攻防之间
移动安全之道

Charles Song
@SharkTeam

OWASP 中国
The Open Web Application Security Project

目录

OWASP 中国
The Open Web Application Security Project

攻防之间

寻移动安全之道

通付盾® PayEgis

OWASP 中国
The Open Web Application Security Project

SharkTeam authored 2 days ago　　latest commit 5a65fdf11f

RawDexClassLoader	更新简介	2 days ago
README.md	增加项目介绍	2 days ago

README.md

通付盾第一代安全加固方案开源

项目简介

APK安全加固是面向移动应用程序的深度安全保护服务，可以为您的APP穿上一层"软猬铠甲"，通过加密、加壳、RPC、动态加载等技术为您的应用进行全方位安全保护，有效防止逆向工程、反编译、嵌入病毒、非法扣费等恶意行为。

随着Android ART模式和Android 5.0系统的普及，应用加固已全面迎来第二代API定制加固时代，需要更多的开发者和研究人员一起投入到移动安全行业。为了为移动安全领域做出更大的贡献，通付盾现开源第一代安全加固方案（Dex文件整体加密），树立移动安全开放精神和开源标准。加密等级和方案优劣上与友商的企业版相当，研究人员可在此基础上进一步优化。

URL：https://github.com/SharkTeam/ApkProtect

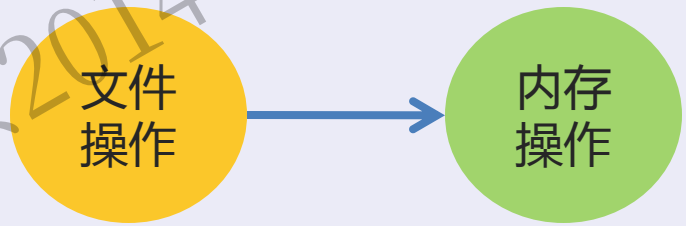
OWASP 中国
The Open Web Application Security Project

项目构成

该项目的开源分组件进行，将第一代安全加固中使用的关键技术改造成可独立使用的安全组件，方便广大开发者对其用途进行扩展。主要的部分有：

- RawDexClassLoader：自定义封装的DexClassLoader，可以实现将一段内存中Dex文件的映射加载进虚拟机。
- 其余组件待发布

- Dex文件保护
- 资源文件保护
- xml文件保护
- 内存保护
- so保护

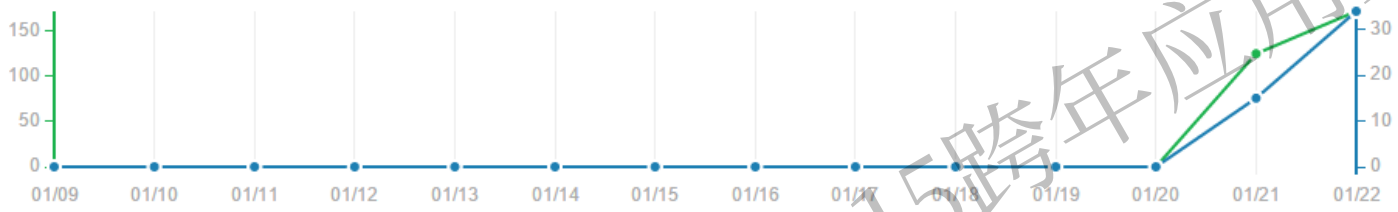


更加安全 **更加快速** **更加灵活**

URL：https://github.com/SharkTeam/ApkProtect

OWASP 中国
The Open Web Application Security Project

Visitors



297
Views

45
Unique visitors

Popular content

Content	Views	Unique visitors
SharkTeam/ApkProtect	47	15
ApkProtect/RawDexClassLoader at ...	32	9
ApkProtect/RawDexClassLoader/lib...	6	4
ApkProtect/RawDexClassLoader/sr...	6	3
ApkProtect/RawDexClassLoader/lib...	5	4
ApkProtect/RawDexClassLoader/g...	4	3
ApkProtect/RawDexClassLoader.ja...	4	2
ApkProtect/RawDexFile.java at master	3	2
增加内存加载Dex的模块，上传Java...	3	2
ApkProtect/RawDexClassLoader/as...	2	2

