MDCC 2016
中国移动开发者大会
Mobile Developer Conference China 2016

微信Tinker热补丁实践演进之路

shwenzhang | 张绍文
2016年9月

关于我
——ABOUT ME

张绍文 毕业于哈尔滨工业大学

搜狗

手机输入法Android组 (2012.02~2013.07)

微信

基础优化组 (2013.07~2015.05)

基础组件组 (2015.06~至今)

- **长期负责**
  - 微信插件化，性能体验，质量监控，编译
  - 微信网络组件，跨平台开发
- **目前负责**
  - WeMobileDev公众号
  - 终端质量运营平台
  - Tinker热补丁项目

目录
Contents

何为热补丁

可以让应用无需重新安装下能够自动更新

12小时
90%+

32M
100K

随意调
试

两大流派

Native

- AndFix
- KKFix

Java

- Qzone
- Tinker
- robust
- nuwa
- amigo
- rocooFix

热补丁技术哪家强？

微信设计目标

稳定性与兼容性

微信数亿用户的
设备上稳定运行

性能

非补丁版本影响
补丁大小

易用性

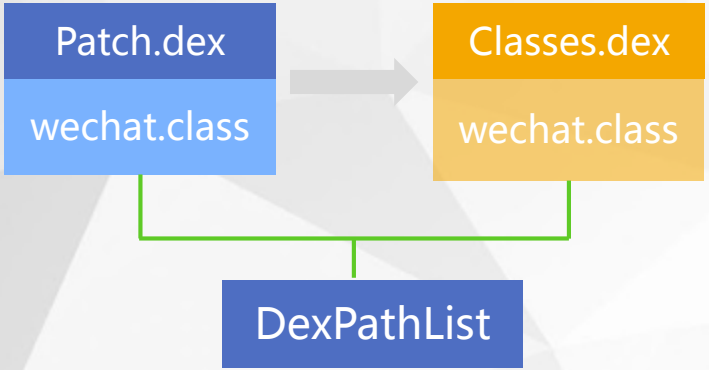
简单易用
完整支持

“高可用”的补丁框架

目录
Contents

v1.0-2015年9月

基于Qzone的classloader方案



主要问题

Class resolved by unexpected DEX crash

解决思路

Class插桩阻止类判别为preverify

安卓App热补丁动态修复技术介绍

V1.0-晴天霹雳

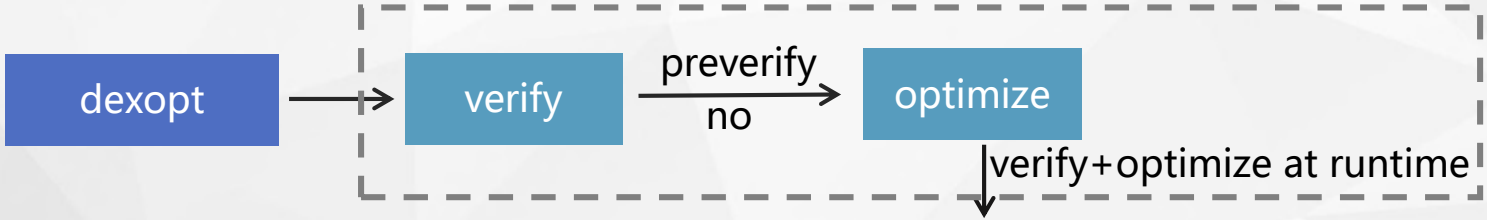
启动耗时报警


```
#accinfo.crashTime=2015-10-11 21:48:07.227+0800
#crashContent=
java.lang.NullPointerException
at com.tencent.mm.ui.LauncherUI.init(LauncherUI.java:1447)
....
at java.lang.reflect.Method.invokeNative(Native Method)
at java.lang.reflect.Method.invoke(Method.java:511)
at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:551)
at dalvik.system.NativeStart.main(Native Method)
```

Art平台补丁后无法启动

static Boolean **addFriendTipsShow** = false

V1.0-Dalvik



DEX Opcode	ODEX Opcode	Optimization
iget	iget-quick	inline, use byte offset, vtable for faster 0(n) ->0(1)
iput	iput-quick	
invoke-virtual	invoke-virtual-quick	

插桩方案

- **性能损耗**
- **Optimize full mode**
- **hack preverify flag**

V1.0-Art平台

字节码

```
0x01bc: iget-object v0, v9,
Lcom/tencent/LauncherUI;
com.tencent.LauncherUI.addFriendTipsShow
//field@40469
```

>>

机器码

```
0x0204c05a: 2a0a          cmp    r2, #10
0x0204c05c: f2c086a9      blt.w  +3410)
0x0204c060: f3bf8f5b      dmb    ish
0x0204c064: f8d06820      ldr.w  r6, [r0, #2080]
```

