Mobile Game Security

Is IL2CPP So Secure?

About Me

- nevermoe
  - Interest：Swimming, Skiing, (Pretend to be) Otaku
  - Bio：

Contents

- Attack & Defense of Mobile Games
- Introduction to IL2CPP
- IDA Plugin
- Conclusions

Attack & Defense of Mobile Games (Cheating)

- Network Traffic Manipulation
  - Replay
  - Request or Response Tampering
- Local Modification
  - Memory Cheat
  - Speed Hack
  - File Tampering
  - Binary Patch
  - hook

Network Traffic Manipulation

Local Modification

Attack & Defense of Mobile Games (Anti-cheating)

- Network Traffic Manipulation
  - Replay －> Add Token
  - Request or Response Tampering －> Encryption / SSL Pinning
- Local Tampering
  - Memory Cheat －> Memory Encrytion
  - Speed Hack －> Local Detection / Sever Timestamp
  - File Tampering －> Local File Encryption / Hash Check
  - Binary Patch －> Packing / Obfuscation / Hash Check
  - Hook －> Anti debug / Hook Framework Detection / Injection Detection

Attack & Defense of Mobile Games (Game Engines)

- Unity3D
  - Both 2D and 3D Supported
  - Cross Platform
  - Source Code is Partially Open
- Cocos2d-x
  - Dedicated to 2D
  - Cross Platform
  - Open Source
- FlashAIR/Unreal/Corona etc.
- Customized Engine

Market Share is overwhelming

Attack & Defense of Mobile Games (Unity3D Anti-cheating Overview)

- Unity3D Anti-cheating Toolkit
  - Memory Encryption
  - Speed-hack Detection
  - Etc.

=>This kind of protection fails once the binary is reversed

Attack & Defense of Mobile Games (Purpose)

* This kind of protection fails once the binary is reversed

- iOS -> IL2CPP
  - Easy to get
  - No Packing or Obfuscation

=> To reverse assembly code?

- Android -> Mono
  - Packing
  - Obfuscating

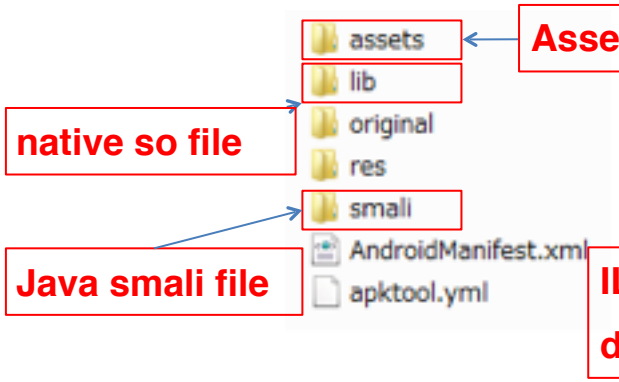
=> Or to reverse obfuscated code?

=> Read the Assembly Code!

Introdcution to IL2CPP

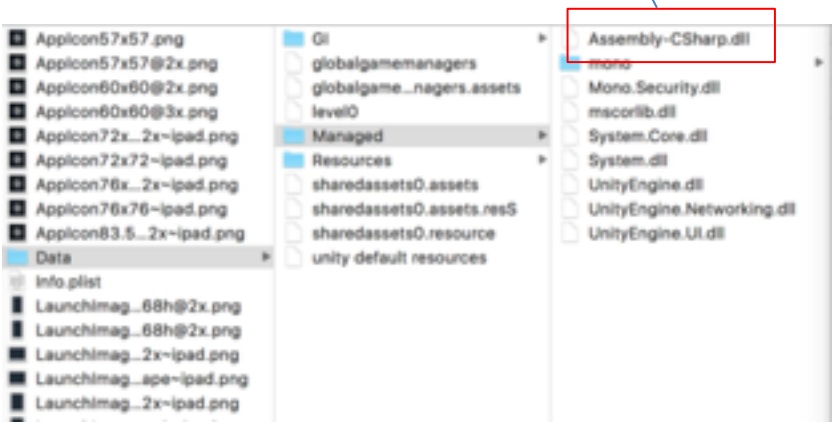
（Without IL2CPP / Scripting Backend: Mono ）

