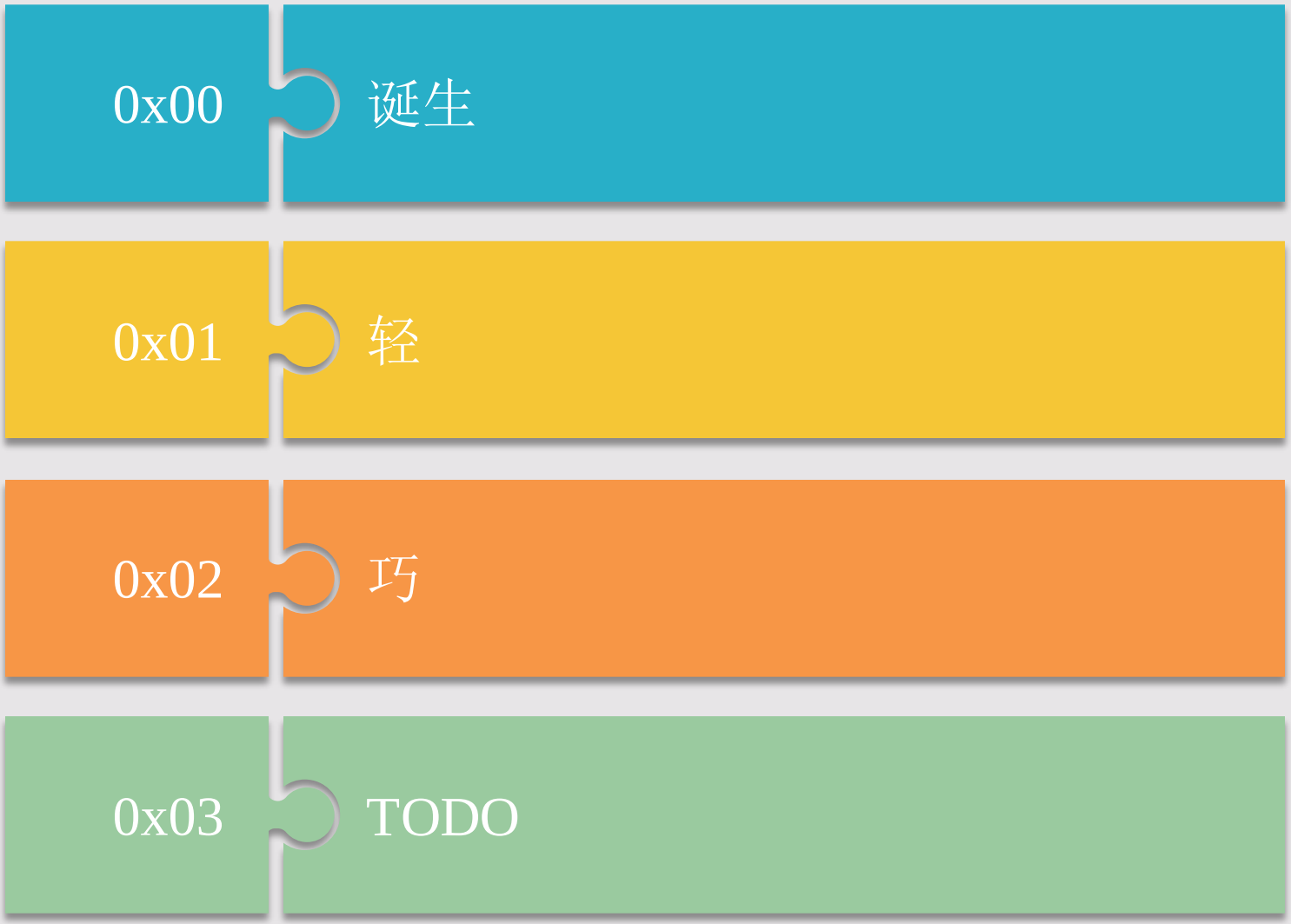
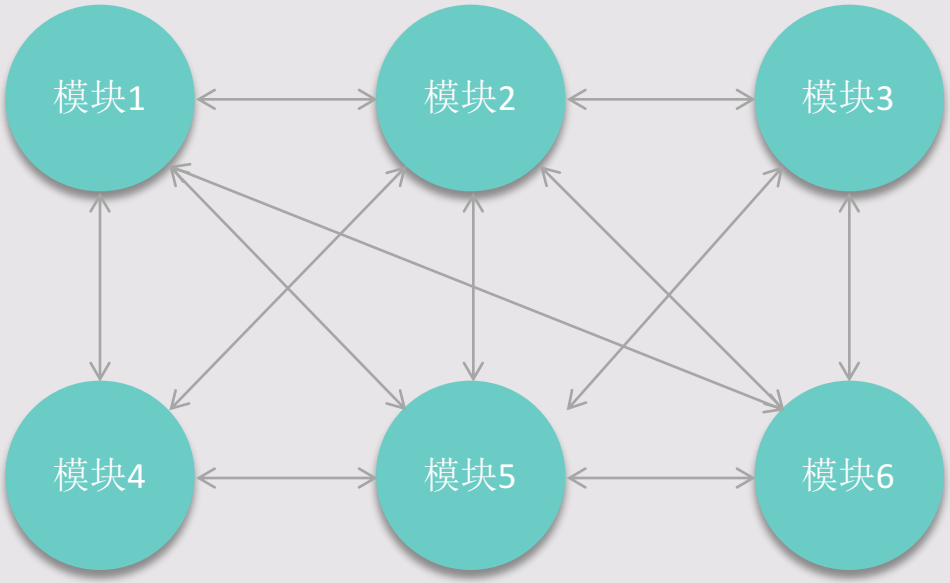
Small：插件化轻巧之道

