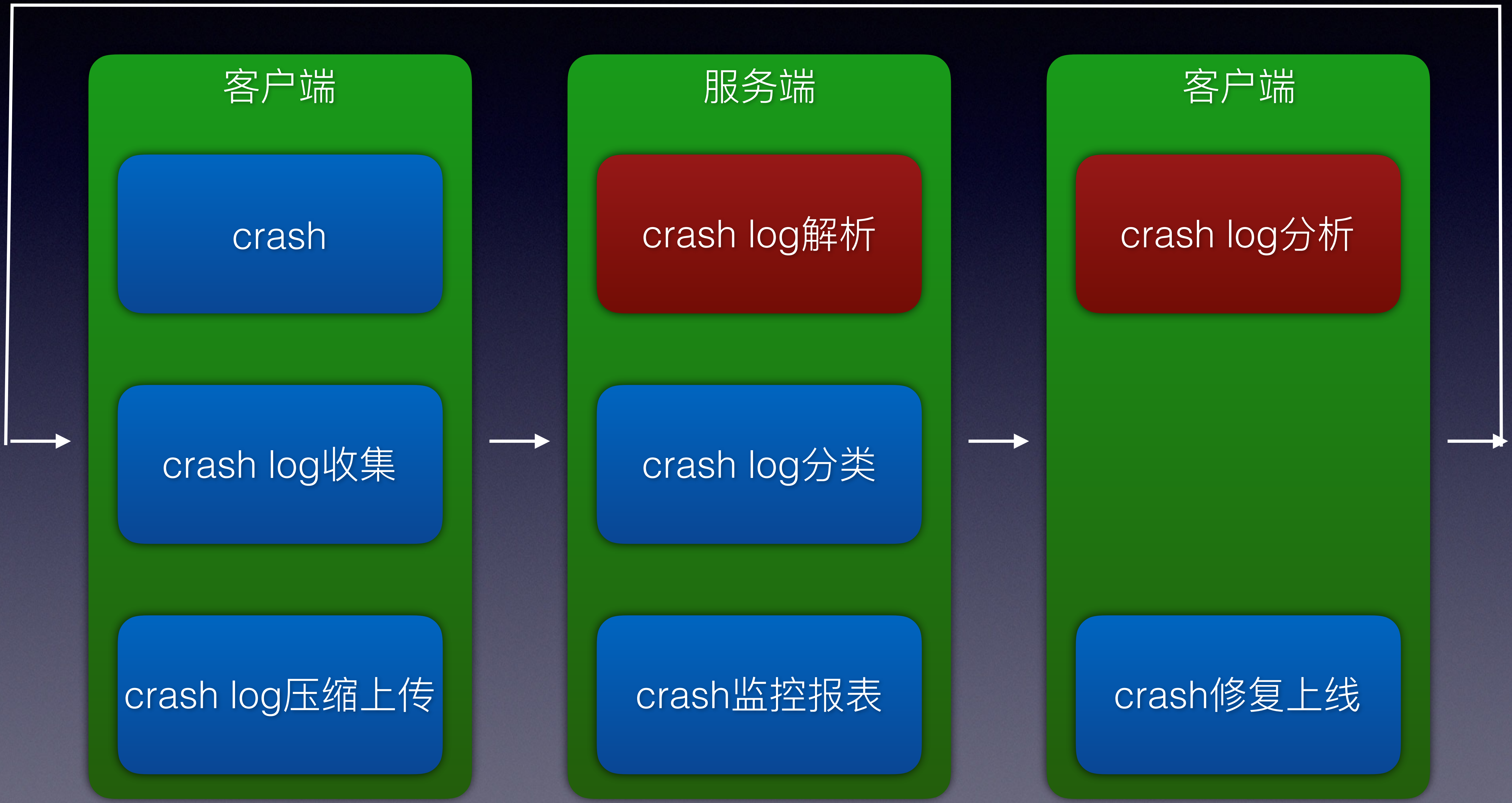
百度地图Crash跟踪体系及修复经验分享

iOS平台crash专项

- Crash跟踪体系
- Crash修复经验
- Case Study

Crash跟踪体系：crash



客户端

crash

crash log收集

crash log压缩上传

服务端

crash log解析

crash log分类

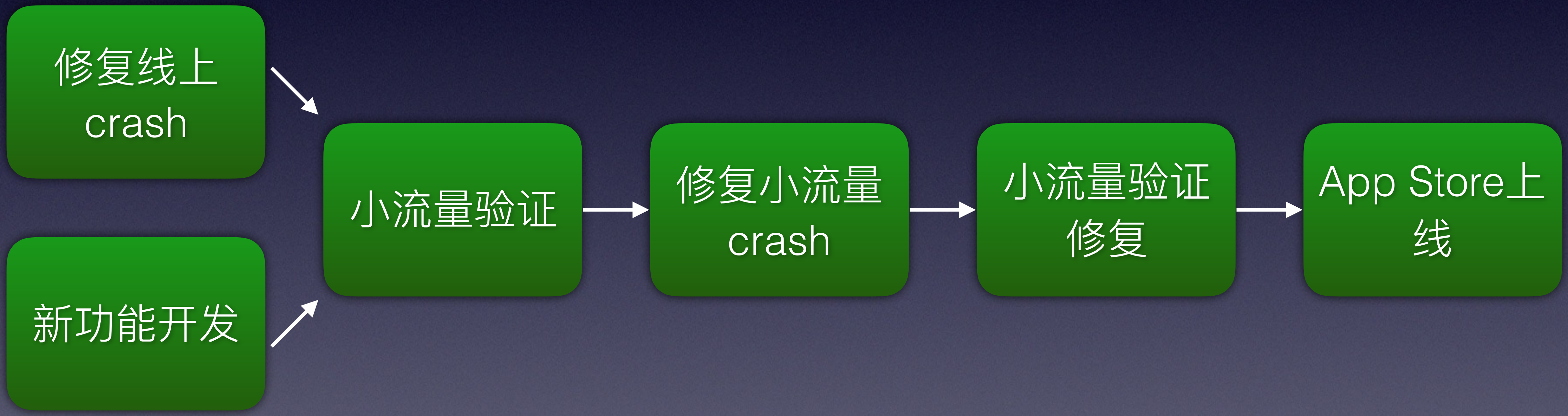
crash监控报表

客户端

crash log分析

crash修复上线

Crash跟踪体系： 发版



修复线上crash

新功能开发

小流量验证

修复小流量crash

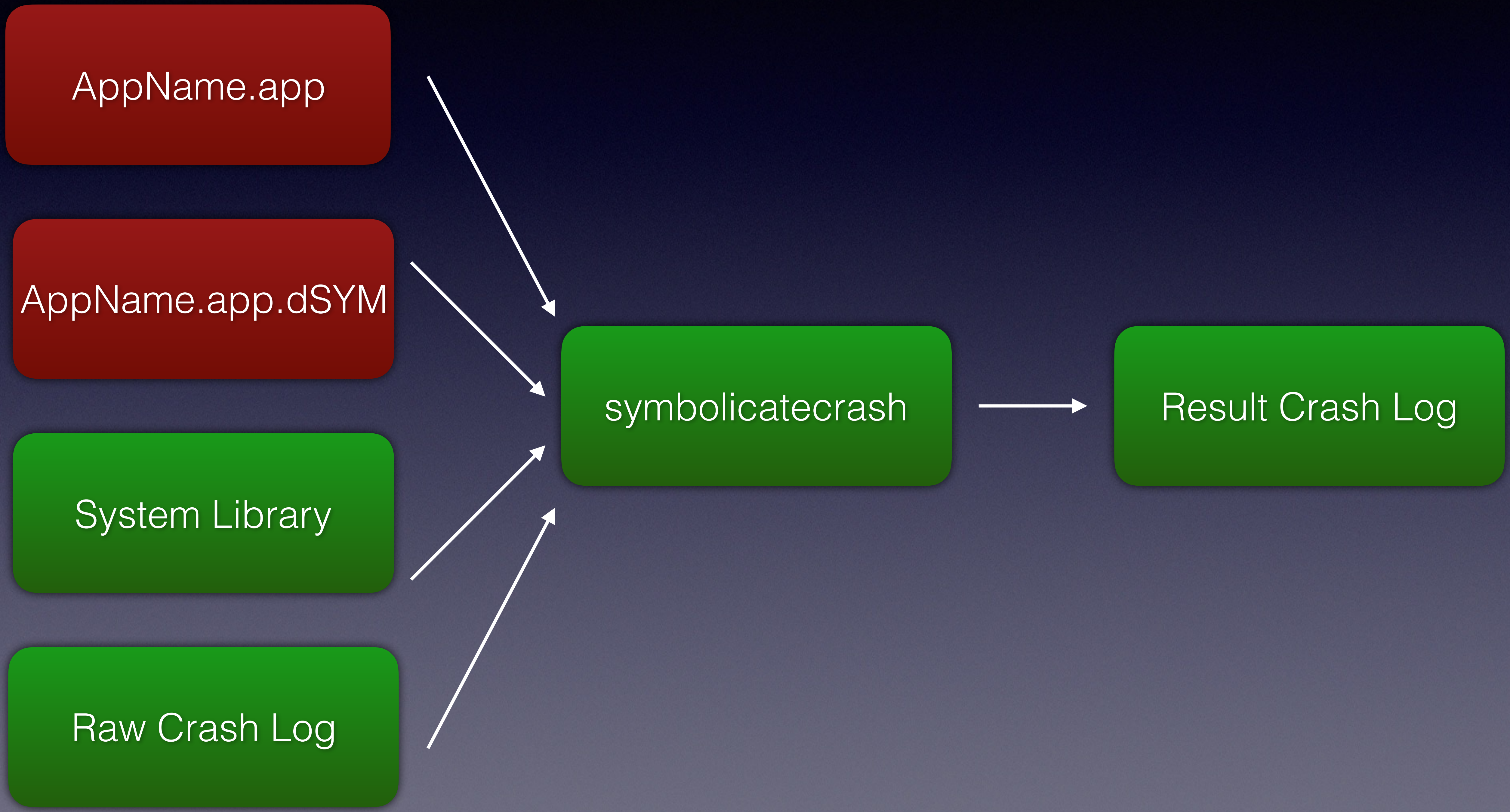
小流量验证修复

App Store上线

crash log的结构

- Header
- Exception Codes，Crashed Thread
- Last Exception Backtrace(Application Specific Information)
- Backtrace
- Thread State
- Binary Images
- 自定义内容

