内容目录

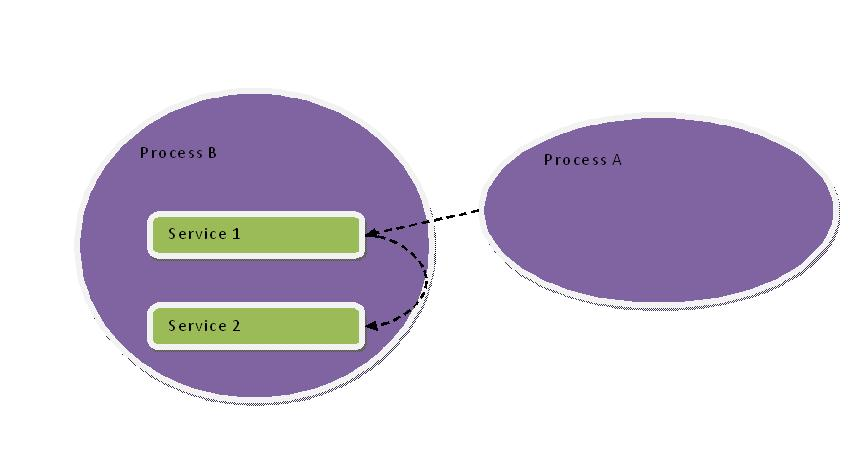
[clearCallingIdentity/restoreCallingIdentity 1](#__RefHeading___Toc7917_695259283)

[binderDied 1](#__RefHeading___Toc7919_695259283)

[oneway 2](#__RefHeading___Toc7921_695259283)

### clearCallingIdentity/restoreCallingIdentity

客户端A调用服务端B的服务，然后B又调用自己的服务或者方法

1. process B在被process A IPC调用时, process B需知道process A的UID和PID，来检查process A的访问权限，此时mCallingUid和mCallingPid保存的是process A的UID和PID。

2. 在IPC远程调用process B的过程中，process B的方法调用了同进程中的service的接口，process B既是调用方也是被调用方，虽然这个过程比较无聊，但是鉴于IPC过程的不透明性，因此process B仍然需要进行权限检测。

在B进程自己调用自己资源的时候可通过如下两个方法

public static final native long clearCallingIdentity();

public static final native void restoreCallingIdentity(long token);

先将A的UID、PID进行备份并且替换B的UID、PID，开始操作B的资源

token = clearCallingIdentity();

调用完成后，再恢复成A的UID、PID

### binderDied

**1. 原理**

当Binder非正常消亡的时候，会导致远程调用失败，这样客户端功能就会受到影响。

解决：给Binder设置一个死亡代理，当Binder死亡时，我们就会收到通知，这个时候可以重新发起连接。

**2. 制作**

**2.1 前期准备**

客户端：MainActivity.java

@Override

protected void onCreate(Bundle savedInstanceState) {

super.onCreate(savedInstanceState);

setContentView(R.layout.activity\_main);

createService();

}

/\*连接Service端，获取mIBookManger\*/

private void createService(){

ServiceConnection connection = new ServiceConnection() {

@Override

public void onServiceConnected(ComponentName name, IBinder service) {

//初始化mIBookManger

mIBookManager = IBookManager.Stub.asInterface(service);

}

@Override

public void onServiceDisconnected(ComponentName name) {

}

};

Intent intent = new Intent(this,BookService.class);

bindService(intent,connection,BIND\_AUTO\_CREATE);

}

Service端：BookService.java

**2.2使用**

创建IBinder.DeathRecipient接口，重写其中的binderDied()，当Binder死亡时候，回调该方法。

private IBinder.DeathRecipient mDeathRecipient = new IBinder.DeathRecipient() {

@Override

public void binderDied() {

if (mIBookManager != null){

//解除绑定当前接口

mIBookManager.asBinder().unlinkToDeath(mDeathRecipient,0);

}

mIBookManager = null;

createService();

}

};

当然解除绑定之后，还需要绑定接口

/\*连接Service端，获取mIBookManger\*/

private void createService(){

...(连接之前的代码)

try {

//绑定接口,等待回调

mIBookManager.asBinder().linkToDeath(mDeathRecipient,0);

