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

原创

csdn业界要闻 于 2017-12-01 15:56:14 发布 800 收藏
文章标签： 安全 启明星辰 王东 看雪安全开发者峰会
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/csdn_bang/article/details/80133053
版权

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。

IoT现在为什么这么火？究其原因还是与它所处的发展阶段有关，这同最初移动端刚兴起时如出一辙，即相关的防护措施没跟上，机会自然也就多了。很大一部分为智能设备做开发的程序员往往只关注如何实现功能，而忽略了其中的安全问题，对安全研究者来说会发现世界原来如此简单。此外，工控安全问题也日渐凸显了出来，一旦这些基础设施出了事情，那么所带来的后果往往是灾难性的，例如之前的乌克兰电网被黑事件。启明星辰ADLab西南团队负责人王东在主题演讲中为我们带来有关智能化安全的探讨，相信各位对所处的这个万物智能世界中存在的安全问题有更深刻的认识。

启明星辰ADLab西南团队负责人王东

> 王东，启明星辰ADLab西南团队负责人，十年网络安全研究经验，曾任职于电子科技大学。2008年开始网络安全研究，擅长windows内核安全对抗、恶意代码分析、主动防御、rootkit/antirootkit、软件调试和漏洞分析。2016年加入启明星辰，开始物联网安全研究和工业控制系统安全研究。目前专注于基础应用组件、智能设备、智能应用和电力工业控制系统的漏洞挖掘，向Imagemagick、Graphicmagick、GNU binutils、Advantech、ICS-CERT、Cisco、汽车电子、家电穿戴、工业控制等提交了多个漏洞。

以下为演讲速记：

王东：大家好，我是来自启明星辰的王东，同时也是ADLab西南团队的负责人。今天给大家分享的议题是智能化的安全，涉及到智能设备、智能应用和ICS。我们对智能化的安全很感兴趣，作为一个安全研究人员，以前更多是找别人的问题，发现别人的安全风险，如今安全人员自己也面临安全风险了，因为我们无法抗拒这些智能设备应用带来的便利。

2008年开始，我开始在电子科大做安全研究，那时安全软件的主动防御很火。2016年加入启明星辰做安全研究，2017年跟东方电气成立工控信息安全联合实验室做ICS的安全研究，主要工作是漏洞挖掘。整个智能化是由IOT推动的，IOT带来了很多概念：万物互联，万物智能，万物智慧，现在已经上升到这个智慧地球的概念了。比如，智能冰箱/智能汽车/智慧医疗，他们给我带来了一些智能化的功能，解决了一些问题。但是，智能化并没有让安全变得智能，反而把传统信息化的安全问题全部保留了下来。比如说汽车，以前是没有联网功能的，要进行攻击只能物理接触，现在汽车联网了智能了，黑客也就可以远程攻击了，这是腾讯安全团队对特拉斯汽车的远程攻击。卡巴斯基的统计表明，IOT的安全威胁数量直线上升。除了数量上的变化，我们认为还有一些本质上的改变，这个本质上的改变我归结为Security到Safety。这里的Safety指的是一个人的物理特性，一旦被攻击就是永久不可恢复。

传统Security带来的损失都是逻辑性的，都是可以恢复的，因为在本质上它不是一个物理问题，只是一个逻辑量的表征。就像小区旁边的树一样，被台风刮掉对于你个人来说没有物理影响，只需要给一点钱让物业帮你修复就行了。传统Security的补救比较简单，一般只需要做一些备份和恢复（大部分厂商都会做），清除恶意代码和还原数据库。传统Security的补救成效也很明显，备份恢复可以恢复受攻击的业务，给客户赔礼道歉再补偿点经济损失就万事大吉了。这些安全事故慢慢就会被遗忘掉，比如当年删库的某站，数据恢复后这个网站的业务还是一如既往，只是抽风了一阵而已。总结起来，传统Security漏洞可以做到更改任何逻辑量，在数字世界中发起任意攻击，但就是无法穿透”叹息之墙”危害到人的物理本体，即使他拥有类似五小强的越级挑战能力。但是”叹息之墙”是可以打破的，智能化就是破墙的太阳般光芒。比如说智能冰箱，通过安全漏洞控制温度，可以让食物变质吃坏人，或者让一些需要恒温的医疗用品产生质变，给人用了没有效果或者产生医疗事故。又如智能汽车，远程攻击使高速熄火，伤人十分危险。针对工业控制系统，比如说像火力发电，是要烧蒸汽来带动这个汽轮机的旋转，如果温控被攻击出事了，炸的不是一口简单的小锅，那锅非常大，一旦炸了这个厂里面的人也会被炸飞。所以，智能化可以轻易将逻辑世界的Security问题可以演变为物理世界的Safety问题，我们接下来看例子。