crash log解析



AppName.app

AppName.app.dSYM

System Library

Raw Crash Log

symbolicatecrash

Result Crash Log

crash log解析 FAQ:uuid

1. Crash Log

```
Binary Images:
       0x1000 -        0x222fff + AppName arm64  <1234567890abcdef1234567890abcdef> /var/
mobile/Containers/Bundle/Application/ABCDEF01-1234-5678-9ABC-DEF012345678/
AppName.app/AppName
```

2. App Binary(每个架构一行)

```
dwarfdump --uuid AppName.app/AppName
UUID: 12345678-90AB-CDEF-1234-567890ABCDEF (arm64) AppName.app/AppName
```

3. dSYM(每个架构一行)

```
dwarfdump -u AppName.app.dSYM
UUID: 12345678-90AB-CDEF-1234-567890ABCDEF (arm64) AppName.app.dSYM/Contents/
Resources/DWARF/AppName
```

crash log解析 FAQ:Spotlight

- Xcode Spotlight插件

```
/Applications/Xcode.app/Contents/Library/Spotlight/uuid.mdimporter
```

- mdfind

```
mdls AppName.app.dSYM/
com_apple_xcode_dsym_paths     = (
    "Contents/Resources/DWARF/AppName",
    "Contents/Resources/DWARF/AppName"
)
com_apple_xcode_dsym_uuids     = (
    "9F57F775-AF39-313B-8370-1B21E83B0327",
    "2D9C05E5-89B6-3C44-ADF3-A27EB5BFD87B"
)

mdfind "com_apple_xcode_dsym_uuids == 12345678-90AB-CDEF-1234-567890ABCDEF”
```

