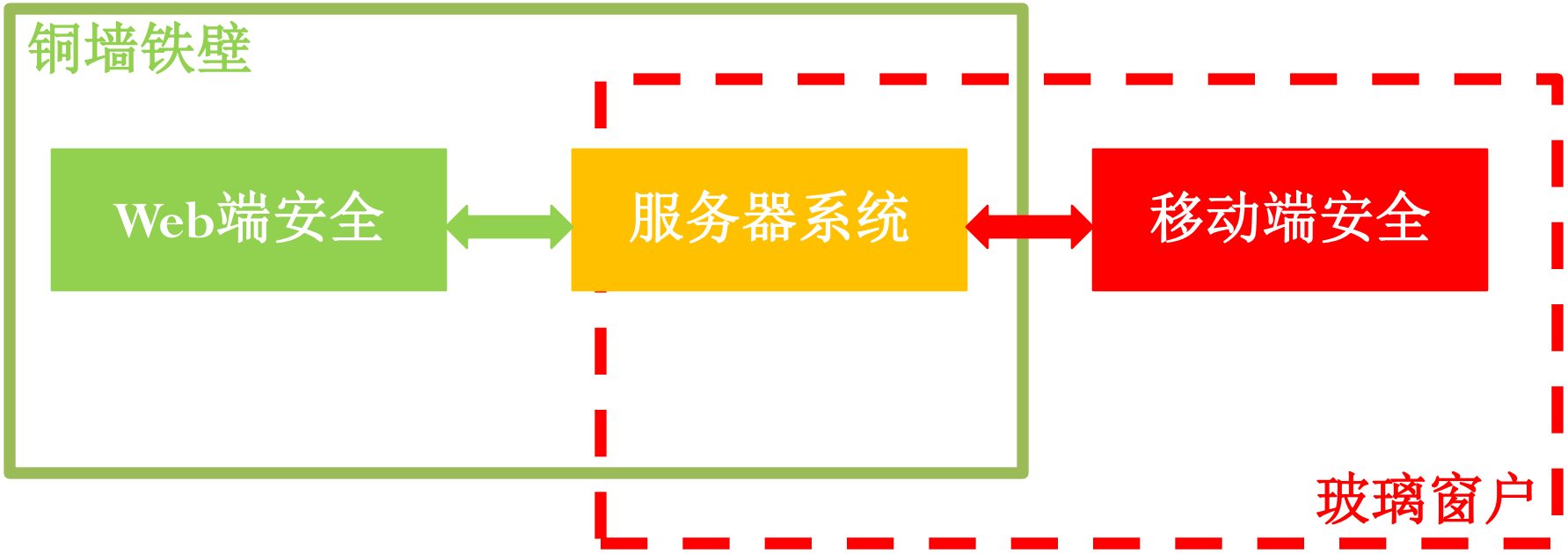
移动安全支付攻防浅析

火点(陈家林)
鲶鱼团队（安卓安全小分队）

议题

- 攻击在哪里？
- App能做什么
- 系统能做什么
- 硬件能做什么

攻击在哪里



即便Web安全防护如铜墙铁壁，由于移动端安全的弱化，等同在坚固的铜墙铁壁上，新开了一个易碎的玻璃窗户，给交易系统带来极大风险。

攻击类型

- 二次打包
- 虚假应用钓鱼
- 短信木马
- DNS劫持，WIFI钓鱼
- 系统输入输出劫持
- 浏览器攻击（Webview提权）

App能做什么

- 签名验证（本地和远程）
- 加固
- 防注入
- 防调试
- 安全键盘

360安全支付模块
盗版网银识别
木马病毒查杀
网络环境监控
支付环境监控
网址安全扫描
二维码扫描监控
短信加密认证

关于签名验证

- App启动，读取apk签名
- 计算hash（MD5，SH1A）
- 上传服务器检验
- 返回错误则停止运行，封号

字符串未加密，代码特征明显

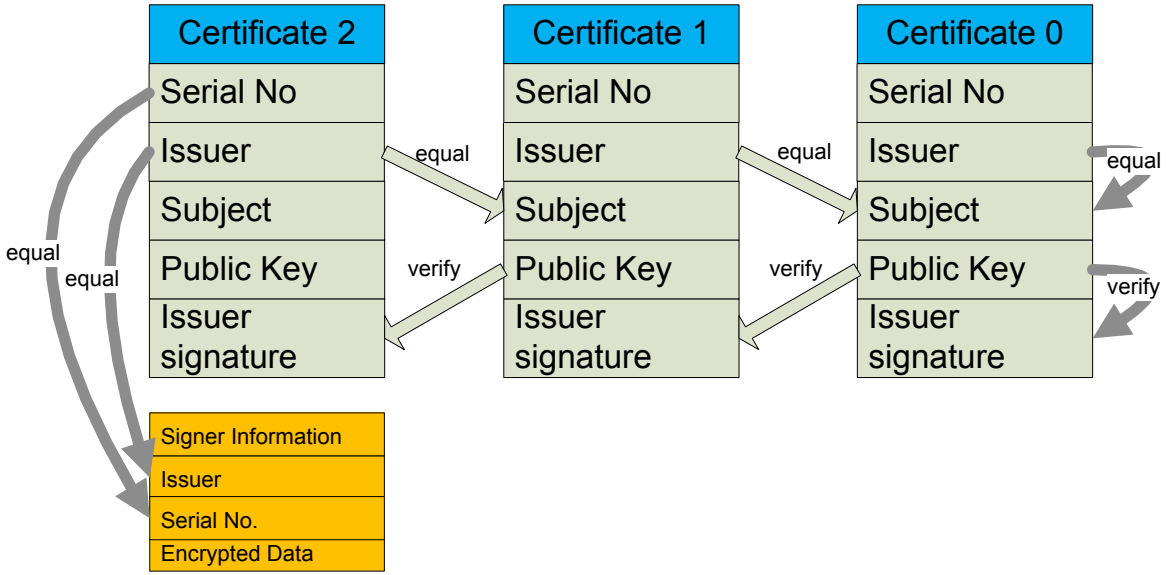
