近年のGame Security診断について

nevermoe

—OWASP NIGHT MEETING

自己紹介

- ✦ nevermoe
  - 趣味：水泳、スキー、引きこもり
  - 履歴：

26年前：中国で生まれ

3年前：渡日　東京大学大学院（CG研究）

八ヶ月前：XXXX株式会社セキュリティ室に新卒入社

  - 仕事：Web、Mobile App、Game等のセキュリティ診断

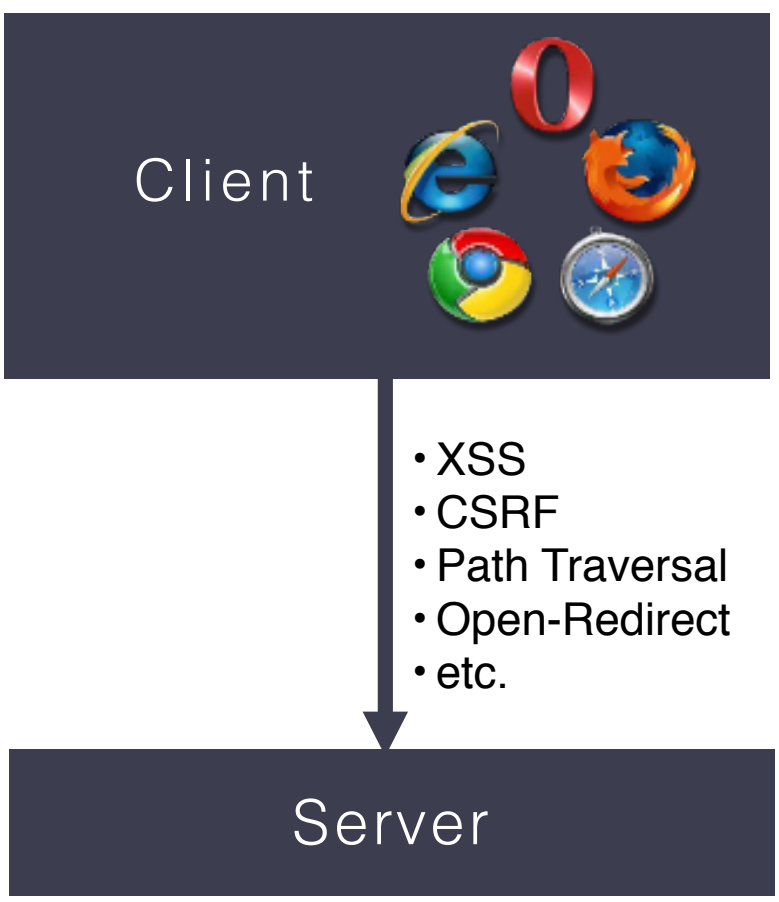
目次

- セキュリティ診断概要
- バイナリー解析
- 通信解析
- 対策＆まとめ

目次

- セキュリティ診断概要
- バイナリー解析
- 通信解析
- 対策＆まとめ

セキュリティ診断概要


Client
• XSS
• CSRF
• Path Traversal
• Open-Redirect
• etc.
Server
Client
• Analyzing the protocol
• Abusing/Cheating
• Bot (un-official client)
• etc.
Server

セキュリティ診断概要

- XSS
- CSRF
- Path Traversal
- Open-Redirect
- etc.

Server

Client

- Analyzing the protocol
- Abusing/Cheating
- Bot (un-official client)
- etc.

Server

目次

- セキュリティ診断概要
- バイナリー解析
- 通信解析
- 対策＆まとめ

ゲームエンジン

- ✦ Unity3D 
  - 2Dでも、3Dでも
  - Cross Platform
  - sourceの一部公開
- ✦ Cocos2d-x
  - 2Dゲームに特化
  - Cross Platform
  - Open Source
- ✦ FlashAIR/Unreal/Corona等
- ✦ 自作

