技术人员的狂欢 | 看雪2020第四届安全开发者峰会顺利落幕

原创

CSDN快讯 于 2020-10-26 16:29:55 发布 2833 收藏
分类专栏： 业界资讯

在5G新基建的浪潮下，网络攻击手段不断升级，攻击范围也扩大到各个领域，新时代的网络安全将面临更复杂严峻的挑战。

10月23日，看雪2020第四届安全开发者峰会（看雪2020 SDC）顺应时代的变化，聚焦全新的网络安全挑战，以“新安全，新未来”为主题，在上海浦东喜来登由由大酒店为大家带来一场技术的饕餮盛宴。

新基建时代，网络安全相关的前沿技术已覆盖到更多领域，包括IoT安全、移动安全、漏洞挖掘、病毒分析、AI安全、工控安全、软件保护等，本次峰会上，看雪就邀请多位重量级嘉宾为广大安全爱好者带来紧抓时下最热门最前沿技术的十大精彩干货议题。此外，峰会还邀请到6位重磅嘉宾就“新安全，新未来”进行深入探讨。

除了主会场的精彩议题分享，2020 SDC分会场还开设安卓高研班线下交流会；会场外，还有极客市集，为大家带来一大波亮眼的黑科技.....

现在就让我们一起来回顾下现场的精彩瞬间吧！

> **第一篇章：期许**

近年来随着各类网络攻击和新型网络诈骗案件的日益增多，网络安全更是越来越受到社会、政府与公众的高度重视。在当下这个互联网时代，网络安全对于国家安全来说，牵一发而动全身，没有网络安全就难以保障国家的安全。

看雪学院举办安全开发者峰会的目的正是为了给关注网络安全的专业人士提供一个分享交流的窗口，也力争让更多普通人开始关注网络安全，助推我国互联网安全的高速发展。

首先，看雪学院创始人段钢先生发表本次峰会开幕词。

段钢先生讲到截至2020年，中国网络安全人才需求量预计达到160万关注在全球范围内网络安全人才仍是稀缺资源，未来安全市场规模将持续增大，将为安全人才带来更多机遇。

随后，百度副总裁马杰先生也对本届峰会送上了美好的祝愿。

马杰讲到过去20年，整个技术形态都产生了很大的变化，我们已经进入了一种智能经济的时代，非常幸运。AI时代的变革将是一次非常重大的革命，其带来的安全问题需要安全人员共同的努力。希望大家一起把AI时代整个产业做大。

> **第二篇章：初心**

每年的安全开发者峰会上，大家最关注的就是看雪邀请行业大牛们分享的精彩议题。每个议题都经过看雪专家团队层层把关，严格保障分享内容绝对够前沿够干货。

“议题只分享纯干货技术”是看雪多年来的初心，也是始终不变的原则。下面，就让我们一起来回顾今年各有千秋的十大干货议题吧！

1、逃逸IE浏览器沙箱：在野0Day漏洞利用复现

今年5月，在一起针对韩国某公司的APT攻击中，研究人员发现黑客集团使用了两个在野0day漏洞：Internet Explorer的远程代码执行漏洞和Windows的特权提升漏洞。本次峰会上，安全研究员曹磊为我们介绍了这两个0Day漏洞逃逸IE浏览器沙箱的原理和过程。最后，他还向我们现场演示了漏洞在Windows10 2004版本下的完整利用过程，为广大技术人员更好地研究漏洞提供了参考。

点评：逃逸沙箱一直是计算机安全领域非常受欢迎的研究方向，其难点在于不仅需要对操作系统有着深刻的理解，而且还需要熟悉编译原理，因为浏览器在渲染网页时会使用一些优化技术来加速代码的执行。这次的演讲深入细节，让人印象深刻，也让人感受到网络攻击背后的复杂性。