- 重新导入

```
mdimport AppName.app.dSYM/
```

crash log解析 FAQ:atos

atos命令的选项:

1. -o 程序或者库的地址
2. -arch
3. -l 加载地址

```
atos -arch arm64 -l 0x100078000 -o AppName.app/AppName 0x0000000101109170
0x0000000101b52c08 0x0000000101124aa4 0x00000001011273e4

Binary Images:
       0x1000 -        0x222fff +AppName arm64  <1234567890abcdef1234567890abcdef> /var/mobile/
Containers/Bundle/Application/ABCDEF01-1234-5678-9ABC-DEF012345678/AppName.app/
AppName
```

crash修复

- 预防
- 日志阅读顺序
- 复现
- 常见crash类型
- 系统crash

crash修复：预防

- Warning
- Static analyze
- Enable Address Sanitizer
- Method swizzle（release运行时）
- 尽早crash，尽一切可能crash

crash修复：顺序

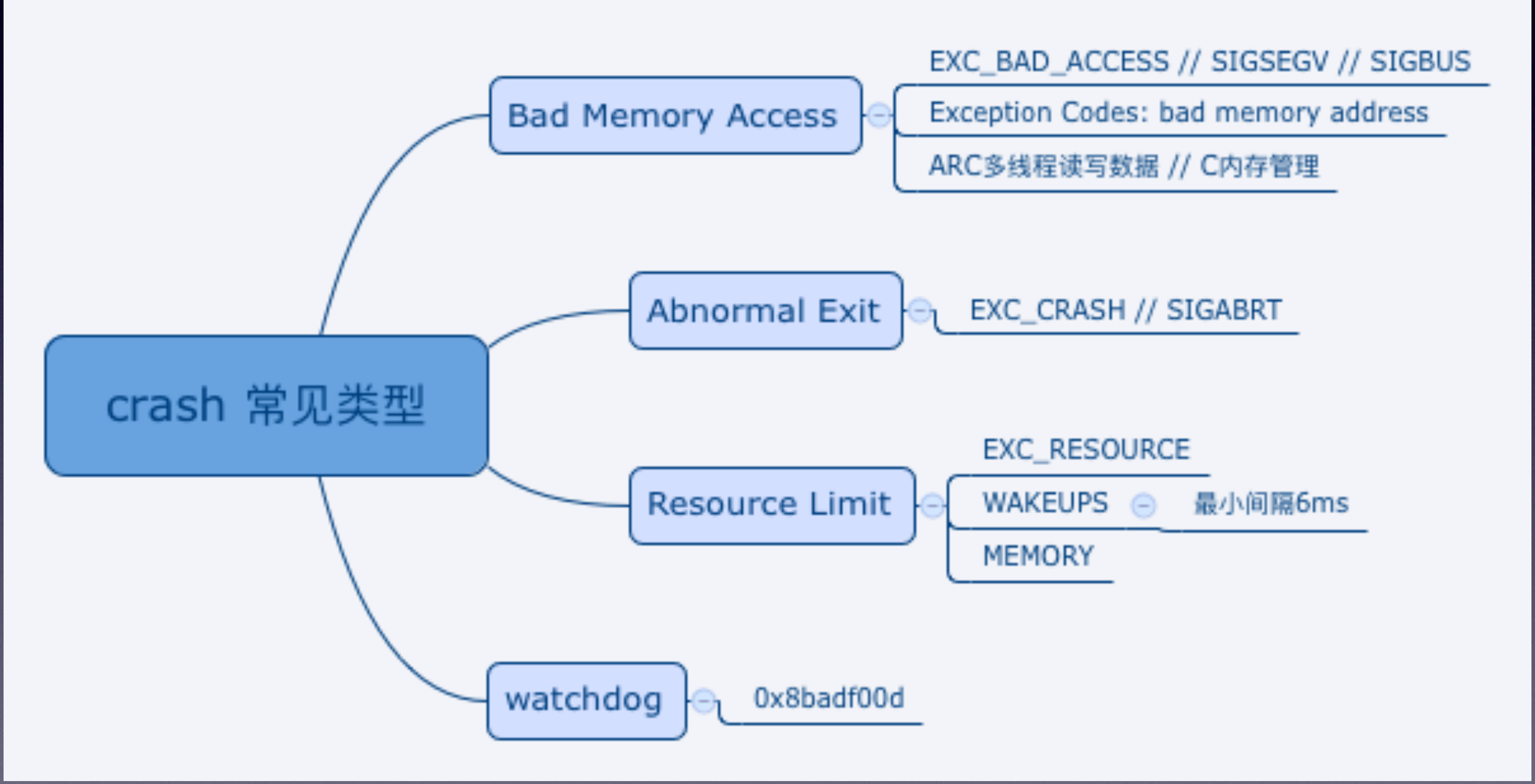
- Last Exception Backtrace
- Exception Codes，Crashed Thread
- Backtrace (crashed thread)
- Thread State
- 自定义内容，页面跳转，点击事件