圧倒的にシェアが高い

Unity3dゲーム現状

✦Android -> Mono

- パッキング
- 難読化

=> 難読かされた
コードをリバーシング？

✦iOS -> IL2CPP

- 取得は簡単
- パッキング、難読化一切なし

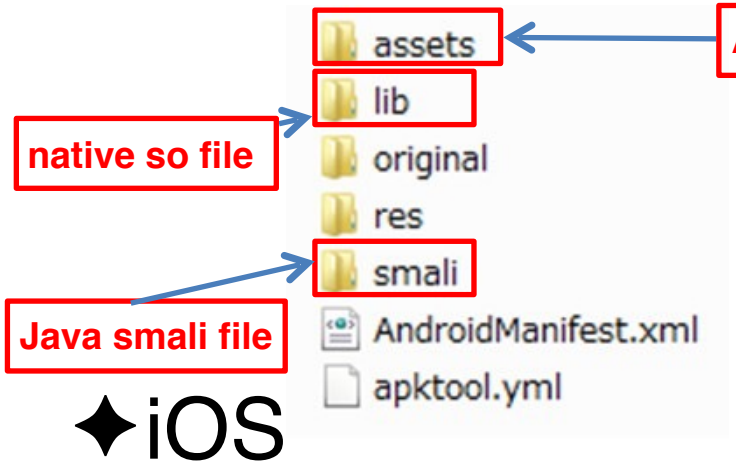
=> シンボルのない
アセンブラを
リバーシング？

★ただし、最近Androidも

IL2CPPサポートするようになった

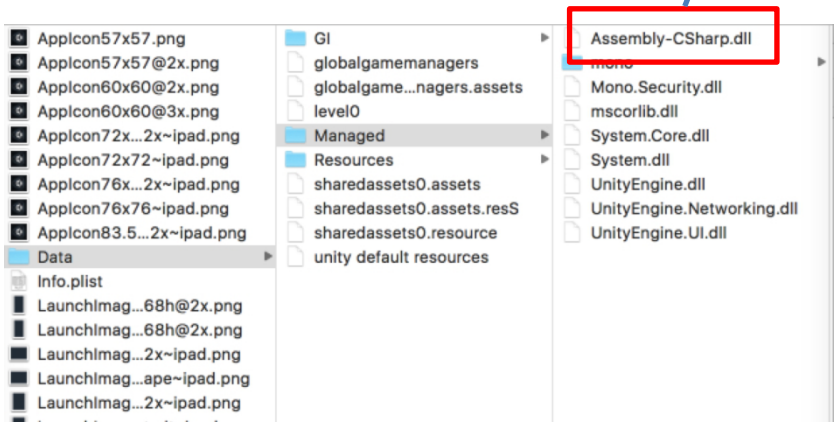
IL2CPP紹介（without IL2CPP）

✦Android



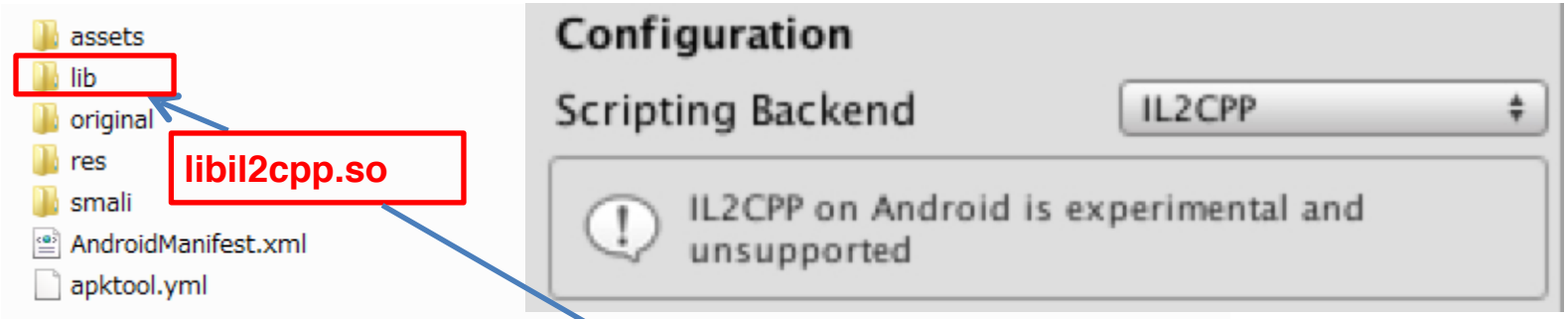

```
public void TakeDamage(int amount)
{
    this.damaged = true;
    this.currentHealth -= amount;
    this.healthSlider.set_value((float)this.currentH
    this.playerAudio.Play();
    if (this.currentHealth <= 0 && !this.isDead)
    {
        this.Death();
    }
}
```

