看雪学院将举办《安全开发者峰会》，有这11个安全议题

转载

weixin_34233421 于 2017-10-27 14:11:00 发布 142 收藏
文章标签： 网络 web安全 json
原文链接：https://yq.aliyun.com/articles/231191

报道的国内的特大侵犯公民个人信息案，某部委医疗服务信息系统遭“黑客”入侵，超过7亿条公民信息遭泄露，还是美国信用评估机构遭黑客入侵，泄露半数美国消费者重要信息，比如姓名、出生日期、家庭地址、社会安全号 SSN、驾驶执照 ID、信用卡信息……

安全问题已不容忽视，对企业负责人或研发人员而言，安全事故频发无疑是一场灾难。而解决安全问题的根本在于做到安全开发。安全设计应在一开始就作为项目开发的一部分来考虑，列入项目计划和开发成本中，并在保护强度、成本、易用性之间进行折衷考虑，选择一个合适的平衡点。

基于此，看雪学院将于11月18日在北京举行2017《安全开发者峰会》,峰会聚焦“安全开发”，旨在以“防”为基准，安全开发为主旨，引导广大企业和开发者关注移动、智能设备、物联网等领域的安全，提高开发和安全技巧，创造出更安全的产品。

会议时间：2017年11月18号

会议地点：北京朝阳区悠唐皇冠假日酒店

峰会嘉宾

段钢：看雪科技创始人及CEO，国内内信息安全领域具有广泛知名度和影响力的安全网站看雪学院(www.kanxue.com)的创始人和运营管理者，信息安全领域的知名作者，所著图书多次获奖。长期致力于信息安全技术研究，对当前安全技术的发展有深入思考。2016年创建上海看雪科技有限公司，致力于PC、移动、物联网安全研究及逆向工程相关的发展，为企业提供智能设备的安全测试等产品和服务。

王军：中国信息安全测评中心总工程师

谈剑峰：现任上海市信息安全行业协会会长，中国中小企业协会副会长，全国信息安全标准化技术委员会委员。上海众人网络安全技术有限公司（简称：众人科技）创始人、董事长，是信息安全领域的资深专家。中国网络信息安全产业新一代领军人物。

谭晓生：360公司CTO兼VP、CPO（首席隐私官），前myspace中国CTO。现任奇虎360副总裁兼首席隐私官（CPO），负责公司网站技术、技术运维、数据分析与挖掘等工作。

季昕华：中国首代黑客代表人物，UCloud创始人之一，现任UCloud首席执行官。

潘柱廷：北京启明星辰信息技术有限公司首席战略官，主要负责公司技术部门管理及公司经营战略的规划。

马杰：百度安全事业部总经理，原安全宝创始人兼CEO，亚州反病毒研究者组织（AVAR）理事。

龚蔚：ID Goodwell，中国黑客教父，早期十大黑客之一，绿色兵团创始人，COG发起人，1999年创立了上海绿盟信息技术有限公司。先任WiFi万能钥匙CSO。

TK（于旸）：江湖外号妇科圣手，腾讯玄武实验室掌门人，安全焦点核心成员，全球最为知名的几位白帽子之一，对Windows 操作系统漏洞方面研究非常深入。

陈彪：现任梆梆安全CTO。曾任职于Intel、Sun等国际知名公司，专注于虚拟机、移动应用保护等领域，获得多项全球和国家发明专利。

高春辉：ID Polo 高，DOS 时代的 Cracker，中国个人站长第一人，成功创办过手机之家、ECShop、IPIP.net 等项目，连续创业的互联网老将，被圈内誉为中国互联网活化石。