首先，我们来看智能设备。智能设备主要是这么几类：家电、穿戴和安防，其他我认为都是一些拿来玩的，没有多大的作用。这是智能设备的架构，比如这个WIFI空调，设备跟云端通常会用TCP/IP协议；APP跟云端一般也是用TCP/IP，有可能是WIFI也有可能是移动网络；设备跟云端之间比较复杂，有可能用TCP/IP也有可能用BLE。

在智能设备中，有一种设备如果不安全就特别不安全，那就是锁。如果这个锁出问题，你晚上睡的很安心，但是第二天一起来你可能就会发现这个世界已经变了。我们研究了两代智锁，第一代就是WIFI锁，他可以用遥控滚动码方式控制这个锁。这个产品经理很聪明，IOT一来他就搭上了智能化的车，开发一个APP，家里都有路由器，配上同时具备滚动码和TCP/IP的设备，这个锁可以快速变为一个智能锁的。针对TCP/IP，我们可以用很多的工具做流量数据分析。使用WIFI协议做智能设备通常都是为了短平快，我们只需要wireshark以及tcpdomp以及路由器就可以做这个设备的网络数据获取和分析。这个锁，我们抓了这个开关门的数据，我们发现这个数据非常的简单，64个字节，并且还用的是广播，还用UDP。这个设备的协议交互非常简单，我让你开门就开门，我让你关门你就关门。我们想知道这里面有没有重放的问题，我们抓取连续开门报文，发现三次报文是非常的相似的，差异是特别小的，差异很有规律，一看就很典型，具有重放的可能性特别大，我们就用pcap抓包然后重放，锁就这么开了。说个题外话，WIFI情况下通常抓包需要把整个网络控制了，如果你攻击别人，即使接入了别人WIFI网络，如果不采用ARP欺骗这种链接劫持办法，也是没法抓取其它设备的网络数据的。

但是，这个设备有一个致命的错误，它用了广播，完全不需要劫持。我们很快把这个锁的交互协议分析出来，最核心是三个变量：序列号、门开关状态，控制key。整个报文64个字节，没有加密，我不知道是不是开发人员想忽悠用户，他做了异或加密。如果想开这个锁，必须提供正确的SN和key，也就是说Key以及Sn不对，这个锁就会拒绝执行命令。看完协议结构，我们发现是完全可以破解的，拿到一个广播报文，就可以把这个Key以及SN都可以破开，这里面SN只需要做一次异或计算就可以拿到。Key会复杂一点，因为key通过key2方式再做了异或。用两个非常简单的公式可以把这个算出来了。如果说我们从来没有办法进入这个锁的局域网，比如说这个锁是放在你家里，你在北京我在成都，我怎么样可以攻击你这个锁呢？我们可以看一下它的特性，他可以帮助我们做这个事情。先抓一下广域网的报文，通过手机抓到通过电信移动网络的报文，发现这个报文跟局域网条件下的报文没有任何的改变。首先，锁的协议我们已知道；其次是SN，我们发现这个序号是可预测的，信息安全里面所有安全都来自于不可预测，如果预测的话也就没有什么安全性了；再次，锁的Key绝大多数都是654321，因此锁从安装到使用，没有任何一个过程会有Key的影子，绝大用户都会是一键绑定和使用，导致大部分密钥都会是这个样子。也即是说，你在家里不停的修改sn，然后用654321，就可以开关很多锁。

来送一个惊喜，前面说我们需要抓包和分析，这个还是有点复杂，我们来一个小孩子都可以玩的。一部手机，下载APP，到目标门口做一次蹭网，打开APP做一次绑定，然后可以回家了，从此可以在任何地方可以控制这个锁了，整个绑定没有任何交互过程，整个绑定机制是不需要用户介入的。蹭网也很简单，我们都知道有一个神器可以让你蹭网的。

我们再来看修复方法，最直接就是采用安全交互协议，不过这没啥意义。人家用Wifi不就是想开发快，你用一个安全协议还不如用蓝牙。怎么样改进可以带病的工作，任何防御都不是绝对的，看看怎么样提高攻击成本。