crash修复：复现

调试器：

1. 相同的Xcode，相同的代码，release版本
2. 符号断点，从app到系统库，从特殊到一般
3. 读写变量 / 寄存器，复现crash
4. 逆向分析crash原因

常见crash类型



crash 常见类型

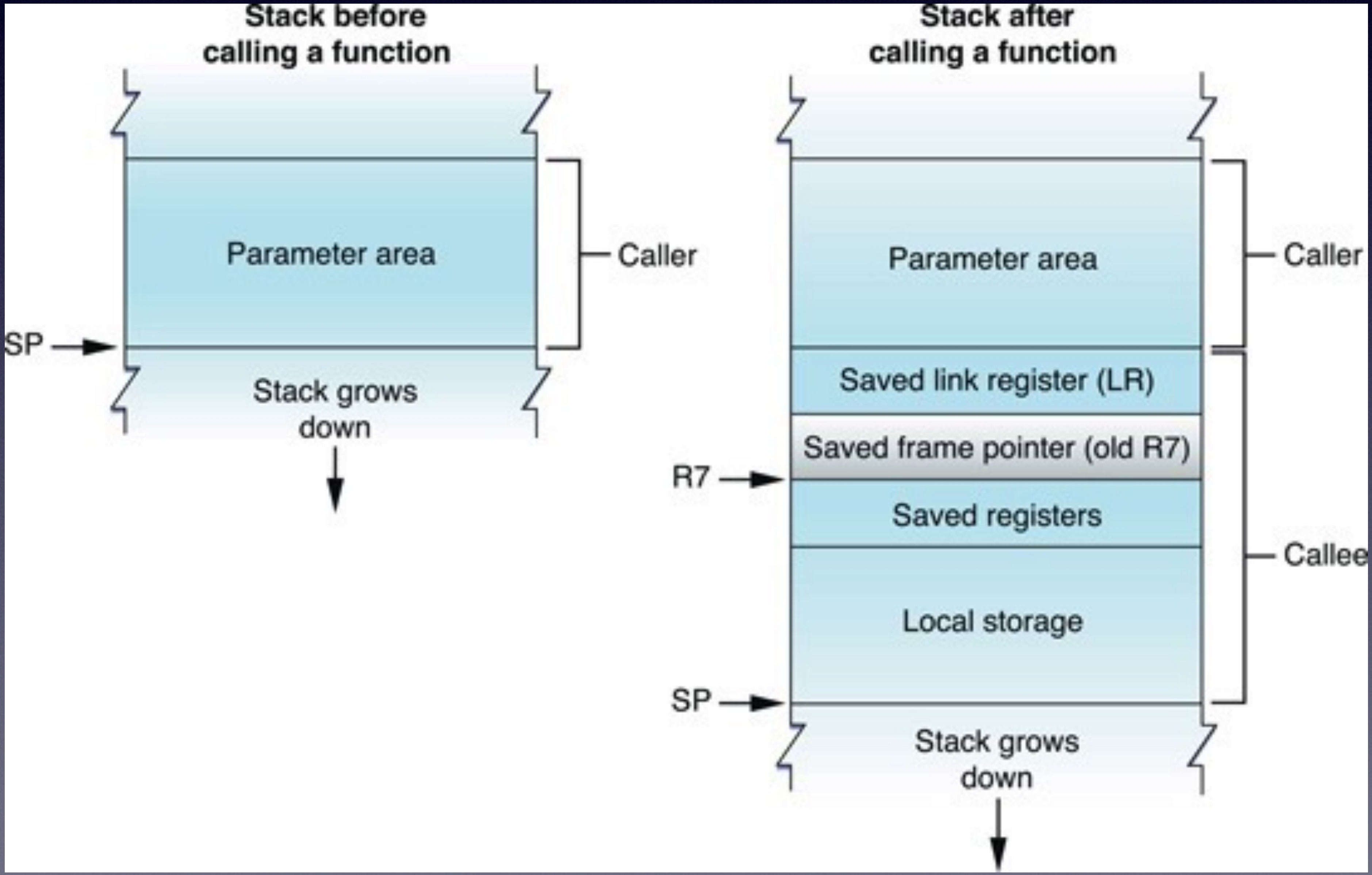
- Bad Memory Access
  - EXC_BAD_ACCESS // SIGSEGV // SIGBUS
  - Exception Codes: bad memory address
  - ARC多线程读写数据 // C内存管理
- Abnormal Exit
  - EXC_CRASH // SIGABRT
- Resource Limit
  - EXC_RESOURCE
  - WAKEUPS
    - 最小间隔6ms
  - MEMORY
- watchdog
  - 0x8badf00d