用时查找

在Dalvik平台，最终会通过field id查找到正确的变量

内存地址错乱

在Art平台，由于增加了Field, 导致整体内存地址错乱

```
static ImageView sightChangeImage;
```

V1.0-牛刀小试

“高可用”的补丁框架

稳定性与兼容性

性能

- ~~性能影响~~
- ~~补丁大小~~

易用性

- 简单易用
- 完整支持

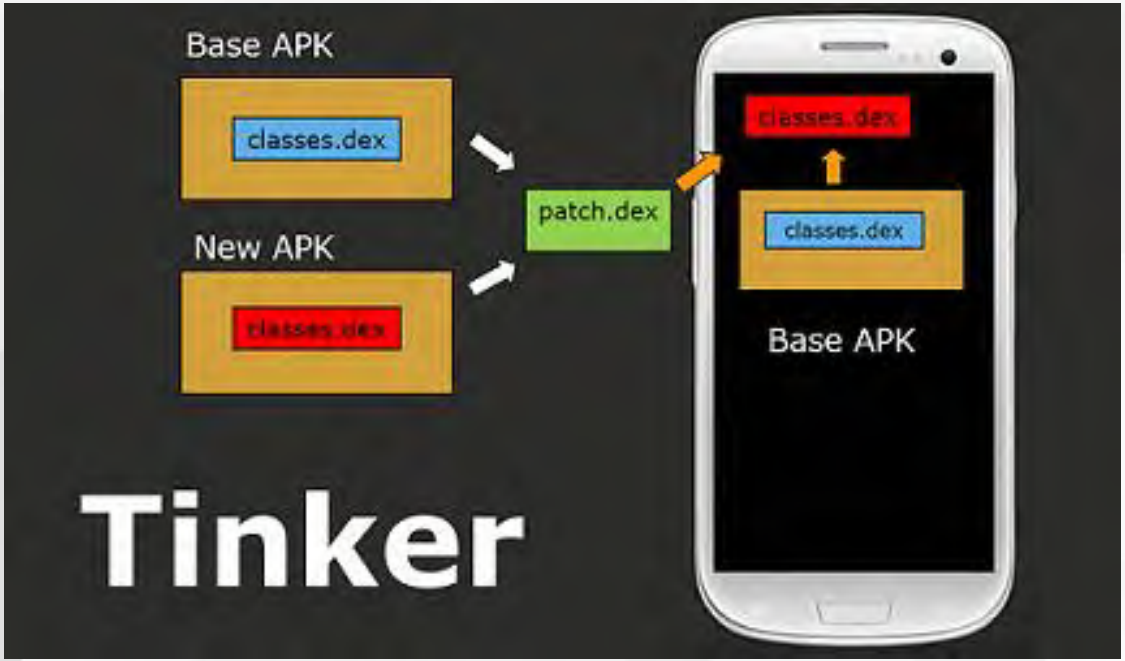
96.3%
五天成功率

-31%
启动耗时

800K
补丁包大小

目录
Contents

V2.0-2016年2月



基于全量合并方式

- Gradle Instant run
- Buck exopackage

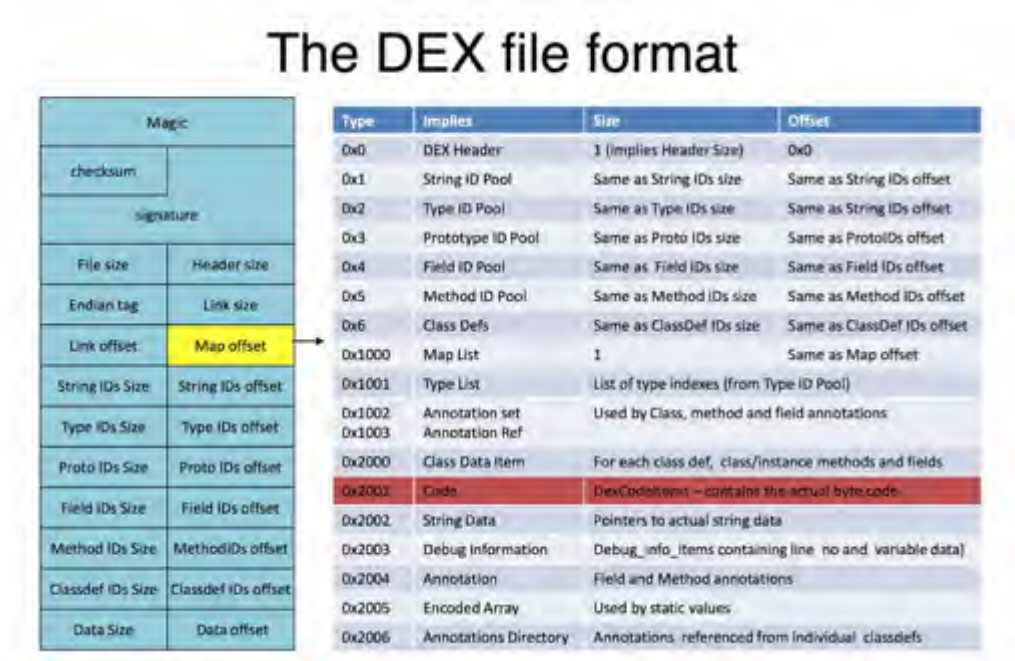
Diff算法

- BsDiff
- DexMerge
- DexDiff

Diff设计目标

- Diff结果小
- 占用内存小，合成速度快
- 支持新增、删除、修改class

V2.0-Dex格式



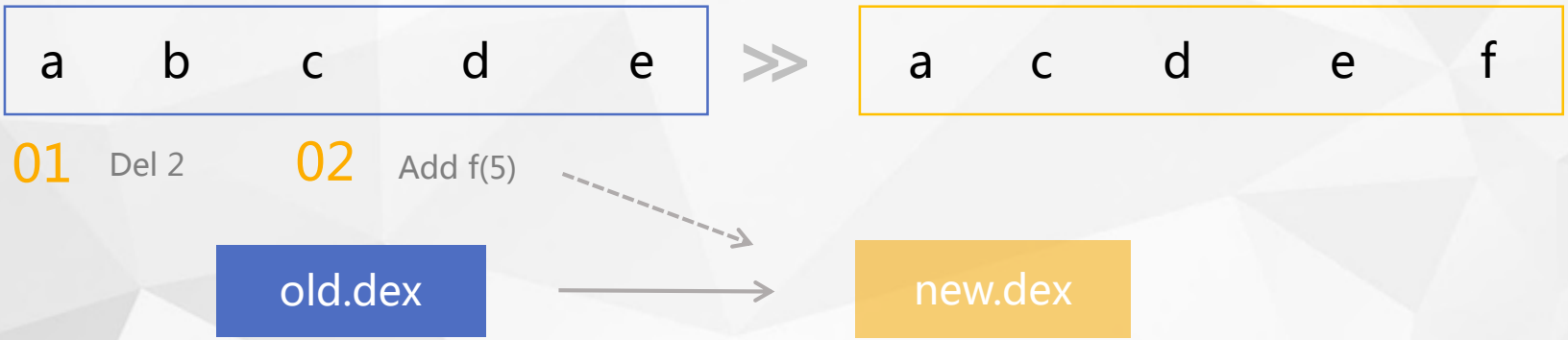
Type	Implies	Size	Offset
0x0	DEX Header	1 (implies Header Size)	0x0
0x1	String ID Pool	Same as String IDs size	Same as String IDs offset
0x2	Type ID Pool	Same as Type IDs size	Same as String IDs offset
0x3	Prototype ID Pool	Same as Proto IDs size	Same as ProtoIDs offset
0x4	Field ID Pool	Same as Field IDs size	Same as Field IDs offset
0x5	Method ID Pool	Same as Method IDs size	Same as Method IDs offset
0x6	Class Defs	Same as ClassDef IDs size	Same as ClassDef IDs offset
0x1000	Map List	1	Same as Map offset
0x1001	Type List	List of type indexes (from Type ID Pool)	
0x1002 0x1003	Annotation set Annotation Ref	Used by Class, method and field annotations	
0x2000	Class Data Item	For each class def, class/instance methods and fields	
0x2001	Code	DexCodeItems – contains the actual byte code	
0x2002	String Data	Pointers to actual string data	
0x2003	Debug Information	Debug_info_items containing line no and variable data)	
0x2004	Annotation	Field and Method annotations	
0x2005	Encoded Array	Used by static values	
0x2006	Annotations Directory	Annotations referenced from individual classdefs	

