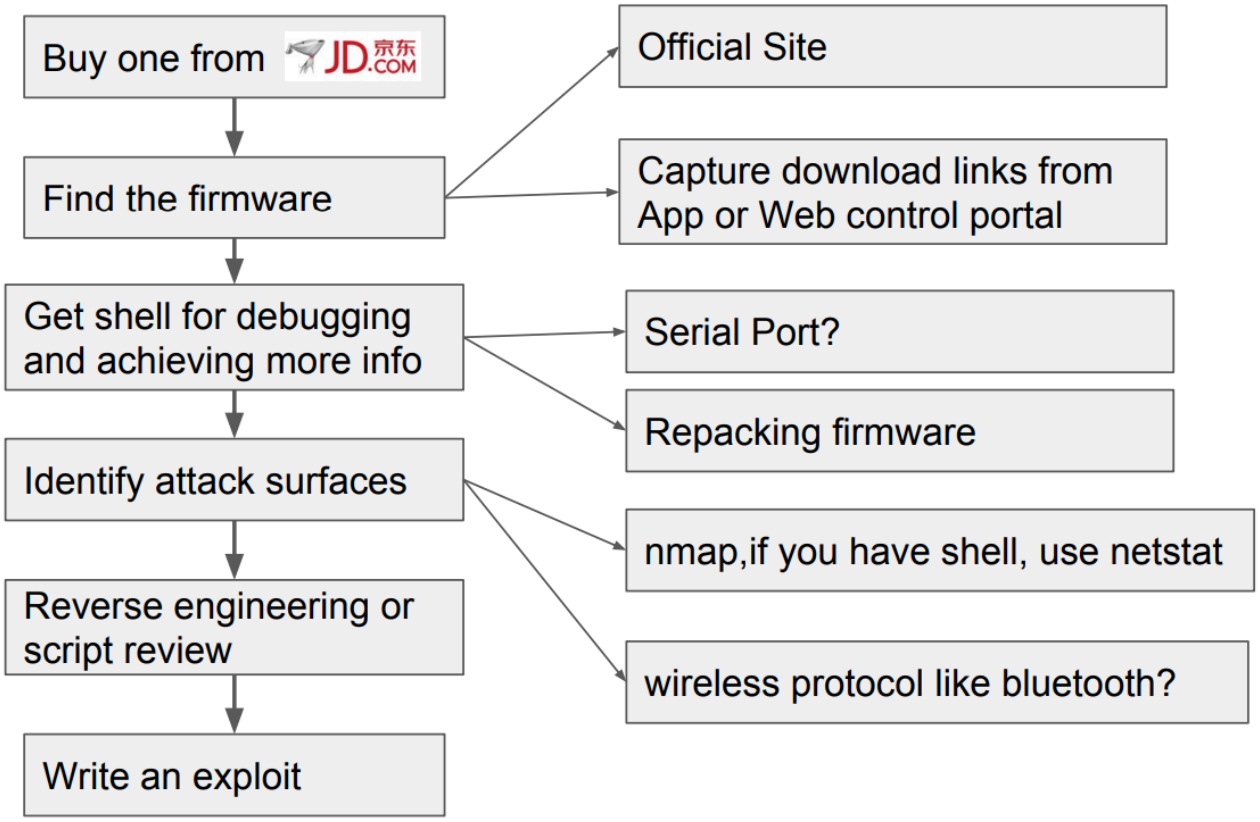
参考

https://zhuanlan.zhihu.com/p/35411393

https://payatu.com/iot-security-part-1-101-iot-introduction-architecture/

路由器分析

总流程



找分析入口

从数据接收点分析

TCP

- listen
- recv

UDP

- recvfrom

使用关键字

HTTP

GET/POST/HTTP 1.1/Accept/Authorization/Cookie

UPNP SSDP

M-SEARCH/ssdp:discover

漏洞审计的技巧

缓冲区溢出

- 在 IDA 里面搜索&交叉引用 容易出现问题的函数， `strcpy/sprintf/sscanf/...`
- 注意相对安全的内存拷贝函数的 **长度参数** 和 **缓冲区实际长度** 是否匹配 `memcpy/strncpy/snprintf/...`
- 注意对 缓冲区的循环操作。

整数溢出

- 注意协议数据中的整数字段的处理（在某些指令时进行的类型强转，比如：无符号和有符号数比较）

格式化字符串漏洞

- 在 IDA 里面看 `printf/sprintf/snprintf/...` 这类函数的使用

UAF 和 Double free

- 注意内存的分配和释放是否匹配
- 对程序要有全局观

堆/栈未初始化漏洞

- 注意变量是否经过初始化过程，特别是那些由上层传入，或者会传到下层函数的变量

来源

《智能硬件漏洞挖掘与利用实践.pdf》