# Binary Reverse Engineering And Analysis

Course 9: RE++

Caragea Radu

April 16, 2021

# Recap for RE

- Assembly
- PE/ELF
- Compiled C programs
- General principles:
  - Static/dynamic analysis
  - $\blacksquare \ \ Whitebox/Graybox/Blackbox$

# Reverse Engineering in Other Languages?

■ PopularitY of Programming Language Index: https://pypl.github.io

Rank	Change	Language	Share	Trend
1	ige	Python	30.17 %	-0.2 %
2		Java	17.18 %	-1.2 %
3		JavaScript	8.21 %	+0.2 %
4		C#	6.76 %	-0.6 %
5	<b>^</b>	C/C++	6.71 %	+0.8 %
6	Ψ.	PHP	6.13 %	+0.0 %
7		R	3.81 %	+0.0 %
8		Objective-C	3.56 %	+1.1 %
9		Swift	1.82 %	-0.4 %
10	<b>^</b>	Matlab	1.8 %	-0.0 %
11	<b>^</b>	Kotlin	1.76 %	+0.2 %
12	44	TypeScript	1.74 %	-0.1 %
13	<b>^</b>	Go	1.34 %	+0.0 %
14	<b>4</b>	VBA	1.22 %	-0.1 %
15		Ruby	1.13 %	-0.1 %
16	<u>ተተ</u>	Rust	1.13 %	+0.5 %
17	<u>ተተተተተ</u>	Ada	0.68 %	+0.4 %
18	<b>4</b>	Visual Basic	0.67 %	-0.3 %
19	+++	Scala	0.66 %	-0.4 %
20	ተተተተ	Lua	0.55 %	+0.2 %

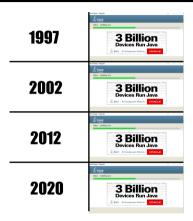
# Python

- Bytecode ".pyc" files
- Can be bundled (e.g. py2exe, pyinstaller)
- Contains interpreter, dependencies, bytecode
- How do we approach it? DEMO

### Python tools

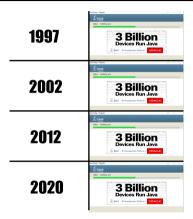
- py2exe unpacker github.com/matiasb/unpy2exe
- pyinstaller unpacker github.com/extremecoders-re/pyinstxtractor
- py2, py3 until 3.8 github.com/rocky/python-uncompyle6
- py3 from 3.8 github.com/rocky/python-decompile3

### Java



- Compiles source code to Java bytecode (.class files)
- Bytecode can be run on any architecture. Why?

### Java



- Compiles source code to Java bytecode (.class files)
- Bytecode can be run on any architecture. Why?
- Java Virtual Machine interprets the bytecode

# Java bytecode 1/3

```
2⊖ public class HelloWorld {
 4⊖public static long gcd(long a, long b){
       long factor= Math.min(a, b);
      for(long loop= factor;loop > 1;loop--){
         if(a % loop == 0 && b % loop == 0){
            return loop:
10
11
       return 1:
12 }
13
14
150
        public static void main(String[] args) {
16
           // Prints "Hello, World" to the terminal window.
17
           System.out.println("Hello, World");
18
19
20 }
```

