十大干货安全议题，足以展望今年网络安全趋势

转载

blackorbird 于 2019-07-01 14:30:20 发布 729 收藏
原文链接：https://www.bagevent.com/event/2195041?bag_track=895628

夏天可以看雪吗？

答案是肯定的。

因为，看雪2019 安全开发者峰会即将于7月20日在北京国家会议中心开幕

2019 安全开发者峰会（SDC）是由拥有19年悠久历史的老牌安全技术社区——看雪学院主办，CSDN、开源中国、博客园协办，会议面向开发者、安全人员及高端技术从业人员，是国内开发者与安全人才的年度盛事。作为开发与安全领域内，最具影响力的互联网安全合作交流盛会之一，SDC始终致力于建立一个多领域、多维度的高端安全交流平台，推动互联网安全行业的快速成长与广泛合作。

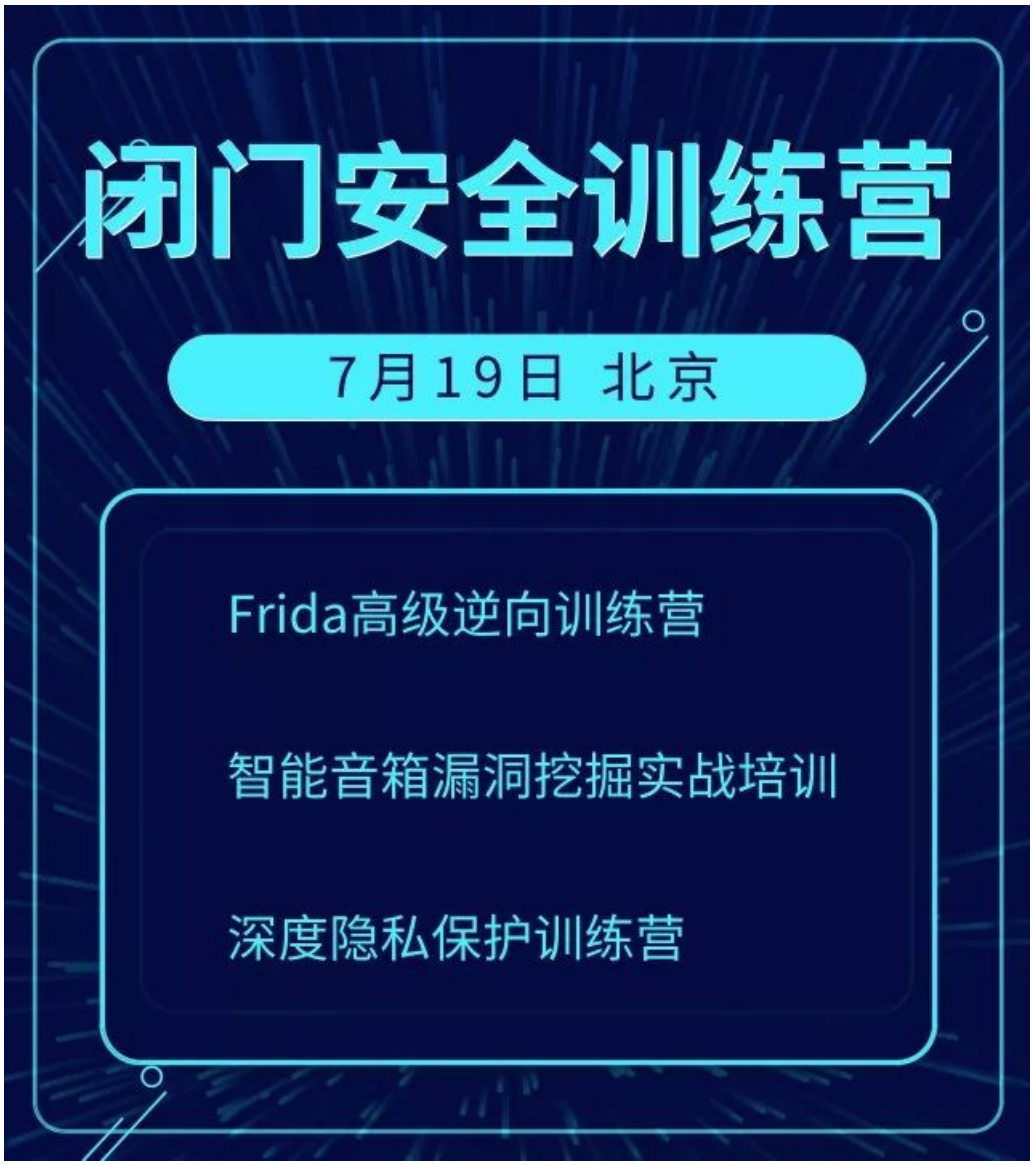
自2017年7月份开始举办第一届峰会以来，会议始终秉承着技术与干货的原则，议题内容覆盖物联网、智能设备、区块链、机器学习、WEB安全、逆向、安卓、iOS等前沿领域，吸引了业内众多顶尖的开发者和技术专家。

