掌上信安的矛盾之争

在 2020 年，网络威胁随着云技术、大数据、物联网、人工智能等技术的发展也将进化，变得更加复杂、棘手、难以应对。网络安全投入持续增加，市场规模将进一步扩大，发展潜力也将继续被激发出来。网络威胁将仍然是安全行业发展的主要驱动力，而国家政策要求是安全市场增长的重要推动力。此外，技术变革将催生安全行业中新的应用场景与市场空间。在威胁、政策、技术的多重驱动下，信息网络安全行业需求将更加旺盛，发展将更加成熟。

随着智能手机的普及程度不断提高，中国移动互联网月度活跃设备规模触顶 11.4 亿，手机已经成为人们生活密不可分的一部分，伴随着智能硬件的性能提升，智能手机已经成为了当前热门的攻防平台。国内手机市场整体处于极度危险的状态，而使用量较多的机型中，平均每个机型的系统中存在的系统漏洞也都处于 10 个以上，而相对较安全一些的手机则使用量不多，因此也一定程度上造就了国内针对安卓设备的各类木马病毒攻击纷繁不断的情况。隐私泄露问题更是成为智能手机安全攻防的重要方面，无论是 Android 还是 iOS 都在该方面投入了大量的工作，在可以预见的将来在巨大的利益面前，矛与盾仍将在这一方面厮杀。

最近数年来，随着伪基站、黄貂鱼（IMSI-catcher）技术的快速发展，大家的手机很容易被这类设备信号劫持。它们可以精确定位手机、窃听通信、发送垃圾信息甚至远程植入木马。伪基站是相对于基础电信运营商架设的正常基站而言，由不法分子临时搭建，用于实施电信诈骗或扩散垃圾信息的无线电收发设备。伪基站是网络诈骗和非法营销的重要技术工具。它能够搜取以其为中心、一定半径内范围内的手机信号，之后使用任意号码，如冒充公共服务号码，强行向其影响范围内的手机发送短信息，普通用户往往难辨真伪。伪基站即假基站，设备一般由主机和笔记本电脑组成，通过短信群发器、短信发信机等相关设备能够搜取以其为中心、一定半径范围内的手机卡信息，通过伪装成运营商的基站，冒用他人手机号码强行向用户手机发送诈骗、广告推销等短信息。

以黄貂鱼技术为例子，黄貂鱼的监控行为非常隐蔽，但如果你有足够密度的城市蜂窝网络分布图视图，便能够检测到相关的异常行为。为了以正常蜂窝网络相同的频率进行信号广播，黄貂鱼可以模拟合法基站的可识别属性如 MCC、MNC、基站 ID 等。黄貂鱼通常会使用更强的信号广播来劫持手机，并远离模拟的真基站，以避免干扰到真基站的运作。为避免干扰基础网络，黄貂鱼假冒附近基站时，会在不同频率/频道上广播信号。大多数基站只在一个或两个频道传输信号，如果某个基站总是不停地换频道，那么很可能是附近有人在用黄貂鱼。每个基站都会广播自身的配置属性，以便手机调整信号、通报基站支持的功能。这些属性是独特的，但同一城市、同一运营商下基站的大部分属性都相同。黄貂鱼必须广播自己是某运营商网络的基站，除非窃听者将它配置为完全仿照模式，所有属性和该网络基站一致，否则它是可识别的。

APP 加固和免杀技术的研究也是智能手机传统安全的重点，前者的目标是保护 APP 不被逆向破解者给分析，后者是为了掩盖特征，逃过杀软或者行为管理软件的识别。在传统混淆技术中，主要是代码混淆，Java 混淆的一般方法是字符串加解密、ProGuard 和 DexGuard。Native 混淆的方式主要有 Ollvm、字符串混淆和 libsgmain。反反编译器主要是通过增加花指令进行重打包对抗，例如 jd-gui、dex2jar、baksmali、shakaapktool、androguard。反调试的方法主要有签名校验、模拟器检测、hook 检测、root 检测。在 APP 加固方面主要有业务场景加固中的安全键盘、防拷贝、防截图等，还有 Java 源码加固，例如华为的方舟 Java2C。Dex 加固又有整体型，抽取型，Dex2C 和 VMP。So 加固又有节加密、函数加密、动态注册、hook 重定向和自定义 linker 之类的。内存免杀技术中重打包、VA 和 Hotfix 又更为普遍。