} catch (RemoteException e) {

e.printStackTrace();

}

}

### oneway

oneway 关键字用于修改远程调用的行为。

1.本地调用

如果 oneway 用于本地调用，则不会有任何影响，调用仍是同步调用。

2.远程调用

使用该关键字时，远程调用不会阻塞；它只是发送事务数据并立即返回。接口的实现最终接收此调用时，是以正常远程调用形式将其作为来自 Binder 线程池的常规调用进行接收。

注意，IBinder接口类中定义了一个名为FLAG\_ONEWAY的整型变量，该变量的意义非常重要。当客户端利用Binder机制发起一个跨进程的函数调用时，调用方（即客户端）一般会阻塞，直到服务端返回结果。这种方式和普通的函数调用是一样的。但是在调用Binder函数时，如果指明了FLAG\_ONEWAY标志，则调用方只要把请求发送到Binder驱动即可返回，而不用等待服务端的结果，这就是一种所谓的非阻塞方式。在Native层中，涉及的Binder调用基本都是阻塞的，但是在Java层的framework中，使用FLAG\_ONEWAY进行Binder调用的情况非常多，以后经常会碰到。

思考：使用FLAG\_ONEWAY进行函数调用的程序在设计上有什么特点？这里简单分析一下：对于使用FLAG\_ONEWAY的函数来说，客户端仅向服务端发出了请求，但是并不能确定服务端是否处理了该请求。所以，客户端一般会向服务端注册一个回调（同样是跨进程的Binder调用），一旦服务端处理了该请求，就会调用此回调函数来通知客户端处理结果。当然，这种回调函数也大多采用FLAG\_ONEWAY的方式。

# 一 binder调用 overview

## 1.1 C程序示例

git clone https://github.com/weidongshan/APP\_0003\_Binder\_C\_App.git

### 1.1.1 框架分析

frameworks/native/cmds/servicemanager/bctest.c

注册服务的过程:

a. binder\_open

b. binder\_call(bs, &msg, &reply, 0, SVC\_MGR\_ADD\_SERVICE)

// 含有服务的名字

// 它会含有servicemanager回复的数据

// 0表示servicemanager

// code: 表示要调用servicemanager中的"addservice函数"

获取服务的过程:

a. binder\_open

b. binder\_call(bs, &msg, &reply, target, SVC\_MGR\_CHECK\_SERVICE)

// 含有服务的名字

// 它会含有servicemanager回复的数据, 表示提供服务的进程

// 0表示servicemanager

// code: 表示要调用servicemanager中的"getservice函数"

Binder系统\_C程序框架分析了binder\_call函数对binder\_io的解析处理，交给binder\_write\_read的write\_buffer/read\_buffer。

### 1.1.2 编写程序

服务端：test\_server.c

客服端：test\_client.c

## 1.2 驱动情景分析

git clone https://github.com/weidongshan/DRV\_0003\_Binder.git

### 1.2.1数据结构浅析

test\_client.c

handle = svcmgr\_lookup(bs, svcmgr, "goodbye");

handle = svcmgr\_lookup(bs, svcmgr, "hello");

handle是进程A对进程B提供的服务的引用。

Binder系统\_驱动情景分析1\_IPC数据交互过程.jpg

### 1.2.2 打印数据交互过程

应用程序，BC\_TRANSACTION、BC\_REPLY写，BR\_TRANSACTION、BR\_REPLY读。只有这四个涉及到进程间的交互，其他的BC和BR是和驱动之间的交互用于改变和报告状态。

res = ioctl(bs->fd, BINDER\_WRITE\_READ, &bwr);

drivers/android/binder.c

static long binder\_ioctl(struct file \*filp, unsigned int cmd, unsigned long arg)

switch (cmd) {

case BINDER\_WRITE\_READ:

ret = binder\_ioctl\_write\_read(filp, cmd, arg, thread);

case BC\_TRANSACTION:

binder\_transaction(proc, thread, &tr, cmd == BC\_REPLY, 0);

