金融移动应用安全解决方案

Financial security solutions for mobile applications

Xkungfoo+北京娜迦信息科技发展有限公司

xKungfoo 2015
www.nagapt.com

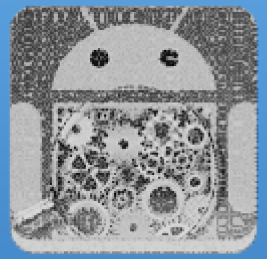
全方位安全服务

◆全面深化检测移动应用，一站式完成各种安全审计测评，针对性评估，定制化服务。

移动原生应用 真机兼容性评测

- 270台真机全天候测试原生应用的兼容性测试，更好的解决应用加固前的各类问题；

移动原生应用 安全审计评测



- 涵盖所有移动安全检测服务项，有效控制安全风险，从代码审计到业务逻辑安全环环相扣；

服务器 安全审计评测

- 对服务器进行全面审计，多层针对化解决安全隐患，专有通讯加解密服务器定制，提供优化建议措施，让系统运行更快速，更安全；

安全性

一站式安全审计评测

兼容适配的重要性

- 270+台真机全天候测试原生应用的兼容性测试；

- 标准化制式适配性报告

云测性能报告

性能概况		安装耗时	启动耗时	CPU占用	内存PSS	
	平均值	30.9s	6.2s	6.49%	58.89MB	
	最大值	259.62s	12.07s	100.00%	415.34MB	
	(手机型号)	三星 GT-S5830 2.3.4	TCL W989 2.3.7	天语 T60 4.2.2	三星 SM-N9106W 4.4.4	

云测终端测试报告

加固通过：565台	加固失败：9台	总测试台数：574台	通过率：98.43%

通过机型

摩托罗拉 XT685 4.0.4	努比亚 NX501 4.2.2	摩托罗拉 MT680 2.3.7	博瑞 T5 4.2.2
欧奇 A30圣琴 4.2.2	三星 GT-I8552 4.1.2	尼采 A700 4.2.2	橙石 WA1 4.4.4
三星 GT-I8558 4.2.2	三星 GT-I9152 4.2.2	三星 GT-I9082i 4.1.2	飞利浦 I908 4.4.2
三星 GT-I9152P 4.3	三星 GT-I9502 4.4.2	三星 GT-I9295 4.4.2	华为 C8813 4.1.1
三星 GT-I9508 4.4.2	三星 GT-S7568I 4.1.2	三星 GT-P3100 4.1.2	华为 G520-5000 4.1.2
三星 GT-P7510 3.2	三星 SCH-I879 4.1.2	三星 GT-S7562i 4.0.4	华为 G730-U00 4.2.2
三星 GT-S7898I 4.1.2	三星 SGH-T989 4.0.3	三星 SCH-I829 4.1.2	华为 MT2-L05 4.2.2
三星 SCH-i919 2.3.6	三星 SM-G3588V 4.3	三星 SCH-P729 4.2.2	华为 T8951 4.0.4

未通过机型

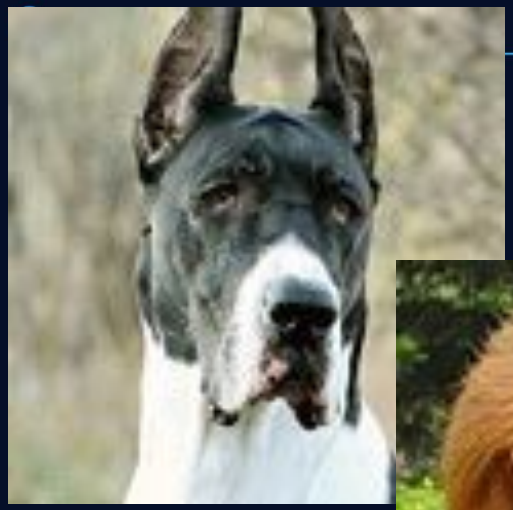
奇酷 QO M1 2.3.5	TCL W989 2.3.7	琦基 I9220M 4.1.1	索爱 LT18i 2.3.4	圣柏 S138 4.1.2
HTC A510c 2.3.3	LG C660 2.3.4	摩托罗拉 MZ606 3.1	海尔 HT-IT10 2.3.5	