韩争光（TB）：上海犇众信息技术有限公司创始人 & CEO，国际顶级安全团队盘古核心。

董志强：“七剑”之一的腾讯云鼎实验室掌门人 Killer 。

袁仁广（袁哥）：腾讯湛泸实验室袁哥，2008北京奥运会特聘信息安全专家，中国国家信息安全漏洞库特聘专家。

段海新：清华大学网络科学与网络空间研究院，网络与信息安全实验室主任。

彭瀛：爱加密的创始人及董事长。

谭万里：硬土壳安全创始人，新安全生态实践者

范俊伟：几维安全联合创始人、CEO

陆麟：ID：lu0，早期十大黑客之一，Windows 内核专家，驱动专家。

杨冀龙：ID老杨，早期十大黑客之一，安全焦点创始人，《网络渗透技术》作者，知道创宇公司副总、CTO，著名安全组织XFOCUS的核心成员。

峰会日程

9:00	大会致辞	王军	中国信息安全测评中心总工程师
9:15- 9:45	业务安全发展趋势及对安全研发的挑战	毕裕	威胁猎人创始人兼 CEO
9:45-10:15	java json 反序列化之殇	廖新喜	绿盟科技网络安全攻防实验室安全研究员
10:45-11:15	一石多鸟——击溃全线移动平台浏览器	roysue	看雪 iOS 小组组长 roysue
11:15-11:45	Flash 之殇 - 漏洞之王 Flash Player 的末路	仙果	看雪论坛【二进制漏洞】版主
11:45-12:00	抽奖		
12:00	午餐		
13:30-14:00	一种以 IOT 漏洞对抗 IOT 僵尸网络的方法	王启泽	启明星辰 ADLab 安全研究员
14:00-14:30	Windows 10 新子系统*新挑战	陆麟	ID：lu0，早期十大黑客之一，Windows 内核专家，驱动专家，上海高重信息科技有限公司 CIO
14:30-15:00	移动 APP 灰色产业案例分析与防范	无名侠	看雪会员
15:00-15:30	游戏外挂对抗的安全实践	胡和君	
15:30-16:00	开启 IoT 设备的上帝模式	杨经宇	腾讯反病毒实验室高级工程师
16:00-16:30	浅析 WEB 安全编程	汤青松	婚博会 PHP 高级工程师
16:30-17:00	那些年，你怎么写总会出现的漏洞	邓永凯	
17:00-17:40	嘉宾座谈		
17:40-18:00	看雪 CTF2017 颁奖典礼		
18:00-18:10	抽奖		
18:00	会议结束		

演讲者及议题介绍

议题1：业务安全发展趋势及对安全研发的挑战

议题概要：

业务安全在2012年之前还只是以阿里、腾讯及携程等为主的局部战场，近些年随着垂直电商、社交、移动游戏和O2O等领域的快速发展，业务安全及反欺诈被更多的视线关注，但多数厂商并没有像阿里和腾讯一样与黑产相爱相杀一起成长，面对黑产的攻击会一时无措。作为防守方，除了对抗技术外，也要增强对黑产的认知，了解当前在一些业务核心问题上的对抗阶段和思路。

从我们接触的多个案例表明多数甲方在业务安全及反欺诈上很被动的主要原因是缺乏对黑产的认知，这个议题会从国内业务安全发展过程来帮助甲方研发梳理业务安全对抗思路并对当前主要的一些风险场景具体说明。

演讲嘉宾介绍：

毕裕，威胁猎人创始人兼CEO。曾任职于腾讯和猎豹移动，2011年起负责腾讯相关黑产研究及对抗。2015年起在台北负责猎豹移动海外安全团队，负责海外移动安全的相关产业链研究及打击。2016年与团队创业，专注互联网黑产研究及业务安全防护。

议题2：java json反序列化之殇

议题概要：

随着REST API的流行，JSON的使用也越来越多，但是其中存在的安全问题却不容忽视，特别是由于反序列化导致的远程代码执行更是威力十足。在这次演讲中，主要阐述java json库的反序列化特性导致的RCE。首先会介绍Gson，Jackson和Fastjson这三个最常用的JSON序列化库的序列化和反序列的操作，接着分析其安全机制，从其安全机制上发现哪些潜在的安全漏洞。然后会公布一些未公开的反序列化的的payload（以Fastjson举例说明），当然也可能包括0day，并且会对这些payload分类解读，从field类型，property类型的触发机制加以概括归纳。最后会从开发，运维的角度来防御这类安全问题。

