客户端安全解决方案介绍

2015/6/27

广州江南科友科技股份有限公司

目录

1 背景

随着智能移动终端和互联网金融的飞速发展，以手机银行、手机理财工具、第三方支付为代表移动支付越来越普及。

根据《腾讯移动安全实验室 2014 第一期手机支付安全报告》统计：截止到 2014 年第一季度，第三方支付类、电商类、团购类、理财类、银行类这五大手机购物支付类 APP 下载量在迅猛增长。统计发现，手机支付购物类软件共有 364 款，其下载量占全部软件下载量的 30.38%。

移动支付在给社会带来方便、快捷的同时，也带来了不少安全隐患。

根据《腾讯移动安全实验室 2014 第一期手机支付安全报告》统计：2011 年、2012 年、2013 年，腾讯手机管家截获的手机病毒包分别为：25404 个、177407 个、763351 个。2012 年是 2011 年的 6.98 倍、2013 年截获的手机病毒包是 2011 年的 30 倍。2014 年第一季度,截获手机病毒包数 143945 个，感染手机病毒用户数达到 4318.81 万。其中,手机支付类病毒呈现突飞猛进的发展势头。

江南科友对移动客户端具有代表性安全攻击方式进行了分类：

- 病毒与木马——操作系统层面

  恶意程序后台自动运行。主要有以下几种攻击方式：

  - 按键截获

    通过钩子钩住系统键盘接口、输入法键盘接口等手段截获用户按键信息；

  - 屏幕截获

    通过后台录像或记录显示屏输入坐标的方式盗取用户密码、账号信息；

  - 短信攻击

    通过拦截支付过程的验证短信、后台发送验证短息的方式盗取账户资金。

- 山寨应用（又称二次打包或静态注入）——app 层面

  攻击者修改正版 APP 生成山寨应用冒充正版侵害用户合法权益。

  主要攻击方式分为以下两种：

  - 本机交易

    攻击在用户的手机上进行。山寨 APP 通过修改数交易数据的金额、收款账号的