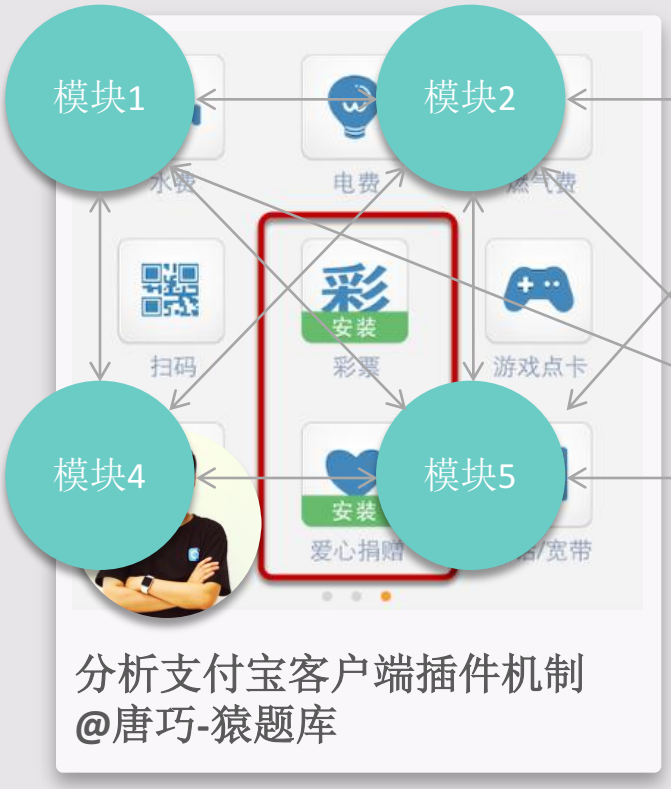
林光亮


0x00
诞生
0x01
轻
0x02
巧
0x03
TODO

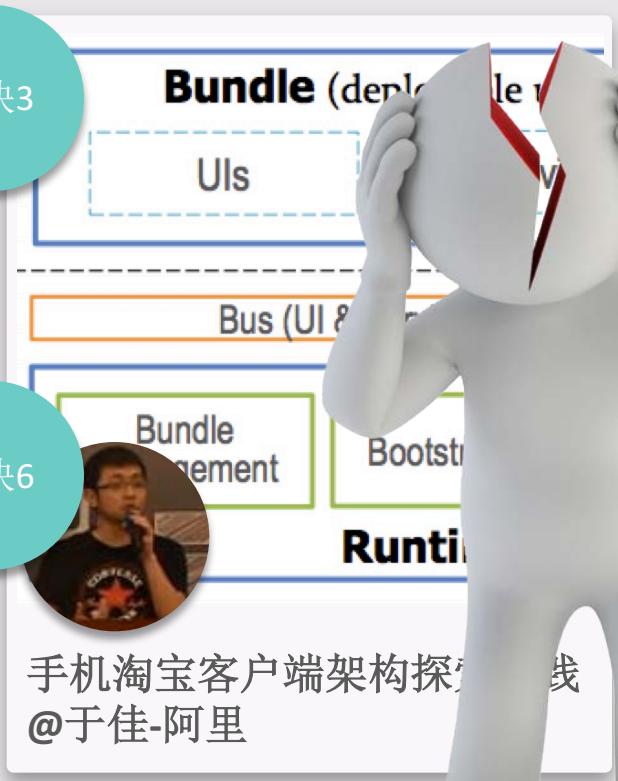
诞生



诞生

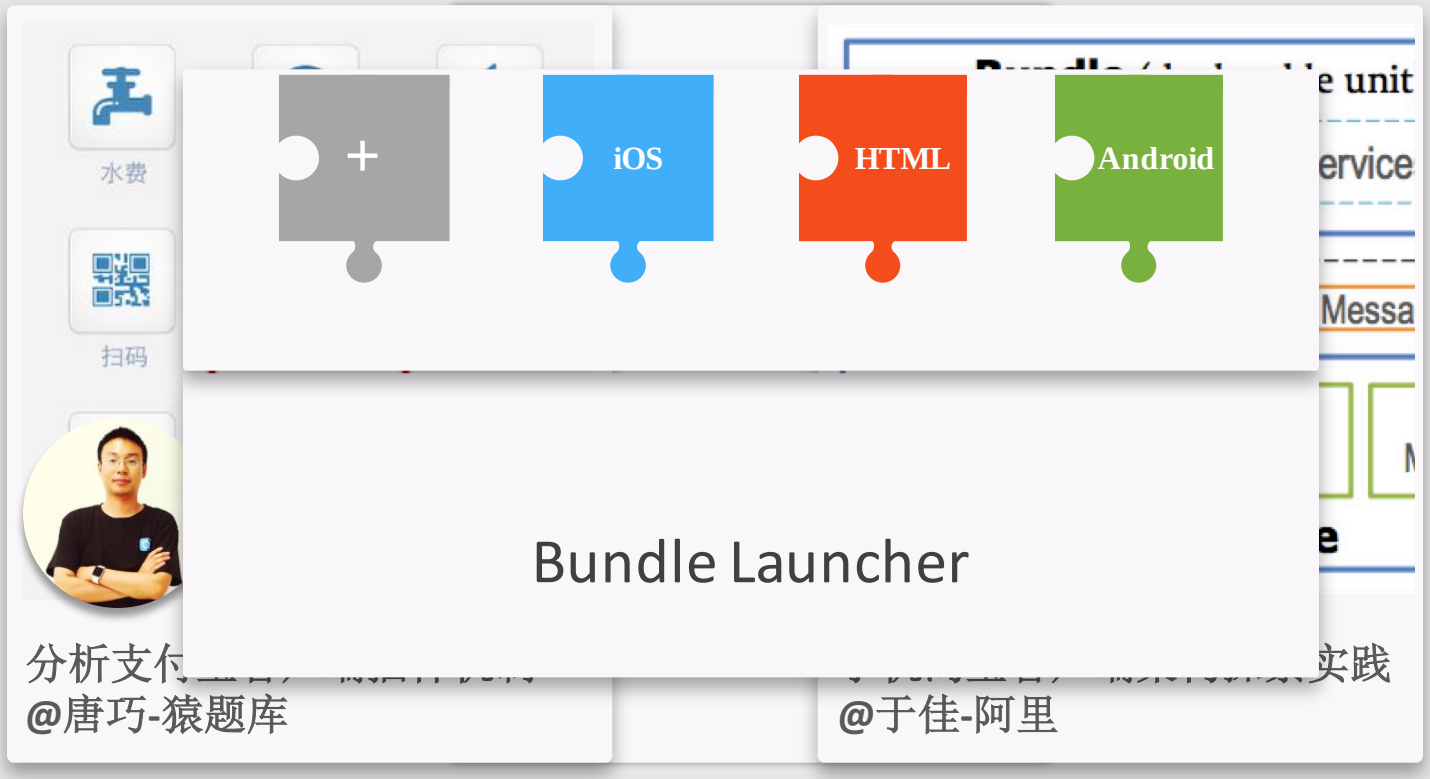


分析支付宝客户端插件机制
@唐巧-猿题库



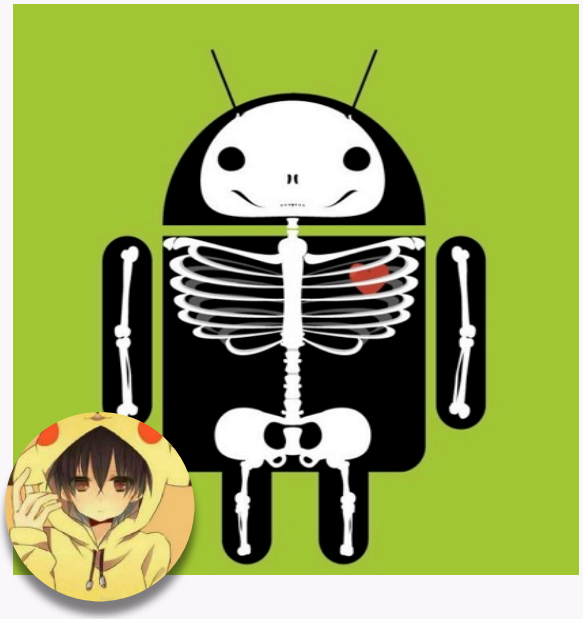
手机淘宝客户端架构探
@于佳-阿里

诞生



诞生

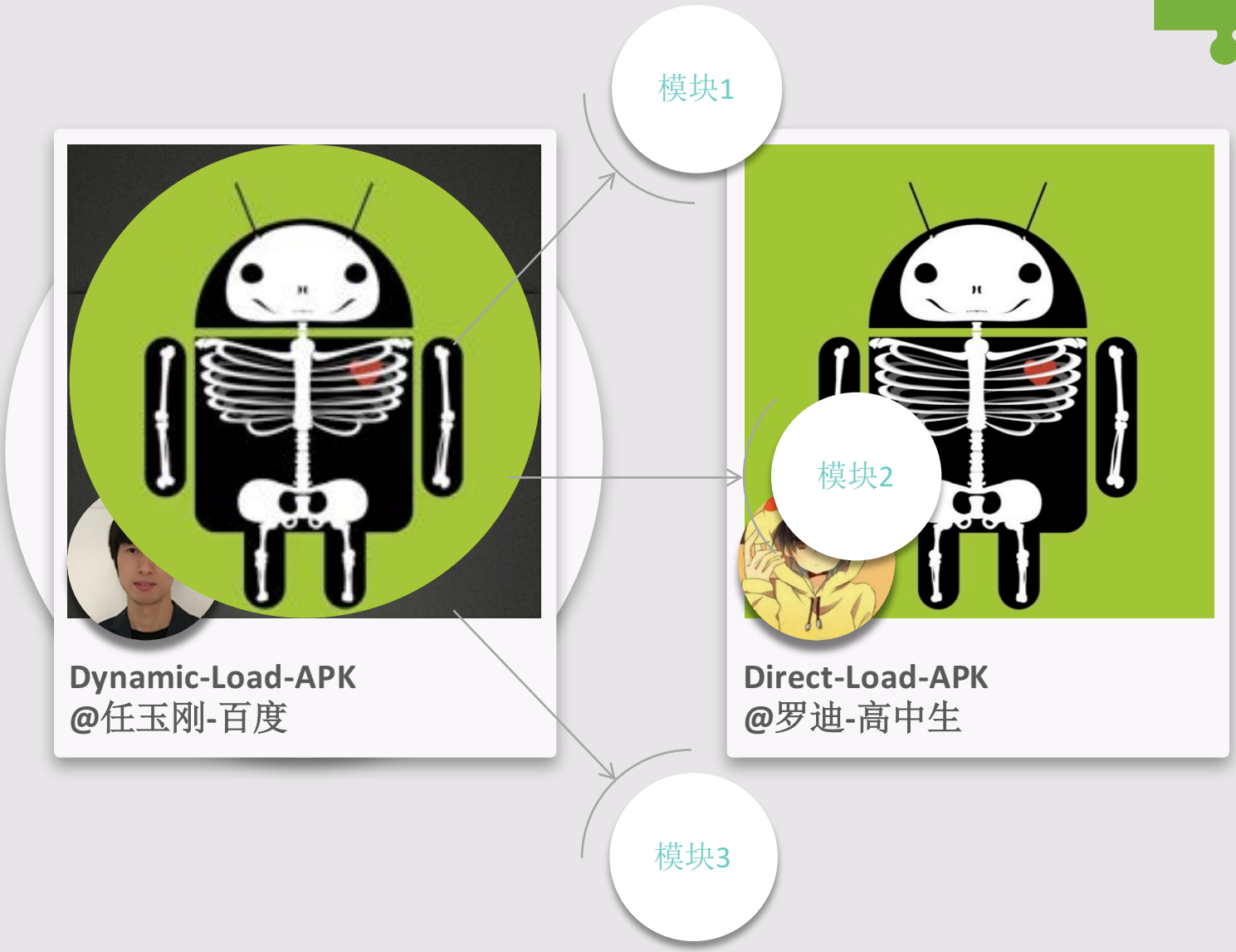
Dynamic-Load-APK
@任玉刚-百度



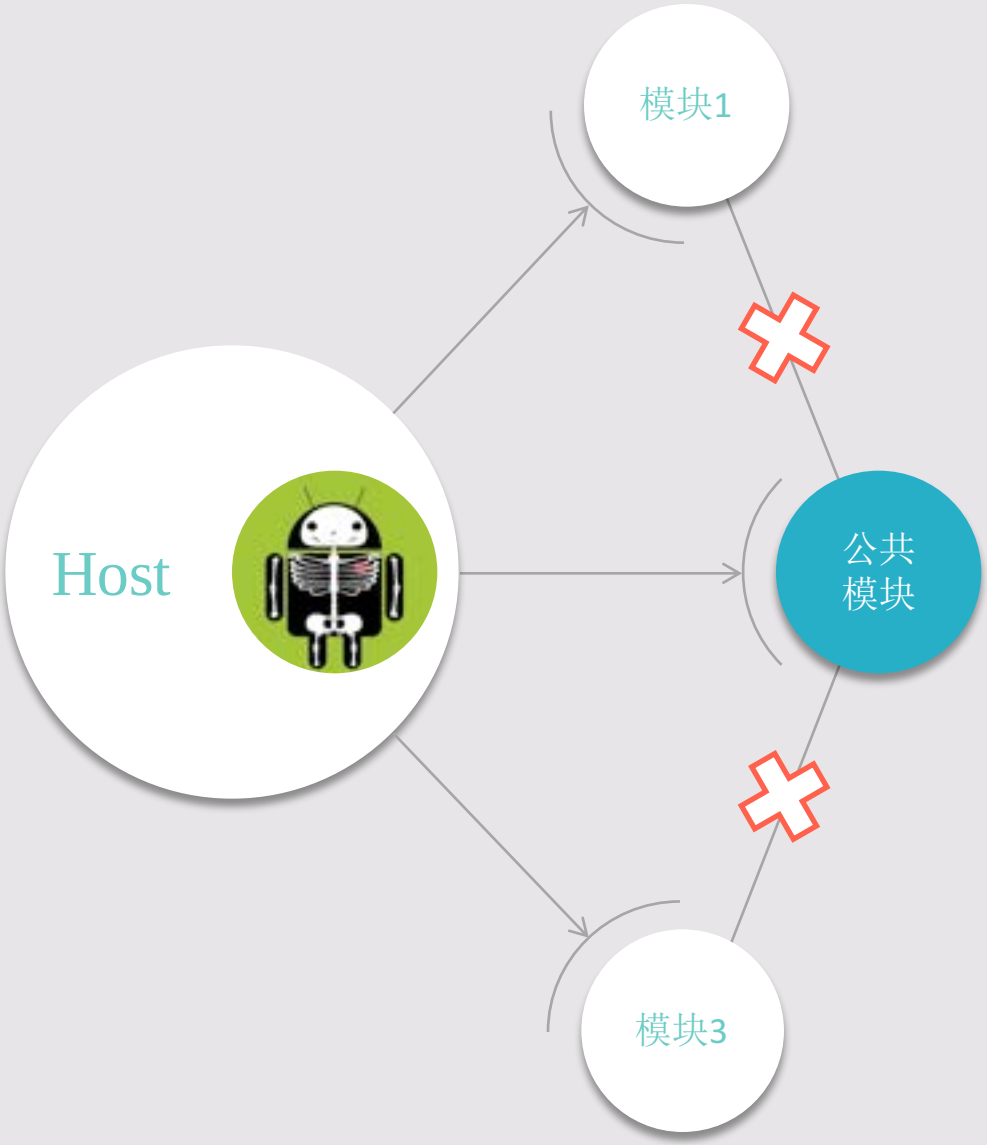
Direct-Load-APK
@罗迪-高中生

诞生

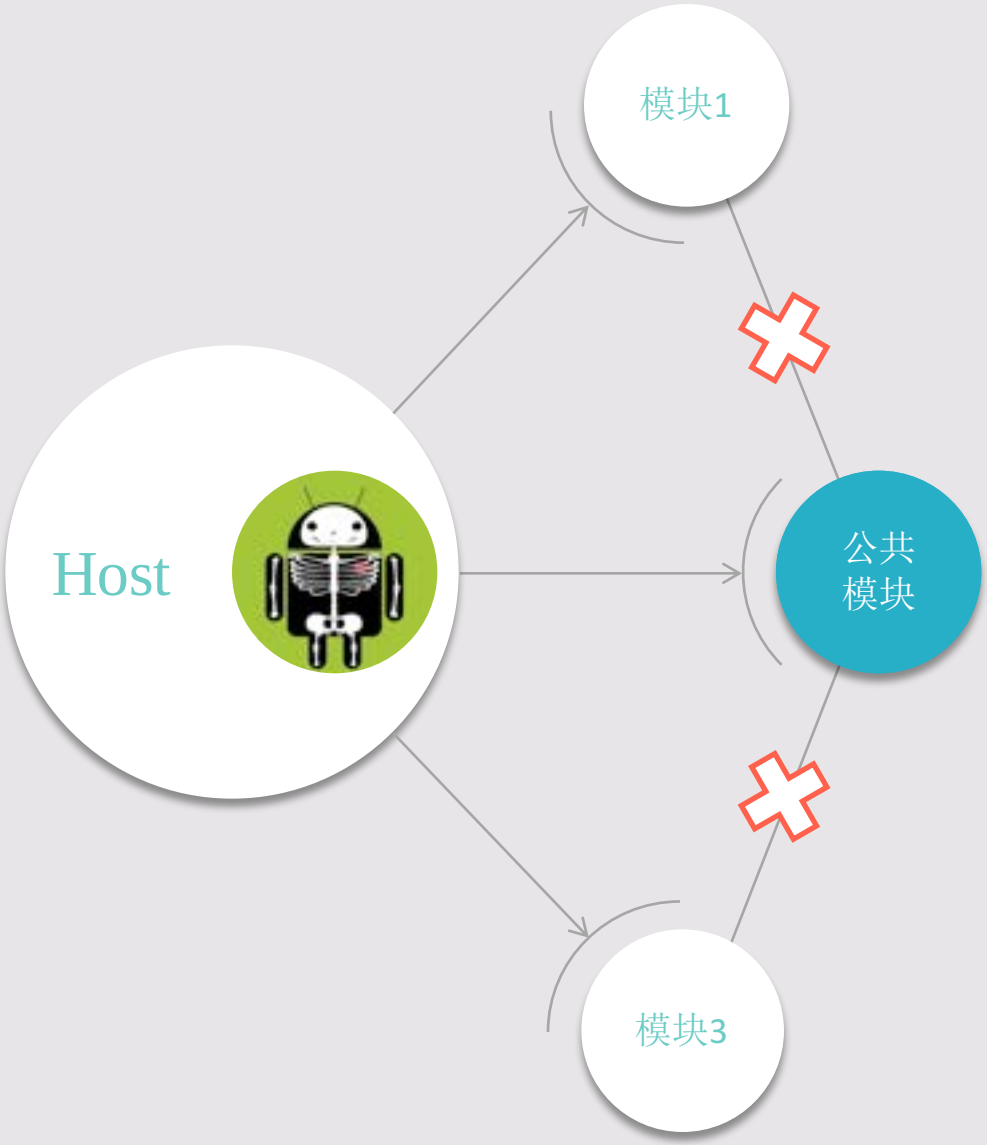

Android


模块1
模块2
模块3
Dynamic-Load-APK
@任玉刚-百度
Direct-Load-APK
@罗迪-高中生

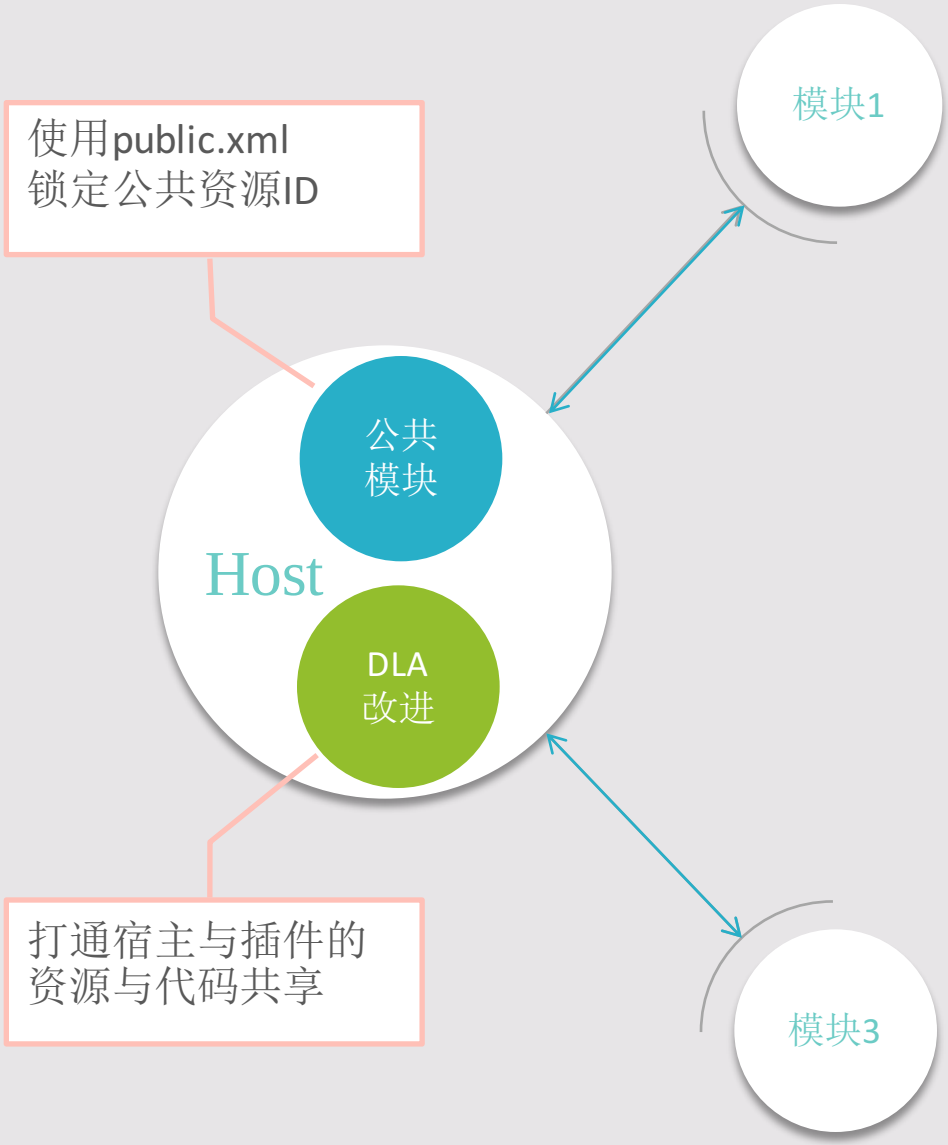
诞生



诞生

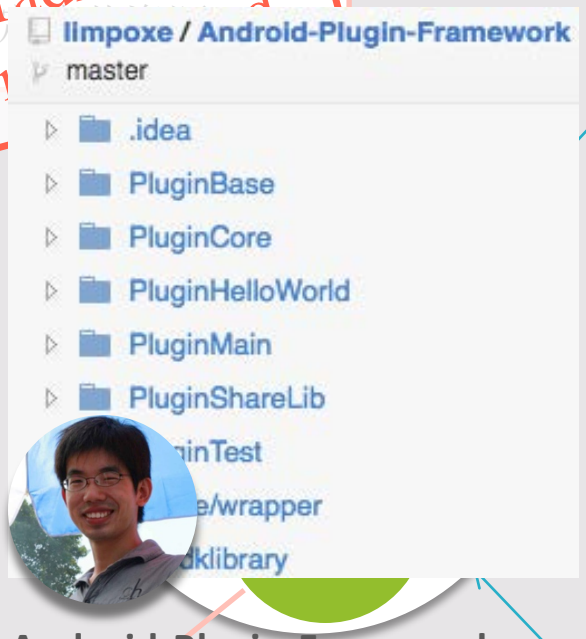


诞生


使用public.xml
锁定公共资源ID
模块1
公共
模块
Host
DLA
改进
打通宿主与插件的
资源与代码共享
模块3

诞生

Gradle 1.3+



Android-Plugin-Framework
@Limpoxe

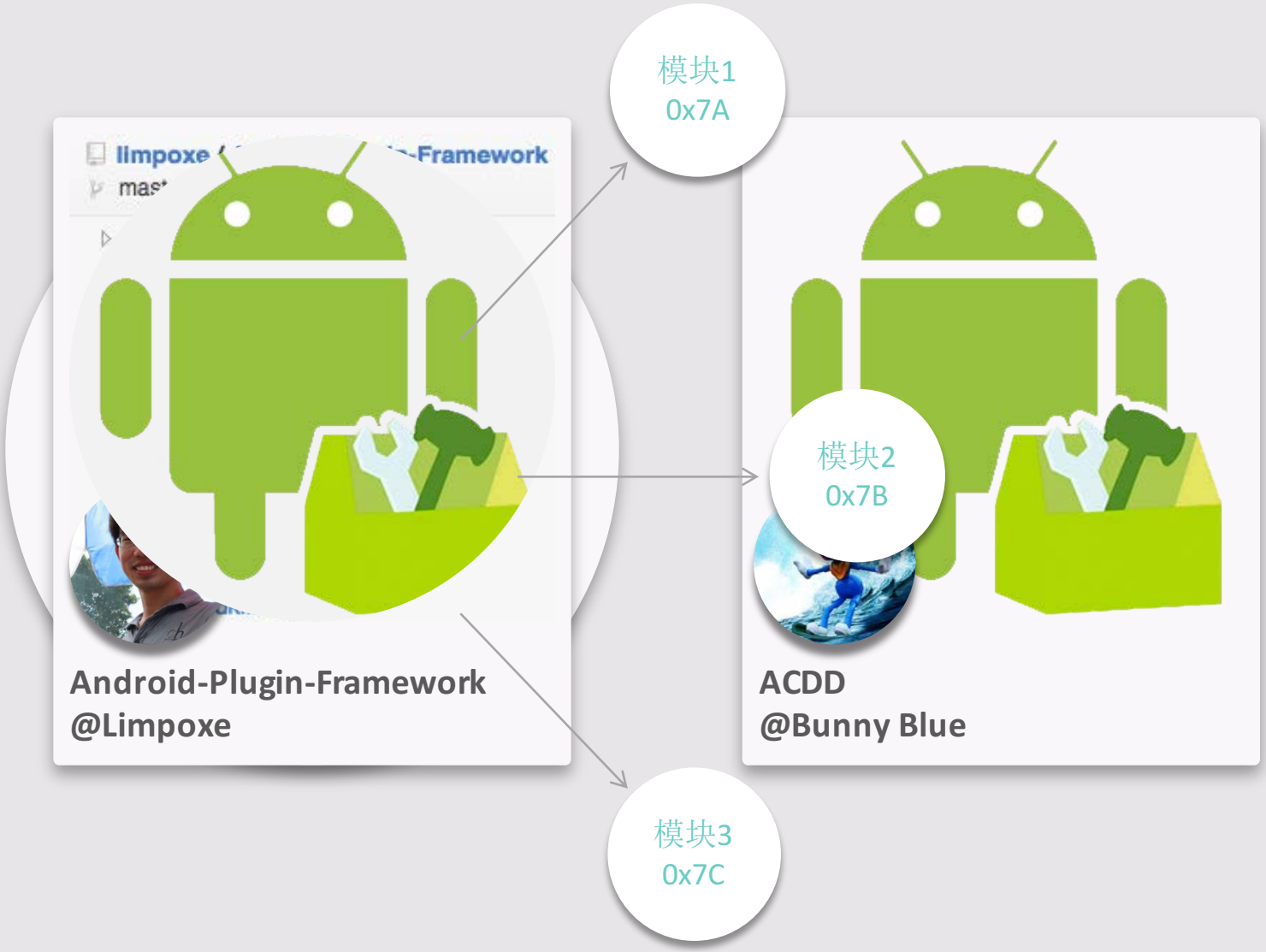
打通宿主与插件的
资源与代码共享

模块1

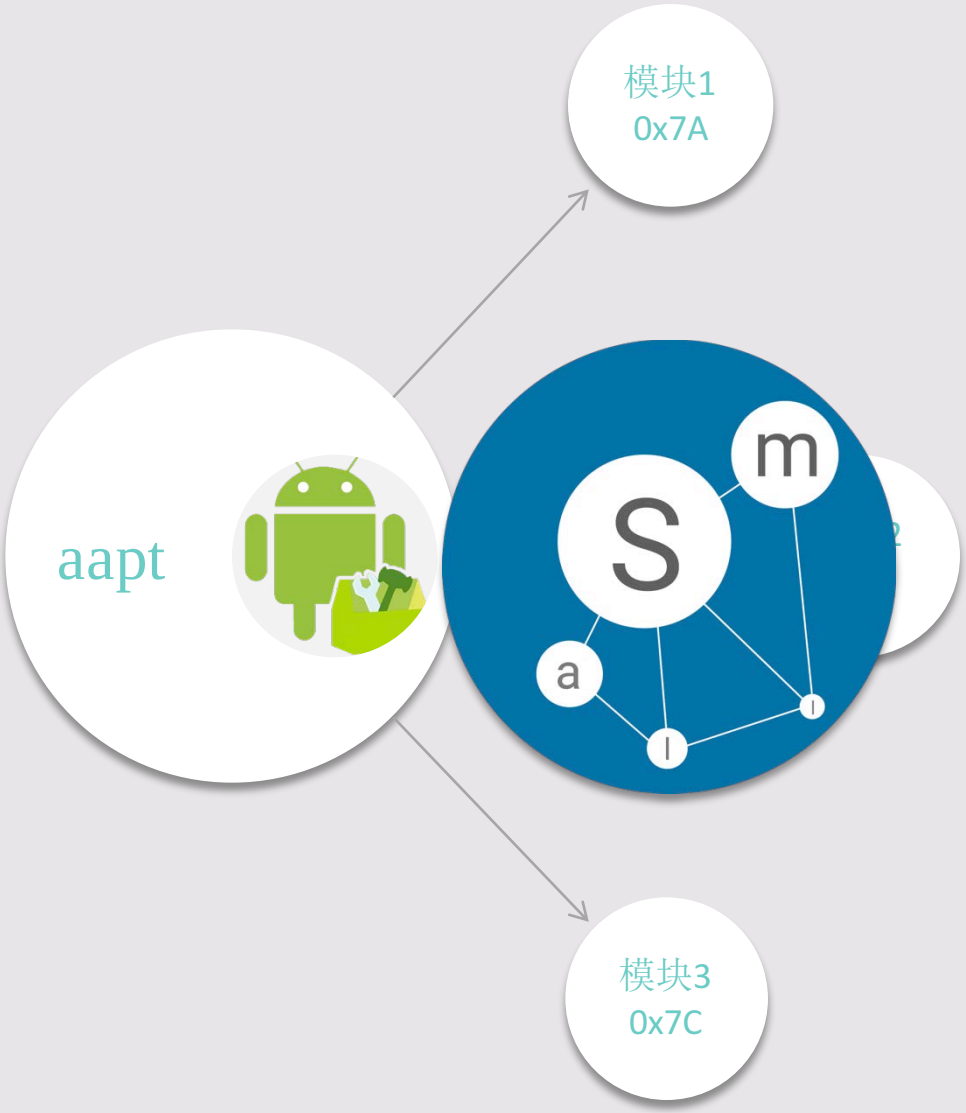
ACDD
@Bunny Blue

模块3

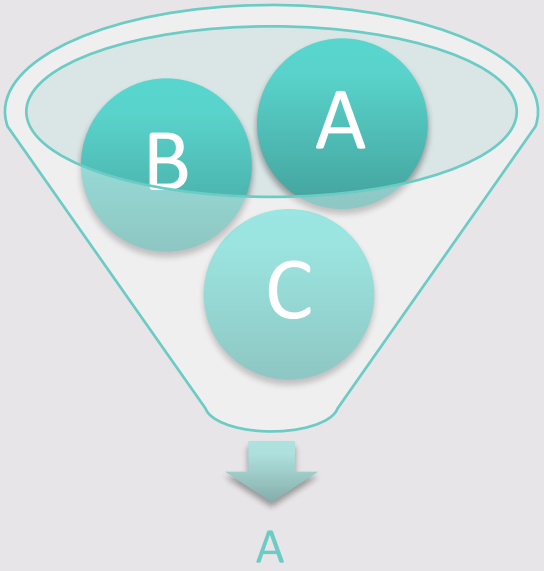
诞生


模块1
0x7A
模块2
0x7B
模块3
0x7C
Android-Plugin-Framework
@Limpoxe
ACDD
@Bunny Blue

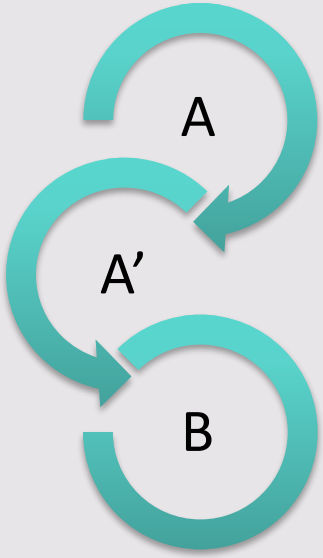
诞生



轻

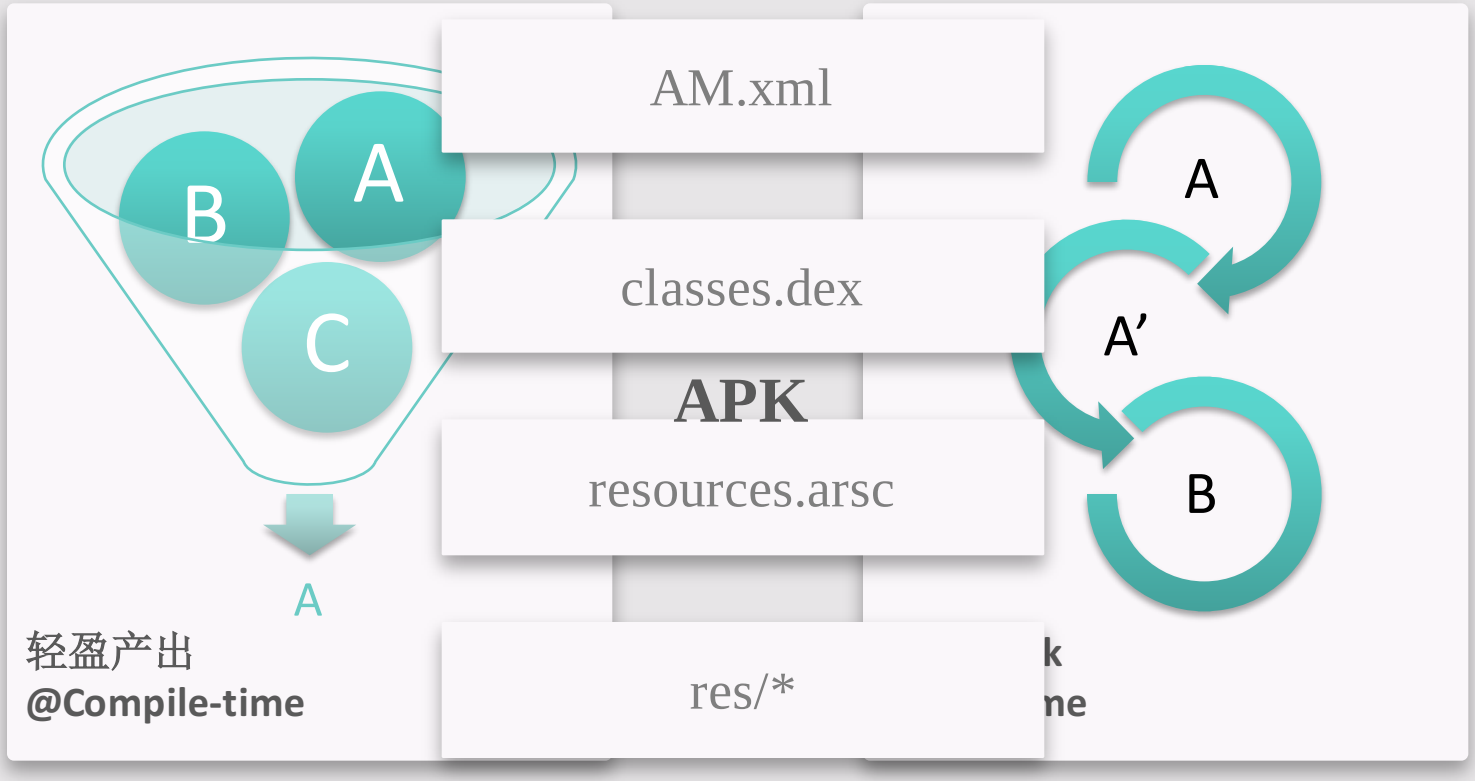


轻盈产出
@Compile-time



轻度Hook
@Run-time

轻/轻盈产出


AM.xml
B
A
C
classes.dex
APK
resources.arsc