- Android




```
namespace MiniJSON
{
    public static class Json
    {
        public static object Deserialize(string json)
        {
            if (json == null)
            {
                return null;
            }
            return Json.Parser.Parse(json);
        }

        public static string Serialize(object obj)
        {
            return Json.Serializer.Serialize(obj);
        }

        private sealed class Parser : IDisposable
        {
            private const string WORD_BREAK = "{}[],:\"";

            private StringReader json;

            private char NextChar
            {
                get
                {
                    return Convert.ToChar(this.json.Read());
                }
            }

            private Json.Parser.TOKEN NextToken
            {
                get
                {
                    string nextWord;
                    Dictionary<string, int> strs;
                    int num;
                    this.EatWhitespace();
                    if (this.json.Peek() == -1)
```

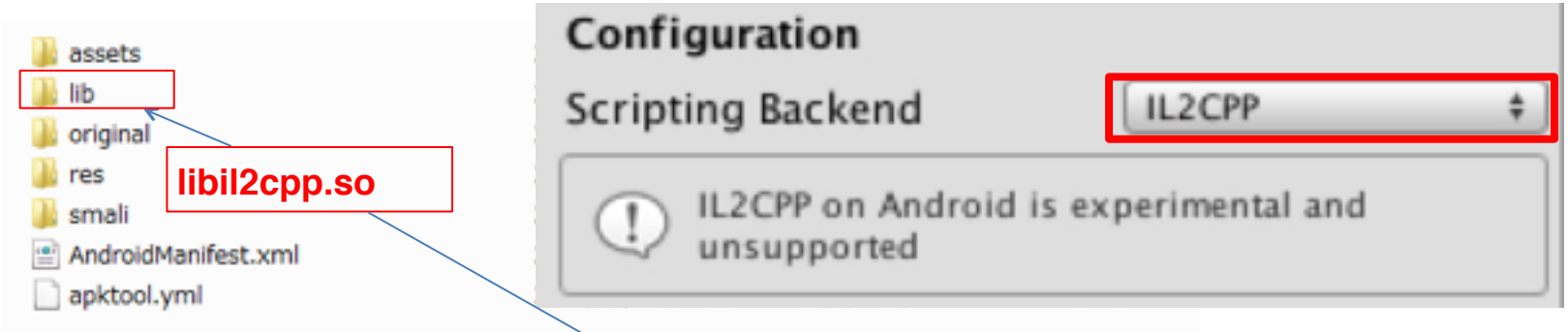
- iOS



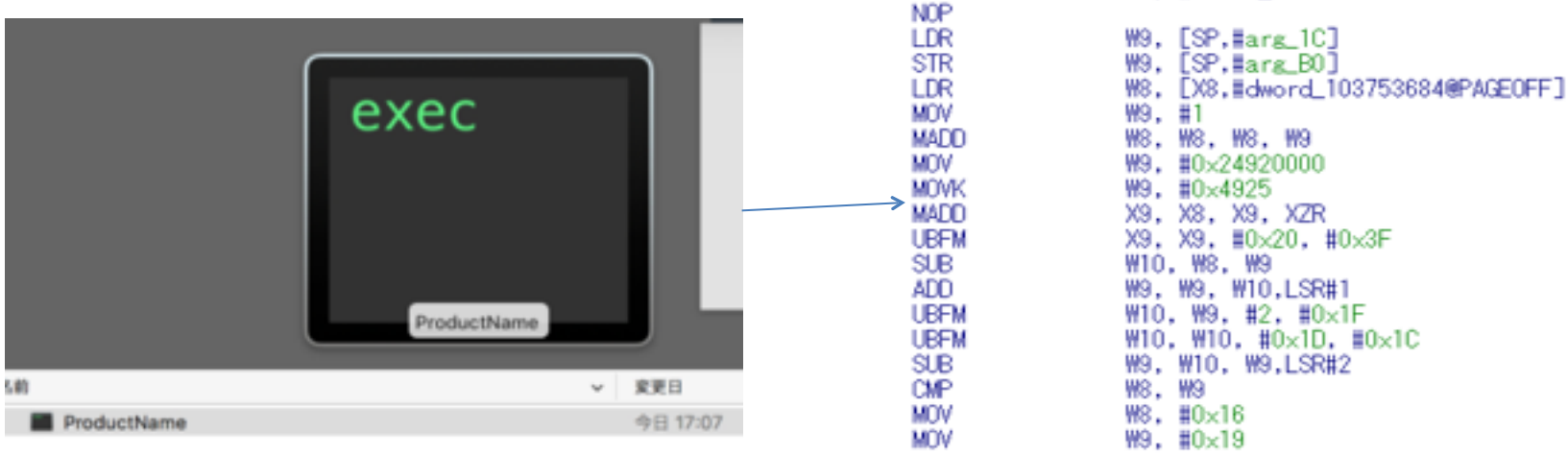
Introdcution to IL2CPP

（With IL2CPP / Scripting Backend: IL2CPP）

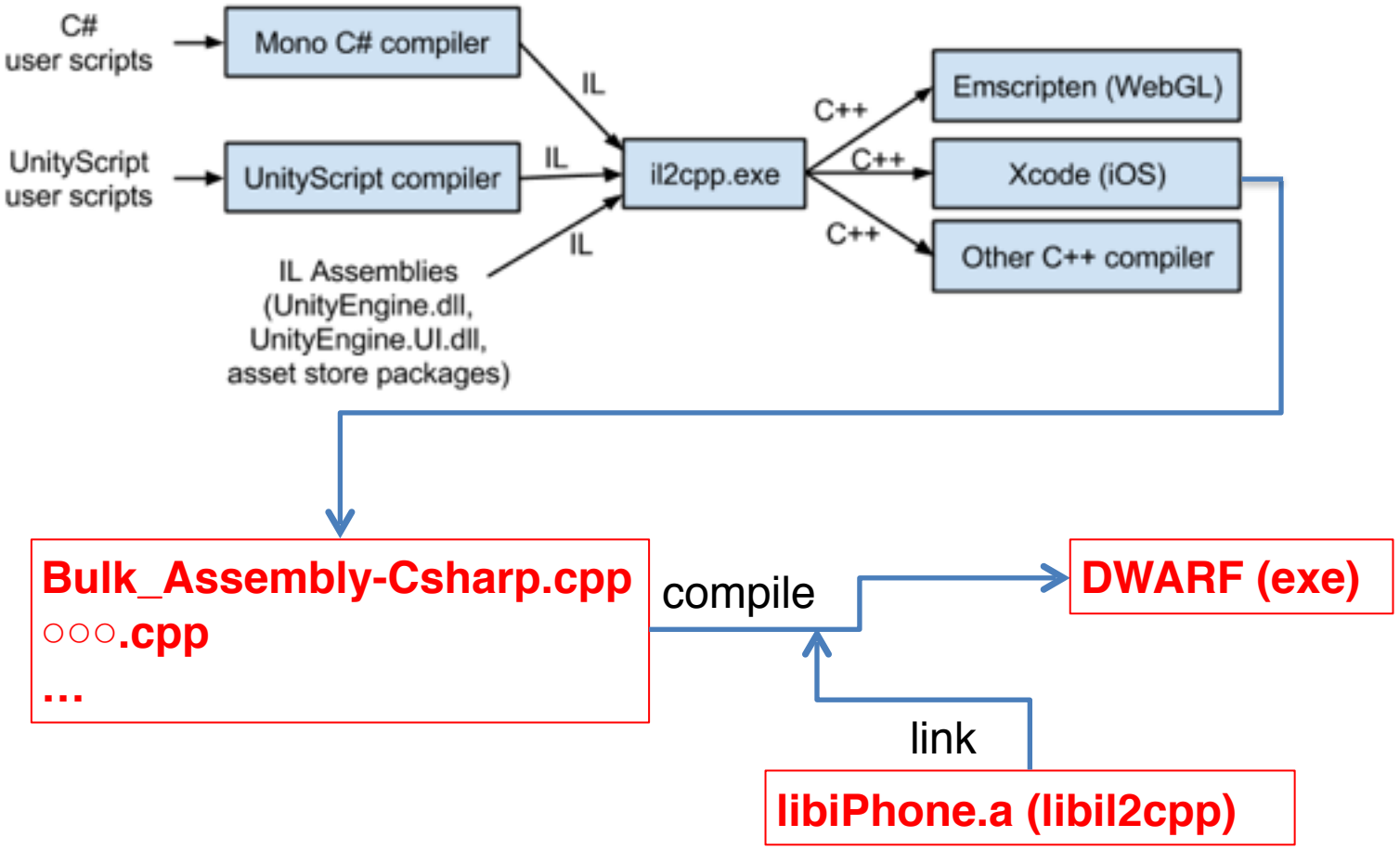
- Android



- iOS



Introdcution to IL2CPP (Overview)



Introdcution to IL2CPP (Functions of libil2cpp)

- libil2cpp (libiPhone.a etc.)
  - Support VM
  - Garbage Collection
  - Metadata Loader