URL：https://github.com/SharkTeam

OWASP 中国
The Open Web Application Security Project

攻防之间

寻移动安全之道

通付盾® PayEgis

移动攻击方式分析

OWASP 中国
The Open Web Application Security Project

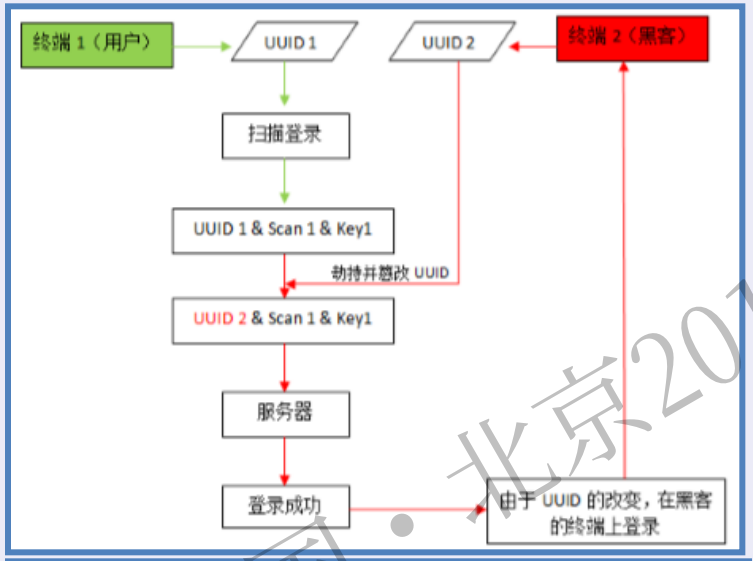
- 针对移动支付进行深层分析，形成全面的移动支付行业研究报告。
- 包含**近场支付**、**远程支付**类型，覆盖主流移动支付方案
- 超过**数百家**手机银行、第三方支付客户端安全测评，**均发现安全隐患**
- 包含**4大类**、**60多项**风险弱点，**9类**典型威胁

1. 网络中间人攻击
2. 组件劫持攻击
3. 组件能力滥用
4. 调试敏感信息泄漏
5. 服务器注入攻击
6. 客户端注入攻击
7. 网络传输信息泄漏
8. 外部存储信息泄漏
9. 内部存储信息泄漏

线下二维码安全

OWASP 中国
The Open Web Application Security Project

原理分析：




```
loc_43CB6
ADD     R0, SP, #0xB78+var_AF4
LDR     R1, [SP,#0xB78+var_B10]
BL      sub_14F6C
LDR     R3, [SP,#0xB78+var_B50]
LDR     R1, [SP,#0xB78+var_B4C]
LDR     R2, =(aCgiBinMicromsg - 0x43CD4)
STR     R3, [SP,#0xB78+var_B78]
LDR     R3, [SP,#0xB78+var_B48]
STR     R1, [SP,#0xB78+var_B74]
MOVS    R1, #0x80
STR     R3, [SP,#0xB78+var_B70]
LDR     R3, [SP,#0xB78+var_AE0]
ADD     R2, PC          ; "/cgi-bin/micr
ADD     R0, SP, #0xB78+s ; s
```

视频演示：

视频录制粗糙，见谅！

应该到我口袋的钱怎么到了你的口袋？

通信安全和Web Api安全隐患

OWASP 中国
The Open Web Application Security Project

某App的后台webapi存在sql注入，导致后台数据库被拖库！

常用移动安全产品简介

OWASP 中国
The Open Web Application Security Project

手机卫士

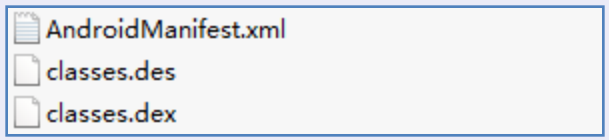
目前市面上比较常见的移动安全产品，安装这类软件不仅能够进行手机性能优化，移动软件的监控与卸载，还可快速扫描手机中已安装的软件，查杀病毒木马和恶意软件等，保护用户的隐私与财产安全。

