安全小课堂第五十三期【智能硬件漏洞挖掘入门指导】

京东安全应急响应中心 2017-04-14

随着科技的发展，智能硬件逐渐进入人们的生活。比如扫地机器人、智能冰箱、智能音箱等。一方面智能硬件给人们的生活带来了前所未有的便利，但另一方面智能硬件也潜藏着安全危险，智能硬件网络安全方面的漏洞是导致危险的一个重要因素。

JSRC **安全小课堂第五十三期**，我们来邀请讲师分享了关于智能硬件网络安全方面的漏洞挖掘的一些知识。感谢讲师**陆羽**、**0xgg**师傅的分享，感谢JSRC白帽子px1624、東.、胖猴粉、数据流、苦逼司马、沦沦、1ce、DragonEgg的讨论。

智能硬件存在的漏洞类型有哪些呢？

京安小妹

我们知道智能硬件一般包含：硬件、固件、App、云平台这几大部分。相应的从攻击面可以分为：固件漏洞、App漏洞、云端漏洞、通信协议漏洞。

在固件、App、云服务这几个点上，都会涉及数据存储，所以都可能存在数据存储不安全的漏洞（明文存储默认用户名、密码，身份认证信息，明文存储配置信息等）。

固件漏洞网上路由器的例子很多了。App漏洞通常也包括传统的web漏洞，比如任意用户注册、用户信息泄露、越权、撞库等等。

智能硬件常见的通信协议HTTP、HTTPS、Zigbee、蓝牙、websocket、XMPP、COAP、MQTT，协议比较多，大家搞web的，HTTP、HTTPS这些应该比较清楚

智能硬件的操作系统有Android、linux、VxWorks、FreeRTOS等。

这些方面都有可能存在问题。

讲师：陆羽、0xg

白帽子观点：vxworks是嵌入式设备的居多吧 。

白帽子提问:好像还有的协议是自己的 不公开的，是不是?

些是厂商自己开发的私有协议，但如果设计时考虑不周全，可能安全问题更多。当然也不能一棍子打死了，不过开发私有协议，能保证好安全性，还是很有难度的。

讲师：陆羽、0xgg

白帽子观点:主要你都不知道他是啥协议，还得去分析，所以很多人搞未知协议 为了节省时间，都是直接模糊测试。

智能硬件漏洞的危害会有多大呢?

京安小妹

从个人层面讲，比如智能摄像头远程控制漏洞、越权访问漏洞会导致用户被监控、隐私泄露，可能会遭遇财产损失。如果智能汽车出现漏洞，可能直接导致交通事故，威胁人身安全。
从企业层面讲，如果企业生产的智能硬件出现漏洞，被黑客批量控制实施攻击行动，会给企业产生很大的负面影响；去年新闻比较多了，大家应该知道。
如果智能工厂出现安全漏洞，被黑客攻击控制，可能导致生产中断、生产事故，给企业造成严重的财产损失。
从国家层面讲，重要的国家企事业单位中，如果使用的智能硬件存在漏洞，被黑客控制就可能导致泄露国家机密，如果黑客控制大量物联网设备，也可能对重要的网络设施实施DDos攻击，这些都可能威胁国家安全。所以现在，国家也很重视网络安全。

讲师：陆羽、0xgg

掘智能硬件漏洞需要具备什么样的基础能力呢?

京安小妹

1.需要了解智能硬件的架构、工作原理。
2.需要熟悉常见二进制、App、Web、通信协议等各种漏洞及原理，可以先深入学习一个方向。分析固件漏洞，需要熟悉智能硬件的操作系统，如Android、linux、VxWorks、FreeRTOS等。逆向分析固件也需要掌握ARM、MIPS汇编知识、硬件开发基础知识。分析App漏洞，则要学习Android、IOS App逆向知识及漏洞。分析云平台漏洞，则需要学习Web相关安全知识。
3.分析通信协议漏洞，也需要学习常见的通信协议HTTP、HTTPS、Zigbee、蓝牙、websocket、XMPP、COAP、MQTT及网络数据分析工具burp、wireshark的使用。
可以根据自己特长，选一个比较熟悉的方向进行学习、研究。
不用全部掌握，可以先挑一两个擅长的方向，先动手练起来，等掌握了一个方向后，再往其他方向发展。先搞自己擅长的，容易有成就感，这样比较容易继续学习下去。不要直接挑个硬骨头去啃，容易打击信心。