2、LightSpy：Mobile间谍软件的狩猎和剖析

iOS封闭的生态系统真的足够安全吗？殊不知，今年1月，就有间谍软件LightSpy锁定特殊iOS用户进行“Water Hole”攻击。在本议题中，深信服安全专家Lilang Wu就为我们分享了其团队发现的该全新手机间谍软件LightSpy，以及同样针对Android设备的相似恶意软件家族dmsSpy的整体功能及传播方式。相信广大安全研究员能通过本议题对全新的手机间谍软件有所了解，在今后的攻击来临前有所准备。

点评：没想到吧？即使是最安全的iPhone，仍旧有可能遭受到最新的间谍软件的攻击！只要你点击了不明链接，手机瞬间不再属于你。间谍软件可以监控浏览器、聊天软件，甚至插入后门、解密聊天记录。Android也不能幸免。听了这次演讲，我们可以知道以后要少点击不明链接，也要经常更新操作系统到最新版本。

3、Dex格式消亡史——最新Dex保护技术：流式编码

当下常用的DexVmp虚拟保护技术,某种程度上抑制了脱壳的自动化，但是随着攻防的演进已暴露出不足之处。对现有的Dex加固方案进行革新很有必要。在该演讲中，360加固保团队负责人曹阳为我们介绍了一种开创性的全新Dex保护方案，通过对字节码重新编码，自定义变长指令，而非以往的映射表形式。这种升级之后的DexVmp方案，使基于映射表完美还原代码成为历史。全新方式吸引了众多安全爱好者的目光，有助于大家的安卓防守和加固认知，达到新的水平。

点评：和PC壳的发展路径类似，安卓平台软件壳的发展从文件粒度、函数粒度、到指令粒度。对应的技术随着破壳技术的升级而不断迭代，形成了较为成熟且复杂的体系，目前已进入最高强度的VMP对抗。它们保护着我们日常所用的App，为阻挡黑灰产立下了赫赫战功。

4、Android WebView安全攻防指南2020

WebView已成为Android App中最容易出现重大漏洞的薄弱环节。为此，本次峰会上，OPPO子午互联网安全实验室安全专家何恩基于自身漏洞挖掘所积累的丰富案例，对WebView安全配置、白名单校验、Js2Java接口安全、Intent Scheme校验等典型漏洞案例进行了介绍和分析。通过本演讲，开发者能了解到Android WebView最新的典型漏洞类型及其利用手法，从而获得安全编程方面的指南。

点评：可能大家都试过在一个App中点开网页链接吧？殊不知，这其中也包含着一定的风险。Android系统中，这一功能由Webview实现。Webview需要处理不受信任的网络输入，同时又和App有着交互的过程。这场演讲告诉我们浏览恶意网页可能导致Webview被攻破。

5、生物探针技术研究与应用

本议题中，小盾安全算法总监王巍详细地从当前主流的实现方案及其优缺点、特征工程方法、参数调优手段等几大方面，让参会者深入了解这项前沿技术。此外，他还基于一个工业标准模型，细致入微地拆解从数据采集、特征抽取、模型选型以及调优的探针技术的建模全流程，让参会者获悉如何才能构建一套完整的生物探针风控体系。

点评：生物探针并不是生物学的一个概念，而是指采集用户使用手机时的传感器数据和屏幕轨迹数据的技术。有了生物探针，可以做到无感认证。比如说，每个人使用手机触屏输入字符都有一定的规律可循，如果App可以掌握这种规律，就可以做到可靠地验证用户的目标。这需要用到诸如人工智能、统计推断等技术。

6、世界知名工控厂商 密码保护机制突破之旅

密码保护系统作为工控安全的“大门”，安全性令人堪忧。本次演讲，绿盟科技格物实验室资深工控安全研究员高剑以西门子、施耐德、罗克韦尔等世界知名工控厂商的核心控制设备为研究对象，讲述其密码保护机制的缺陷及突破思路。最后，他还给我们总结出几种行之有效的攻击思路和实现方法，并针对这些缺陷提出了安全设计上的建议。