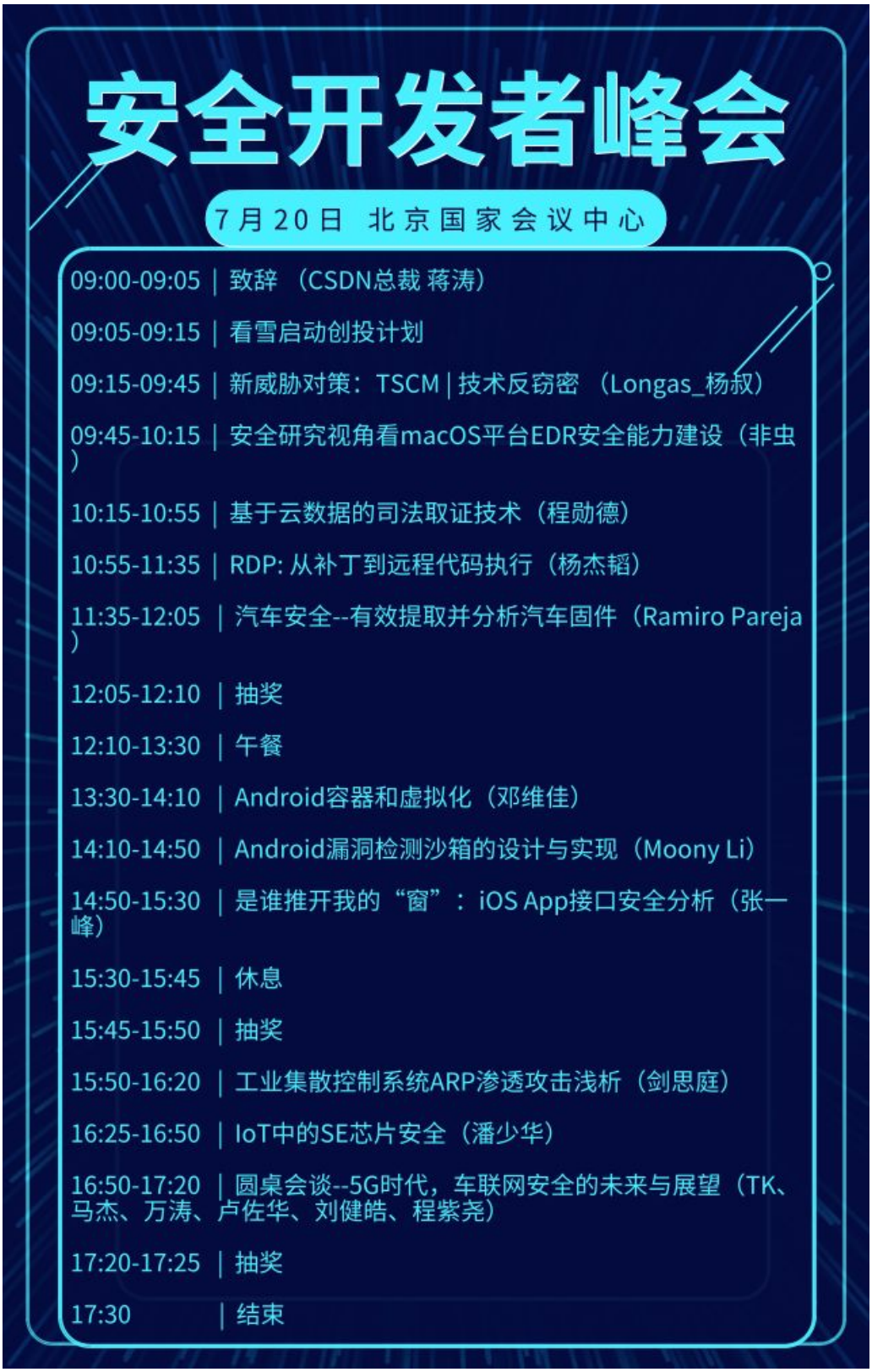
会议时间：2019年7月19日～20日

会议地点：中国·北京·国家会议中心

会议规模：1000人+

会议日程：


闭门安全训练营
7月19日 北京
Frida高级逆向训练营
智能音箱漏洞挖掘实战培训
深度隐私保护训练营

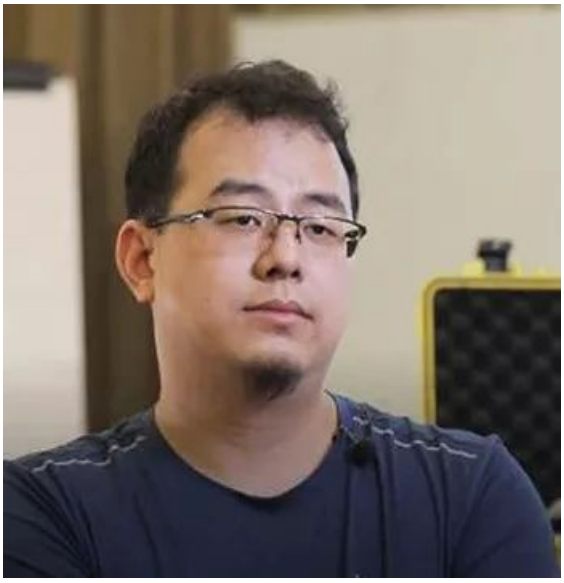


十大干货议题一览

1、新威胁对策：TSCM | 技术反窃密

反技术窃密对策（TSCM，Technical Surveillance Counter Measures），作为目前最直接的商业安全防范技术方案，能有效防范各种利用技术手段开展的窃密及非法监控行为，越来越受到各国政府和企业的重视，需求日益增涨。

本次议题将带来以下内容：1）2019，企业面临的新威胁趋势；2）典型技术窃密的手段与案例；3）企业研发环境窃密手段分析；4）企业供应链窃密手段分析；5）TSCM，技术反窃密；6）企业物理风控防护的要素。



杨叔（Longas），RC2反窃密实验室负责人，ZerOne无线安全团队创始人，“商业安全&隐私保护”系列认证课程的创始人与推广人。16年信息安全行业及隐私保护从业经验，并多年致力于无线攻防/通信安全防窃密的研究与实践。曾任职NSFOCUS、华为、阿里巴巴等行业大公司的安全团队负责人、专家组组长及安全研究员等。曾应邀在KCON、Xkungfoo、CNCERT、VARA、QCON、OWASP、GHRC(CDG)、XDef、OWASP、SSC、CSSS、CACSC等三十多个国内外黑客/安全会议及沙龙上担任演讲嘉宾。也是《无线网络攻防实战》系列书籍原创作者。

