When JAVA going SMART: Android JNI Source Code Analysis

frostwing98

NJU-SWI

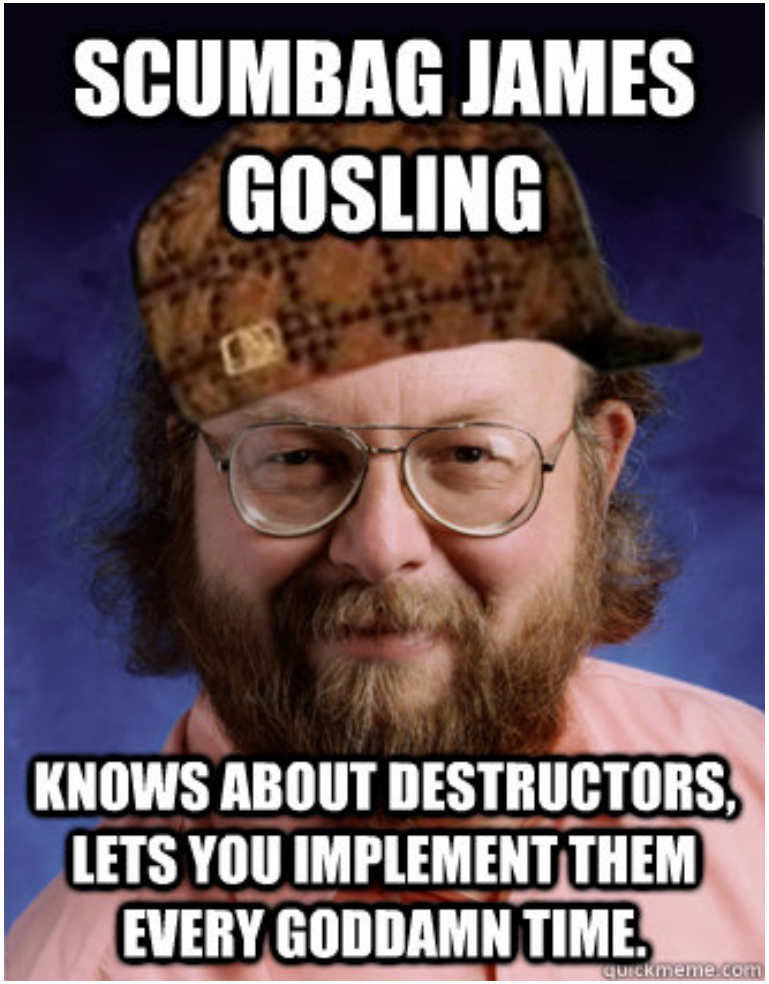
March 6, 2019

Table Of Contents I

Outline I


BJARNE STROUSTRUP
IS WATCHING YOU CODE
quickmeme.com


BJARNE STROUSTRUP
IS WATCHING YOU CODE
quickmeme.com


SCUMBAG JAMES GOSLING