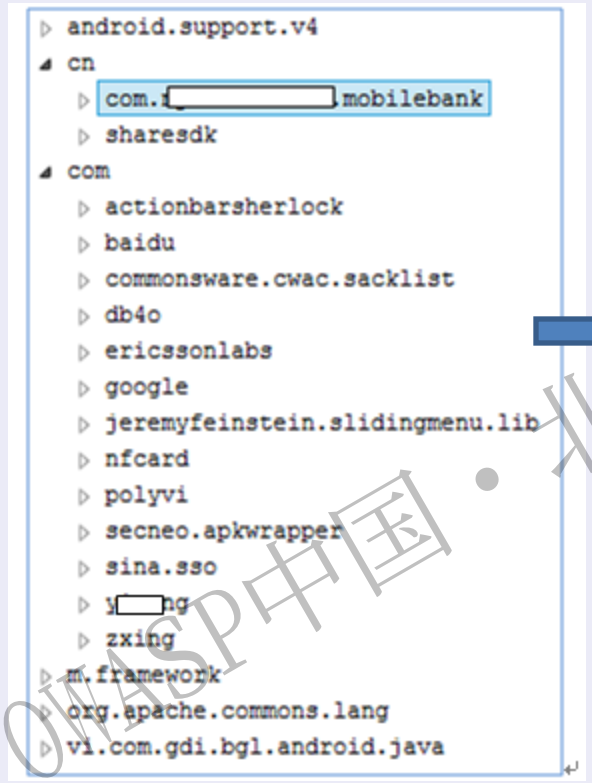
应用加固

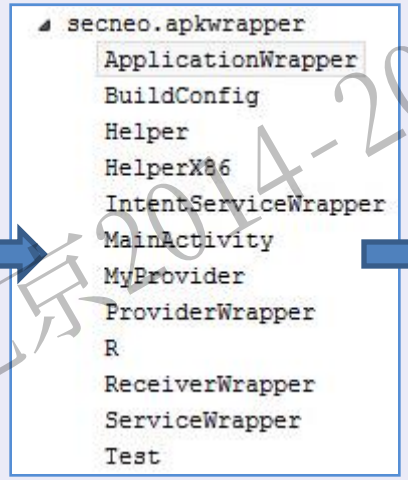
近两年兴起的移动应用保护产品，与传统的手机卫士不同，应用加固是在病毒木马侵袭之前，对移动应用进行提前加密加壳保护，有效防止逆向工程、反编译、嵌入病毒、非法扣费等恶意行为。

某新型安全加固方法

OWASP 中国
The Open Web Application Security Project



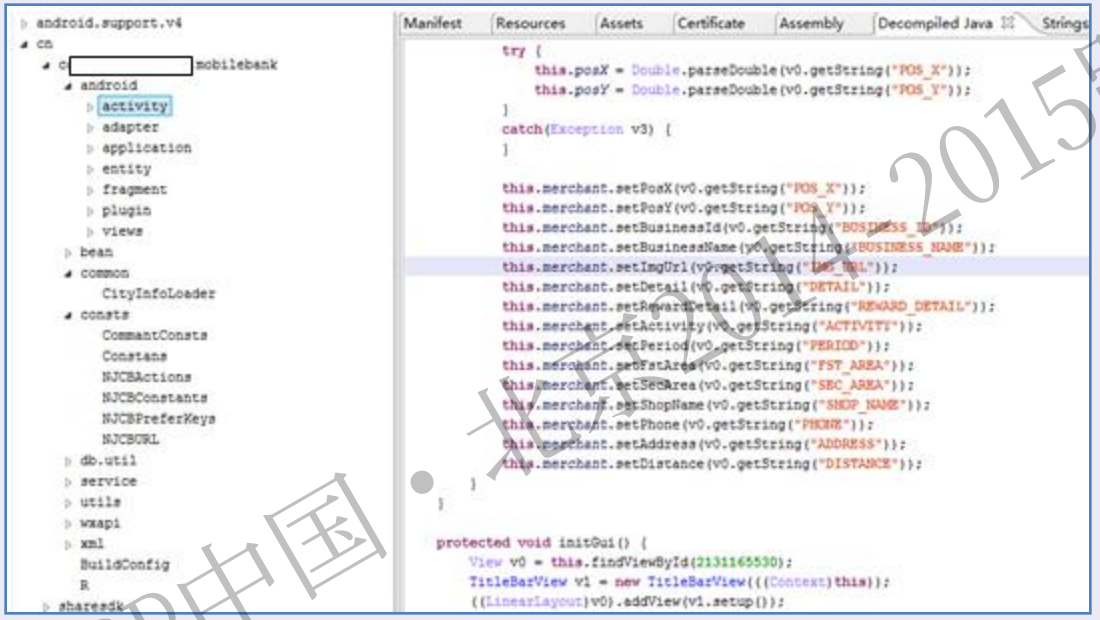





```
public class ApplicationWrapper extends Application {
    private static String PACKAGE_NAME;

    static {
        ApplicationWrapper.PACKAGE_NAME = "cn.com[redacted]mobilebank";
        if(Helper.getCPUABI().equals("x86")) {
            System.loadLibrary("DexHelper-x86");
        }
        else {
            System.loadLibrary("DexHelper");
        }

        Helper.installApplication(ApplicationWrapper.PACKAGE_NAME);
    }

    public ApplicationWrapper() {
        super();
    }

    public void onCreate() {
        super.onCreate();
        Helper.n1(this.getApplicationInfo().sourceDir);
    }
}
```