}

static int binder\_ioctl\_write\_read(struct file \*filp,

unsigned int cmd, unsigned long arg,

struct binder\_thread \*thread) {

ret = binder\_thread\_write(proc, thread, bwr.write\_buffer, bwr.write\_size, &bwr.write\_consumed);

ret = binder\_thread\_read(proc, thread, bwr.read\_buffer, bwr.read\_size, &bwr.read\_consumed, filp->f\_flags & O\_NONBLOCK);

}

static int binder\_thread\_write(struct binder\_proc \*proc,

struct binder\_thread \*thread,

binder\_uintptr\_t binder\_buffer, size\_t size,

binder\_size\_t \*consumed) {

/\*print info: proc'name, proc id, thread id, cmd'name\*/

**printk**("%s (%d, %d), %s : %s\n", proc-tsk->comm, proc->pid, thread->pid, \_\_FUNCTION\_\_, cmd\_name(cmd));//cmd\_name来自客户端APP binder.c

switch (cmd) {}

}

static int binder\_thread\_read(struct binder\_proc \*proc,

struct binder\_thread \*thread,

binder\_uintptr\_t binder\_buffer, size\_t size,

binder\_size\_t \*consumed, int non\_block) {

/\*print info: proc'name, proc id, thread id, cmd'name\*/

**printk**("%s (%d, %d), %s : %s\n", proc-tsk->comm, proc->pid, thread->pid, \_\_FUNCTION\_\_, cmd\_name(BR\_NOOP));

if (put\_user(BR\_NOOP, (uint32\_t \_\_user \*)ptr))//在所有的put\_user前面打印

**printk**("%s (%d, %d), %s , print data :\n", proc-tsk->comm, proc->pid, thread->pid, \_\_FUNCTION\_\_);

hexdump(t->buffer->data, tr.data\_size);

}

static void binder\_transaction(struct binder\_proc \*proc,

struct binder\_thread \*thread,

struct binder\_transaction\_data \*tr, int reply,

binder\_size\_t extra\_buffers\_size) {

**binder\_debug**(BINDER\_DEBUG\_TRANSACTION,

"%d:%d BC\_REPLY %d -> %d:%d, data %016llx-%016llx size %lld-%lld-%lld\n",

proc->pid, thread->pid, t->debug\_id,

target\_proc->pid, target\_thread->pid,

(u64)tr->data.ptr.buffer,

(u64)tr->data.ptr.offsets,

(u64)tr->data\_size, (u64)tr->offsets\_size,

(u64)extra\_buffers\_size);

else

**binder\_debug**(BINDER\_DEBUG\_TRANSACTION,

"%d:%d BC\_TRANSACTION %d -> %d - node %d, data %016llx-%016llx size %lld-%lld-%lld\n",

proc->pid, thread->pid, t->debug\_id,

target\_proc->pid, target\_node->debug\_id,

(u64)tr->data.ptr.buffer,

(u64)tr->data.ptr.offsets,

(u64)tr->data\_size, (u64)tr->offsets\_size,

(u64)extra\_buffers\_size);

。。。

if (copy\_from\_user(t->buffer->data, (const void \_\_user \*)(uintptr\_t)

tr->data.ptr.buffer, tr->data\_size)) {

binder\_user\_error("%d:%d got transaction with invalid data ptr\n",

proc->pid, thread->pid);

return\_error = BR\_FAILED\_REPLY;

return\_error\_param = -EFAULT;

return\_error\_line = \_\_LINE\_\_;

goto err\_copy\_data\_failed;

}

/\* print data\*/

**printk**("%s (%d, %d), %s , print data :\n", proc-tsk->comm, proc->pid, thread->pid, \_\_FUNCTION\_\_);

hexdump(t->buffer->data, tr->data\_size);//hexdump来自客户端APP binder.c

if (copy\_from\_user(offp, (const void \_\_user \*)(uintptr\_t)

tr->data.ptr.offsets, tr->offsets\_size)) {

binder\_user\_error("%d:%d got transaction with invalid offsets ptr\n",

proc->pid, thread->pid);

return\_error = BR\_FAILED\_REPLY;

return\_error\_param = -EFAULT;

return\_error\_line = \_\_LINE\_\_;

goto err\_copy\_data\_failed;

