安全小课堂第八十二期【移动安全之APP加固】

原创：京东安全 京东安全应急响应中心 1月22日

移动互联网的火热，让移动APP的开发、运营、维护成为各企业抢占市场的“制高点”，但移动APP的安全保障也就成为一个不容忽视的重大问题。本期小课堂邀请到JSRC白帽子来讲解关于移动应用APP安全加固的那些事。

JSRC **安全小课堂第八十二期**，邀请到**骑虎打狗**作为讲师就**移动安全之APP加固**为大家进行分享。也感谢白帽子盆友的精彩提问与互动~

为什么app应用需要安全加固?

京安小妹

骑虎打狗:

app应用需要安全加固的原因，我觉得可以从两个方面来讲。一是人们上网习惯慢慢从PC端转向了移动端，越来越多的智能设备、移动终端、各种各样的应用app开始渗透生活的方方面面，其实它们很多就是我们所熟悉的Android/iOS应用，普及广泛必然黑产集聚，安全也就接憧而至。还有一个就是移动app的安全现状导致了一款app在发布时，必然要进行简单粗暴的安全加固。web安全一直老生常谈，web安全开发市场也相对饱和，但app的开发者深刻懂得安全的人也少之又少，这也是为什么有些不了解安全的中小app选择直接加壳做安全，简单粗暴。而有移动安全开发团队的大厂，如支付宝，则不需要用加壳来自慰，依然满满自信的裸奔在市场上。

讲师

app安全加固实现原理是什么呢？能不能简单介绍一下

京安小妹

骑虎打狗：

谈到app安全加固，就安卓来说，这里我只说一下加壳，一般加壳的侧重点就是对原始的dex/so/dll等进行隐藏、混淆、加花、代码抽离等操作，在程序运行过程中，对隐藏加密的原始dex再进行还原，以执行原有逻辑。现在普遍的认为Android的加壳技术根据强度分为4代：1整体的dex的加壳隐藏；2防调试防Dump出现；3方法体抽离；4.Vmp加壳/so加壳。无论哪一代，运行时解密不会变，所以即使是4代的字节码置换虚拟技术也可以在内存中修复，拿到完整的dex。至于ios加固，现在很多安全厂商的做法是Xcode插件，编译过程中对逻辑进行混淆、扁平化处理等方式。现在安卓加壳太普遍了，一般很多应用都是加壳了事

讲师

那加固是主要对哪几个地方进行加强的呢？

京安小妹

骑虎打狗：

从泛义来讲，app安全加固不仅仅是源码加壳，如果开发者的安全意识很强，加壳只是app安全很小的一个方面。

app我一般分类3类：Android、ios、h5（混合）

app安全加固也包括两个方面：

1.客户端本体的安全：四大组件安全、本地数据安全、WebView安全、安全配置、界面劫持、界面敏感信息显示、日志安全、内置账号泄露、测试信息泄露、手机密码安全、设备识别安全、环境清场

2.业务安全：Http/Https中间人攻击、手机验证码安全、数据封包弱加密、登录会话机制、用户信息泄露、敏感请求重放攻击、请求越权。

针对不同的安全点，可以采取的安全措施：加壳（dex/so）、文件校验（签名校验/dex/包体/特殊文件等）、不返回多余信息、不打印多余信息、封包验签、时间戳验证、https校验SSL证书、敏感数据不落地、对用户做好安全提示、敏感操作进行环境清场、敏感操作进行用户状态二次校验、手势密码做全局FLAG、设备绑定信息糅合多个因子等等

讲师

app进行安全加固有哪些作用?

京安小妹

骑虎打狗：

app安全加固的作用主要有：

1.防止被二次打包。二次打包的害处有：app原创技术被抄袭、界面被模仿，换了皮后被重新放到市场上；二次打包后方便黑客调试分析、跟踪关键逻辑；app被插入盗号木马，并流传在朋友圈、Q群、论坛、网盘等，影响公司形象；

2.安全加固最重要也是最终的目的是最大程度的保障业务安全，防止协议被脱端重写，防止业务活动被撸羊毛。

讲师

那师傅有啥比较好的app加固平台推荐的呢

京安小妹

骑虎打狗：

市面目前很多app加固平台，各大厂商也有免费的，像360、百度、腾讯乐固、网易盾、阿里聚安全。收费的有爱加密、梆梆、娜迦、几维、顶象科技。个人应用一般可以使用360的加固。对于实实在运营的企业app建议大家使用爱加密的收费版本，收费与免费的区别就是兼容性、应急响应、售后服务的有力支持。爱加密目前技术已经发展到双VMP（dex+so）多重加密，支持多种自定义加固，如防止模拟器运行、防止界面截图、防止界面劫持、本地数据强加密（sharedPerence/SQl数据）、防止内存Dump等，并且现在已支持强大的协议加密。

讲师

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心