KNOWS ABOUT DESTRUCTORS, LETS YOU IMPLEMENT THEM EVERY GODDAMN TIME.
quickmeme.com

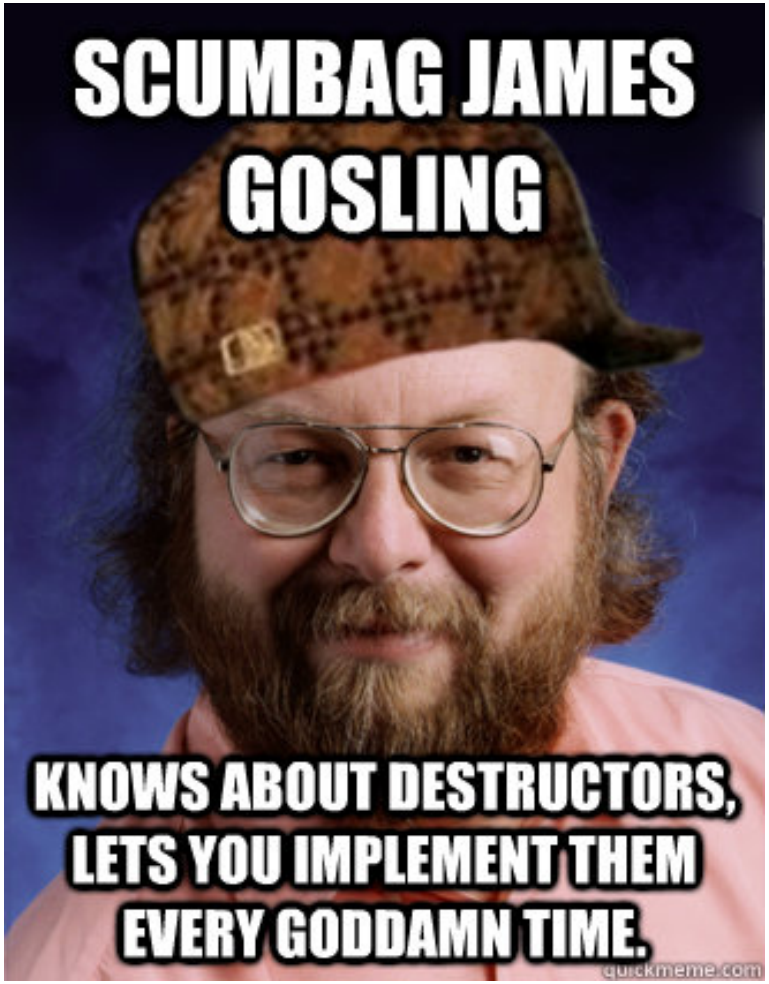


Figure: cpp ♂ java

What is JNI

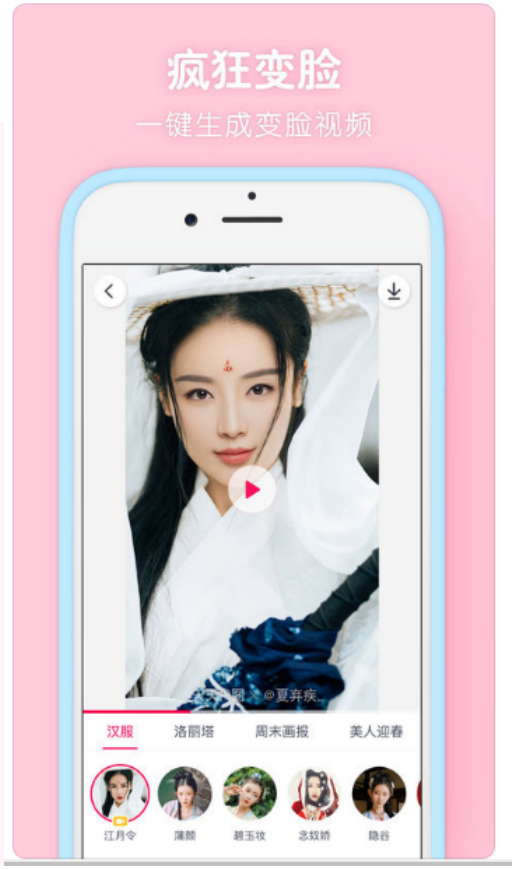
Java Native Interface

- A foreign function interface programming framework
- Enables Java code to call/be called by native applications
- Or libraries in C/C++

