腾讯反病毒实验室安全研究员杨经宇：开启IoT设备的上帝模式

原创

csdn业界要闻 于 2017-12-01 16:16:05 发布 746 收藏
文章标签： 腾讯 安全 杨经宇 看雪安全开发者峰会

本文链接：https://blog.csdn.net/csdn_bang/article/details/80133055

11月18号，2017看雪安全开发者峰会在北京悠唐皇冠假日酒店举行。来自全国各地的开发人员、网络安全爱好者及相应领域顶尖专家，在2017看雪安全开发者峰会汇聚一堂，只为这场“安全与开发”的技术盛宴。

伴随着IoT设备大量涌入智能家居领域，大众的安全也将面临更严峻的挑战。IoT设备因为自身与传统PC设备在硬件和软件上的巨大差异，引发了新的安全问题。峰会现场，腾讯反病毒实验室安全研究员杨经宇以摄像头固件校验漏洞为例，着重介绍了一种伪造固件绕过固件校验算法进行Root设备的方法，该漏洞也被CNNVD收录，并被评级为中危漏洞。

而IoT设备被破解之后，带来的安全隐患也不仅局限于监听监控。杨经宇还以一个DDNS智能硬件的root漏洞为例，详细讲解了如何将一个原本不具备WiFi功能的IoT设备开启WiFi功能，这将可能引发更多意想不到的攻击。在演讲最后，杨经宇对IoT安全的缓解机制提出建议，即通过固件签名、保护种子、物理手段，能够对固件校验、密码生成、WiFi扫描过程中出现的IoT设备漏洞进行有效防御。

腾讯反病毒实验室安全研究员杨经宇

> 杨经宇（Jingle）毕业于伦敦大学信息安全专业，现就职于腾讯反病毒实验室，从事恶意代码研究工作。开发的腾讯哈勃分析系统开源版入选过BlackHat兵器谱。热爱IoT安全，病毒分析等领域的研究。

以下为演讲速记：

2017年是IoT蓬勃发展的一年，同时也是IoT相关安全问题爆发的一年。在这个机遇与挑战并存的时代里，我们需要去主动面对未知的世界。今天我给大家带来了关于IoT设备root权限相关的一个技术分享。题目中的上帝模式，就是指获得了IoT系统root权限之后的状态，因为进入root模式后，大量的保护机制可以被绕过，能够开启之前被禁用的功能，能够获得至高无上的权限，所以将root模式称之为上帝模式。

首先介绍一下我自己。我叫jingle，硕士毕业于伦敦大学信息安全专业，本科毕业于北京师范大学计算机专业。现在就职于腾讯反病毒实验室，从事安全研究工作。参与开发的腾讯哈勃分析系统开源版（HaboMalHunter）入选过BlackHat兵器谱。我个人非常热爱安全技术，希望能够和大家相互交流和学习。

接着介绍一下，本次议题的大纲。IoT安全的范围非常广泛，涉及技术和非技术等多方面的交叉，但是我们今天会聚焦在技术方面，会专注于讨论IoT设备 root相关的安全问题。包括root IoT设备的常用方法，获得root权限后的安全威胁，和对应的缓解措施。

另外需要说明的是，本次议题介绍的漏洞案例，都向CNNVD进行了报送，并得到了确认。其次因为我们只关心技术，就隐去了相关厂商的名字。

背景介绍

因为IoT安全属于新兴安全领域研究，我准备首先简单介绍一下一些相关的背景知识。

大众眼中的IoT

在大众看来，IoT就是万物互联，IoT让生活变得更便捷。比如智能开关，让人和家用电器之间突破了空间的限制，例如通过自动定时，在我下班前，电暖气就会自动启动，一回家整个屋子是温暖的，等到白天上班，电暖气就会自动断电，这样就不会担心家里没人，万一失火的问题。从这里例子，大家也能看出，其实安全会是大家非常关心的一个方面，大家会担心用电安全，使用摄像头会担心隐私的安全，这些都是我们作为安全研究人员应该去考虑改进的方向。

