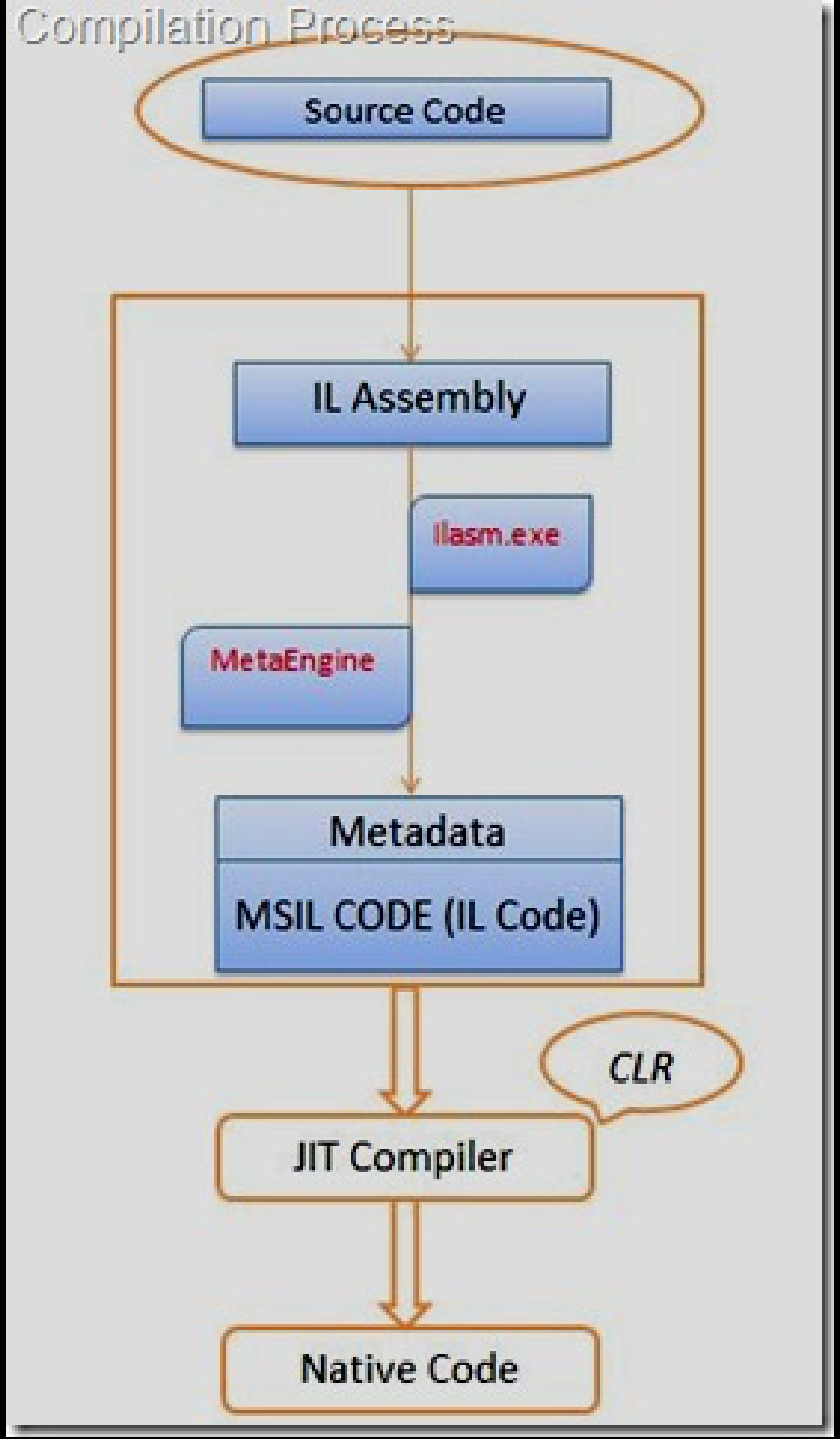
Unity3D Game Hacking

Talk by

Alberto Xamin

0x0

Understanding the compilation process



Understanding the compilation process

TLDR;

Assembly-CSharp.dll

has all that we need

The tools

Windows: dnSpy https://github.com/0xd4d/dnSpy
MacOS/Linux: ILSpy https://github.com/icsharpcode/ILSpy

The tools (footnotes)

