Reversing MobileDevice

Sam Marshall

What is MobileDevice?

- Framework for communicating with iOS devices
- Handles all types of iOS device based interactions

Why haven't I heard of this before?

This framework is private.

What does that mean to me, as a developer?

- Cannot be used in MAS (Mac App Store) apps
- Undocumented!
- Likely to change without warning and ruin your app

This doesn't sound very good…

Good News,
Everyone!

SDMMobileDevice

What is this?

By completely reverse engineering Apple's MobileDevice framework, SDMMobileDevice replicates the core functionality while removing some of the complications of use.

Although being completely new code, it stays true to the original design.

How is this better?

- MobileDevice.h
  - Less documented
  - C header file
- MobileDeviceAccess
  - Cocoa wrapper for MobileDevice.h
  - Follows design of the MobileDevice framework

```
typedef struct LockdownConnection {
     uint64_t connection;      // 0
     SSL *ssl;                 // 8
     uint64_t *pointer;        // 16
     uint64_t length;          // 24
} __attribute__ ((packed)) LockdownConnection;

struct AMDevice {
     unsigned char header[16];           // 0 AMDeviceClass CF Header
     int32_t device_id;                  // 16
     int32_t location_id;                // 20
     uint16_t product_id;                // 24
     int16_t padding0;                   // 26
     int32_t unknown1;                   // 28
     CFStringRef unique_device_id;       // 32
     int32_t unknown2;                   // 36
     int32_t connection_type;            // 40 (1 for USB, 2 for WiFi)
     unsigned char unknown3[4];          // 44
     LockdownConnection *lockdown_conn;  // 48
     unsigned char unknown4[4];          // 52
     CFStringRef session;                // 56
     int32_t padding1;                   // 60
     pthread_mutex_t mutex_lock;         // 64
     unsigned char unknown5[60];         // 68
     CFStringRef service_name;           // 128 bonjour service name
     unsigned int unknown6;              // 132
     int32_t interface_index;            // 136
     int8_t device_active;               // 140
     unsigned char unknown7[3];          // 141
     int32_t unknown8;                   // 144
     unsigned char unknown9[4];          // 148
     CFDataRef network_address;          // 152 stores sockaddr_storage
     unsigned char unknown10[4];         // 156
     CFDataRef unknown11;                // 160
     unsigned char unknown12[4];         // 164
} __attribute__ ((packed)) AMDevice;
```

Features

Services

- Content syncing (media, contacts, mail, etc.)
- Backups
- File transfers (AFC)
- App installation
- System services (debugging, device settings)

Usability

- Open source
- C, CoreFoundation
- Cocoa framework coming soon

Questions

https://github.com/samdmarshall/SDMMobileDevice

http://samdmarshall.com