在现在有简单的方式就是拿市面上的大厂 App 解包之后，安插进自己的代码，重打包，然后可以创造机会让对方下载，比如公司规定安装某银行的手机客户端，邮件里还附上了 APK，对方大概率会下载安装；或者有机会接触对方手机的话，直接就把他原来的微信卸载了，装上自己重打包的微信；你的代码就跑在微信里，所

有的权限都继承自微信，那其实他在攻击者眼中就没有秘密了。想要将远控、或上传等代码隐藏好，实现不落地加载的话，可以将核心逻辑不要直接重打包进包里，而是做个 hotfix，等 App 执行一段时间之后，再通过下发补丁包，让已安装的客户端来执行远控代码。得益于安卓平台的开放性，热修复在安卓平台几乎无所不能，可以修复资源文件、修复代码，甚至连 so 库都可以修复，常用的框架有阿里系的 AndFix、Hotfix，腾讯系的 Tinker、QFix，还有美团的等等。这些本应用于动态修复 bug、免重安装修复 bug 的热修复框架，到了红队手中也是摇身一变，就好比张小泉的菜刀，切菜好用，摇身一变就是“中国菜刀”。最后再介绍一种动态掩盖特征的方法，那就是用 VA 来“加固”，VA 等多开工具将安卓系统与 VA 内的应用隔离，使得应用的静态特征被动态掩盖，目前已有广泛的恶意应用使用 VA 对自身重打包，重打包后的应用包名、软件名与原应用不同，从而逃过静态查杀。等到 VA 运行时，可以解密恶意应用 Apk，通过反射等技术欺骗安卓系统来运行未安装在系统中的 Apk，到这一步就跟正常的 App 无异了，VA 的本质就跟 Windows 平台上的壳技术差不多，先于恶意应用前运行，瞒过杀软之后，再将恶意应用释放出来运

在智能手机武器化方面得益于硬件性能的提升已经达到了一个新的高度，无论是电影里还是大家通常的认知当中，似乎总是有个固定的印象：黑客与电脑才是标配——仿佛只要给黑客一台电脑和一根网线，他就能自如渗透进任何一个目标网络。一名黑客只有用电脑才能施展他的技术吗？事实上，得益于 Android 系统的开源和开放性，许多的安全审计工作已经可以在强大的智能手机平台上完成。

得益于 Nethunter Rootless 的不断完善，安卓平台无需 root 即可运行 kail Linux 最多 85%的功能，如果带 root、三方 recovery 和 Kali 定制内核的完整版 Nethunter 即可运行完整的 Kali Linux 应用环境。能为 Android 设备增加无线破解、HID 攻击等硬件功能，以及 NMAP、SQLMap、Metasploit 等黑客工具，骇客可以使用它进行伪造 WIFi 热点、发动远程攻击，其功能一应俱全。除了上述工具外，黑客还可以把手机当做操作器，通过连接远程服务器的方式来发起网络攻击。虽然因为其屏幕小、手机代码阅读困难给黑客带来一定的麻烦，但这种攻击方式完全不

受具体系统或硬件设备的限制，具备较高的隐蔽性和机动性——上一分钟，还在咖啡厅里用公共 wifi 远程攻击了一个服务器，下一分钟，已经悠闲地端着一杯咖啡走在了回家的路上。

随着 5G 通信技术的发展，智能手机在人们生活中的地位只增不减，甚至有可能成为未来绝大部分普通用户唯一的网络终端设备，围绕着这一平台的网络攻防战还有很长的路。作为一名新时代信息安全的学生，我觉得我们应该关注未来安全研究热点，努力学习相关知识，为更安全的 5G 时代做出自己的贡献。