crash修复：系统crash

- 自定义日志
- 相关代码review
- 猜一猜

crash修复：一点汇编

- 调用约定，参数传递，返回值



crash修复：总结

- 确定性系统
- 分析数据
- 不轻易放过你曾经追过的crash

Case study: 快速枚举

```
// PBArray is an immutable array class that's optimized for storing primitive
// values.  All values stored in an PBArray instance must have the same type
// (PBArrayValueType).  Object values (PBArrayValueTypeObject) are retained.
@interface PBArray : NSObject <NSCopying, NSFastEnumeration>
{
@protected
    PBArrayValueType    _valueType;
    NSUInteger          _capacity;
    NSUInteger          _count;
    void *              _data;
}

- (NSUInteger)count;
- (id)objectAtIndex:(NSUInteger)index;
- (BOOL)boolAtIndex:(NSUInteger)index;
- (int32_t)int32AtIndex:(NSUInteger)index;
- (uint32_t)uint32AtIndex:(NSUInteger)index;
- (int64_t)int64AtIndex:(NSUInteger)index;
- (uint64_t)uint64AtIndex:(NSUInteger)index;
- (Float32)floatAtIndex:(NSUInteger)index;
- (Float64)doubleAtIndex:(NSUInteger)index;
- (BOOL)isEqualToArray:(PBArray *)array;

@property (nonatomic,assign,readonly) PBArrayValueType valueType;
@property (nonatomic,assign,readonly) const void * data;
@property (nonatomic,assign,readonly,getter=count) NSUInteger count;

@end
```

Case study: 快速枚举

```
typedef struct {
    unsigned long state;
    id __unsafe_unretained __nullable * __nullable itemsPtr;
    unsigned long * __nullable mutationsPtr;
    unsigned long extra[5];
} NSFastEnumerationState;


- (NSUInteger)countByEnumeratingWithState:(NSFastEnumerationState *)state objects:(id
*)stackbuf count:(NSUInteger)len
{
    PBArrayValueTypeAssert(PBArrayValueTypeObject);

    if (state->state >= _count)
    {
       return 0; // terminate iteration
    }

    state->itemsPtr = (id *)_data;
    state->state = _count;
    state->mutationsPtr = (unsigned long *)self;

    return _count;
}
```