}

}

### 1.2.3 服务注册过程概述\_分析

./service\_manager &

[ 32.566620] service\_manager (1362, 1362), binder\_thread\_write : BC\_ENTER\_LOOPER

[ 32.566712] service\_manager (1362, 1362), binder\_thread\_read : BR\_NOOP

//往下就休眠了，等待其他服务向他注册消息

./test\_server &

[ 38.320197] test\_server (1363, 1363), binder\_thread\_write : BC\_TRANSACTION

[ 38.320284] binder: 1363:1363 BC\_TRANSACTION 2 -> 1362 - node 1, data beca6a5c-beca6a4c size 96-4

[ 38.320383] test\_server (1363, 1363), binder\_transaction , print data :

[ 38.320454] 0000: 00 . 00 . 00 . 00 . 1a . 00 . 00 . 00 . 61 a 00 . 6e n 00 . 64 d 00 . 72 r 00 . – bio\_put\_string16\_x(&msg, SVC\_MGR\_NAME);

[ 38.329064] 0016: 6f o 00 . 69 i 00 . 64 d 00 . 2e . 00 . 6f o 00 . 73 s 00 . 2e . 00 . 49 I 00 .

[ 38.337917] 0032: 53 S 00 . 65 e 00 . 72 r 00 . 76 v 00 . 69 i 00 . 63 c 00 . 65 e 00 . 4d M 00 .

[ 38.346771] 0048: 61 a 00 . 6e n 00 . 61 a 00 . 67 g 00 . 65 e 00 . 72 r 00 . 00 . 00 . 00 . 00 .

[ 38.355646] 0064: 05 . 00 . 00 . 00 . 68 h 00 . 65 e 00 . 6c l 00 . 6c l 00 . 6f o 00 . 00 . 00 . – bio\_put\_string16\_x(&msg, name);

[ 38.364475] 0080: 85 . 2a \* 62 b 73 s 7f . 01 . 00 . 00 . e0 . 88 . 00 . 00 . 00 . 00 . 00 . 00 . – bio\_put\_obj(&msg, ptr); obj, type, binder, cookie

[ 38.373350] test\_server (1363, 1363), binder\_thread\_read : BR\_NOOP

[ 38.379521] service\_manager (1362, 1362), binder\_thread\_read : BR\_TRANSACTION

[ 38.386633] service\_manager (1362, 1362), binder\_thread\_read , print data :

[ 38.393567] 0000: 00 . 00 . 00 . 00 . 1a . 00 . 00 . 00 . 61 a 00 . 6e n 00 . 64 d 00 . 72 r 00 .

[ 38.402410] 0016: 6f o 00 . 69 i 00 . 64 d 00 . 2e . 00 . 6f o 00 . 73 s 00 . 2e . 00 . 49 I 00 .

[ 38.411263] 0032: 53 S 00 . 65 e 00 . 72 r 00 . 76 v 00 . 69 i 00 . 63 c 00 . 65 e 00 . 4d M 00 .

[ 38.420127] 0048: 61 a 00 . 6e n 00 . 61 a 00 . 67 g 00 . 65 e 00 . 72 r 00 . 00 . 00 . 00 . 00 .

[ 38.428971] 0064: 05 . 00 . 00 . 00 . 68 h 00 . 65 e 00 . 6c l 00 . 6c l 00 . 6f o 00 . 00 . 00 .

[ 38.437824] 0080: 85 . 2a \* 68 h 73 s 7f . 01 . 00 . 00 . 01 . 00 . 00 . 00 . 00 . 00 . 00 . 00 .