res/*
A
轻盈产出
@Compile-time
A
A’
B

轻/轻盈产出

拆分粒度/方案

轻/轻盈产出

```
0000000: 0200 0c00 4804 0000 0100 0000 0100 1c00  ....H...........
0000010: 8c00 0000 0400 0000 0000 0000 0001 0000  ................
0000020: 2c00 0000 0000 0000 0000 0000 2500 0000  ,...........%...
0000030: 4800 0000 5700 0000 2222 7265 732f 6d69  H...W..""res/mi
0000040: 706d 6170 2d68 6470 692d 7634 2f69 635f  pmap-hdpi-v4/ic_
0000050: 6c61 756e 6368 6572 2e70 6e67 0020 2072  launcher.png.  r
0000060: 6573 2f6d 6970 6d61 702d 6864 7069 2d76  es/mipmap-hdpi-v
0000070: 342f 6963 5f70 6c75 6769 6e2e 706e 6700  4/ic_plugin.png.
0000080: 0c0c 4c65 6172 6e69 6e67 4172 7363 0006  ..LearningArsc..
0000090: 0650 6c75 6769 6e00 0002 2001 b003 0000  .Plugin... .....
00000a0: 7f00 0000 6e00 6500 7400 2e00 7700 6500  ....n.e.t...w.e.
00000b0: 7100 7500 6900 6300 6b00 2e00 6100 7200  q.u.i.c.k...a.r.
00000c0: 7300 6300 0000 0000 0000 0000 0000 0000  s.c.............
00000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000110: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000120: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000130: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

