关于看雪安全峰会--web小萌新的内心独白

原创

itest_2016 于 2017-11-27 10:08:45 发布 440 收藏 1
分类专栏： 安全测试 文章标签： 安全
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/itest_2016/article/details/78642185
版权


安全测试 专栏收录该内容
22 篇文章 1 订阅
订阅专栏

这次的看雪安全峰会是看雪举办的第一届安全峰会，看雪作为国内二进制的黄埔军校，已经走过了17个年头，看雪培养了大批的安全人才，所以这次峰会可以说是安全圈特别是二进制圈大佬们的分享、聚会。作为一个web小萌新非常有幸可以参加第一届峰会，简单写一下参会的一些感受。

首先可以肯定的是，这次会议的质量还是很高的，爆了3个0day和1个1day，其中包括一个win10的0day。议题的范围包括：安全编程、软件安全测试、智能设备安全、物联网安全、车联网安全、漏洞挖掘、APP加密与解密、系统安全等。还有一个看雪坛主及老会员座谈和下午的嘉宾座谈。

第一个议题是flash漏洞攻防，主讲人是看雪的二进制板块版主：仙果。仙果早有耳闻，第一眼看到他的感觉是：“如此年轻”，然而他已经在二进制这个领域拥有了10年+的工作经验。在这个议题中展示了一个通过flash的漏洞可以完成目标机器的收集，而这一系列只需要你打开一个URL就可以实现，即使你打了所有操作系统的补丁。他当时演示的是收集计算机的软件安装信息和操作系统信息，这些信息在apt攻击中是非常重要的，当然你也可以利用这个漏洞去做其他的事情。

Flash使用的范围很广，即使慢慢的很多大厂都开始慢慢抛弃flash，但是flash基本还是每台计算机的必备组件。想想在内网中，如果一个访问量很大的内部门户被攻击者嵌入了flash的exp那么基本整个内网就暴露给攻击者了，攻击者可以收集所有他需要的信息为后面的进一步渗透做准备，确实攻击成功需要flash版本存在漏洞，但是又有多少人会去升级他的flash版本呢？还有在office或者pdf中也可以嵌入flash，flash的漏洞也是可以触发的。作为防守方来说真的很难去防御，即使你可以保证所有内网系统都不会被攻击者嵌入恶意代码但是攻击者仍然可以利用钓鱼邮件发送带有恶意代码的pdf或者office来进行攻击。正式因为flash使用的范围如此之广所以才让防守方如此被动，基本很难防御。这也是为什么flash的漏洞在apt中如此受欢迎的原因，在前几年hacking team泄露的数据中就有好几个flash的0day，flash也就是在那一年荣登漏洞之王。

第二个议题呢是web安全编程，因为主讲人是开发所以你懂得。大概介绍了：SQL注入、xss、CSRF、越权、支付漏洞。然后分别讲了一下这个漏洞是怎么回事，怎么利用，怎么修复。

我比较关心的是支付漏洞，讲到支付那一块的时候主要介绍了两个比较典型的支付漏洞：一个是通过修改商品的价格还有一个是通过更改商品的数量。在修复方案中他提出了要对价格做后端校验，同时对数量不能为负，限制低价、免费购买商品。其实他这个修复方案还是有问题的，如果数量为小数的时候还是可以被绕过，导致损失。还有支付漏洞根据不同的业务场景可能会有不同的安全问题也就是有不同的安全修复方案。常见的除了更改商品的价格和数量之外，还有更改运费、更改数量为小数、优惠券重复使用、条件竞争导致的支付风险、优惠折扣导致的安全风险等等。虽然这个议题从安全的角度来看很简单，但是主讲人作为一个安全开发人员已经算是知晓web安全中很多常见的安全漏洞了并且对每种漏洞的修复非常熟悉.

第三个议题是业务安全相关的内容，其实我对这个是非常感兴趣的，但是因为可能是作者的定位是讲一个概况，所以讲了一下历史然后举了一些例子。以某鹏特饮为例讲了一下薅羊毛。某鹏特饮会在瓶盖上打一个二维码然后你去扫码关注公众号可以兑换几毛钱到几块钱甚至几十块钱不等，黑产团队会回收这种瓶盖然后批量操作领取“羊毛”。

又举了某OFO的例子，每天补贴的100多万被黑产刷单团队拿走了30%以上。然后该OFO在花掉大概4000万人民币之后彻底宣告失败，我们肯定不能说因为安全问题导致这个公司的失败，但是安全是作为其中的重要一环。同时又介绍了打码平台和情报的获取，听完之后还是觉得黑产团队太会玩。有句话怎么说的，他们（黑产）有着比防守方更多的人力、更多资源、他们比防守方更聪明，这样一帮人如果盯着你你害不害怕？同时，还提到了一个概念：攻守方的信息不对称。往往是被黑了自己还不知道。