Log未加密，打开log一目了然

函数名有signature，太明显

QQ签名验证被绕过的故事

关于签名验证

- Android系统签名漏洞，就遭殃了

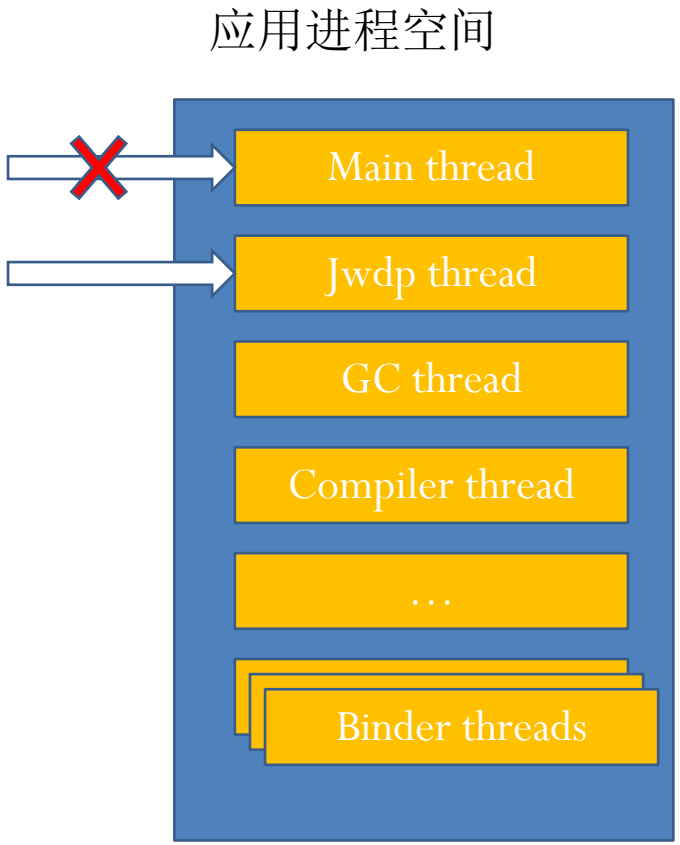


安卓“假ID”签名漏洞，竟然骗过了支付宝和360

- http://blog.csdn.net/android_squad/article/details/41653171
- http://www.csdn.net/article/2014-08-07/2821107-Android-Fake-ID-Bugs

关于防注入

- 你根本无法阻挡动态调试
  - 一个线程只能ptrace一次
  - 任意线程都可以ptrace
  - 线程间数据共享
  - 然后，没有然后了…



关于安全键盘

- 自带随机键盘并不安全，同样可以被劫持

系统能做什么

- 第一时间OTA更新Google security patch
- SE Linux Policy增强，缩小攻击面
  - 举例：install-recovery.sh