点评：工控系统安全历来是安全会议的热门探讨话题，因为它们实在是太重要和关键了。想象一下，如果炼油厂因为控制系统被攻击而爆炸，如果自来水厂因为被攻击而停水，那将给国计民生带来多大的损害？这次演讲，让我们看到了居然有一些上古密码验证漏洞存在于这些“外国进口”设备上，让人实在是不放心。

7、敲开芯片内存保护的 最后一扇“门”

内存保护芯片作为守卫所有设备数据和安全的最后一道防线，至关重要。本议题中，阿里云安全IoT平台高级安全工程师付鹏飞为我们介绍了emmc、NoR Flash、NAND Flash等通用芯片的固件提取方案，并针对芯片本身读保护进行注入型安全绕过，对内存保护芯片进行低成本的侧信道攻击达到固件提取的效果。此外，他还开源了一些通用的固件提取硬件（PCB图纸）+软件的方案。相信安全工程师都能通过议题了解到更低成本高效的安全加固和防解包方案。

点评：是不是很好奇黑客是怎么从iPhone、IoT设备中提取出固件进行分析的呢？这就涉及到比较底层的硬件、电工等方面知识。通过侧信道攻击，我们还可以判断CPU可能在做什么，有助于我们破解芯片的奥秘。

8、基于量子逻辑门的代码虚拟（vmp）保护方案

vmp/tmd代表了vm技术的两个方向，但至今其技术原理一直没有太大突破。本次峰会上，VxProtect安全团队创始人赵川突破常规，从“量子逻辑门”出发，从vm底层原理探讨包括“万用逻辑门”、“ALU-算数计算器”、“代码条件分支路径隐藏”、“多态变形编译器”等相关前沿技术，为广大安全圈人士提供“安全性与性能比”更高的全新vm保护思路。

点评：在代码保护的构建过程中，我们需要增加代码复杂度，同时又不牺牲代码运行速度。这看似是不可能的任务。“遇事不决，量子力学”，一句玩笑话竟然成为一种新的思路。用量子力学逻辑运算来混淆代码，可以同时提高安全性、提高性能、减小代码体积，这思路实在是绝了。

9、麒麟框架：现代化的逆向分析体验

作为麒麟框架团队核心成员，孔子乔和武晨旭在演讲中阐述了麒麟框架在MBR实模式分析中的独特作用，并展示麒麟IDA插件如何为IDA Pro带来插桩分析、可视化模拟和反混淆等高级二进制分析功能。麒麟框架所带来的前所未有的插桩分析体验，让台下的安全爱好者都听得兴致勃勃。

点评：麒麟框架的设计目标是将逆向过程现代化，解决Hook不便、插桩不便、配调试环境不便的难题。它支持多架构、多系统，在现场的演示中，我们看见了它强大的能力。结合IDA插件，更是提高了逆向体验。不仅如此，演讲嘉宾最后还介绍了消OLLVM平坦化的相关内容，令人印象深刻。

10、高通移动基带系统内部揭密

移动基带系统的建设是5G时代各国竞相争取的科技高地。本议题中，阿里安全IoT安全研究团队Leader谢君通过对移动基带佼佼者高通的移动4G/5G基带系统进行深度的逆向工程，从Hexagon DSP芯片指令架构以及微内核操作系统QuRTOS的实现方式进行深入探究，介绍包括QuRTOS系统的内存管理、系统间通信、设备管理等特性，从而为我们深度解密高通移动基带系统的内部实现逻辑和运作方式

点评：基带安全对于移动安全是至关重要的，因为攻击者可能通过发送恶意信息来劫持基带乃至劫持整个手机。高通的基带部署了许多防御机制，但这并不能阻碍研究者的研究热情。而这次演讲告诉我们，基带安全往往就在那些最复杂的细节之中体现。