2、安全研究视角看macOS平台EDR安全能力建设

EDR（Endpoint Detection and Response）终端检测与响应平台是近年最流行的安全产品之一。它强调防御、检测与响应一体化的安全解决方案。目前，国内外的安全厂商都在积极的响应与储备相应的安全能力。

本议题主要围绕几方面内容：1. EDR的功能与架构；2. macOS系统的安全特性与能力；3. macOS系统平台的终端Agent开发安全能力建设的技术方案；4. macOS平台Agent的限制与注意事项。

本议题试图从安全研究与Agent实现的视角，讲解macOS平台的EDR安全能力建设。

听众收益：了解EDR产品的技术原理与架构，相关的安全防护与防御机制，并了解在macOS终端上的Agent实现的原理与技术方案。

演讲嘉宾：丰生强 （ID：非虫），奇安信安全威胁情报中心安全研究员，专注软件安全领域。《Android软件安全与逆向分析》、《macOS软件安全与逆向分析》、《Android软件安全权威指南》作者。

3、基于云数据的司法取证技术

议题简介：移动生态的封闭化，为司法取证带来很多挑战。但是iOS和Android数据云端化已成为一种行业趋势，虽然会带来一些安全隐患，但也给司法取证带来了新的机会。本议题将会讲解iOS、Android云端数据收集类型、数据获取技术难点，并提供相应的解决方案。