resources.arsc

轻/轻盈产出/arsc格式

```
0000000: 0200 0c00 4804 0000 0100 0000 0100 1c00  ....H...........
0000010: 8c00 0000 0400 0000 0000 0000 0001 0000  ................
0000020: 2c00 0000 0000 0000 0000 0000 2500 0000  ,...........%...
0000030: 4800 0000 5700 0000 2222 7265 732f 6d69  H...W..""res/mi
0000040: 706d 6170 2d68 6470 692d 7634 2f69 635f  pmap-hdpi-v4/ic_
0000050: 6c61 756e 6368 6572 2e70 6e67 0020 2072  launcher.png.  r
0000060: 6573 2f6d 6970 6d61 702d 6864 7069 2d76  es/mipmap-hdpi-v
0000070: 342f 6963 5f70 6c75 6769 6e2e 706e 6700  4/ic_plugin.png.
0000080: 0c0c 4c65 6172 6e69 6e67 4172 7363 0006  ..LearningArsc..
0000090: 0650 6c75 6769 6e00 0002 2001 b003 0000  .Plugin... .....
00000a0: 7f00 0000 6e00 6500 7400 2e00 7700 6500  ....n.e.t...w.e.
00000b0: 7100 7500 6900 6300 6b00 2e00 6100 7200  q.u.i.c.k...a.r.
00000c0: 7300 6300 0000 0000 0000 0000 0000 0000  s.c.............
00000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000110: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000120: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000130: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

轻/轻盈产出/arsc格式

hex(LE) 小端代码	struct 数据结构