程序员眼中的IoT

在座的各位大部分都是搞技术的，我们转换一下视角，看一下程序员眼中的IoT是什么样子的。在程序员看来，IoT设备就是具备联网功能的嵌入式设备。所谓嵌入式设备，主要由嵌入式CPU，一般是ARM或者是MIPS，硬件外设，例如内存、USB、网卡和传感器等，和嵌入式操作系统，大部分是Linux系统，这三部分组成。联网功能主要涉及一些通信协议，例如WIFI、蓝牙、3G和目前最新的NB-IoT协议等。

这些设备首先通过传感器采集信息，例如温度、湿度、图像和声音等，其次将这些信息通过通信协议上传至云端服务器，云端服务器对数据进行录入、整理、挖掘，然后将结果反馈给用户，同时这些IoT设备也能够接收来自用户和服务器的指令，做出相应的动作，例如开关电路、移动摄像头等。

安全研究人员眼中的IoT

接着我们聊一聊，安全研究人员眼中的IoT。第一印象，就是一座金矿，因为只要去挖，就一定有漏洞。造成目前IoT安全现状的原因有哪些呢？首先，IoT技术目前处于高速发展的阶段，安全基础设施建设的速度没有跟上，现在还处于发现漏洞，修补漏洞这种后知后觉的状态。

其次，由于IoT设备计算资源的限制，导致已有的安全机制很难平移到IoT上。例如一个家用摄像头，内存64MB，rom flash 32 MB, 很难将IDS、IPS和防火墙这些成熟的网络安全服务植入进去，例如一个规则库都要比整个内存还大。

今天我们就来关注一下IoT安全中非常重要的一环，root相关的安全问题。这里首先想和大家一起思考一下本次分享最关键的一个问题。

为什么要root

首先用户有root IoT设备的需求，因为能够突破限制，例如很多用户将品牌路由器刷固件，换成openwrt。其次开发人员也有需求，比如分析竞品的功能。需求最多的是安全研究人员，为了更好的研究IoT设备，需要获得系统的root权限，例如可以提取固件，进行静态分析，也能够获得系统的运行参数，例如Linux分区信息，启动参数等，甚至能够直接在设备上动态调试。这一切都是为了更早的发现漏洞，让IoT设备更安全。最后，需求最强烈的是黑产，因为有利益的原动力在支持，获得root权限后能够更方便的刷流量、薅羊毛、DDOS和挖矿。我们安全研究人员每天都在和黑产进行对抗，进行赛跑，就是为了比攻击者更早的发现漏洞，为大家提供一个更安全的环境。

Root方法

接着我们来聊一下，root IoT设备的方法。首先，需要对IoT设备的进行攻击建模，然后分析各个攻击面，最后从这些攻击面中找出薄弱环节。

如图所示，一个IoT设备模型可以分为硬件层、网络层、系统层、应用层这四大攻击面，每个攻击面中的任何微小的漏洞都有可能成为获得root权限的关键点。

硬件层

首先我们来看一下硬件层，硬件层安全其实是IoT安全与传统的软件安全、web安全差异最大的一层。因为在传统安全观念中，硬件层面的安全问题获得的关注度比较低，爆出的漏洞评分也不会很高，甚至某些漏洞提交要求中，明确要求非物理接触，需要远程攻击。但是，IoT安全不同于传统安全，物理层的安全非常重要。因为无论是从哪个途径获得了root权限，最后带来的安全威胁都是非常大的。

对于物理层的攻击，今天主要介绍两个方法，第一个是串口（UART）调试，第二个是SPI flash编程器。

对于串口调试，这是一个非常直接的获取IoT设备root权限的方法，只需要找到电路板中的一些关键词，例如VCC，3.3V，GND，RX，TX甚至直接有标明UART的接口，然后用万能表测量一下启动阶段的电压，找出接地和VCC，然后尝试一下RX，TX，一般就能确定串口接口，接着用远程终端连接串口，就能直接获得一个Linux shell，而且用户绝大多数情况就是root。串口调试，能够获得非常重要的运行时参数，例如MTD的分区表，Linux系统的启动参数，获得root权限后，能够读取/dev/mtdN这个设备文件，将IoT的rom数据读出，其中就包含了非常重要的固件数据。