系统能做什么

- 输入输出子系统的保护

输入节点

```
root@[redacted]/dev/input # ll -Z
crw-rw---- root     input             u:object_r:input_device:s0 event0
crw-rw---- root     input             u:object_r:input_device:s0 event1
crw-rw---- root     input             u:object_r:input_device:s0 event2
crw-rw---- root     input             u:object_r:input_device:s0 event3
crw-rw---- root     input             u:object_r:input_device:s0 event4
crw-rw---- root     input             u:object_r:input_device:s0 event5
crw-rw---- root     input             u:object_r:input_device:s0 event6
crw-rw---- root     input             u:object_r:input_device:s0 event7
crw-rw---- root     input             u:object_r:input_device:s0 event8
crw-rw---- root     input             u:object_r:input_device:s0 mice
crw-rw---- root     input             u:object_r:input_device:s0 mouse0
```

输出节点

```
root@[redacted]:/dev/graphics # ls -al
crw-rw---- system   graphics  29,   0 1970-02-19 11:31 fb0
crw-rw---- system   graphics  29,   1 1970-02-19 11:31 fb1
```

系统能做什么

- 但是Root在所难免，那就让Root破坏降至最低

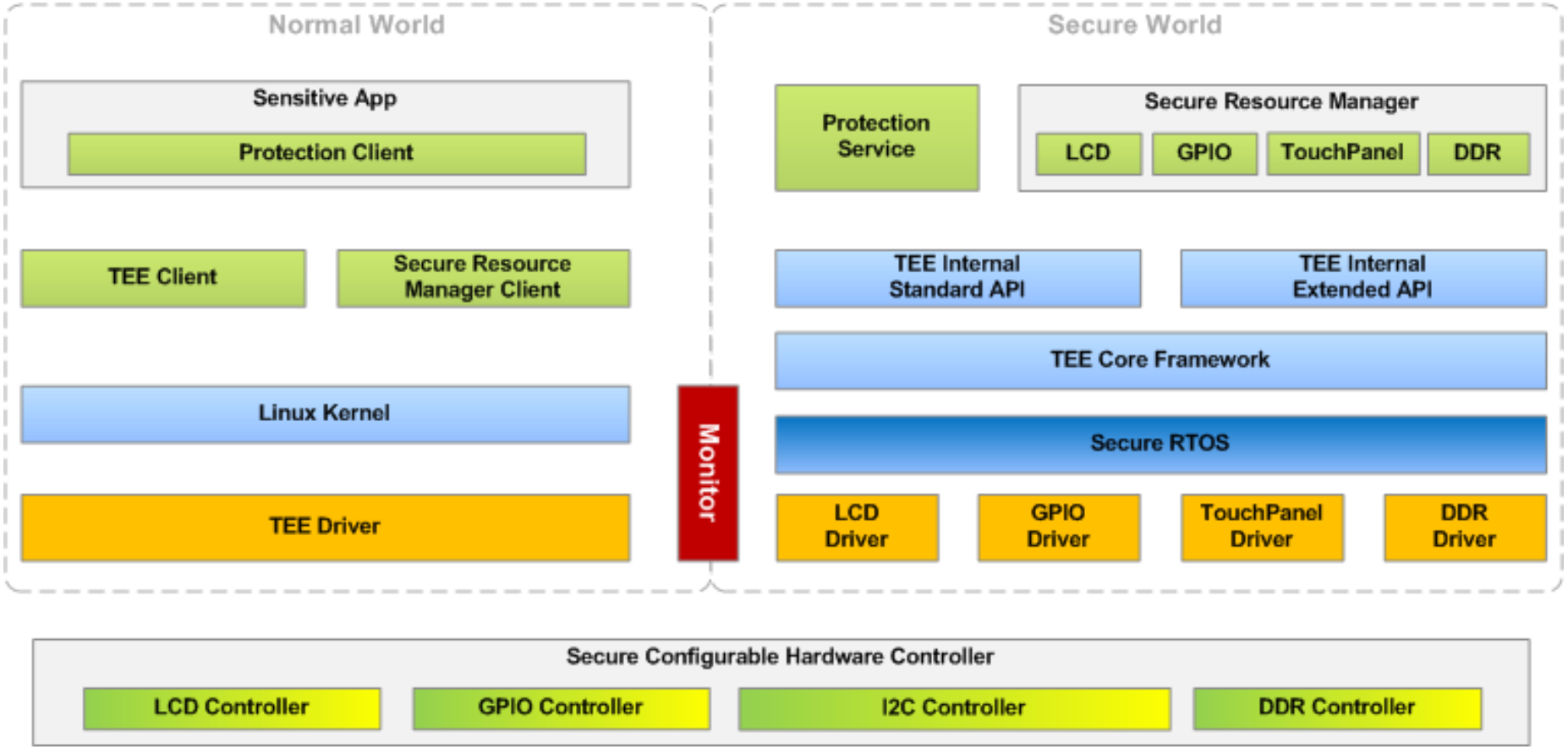
手机厂商	Root检测方案
厂商1	双进程Root检测，利用linux文件系统inotify机制监听system分区变化，root标记写入加密分区，开机显示
厂商2	限制mount系统调用，Root之后也无法将system分区mount成rw
厂商3	限制shell root，几乎不能干任何事情