重放攻击，这个是因为协议交互是无状态导致的，锁侧不能区分这次交互以及上次的区别。APP在发开关门之前执行一个额外的命令，从锁端获得一个随机数ramdom。获得之后需要把这个random带过去，缩侧可以进行校验，这样每次都不一样，抓包重放也没用。

默认密钥，它是一个界面交互的问题，我们改变这个交互的设计就可以了，强制加入密钥修改，连锁都不用重新改造。

信息泄露，这个非常严重，首先限制广播，广播应该只在设备绑定的初始阶段用广播，或者说你想搜索控制器的时候可以用广播，广播不能附带额外的信息。其次限制SN泄露，SN基于GUID的风格就可以黑客很难做猜测了；还有一个限制密钥，这个里面直接把密钥通过两轮异或的方式来做编码，其实没有什么用，我们前面讲加的一个状态可以用共享密钥加密这个随机数，可以限制这个密钥的泄露。 当然了，不仅仅是这个智能锁，我们在空调以及插座和冰箱里面都有这个问题。

总结下来是：WIFI主网本身不提供安全性，开发出来确实简单，调试也很简单，但是这个攻击者其实也是非常简单的。

智能设备除了使用WIFI还有这个蓝牙，其实蓝牙很早就有了，但是蓝牙在早期没有什么作用，功耗无优势，还有强制配对。当然了，开发也很麻烦，基于bsd-socket的风格。低功耗就好玩了，能耗非常明显，关键是它的开发很简单，配对方式比较灵活。BLE也是强制配对，只不过支持不需要通过第二信道传输这个配对密钥。BLE的开发是很简单，基于GATT，GATT开发非常简单。还有一个高带宽也不是总需要，互联网访问不是总需要的。比如这里有两款锁，一款是比较便宜的BLE锁，一款是很贵的BLE锁。相比Wifi，ble自带安全光环。点对点通讯，不需要中间设备，跳频传输，信道加密。导致抓包很麻烦，通常要三个广播一起抓，关键抓包设备还不便宜。这样会导致直接网络层搞就很麻烦，但是我们不一定要直接从网络层来突破，比如GATT。

Gatt开发很简单，那到底有多简单呢，只能说简单是到让你疯狂。所有的Gatt分为Gatt服务，所谓的服务是在GATT管理器中，服务也有很多属性，属性对应存取数据。数据有各种各种的描述，每一个描述都是数据的某个的维度表达，比如回调通知描述…特别像COM开发，通过UUID来定位，不需要关注底层的连接。开发代码很简单，比如这个代码，非常简答。

第一款的不联网的BLE锁怎么样攻掉？这个锁是不联网的，我们只需要Gatt里面找UUID，再回溯就可以看到里面的加密是什么样子，再展开就可以看到跟用户相关的提示，还没有MAC绑定机制，我们只需要写一个假的APP，调用GATT接口，就可以把这个锁打开。第二款的BLE设备是需要连网的，这个锁超级贵。这个锁必须手机号注册，必须联网，必须联网才能开门。开门本身不用WIFI，但是连网才可以得到这个密钥，这个锁可以授权给别人开门，但是也得联网。不仅仅是这个锁的一般信息，核心的控制信息都是存储在这个云上，直接把这个云端搞定就可以打开锁了。

我们深入分析发现，这个锁里面有别的东西。这个锁里面采用这个域名信息跟这个厂商品牌完全没有任何关系，我们做了一系列的分析，发现它是另外一个知名锁厂商的域名，这个锁还供应了好几家。这其实也是一个比较经典的问题，只是…硬件代工了，软件代工了，连用户数据跟运营也都代工了…。这些不同厂商锁的用户数据都在一个地方，哪一家公司出的问题会被一锅端。一些简单的修复值得去做，加固一定要做，密钥交换也可以做一些事情。绑定MAC。

前面说的是设备，我们可以看一下智能应用。智能应用现在有很多了，有单车、汽车，我最喜欢的是医疗。有两个经典问题，前面婚博会的专家已经讲了这个帐号安全以及数据泄露，这是非常有用的。帐号安全来自没有限制登陆尝试，特别是账号找回的尝试，也就是说只要破解了验证码就可以了。但是主流的验证码的运算空间是相当有限，4位空间，一般是一万次就够了，100个/秒的尝试则需要不到2分钟。6位一般是用于金融证券或者互联网公司出品的应用。