某新型安全加固方法

OWASP 中国
The Open Web Application Security Project

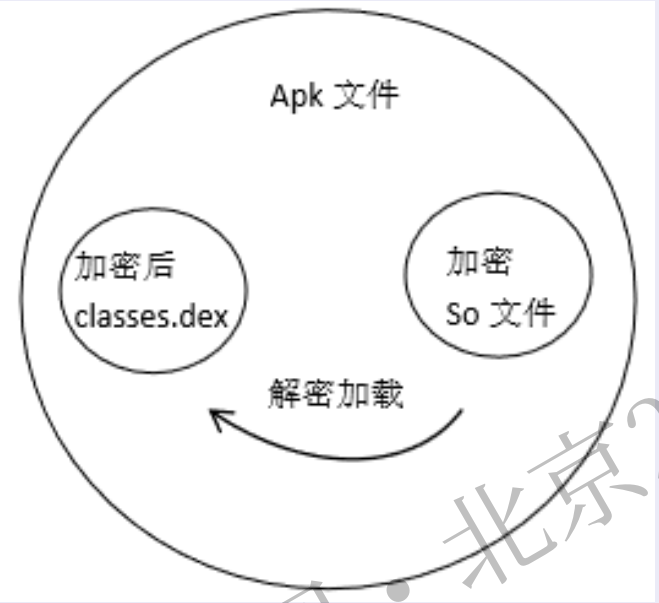


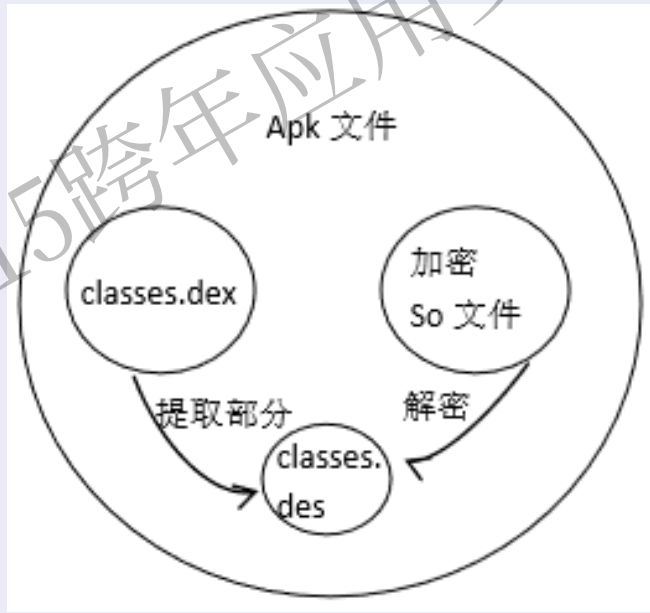
1：Dex整体加固方案的变形。

2：这种应用加固方案在Android Art模式和Android 5.0上兼容性不好，只能采用“预编译”的方式来兼容，但这种预编译的方式会带来程序效率问题

某新型安全加固方法

OWASP 中国
The Open Web Application Security Project





Good **But** **Not Enough ！**

效率 ？ **兼容性 ？** **脱壳器ZjDroid？**

OWASP 中国
The Open Web Application Security Project

攻防之间
寻移动安全之道

通付盾® PayEgis

通付盾移动安全体系

OWASP 中国
The Open Web Application Security Project

移动应用攻击

- 原版应用
- 反逆向
- 逆向分析源码
- 反篡改
- 恶意代码注入
- 反欺诈
- 吸费、广告
  窃取账号等

应用安全三战法：反逆向、反篡改、反欺诈

移动数据：自学习、自适应 ->自防御

OWASP 中国
The Open Web Application Security Project

风险管理

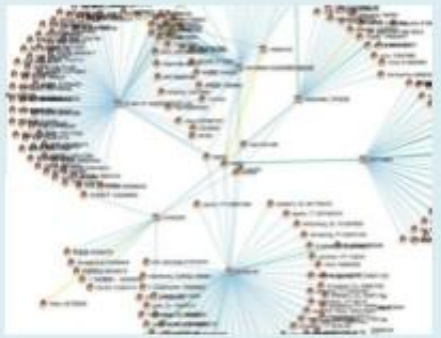
采用规则、黑白名单、策略模型相结合方式防范欺诈风险

设备信誉

基于设备行为的征信体系，提供设备多种属性查询、信誉值查询

关系图谱

引入第三方数据，提供设备、账号关联、社交图谱分析，实现精准营销



风控 | 决策 | 关联

OWASP 中国
The Open Web Application Security Project

谢谢！

通付盾®
PayEgis