演讲者及议题概要

PAC 研究

Brandon Azad

议题概要

苹果继续推出硬件缓解措施，使针对 iPhone 的攻击变得更加困难。在本议题中，我们将分析苹果在 A12 SOC 上实现的 PAC 机制。与原来的 ARM 设计相比，PAC 大大加强了对内核攻击的防护。基于任意内核读/写，我们将测试 PAC 的行为表现、推测 PAC 的实现、并尝试找到绕过它的方法。我将介绍我发现的绕过 PAC 获得内核代码执行的 5 种不同技术。

演讲嘉宾介绍

Brandon Azad 是 Google Project Zero 的安全研究员，专门研究 MacOS 和 iOS 安全。

钉枪：突破 ARM 特权隔离

宁振宇张锋巍

议题概要

现在的处理器都配备了调试功能，以方便程序的调试和分析。尽管调试体系结构已经提出多年，但是调试功能的安全性还没有得到充分的检查，因为它通常需要物理访问才能在传统的调试模型中使用这些功能。

ARM 引入了一个新的调试模型，该模型自 ARMv7 以来不需要任何物理访问。在这种新的调试模型中，主机处理器能够暂停和调试同一芯片上的另一个目标处理器(处理器间调试)。Nailgun 攻击的思想是利用这种处理器间调试能力，因为它允许低权限处理器暂停和调试高权限的目标处理器。

我们的实验发现了许多易受攻击的设备，包括 Raspberry Pi 这样的物联网设备、所有基于 ARM 的商业云平台，以及华为、摩托罗拉和小米等移动电话。为了进一步验证，我们证明了钉枪攻击可以用于访问 Raspberry PI 上的安全配置寄存器(只有在安全状态下才能访问)，并使用非安全内核模块提取存储在华为 Mate 7 安全内存中的指纹图像。

演讲嘉宾介绍

宁振宇是韦恩州立大学计算机科学系的博士生。他 2011 年从同济大学毕业，获得了计算机科学的硕士学位，研究方向是硬件辅助系统安全、嵌入式系统和可信执行环境。

张锋巍是韦恩州立大学计算机科学系 COMPASS(计算机与系统安全)实验室主任、助理教授。2015 年，他获得乔治梅森大学(George Mason University)计算机科学博士学位。他的研究兴趣在系统安全领域，重点是可信执行、硬件辅助安全等。张锋巍在系统安全方面有 10 年以上的工作经验。他的工作得到了安全社区的广泛认可，发表了 30 多篇顶级会议/期刊论文。

危险的文件快传应用：亿级用户量的隐私泄露漏洞的发现、利用和防御

张向前刘惠明

议题概要

目前，大部分厂商的手机都会预装文件快传应用，这些应用相比蓝牙、WiFi 等传统的传输工具更方便快捷。然而，用户在享受方便快捷的同时面临着巨大的安全风险。我们的研究发现大部分的文件快传应用都存在安全风险，这会造成文件被窃取、篡改等，甚至造成更加严重的后果。

通过对主流的 Android 手机厂商预装的文件快传应用逆向分析，我们发现了数十个高危漏洞。这些应用在设计上存在许多安全缺陷，导致用户隐私数据泄露、文件被窃取、任意文件下载甚至远程代码执行等。我们将展示详细的漏洞细节和利用方法。我们也对市面上大量的第三方应用进行了研究，发现它们同样存在严重的安全漏洞。这些应用加起来有超过十亿的用户量，但是它们的安全风险却一直被人们忽略，攻击者可以轻松获取和篡改附近使用此类应用传输的文件。我们详细总结了快传类应用的所有攻击面，并展示两种通用的攻击方法。我们也会展示相关 demo 和工具。

另外，我们也会分享对相关漏洞的修复建议，并提出了一种兼顾安全和便捷性的文件快传方案。目前我们正在与主流的手机厂商合作推动修复漏洞。通过这次分享，希望手机厂商和第三方开发者重视此类应用的安全性，共同保护用户的数据安全。

演讲嘉宾介绍

张向前是腾讯安全玄武实验室安全研究员，研究方向是移动安全。曾发现多个 Android 内核和系统安全漏洞，并获得 google 致谢。

刘惠明是腾讯安全玄武实验室安全研究员，研究方向是移动安全和 iot 安全。他曾经在包括 CanSecWest 和 BlackHat Asia 等多个会议上发表过演讲。