本议题可以让更多的开发者理解Java反序列化漏洞，做好安全编码，做好安全防护，减少被黑客骚扰的机会。

演讲嘉宾介绍：

廖新喜(xxlegend)，绿盟科技网络安全攻防实验室安全研究员，擅长代码审计，Web漏洞挖掘，拥有丰富的代码审计经验，曾在Pycon 2015 China大会上分享Python安全编码。安全行业从业六年，做过三年开发，先后担任绿盟科技极光扫描器的开发和开发代表，目前专注于Web漏洞挖掘，Java反序列化漏洞挖掘，给RedHat，Amazon提交多份漏洞报告。2016年网络安全周接受央视专访。

议题3： 一石多鸟——击溃全线移动平台浏览器

议题概要：

浏览器早已成为我们日常生活中不可或缺的一部分，这种攻击可以造成大范围的用户信息泄露，不仅局限于网站上手机上填写的姓名电话、信用卡银行卡等用户基础信息，更包括了我们日常生活中频繁使用的淘宝购物，“扫一扫”、“公众号”、“小程序”、共享单车H5、饿了么H5等等贴近生活的一线App，所有App均不同程度的使用了某种Webview的实现。一旦被意图不轨者掌握并利用，后果非常严重。针对应用层的攻击频次连年增长，攻击方式更加多元，而越来越多企业的业务又依靠互联网来实现，防止应用层安全失守成为企业不可回避的问题，做好应用层安全也成为厂商和企业不可或缺乃至不可推卸的责任。

演讲嘉宾介绍：

Roysue，看雪iOS板块版主，iOS独立安全研究员，《iOS黑客养成笔记：数据挖掘与提权基础》电子工业出版社今年11月出版，《JavaScript内核逆向与爆破指南》正在撰写中。

议题4：Flash之殇 - 漏洞之王 Flash Player的末路

议题概要：

Flash Player 作为最受欢迎的多媒体软件，一直以来都受到大众的软件，遥想当年的闪客精灵时代，何其风光。自从Flash Player荣登"漏洞之王"的宝座之后，Flash 就成了"千夫所指"的对象，本议题就以Flash player为题，为大家带来Flash Player漏洞利用史，展现Flash 漏洞利用技术和攻防对抗技巧。

演讲嘉宾介绍：

仙果，十年以上的网络安全从业经验，致力于网络攻防对抗技术研究，专注软件漏洞的分析与利用，看雪论坛二进制漏洞版主。

议题5：一种以IOT漏洞对抗IOT僵尸网络的方法

议题概要：

由于安全机制的缺失，现有的iot设备往往存在较多安全问题。

另外现网中有大量OEM设备，当IOT设备的安全问题被发现后，这些OEM的IOT设备的安全补丁往往得不到厂家及时开发。

另外由于用户安全意识不够，IOT设备的安全补丁也没有得到用户的及时更新。

这些问题使得大量的IOT设备已经被僵尸网络所控制。

在对抗僵尸网络的过程中，人们采用的方法较多的是进行流量清洗和关闭c&c服务器的方法。

但是这些方法并不能有效地帮助有问题的IOT设备避免受到僵尸网络的下一次控制。

如何在大规模僵尸网络发动攻击前，快速主动地修复被僵尸网络控制的IOT设备安全漏洞，从而削弱僵尸网络的破坏能力?

演讲者提出了一种以IOT漏洞对抗IOT僵尸网络的方法。

演讲嘉宾介绍：

王启泽，看雪ID(ggggwwww)，启明星辰ADLab（积极防御实验室）安全研究员&看雪智能硬件小组成员。他所研究的领域涵盖移动通信安全、IOT安全，曾在移动通信安全领域有15年的工作经验。

议题6： Windows 10新子系统*新挑战

议题概要：

本演讲课题讲述Windows10系统因对Linux系统的支持所带来改变以及伴随而来的安全挑战。

演讲嘉宾介绍：

陆麟，中国最老的十大黑客之一，Windows系统内核专家！原NEC中科院软件研究所专家。现任上海高重信息科技有限公司CIO。长期研究系统内核。多年耕耘信息安全领域。