https://source.android.com/devices/tech/dalvik/dex-format.html

- **低内存、快速**
  每段处理，一次读写
- **引用修正**
  - index修正，排序校验
  - offset修正，无序且互相引用
- **合法校验**
  四字节对齐、dexopt、dexoat校验

V2.0-Diff方案

Index区域



结果

用例ID	原始Dex大小（KB）	新Dex大小（KB)	BSDiff(KB)	DexDiff(KB)	时间(ms)	峰值内存(M)
1	228.72	624.76	48.00	1.64	95	3
2	10617.16	10617.7	260.00	7.64	7917	26
3	12723.15	12723.2	173.00	1.56	9517	32
4	12744.78	12744.78	10570.00	5881	8448	39

V2.0-晴天霹雳

来自小米的Anr

本周开发版升级后微信启动一分钟以上

0

--

升级后微信启动慢

0 101

--

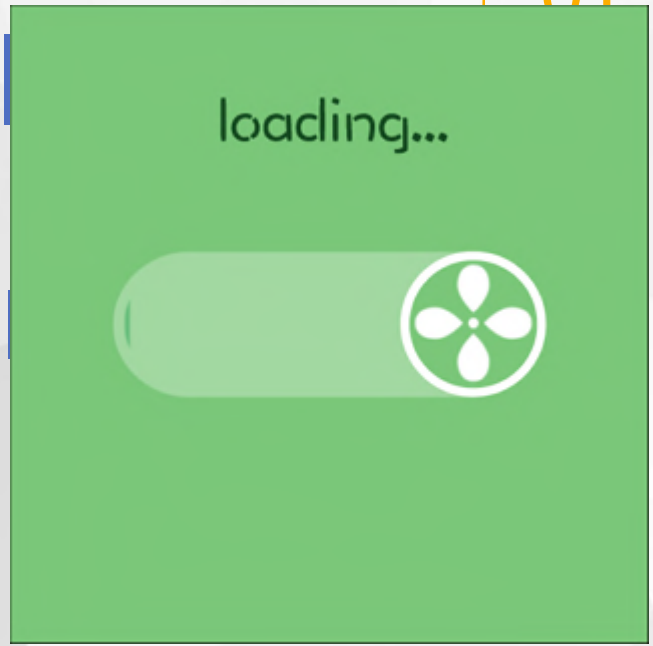

```
java.lang.IllegalAccessError:
Illegal class access: 'com.tencent.mm.ui.conversation.ConversationOverscrollListView'
attempting to access 'com.tencent.mm.ui.conversation.ConversationOverscrollListView$c'
(declaration of 'com.tencent.mm.ui.conversation.ConversationOverscrollListView'
appears in /data/user/0/com.tencent.mm/tinker/patch-a002c56d/dex/classes2.dex)
```