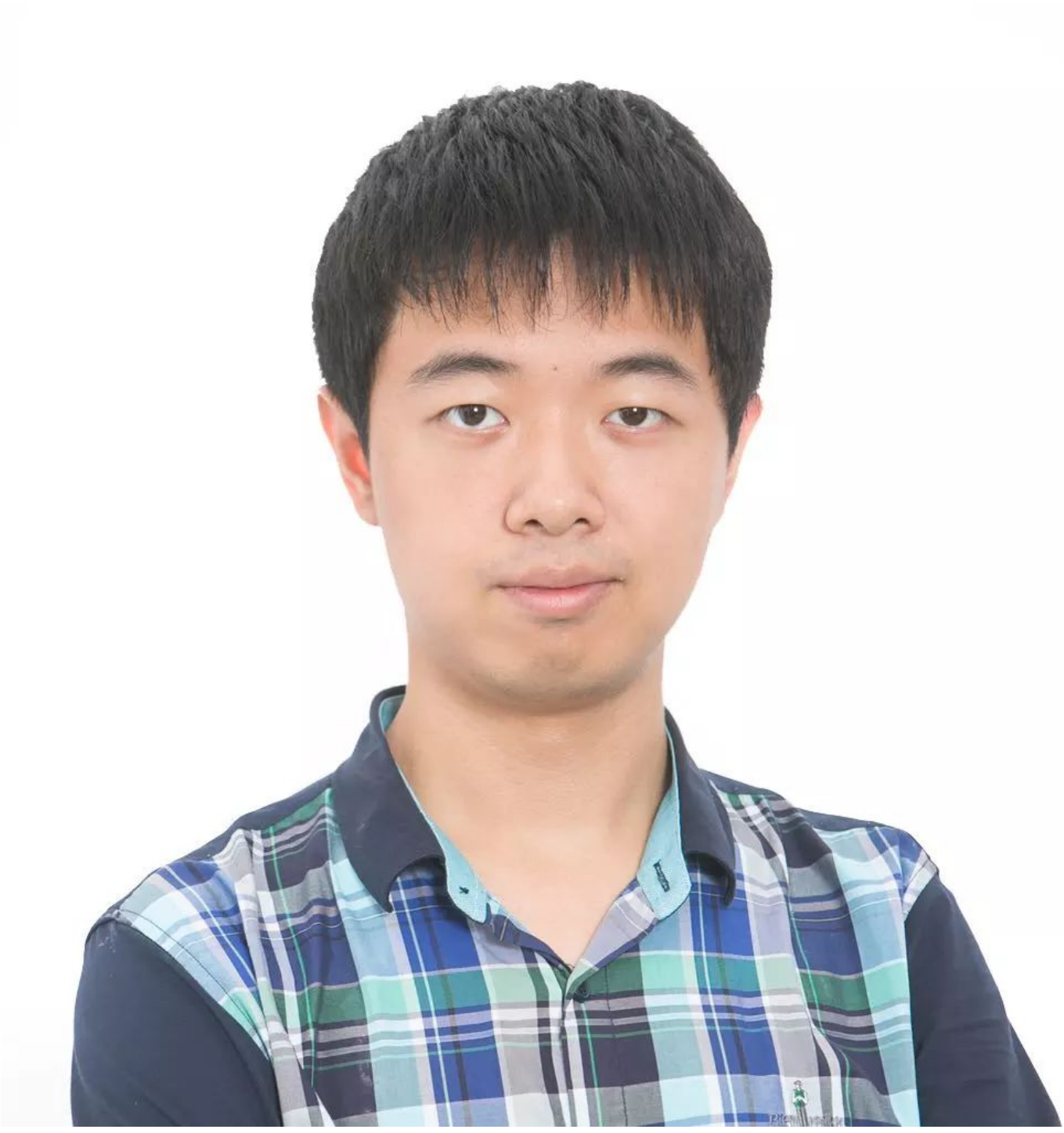
听众收益：了解iOS和Android云备份、云同步和TOKEN机制，并了解目前最新的智能手机取证技术。

演讲嘉宾：程勋德，万兴首席安全架构师。《加密与解密（第4版）》联合作者，从事PC Android逆向工作8年。

4、RDP: 从补丁到远程代码执行

议题简介：CVE-2019-0708是微软于今年5月14日修补的一个存在于Win7/Server2008R2等操作系统远程桌面服务上可造成远程代码执行问题的漏洞。远程桌面服务本身是一个在企业中被广泛应用的服务，此次漏洞的曝光也立刻引起了广大安全人员及爱好者的注意，但是长时间以来一直缺乏详细利用方法的资料。本次演讲将讲述从补丁对比，相关服务二进制分析到最后远程代码执行的全过程，详细介绍漏洞相关的RDP协议内容，分析远程桌面服务的攻击面，最后介绍攻击缓解策略及其原理。