有的时候账号找回看上去没有那么直接，比如会做一个签名，但是签名没有什么用因为它是固定化了；比如加密，加密其实也没有什么用，加密也是在APP端做固化了；比如用HTTPS，一开始我们也比较头痛，但是我们发现可能会存在着这个证书校验不严格，通过这种方式我们把某合资汽车直接开走。

我们也来送惊喜：有时候找回的时候直接把验证码给你看，既通过电信网的反馈给你，也同时通过这个网络把这个验证码反馈给你，我认为肯定是程序员忘记调试开关了，你说呢。

前面是帐号安全，再看数据泄露，这是典型的平级越权，这非常多，无论是大公司还是小公司都有这样的问题。有合资汽车以及国产汽车都有这个问题，还有非常有名的一些医院。这些非常好玩，最可怕的是汽车，可以用你的身份开车或者把你的车开走，但是一旦撞了人，这个锅你是很难逃得掉的。HTTPS的方法一定要用对，用不对除了增加计算开销成本没有任何安全收益。

最后分享下工控，这一块我们是跟东气联合研究，2017年成立了联合实验室，跟他们一起研究原因很简单，很多工业控制我们不懂，比如说核电。我们的研究涵盖到这些协议以及设备，现在已经披露的大部分ICS漏洞主要是上位机的漏洞，因为这上面这些比较好做。我们的行业主要做电力行业，我们涉及到火电/水电/核电/气电/风电/光伏，光伏主要是面向个人。研究涉及到输电配电以及供电三个环节。现在大部分工控研究主要是做信息侧，这一块很好做，有管理系统，基于WEB的HMI/SCADA、基于Windows/LINUX的上位机软件、和安卓应用也在开始应用。研究这些有成熟的工具，所以也是比较好做的。信息侧问题非常多，比如弱口令。我们安全专业人员认为这是非常可怕，但是工控专业人员却认为这个东西从来都不可怕，他们认为强密码才可怕，我觉得这是行业的认知差异。工控生产环境中的设备需要有人执守或者维护的，使用强密码容易导致再紧急处理时失误，在争分夺秒的时候大小写和特殊字符都可能导致处理不及时而触发破坏性事故，所示即使用了强密码也会直接以某种方式呈现出来。我们前期发现了大量工控信息侧的安全漏洞。

我们的研究主要还是集中在设备侧，这是网上可以买到控制器设备，但在实际环境不是这个样子，而是这个样子，这还是搭到一半的样子。要分析控制器设备的安全漏洞，需要注意一些坑：比如不使用安全协议，设备性能很差，没有任何调试的支持。

对于本身是不安全的协议，有什么安全问题，这一开始非常让我们头疼。从安全角度看，只是需要理解这个PLC中线圈和寄存器的物理意义，就可以随意控制设备炸掉还是不炸。

ICS有一个特性是对时间非常敏感，通常IT系统讲的是最小延迟时间或者平均延迟时间，工控里面讲最大延迟时间，比如说电力的协议，周期只有4毫秒，超过4毫秒是丢包，再超过4毫秒这个会话就会被人断开了，任何影响这个实时性的问题都可能导致安全问题。

另外，ICS设备的性能太低，测试稍不注意就会让测试目标拒绝服务。并且ICS设备大多没有调试接口，也没有屏显，测试时如何判定设备是否发生了异常也是一件难事。控制器上的LED灯的颜色可以反馈部分异常，比如通常红色表示有问题，但我们还是很难知道红灯的具体含义，问供应商说不知道，问厂商不理。我们最后采取固件分析这条道来分析控制器，发现有很多的安全问题：总的来说就是，工控开发很封闭，写代码的人都是假定所有参与方都是良民的。比如针对某款电力控制器，我们发现了一系列的安全缺陷，抢占连接、后门口令、内存消耗、拒绝服务。比如这个设备的后门口令，我们告诉厂商，厂商先否认后门，说不存在，然后又告诉我们这个口令是开发人员用，不会对用户开放。难道不对用户开放的口令，就是安全的口令？这是我们发现最复杂的一个漏洞，是多任务条件下面的交互时序没有考虑异常条件，导致认证过程发生拒绝服务，从而拒绝合法的认证请求。

工控漏洞的修复过程非常复杂，我们已经知道控制器的漏洞怎么修复，但是我们没法修复，只能依靠厂商。除此外，生产部门告诉我们，18个月之后再补。因为我们这个电力设备的停机检修是排了计划表的，我们不能想停就停，电网调度侧可不是你想接入就接入的，也不是想断开就断开的，一切都得按计划行事。

谢谢大家！

> 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
- 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
- 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
- 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