Introdcution to IL2CPP (Metadata)

void EnemyAttack(…)

```
IL_0045:
    {
        PlayerHealth_t1138339563 * L_7 = __this->get_playerHealth_6();
        NullCheck(L_7);
        int32_t L_8 = L_7->get_currentHealth_3();
        if ((((int32_t)L_8) > ((int32_t)0)))
        {
            goto IL_0066;
        }
    }
    {
        Animator_t2776330603 * L_9 = __this->get_anim_4();
        NullCheck(L_9);
        Animator_SetTrigger_m514363822(L_9, _stringLiteral4088827653, /*hidden argument*/NULL);
    }
```

```
tDistance.m_EffectColor.
m_EffectDistance.m_UseGr
aphicAlpha.effectColor.e
ffectDistance.useGraphic
Alpha.Assembly-CSharp.As
sembly-CSharp.dll.EnemyA
ttack.OnTriggerEnter.OnT
riggerExit.Attack.timeBe
tweenAttacks.attackDamag
e.anim.playerHealth.play
erInRange.EnemyHealth.am
ount.hitPoint.TakeDamage
.Death.StartSinking.star
```

```
ordering.Internal error.
 Trying to destroy objec
t that is already releas
ed to pool.Mesh can not
have more than 65000 ver
ticesPlayerPlayerDeadwhe
reisthelog?DeadSpawnGame
OverScore: DieShootableF
ire1_name This is not po
ssible to be called for
standalone input. Please
```

Data/Managed/Metadata/global-metadata.dat

Introdcution to IL2CPP (Analysis Approach)

- Analysis Approach
  - By analyzing libiPhone.a
    - This File is guaranteed to exist
    - With Symbol
  - By analyzing source code of libil2cpp
    - Source code is attached when building a Windows Store App

Introdcution to IL2CPP (Loading Metadata)

- Read Global-metadata.dat and cast

```
//MetadataCache.cpp
void MetadataCache::Initialize()
{
    s_GlobalMetadata = vm::MetadataLoader::LoadMetadataFile ("global-metadata.dat");
    s_GlobalMetadataHeader = (const Il2CppGlobalMetadataHeader*)s_GlobalMetadata;
    assert (s_GlobalMetadataHeader->sanity == 0xFAB11BAF);
    assert (s_GlobalMetadataHeader->version == 21);
    ...
}
```

Introdcution to IL2CPP (Loading StringLiteral)

```
//MetadataCache.cpp
void MetadataCache::InitializeMethodMetadata (uint32_t index)
{
    ......
    for (uint32_t i = 0; i < count; i++)
    {
        ......
        switch (usage)
        {
         ......
        case kIl2CppMetadataUsageStringLiteral:
            *s_Il2CppMetadataRegistration->metadataUsages[destinationIndex] = GetStringLiteralFromIndex (decodedIndex);
            break;
        default:
            ....
        }
    }
```

```
//Il2CppMetadataUsage.cpp
extern void** const g_MetadataUsages[7877] =
{
    (void**)&Contraction_t1673853792_0_0_0_var,
    (void**)&Level2Map_t3322505726_0_0_0_var,
    (void**)&String_t_0_0_0_var,
    (void**)&TypedReference_t1025199857_0_0_0_var,
    (void**)&ArgIterator_t2628088752_0_0_0_var,
    (void**)&Void_t1841601450_0_0_0_var,
    ...
    ...
    ...
    (void**)&_stringLiteral2004437333,
    (void**)&_stringLiteral3025533088,
    (void**)&_stringLiteral3687436746,
    (void**)&_stringLiteral2779811765,
    (void**)&_stringLiteral273729679,
};
```

Introdcution to IL2CPP (Loading MethodInfo)