来自华为的Crash

V2.0-厂商OTA的挑战

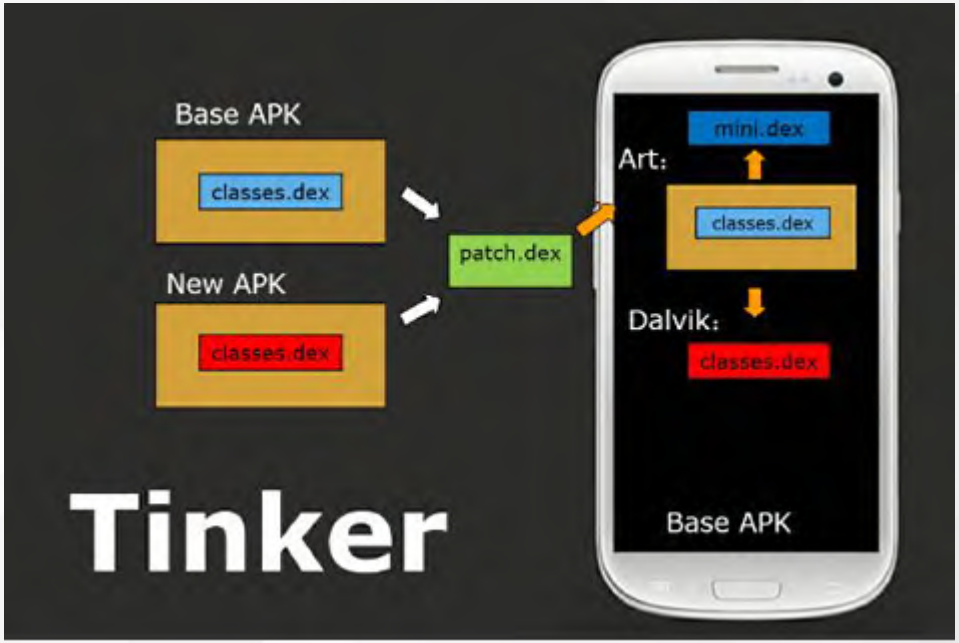
01

Dalvik: modtime/crc



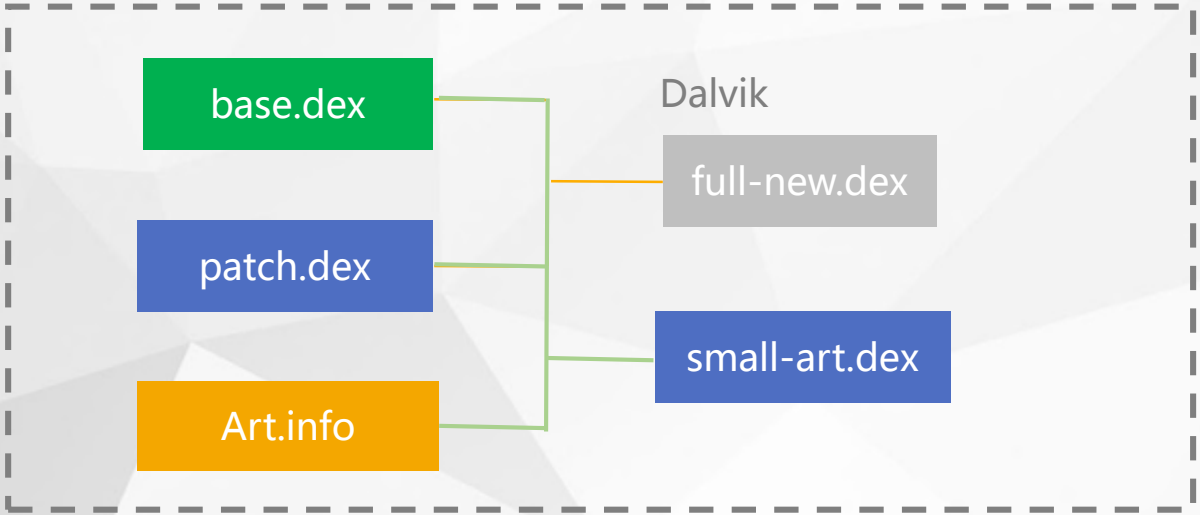
FingerPrint change？提供加载页

Art



分平台合成，在Art只合成与v1.0一致的小Dex

V2.0-厂商OTA的挑战



难点

- small class收集
- ClassN处理
- 偏移如何修正
- art.info的大小
- 有效性校验

解决问题

01 Dalvik全量合成，解决了插桩带来的性能损耗

02 分平台合成，解决了全量合成方案占用rom体积过大

03 Art.info仅仅1-20K, 解决由于补丁包可能过大

V2.0-其他技术挑战

Android N

Xposed

Classloader

DexDiff

V2.0-自创功法

“高可用”的补丁框架

- ~~稳定性与兼容性~~
- **性能**
  - 性能影响
  - 补丁大小
- **易用性**
  - 简单易用
  - 完整支持

94.1%
五天成功率

-2%
启动耗时

10K
补丁包大小

目录
Contents

V3.0-2016年4月

加载
什么类可以修改

合成
进程隔离与通知

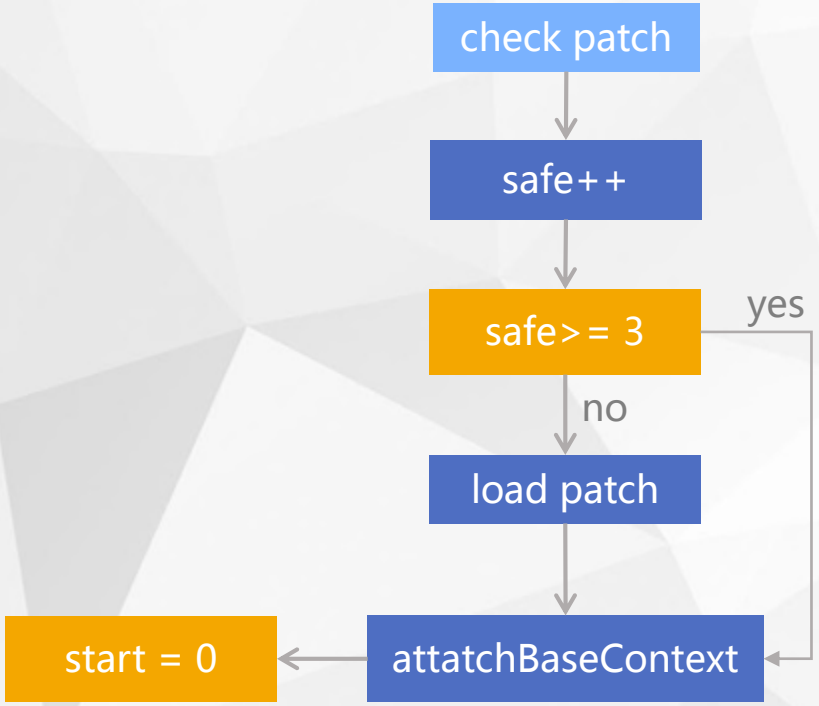
异常熔断
出现异常情况，及时回退

一致性
版本一致性，代码一致性

监控回调
对加载与合成整个过程的监控回调

安全
补丁签名与合成结果校验

V3.0-异常熔断



Java Crash

- load {try catch Throwable} --> onLoadException
- patch {try catch Throwable} --> onPatchException