Case study: 快速枚举

```
    NSArray *array = @[@"ABC", @"DEF", @"GHI"];
    for (NSString *str in array) {
        NSLog(@"%@", str);
    }
// Rewriter for ObjC2's foreach statement:
    NSString *elem;
    NSFastEnumerationState enumState = { 0 };
    __unsafe_unretained id __rw_items[16];
    id l_collection = (id)array;
    unsigned long limit = [l_collection countByEnumeratingWithState:&enumState
                                                            objects:__rw_items count:16];
    if (limit) {
        unsigned long startMutations = *enumState.mutationsPtr;
        do {
            unsigned long counter = 0;
            do {
                if (startMutations != *enumState.mutationsPtr)
                    objc_enumerationMutation(l_collection);
                elem = (NSString *)enumState.itemsPtr[counter++];
                NSLog(@"%@", elem);;
            __continue_label: ;
            } while (counter < limit);
        } while ((limit = [l_collection countByEnumeratingWithState:&enumState
                                                            objects:__rw_items count:16]))
        elem = nil;
    __break_label: ;
    }
    else
        elem = nil;
```

Case study: 快速枚举

- 代码没有修改
- 发生在64位设备
- 64-Bit Transition Guide for Cocoa Touch
- Tagged pointers

```
- (NSUInteger)countByEnumeratingWithState:(NSFastEnumerationState *)state objects:(id
*)stackbuf count:(NSUInteger)len
{
    PBArrayValueTypeAssert(PBArrayValueTypeObject);

    if (state->state >= _count)
    {
       return 0; // terminate iteration
    }

    state->itemsPtr = (id *)_data;
    state->state = _count;
    state->mutationsPtr = (unsigned long *)object_getClass(self);

    return _count;
}
```

Case study: OpenGL ES

```
Thread 0 name: Dispatch queue: com.apple.main-thread
Thread 0 Crashed:
0  libGPUSupportMercury.dylib   0x30570094 gpus_ReturnNotPermittedKillClient + 0
1  libGPUSupportMercury.dylib   0x305700ae gpus_KillClient ( )
2  libGPUSupportMercury.dylib   0x305705ba gpusSubmitDMABuffers ( )
3  IMGSGX535GLDriver            0x34bd29b8 SubmitPacketsIfAny ( )
4  IMGSGX535GLDriver            0x34bd2ad0 glrFlushContextToken ( )
5  GLEngine                 0x37719c4a gliPresentViewES ( )
6  OpenGLES                 0x323df6b4 -[EAGLContext presentRenderbuffer:] ( )
```

Technical Q&A QA1766
How to fix OpenGL ES application crashes when moving to the background

Case study: OpenGL ES

```
Thread 32 Crashed:
0   libGPUSupportMercury.dylib        0x000000018ec21f08 gpus_ReturnNotPermittedKillClient + 12
1   WebCore                           0x0000000184c6fc90 WebCore::GraphicsContext3D::reshape(int, int) + 528
2   WebCore                           0x000000018557a2d4
WebCore::WebGLRenderingContextBase::initializeNewContext() + 640
3   WebCore                           0x0000000185579d78
WebCore::WebGLRenderingContextBase::WebGLRenderingContextBase(WebCore::HTMLCanvasElement
*, WTF::PassRefPtr<WebCore::GraphicsContext3D>, WebCore::GraphicsContext3D::Attributes) + 516
4   WebCore                           0x0000000185573248
WebCore::WebGLRenderingContext::WebGLRenderingContext(WebCore::HTMLCanvasElement*,
WTF::PassRefPtr<WebCore::GraphicsContext3D>, WebCore::GraphicsContext3D::Attributes) + 40
5   WebCore                           0x000000018557954c
WebCore::WebGLRenderingContextBase::create(WebCore::HTMLCanvasElement*,
WebCore::WebGLContextAttributes*, WTF::String const&) + 1280
…
…
```

Q&A