方式直接在用户的手机上完成盗取资金的全部过程。

- 骗取密码后，换机交易

攻击者在用户手机上盗取账号、密码等关键信息后通过网络或者短信发送给入侵者，入侵者在其他手机上完成资金窃取。

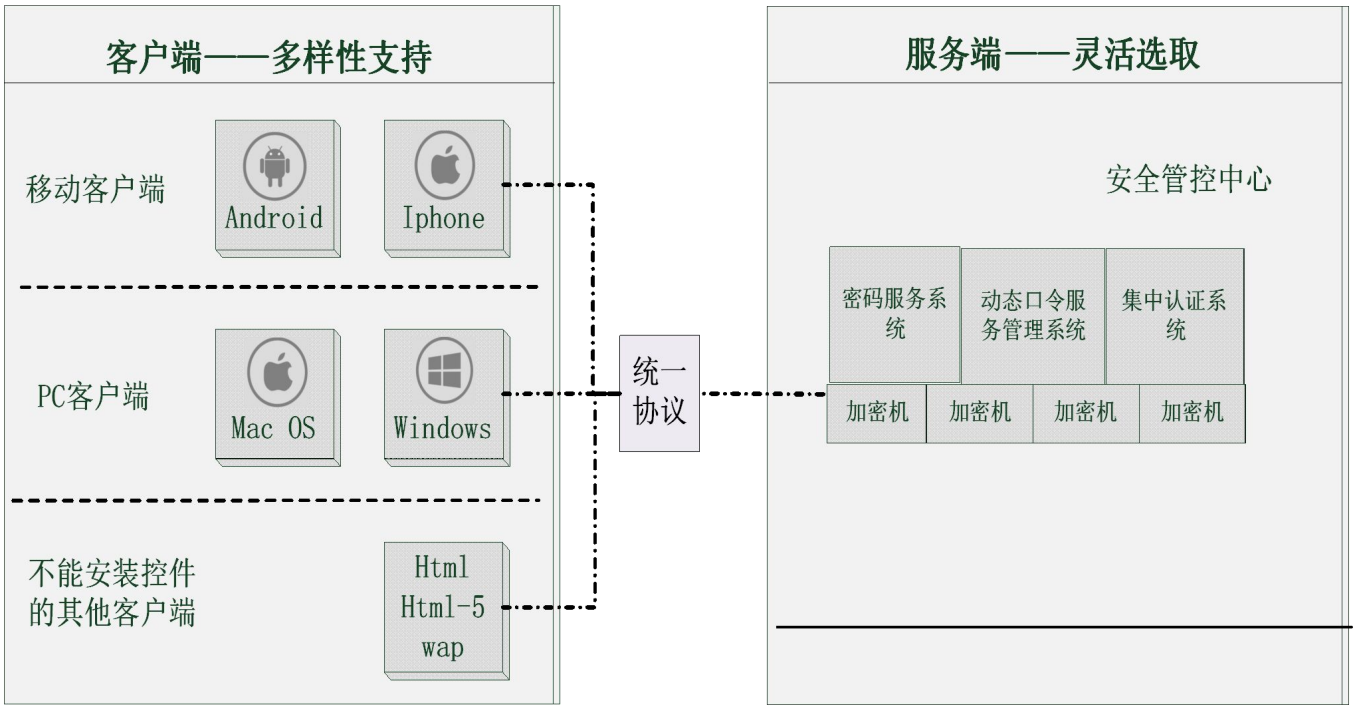
➢ 网络攻击——网络层面

入侵者通过提供免费 wifi 或者伪装公用 wifi 等方式从网络数据包中盗取敏感信息、修改交易内容等方式侵害 APP 用户的利益。

在此背景下，广州江南科友科技股份有限公司设计实现了完整有效的客户端安全解决方案。该安全解决方案有如下特点：

2 客户端安全总体解决方案

2.1 总体结构图



2.2 说明

- **客户端多样性支持**

  江南科友客户端安全解决方案支持各种客户端，包含：

  - 移动客户端——Android & IPhone

    科友提供移动客户端 app **安全开发套件**，对于 android 客户端另提供**安全外壳**。

  - PC 客户端——Mac OS & Windows

    PC 客户端安全用浏览器安全插件实现。

  - 其他客户端——不能安装控件的其他客户端环境

    - 手机 wap 环境
    - 跨平台的 Html-5 应用
    - 其他纯 Html 客户端环境，如电视支付等

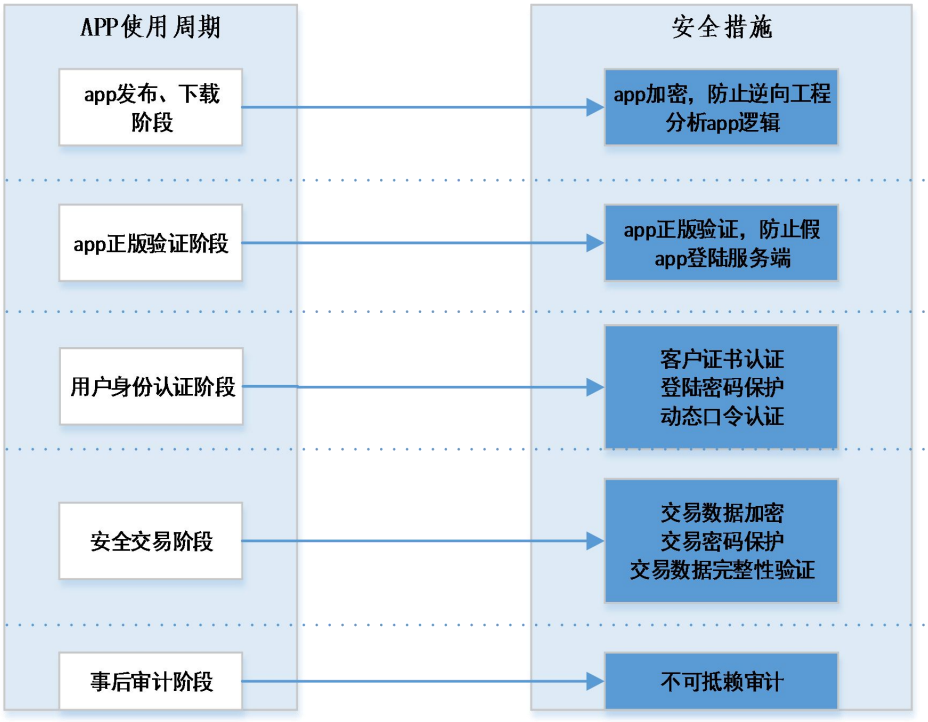
      针对该类客户端环境，提供 JavaScript 开发套件。

- **服务端灵活选取——**根据客户端现有环境灵活对应服务端结构：
  - 安全管控中心包括：密码服务系统、动态口令服务系统、集中认证系统
    - 密码服务系统负责密码认证和交易安全
    - 动态口令服务系统负责客户端动态口令的验证
    - 集中认证系统负责证书管理和验证