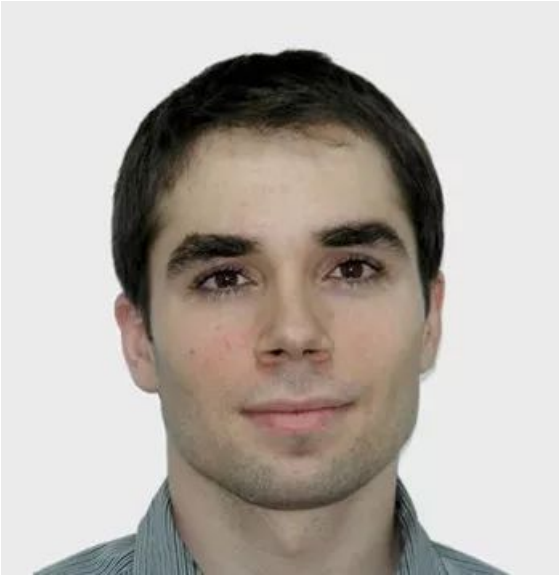
听众收益：了解RDP协议，低版本Windows内核漏洞利用方法。



演讲嘉宾：杨杰韬，腾讯科恩实验室安全研究员，主要研究二进制分析、漏洞挖掘与利用，腾讯eee战队成员，A*0*E联队成员，曾与团队成员多次参与国内外顶尖CTF比赛。

5、There will be glitches: Extracting and analysing automotive firmware efficiently

议题简介：《汽车安全——有效地提取并分析汽车固件》，本议题将演示如何使用故障注入等硬件攻击手法来从不存在软件漏洞的安全ECU中提取固件。获得固件后，我们将讨论有效分析汽车固件的成功方法。为了提供一个具体的例子，我们将演示我们为其中一个目标（一个仪表板）编写的自定义模拟器，并展示它可以准确地执行动态分析。我们的模拟器使我们能够快速了解固件的功能，提取攻击者感兴趣的秘密，并将模糊测试应用于目标接口。最后，我们将解释这些问题的真实影响，它们如何导致可扩展的攻击，以及如何保护今天的汽车。



演讲嘉宾简介：Ramiro Pareja是Riscure位于中国的安全测试实验室的技术负责人，在硬件安全方面拥有丰富的经验，专注于嵌入式系统和SoC安全。

6、Android容器和虚拟化

议题简介：自droidPlugin问世以来，各种热发插件框架变得越来越流行，在安全方面也发展出了各种Android多开容器的实现。伴随着YAFA、Epic这样的ARTHook框架问世，我们开启了容器内App的上帝模式，可以非常容易的控制App的内部逻辑。在ARTHook足够稳定的情况下，我们有各种思路实现对APK的代码注入，同时提供统一方案完成常见注入检测对抗。Android容器有开始又了各种新的玩儿法。

本议题围绕Android容器，介绍目前开源的容器方案，并探讨容器的实现原理、可能遇到的挑战，以及其他可能的实现方式和这些特定实现可能带来的魔力。

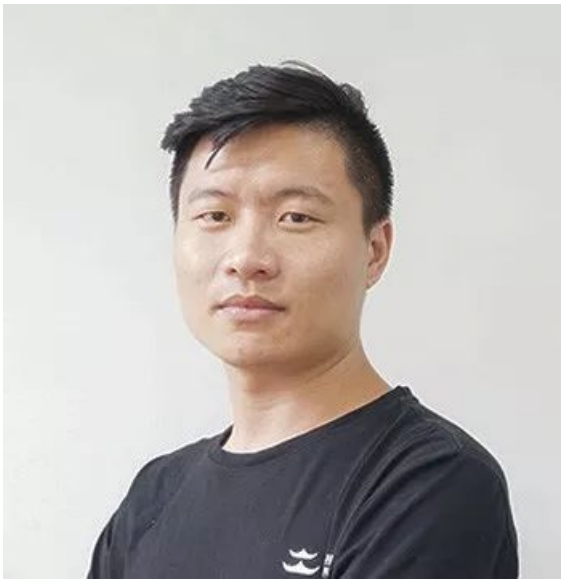
听众收益：了解多开机制原理，免root注入控制app的方法，基于容器绕过杀毒软件检测。

嘉宾简介：邓维佳（ID：virjar）。川大软件工程专业毕业。爱好爬虫、抓取相关技术。同时对移动安全有浓厚的兴趣，玩过iOS/Android逆向。目前最喜欢的是Android安全相关技术研究，包括App加固脱壳、Android群控技术、Android多开容器等。