0200	ResTable_header
0100	ResStringPool_header
0002	ResTable_package
0100	ResStringPool_header
0100	ResStringPool_header
0202	ResTable_typeSpec
0102	ResTable_type

```
0100 0000 0100 1c00  ....H.........
0000 0000 0001 0000  ................
0000 0000 2500 0000  ,...........%...
2222 7265 732f 6d69  H...W...""res/mi
692d 7634 2f69 635f  pmap-hdpi-v4/ic_
2e70 6e67 0020 2072  launcher.png.  r
702d 6864 7069 2d76  es/mipmap-hdpi-v
6769 6e2e 706e 6700  4/ic_plugin.png.
6e67 4172 7363 0006  ..LearningArsc..
0002 2001 b003 0000  .Plugin... .....
7400 2e00 7700 6500  ....n.e.t...w.e.
6b00 2e00 6100 7200  q.u.i.c.k...a.r.
0000 0000 0000 0000  s.c.............
0000 0000 0000 0000  ................
0000 0000 0000 0000  ................
0000 0000 0000 0000  ................
0000 0000 0000 0000  ................
0000 0000 0000 0000  ................
0000120: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000130: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

轻/轻盈产出/arsc格式

hex(LE) 小端代码	struct 数据结构
0200	ResTable_header
0100	ResStringPool_header
0002	ResTable_package
0100	ResStringPool_header
0100	ResStringPool_header
0202	ResTable_typeSpec
0102	ResTable_type