全球卫星搜救系统的安全性分析

郝经利

议题概要

全球卫星搜救系统是一个基于卫星的搜索与救援系统，针对分析这些信号时发现，这个系统被严重干扰，同时也发现了这个系统的其他一系列脆弱环节及被攻击的可能性。

演讲嘉宾介绍

360 安全研究院研究员，独角兽团队成员，主要研究方向为卫星通信。

模糊测试蜂窝网络(如果允许的话)

Yongdae Kim

议题概要

为防止意外故障，3GPP 等标准已经定义了 LTE 的安全特性，但有研究发现了一些 LTE 的漏洞，如 DNS 劫持、使用虚假基站的 DoS 攻击和用户位置跟踪。然而，这些研究都没有将重点放在分析运营 LTE 网络中的网络侧问题上，尽管这种性质的漏洞一旦被利用就会影响到许多用户。由于 LTE 中的控制平面组件（control plane components）仍未得到充分的研究，

我们通过构造精心制作的恶意输入、动态分析产生的核心网络响应，研究了在运行的 LTE 网络(以及蜂窝调制解调器)中控制平面过程中的潜在问题。
在这篇演讲中，我将介绍 LTEFuzz，这是一种用于 LTE 的半自动测试工具，它对 LTE 控制平面程序的安全属性进行了广泛的测试。LTEFuzz 动态生成测试用例并将其发送到目标网络或设备，然后通过检查来自目标的测试器和受害者设备的响应，确定性地分类发现有问题的行为模式。为了系统地生成测试用例，我们首先通过广泛分析 3GPP 规范中规定的网络组件的正确行为和它们的安全需求，创建了三个安全属性。通过对运行中的网络进行测试，我们发现了 51 个漏洞(36 个新漏洞和 15 个以前已知的漏洞)，这些漏洞主要是由于对 1)未受保护的初始过程、2)精心编制的普通请求、3)具有无效完整性保护的消息、4)重放消息和 5)安全过程绕过而造成的。我将通过利用我们在运行网络中发现的漏洞来展示新的攻击场景，介绍确切的根源分析。分析和解决这些问题的潜在对策。

演讲嘉宾介绍

Yongdae Kim 是韩国科学技术院（KAIST）教授、网络安全研究中心的主任。他于南加州大学计算机科学系获得博士学位。2002 至 2012 年间，他在明尼苏达双城大学计算机科学与工程系担任副教授/助理教授。去美国之前，他在 ETRI 工作了 6 年，以确保韩国网络基础设施的安全。2013 至 2016 年间，他担任 KAIST 主席教授，并于 2005 年获得了美国国家科学基金会职业成就奖和明尼苏达大学 McKnight Land-Grant 教授奖。目前，他是 ACM TOPS 的副主编，并在 2012-2018 年间担任 NDSS 的指导委员会成员。他的主要研究包括针对新兴技术的新攻击和分析方法，如无人机/自动驾驶汽车、4G/5G 蜂窝网络和 BlockChain 等网络物理系统。

DramaQueen - Drammer 和 Rampage 攻击之旅

Victor van der Veen

议题概要

在过去的两年内，Rowhammer 漏洞从一开始被认为是很难利用的内存错误逐渐变成一种稳定的攻击向量。研究人员不但演示了针对桌面系统的攻击，还通过单字节翻转成功攻陷了云和移动设备，这些都不依赖于任何的软件漏洞。本议题将会深入介绍利用 Drammer（2016）和 Rampage（2018）在安卓系统上实现权限提升的技术细节。
在简单介绍 Rowhammer 漏洞原理及如何在移动设备（ARMv7/ARMv8）上触发后，我们会详细介绍如何对物理内存进行布局的技术。我们将演示如果通过安卓的/dev/ion 设备来控制分配连续的物理页面。通过 ion 接口，我们可以精确得控制页表所在的内存位置，这也是基于 Rowhammer 漏洞提权攻击的第一种方式：Drammer。随后我们来评估 Google 的相关修补：移除了 ion 中的连续堆内存。从而引出了本议题中介绍的第二部分内容：Rampage。我们会介绍一种新的技术来重新完成物理内存布局，这种方式不再依赖于连续内存的分配器。最后作为结论，我们提出针对 Rowhammer 的缓解机制并预测未来的攻击会是如何的。