7、是谁推开我“窗”：iOS App接口安全分析

议题简介：议题涉及接口有两种，分别是URL Scheme和JSBridge ，URL Scheme是iOS 系统提供的应用间跨进程通信机制，通过该接口允许应用相互调起并传递参数；JSBridge是使用Hybrid模式开发应用中JavaScript与Native代码的交互接口，以增强JavaScript与Native代码交互能力。在日常iOS APP审计过程中发现多个由于URL Scheme和JSBridge接口设置或鉴权不当导致的安全漏洞，结合应用其他漏洞可以实现如远程窃取Cookie、远程沙箱任意文件上传、存储型XSS及业务逻辑漏洞等。

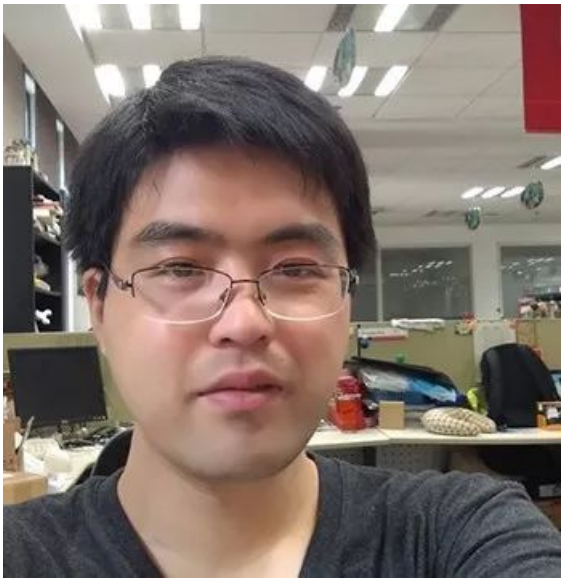
本次演讲首次披露由于iOS APP URL Scheme和JSBridge接口导致的安全漏洞。



演讲嘉宾：张一峰，北京长亭科技移动安全负责人，负责移动APP安全审计、源码审计等漏洞挖掘工作。全球互联网技术大会网络安全专场演讲嘉宾，2018华为终端安全奖励计划大会圆桌会议嘉宾，2018 DEFCON Demo Labs speaker。

8、Android漏洞检测沙箱的设计与实现

议题简介：本议题介绍业界落地的0day攻击检测的Android安全沙箱的设计与实现，基于Frida Hook以及内核代码插桩技术实现了典型的0day漏洞利用技术的检测包括Heap Spray，ROP等检测技术。



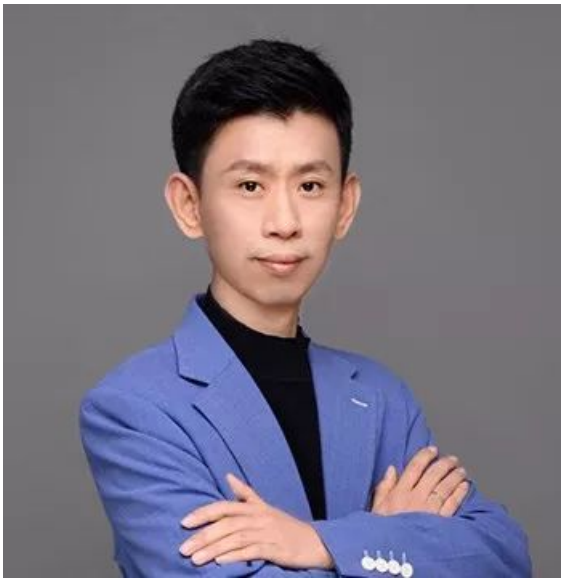
演讲嘉宾：moony li （李月锋）, @Flyic of twitter, @SilverMoonSecurity of Github，趋势科技技术架构师，移动安全威胁研究组项目组长，10年安全开发经验，精通Windows、Mac安全沙箱开发；熟悉Android，iOS等平台漏洞挖掘与利用，红蓝攻防对抗。

作为演讲者参加过很多国际知名安全会议：HITCON 2016、CodeBlue 2016、Pacsec 2016、BlackHat Europe 2016、Code Blue 2017、Black Hat Asia 2018、Black Hat USA 2018 Arsenal、Black Hat Europe 2018、Blackhat USA 2019。

9、工业集散控制系统的脆弱性分析

议题简介：工业集散控制系统为工控系统种类之一，主要分布在石油、化工、冶金、水泥、水系统，本演讲主要介绍工业集散控制系统系统结构，工业网络拓扑。在此系统结构上可能存在脆弱性的分析，针对工业集散控制系统的网络层引发的安全思考，同时提供针对工业集散控制系统的安全防护方法和措施。