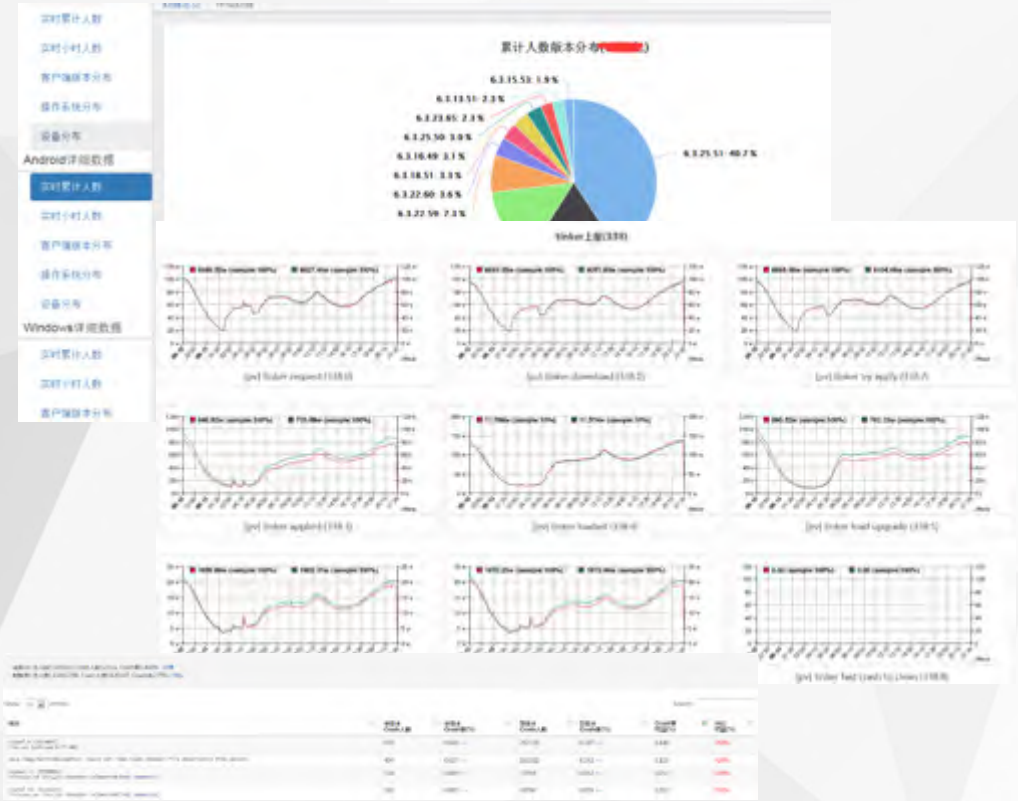
Native/UnCaught Crash

- 安全启动模式，单一进程连续三次无法启动，清除patch

Crash Protect

- 程序启动10s内多次Crash，清除patch
- crash时Xposed判别，清除patch

V3.0-监控回调



Load Report

补丁加载过程中的相关信息

- 加载结果/耗时
- 失败原因
- crash信息

Patch Report

补丁合成过程中的相关信息

- 加载结果/耗时
- 失败原因
- crash信息

V3.0-一致性

一致性

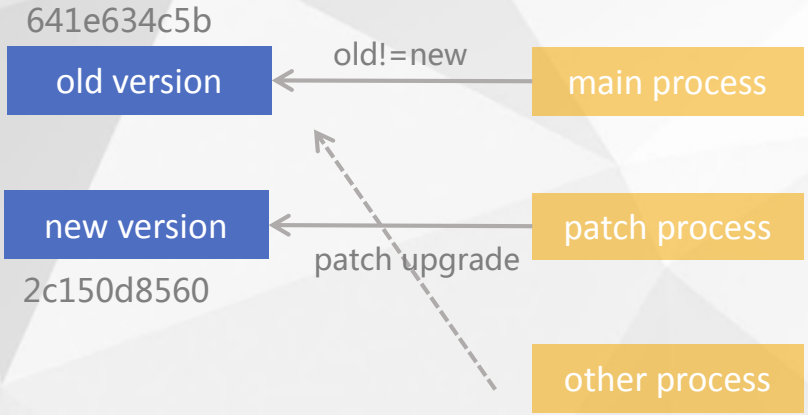
01 **进程一致性**

不同的进程需要保证加载同一个版本的补丁

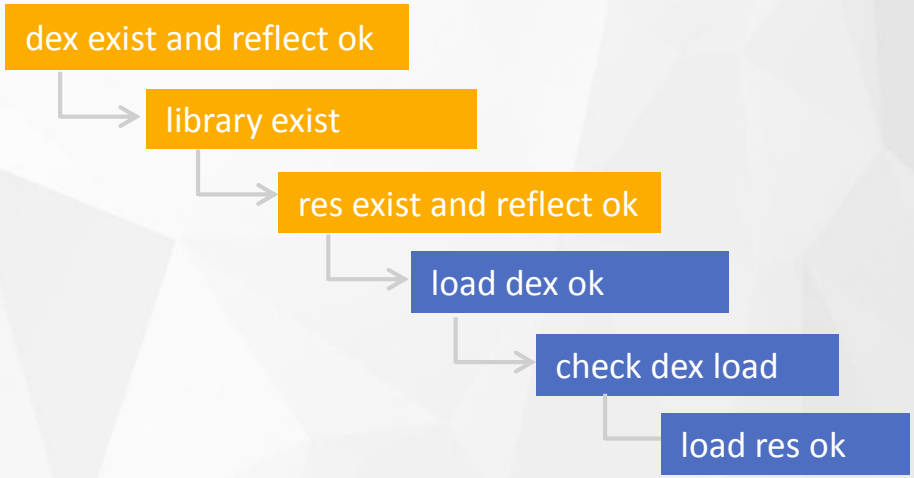
02 **逻辑一致性**

dex, library与资源应该同时成功，或者失败

进程一致性