```
0200 0c00 4804 0000 0100 0000 0100  1c00
8c00 0000 0400 0000 0000 0000 0001 0000
2c00 0000 0000 0000 0000 0000 2500 0000
4800 0000 5700 0000 2222 7265 732f 6d69
706d 6170 2d68 6470 692d 7634 2f69 635f
6c61 756e 6368 6572 2e70 6e67 0020 2072
6573 2f6d 6970 6d61 702d 6864 7069 2d76
342f 6963 5f70 6c75 6769 6e2e 706e 6700
0c0c 4c65 6172 6e69 6e67 4172 7363 0006
0650 6c75 6769 6e00 0002 2001 b003 0000
7f00 0000 6e00 6500 7400 2e00 7700 6500
7100 7500 6900 6300 6b00 2e00 6100 7200
7300 6300 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
```

轻/轻盈产出/arsc格式

hex(LE) 小端代码	struct 数据结构
0200	ResTable_header
0100	ResStringPool_header
0100	ResStringPool_header
0202	ResTable_typeSpec
0102	ResTable_type

资源ID	PP 包ID	TT 类型ID	NNNN 项目ID
0x			

```
table: {
  package: { id: 0x7F, name: "net.wequick.arsc" },
  strings: [
    "res/mipmap-hdpi-v4/ic_launcher.png",
    "res/mipmap-hdpi-v4/ic_plugin.png",
    "LearningArsc",
    "Plugin"
  ],                    01      02      03      04
  typeStrings: [ "attr", "mipmap", "string", "style" ],
  keyStrings: [
    "ic_launcher", "ic_plugin", "app_name",
    "s_plugin", "AppTheme", "PluginTheme"
  ],
  typeSpecs: [
01  { types: [] },                0000                0001
02  { types: [ Configs@ic_launcher, Configs@ic_plugin ] },
03  { types: [ Configs@app_name, Configs@s_plugin ] },
04  { types: [ Configs@AppTheme, Configs@PluginTheme ] }
  ]
}
```

资源ID 并非实际存在

轻/轻盈产出/arsc分离

想象中最简单的分离方式

```
host (0x7f)
    |-- mipmap (02)
    |       |-- ic_launcher (0000)
    |       `-- ic_plugin (0001)
    `-- values
            |-- strings.xml (03)
            |       |-- app_name (0000)
            |       `-- s_plugin (0001)
            `-- syles.xml (04)
                    |-- AppTheme (0000)
                    `-- PluginTheme (0001)
```

```
plugin (0x7f)
    |-- mipmap (02)
    |       |-- padding_mipmap_0000
    |
    `-- values
            |-- strings.xml (03)
            |       |-- padding_string_0000
            |
            `-- syles.xml (04)
                    |-- padding_style_0000
```

存在问题：必须补齐资源(输出变大)、只能分离一个插件

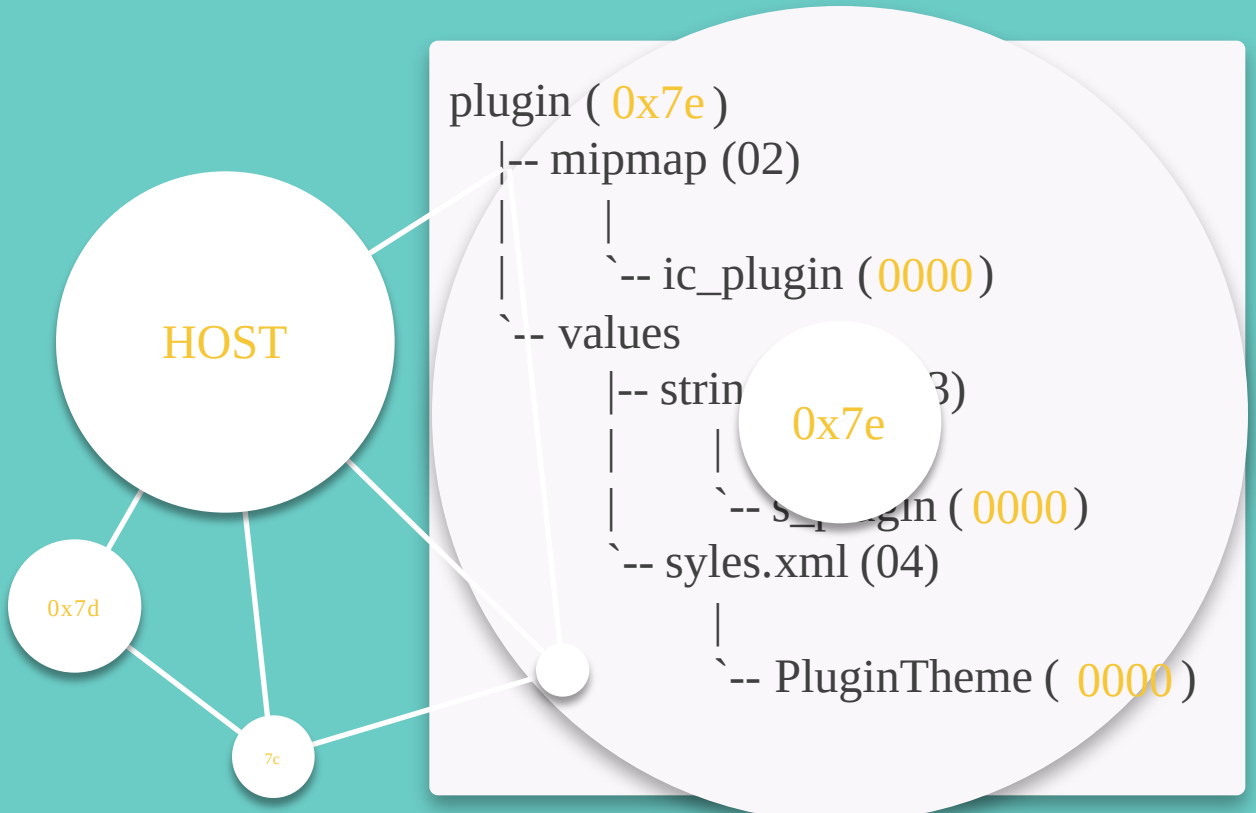
轻/轻盈产出/arsc分离

实践中最极致的分离方式

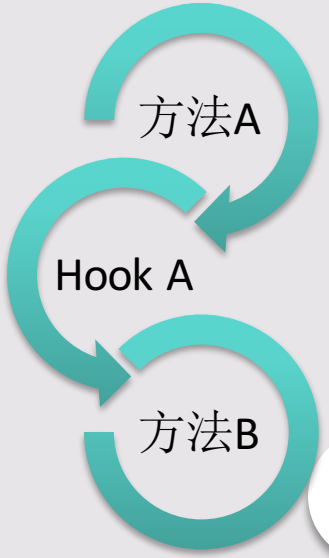
```
host (0x7f)
    |-- mipmap (02)
    |       |-- ic_launcher (0000)
    |
    `-- values
            |-- strings.xml (03)
            |       |-- app_name (0000)
            |
            `-- syles.xml (04)
                    |-- AppTheme (0000)
```