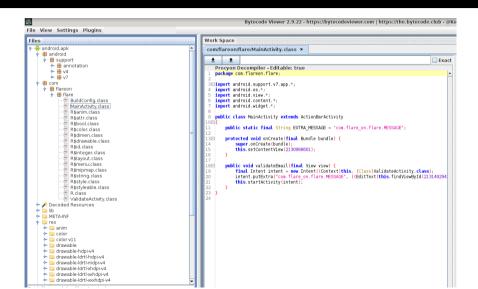
# Java bytecode 2/3

```
. . . . . . . . 7 . % . . . . . .
         00 14 00 15 09 00 16 00
                                  17 08 00 18 0a 00 19 00
         1a 07 00 1b 07 00 1c 01
                                  88 86 3c 69 6e 69 74 3e
                                                             .....sinit>
            00 03 28 29 56 01
                              00
                                  04 43 6f 64 65 01
                                                             ...()V...Code..
         4c 69 6e 65 4e 75 6d 62
                                  65 72 54 61 62 6c 65 01
                                                            LineNumberTable.
         00 03 67 63 64 01 00 05
                                  28 4a 4a 29 4a 01 00 0d
                                                             ..acd...(11)1...
         53 74 61 63 6b 4d 61 70
                                  54 61 62 6c 65 81 88 84
                                                            |StackManTahle...
         6d 61 69 6e 01 00 16 28
                                  5b 4c 6a 61 76 61 2f 6c
                                                            main...([Ljava/l
            6e 67 2f 53 74 72 69
                                                            lang/String:)V...
                                  6e 67 3b 29 56 01 00 0a
                                                            |SourceFile...Hel
         53 6f 75 72 63 65 46 69
                                  6c 65 01 00 0f 48 65 6c
                                  6a 61 76 61 0c 00 08 00
                                                            loWorld.java....
         09 07 00 1d 0c 00 1e 00
                                                            !!...Hello. World
         21 01 00 0c 48 65 6c 6c
                                  6f 2c 20 57 6f 72 6c 64
                                                            07 00 22 0c 00 23 00 24
         57 6f 72 6c 64 01 00 10
                                  6a 61 76 61 2f 6c 61 6e
                                                            |World...iava/lan
000000f0 67 2f 4f 62 6a 65 63 74
                                  01
                                                            g/Object...java/
                                                            llang/Math...min.
00000100 6c 61 6e 67 2f 4d 61 74
                                  68 01 00 03 6d 69 6e 01
                                                            ..java/lang/Syst
            10 6a 61 76 61 2f 6c
                                  61 6e 67 2f 53 79 73 74
00000120 65 6d 01 00 03 6f 75 74
                                  01 00 15 4c 6a 61 76 61
                                                            lem...out...Liava
            69 6f 2f 50 72 69 6e
                                  74 53 74 72 65 61
                                                            /io/PrintStream:
            00 13 6a 61 76 61 2f
                                  69 6f 2f 50 72 69 6e 74
                                                            |...java/io/Print
                                                            |Stream...println
00000160 01 00 15 28 4c 6a 61 76
                                  61 2f 6c 61 6e 67 2f 53
                                                            ...(Liava/lang/S
         74 72 69 6e 67 3b 29 56
                                                            Itring:)V.!....
00000180 00 00 00 03 00 01 00 08
            1d 00 01 00 01 00 00
                                                             . . . . . . . . . . * . . . . .
000001a0 00 00 01 00 0b 00 00 00
                                                             . . . . . . . . . . . . . . 0 . . .
         08 00 00 00 32 1e 20 b8
                                  88 82 37 84 16 84 37 86
                                                            ....2. ...7...7.
                                                             . . . . . . ! . . . a . . . . .
000001e0 20 16 06 71 09 94 9a 00
                                                             ..q.....e
         37 06 a7 ff de 0a ad 00
         1a 00 06 00 00 00 05 00
                                  87 88 86 88 12 88 87 88
         24 00 08 00 27 00 06 00
                                  30 00 0b 00 0e 00 00 00
                                                            1$...'...0.....
                                  1b fa 00 08 00 09 00 0f
                                  00 25 00 02 00 01 00 00
                                                             10 00 01 00 0a 00 00
         00 09 b2 00 03 12 04 b6
                                                            1......
00000250 0b 00 00 00 0a 00 02 00
                                  00 00 11 00 08 00 12 00
                                                            1......
00000260 01 00 11 00 00 00 02 00
00000269
```

# Java bytecode 3/3

```
2@ public class HelloWorld {
             4⊕public static long gcd(long a, long b){
                   long factor= Math.min(a, b);
                   for(long loop= factor:loop > 1:loop--){
                      if(a % loop == 0 && b % loop == 0){
                         return loop;
             9
                   return 1:
            12 }
            14
            15⊜
                    public static void main(String[] args) {
            16
                       // Prints "Hello, World" to the terminal window.
                        System.out.println("Hello, World");
            18
            19
            20 }
  public class HelloWorld
    public static long gcd(long paramLongl, long paramLong2) {
      long 11 = Math.min(paramLong1, paramLong2): long 12:
60
      for (12 = 11: 12 > 1L: 12--) {
        if (paramLong1 % 12 == OL && paramLong2 % 12 == OL) {
          return 12:
      return 1L:
    public static void main(String[] paramArrayOfString) { System.out.println("Hello, World"); }
```

### Example: Java in APK



# Mobile Security

- More than just the Android ecosystem
- Dynamic analysis gets very interesting
- Bytecode interconnects with native code

# C# code

- .NET and CLR
- Bytecode, same as Java => decompilable
- Obfuscators exist (including commercial ones)

### .NET reversing 1/2

```
// CODE YREF: XXXXXXXXXXXXXXX Form1 ctor+7th
                 class [System.Windows.Forms]System.Windows.Forms.Label XXXXXXXXXXXXXXX.Form1::lbl title
newobi
stfld
                 class [System.Windows.Forms]System.Windows.Forms.PictureBox XXXXXXXXXXXXXXXX.Form1::pbRoge
newobi
stloc.0
ldfld class [System.Windows.Forms]System.Windows.Forms.PictureBox XXXXXXXXXXXXXXXXXX.Form1::pbRoge
callvirt instance void [System] System.ComponentModel.ISupportInitialize::BeginInit()
 ldlec.0
 ldstr aMicrosoftSansS // "Microsoft Sans Serif"
1dc . 14 . 0
1dc.14.3
1dc 14 0
newobj instance void [System.Drawing]System.Drawing.Font::.ctor(string, float32, valuetype [System.Drawing]System.Drawing.FontStyle.
callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set.Font(class [System.Drawing]System.Drawing.Font)
1de i4 Ovt
newobj instance void [System.Drawing]System.Drawing.Point::.ctor(int32, int32)
callyirt instance void (System Windows Forms | System Windows Forms | Control : set Location (valuetype (System Drawing | System Drawing | System Drawing | System | Drawing |
 1d1oc.0
callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set Name(string)
 1d1oc 0
1dc i4 s 0x34
newobi instance void [System.Drawing]System.Drawing.Size::.ctor(int32, int32)
callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set Size(valuetype [System.Drawing]System.Drawing.Size)
callwirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set TabIndex(int32)
 1d1oc 0
ldstr aDecode
 callvirt instance void [System, Windows, Forms | System, Windows, Forms, Control::set Text(string)
callwirt instance void [System.Windows.Forms]System.Windows.Forms.ButtonBase::set UseVisualStyleBackColor(bool)
 ldlec.0
 ldarg.0
ldftn instance void XXXXXXXXXXXXXXXXXX.Forml::btnDecode Click(object sender, class [mscorlib]System.EventArgs e)
newobi instance void [mscorlib]System.EventHandler::.ctor(object. native int)
callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::add_Click(class [mscorlib]System.EventHandler)
 ldarg.0
ldfld class [System.Windows.Forms|System.Windows.Forms.Label XXXXXXXXXXXXX Formi::lbl title
```