听众收益：了解工业集散控制系统结构和使用环境，熟悉工业集散控制系统的现存的脆弱性和漏洞，掌握工业集散控制系统安全防护方法。



演讲嘉宾：剑思庭，复旦大学软件工程硕士，工控安全高级研究员，暗影安全团队，中国自动化协会常任理事，Kcon 2018讲师，开发Ethernet/IP协议设备嗅探工具。

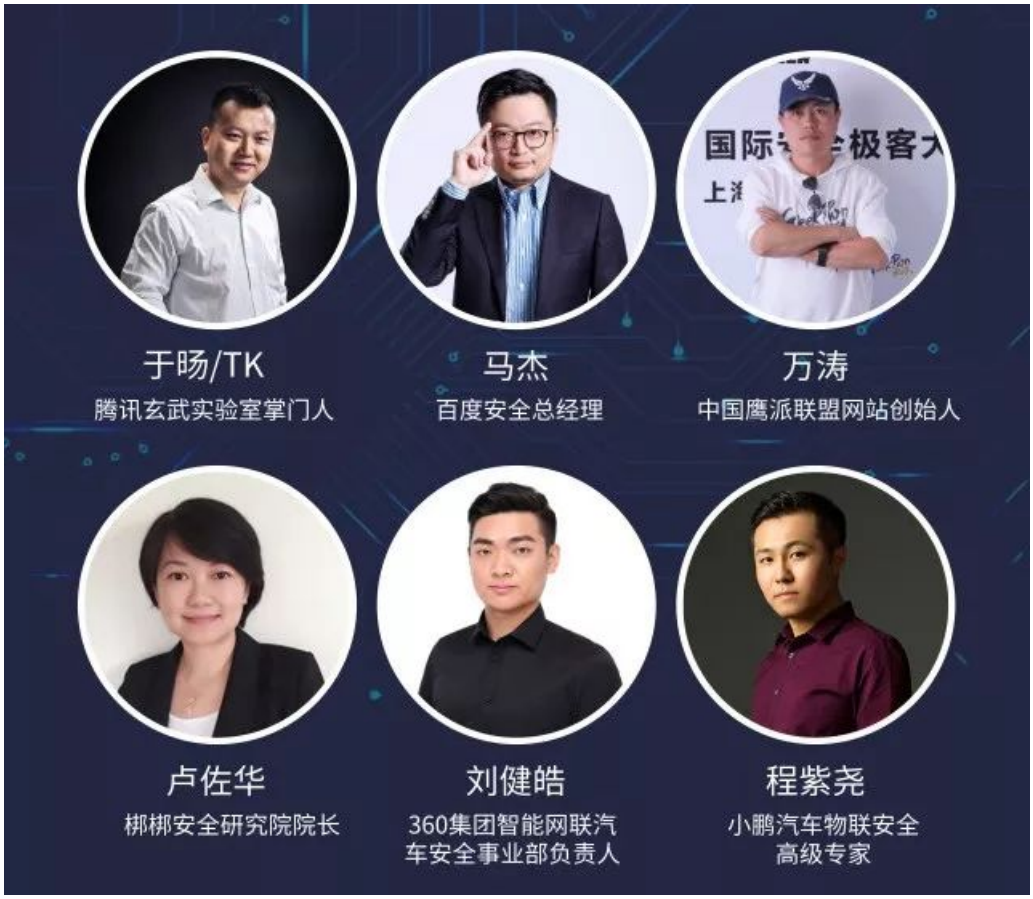
10、IoT中的SE芯片安全

议题简介：随着物联网的发展，IoT设备自身的安全性越来越重要，要做到端对端加密，SE芯片是最基础的一个环境。议题从SE芯片特性及SE芯片在IoT设备中提供的功能及加密引擎方面进行安全性的分析，来剖析如何通过恰当的使用SE芯片来实现更安全有效的IoT安全环境。共分为4个章节介绍：为IoT设备安全SE情况（以智能门锁场景为例），SE芯片具有的特性，为SE芯片在IoT设备的实际设计中的硬件设计安全风险，SE芯片在IoT设备的实际设计中易产生的安全问题。

嘉宾简介：潘少华，江苏知道创宇负责人、物联网安全研究团队负责人，中国区块链应用研究中心理事，中国互联网站状况及其安全报告编委会指导委员。江苏知道创宇主要方向为物联网产品的安全研究及其解决方案，团队曾先后破解多款国内外知名硬件数字钱包，有着丰富的智能云锁、智能家居、智能表的安全测试经验。