✦iOS



IL2CPP紹介（with IL2CPP）

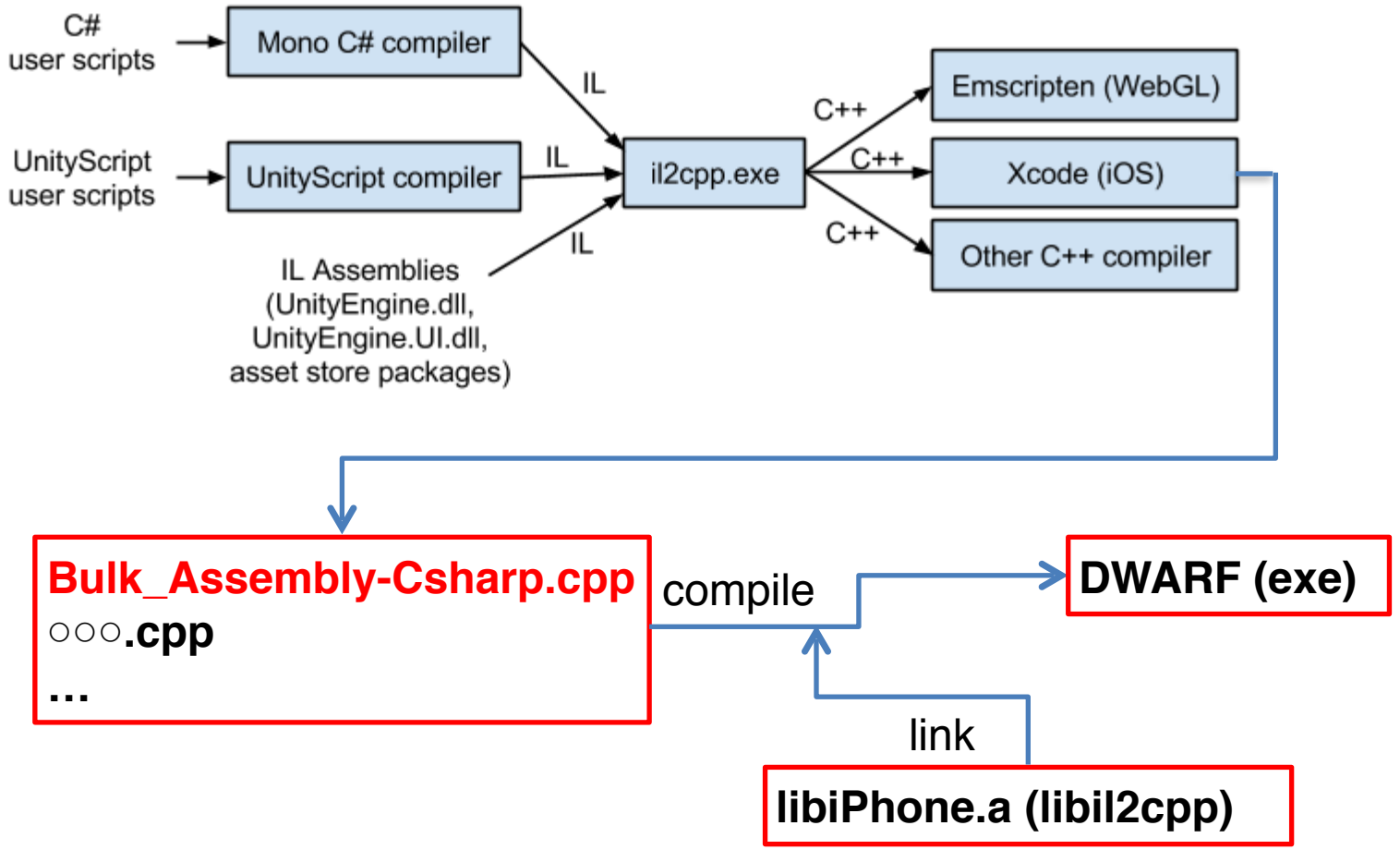
✦Android



✦iOS


```
LDR             X8, [SP,#arg_10]
STR             X8, [SP,#arg_A8]
ADRP            X8, #dword_103753684@PAGE
NOP
LDR             W9, [SP,#arg_1C]
STR             W9, [SP,#arg_B0]
LDR             W8, [X8,#dword_103753684@PAGEOFF]
MOV             W9, #1
MADD            W8, W8, W8, W9
MOV             W9, #0x24920000
MOVK            W9, #0x4925
MADD            X9, X8, X9, XZR
UBFM            X9, X9, #0x20, #0x3F
SUB             W10, W8, W9
ADD             W9, W9, W10,LSR#1
UBFM            W10, W9, #2, #0x1F
UBFM            W10, W10, #0x1D, #0x1C
SUB             W9, W10, W9,LSR#2
CMP             W8, W9
MOV             W8, #0x16
MOV             W9, #0x19
```

IL2CPP紹介


C#
user scripts
Mono C# compiler
IL
UnityScript
user scripts
UnityScript compiler
IL
IL Assemblies
(UnityEngine.dll,
UnityEngine.UI.dll,
asset store packages)
IL
il2cpp.exe
C++
C++
C++
Emscripten (WebGL)
Xcode (iOS)
Other C++ compiler
Bulk_Assembly-Csharp.cpp
○○○.cpp
…
compile
DWARF (exe)
link
libiPhone.a (libil2cpp)

Metadata

Bulk_Assembly-Csharp.cpp

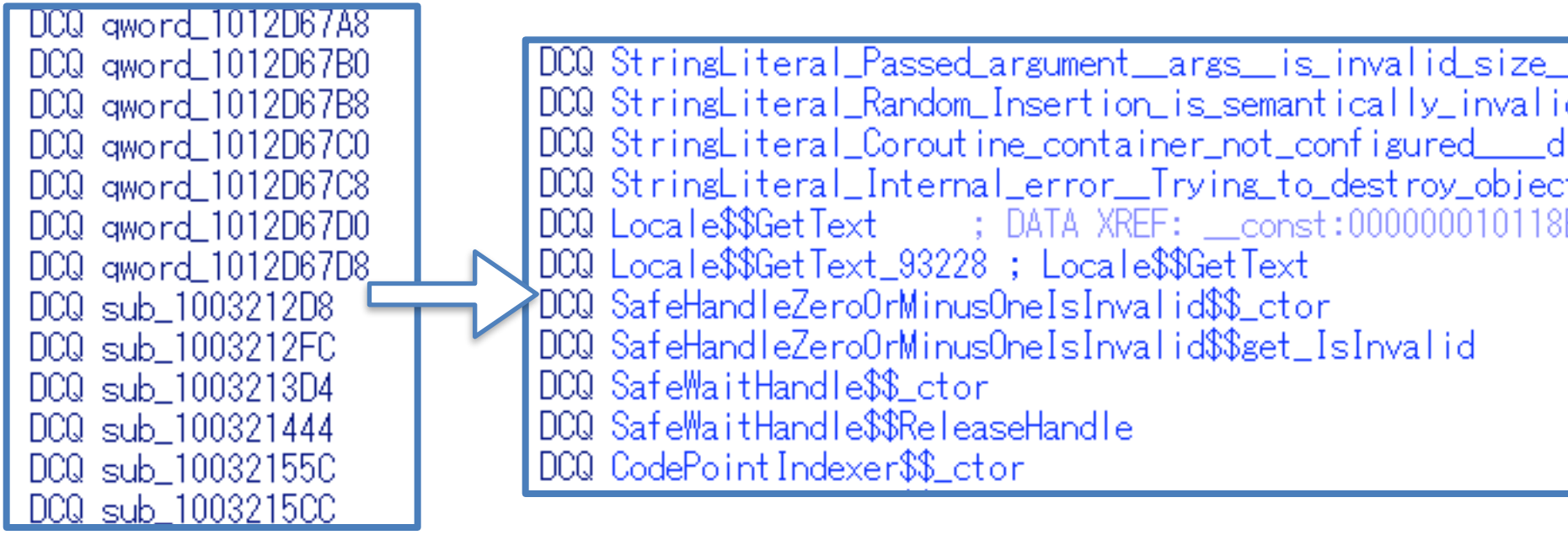
```
extern "C"  void EnemyHealth_Death_m1976714863 (EnemyHealth_t3285426352 * __this,
    const MethodInfo* method)
{
    static bool s_Il2CppMethodIntialized;
    if (!s_Il2CppMethodIntialized) { ... }
    {
        __this->set_isDead_11((bool)1);
        CapsuleCollider_t720607407 * L_0 = __this->get_capsuleCollider_10();
        NullCheck(L_0);
        Collider_set_isTrigger_m1298573031(L_0, (bool)1, /*hidden argument*/NULL);
        Animator_t69676727 * L_1 = __this->get_anim_7();
        NullCheck(L_1);
        Animator_SetTrigger_m3418492570(L_1, _stringLiteral4136222740,
            /*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
ticesPlayerPlayerDeadyhe
reisthelog?DeadSpawnGame
OverScore: DieShootableF
ire1_name This is not po
ssible to be called for
standalone input. Please
```