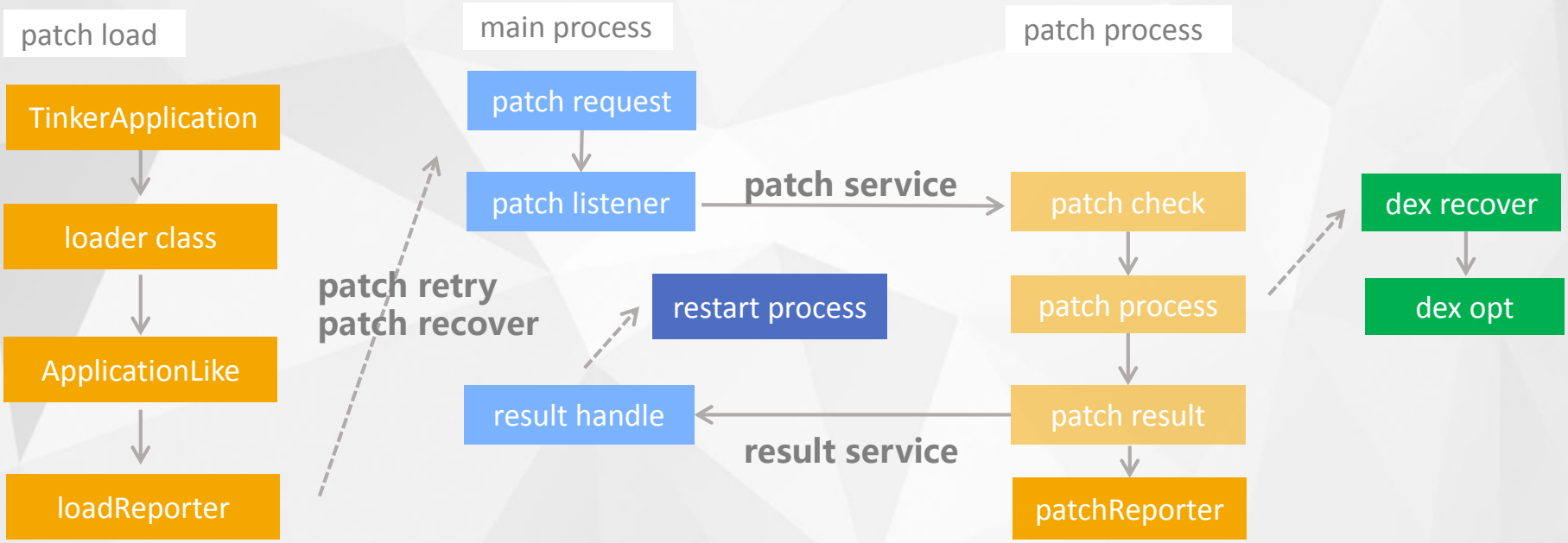
逻辑一致性



V3.0-加载与合成

补丁加载 补丁如何加载，什么类可以修改，类如何隔离

补丁合成 补丁合成进程隔离，结果及时通知



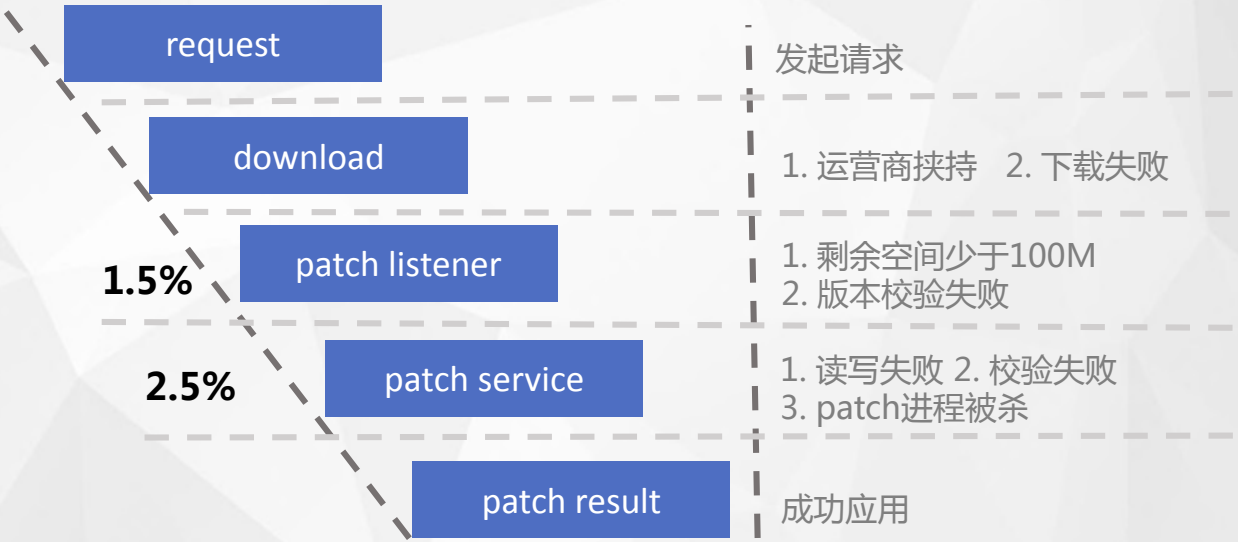
V3.0-修炼内功

“高可用”的补丁框架

- **稳定性与兼容性**
- **性能**
  - 性能影响
  - 补丁大小
- **易用性**
  - ~~简单易用~~
  - ~~完整支持~~

95.3% 五天成功率

96.3% v1.0



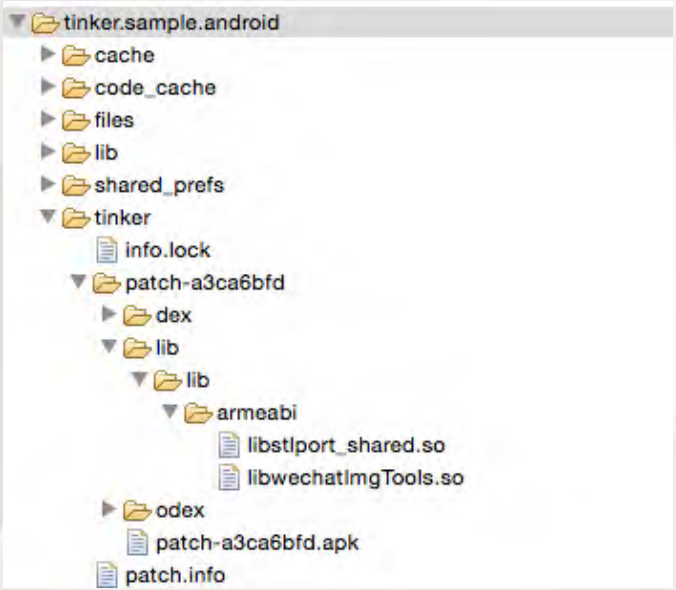
目录
Contents

V4.0-Library处理

核心问题

01 多abi获取不准备，反射出问题

02 32位与64位问题



尽量少的hook

- LoadLibraryFromTinker("assets/x86", "stlport_shared");
- LoadLibrary("stlport_shared");

