平台级金融安全-移动安全OS

By e4gle
Sudo Team
http://www.sudo-team.com
1949479@qq.com

xKungfoo 2015

目录

- 目前主要的移动安全威胁分析
- 针对金融领域的主要的解决方案
- 提出一个安全移动OS平台级的技术方案

目前主要的移动安全威胁

应用安全威胁

- 金融支付威胁
- 企业业务威胁
- 个人应用威胁 - 游戏。。。
- 个人隐私

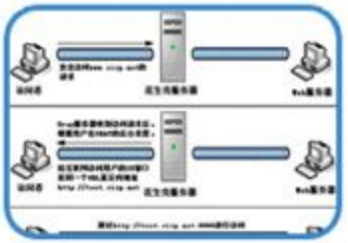
数据安全威胁

- 个人隐私数据
- 企业业务数据

金融类移动安全分析

界面劫持

二次打包



服务器地址被盗取或篡改

存档修改

盗取用户名、密码

2013年移动金融安全问题爆发，出现了“洛克蠕虫”、“银行悍匪”等高危的银行支付类病毒。此类病毒能够专门针对手机银行端窃取用户帐号密码。同时，为了更好的规范银行手机支付，中国人民银行、中国银行业监督管理委员会也制定了一系列的移动金融的安全规范和安全评估要求，强调移动银行的安全，需要从根本上杜绝安全支付风险，比如键盘防止输入法攻击、监听短信，窃取通话记录，读取手机中安装的购物客户端、银行客户端等等。

界面劫持

二次打包


1、某应用市场
2、某度推广
某 du 推广
3、流氓软件绑定模块
下载经过二次打包的APK
PROCESSING
监听内存
数据库
私密文件

对于消费者的安全威胁

移动安全的两大隐患

应用对应用的攻击

应用对数据的攻击

一个恶意的APP可能产生的威胁

主要解决方案


应用层：
应用源审核与检测、APP加固
平台层：
卫士级应用、双系统
硬件层：
强身份鉴别、trustzone、Tee
普适性增加

目前的平台级方案存在的问题

移动应用安全组件：APPseparator

By Sudu team
http://sudu-team.com

xKungfoo 2015

APPseparator- 增强的应用加密沙箱

- 沙箱的概念首先是隔离文件系统，限制APP之间的数据访问来增强安全性
- 安卓的原生沙箱基于用户ID，利用了Linux原有的DAC机制进行的隔离
- Sd卡的数据仍然混存，由于sd卡上的文件权限设置不是很严谨，容易产生数据安全问题
- 由于安卓原生APP的数据没有完全被沙箱隔离，所以也会随着系统的运行产生大量垃圾数据，app卸载不干净，影响系统运行效率

APPseparator- 增强的应用加密沙箱

APPseparator- 增强的应用加密沙箱

APPseparator- 增强的应用加密沙箱

APPseparator- 增强的应用加密沙箱

移动应用安全组件（实验）：APPcontainer

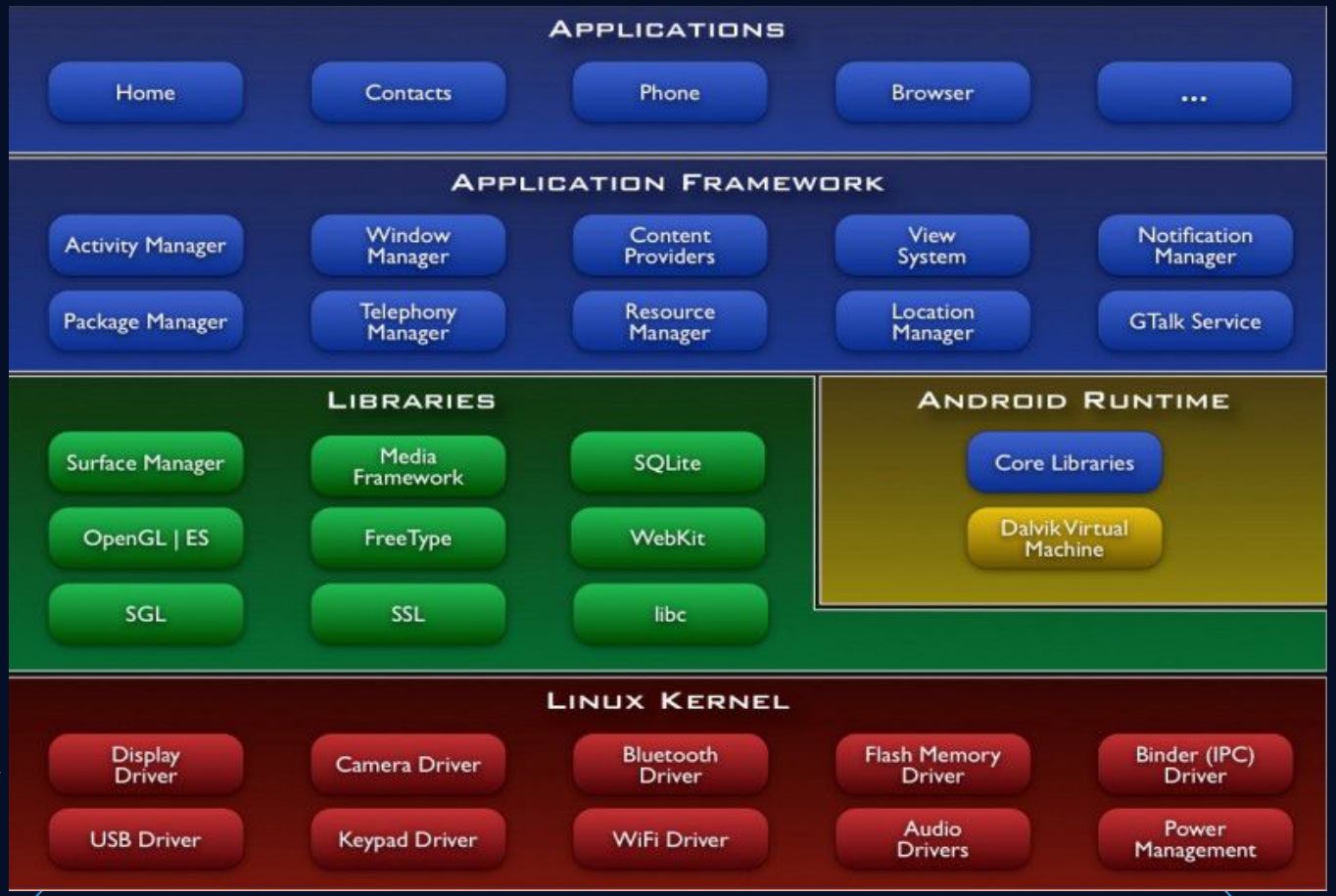
By Sudu team
http://sudu-team.com

xKungfoo 2015

APPcontainer- 移动应用安全容器

- 和Docker不同的是我们需要在移动系统中实现应用容器，则需要在框架层以及内核层针对安卓应用的特性进行隔离。

隔离四大组件
隔离应用资源



内核层的支持
SELinux

APPcontainer- 移动应用安全容器

支付容器




社交容器



非安全容器

APPcontainer- 移动应用安全容器

基于android的安全移动OS：GOS

By Sudu team
http://sudu-team.com

xKungfoo 2015

GOS

更多探讨请访问项目网站及加微信进行深度技术交流

By Sudu team

http://sudu-team.com

微信：kiwiai

xKungfoo 2015