智能设备安全畅谈—安全小课堂第四十期

京东安全应急响应中心 2016-12-30

安全小课堂第四十期

毋庸置疑，智能设备将是下一场技术革命。智能设备给人们带来新的便利和奇迹令人欢呼，但其安全性也不容忽视。本期来聊聊智能设备安全。

本期邀请到四叶草安全CSO朱利军先生（ID：Rabit2013），四叶草安全实验室负责人。四叶草安全实验室IOT安全研究小组对IOT设备漏洞挖掘与研究颇有成就。

文丨豌豆妹　图丨源自网络

> > > 1 < < <

豌豆妹

能介绍下智能硬件设备常见的安全问题吗？

哆啦A梦

智能硬件常见的问题整体上分为两类：系统安全问题和网络通信安全问题。详细的说，系统安全问题包括系统常见的漏洞，例如注入、命令执行、未授权访问、弱口令、系统设计缺陷等等。网络通信安全主要包括网络通信过程中，通信数据是否安全、身份认证是否安全、密钥分发和管理是否安全等等，具体来说，既包括传统的安全漏洞，也包括硬件设备特有的漏洞，例如调试接口未关闭、系统能被root等等。

> > > 2 < < <

豌豆妹

智能硬件设备存在的危害性呢？

哆啦A梦

随着万物互联时代的到来，基本上所有的智能硬件都接入网络，最大危害主要包括敏感数据泄露、个人隐私被监控，导致社会生活混乱，甚至会威胁生命安全。例如智能交通网络，假设连网的交通红绿灯控制系统被攻击，十字路口将出现惨不忍睹的混乱状况。例如正在高速运行的高铁控制系统，如果被攻击，导致紧急刹车，车上乘客的生命岌岌可危。一旦所有的硬件接入网络，大家就没什么隐私可言。还有像一些工业控制系统、卫星导航，一旦接入网络，其危害不言而喻。

> > > 3 < < <

豌豆妹

请分享一例智能硬件经典的攻击案例，并进行深入分析吧~

哆啦A梦

我来分享下我们实验室当时挖掘某智能物联网家居的过程。我们之前做了次研究，一套家用物联网设备，其中包括无线路由、视频盒子、数字电视、烟雾传感器等等。当时分析发现无线路由存在命令执行漏洞，可导致无线路由远程被root，视频盒子被发现调试接口未关闭，导致视频盒子可被root，且视频盒子与云端通信未进行加密验证，可被攻击者劫持，在视频盒子中逆向分析得到与云端交互的账号密码，可以读取云端存储的所有数据，再例如其中的烟雾传感器，经dump固件，对固件进行逆向分析，发现存留调试接口，且通信数据可被伪造。像这样类似的漏洞基本上很多智能硬件都存在。

> > > 4 < < <

豌豆妹

那在智能硬件安全设置方面，需考虑的点有哪些呢？

哆啦A梦

目前对于智能硬件来说没有一套完整健全的安全标准，那么我们从漏洞研究的角度上来总结，整体上分为系统设计时需要考虑的点和网络通信需要考虑的点。
从系统设计来说首先需要避免各种各样传统漏洞的出现，其次需要在设计生产时避免各种调试和相关的接口暴露，最后还需要考虑系统通信密钥存储可能出现的风险。
从网络通信来说，首先需要保证通信协议的安全，其次需要保证设备与云端认证的安全，最后还需要保证通信数据的安全。

> > > 5 < < <

豌豆妹

如何发现智能硬件的安全风险呢？

哆啦A梦

对于智能硬件需要挖掘各种各样的漏洞，并发现安全风险，其实要求挺高的，不过对于一个安全研究者来说没什么难度。首先你需要了解常见的各种各样漏洞，熟悉漏洞原理，其次你需要熟悉各种各样的智能设备的架构和工作原理业务逻辑等等，第三你需要对固件、汇编代码有熟悉的了解，第四你需要有一个好奇的心和极强的动手能力，这四点结合起来你就可进入智能硬件风险研究的大门，其他的还需要漏洞研究的经验与积累。这块其实需要大家很熟悉漏洞原理，然后也需要大家脑洞大开+执行力强，当然一些基础的技能也是必须的，例如逆向分析，调试等。

> > > 6 < < <

豌豆妹

基于美国遭受大面积断网事件，智能硬件在工业物联网的重要地位能分析下么？

哆啦A梦

本次攻击的一个重要来源是感染了“未来”(Mirai)病毒程序的僵尸网络，共有超过百万台物联网设备成为此次“瘫痪”的媒介，此次事件只是智能硬件在生活中的一个很小的例子。无论是车联网，还是工控网络，或是传统的互联网，万物互联将开启新的网络时代，所有的设备，无论是传统设备还是新型智能设备都将接入网络，随之智能工业控制系统的出现，智能设备在工业网络或者物联网都将是一个爆发式的增长，智能硬件带来便利生活的同时，也埋下很大祸根，投入使用的智能硬件一旦出现任何安全事件，其造成的损失将难以估算，甚至可能让一个国家灭亡。现在各地区都在构建智慧城市，在建设中各种各样的设备都被接入，ddos只是个很暴力的玩法，现在咱们开始搞IOT研究也是这个道理。智能设备厂商在开发设计时就缺一些安全标准。现在很多产商开始注意到这类问题的存在，但是他们很多不懂安全，也不知道存在哪些攻击方式，对于研究者来说是一个黄金期。

豌豆妹

好嘞~谢谢小伙伴的大力分享。如果你对智能硬件设备安全也感兴趣，可以在后台留言互动哟~

微信公众号：jsrc_team
新浪官方微博：
京东安全应急响应中心