```
plugin ( 0x7e )
    |-- mipmap (02)
    |       |
    |       `-- ic_plugin (0000)
    `-- values
            |-- strings.xml (03)
            |       |
            |       `-- s_plugin ( 0000 )
            `-- syles.xml (04)
                    |
                    `-- PluginTheme (  0000 )
```

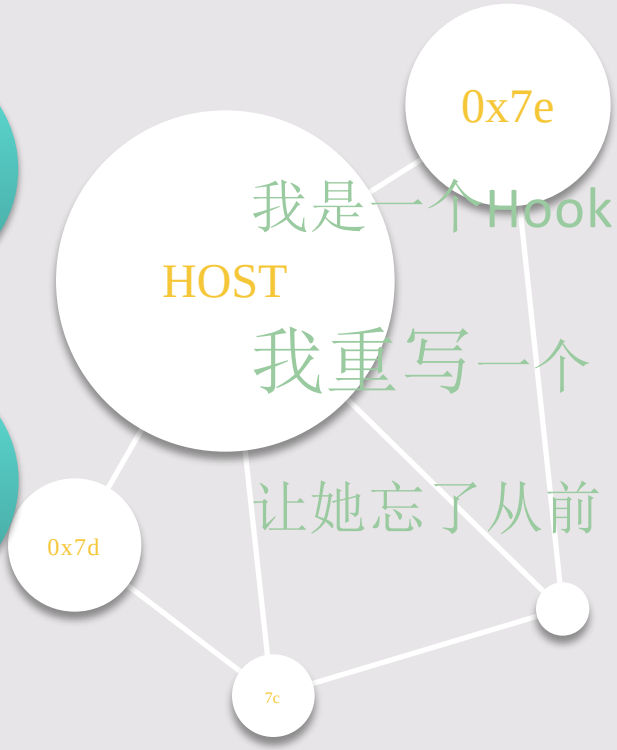
轻/轻盈产出


HOST
0x7d
7c
plugin (0x7e)
|-- mipmap (02)
|
`-- ic_plugin (0000)
`-- values
`-- syles.xml (04)
`-- PluginTheme (0000)
0x7e

轻/轻度Hook



一个对象

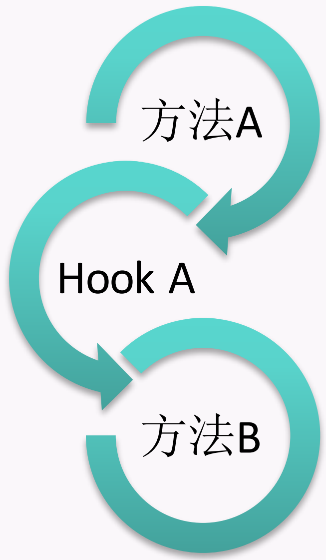


我是一个Hook

我重写一个「对象」的「方法」

让她忘了从前

轻/轻度Hook



一个对象

我是一个Hook

我是一个「对象」的「方法」

我重写

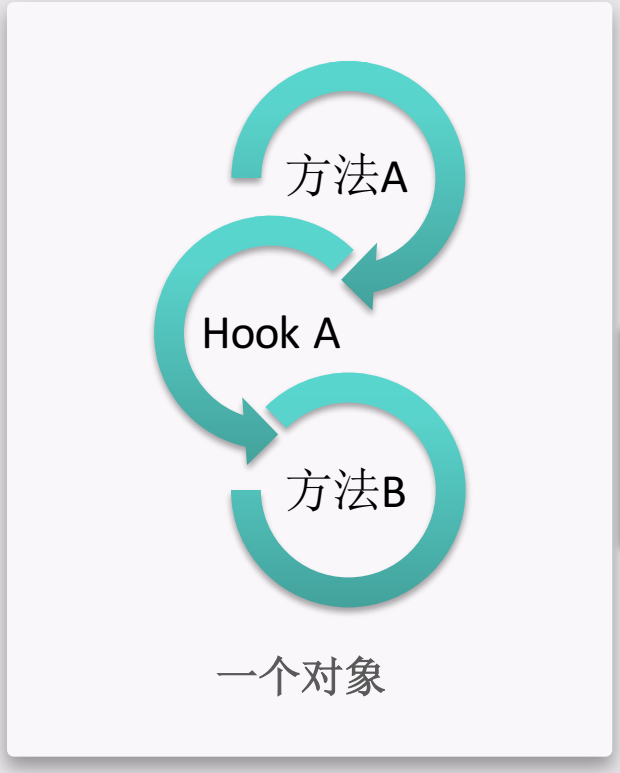
她「静态」的坐着

我让她思寻从前

她的方法由我「重放」

我触发她的进程

轻/轻度Hook



但是首先

我要找到她

在我的「进程」里

启动
插件Activity

坐着

她的方法向我「开放」

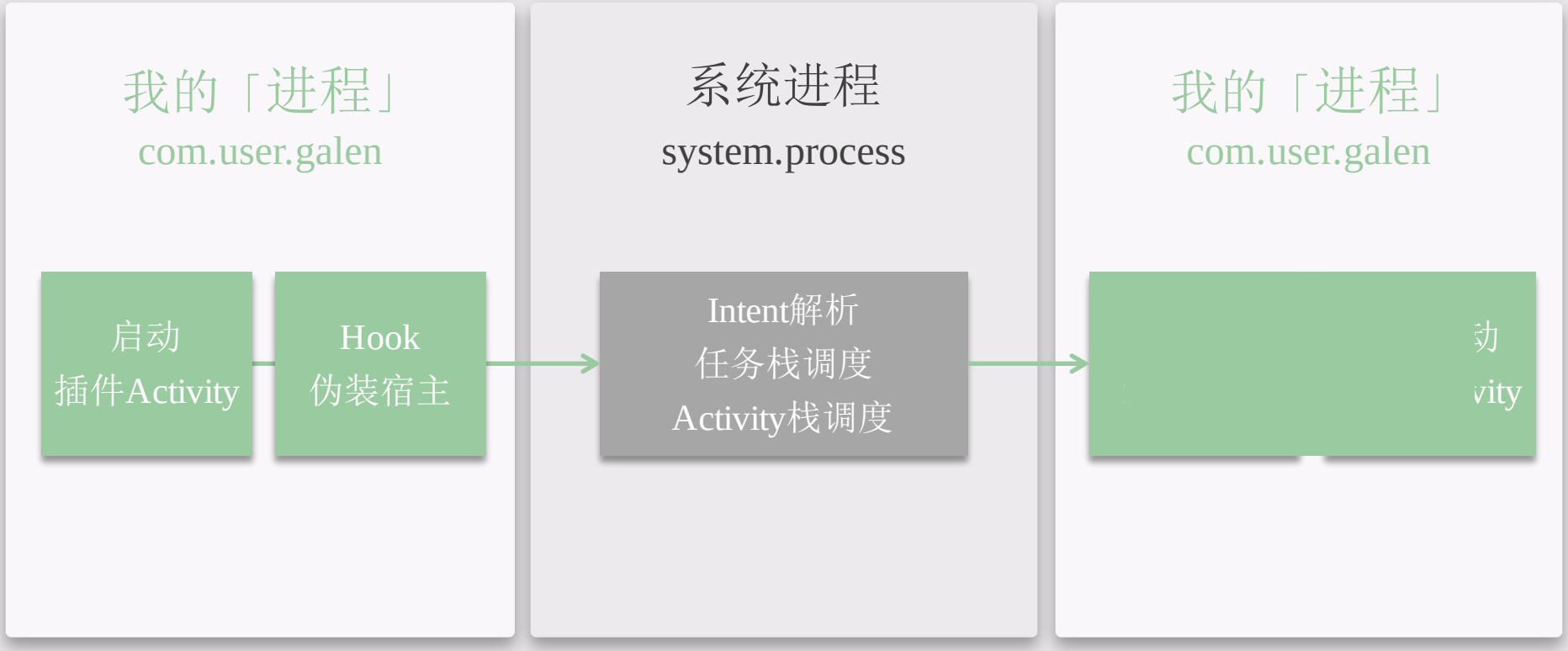
轻/轻度Hook


我的「进程」
com.user.galen
启动
插件Activity
系统进程
system.process
Intent解析
Activity栈调度
Not Found
我的「进程」
com.user.galen
实际启动
插件Activity

轻/轻度Hook


我的「进程」
com.user.galen
捆
系统进程
system.process
Intent解析
Activity栈调度
Not Found
我的「进程」
com.user.galen
实际启动
插件Activity

轻/轻度Hook


我的「进程」
com.user.galen
启动
插件Activity
Hook
伪装宿主
系统进程
system.process
Intent解析
任务栈调度
Activity栈调度
我的「进程」
com.user.galen

轻/轻度Hook

Small

Droid Plugin

Android-Plugin-Framework
ACDD

Dynamic-Load-APK
Direct-Load-APK

```
private Activity performLaunchActivity(ActivityClientRecord r, Intent customIntent) {
    // 创建Activity
    if (r.activityInfo.targetActivity != null) {
        component = new ComponentName(r.activityInfo.packageName,
                r.activityInfo.targetActivity);
    }
    java.lang.ClassLoader cl = r.packageInfo.getClassLoader();
    activity = mInstrumentation.newActivity(
            cl, component.getClassName(), r.intent);

    // 绑定Context
    Context appContext = createBaseContextForActivity(r, activity);
    activity.attach(appContext, this, getInstrumentation(), ...);
    // 设置主题
    int theme = r.activityInfo.getThemeResource();
    if (theme != 0) {
        activity.setTheme(theme);
    }