讲师：陆羽、0xgg

能不能举个例子讲一讲如何挖掘智能硬件漏洞呢？

京安小妹

比如，分析一款智能电视，我们先要了解它架构和业务流程。智能电视使用Android系统，带Wifi功能，通过网络连接云端服务器获得视频节目。智能电视还有一个安卓App，可以通过手机app来控制电视换台、调节音量、开关电视、查看历史观看记录等等，了解了这些之后，我们可以分析智能电视的安卓系统是不是存在已知漏洞，是不是开启了adb远程调试接口，如果开启了，是不是在暴露在公网上，如果是，则可被远程安装安卓木马。然后我们可以逆向分析安卓app，查看是否有注册功能，是否输入界面存在sql注入。
可以把app常见漏洞试一下，比如任意用户注册、用户信息泄露、越权、撞库。
比如绑定设备功能校验逻辑是否有问题，可绑定别人的电视。
还可以对App通信进行抓包，分析发送控制电视的指令，是否可重放，是否存在越权。

讲师：陆羽、0xgg

白帽子观点：有的还得熟悉网络这块的东西，的确门槛挺高。
白帽子提问：有相关书籍推荐吗？

《智能硬件安全》、《硬件安全攻防大揭秘》都可以作为入门书籍，入门之后，剩下的就是多在网上看看技术文章了。网上会有比较新的资料，写到书里面的都会晚一两年，看雪有个智能硬件板块。

讲师：陆羽、0xgg

作为企业需要怎样做以避免智能硬件出现漏洞呢？

京安小妹

首先企业要重视安全问题，提高技术人员的安全知识或招募相关安全人才。从设计时就要做好安全设计，比如重要数据需要加密存储，通信需要使用安全协议并加密传输数据，需要有身份认证、业务授权功能等等。

开发时，开发人员需要了解常见安全漏洞及原理，了解如何开发才能避免出现这些漏洞。测试时，需要进行安全测试，检测是否存在安全漏洞。很多智能硬件漏洞，主要还是设计时就没有考虑到安全问题。

讲师：陆羽、0xgg

白帽子提问1：某些摄像头刚开始是不联网的，最开始app跟摄像头绑定的时候 通过声音来实现的，然后app操作让摄像头联网，这个过程通信是用蓝牙 还是啥？声波那个是啥通信方式？

配对用的那个声波就是声音。具体协议不知道，类似摩斯电码一样的。直接传输的铭文的wifi热点名字和密码，然后摄像头直接识别后配对，连接网络。APP并没有通过蓝牙、红外或者nfc让设备联网，密码是通过声波直接传输给摄像头的。

讲师：陆羽、0xgg

白帽子提问2：是不是噪音大就会干扰?

是的。噪音大的时候会导致无法识别密码，无法配对，所以要保持周边安静。

讲师：陆羽、0xgg

还有什么补充吗?

京安小妹

手机和智能设备之间的通讯主要靠云端传输，硬件连接云端接口，手机也连接云端接口。这样完成通讯，很少智能硬件使用直连的。目前还有另外集中配对方式，蓝牙、zigbee、wifi热点方式，蓝牙不用解释大家都理解，zigbee跟蓝牙类似。但是成本更低功耗更低。但是有一定的安全风险，能抓到配对过程中的明文密码。
wifi热点方式就是设备自建一个wifi，默认没有密码，或者默认密码，初次配对后通过wifi内网http接口从手机把wifi密码直接推送给智能硬件，完成联网配置。联网后手机和硬件之间就是通过云端接口通信了，目前蓝牙4.0以上的安全性还是不错的，再次配对开启wifi通常需要手动插针或者按钮几秒，完成初始化才可以再次配对。NFC不是所有手机都有的。所以这种配对方式不会广泛应用。
白帽子提问：关于使用声波配对，周边有噪音也能成功，是因为做了降噪处理了？
陆羽：是的。另外使用的频段本身也不太会有噪音。有可能真正用到的声音频段耳朵未必能听见。电子 元器件可以接受到。吱吱声不一定就是数据本身，使用更低的频段可以避免和自然噪声冲突的问题。

讲师：陆羽、0xgg

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文