Data/Managed/Metadata/global-metadata.dat

シンボル復号



IDA Plugin: https://github.com/nevermoe/unity_metadata_loader
Slide: https://www.nevermoe.com/wp-content/uploads/2016/11/avtokyo_jp_re.pdf

目次

- セキュリティ診断概要
- バイナリー解析
- 通信解析
- 対策＆まとめ

通信改ざん対策

✦SSL Pinning △

- ただしく実装されない可能性がある
- 汎用性ツールによるbypass可能？

✦電文、パケットのHashチェック △

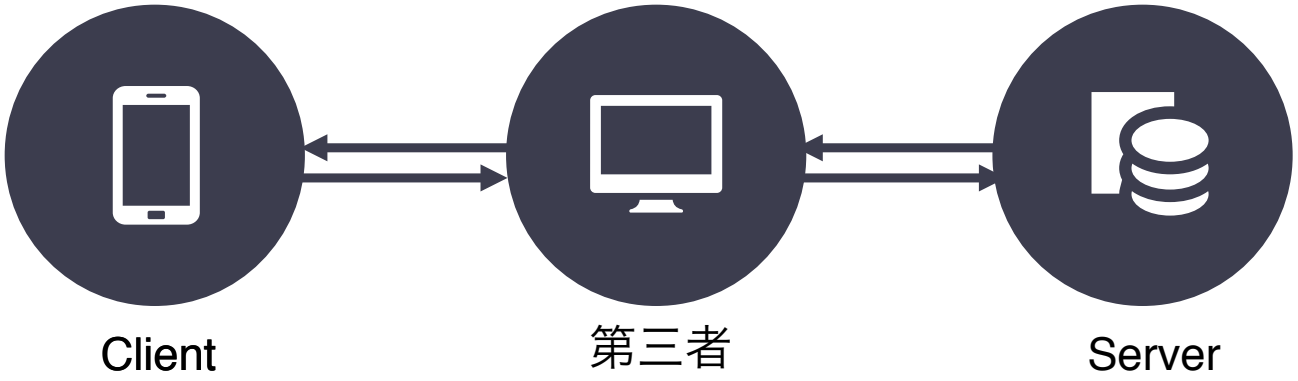
- integrityが保証されるが、通信内容が見える（protocol分析される）

✦通信暗号化 ◯

- バイナリー解析しないとリバーシング難しい
- 汎用性解析ツールがない
- 現状一番使われいる

SSL Pinning現状

- SSL Pinning Bypass



	Normal App (Android)	Normal App (iOS)	Game (Unity3d)	Game (Cocos2d-x)
SSL Pinning	○	○	✖	△
Bypass Tool	JustTrustMe	ssl-kill-switch	✖	✖

通信プロトコル

- ✦ 通常のApp
  - JSON
  - XML
  - Protobuf: https://developers.google.com/protocol-buffers/
  - Thrift: https://thrift.apache.org/
  - MessagePack: http://msgpack.org
- ✦ ゲームにとって
  - JSON
  - MessagePack
  - Protobuf

通信プロトコル比較

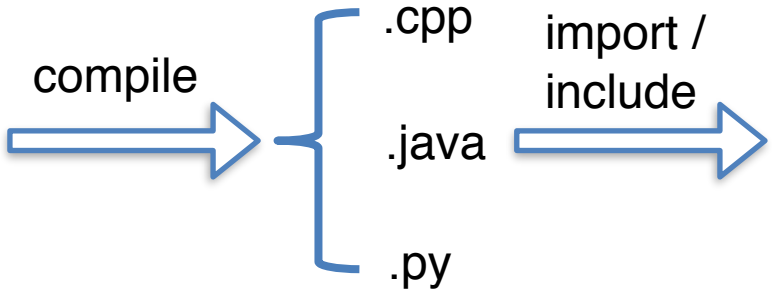
- ✦ JSON
  - 人間の目で読める
  - パースが簡単
  - overheadが大きい
- ✦ MessagePack
  - JSON-like
  - 人間の目で読めない（バイナリー）
  - パースが簡単
- ✦ Protobuf
  - Dense data
  - 人間の目で読めない（バイナリー）
  - schema (.proto)ファイルがないとdecodeが難しい
  - 処理速度が速い
  - 暗号化手法ではない！

Protobuf解析

✦ Protobuf

// .proto

```
message Person {
  required string name = 1;
  required int32 id = 2;
  optional string email = 3;
}
```



// .cpp

```
Person john;
fstream input(argv[1],
    ios::in | ios::binary);
john.ParseFromIstream(&input);
id = john.id();
name = john.name();
email = john.email();
```

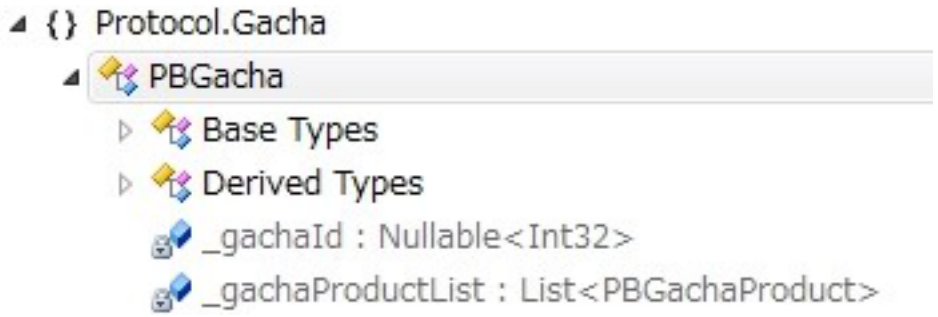
// .java

```
Person john = Person.newBuilder()
    .setId(1234)
    .setName("John Doe")
    .setEmail("jdoe@example.com")
    .build();
output = new FileOutputStream(args[0]);
john.writeTo(output);
```