系统能做什么

- 验证码短信保护
- 4.4之后，短信拦截需要默认短信，攻击和保护都被拒之门外

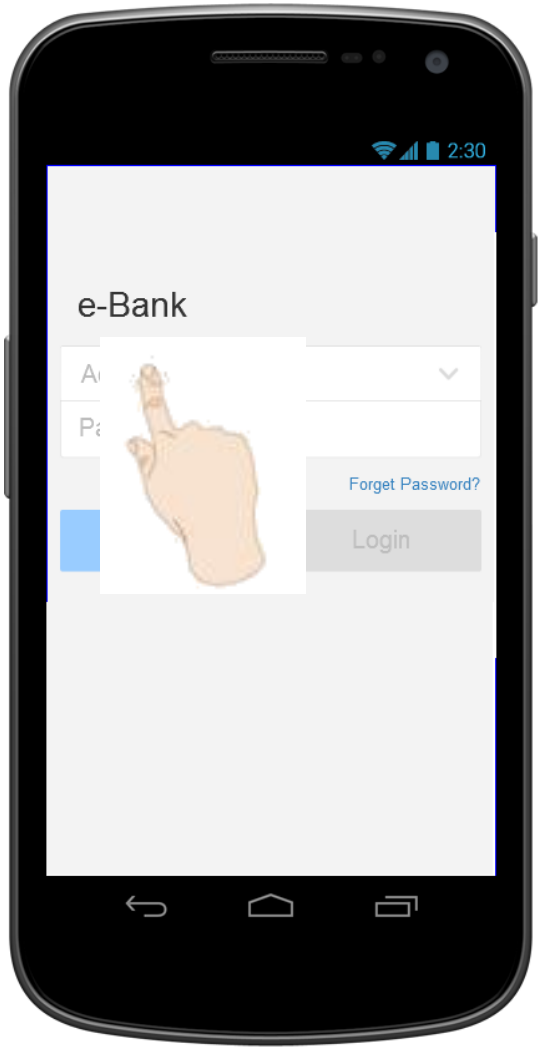
Demo

硬件能做什么 – TrustZone/TEE

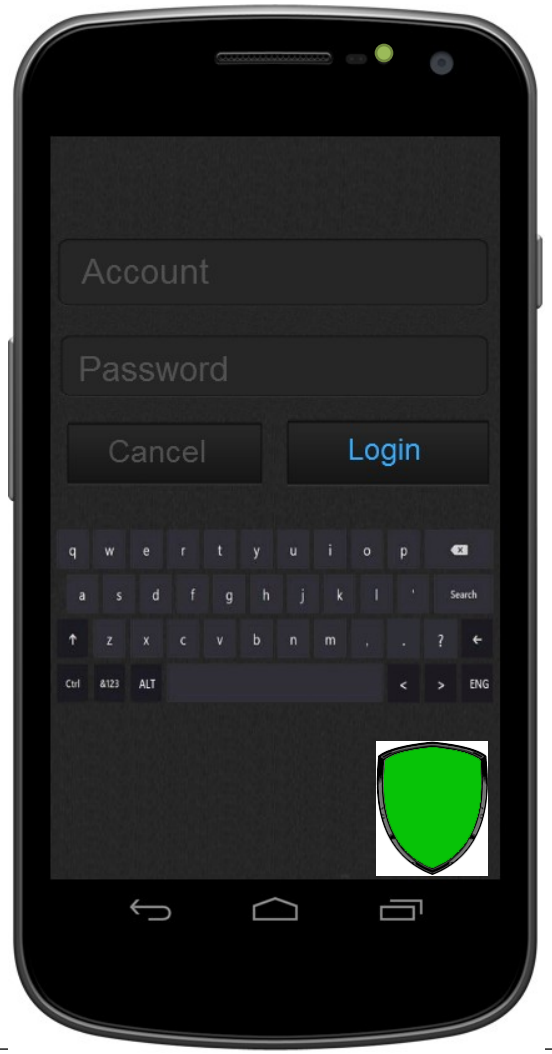


硬件能做什么 – 安全输入

Normal World



Secure World



谢谢

微博：鲶鱼团队

博客： http://blog.csdn.net/android_squad