Unix command:

```
ilspycmd /path/to/Assembly-CSharp.dll -p -o OutputFolder

/*
-p Indica di creare un progetto CSharp
Se non viene specificata una cartella con -o, viene tutto
stampato nel terminale
*/
```

dnSpy is based from ILSpy

dnSpy demo

nothing to see here

Oh no, obfuscation

```
using O111; using O111.l1000; using System; using System.Collections; using
System.l1001; using System.l1010; using System.Text; public class l1011 {
public string l1100; public int l1101; public l1011(string l1011) { l1100 =
O1110(l1011); } public int O1111 { get { if (l1101 == 0) return 1; if (l1101
== 1 && l1100 == "v\u006F\u0069\u0064") return 012; return 3; } } public bool
O10000 { get { return l1101 == 0 && l1100 == "\u0076oid"; } } public string
O10001(int O10010, bool O10011, bool l10100) { if (l1101 == 0) return l1100;
if (O10010 == 0) return l1100+l10101(l10100 ? '\u0050' : '\u002A'); if (l1101
> 1 || O10011 || O10010 == 1) return "\u0049n\u0074\u0050\u0074\u0072"; if (
l1100 == "\u0076o\u0069d") switch (O10010) { case 2 : return "b\u0079\u0074\
u0065[\u005D"; case 3 : return "sbyte\u005B]"; case 4 : return "\u0073\u0068\
u006Fr\u0074[]"; case 5 : return "\u0075\u0073h\u006Fr\u0074\u005B]"; case
6 : return "\u0069\u006E\u0074[\u005D"; case 7 : return "\u0075int[]"; case
8 : return "\u0066\u006C\u006Fa\u0074[]"; case 011 : return "d\u006Fu\u0062\
u006C\u0065\u005B]"; } return l1100+"\u005B]"; } string l10101(char O10110) {
l10111 O11000 = new l10111(); for (int O11001 = 0; O11001 < l1101;
O11001++ )O11000.l11010(O10110); return O11000.O10001(); } public bool O11011 {
get { return l1101 > 0; } } public int O11100 { get { switch (l1100) { case "
v\u006Fid" : return 0; case "b\u0079\u0074\u0065" : case "\u0073b\u0079te" :
return 1; case "s\u0068o\u0072\u0074" : case "\u0075\u0073h\u006Fr\u0074" :
return 2; case "i\u006Et" : case "u\u0069nt" : return 4; case "\u0066loat" :
return 4; case "\u0064\u006F\u0075b\u006Ce" : return 8; default : throw new
l11101("unkno\u0077\u006E \u0062\u0061se\u0020\u0074ype"); } } } static
O11110 l11111; public static string O1110(string l1011) { if (l11111 == null)
l11111 = O100000(); string l100001 = (string)l11111[l1011]; if (l100001 ==
null) { l100010.l100011.l100100("\u0077a\u0072\u006Ei\u006Eg:\u0020u\u006Ekno\
u0077\u006E\u0020\u0074\u0079\u0070\u0065\u0020\u0022"+l1011+"\u0022\
u0020use \u0061\u0073 \u0069\u0073."); l11111[l1011] = l1011; l100001 =
l1011; } return l100001; } static O11110 O100000() { O11110 l100001 = new
O11110(); l100001["v\u006Fid"] = "\u0076o\u0069\u0064"; l100001["\u0047L\
u0076oid"] = "v\u006F\u0069\u0064"; l100001["G\u004Cenum"] = "u\u0069n\
u0074"; l100001["G\u004Cby\u0074\u0065"] = "\u0062\u0079t\u0065"; l100001["\
u0047\u004C\u0073h\u006F\u0072\u0074"] = "\u0073hort"; l100001["\u0047Lint"]
= "\u0069\u006E\u0074"; l100001["\u0047Lsizei"] = "i\u006Et"; l100001["\
u0047L\u0075\u0062yt\u0065"] = "b\u0079t\u0065"; l100001["\u0047\u004C\u0075\
u0069n\u0074"] = "\u0075int"; l100001["G\u004Cfloat"] = "\u0066l\u006F\
u0061t"; l100001["\u0047L\u0075short"] = "ushor\u0074"; l100001["G\u004Cclamp\
u0066"] = "f\u006Coat"; l100001["\u0047Ldouble"] = "d\u006Fuble"; l100001["\
u0047L\u0063lampd"] = "\u0064ouble"; l100001["G\u004Cbo\u006F\u006C\u0065\
u0061n"] = "\u0062yte"; l100001["\u0047\u004C\u0062i\u0074\u0066iel\u0064"]
= "\u0075int"; return l100001; } }Lorem ipsum
```

Deobfuscation

Which obfuscation was used?

We can use exeinfoPE http://exeinfo.xn.pl

```
/*
that domain is about to expire, I reuploaded it to gDrive
you need a unitn account to access the file

https://goo.gl/6KcakZ
*/
```

Let’s play

Cheat demo

What about non windows games

We still have the dlls

MacOS: game.app/Contents/Resources/Data/Managed
Android: game.apk/assets/bin/Data/Managed

I can’t find any dll and I’m sure the game was made with Unity how is this possible?
They used Playmaker (example: Inside)

How to prevent cheating

Check the hash of the dll

Let the server handle the game, the clients should only send commands.

Obviously you can’t always do that for example in realtime action games but you can do a strict check for out of ordinary behaviours

(You can’t stop that, It’s only a matter of time)

That’s the end.

Aka question time.