Protobuf解析

✦ .protoファイルあればもちろん復号できる

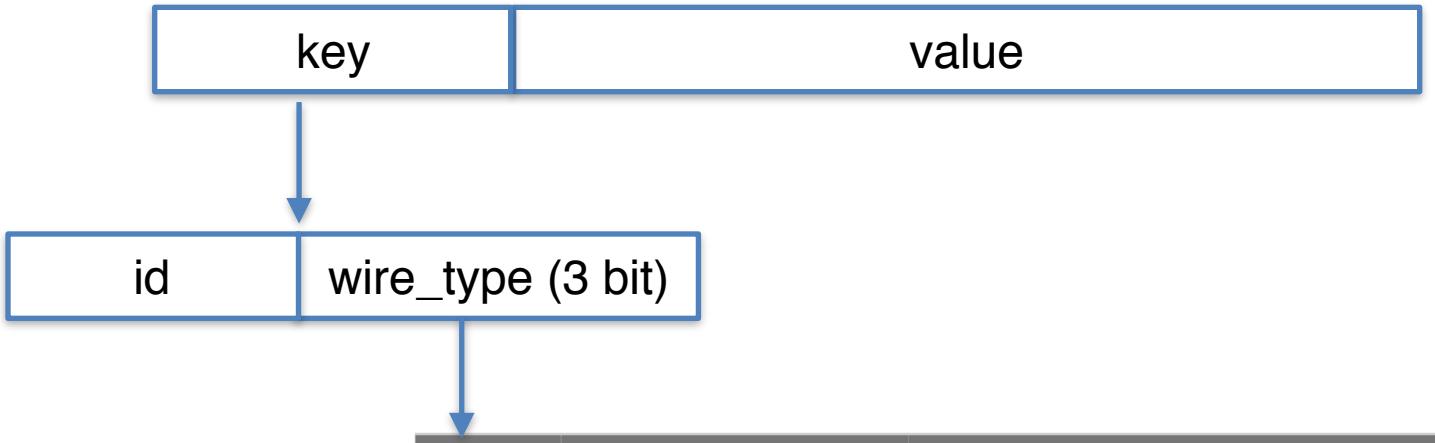
✦ java、c#のILをdecompileすればも復号可能



★IL2CPPを使用すると？

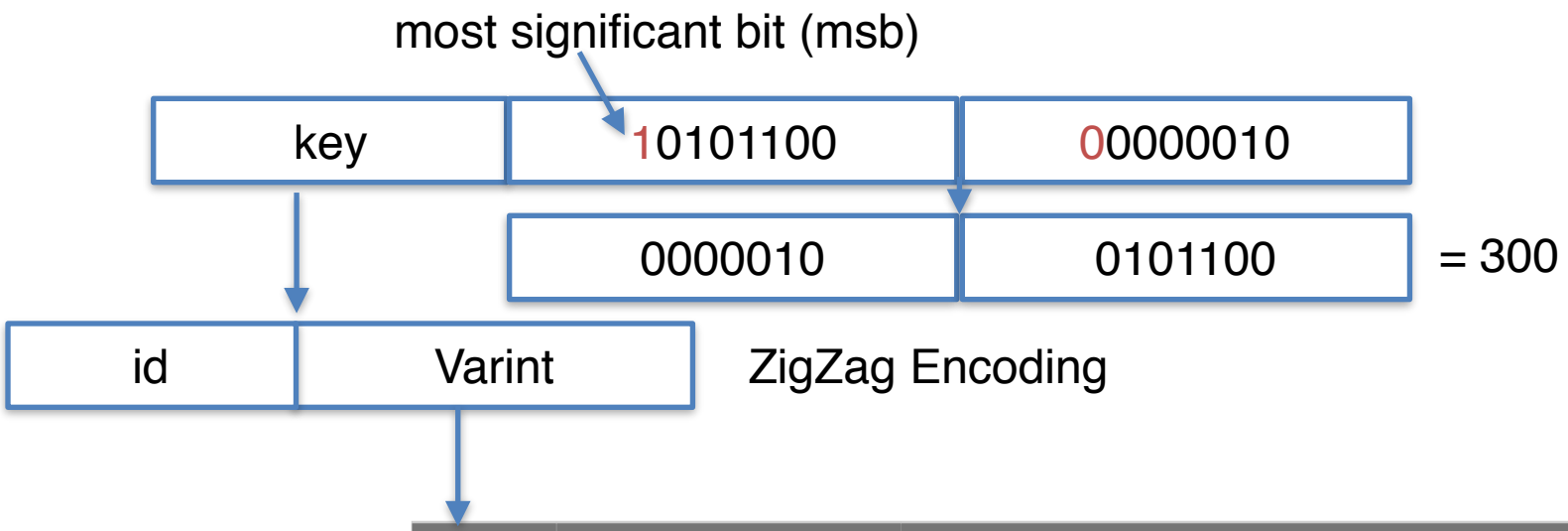
- Protobuf Encoding (https://developers.google.com/protocol-buffers/docs/encoding)