对于SPI flash编程器，如果接触过嵌入式开发的朋友会非常熟悉。SPI flash编程器配合这个芯片夹子，绕过了CPU，直接针对IoT设备的nor flash进行读写，因为这个时候，设备都没有启动，所以任何在软件层面的安全措施都阻挡不了通过编程器读写固件的操作。在我实际研究过程中，大约20多款IoT设备都能够成功读写固件，只有一个sop16的nor flash芯片，只能读取，写入的时候出现乱码，造成设备变砖。通过编程器dump出的固件，可以用于后续的静态分析，找到root的方法。

这里友情提示，两种基于硬件的攻击手段都有可能损坏设备，尤其是烧录固件。幸亏IoT设备大多数都比较便宜，所以目前我还没有破产。

网络层

接着我们将注意力转移到网络层。在这一层中，既有传统安全的用武之地，又有IoT安全的特殊之处。

首先，大部分IoT设备使用了wifi，另外有一些使用了有线网络。那么，对于这些基于TCP/IP的设备，传统的渗透测试技术仍然能够发现大量的漏洞。

其次，IoT设备的联网协议，不只有TCP/IP。还会涉及蓝牙，3G和NB-IOT等无线协议。这里每一个新功能，新协议都会多多少少暴露出一些安全问题。这里有广阔的空间留给大家去探索。例如今年爆发的针对蓝牙的Blueborne[1]。

系统层

接着我们来看一下系统层有哪些安全问题。大部分IoT设备是一个安装了Linux的嵌入式设备。这里Linux系统出现的问题，都会被引入到IoT设备中。例如shellshock、dirtycow这些漏洞，会被恶意软件用来攻击IoT设备，获得root权限。另外一些系统设计的问题也会造成严重的后果。

这里和大家分享一个腾讯反病毒实验室提交给CNNVD的漏洞。

这个漏洞非常好理解，但是因为产品已经发布，而且有多个版本，修改的成本和难度可想而知会非常高。

应用层

最后我们来关注一下应用层的安全，应用层因为承载着非常多的需求，每种IoT的功能也不一样，很难有一些通用的攻击手段。这里需要掌握ARM和MIPS的逆向和动态调试技术才能更好的挖掘应用层的漏洞。这里用腾讯反病毒实验室报送给CNNVD的另一个漏洞来介绍一下应用层的安全分析方法。

至此，我们发现IoT的四大层面，物理层、网络层、系统层和应用层都有安全问题，都有可能导致攻击者获得root权限。那么，接下来，我们一起思考一下，当攻击者获得了IoT设备的root权限后，会引发多么严重的安全威胁呢。

安全威胁

从一名Linux程序员的角度来看，获得了root权限就是获得了至高无上的权利，这也就是本次分享上帝模式的由来。简单来说，如果是攻击者发动远程攻击，获得了IoT设备的root权限，那么除了攻击者抱不走你的设备，他可以在软件层面做任何事情。

相比传统的Linux安全，IoT安全面临的威胁会非常大。首先由于IoT计算能力的限制，IoT设备就无法抵御一些之前常见的网络攻击，更不要提0day攻击，导致针对IoT设备的蠕虫会在近些年大量爆发。其次，由于IoT特殊的使用场景，导致固件更新是一个成本非常高的操作。大量的用户不会主动更新固件，这就导致即使厂商针对漏洞进行了修补，由于用户没有及时更新固件，导致IoT设备仍然被已知漏洞入侵，获得root权限。最后，因为IoT设备得天独厚的运行环境，7*24小时不间断工作，实时接入互联网，甚至具备录音录像功能，一旦IoT设备被攻击者控制，就能够持续不断的进行恶意行为。

