

# Simple DriverKit Setup

## In XCode

- Create new project
- Select macOS > DriverKit Driver (search if needed)
- Supposed to include entitlements by default
- **.iig file**; class definition for driver

```
// MyUserUSBInterfaceDriver.iig

public:
    virtual bool init () override;
    virtual kern_return_t Start (IOService *provider) override;
    virtual kern_return_t Stop (IOService *provider) override;
    virtual void free () override;

protected:
    virtual void ReadComplete (OSAction *action,
                               IOReturn status,
                               uint32_t actualByteCount,
                               uint64_t completionTimestamp)
        TYPE(IOUSBHostPipe::CompleteAsyncIO);
```

**kern\_return\_t Start & Stop;** IOKit Lifecycle methods

**IOUSBHostPipe;**

- Protocol that DriverKit callbacks MUST conform to.
- All instance variables must be allocated by the driver at **time of initialization**

1. **Declare struct to hold all instance vars;**

```
// MyUserUSBInterfaceDriver.cpp Instance Variable Definition

struct MyUserUSBInterfaceDriver_IVars
{
    IOUSBHostInterface      *interface;
    IOUSBHostPipe           *inPipe;
    OSAction                *ioCompleteCallback;
    IOBufferMemoryDescriptor *inData;
    uint16_t                 maxPacketSize;
};
```

- Include all instance vars you would've included in the kernel class b4
- **Same USB kernel types as Kext**
  - **IOUSBHostInterface** provider
  - **IOUSBHostPipe** object
    - Performs IO
  - **OSAction** object
    - “Encapsulated” Async callbacks (IO)
- **Allocate at init**

**init “routine”;**

```
// MyUserUSBInterfaceDriver.cpp init () method

bool
MyUserUSBInterfaceDriver::init ()
{
    bool result = false;

    result = super::init();
    __Require(true == result, Exit);

    ivars = IONewZero(MyUserUSBInterfaceDriver_IVars, 1);
    __Require_Action(NULL != ivars, Exit, result = false);

Exit:
    return result;
}
```

- Calls **init** on **superclass** same as **Kext**
- **Allocates struct**

### Start implementation;

```
// MyUserUSBInterfaceDriver.cpp Start () method

kern_return_t
IMPL (MyUserUSBInterfaceDriver,
      Start)
{
    kern_return_t             ret;
    IOUSBStandardEndpointDescriptors descriptors;

    ret = Start(provider, SUPERDISPATCH);
    __Require(kIOReturnSuccess == ret, Exit);

    ivars->interface = OSDynamicCast(IOUSBHostInterface, provider);
    __Require_Action(NULL != ivars->interface, Exit, ret = kIOReturnNoDevice);
    ...
}
```

- Calls into superclass and validates provider
- “Slightly different” then kernel implementation...
- **IMPL**; Required to support **user process > kernel proxy object** IPC
- **Start**; **kext** called **superstart**

### USB DriverKit API;

```
// MyUserUSBInterfaceDriver.cpp Start () continued...

ret = ivars->interface->Open(this, 0, NULL);
__Require(kIOReturnSuccess == ret, Exit);

ret = ivars->interface->CopyPipe(kMyEndpointAddress, &ivars->inPipe);
__Require(kIOReturnSuccess == ret, Exit);

ret = ivars->interface->CreateIOBuffer(kIOMemoryDirectionIn,
                                         ivars->maxPacketSize,
                                         &ivars->inData);
__Require(kIOReturnSuccess == ret, Exit);
```

## Allocate OS attribute object to encapsulate the callback;

```
// MyUserUSBInterfaceDriver.cpp Start () continued...

ret = OSAction::Create(this,
                      MyUserUSBInterfaceDriver_ReadComplete_ID,
                      IOUSBHostPipe_CompleteAsyncIO_ID,
                      0,
                      &ivars->ioCompleteCallback);

__Require(kIOReturnSuccess == ret, Exit);

ret = ivars->inPipe->AsyncIO(ivars->inData,
                                ivars->maxPacketSize,
                                ivars->ioCompleteCallback,
                                0);

__Require(kIOReturnSuccess == ret, Exit);
```

## Witchcraft and wizardry;

```
scott@scotts-mac ~ % ps -ax | grep -i myuser
2572 ??    0:00.08 /System/Library/DriverExtensions/MyUserUSBInterfaceDriver.dext/MyUserUSBInterfaceDriver com.apple.MyUserUSBInterfaceDriver 0x100002632
 501 ttys009  0:37.58 log stream --predicate sender = "MyUserUSBInterfaceDriver.dext" --style syslog
2578 ttys005  0:00.01 grep -i myuser
scott@scotts-mac ~ % sudo llDb
Password:
Sorry, try again.
Password:
Password:
(lldb) process attach --pid 2572
Process 2572 stopped
* thread #1, stop reason = signal SIGSTOP
  frame #0: 0x00000001003437ea libsystem_kernel.dylib`__sigsuspend_nocancel + 10
libsystem_kernel.dylib`__sigsuspend_nocancel:
--> 0x1003437ea <-19>: jae 0x1003437f4           ; <+20>
 0x1003437ec <-12>: movq %rax, %rdi
 0x1003437ef <-15>: jmp 0x100326f21           ; error_nocancel
 0x1003437f4 <-29>: retq
Target 0: (MyUserUSBInterfaceDriver) stopped.

Executable module set to "/System/Library/DriverExtensions/MyUserUSBInterfaceDriver.dext/MyUserUSBInterfaceDriver".
Architecture set to: x86_64h-apple-driverkit-.
(lldb) █
2019-06-04 10:25:31.397586-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) init (76) -
2019-06-04 10:25:31.397586-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) Start_Impl (189) -
2019-06-04 10:25:31.458614-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:31.458711-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:37.858863-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:41.058911-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:44.259001-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:47.427121-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete_Impl (286) - Spinning forever
█
```