[ 38.447188] test\_server (1363, 1363), binder\_thread\_read : BR\_INCREFS

[ 38.453114] test\_server (1363, 1363), binder\_thread\_read : BR\_ACQUIRE

[ 38.459748] test\_server (1363, 1363), binder\_thread\_read : BR\_TRANSACTION\_COMPLETE

[ 38.467270] service\_manager (1362, 1362), binder\_thread\_write : BC\_ACQUIRE

[ 38.474004] test\_server (1363, 1363), binder\_thread\_read : BR\_NOOP

[ 38.480122] service\_manager (1362, 1362), binder\_thread\_write : BC\_REQUEST\_DEATH\_NOTIFICATION

[ 38.488626] service\_manager (1362, 1362), binder\_thread\_write : BC\_FREE\_BUFFER

[ 38.495828] service\_manager (1362, 1362), binder\_thread\_write : BC\_REPLY

[ 38.502538] binder: 1362:1362 BC\_REPLY 5 -> 1363:1363, data bed9fa4c-bed9fa3c size 4-0

[ 38.510404] service\_manager (1362, 1362), binder\_transaction , print data :

[ 38.517345] 0000: 00 . 00 . 00 . 00 .

[ 38.520994] test\_server (1363, 1363), binder\_thread\_read : BR\_REPLY

[ 38.527250] test\_server (1363, 1363), binder\_thread\_read , print data :

[ 38.540003] 0000: 00 . 00 . 00 . 00 .

[ 38.543642] service\_manager (1362, 1362), binder\_thread\_read : BR\_NOOP

[ 38.550253] test\_server (1363, 1363), binder\_thread\_write : BC\_FREE\_BUFFER

[ 38.557063] service\_manager (1362, 1362), binder\_thread\_read : BR\_TRANSACTION\_COMPLETE

[ 38.566481] service\_manager (1362, 1362), binder\_thread\_read : BR\_NOOP

[ 38.571459] test\_server (1363, 1363), binder\_thread\_write : BC\_ENTER\_LOOPER

[ 38.578368] test\_server (1363, 1363), binder\_thread\_read : BR\_NOOP

svcmgr: add\_service('hello'), handle = 1

ret = svcmgr\_publish(bs, svcmgr, "hello", hello\_service\_handler);

int svcmgr\_publish(struct binder\_state \*bs, uint32\_t target, const char \*name, void \*ptr)

{

int status;

unsigned iodata[512/4];

struct binder\_io msg, reply;

**//1. 构造数据**

**//a. 构造binder\_io**

//下面函数对应到用户空间binder.c里面，

bio\_init(&msg, iodata, sizeof(iodata), 4);//前十六个字节空出来offs

bio\_put\_uint32(&msg, 0); //32对应4字节，放入了00 00 00 00data->

bio\_put\_string16\_x(&msg, SVC\_MGR\_NAME);//"android.os.IServiceManager"，放入长度len=0x1A(4字节)，字符串用两个字节存放一个字符6100 6e00 6400 ...

bio\_put\_string16\_x(&msg, name);//"hello"，05000000 6800 6500…-<data

bio\_put\_obj(&msg, ptr);//前十六个字节，有四个位置可以一一指向构造出来的 flat\_binder\_object

{

struct flat\_binder\_object \*obj;

obj->flags = 0x7f | FLAT\_BINDER\_FLAG\_ACCEPTS\_FDS;//实体或者是引用，只有test\_server服务提供者能传实体，client、service\_manager只能传引用

obj->type = BINDER\_TYPE\_BINDER;

obj->binder = (uintptr\_t)ptr;//传入的handler: flag实体对应实体(处理函数的地址)，应用对应引用

obj->cookie = 0;

}

if (binder\_call(bs, &msg, &reply, target, SVC\_MGR\_ADD\_SERVICE))

int binder\_call(struct binder\_state \*bs,

struct binder\_io \*msg,

struct binder\_io \*reply,

uint32\_t target, uint32\_t code)

{

int res;

struct binder\_write\_read bwr;

struct {

uint32\_t cmd;

struct binder\_transaction\_data txn;

} \_\_attribute\_\_((packed)) writebuf;

unsigned readbuf[32];

if (msg->flags & BIO\_F\_OVERFLOW) {

fprintf(stderr,"binder: txn buffer overflow\n");

goto fail;