Protobuf解析



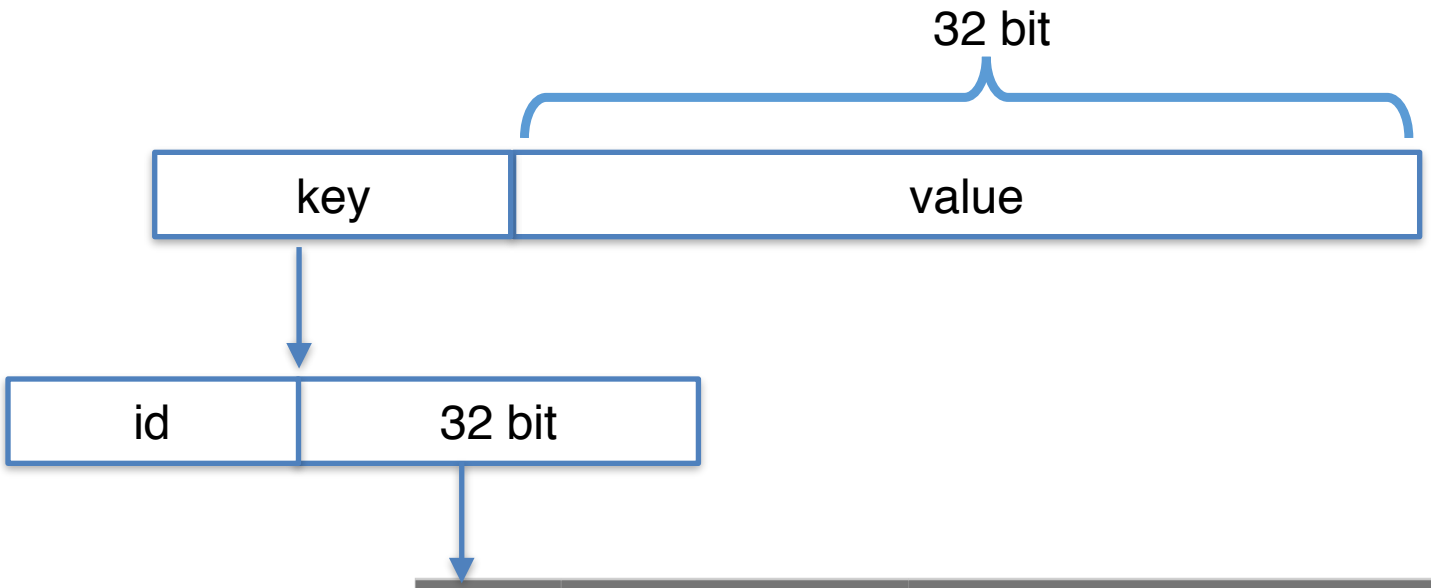
Type	Meaning	Used For
0	Varint	int32, int64, uint32, uint64, sint32, sint64, bool, enum
1	64-bit	fixed64, sfixed64, double
2	Length-delimited	string, bytes, embedded messages, packed repeated fields
3	Start group	groups (deprecated)
4	End group	groups (deprecated)
5	32-bit	fixed32, sfixed32, float

Protobuf解析



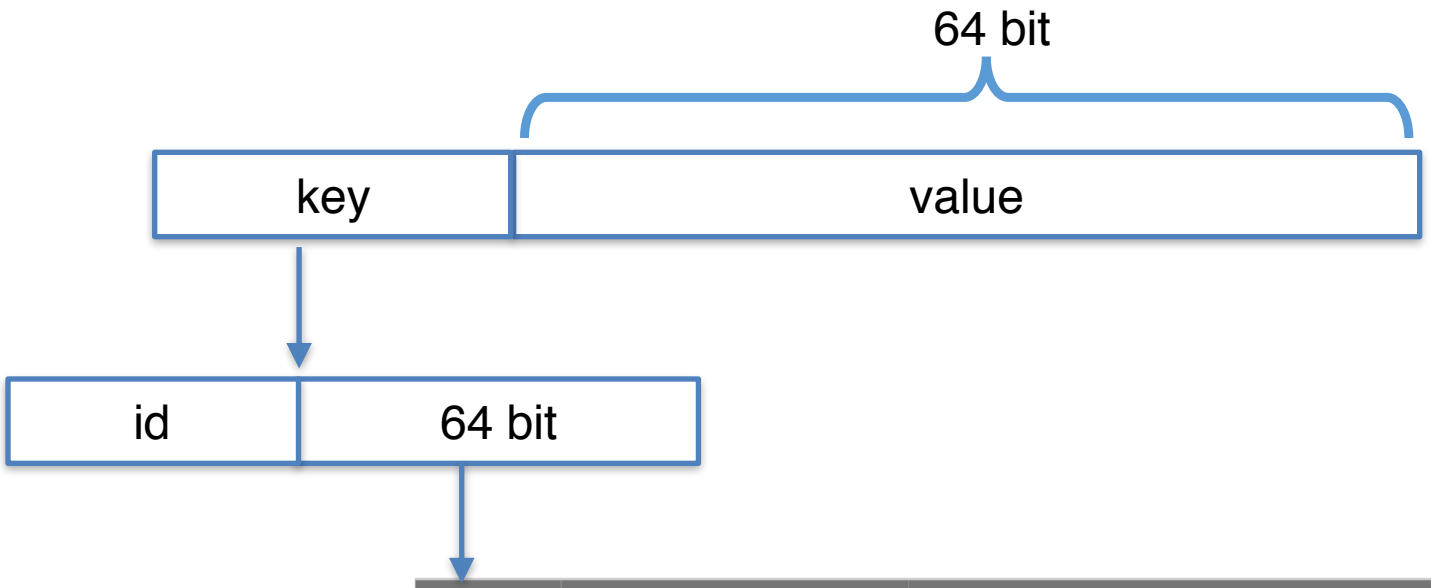
Type	Meaning	Used For
0	Varint	int32, int64, uint32, uint64, sint32, sint64, bool, enum
1	64-bit	fixed64, sfixed64, double
2	Length-delimited	string, bytes, embedded messages, packed repeated fields
3	Start group	groups (deprecated)
4	End group	groups (deprecated)
5	32-bit	fixed32, sfixed32, float