# .NET reversing 2/2

```
Edit View Debug Window Help 👩 🔘 🛂 № C# 🔻 🔻 💆 🕒 Start 🔎
                                                                                                                                                                                    InitializeComponent(): void >
 Assembly Explorer

■ In a control of the property of the pro
       b 11 DE
                ▶ ■■ References
                Þ ■ Resources
                4 % Form1 @02000002
                                  P Rase Type and Interfaces
                                  P Derived Types
                                                                                                                                                                                                                                button.Location = new Point(210, 387);
                                                                                                                                                                                                                                button.Size = new Size(139, 52);
                                       components: |Container @04000001
                                       ♣ Ibl title: Label @04000002
                                        pbRoge: PictureBox @04000003
                                                                                                                                                                                                                                this.lbl title.Font = new Font("Microsoft Sans Serif", 20f. FontStyle.Regular, GraphicsUnit.Point, 0):
                       Program @02000003
                                                                                                                                                                                                                                this.lbl title.Location = new Point(95, 18);
                ↓ () XXXXXXXXXXXXXXX Properties
 mscorlib (2.0.0.0)
 System.Windows.Forms (2.0.0.0)
 ▶ 🗗 System (2.0.0.0)
System Drawing (2.0.0.0)
                                                                                                                                                                                                                                this pbRoge Size = new Size(401, 316):
                                                                                                                                                                                                                                base.AutoScaleDimensions - new SizeE(6f. 13f):
                                                                                                                                                                                                                                base.ClientSize - new Size(566, 444);
                                                                                                                                                                                                                                base.FormBorderStyle = FormBorderStyle.Fixed3D;
```

### Decompetition 2021



#### Decompetition

#### Congratulations to ppp for taking first place!

Calling all reverse engineers! Test your reversing skills against the systems languages of the twenty-first century: C, C++, Go, Rust, and Swift. Given only a binary, can you recreate the original source code?



Your candidate source code will be compiled, and the resulting binary will be tested and disassembled. The majority of your score will come from the intersection over union of your disassembly versus the target disassembly. How close can you get to a perfect reconstruction?

#### The Details

#### Playing

Anyone with an internet connection and a web browser can play. Access to a reverse engineering program is recommended but not required. If you don't have any reversing software installed, check out Binary Ninja Cloud.

This is a team competition. There's no team size limit.

# Decompetition 2021

#### Challenges

You'll need to log in or register before you can access the challenges.

Challenge	Lang.	Value	Score
baby-c #1	С	200	⊕ ±
baby-cpp #2	cpp	200	@ 生
baby-go #3	go	200	@ ±
baby-rust #4	rust	300	@ ±
baby-swift #5	swift	300	⊕ 坐
bandate #6	swift	400	⊕ ⊁
batsounds #7	go	300	@ ±
bitesize #8	С	100	@ ±
cardigan 🗝	swift	500	@ ±
carshop #10	go	300	⊕ ⊁
fabulous #11	go	200	@ ±
habidasher #12	rust	200	⊚⊁
julie #13	go	300	@ ±
lambic #14	cpp	400	⊕ ⊀
pedigree #15	cpp	200	⊚坐
prime #16	С	100	
rootkit #17	С	100	@ ±
s2ring #18	rust	500	⊕ ⊀
streamy #19	cpp	400	⊕坐
switcher #20	go	200	⊕ ±
toobz #21	rust	300	@ ±
unfair #22	срр	200	⊕坐
wolfgang #23	go	300	@ ±

# Going further

- Malware analysis from RPISEC: github.com/RPISEC/Malware
- Mobile Security from EURECOM: mobisec.reyammer.io
- PoC||GTFO: www.alchemistowl.org/pocorgtfo
- Hex-Rays blog: www.hex-rays.com/blog

#### Practice

- Any Questions?
- https://pwnthybytes.ro/unibuc\_re/09-lab.html