}

**//b. 转为 binder\_transaction\_data**

writebuf.cmd = BC\_TRANSACTION;//四大类型之一

writebuf.txn.target.handle = target;//0-servicemanager

writebuf.txn.code = code;//SVC\_MGR\_ADD\_SERVICE-注册服务

writebuf.txn.flags = 0;

writebuf.txn.data\_size = msg->data - msg->data0;///放入msg数据

writebuf.txn.offsets\_size = ((char\*) msg->offs) - ((char\*) msg->offs0);//data-><-data 大小

writebuf.txn.data.ptr.buffer = (uintptr\_t)msg->data0;//data

writebuf.txn.data.ptr.offsets = (uintptr\_t)msg->offs0;//offs

**//c. 放入 binder\_write\_read**

bwr.write\_size = sizeof(writebuf);

bwr.write\_consumed = 0;

bwr.write\_buffer = (uintptr\_t) &writebuf;

hexdump(msg->data0, msg->data - msg->data0);

for (;;) {

bwr.read\_size = sizeof(readbuf);

bwr.read\_consumed = 0;

bwr.read\_buffer = (uintptr\_t) readbuf;

**//2. 发送数据ioctl**

res = ioctl(bs->fd, BINDER\_WRITE\_READ, &bwr);

}

return -1;

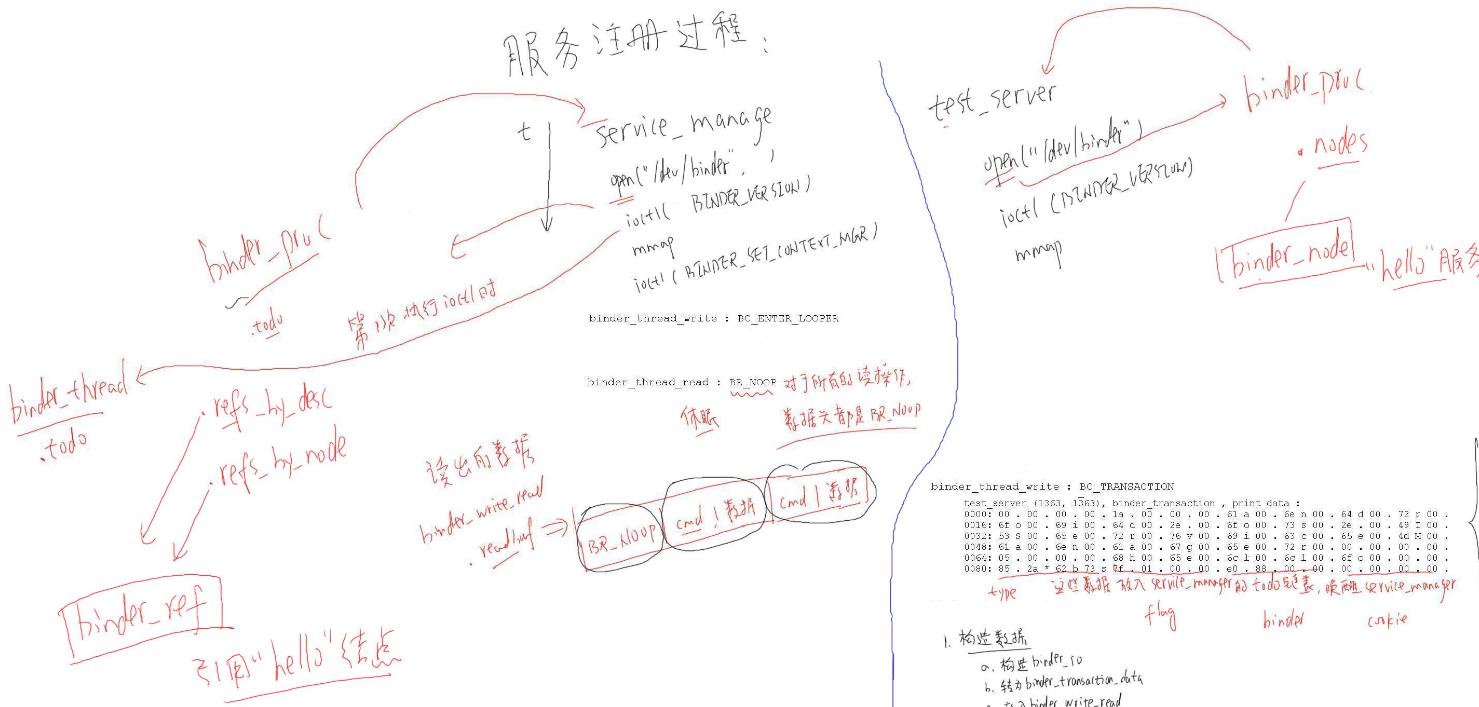
status = bio\_get\_uint32(&reply);

binder\_done(bs, &msg, &reply);

return status;