- **ps -ax | grep -i myuser**
  - Shows the driver is running
  - PID is 2572
- **sudo llDb**
  - llDb will show what's happening in the driver
- **process attach —pid 2572**
  - Attach to the target process

```

Target 0: (MyUserUSBInterfaceDriver) stopped.
*Executable module set to "/System/Library/DriverExtensions/MyUserUSBInterfaceDriver.dext/MyUserUSBInterfaceDriver".
Architecture set to: x86_64h-apple-driverkit-.

(lldb) thread list
Process 2572 stopped
* thread #1: tid = 0x1e19b, 0x00000001609437ea libsystem_kernel.dylib`_sigsuspend_nocancel + 18, stop reason = signal SIGSTOP
  thread #2: tid = 0x1e19c, 0x00000001600015c5 MyUserUSBInterfaceDriver`MyUserUSBInterfaceDriver::ReadComplete_Impl(this=0x0000600003004058, action=<unavailable>, status=0, actualByteCount=4, completionTimestamp=<unavailable>) at MyUserUSBInterfaceDriver.cpp:289:9, queue = 'MyUserUSBInterfaceDriver-Default'
(lldb) thread select 2
MyUserUSBInterfaceDriver was compiled with optimization - stepping may behave oddly; variables may not be available.

* thread #2, queue = 'MyUserUSBInterfaceDriver-Default'
  frame #0: 0x00000001600015c5 MyUserUSBInterfaceDriver`MyUserUSBInterfaceDriver::ReadComplete_Impl(this=0x0000600003004058, action=<unavailable>, status=0, actualByteCount=4, completionTimestamp=<unavailable>) at MyUserUSBInterfaceDriver.cpp:289:9 [opt]
  286     debug("Spinning forever\n");
  287
  288     loop = true;
-> 289     while (true == loop) { }
  290
  291     debug("Goodbye\n");
  292     *(volatile uint32_t *)0 = 0xdeadbeef;
(lldb) 

```

2019-06-04 10:25:31.397586-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) init (76) -
2019-06-04 10:25:31.397654-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) Start\_Impl (189) -
2019-06-04 10:25:31.458614-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:34.658711-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:37.858863-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:41.058911-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:44.259001-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:47.427121-0700 localhost kernel.development[0]: (MyUserUSBInterfaceDriver.dext) ReadComplete\_Impl (286) - Spinning forever
]

And here, we've definitely got

- **thread list**

- Find the thread running the **readComplete** method
- We can see that it is thread #2

- **thread select 2**

- Select thread #2
- Shows an infinite loop is occurring
- Shows a de-referenced null pointer that would crash the driver
- Shows the driver crashed but restarted w/out effecting the rest of the system

- **expression loop = false**

- Modify loop variable
  - Only able to do this in user space not kext

- **detach**

- detaches lldb from the process

On unplug you can see that your **stop** and **free methods** run as normal

```

Process 2572 stopped
* thread #1: tid = 0x1e19b, 0x00000001003437ea libsystem_kernel.dylib`__sigsuspend_nocancel + 19, stop reason = signal SIGSTOP
  thread #2: tid = 0x1e19c, 0x00000001000015c5 MyUserUSBInterfaceDriver`MyUserUSBInterfaceDriver::ReadComplete_Impl(this=0x000000003004058, action=<unavailable>, status=0, actualByteCounts4, completionTimestamp=<unavailable>) at MyUserUSBInterfaceDriver.cpp:289:9, queue = 'MyUserUSBInterfaceDriver-Default'
[11db] thread select 2
MyUserUSBInterfaceDriver was compiled with optimization - stepping may behave oddly; variables may not be available.
* thread #2, queue = 'MyUserUSBInterfaceDriver-Default'
  frame #0: 0x00000001000015c5 MyUserUSBInterfaceDriver`MyUserUSBInterfaceDriver::ReadComplete_Impl(this=0x000000003004058, action=<unavailable>, status=0, actualByteCount
#4, completionTimestamp=<unavailable>) at MyUserUSBInterfaceDriver.cpp:289:9 [opt]
  286     debug("Spinning forever\n");
  287
  288     loop = true;
-> 289     while (true == loop) {
  290
  291     debug("Goodbye\n");
  292     *(volatile uint32_t *)0 = 0xedeadbeef;
[11db] expression loop = false
(volatile bool) $0 = false
[11db] detach
Process 2572 detached
[11db] █

```

2019-06-04 10:25:31.397580-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] init (76) -
2019-06-04 10:25:31.397655-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] Start\_Impl (180) -
2019-06-04 10:25:31.458614-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:34.658711-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:37.858863-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:41.058911-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:44.259061-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:47.427221-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (286) - Spinning forever
2019-06-04 10:25:48.053925-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (291) - Goodbye
2019-06-04 10:25:48.098524-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] init (76) -
2019-06-04 10:25:48.098607-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] Start\_Impl (180) -
2019-06-04 10:25:48.116713-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:25:48.324952-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:26:52.817987-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (278) - 4 bytes completed with 0x00000000
2019-06-04 10:26:54.281519-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] ReadComplete\_Impl (278) - 0 bytes completed with 0xe00002eb
2019-06-04 10:26:54.281582-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] Assert: KIOReturnSuccess == status, , line: 281, value: 0
2019-06-04 10:26:54.282043-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] Stop\_Impl (262) -
2019-06-04 10:26:54.282175-0700 localhost kernel.development[0]: [MyUserUSBInterfaceDriver.dext] free (95) -

That's all for now!