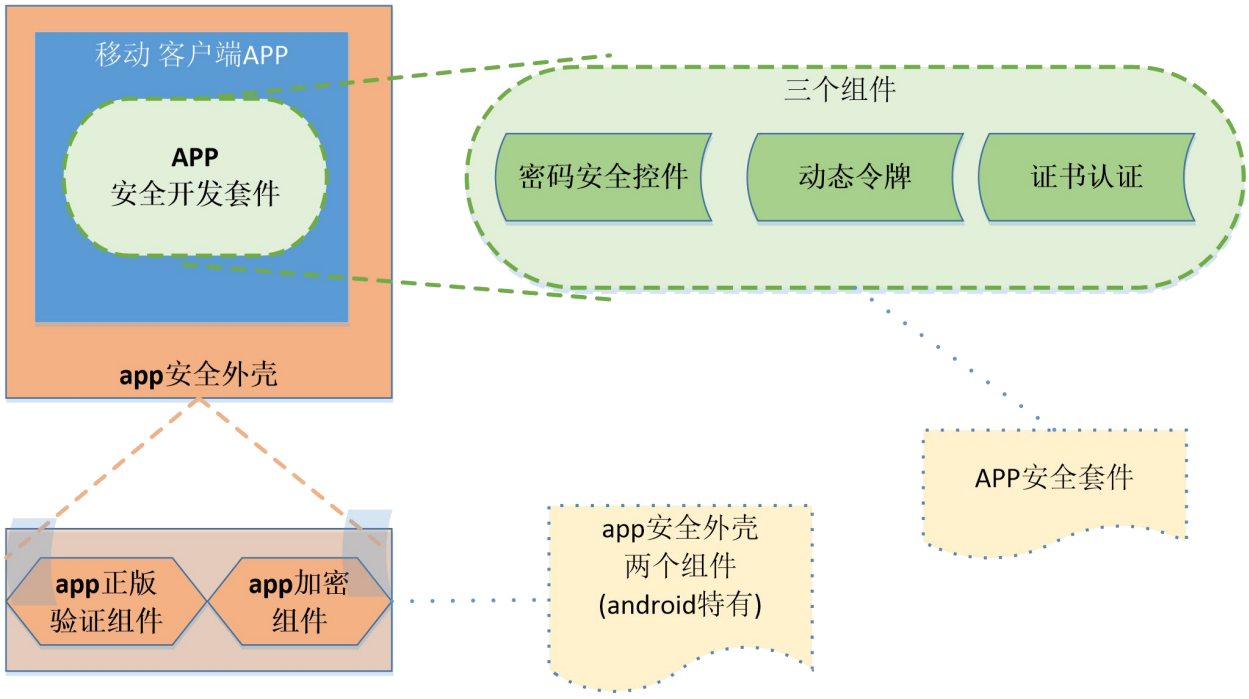
3 移动客户端安全方案

3.1 移动客户端安全总体策略

江南科友移动客户端解决方案为移动 APP 发布下载、认证、交易、网络传输、事后审计等整个使用周期实施了全方位的安全防护。



3.2 移动客户端安全方案说明



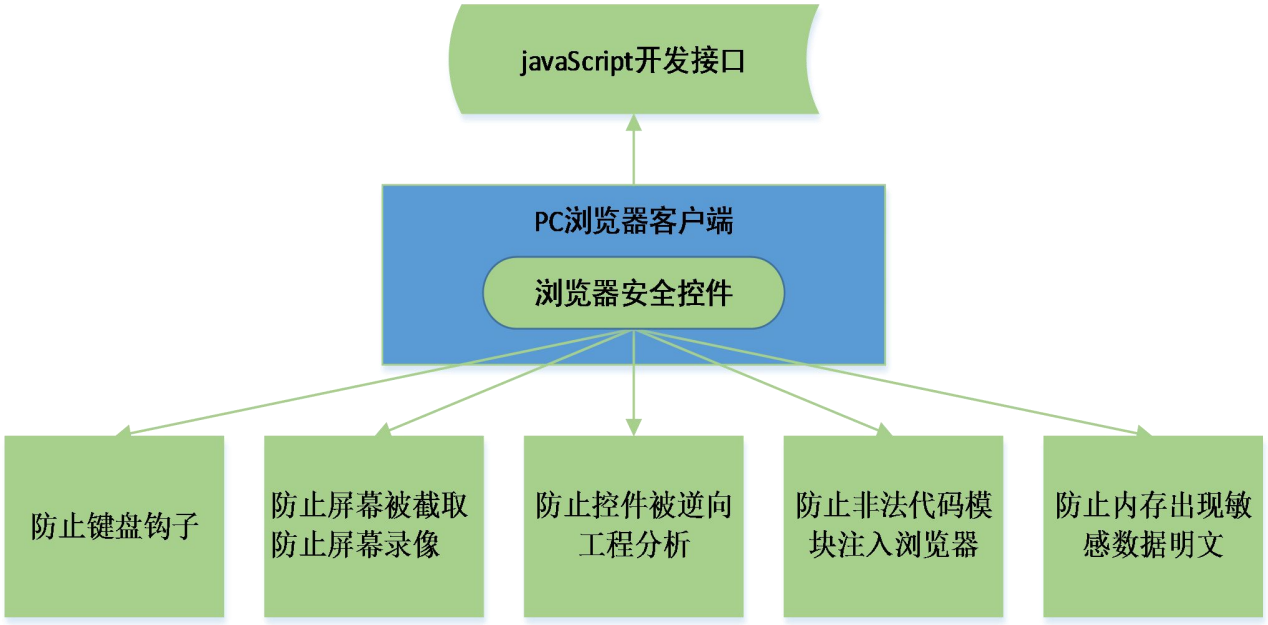
移动客户端安全方案说明			
分类	**组件**	**功能简介**	**备注**
APP 安全 套件	密码安全控件	自绘随机键盘，为 app 输入密码提供安全的环境	针对 Android 和 Iphone 的 APP 应用
		防止后台进程对屏幕录像盗取机密数据	
		防止恶意程序勾取系统键盘接口盗取机密数据	
		防止恶意程序读取 android 系统文件记录每次按键坐标后重现敏感数据	
		敏感数据加密	
	动态令牌	提供动态口令身份验证	
	证书认证	提供基于 x509 的证书申请、身份验证、证书签名验签功能	
APP 安全 外壳	APP 正版验证组件	验证 app 的完整性，防止二次打包后的伪 app 连接服务端	仅针对 Android APP 的应用
	APP 加密组件	对整个 app 加密，	