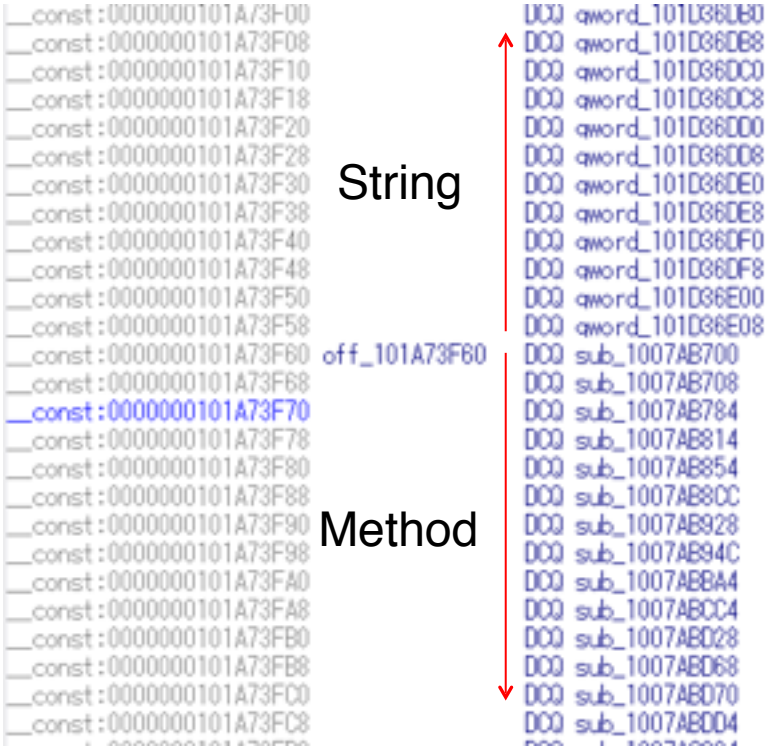
```
// Class.cpp
void SetupMethodsLocked (Il2CppClass *klass, const FastAutoLock& lock)
{
    ...
    for (MethodIndex index = start; index < end; ++index) {
        ...
        newMethod->name = MetadataCache::GetStringFromIndex (methodDefinition->nameIndex);
        ...
        newMethod->methodPointer = MetadataCache::GetMethodPointerFromIndex (methodDefinition->methodIndex);
        ...
    }
    ...
}
```

```
// MetadataCache.cpp
Il2CppMethodPointer
MetadataCache::GetMethodPointerFromIndex
(MethodIndex index)
{
    ...
    return s_Il2CppCodeRegistration-
>methodPointers[index];
}
```

```
extern const Il2CppMethodPointer g_MethodPointers[16812] =
{
    Locale_GetText_m[illegible]433032,
    Locale_GetText_m2553164138,
    SafeHandleZeroOrMinusOneIsInvalid__ctor_m3340306667,
    SafeHandleZeroOrMinusOneIsInvalid_get_IsInvalid_m2033528032,
    SafeWaitHandle__ctor_m1710231470,
    SafeWaitHandle_ReleaseHandle_m634725016,
    ...
    VignetteAndChromaticAberration__ctor_m3270745889,
    VolumeHandler_Start_m3226079559,
    VolumeHandler_SetVolume_m3613034220,
    VolumeHandler_OnDestroy_m1170460248,
    VolumeHandler__ctor_m818831955,
};
```

IDA Plugin (Mapping to IDA)

- iOS




```
//Il2CppMetadataUsage.cpp
extern void** const g_MetadataUsages[7877] =
{
    (void**)&Contraction_t1673853792_0_0_0_var,
    (void**)&Level2Map_t3322505726_0_0_0_var,
    (void**)&String_t_0_0_0_var,
    (void**)&TypedReference_t1025199857_0_0_0_var,
    (void**)&ArgIterator_t2628088752_0_0_0_var,
    (void**)&Void_t1841601450_0_0_0_var,
    ...
    ...
    ...
    (void**)&_stringLiteral2004437333,
    (void**)&_stringLiteral3025533088,
    (void**)&_stringLiteral3687436746,
    (void**)&_stringLiteral2779811765,
    (void**)&_stringLiteral273729679,
};
```

```
extern const Il2CppMethodPointer g_MethodPointers[16812] =
{
    Locale_GetText_m1954433032,
    Locale_GetText_m2553164138,
    SafeHandleZeroOrMinusOneIsInvalid__ctor_m3340306667,
    SafeHandleZeroOrMinusOneIsInvalid_get_IsInvalid_m2033528032,
    SafeWaitHandle__ctor_m1710231470,
    SafeWaitHandle_ReleaseHandle_m634725016,
    ...
    VignetteAndChromaticAberration__ctor_m3270745089,
    VolumeHandler_Start_m3226079559,
    VolumeHandler_SetVolume_m3613034220,
    VolumeHandler_OnDestroy_m1170460248,
    VolumeHandler__ctor_m818831955,
};
```

IDA Plugin (Notes)

- Unity Version later than 5.3.6
  - Metadata version 21
- iOS, Android： Auto-load
- Other platform： Manual-load
- IDA failed to make xref or function when parsing Android’s binary. (So iOS version is recommended)

Demonstrations

1. Plugin Usage
2. Cheating Demo

Conclusions

- Cheating and Anti-cheating is dynamic
- Do NOT rely only on IL2CPP to protect your binary
- Counter measure：Obfuscating strings in metadata
- Source Code: https://github.com/nevermoe/unity_metadata_loader

Thank you!