真机终端测试报告

客户端名称		客户端版本号		完版本号			
测试机型		通过机型数量		通过率			
项目经理签名			时间				

编号	类型	测试机型	版本号	是否正常	现象	备注	曾出问题机型	重要机型
1		nexus 9	5	正常				
2	nexus	nexus 6	5	异常	输一锁后未响应	黑包无响应		
3		Nexus 5 （ART）	4.4.4	正常				
4		三星 GT-I9508	阿里云	正常			是	
5		三星 i9023	4.4.4	正常				
6		三星 SM-N9150	4.4	正常				
7		三星 SM-N9006 Note3 非定制版	5	正常				
8		三星 SM-G9006V s5 联通4G	4.4.2	正常				是
9		三星 SM-G9008V s5 移动4G	4.4.2	正常				是
10		三星 S7898	4.1.2	正常				
11		三星 I9105p	4.1.2	正常				
12		三星 I9250	4.3	正常				
13		三星 I9228	4.1.2	异常	通讯超时			
14		三星 GT-N7100	4.1.2	正常			是	
15		三星 Galaxy Nexus	4.2.2	正常				

安全的回归-野性的呼唤



D-DOG

E-DOG

G

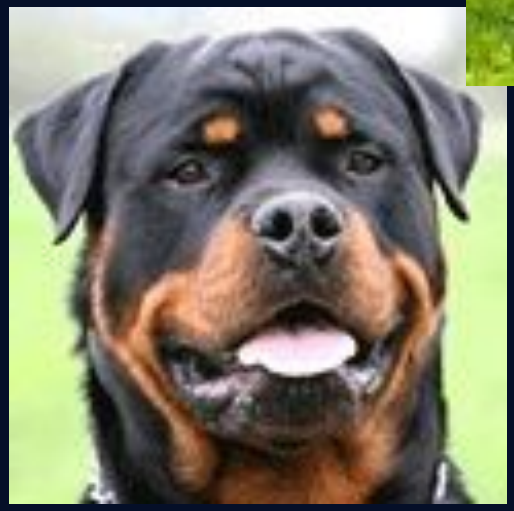
G

G

DOGS

L-DOG

F-DOG



“解剖”APK - DEX篇

D-DOG DEX类加载器

- ✓ 对Dex进行整体加密，内存中整体解密；

“解剖”APK - DEX篇

E-DOG DEX类抽取

- ✓ 对Dex的类进行抽取加密，在运行时进行分段解密；

“解剖”APK - DEX篇

DEX类加载器　　DEX类抽取

NAGA-　　前世今生

为什么有这么高的兼容性？！！

每天奋战14个小时　　连续坚持24个月

“解剖”APK - SO篇

T-DOG DIS原理 - 链接器

读取loader与被保护目标的符号表，字符串表与重定位表

按照Android的哈希规则重新组合loader与目标文件的符号表与字符串表

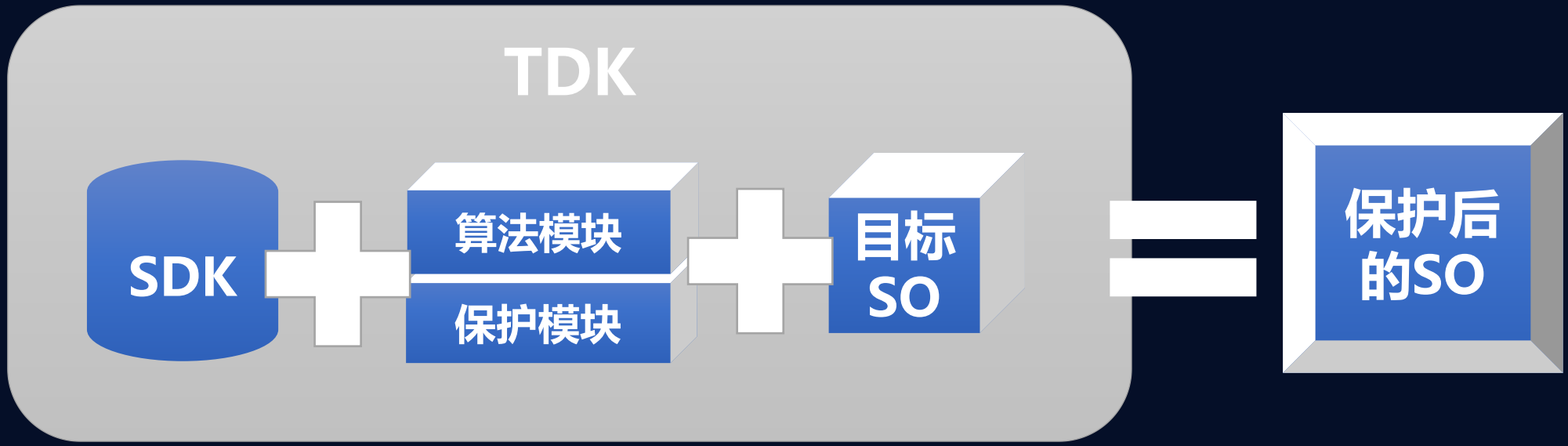
将两个so的代码段合并到一起

合并两个so的重定位表，并修复重定位项到新的基地址

修订动态段中的符号表，字符串表以及重定位表的指向

“解剖”APK - SO篇

T-DOG TDK介绍及原理