Protobuf解析



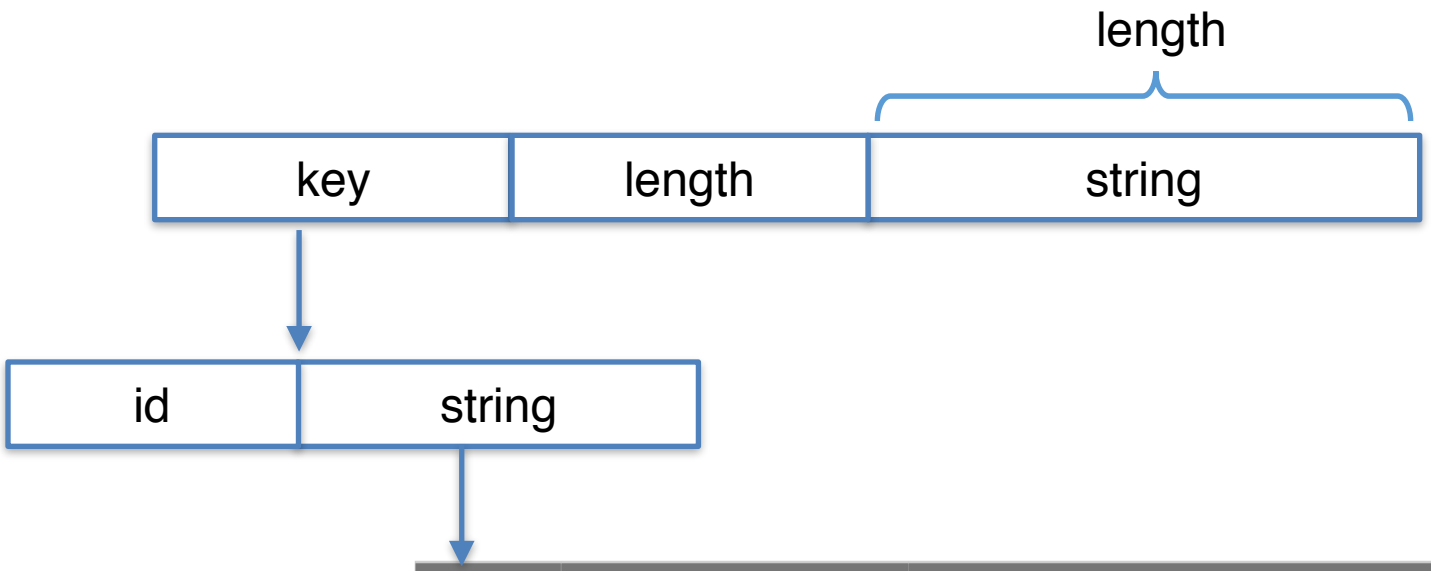
Type	Meaning	Used For
0	Varint	int32, int64, uint32, uint64, sint32, sint64, bool, enum
1	64-bit	fixed64, sfixed64, double
2	Length-delimited	string, bytes, embedded messages, packed repeated fields
3	Start group	groups (deprecated)
4	End group	groups (deprecated)
5	32-bit	fixed32, sfixed32, float

Protobuf解析



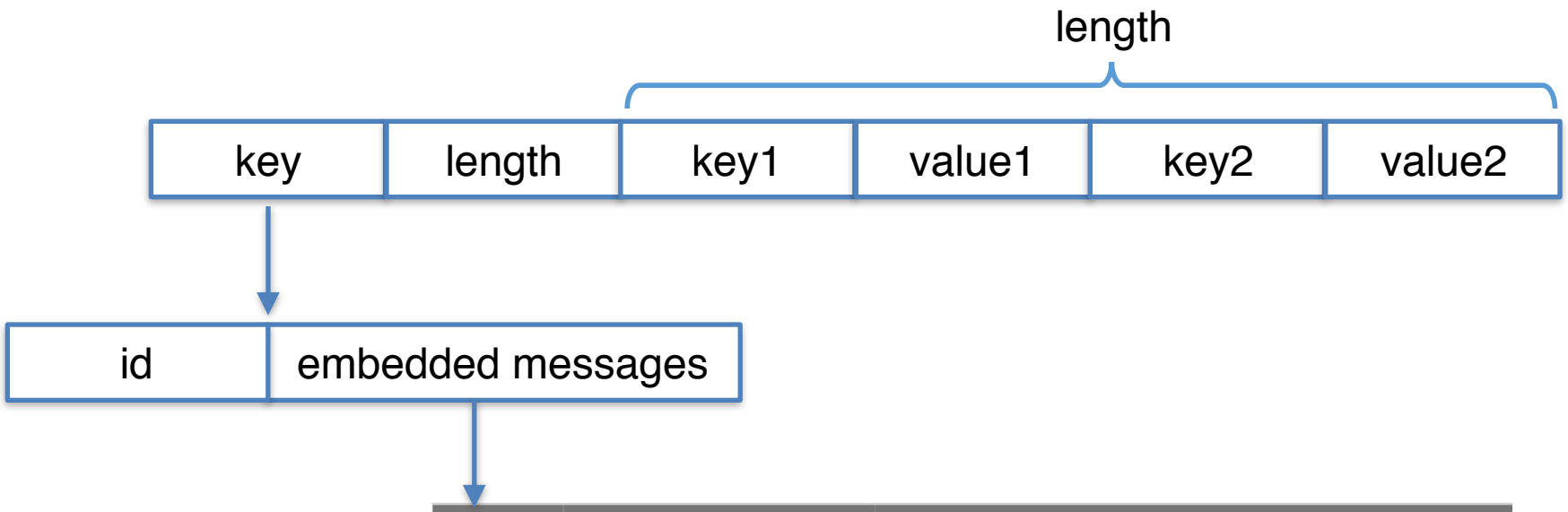
Type	Meaning	Used For
0	Varint	int32, int64, uint32, uint64, sint32, sint64, bool, enum
1	64-bit	fixed64, sfixed64, double
2	Length-delimited	string, bytes, embedded messages, packed repeated fields
3	Start group	groups (deprecated)
4	End group	groups (deprecated)
5	32-bit	fixed32, sfixed32, float

Protobuf解析



Type	Meaning	Used For
0	Varint	int32, int64, uint32, uint64, sint32, sint64, bool, enum
1	64-bit	fixed64, sfixed64, double
2	Length-delimited	string, bytes, embedded messages, packed repeated fields
3	Start group	groups (deprecated)
4	End group	groups (deprecated)
5	32-bit	fixed32, sfixed32, float

