长沙农村商业银行股份有限公司

APP安全加固平台项目需求

信息技术部

2021年2月

目 录

[一、项目背景 1](#_Toc3154)

[二、建设目标 1](#_Toc17223)

[三、建设内容 2](#_Toc10461)

# 一、项目背景

随着移动互联网的快速发展，移动APP已发展成为金融机构网上业务系统中非常重要的一部分。移动APP应用等对外业务应用的普及，扩展了我行原有的业务渠道及业务范围；而移动办公、掌上流程审批等企业内部管理类移动应用产品的不断推出，则丰富了我行的办公空间，提高了办公效率，减少了办公成本。

但与此同时，伴随着移动应用的大量使用，针对移动应用的网络犯罪近年发展迅猛。据普华永道《2018全球信息安全状况调查-中国内地与香港》调查数据显示：来自移动端的安全威胁已经成为企业的最大安全隐患。移动金融APP也成为了黑客的重点攻击目标，其所面临的安全威胁种类和数量也在不断增多。

为提高我行APP移动应用安全性，有效抵挡来自于恶意攻击者对我行互联网业务的恶意攻击，我部需统一规划并建设APP安全加固平台。

# **二、建设目标**

通过本项目平台建设，构建我行APP移动端的安全防护手段，初步建立起一整套纵深、立体化的移动应用安全防护体系，包括Android应用加固、iOS源码加固、HTML5加固、SDK加固及APP安全培训等。达到如下安全目标：

(1) 保障我行移动APP（Android、iOS、SDK、H5）源代码的安全性，避免被逆向分析、篡改、盗用等，保障我行APP移动应用客户端的安全性。

(2) 满足银保监会、人民银行、网信办等监管单位的监管要求。

(3) 建立并持续完善移动应用安全防护体系。

# **三、建设内容**

本次APP安全加固平台项目内容范围包括Android APP加固、iOS APP源码加固、HTML5加固、SDK加固及APP安全培训服务等。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **模块** | **序号** | **功能分类** | **功能描述** |
| 一 | APP安全加固平台 | 1 | Android APP加固 | ①支持通过多DEX文件加密、DEX整体加壳、DEX分离加壳、DEX代码VMP保护等方式，实现DEX文件保护。  ②支持通过SO库文件加壳、SO库高级混淆、SO Linker、SO防调用、SO虚拟化保护等方式，实现SO库文件保护。  ③支持通过DEX文件防篡改、SO库文件防篡改、H5代码防篡改、DLL文件防篡改等方式，实现代码防篡改。  ④支持通过assets资源防篡改、res资源防篡改、AndroidManifest配置文件防篡改等方式，实现资源防篡改。  ⑤支持通过签名文件保护等方式，实现签名防篡改。  ⑥支持通过防动态调试、防进程调试、防内存代码注入、防内存dump、防加速器、防止模拟器运行等方式，实现反调试。  ⑦支持通过防内存数据读取、防内存数据修改、防日志泄漏、本地数据加密等方式实现数据防泄漏。  ⑧支持通过应用防截屏、应用防劫持等方式，实现页面数据保护。  ⑨支持通过加固后APK体积压缩等方式，实现加固后体积压缩等。 |
| 2 | iOS APP加固 | ①支持通过控制流引入/跳转指令插入、基本块调度、指令多样化、基本块分裂、控制流扁平化、控制流间接化、敏感字符串加密、代码虚拟化保护等源代码混淆方式，实现代码保护。  ②支持通过IOS应用动态防护等方式，实现iOS安全防护等。 |
| 3 | SDK加固 | ①支持通过JAR包分离加壳、JAR代码VMP保护等方式，实现JAR包代码保护。  ②支持AAR包加固。  ③支持通过SO库文件加壳、SO库高级混淆、SO Linker、SO防调用、SO虚拟机保护等方式实现SO代码保护。  ④支持通过防Java层调试、防native层调试等方式，实现防调试。  ⑤支持SDK防第三方调用等。 |
| 4 | H5加固 | ①支持通过常量字符串加密、常数加密、加壳保护等方式，实现代码加密。  ②通过二元表达式加密和指令等效转换、控制流平坦化、代码压缩和函数变量名混淆、基本块分裂、垃圾指令注入、JS代码虚拟化等方式，实现代码混淆。  ③支持多态变异模式、禁止控制台输出、防调试、JS域名绑定保护等H5综合防护功能。 |
| 5 | 兼容性要求 | 运行性能：  ①对应用安装包大小，内存占有率，CPU占有率的影响，不能降低用户体验。加固后的应用包应采取压缩技术，实现加固后包体增量为-5%至5%以下。  稳定性：  ②加固程序的稳定性要有保证，应用崩溃不应该是由于加固程序造成的。  适配性：  ③应用需要适配主流的移动操作系统，包括国内主流厂商的定制系统。  ④适配各种分辨率和屏幕尺寸。  ⑤需提供兼容性适配报告。 |
| 6 | 部署方式 | 要求APP加固平台本地化部署在招标人内部网络中。 |
| 7 | 授权使用方式 | 按应用进行授权加固，不限制应用的具体类型和数量（包括但不限于Android APP、IOS APP、SDK、H5），且应用在质保期可无限次加固。 |
| 二 | APP安全培训服务 | 1 | APP安全开发培训 | 从移动应用开发过程中的编码环节入手，对风险点进行讲解，并详细介绍防范措施的技术原理、针对常见移动应用中常见的业务风险进行实例分析。 |
| 2 | APP安全编码培训 | 对开发过程中，编码可能产生的漏洞风险进行讲解介绍。 |
| 3 | APP安全测试培训 | 移动APP常见漏洞测试培训，让培训对象掌握安全测试的技巧及方法，对产品进行安全测试或渗透测试。 |