- TDK是安卓native层sdk，是向开发者提供快捷方便安全的native层的保护设计。

✓无需介入 ✓自定义设计 ✓高效融合

“解剖”APK - SO篇

C-DOG 自定义加解密函数

多种可选加解密函数

涵盖国内外加解密算法

✓ AES,DES,RSA,SM1,SM2,SM3等

定制化加解密函数

✓ 使用自定义加蜜接口和解密接口

“解剖”APK - SO篇

L-DOG

可定制化壳模板

转化为
高级语言

不同版本随机生成C++代码

V1.0 V2.0

模板随版本变化而随机变化

“解剖”APK - SO篇

F-DOG 动态反调试

安全加固后继续兼容适配性测试

真机终端测试报告

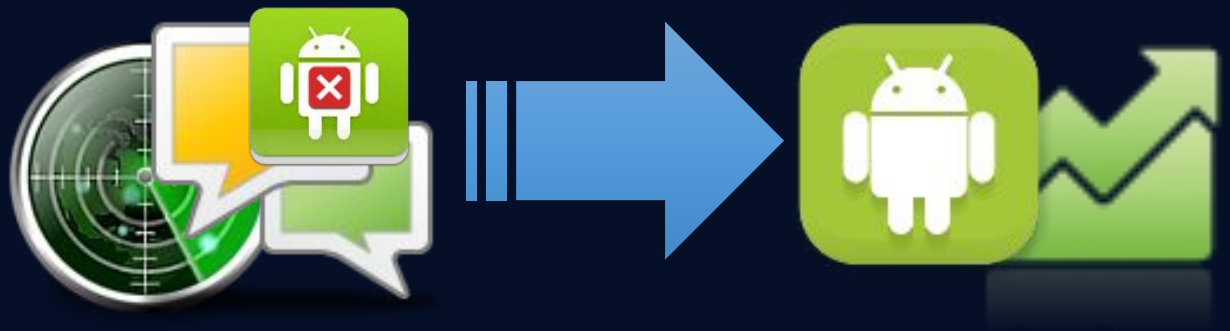
客户端名称			客户端版本号		壳版本号			
测试机型			通过机型数量		通过率			
项目经理签名				时间				
编号	类型	测试机型	版本号	是否正常	现象	备注	曾出问题机型	重要机型
28		三星 i897	2.3.6	正常				
29		三星S7568I移动3G	4.1.2	正常				
30		三星 SM-G3568v 移动4G	4.4.2	正常				
31		三星 N9009	4.4.2	正常				是
32		三星 N9006	5	正常				是
33		三星 N9002	4.4.2	正常				是
34		三星 SM-G5309w 电信4G	4.4.4	正常				
35		三星 G7108v	4.3	正常				
36		三星 SM-G3818 移动3G	4.2.2	正常				
37		三星 SM-A3000	4.4.4	正常				
38		三星 SM-A5000	4.4.2	正常				
39		三星 SM-C1116 联通	4.4.2	正常				
40		三星 GT-I9502 S4 联通3G	4.4.2	正常				
41		三星 N9005 (Note3)	4.4.2	正常				
42		三星 N9006 Note3	4.3	正常				

打造标准化服务流水线

渠道监控

所有渠道，全天候实时监测，一站式分析上报。

分发渠道监测：发现山寨应用，立即上报，进行下架处理。



BBS关键词监测：发现差评，快速回馈厂商，提升品牌质量。

自动更新

智能甄别更新部分，进行差异化更新，后台自动完成。

智能更新

重大BUG

版本回退

出现重大BUG事故，快速响应容灾，实时版本回退。

Show Time
范例演示

NAGA·IN

THANKS!

xKungfoo 2015

www.nagapt.com