演讲嘉宾介绍

Victor van der Veen 目前是高通（Qualcomm）的产品安全工程师。在此之前，Victor 在阿姆斯特丹自由大学获取了计算机的硕士学位及网络安全的博士学位。在 Herbert Bos 教授的带领下，他的研究内容专注于软硬件相关的内存类错误。Victor 第一个提出移动平台也受 Rowhammer 漏洞影响。相关的研究工作（Drammer, Rampage, Guardian）广受好评，包括在 Blackhat 2017 年获取了 Pwnie。同时他还是 TraceDroid 和 Andrubis 的开发者之一，这两个平台用于分析安卓的恶意软件。

无处安放的 shellcode

张弛韩洪立

议题概要

在 Android 用户态，实现完整的漏洞提权越来越困难。从 Android N 开始，一系列的 SELinux 策略被引入，用来限制在用户态进程中创建可执行内存。这使得，即使可以通过漏洞控制用户态进程的 PC，仍然无法按照传统方式安放并执行 shellcode，在用户态进程如 system_server 中，执行完全可控的任意代码变成了一件几乎不可能的事情。

为了打破这一壁垒，绕过用户态的防护措施来实现提权，我们研究并实现了一种全新的用户态进程攻击方法，通过借助 JavaVM 解释器来执行恶意 Java 字节码。与以往的通过执行本地代码来实现提权的方式不同，由于 Java 字节码是以数据的形式存放，依靠 Java 的解释执行机制便不再需要可执行内存了，这就打破了目前 SELinux 防护策略的封堵。

同时，我们也会介绍一个 C0RE Team 率先发现的 Binder 漏洞。这个漏洞源于内核，受影响的是用户态进程。它可以被恶意 APP 用来攻击任意能通过 Binder 与之交互的系统服务进程。我们将会利用这个漏洞演示如何控制 PC，并利用前述绕过技术在 system_server 进程中执行恶意代码。

演讲嘉宾介绍

张弛是奇虎 360 C0RE Team 的一名安全研究员，他主要从事安卓框架层的漏洞挖掘与利用。

韩洪立是奇虎 360 C0RE Team 的一名安全研究员，他专注于安卓操作系统以及 Linux 内核的安全研究。在过去的几年里，他向谷歌、高通、英伟达、华为等厂商上报了数十个致命/高危漏洞，并得到了公开的致谢。

举例 XNU 中的引用计数问题

招啟汛

议题概要

XNU 对很多内核对象使用引用计数机制进行生命周期管理，我会简单介绍该机制，对应的 mitigation 以及两个我发现的具体漏洞例子。

第一个是我在天府杯 2018 远程越狱项目中使用的内核提权漏洞(CVE-2019-6225)。我将会详细讲解这个漏洞的发现过程，root cause 以及如何利用它 取得 tfp0。

第二个是在 iOS 12.2 中修复的另一个类引用计数漏洞 CVE-2019-8528。 这两个漏洞都是沙盒内可以直接调用的内核漏洞，危害性巨大。

演讲嘉宾介绍

招啟汛（@S0rryMybad）是奇虎 360Vulcan 团队的安全研究员，主要专注于浏览器及 macOS/iOS 系统。

他在 Pwn2Own 2017/Mobile Pwn2Own 2017 中攻破了 Safari 浏览器。

他在 2018 年天府杯中攻破了 Edge/Chrome/Safari 以及 iPhoneX 设备的远程越狱，并赢得了最佳个人大奖。

他在微软的 MSRC2018 最佳研究员中排名 23。

新一代移动网络和基带的崛起

Marco Grassi

议题概要

过去的一年中有许多关于新的无线电技术的讨论，例如 5G 技术。

本议题会关注智能手机的基带以及相关领域的技术，阐述它们对智能手机、IoT 设备、汽车及一些关键基础设施的影响。

我们会重点分析 iPhone 手机上全新使用的 Intel 基带并预言未来基带的发展方向。

演讲嘉宾介绍

Marco Grassi(@marcograss) 是腾讯科恩实验室的一名高级研究员。他所在的队伍赢得了 Mobile Pwn2Own 2016 的"Mobile Master of Pwn"。他也在同年的 Pwn2Own 2016 比赛中贡献了针对 Safari 到 root 权限的破解。在 Pwn2Own 2017 比赛中，他发现了 VMWare 逃逸的漏洞。在 Mobile Pwn2Own 2017 的比赛中，他参与了基带及 iOS Wifi 项目的破解，并第三次赢得"Master Of Pwn"。他在许多国际会议上发表过演讲，包括 Black Hat 美国，DEF CON，Infiltrate，CanSecWest，ZeroNights，Codegate，HITB 及 ShakaCon。