> **第三篇章：畅想**

社会飞速发展，信息技术日新月异。我们也必须不断向前奔跑，才能追上它飞速发展的脚步。

作为当下数字化发展的新引擎，“新基建”已成为我国的国家级战略。在以5G为代表的新基建的浪潮下，机遇与挑战并存。

面对未来诸多更严峻复杂的全新安全挑战，本届峰会特别邀请行业大咖举行圆桌会谈。让我们来看看他们对于“新安全，新未来”的畅想以及深刻见解吧。

上海社会科学院互联网研究中心主任惠志斌主持了本次园桌论坛。

华为终端奇点安全实验室主任陈良阐述了5G时代手机将面临的诸多安全挑战，并分享了得益于安全建设的一些成功案例。

面对新基建下安全问题日益复杂化，上海计算机软件技术开发中心网安所副所长吴建华介绍了国家相关机构和单位将会针对这些问题出台的相关标准、建设等。

复旦大学教授、博导杨珉则对当下核心技术人才缺口大的问题，为我们分享了高校在相关网络安全人才培养过程中遇到的问题，并提出相应的解决方案。

而帆一尚行（上汽云中心）首席安全官陈凯对传统汽车行业在5G车联网时代该如何抓住机会，实现转型升级提出了深刻见解。

最后，翼盾科技创始人兼CEO朱易翔对于5G时代的海量数据下，企业和个人该如何保护自己的数据及隐私安全，表达了自己的看法。

> **第四篇章：求同存异**

受疫情影响，本届峰会不同以往，迁移至上海举行。上海是一个海纳百川，开放包容的城市。而看雪安全开发者峰会对于脾气性格各不相同，来自全国五湖四海，操着不同口音的极客们来说，也是这样一个难得的地方。

“因为同样对技术的热爱，让我们相聚在这里。”

在本届峰会的高研班线下研讨会和极客市集上，极客们畅所欲言、各抒己见但也求同存异，酣畅淋漓地分享自己的心得、知识和得意工具。

本次极客市集共汇集了博文视点、RC²、易念科技、人民邮电四家展商，商品涵盖10款常见小型窃密器材、小型反针孔偷拍绵羊墙、隐私保护幸运扭蛋机等有趣的工具和设备，摊位上大家都玩得不亦乐乎。

不知道你有没有在市集上买到自己心意的宝藏，偶遇圈内大佬呢？

> **第五篇章：相伴同行**

看雪经历20年发展至今，被誉为安全界的“黄埔军校”。看雪和所有用户相辅相成，不可分割。很多用户在看雪论坛踏入安全圈，不断学习、成长，终成大器。而看雪也在广大用户的支持下，才能凭借自身的努力，不断在更大的舞台上散发光芒，被更多人所熟知。

为回馈大家对看雪的支持和喜爱，抽奖活动当然是每年必不可少的经典环节。

今年的趣味抽奖活动“摇摇乐”、“知识达人”在场的小伙伴们都积极参与，全场气氛十分火热。

本次的奖品由京东安全、第五空间、博文视点、华为提供，包括机械键盘2个、图书30本、Harmony开发套件5个、Harmony智能小车5个，以及终极大奖京鱼座的蓝牙耳机4个和iphone 11（128G ）1部。非常感谢！

> **第六篇章：再度启程**

在新基建的浪潮下，5G、人工智能、物联网等技术高速发展。互联网在不断发展、演进的过程中，为人们带来便利的同时，也面临着许多新问题和挑战。为了进一步促进网络安全技术交流，看雪将继续关注新时代下网络安全技术领域的最新发展。

已过20岁的看雪，归来仍是少年。我们将永远坚守初心，紧跟时代潮流，密切关注行业动态，继续为网络安全事业的发展贡献自己的力量。

看雪一路走来，离不开合作伙伴们的大力支持和帮助，你们的肯定就是我们前进最大的动力和底气。在此衷心感谢所有为看雪2020提供帮助的合作伙伴们！

感谢钻石合作伙伴：百度安全、华为、深信服科技！

感谢黄金合作伙伴：科锐、豹趣科技、极棒、爱加密、OSRC、TSRC、极光无限、安恒信息、同盾科技！

让我们共同努力，捍卫网络安全事业新生态。

感谢各位朋友们莅临现场。

我们明年再会！

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