Outline I

Applications of JNI

Applications of JNI



Applications of JNI

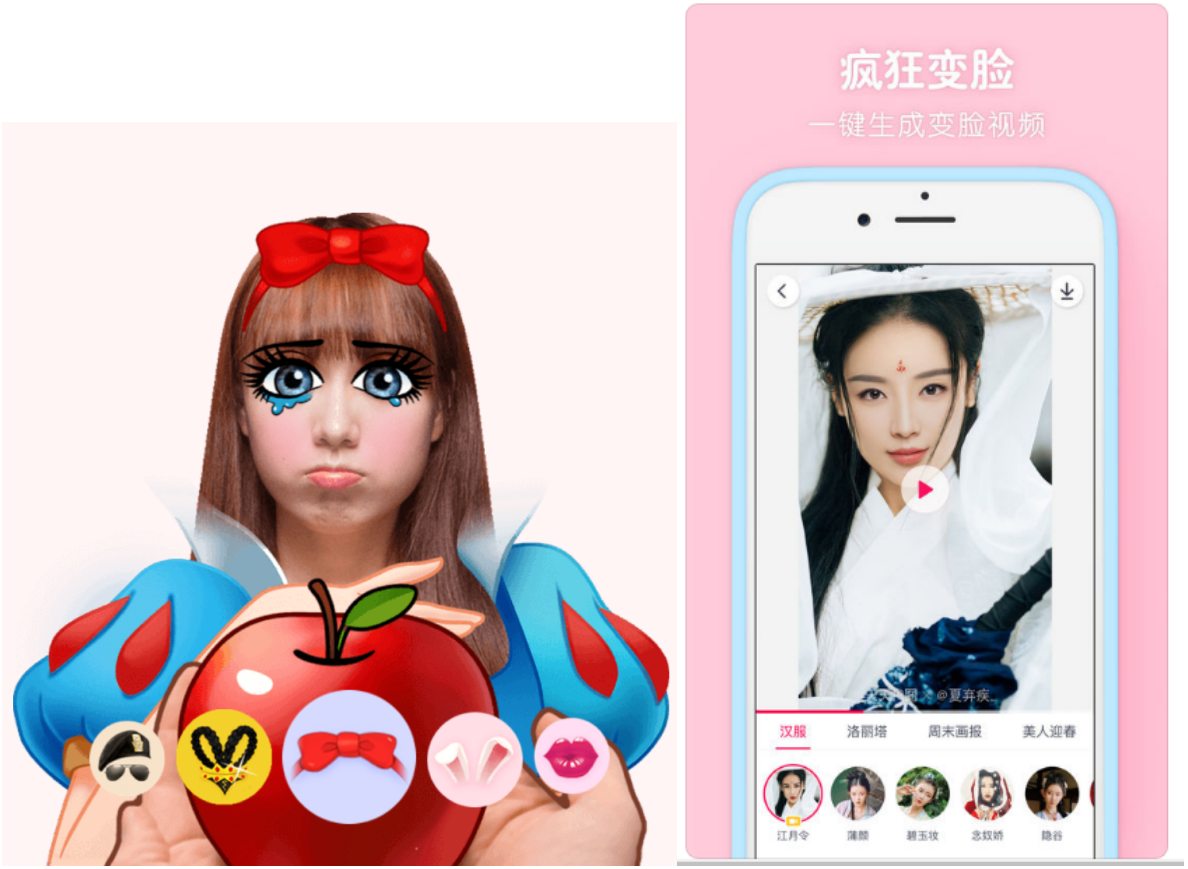


Figure: Android apps with DL frameworks

Outline I

JNI:An example

Outline I

From Init to Zygote

- After boot, Android starts **Init** process
- **Init** then calls **Zygote**
- **Zygote** is initiated. ▸ main->runtime.start()
- After **Init**, call **Zygote** which initiates Java VM and register jni methods.
  ▸ AndroidRuntime::start()->startReg()->register_jni_procs()

With Zygote into Runtime

Init I

- When calling register_jni_procs, register_android_os_MessageQueue is called.
  ▸ register_jni_procs()->register_android_os_MessageQueue()
- Then messageQueue registers the method. ▸ register_android_os_MessageQueue()->RegisterMethodsOrDie()
- Each jni methods calls RegisterMethodsOrDie().

Init II

- Runtime has several init methods, calling jniRegisterNativeMethods in JNIHelper. ▸ Runtime->jniRegisterNativeMethods
- The JNIEnv let JNINativeInterface to process: ▸ _JNIEnv struct

Outline I

Into JNIEnv

- JNINativeInterface has function pointer to RegisterNative: ▸ RegisterNative
- Then invoke RegisterNative let ArtMethod to register: ▸ JNINativeInterface->RegisterNative

Summary

- On boot the system inits init process, then zygote
- Zygote is the father of all APP processes, during the init the VM boots and framework JNI registered
- Zygote invoke register_xxx method to register each module
- Each module invokes RegisterMethodsOrDie to register JNINativeMtehod array
- Eventually it goes into the VM to update each ARTMethod entry_point_from_jni_ by SetNativePointer

Outline I

Through loadlibrary

- System ▸ System
- Runtime ▸ Runtime
- Then into jvm ▸ Runtime_nativeLoad->JVM_NativeLoad
- At last into JNI, ▸ JVM_NativeLoad->LoadNativeLibrary—>Java_OnLoad

Summary

- System.loadLibrary()
- LoadNativeLibrary
- JNI_OnLoad