Protobuf解析



Type	Meaning	Used For
0	Varint	int32, int64, uint32, uint64, sint32, sint64, bool, enum
1	64-bit	fixed64, sfixed64, double
2	Length-delimited	string, bytes, embedded messages, packed repeated fields
3	Start group	groups (deprecated)
4	End group	groups (deprecated)
5	32-bit	fixed32, sfixed32, float

Protobuf解析

- ✦ 再帰的にtry catchで当たってみる。

Protobuf解析

✦ 再帰的にtry catchで当たってみる。

```
phone_number = person.phone.add()
phone_number.number = number
account = phone_number.account.fnum = 666.777
```

encode

```
.A..............
".Zd;.O..?-.....
.@*.....0800000.
....&D*.....0800
000.E...........
```

protoc --decode_raw

```
1 {
  1: "\343\202\217\343\201\237\343\201\227"
  2: 1234
  4: "Zd;\337O\215\363?-\262\235\357\247\306\t@"
  5 {
    1: 1
    2: "0800000"
    3 {
      1: 0x4426b1ba
    }
  }
  5 {
    1: 1
    2: "0800000"
  }
}
2: 0x4048f5c3
```

float型

自作decoder

```
{
    "01:00:embedded message": {
        "01:00:string": "\u308f\u305f\u3057",
        "02:01:Varint": 1234,
        "04:02:bytes": "0x5a:0x64:0x3b:0xdf:0x4f:0x8d:
        "05:03:embedded message": {
            "01:00:Varint": 1,
            "02:01:string": "0800000"
        }
    },
    "02:01:32-bit": 3.140000104904175
}
```

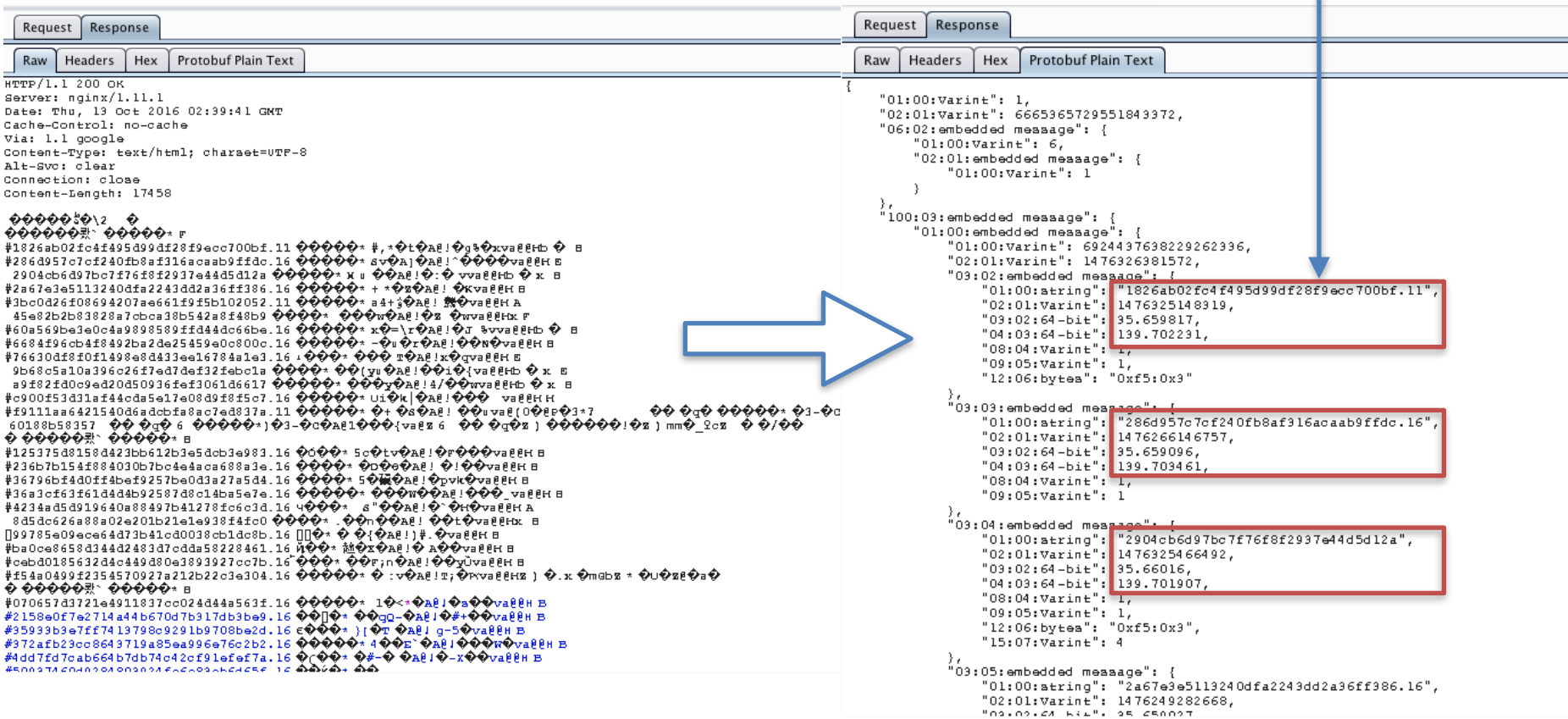
JSON出力、編集、

Re-encodingもサポート

Protobuf解析

✦ burp pluginにしてみる

id、timestamp、座標？



source: https://github.com/nevermoe/protobuf-decoder

目次

- セキュリティ診断概要
- バイナリー解析
- 通信解析
- 対策＆まとめ

対策＆まとめ

✦パケットでも、バイナリーでも、

Non-Cryptographic手法をやめよう

- バイナリー暗号化、難読化！
- 通信暗号化！

✦Game SecurityはDynamicで、

一つの手法に頼ってはいけない

- 対処法：

  開発 —> Anti-cheat SDK —>セキュリティ診断 —> モニタリング

Q&A

Thank you!