V4.0-资源处理

Add asset path?

```
if ((size_t)entryIndex >= allTypes->entryCount) {
    ALOGW("getEntry failing because entryIndex %d is beyond type entryCount %d",
    entryIndex, (int)allTypes->entryCount);
    return BAD_TYPE;
}
```

预埋entry count

- 编译强耦合
- ~~影响基础版本~~
- ~~无法随心所欲~~

全量替换

- Atlas或者携程的插件化框架
- Gradle-instant run

V4.0-异常情况

Transition动画

ResId无法新增、删除，可能出现Res not found

Notification

ResId无法新增、删除，可能出现Res not found

Shortcut

ResId无法新增、删除，可能会变成默认图标

Assets

读取source apk方式无法修改

V4.0-资源包生成

1. 将base.apk解压 36M->83M

2. 将补丁包中修改、新增资源覆盖 4M

3. 排除删除以及Dex、Lib等文件 16M

4. 重新Zip压缩

空间

峰值占用：83+4+36-16=107M

文件数 ：5492个

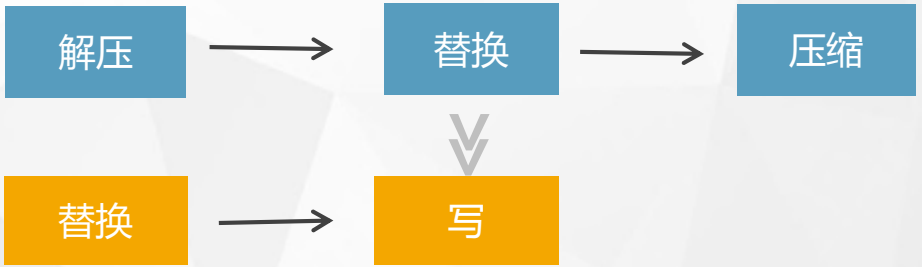
时间

一次解压一次压缩：42S

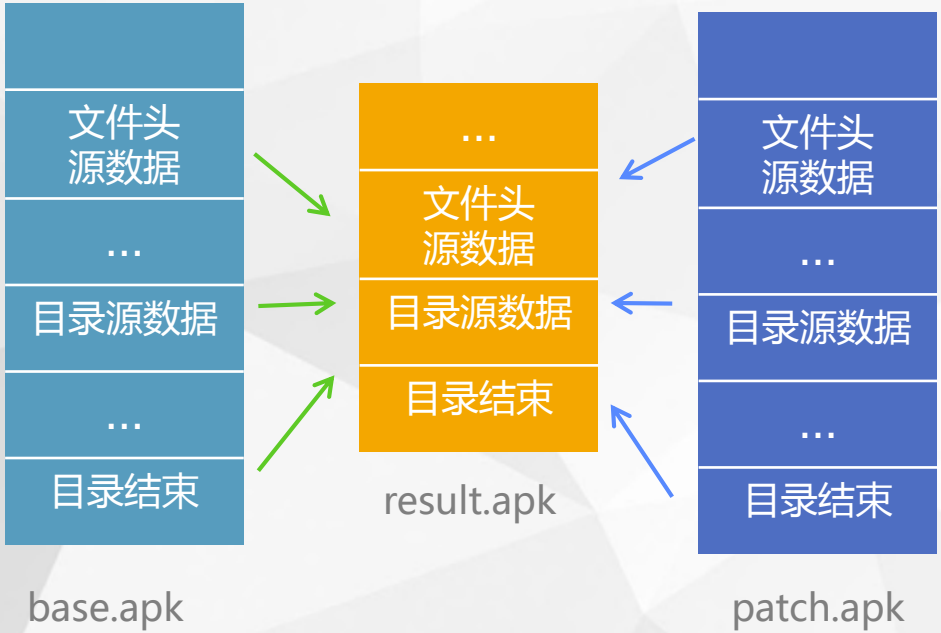
资源包

无法合成后资源包的md5

Header			
Offset	Bytes	Description	
0	4	Local file header signature = 0x04034b50 (read as a little-endian number)	文件头标识，值固定 (0x04034b50)
4	2	Version needed to extract (minimum)	解压文件所需 pkware 最低 版本
6	2	General purpose bit flag	通用位标记
8	2	Compression method	压缩方法
10	2	File last modification time	文件最后修改时间
12	2	File last modification date	文件最后修改日期
14	4	CRC-32	说明采用的算法。
18	4	Compressed size	压缩后的大小。
22	4	Uncompressed size	非压缩的大小。
26	2	File name length (n)	文件名长度
28	2	Extra field length (m)	扩展区长度
30	n	File name	文件名
30+n	m	Extra field	扩展区