    // 触发onCreate
    mInstrumentation.callActivityOnCreate(activity, r.state);
}
```

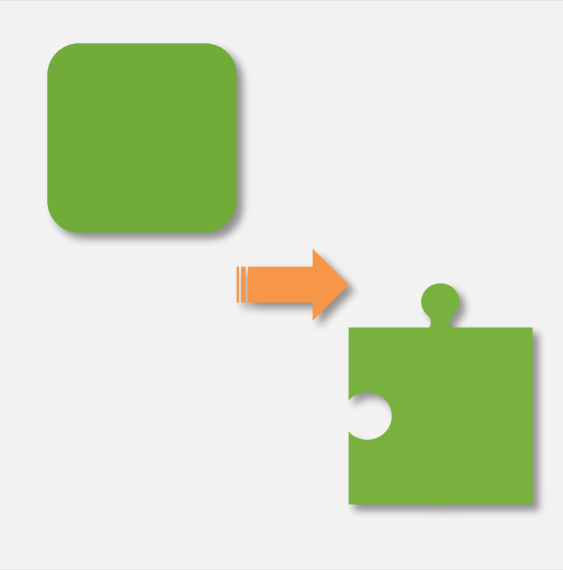
实际启动
插件Activity

轻/轻度Hook

插件方案	代表框架	包数	类加载器个数	资源管理器个数	Context
完全隔离	Droid Plugin	1/插件	1/插件	1/插件	1/插件
	Dynamic-Load-APK	1	1/插件	1/插件	1/插件Activity
	Direct-Load-APK	1	1/插件	1/插件	1/插件Activity
宿主插件两两融合	Android-Plugin-Framework	1	1/插件	1/插件	1/插件Activity
除主题外完全融合	ACDD	1	1	1	1/插件Activity
完全融合	Small	1	1	1	1

巧

IDE友好
@Debug

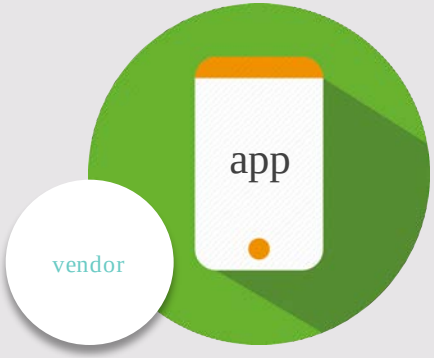


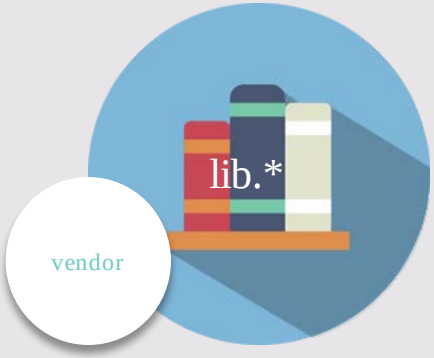
模块变身
@Release

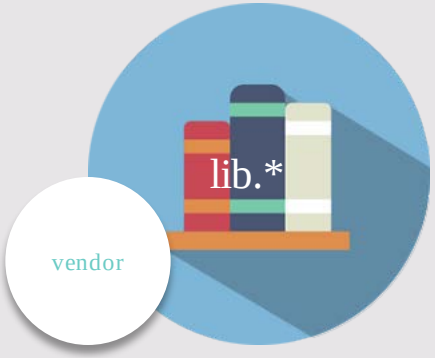
巧/IDE友好

巧/IDE友好

巧/IDE友好







巧/模块变身

模块是开发态，插件是目标态。

模块	开发态	目标态	转换难点
app.*	Application模块 可以依赖其他模块、可以独立运行	带代码、资源的插件	AAR(代码/资源) 剥离
lib.*	Library模块 可以被app.*依赖	带代码、资源的插件	资源ID锁定
[other].*	Application模块 可以独立运行	仅含assets的插件	

巧/模块变身

模块是开发态，插件是目标态。

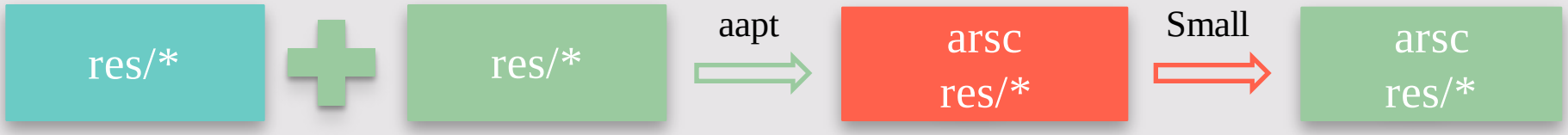
模块	开发态	目标态	转换难点
app.*	Application模块 可以依赖其他模块、可以独立运行	带代码、资源的插件	AAR (代码/资源) 剥离
lib.*	Library模块 可以被app.*依赖	带代码、资源的插件	资源ID锁定
[other].*	Application模块 可以独立运行	仅含assets的插件	

巧/模块变身

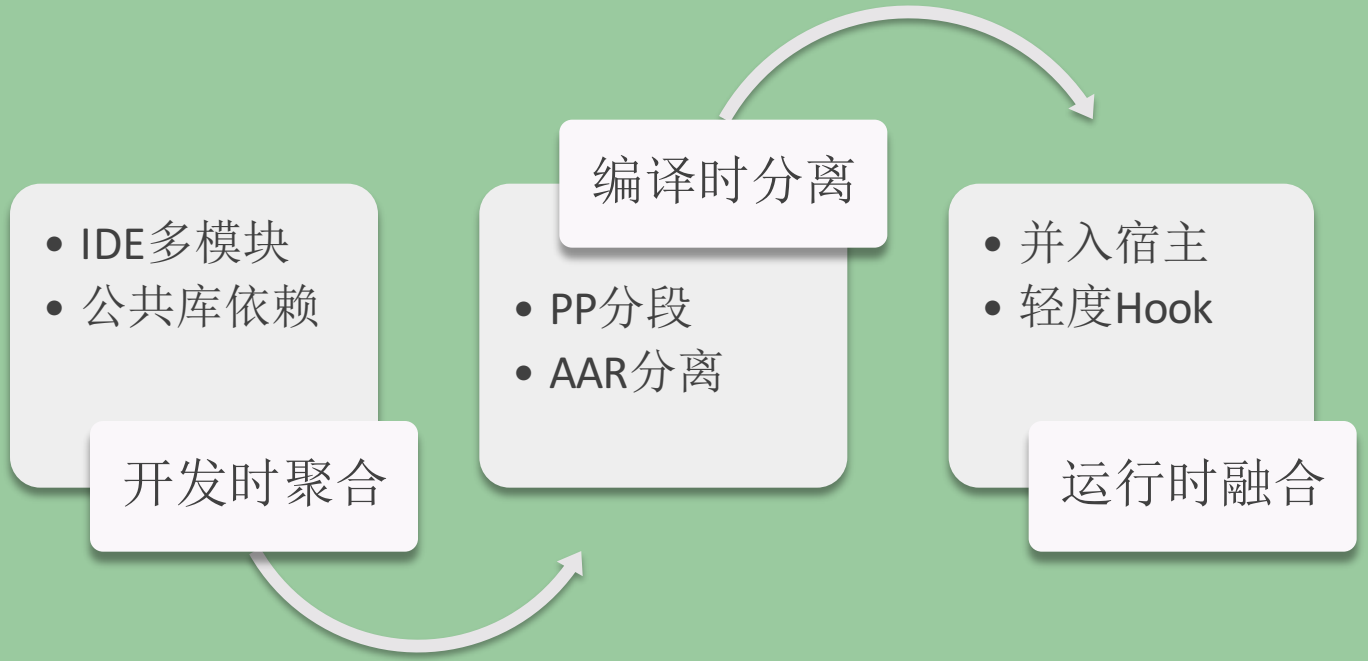
AAR

```
dependencies {
    provided fileTree(dir: 'libs', include: ['*.jar'])
    compile 'com.android.support:appcompat-v7:23.2.1'
    compile 'com.android.support:design:23.2.1'
}
```

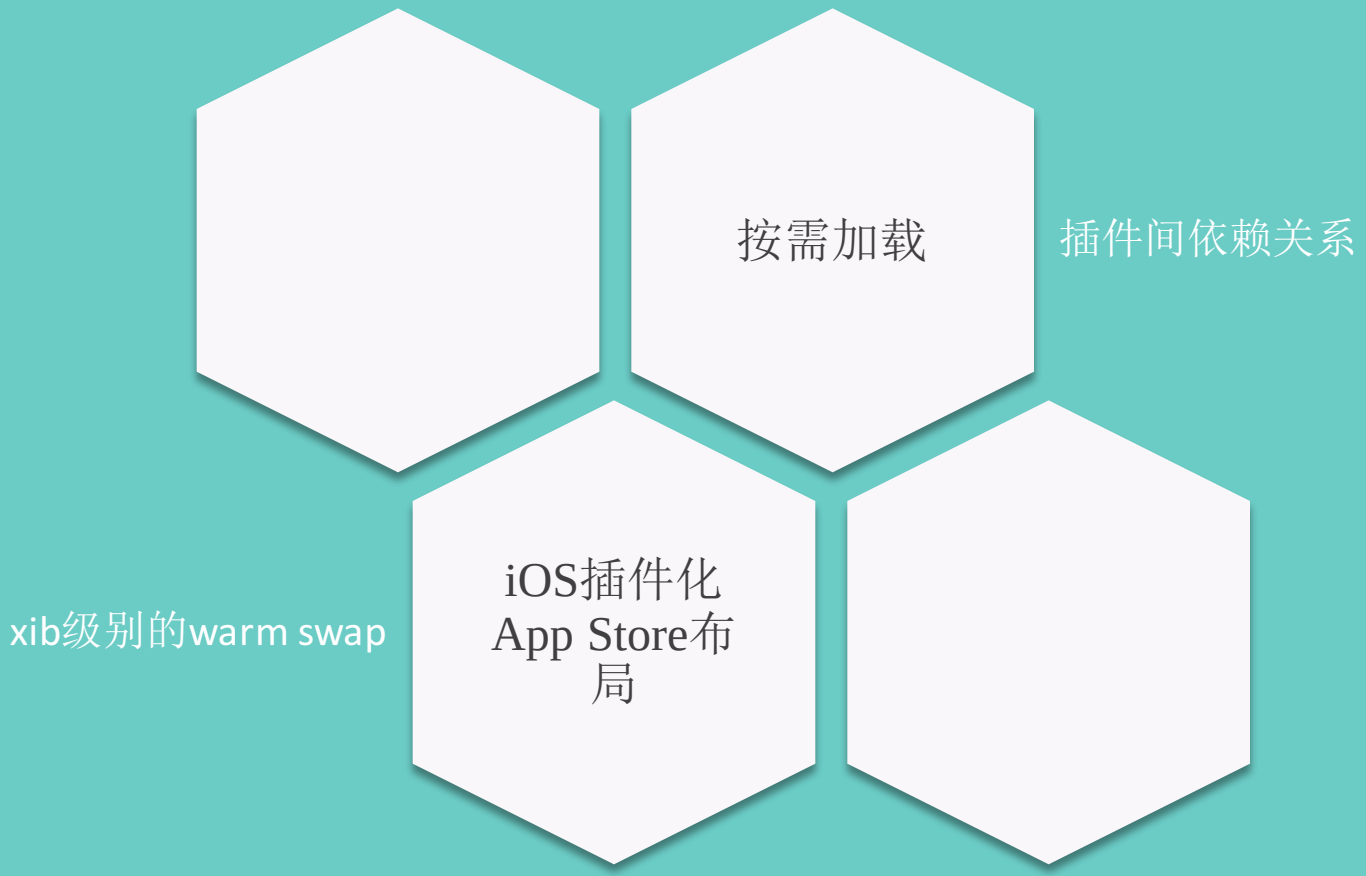
```
app.main
    `-- build/intermediates/exploded-aar
        `-- com.android.support/appcompat-v7/23.2.1
```



高级模块变身



总结



Q & A

Small@wequick
GalenLin