灰烬中燃烧：基带的童话故事

Guy

议题概要

如果你在平时使用的设备中发现了一个远程可利用的漏洞，会发生什么？

如果这个漏洞存在于设备中的重要通信芯片，会发生什么？

基带研究有着较高的准入门槛，因此阻挡了一些资金充裕的研究机构外的人们。

与此同时，基带研究的公开信息仍然不多，许多研究者还不知道基带研究其实并不是火箭技术那么高大上。

虽然没有太多的公开信息，在过去的一年中有一些可以通过空中触发的可利用漏洞被发现并修补。我会在演讲中分享我的经验方法，如何分析这些漏洞的成因。

演讲嘉宾介绍

Guy(@shiftreduce)是一位独立安全研究者，专注于底层安全研究。

然而他并不一直逆向嵌入式设备，他通常会玩塞尔达，任天堂明星大乱斗，然后给女朋友做一些很可爱的礼物。

畅游 EL3：终极提权之旅

闻观行

议题概要

目前大部分使用了 ARM 芯片的移动设备都部署了 TrustZone。最常见的 TrustZone 模型下，设备会被划分成四级特权(EL0-EL3)，以及可信和不可信区域(secure/non-secure)。这样划分结果使得，即便拥有不可信区域 NS-EL1 的操作系统内核权限，仍然无法访问全部内存和外设，很多功能仍被可信区域所阻拦(隐藏)。此前很多关于 TrustZone 的安全研究已经取得过，运行于 S-EL0 的应用(TA)和运行于 S-EL1 的内核(TEE Kernel)的执行权限。但鲜有人关注 Android 手机 EL3 这一层的安全问题。

本议题会带听众从 NS-EL1 开始，进行为期一小时的 EL3 深度游，内容包括：

EL3 和两个区域的逻辑关系；攻击面以及如何找到一个可利用的漏洞（去年 7 月已修复）；如

何一步步利用该漏洞取得 EL3 的执行权限；最后通过一个例子说明 EL3 的特权之特。

演讲嘉宾介绍

闻观行是盘古实验室的安全研究员，他目前关注的是安卓底层的漏洞分析和利用。他之前在 Infiltrate，Black Hat，44con 等安全会议发表过议题。

一些 JSC 的故事

Luca

议题概要

随着不断加强的溢出缓解机制，针对 iOS 系统的远程漏洞攻击面也在迅速变化。本议题首先会介绍一个老的 Webkit 漏洞来展示某一类问题，并分析最新的缓解机制对漏洞利用的影响。随后会介绍一个 JSC 引擎中的高质量漏洞，并且演示如何绕过当前所有的漏洞缓解机制来利用该漏洞。

演讲嘉宾介绍

Luca（@qwertyoruiopz）是一位来自意大利的安全研究人员，他年轻而富有天赋，喜欢破解各种设备。他在去年发布了针对 iOS 10.2 的越狱 Yalu，并且完全绕过了 KPP 防护。他曾经破解过 iPhone，PS4 以及任天堂的 Switch。

/ 会议日程安排 /

5 月 30 日 DAY 1

08:00 - 09:00	签到
09:00 - 09:05	开场致辞
09:05 - 09:55	全球卫星搜救系统的安全性分析
09:55 - 10:45	模糊测试蜂窝网络(如果允许的话)
10:45 - 11:05	茶歇
11:05 - 11:55	举例 XNU 中的引用计数问题
12:00 - 13:30	午餐
13:30 - 14:20	DramaQueen - Drammer 和 Rampage 攻击之旅
14:20 - 15:10	危险的文件快传应用：亿级用户量的隐私泄露漏洞的发现、利用和防御
15:10 - 15:30	茶歇
15:30 - 16:20	PAC 研究
16:20 - 17:10	灰烬中燃烧：基带的童话故事

5 月 31 日 DAY 2

08:00 - 09:00	签到
09:00 - 09:50	无处安放的 shellcode
09:50 - 10:40	新一代移动网络和基带的崛起
10:40 - 11:00	茶歇
11:00 - 11:50	钉枪：突破 ARM 特权隔离
12:00 - 13:30	午餐
13:30 - 14:20	畅游 EL3：终极提权之旅
14:20 - 15:10	一些 JSC 的故事
15:10 - 15:30	茶歇
15:30 - 17:20	BaiJiuCon（Thomas Lim 主持）
17:20 - 17:30	闭幕