资源处理-资源包生成



空间

峰值占用：107M --> 4+36-16=24M

文件数　：5492个 --> 2个

时间

一次读写：42S --> 3S

资源包

合成后资源包的md5

剔除time/extra/comment随机因子

资源处理-资源包校验

20% 合成后md5校验不通过？

应用市场增量算法

- 不保证entry顺序
- 不保证压缩流大小
- 只保证最终解压后的每个文件

替代方式

- 校验resources.arsc md5
- 异步校验核心文件

V4.0-编译目标

```
apply plugin: 'com.tencent.tinker.patch'

tinkerPatch {
    oldApk = "${buildDir}/intermediates/tinkerPatch/current/app-base.apk"
    ignoreWarning = true
    useSign = true

    buildConfig {
        applyMapping = "${buildDir}/intermediates/tinkerPatch/current/app-mapping.txt"
        applyResourceMapping = "${buildDir}/intermediates/tinkerPatch/current/app-R.txt"
        tinkerId = "${buildInfo.REV()}"
    }
    dex {
        dexMode = "raw"
        pattern = ["classes*.dex"]
        loader = [
                "com.tencent.tinker.loader.*",
                "com.tencent.mm.app.Application",
                "com.tencent.mm.loader.stub.BaseBuildInfo"
        ]
    }
    res {
        pattern = ["res/*", "assets/*", "resources.arsc", "AndroidManifest.xml"]
        ignoreChange = ["assets/secondary-program-dex-jars/metadata.txt",
                        "res/raw/android_wear_micro_apk.apk"]
        largeModSize = 100
    }

    lib {
        pattern = ["lib/armeabi/*.so"]
    }
    packageConfig {
        configField("patch.rev", buildInfo.REV())
        configField("patch.client.ver", buildInfo.CLIENT_VERSION())
    }
    sevenZip {
        zipArtifact = "com.tencent.tinker:seven-zip:1.0.0"
    }
}
```

简单易用

- 只要输入一个旧的基础包，即可生成补丁包
- proguard
- mainDex
- 日志与校验

灵活控制

- 可通过pattern灵活控制需要的内容
- 版本管理

减少补丁包

- applyMapping
- appyResourceMapping
- force jumbo
- 7zip

...

V4.0-内外兼修

“高可用”的补丁框架

稳定性与兼容性

性能

- 性能影响
- 补丁大小

易用性

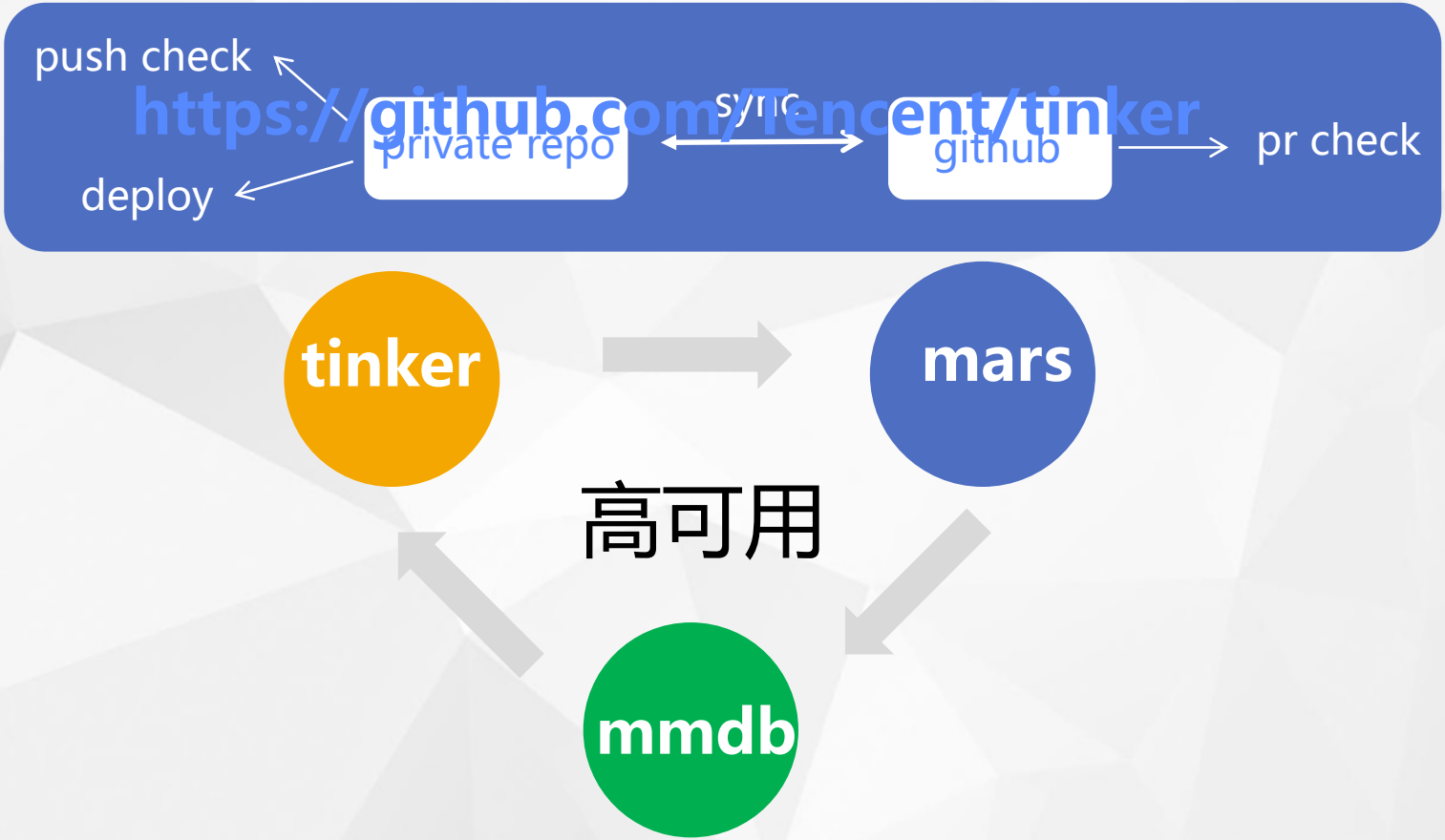
- 简单易用
- 完整支持

性能

- Dalvik占rom体积
- 额外的合成过程，降低成功率

目录
Contents

开源化计划


push check
https://github.com/Tencent/tinker
sync
private repo
github
pr check
deploy
tinker
mars
高可用
mmdb

shwenzhang@tencent.com

WeMobileDev公众号