第四个议题是关于win10的一个0day，主讲人是lu0，中国第一代黑客了很有气场的一个人。Tk说当初从他的博客学习了不少东西，scz又怂恿lu0去更新停更多年的博客（http://www.lu0s0.com/）lu0没有给出具体的利用场景只是讲了一下这个问题，主要是涉及到win10的Linux子系统，因为Linux是大小写敏感而win是不敏感的，然后win把Linux这个特性引过来的时候在内核层做了很多更改以便支持，但是windows这么一大动的话就带来了很多安全问题。两个py文件，一个叫a.py一个叫A.py，这样两个文件在Windows和Windows下的Linux子系统运行的结果竟然是不一样的。

因为我对系统漏洞利用这一块完全没了解过所以我想不出有什么好用的利用场景。会后问lu0你们平时是怎么挖系统漏洞的，他回答说：“时间久了 哪里会出问题不用测就知道了”。感觉挖0day就是随手的事，当然现在Windows下的高危漏洞还是比较难挖的，比如：远程代码执行。他说：Windows没一次大的变动就是那些搞攻击的人的机会，因为肯定会出现问题。延伸到我们的web安全其实也是一样，web系统迭代好几个版本之后即使经过安全测试还是存在很大安全风险，这也是为什么我们进行全量回归的原因之一，也深深感觉到要想真正的保障一个产品的安全都是很不简单的事情。

第五个、第七个和第十二个议题都是关于IOT安全方面的一些知识，最后的嘉宾座谈也是聊得IOT安全方面的点。当前各个乙方对于IOT的安全都在进行研究，并且大家的感觉就是当前这些物联网设备的安全性极差，基本上是一挖一个准。360的谭总是这么说的：在物联网设备安全这方面他们是战无不胜，目前他们接触的所有设备都是有安全问题的。可能是因为IOT这种形式的新颖大家觉得一般人是接触不到设备的系统层的，但是事实情况并不是如此，无论是云端、系统层、应用层、网络层每一个环节都是没有经过安全设计都是存在安全风险的。

这一块比较有意思的是两个：1、是ADLab的一个大牛提的工控设备安全里面的一个例子——弱口令问题。在工控设备中有些是对外网开放的，有些是不对外开放的，工控系统中存在大量的弱口令问题，但是和传统的弱口令不一样的是工控的弱口令很多是无法更改的，如果改了之后密码复杂操作员在遇到紧急情况下万一忘记密码或者因为输入时间过长导致爆炸等事件会直接危及生命财产。这让我比较有感触，在公司里面即使弱口令不会危及生命安全也还是大量存在更不用说工控设备这种特殊的场景了。2、还有一个是360的谭总提的，他们挖了很多很多的IOT设备的漏洞，在挖洞的过程中他们其实是花费了大量的人力成本的，但是如果厂家不买单或者不承认那么其实你这个工作投入是收不回来的，对于企业来说这肯定是不允许的。

第六个议题是关于移动APP灰色产业的，主讲人看上去年级很小但是技术确实不一般。以小米商城为例讲了一下，大概思路是熟悉正常的业务流程---抓包分析---编写自动化工具---抢便宜的商品---倒卖。同时还举了一些针对不同的厂商采用的加固方案攻击者是怎么针对的去破解的。以往我们一直认为安卓APP是很容易被反编译的，那么怎么办呢？第一个我们是做代码混淆，如果安全需求高那么就把关键代码写进so这样你就无法分析了吧？以前我也是这么认为的，但是这个主讲人从攻击者的角度让我对安卓保护又有了新的认识，我们总是自认为这样就很安全了其实我们都是单纯的从我们的角度去考虑，完全没有去深入了解攻击者的套路，他们到底是怎么做的。

例如，你把关键代码写进so，那么你有没有考虑过攻击者真的需要去破解这个so吗？他如果直接调用的话是不是也能实现攻击者的需求？还有so只是ELF，他是可以被逆向分析的。代码混淆也是一样的道理。还有一种方案是加壳，有些壳很容易被脱掉，加了等于没加，还有些壳确实很难被脱掉，但是呢很不好意思如果你不知道攻击者的套路你把壳加错地方了保护了不需要保护的比如一些dex，需要保护的重要位置你反而没有保护。深刻体会到了什么叫做——攻防是对立统一的这句话了。如果你不了解攻击者的套路，那么很可能你做的一些安全措施是一厢情愿。

第八个和第十个议题是关于web安全这块的，两位讲师都是绿盟的。第八个议题是“那些年，你怎么写总会出现的漏洞”这个议题由浅入深的讲解了web安全里面的一些常见漏洞，贴了很多代码，听的时候有种现在做代码审计并且直接bypass的感觉，很好。听完这个议题我觉得不管是后期做渗透测试还是做安全测试对代码审计还有bypass这一块我们还是需要开始去积累，还是有很多东西值得我们去学习。

第十一个议题是“一石多鸟——击溃全线移动平台浏览器”，emm这个议题我没听，当时去找了下基友请教一下漏洞挖掘和恶意软件分析方面的知识和学习方式。第十二个议题是关于无人机的，讲师讲了很多硬件、协议、电路，反正我是一个没听懂=——=

最后，非常感谢看雪科技创始人段院长的赠票，还有非常感谢领导能够给我这次出去学习、交流的机会！