重磅嘉宾，共话5G时代汽车安全

随着5G时代的来临，大容量、低时延的网络传输将变为现实，人类将加速进入万物互联的车联网时代，而汽车作为人们出行必备的交通工具之一，将面临深刻的改革，安全人员将面临怎样的机遇与挑战呢？我们特别邀请到了业内大家，来就此话题进行讨论与分享。



不只GEEK

1、CTF小栈

行走江湖已良久，相逢一笑泯恩仇。身怀绝技意气发，夺旗小栈共交流。看雪学院CTF小栈，特意为CTF爱好者们开辟全新板块，设立CTF小栈，举办线下交流会，为各路赛友英雄提供比赛经验、技术交流，相互切磋的机会。

2、企业公开课

特邀信息安全领域领头企业的安全专家莅临现场，探讨关于企业安全的最新态势与情报，促进企业与企业、企业与用户之间的沟通与交流。

3、极客市集

想要在网络的世界里驰骋，一个强大的工具，必不可少，它能帮助你如鱼得水，来去自如。例如，美国NSA开源的一款二进制分析工具——GHIDRA，它可以帮你分析代码、调试、恶意软件无效化，功能堪比上万块的IDA~

极客市集是一个创意火花碰撞的舞台，自由、开放、包容，让所有热爱网络安全技术的Geek们汇聚一堂，来为分享他们的得力作品！

三大安全训练营，充电不停！

1、《Frida高级逆向》训练营

最近两年来，Frida因为简单易用以及能够支持多平台注入，变得越来越来流行。

本次训练营对Frida进行培训，APP逆向实例分析，动手实验

1. 从Frida的入门开始，到使用Frida进行Android协议分析，再到Android Native算法分析。

2. 包含4个实例分析，对某大型视频类APP，某大型电商类APP，某大型旅游类APP，某大型出行类APP的协议逆向或算法逆向。

3. 包含3个实验，让学员们自己动手来分析算法，被ollvm混淆的算法分析，遇到非标准算法怎么进行分析，某个安全SDK的sign算法分析。

2、智能音箱漏洞挖掘实战培训

在物联网时代，大量的智能化设备将连接到网络上。因此对于智能化设备来说，互联和安全是急需要解决的两大问题。

近年来物联网设备暴露了大量的安全问题，越来越多的企业也关注物联网设备的安全问题，对于物联网安全人才的需求也较大。另外，随着研究的深入，物联网设备攻防对抗也越来越激烈，对于安全研究人员能力要求也越来越高。

本课程旨在以智能音箱为案例，讲述主流智能设备的攻防实战，丰富学员的知识面，提高动手能力及安全研究能力。

3、深度隐私保护训练营

本课程将培养与提升商业安全保密及深度隐私保护防范意识，侧重掌握实用的技术技能，尤其是出行酒店安全与个人隐私保护、企业内部反窃密设备学习，提升公司高层、关键部门及安全人员的商业安全及隐私保护意识。

课程内容包括但不限于：

国内外商业安全概念、恶意竞争常见手段及非法器材、真实商业窃密案例解读、企业研发环境下窃密手段、企业办公/会议安防措施 • 海外出行酒店住宿安防、通用便携式反窃密设备与使用、多场景模拟实训等。

此外，本课程为提高学员掌握实际隐私保护技能，还包含4个实用实验内容，如酒店模拟环境检测等，将采用多组同步实验及考核的方式开展。

7.19日（周五）北京

名额有限，先到先得 扫描上方二维码，立即购买～ 

惊喜大奖等你来拿

10 大精彩议题

1 大圆桌会谈

3 大极客活动

除了上述精彩内容，还有惊喜大奖等着你！

华为P30 PRO、iPad、kindle

签名版图书《加密与解密》

.....

更多惊喜大礼等你来拿！

立即购票

想要买票的小伙伴们要抓紧时间了～

去年峰会的门票早早就被抢购一空

今年要买票的小伙伴们要抓紧时间啦！

2.5折疯狂抢购中！拼手速的时候到啦～

1、购票网址：

https://www.bagevent.com/event/2195041?bag_track=895628

2、扫码购票：

扫描上方二维码，立即购买～

快去抢票啦！快去抢票啦！快去抢票啦！快去抢票啦！2.5折限时抢购已开启！

戳原文，立即购票！