}

3. 进入驱动，binder\_ioctl把数据访日service\_manager进程的todo链表，并唤醒它



a. 根据handle找到目的进程service\_manager

b. 把数据copy\_from\_user放到service\_manager的mmap的空间

c. 处理offset数据 flat\_binder\_object

a. 构造binder\_node给test\_server，node = binder\_new\_node(proc, fp->binder, fp->cookie);

b. 构造binder\_ref给service\_manager

c. 增加引用计数

static void binder\_transaction(struct binder\_proc \*proc,

struct binder\_thread \*thread,

struct binder\_transaction\_data \*tr, int reply)

{

copy\_from\_user();

struct flat\_binder\_object \*fp;

case BINDER\_TYPE\_BINDER:

case BINDER\_TYPE\_WEAK\_BINDER: {

node = binder\_new\_node(proc, fp->binder, fp->cookie);//构造binder\_node给test\_server

ref = binder\_get\_ref\_for\_node(target\_proc, node);//构造binder\_ref给service\_manager

if (fp->type == BINDER\_TYPE\_BINDER)

fp->type = BINDER\_TYPE\_HANDLE;//实体改成引用

}

fp->handle = ref->desc;//修改成引用号1，即第一个引用，service\_manager通过1(desc)找到第一个binder\_ref，再找到binder\_node

struct flat\_binder\_object {

\_\_u32 type;

\_\_u32 flags;

union {

binder\_uintptr\_t binder;

\_\_u32 handle;

};

binder\_uintptr\_t cookie;

};

binder\_inc\_ref(ref, fp->type == BINDER\_TYPE\_HANDLE, &thread->todo);//增加引用计数

}

struct binder\_proc {

struct hlist\_node proc\_node;

struct rb\_root threads;

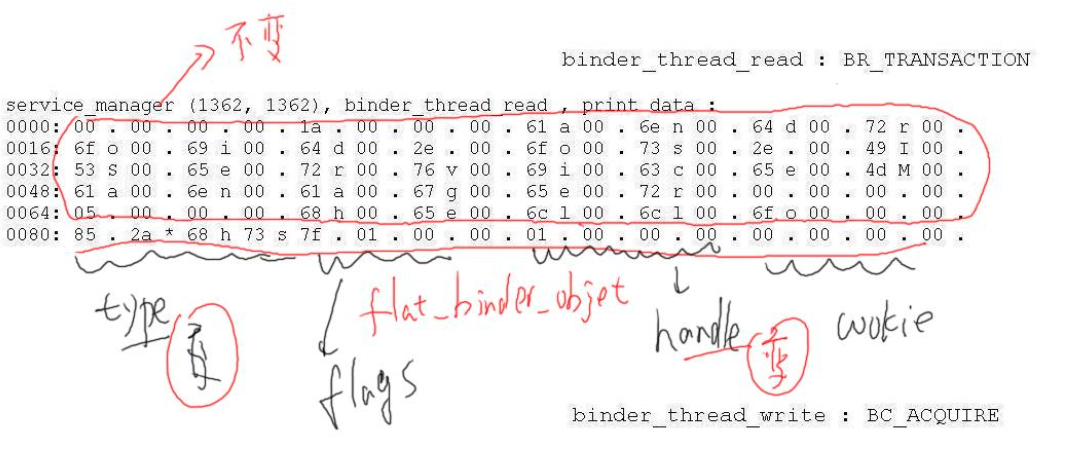
struct rb\_root nodes;

struct rb\_root refs\_by\_desc;

struct rb\_root refs\_by\_node;

。。。

};



service\_manage.c将驱动修改后的数据取出来，do\_add\_service，加入死亡通知，bio\_put\_uint32(reply, 0)，这样test\_server可以读到四个0