议题7： 移动APP灰色产业案例分析与防范

议题概要：

移动互联网时代，互联网业务飞速发展，在这样的大背景下滋润了一条以刷单、倒卖、刷榜、引流、推广为主的灰色产业链。他们以低成本换取了高额的利润，给互联网企业以及用户都带来了巨大的损失。加固技术、风险控制、设备指纹、验证码等技术也都在飞速发展，但实际效果并不能让人满意。

本议题将揭露多个真实案例的技术细节，开发流程，运营流程，并提出一些防护建议，协议安全需要从体系上进行加强。

演讲嘉宾介绍：

无名侠 陈愉鑫 移动安全爱好者，看雪论坛会员

议题8： 游戏外挂对抗的安全实践

议题概要：

介绍什么是定制化对抗，以及定制化对抗在腾讯安全方案中的作用和定位。定制化对抗的运营方式，被动的定制化对抗，基于游戏逻辑的对抗，实时介入游戏逻辑的方案能力介绍。主动的定制化对抗，游戏运营前的安全评审和运营期的漏洞挖掘。游戏运营前进行安全性提升的技术点分享，游戏漏洞挖掘的经验分享。定制化对抗方案的建设方法、定制化对抗方案的成本代价、定制化方案的其他应用。

演讲嘉宾介绍：

胡和君，腾讯游戏安全高级工程师，从事PC端游外挂对抗工作8年，近期主要负责FPS类游戏安全对抗工作，擅长定制化应对FPS类游戏外挂风险。

议题9： 开启IoT设备的上帝模式

议题概要：

当今IoT设备大量涌入智能家居领域，IoT安全和大众的生活息息相关。本议题计划关注IoT设备开启上帝模式(即root模式)的相关安全问题，包括root设备的技术手段, 获得root权限后引发的潜在安全威胁，和缓解安全威胁的一些方法。为了提升效果，会分享两个未公开的IoT设备的root漏洞。演讲主要内容如下：

1. Root IoT设备的常见技术手段: 除介绍常规的弱密码和RCE漏洞外，会以一个中兴摄像头固件校验漏洞为例，介绍伪造固件绕过固件校验算法进行Root设备的方法。

2. Root IoT设备之后潜在的安全威胁：除介绍常见的DDoS, DNS劫持, 监听监控等安全威胁外，会以一个DDNS智能硬件花生棒2的root漏洞为例，介绍如何将一个原本不具备wifi功能的IoT设备开启wifi功能。

3. 缓解机制：分享常见的IoT安全机制，例如固件加密与签名，防火墙等方法。

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，本次分享专注于讨论IoT设备被root后面临的相关安全问题。

演讲嘉宾介绍：

杨经宇（Jingle）毕业于伦敦大学信息安全专业,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。

议题10：浅析WEB安全编程

议题概要：

这次想分享的话题是,安全编码;这次分享当中,会把开发中容易忽略又比较常见的安全问题做一些介绍,之后指导在开发中如何避免安全问题的产生。

演讲嘉宾介绍：

汤青松 中国婚博会PHP高级工程师，2017 Devlink PHP开发者大会 安全话题演讲嘉宾，2015年在网利宝,担任系统研发以及系统安全建设工作，2014年在乌云网,负责乌云众测开发。

议题11：那些年，你怎么写总会出现的漏洞

议题概要：

针对开发者在编码时产生的意料之外的漏洞愿意以及漏洞分析，例如：PHP自身函数，PHP正则缺陷，php和mysql的不一致，格式化字串，各种防御及缺陷绕过等一系列问题。内容包括thinkphp，WordPress，metinfo，ctf题目等各种例子

演讲嘉宾介绍：

邓永凯，web安全研究员，绿盟科技从事安全工作5年，主要负责web漏洞扫描器的开发，web漏洞挖掘及分析，web安全研究工作。现在为绿盟科技应急响应中心从事web安全研究工作，曾创办《安全参考》，《书安》等免费电子安全杂志，白帽子。

本文作者：又田
本文转自雷锋网禁止二次转载， 原文链接