这些恶意行为包括传统的DDOS，就是将IoT设备作为肉鸡，对目标网站发起网络攻击，导致目标网站瘫痪。

其次是近年来流行的挖矿，因为IoT设备一般不会断电，电费也不是攻击者出，即使CPU运算能力十分有限，但是如果形成规模，也是攻击者青睐的一种恶意行为。

最后不要忽略，内网中IoT设备被攻击带来的新的威胁。传统安全防御看重的是外网和内网的边界防御，部署大量的防火墙，IDS和IPS御敌于千里之外。但是万万没有想到，城墙固若金汤，里面的IoT设备被攻击者入侵后，直接从内网发动攻击，去入侵同一网段下的设备。
这里想和大家分享另一个提交给CNNVD的漏洞，这个漏洞非常有意思。

缓解措施

前面讨论了IoT设备被root之后的安全威胁。接下来我们最后聊一聊，相应的缓解措施。目前IoT安全处于攻强守弱，很大程度是因为已有的缓解措施没有很好的利用，这些方法因为人为忽略，或者因为设备性能的问题，无法适配到IoT设备上。今天不作太多的发散，只是提出一些能够针对性的解决方案，用于缓解之前提到的一些漏洞。

首先关于固件校验，这里推荐使用数字签名技术，在发布固件的时候对固件进行签名，在升级，以及之后的每次运行时，进行签名验证。这就解决了CRC被攻击者替换的问题。TI提供了基于RSA的固件数字签名方案，大家可以深入了解。

其次关于密码生成的问题，生成随机密码是可行的，但是随机的种子需要特别的保护好，不要被攻击者获得。

最后是wifi功能无中生有的漏洞，这里最好通过物理手段对IoT功能进行限制，或者直接购买合适的硬件，来避免这种问题的发生。

总结

今天非常有幸能够大家分享关于IoT root权限相关的安全话题。不知大家有没有这种体会，IoT的安全发展也会符合一种自然规律，就是前期攻强守弱，中期焦灼，后期守强攻弱的规律。这种规律在整个互联网发展史上多次出现，例如整个Windows安全的进化，从win2000和Win XP可谓是软件安全的练兵场，到现在Win10每个漏洞都是价值千金。又如web安全的进化，从XSS，SQL 注入，经常是整站脱库，到现在WAF基本是标配。目前IoT安全还处于攻方非常强势的阶段，但是随着IoT安全事件的大量爆发和IoT厂商安全意识的提高，很快就会进入焦灼期，最后随着政策法规的执行和信息安全工作者的努力，整体IoT会朝更安全更可靠的方向发展。非常感谢大家。

参考资料

1.https://www.armis.com/blueborne/
2.https://wikidevi.com/wiki/Ralink_RT5350
3.Basic Secure Boot for OMAP-L138 C6748
4.http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201708-1472

> 注：本文根据大会主办方提供的速记整理而成，不代表CSDN观点。

2017看雪安全开发者峰会更多精彩内容：

- 2017看雪安全开发者峰会在京召开 共商网络安全保障之策
- 中国信息安全测评中心总工程师王军：用技术实现国家的网络强国梦
- 兴华永恒公司CSO仙果：Flash之殇—漏洞之王Flash Player的末路
- 中国婚博会PHP高级工程师、安全顾问汤青松：浅析Web安全编程
- 威胁猎人产品总监彭巍：业务安全发展趋势及对安全研发的挑战
- 启明星辰ADLab西南团队负责人王东：智能化的安全——设备&应用&ICS
- 自由Android安全研究员陈愉鑫：移动App灰色产业案例分析与防范
- 绿盟科技应急响应中心安全研究员邓永凯：那些年，你怎么写总会出现的漏洞
- 腾讯游戏安全高级工程师胡和君：定制化对抗——游戏反外挂的安全实践
- 绿盟科技网络安全攻防实验室安全研究员廖新喜：Java JSON 反序列化之殇
- 阿里安全IoT安全研究团队Leader谢君：如何黑掉无人机