		防止逆向工程、代码动态注入等。	

4 PC 客户端安全

4.1 PC 客户端安全策略总览

提供浏览器安全控件保证客户在 PC 机浏览器上的信息安全。分为 Windows 版本和 Mac OS 版本。



4.2 PC 客户端安全模块意义

PC 客户端安全模块意义			
模块分类	**安全作用**	**原理说明**	**工作层次**
Windows 浏览器安全控件	键盘钩子防护	拦截键盘钩子、定时发送干扰键	应用层、驱动层
	防止屏幕被截取 防止屏幕录像	拦截录屏功能	应用层、驱动层
	防止非法 dll 模块注入浏览器	检测 dll 黑名单,定时清楚黑名单中 dll	应用层、驱动层
	防止控件 dll 被逆向工程分析	Dll 安全混淆加壳	Dll 安全混淆加壳
	防止内存出现敏感数据明文 敏感数据加密	前台键盘驱动层和后台统一编码、加密	前台键盘驱动层和后台统一编码、加密

Mac OS 浏览器安全控件	敏感数据加密	前台控件和后台统一编码、加密	应用层

5 产品清单

说明：

- ✧ 下表中每个无背景颜色方格表示一个独立的客户端产品模块；
- ✧ 每行表示一个功能模块，每列表示一种客户端环境，产品可以按列或按行的方式组合；
- ✧ “A-”表示 Android 平台，“I-”表示 Iphone 平台，“H-”表示 Html/Wap/Html-5 平台；
- ✧ 下表只描述了客户端产品清单。

客户端安全产品清单					
操作系统 / 产品（组件）	**Windows**	**Mac OS**	**Android**	**Iphone**	**Html/Wap/ Html-5**
密码安全控件	Windows 浏览器密码安全控件	Mac OS 浏览器密码安全控件	A-密码安全控件	I-密码安全控件	H-密码加密开发包
动态口令	硬件令牌	硬件令牌	A-动态口令模块	I-动态口令模块	不需要
证书认证	usb-key	暂无	A-证书认证模块	I-证书认证模块	不需要
APP 加密组件	不需要	不需要	APP 加密组件	不需要	不需要
APP 正版验证组件	不需要	不需要	APP 正版验证组件	不需要	不需要

6 兼容性

客户端兼容性	
模块分类	**兼容性**
Windows 浏览器 **安全控件**	浏览器：支持 ie/firefox/chrome/qq 浏览器/360 浏览器/遨游浏览器/uc 浏览器等 操作系统：支持 xp vista win7 win8，支持 64 位和 32 位两个版本
Mac OS 浏览器 **安全控件**	浏览器：支持 safari 浏览器 操作系统：支持 mac 10.5 到 mac 10.10 版本, 支持 64 位和 32 位版本
Android（所有模块）	操作系统：支持 android 4.0 到 android 5.1 密码安全控件 UI：提供 UI 二次开发接口修改 UI 风格，可与任何 UI 风格兼容
Iphone（所有模块）	操作系统：支持 ios 6 到 ios 8.4 版本 密码安全控件 UI：提供 UI 二次开发接口修改 UI 风格，可与任何 UI 风格兼容
Html/Wap/Html-5	支持能够使用 JavaScript 的所有环境