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
  - Whitebox/Graybox/Blackbox

Reverse Engineering in Other Languages?

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

Rank	Change	Language	Share	Trend
1		Python	30.17 %	-0.2 %
2		Java	17.18 %	-1.2 %
3		JavaScript	8.21 %	+0.2 %
4		C#	6.76 %	-0.6 %
5	↑	C/C++	6.71 %	+0.8 %
6	↓	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	↑	Matlab	1.8 %	-0.0 %
11	↑	Kotlin	1.76 %	+0.2 %
12	↓↓	TypeScript	1.74 %	-0.1 %
13	↑	Go	1.34 %	+0.0 %
14	↓	VBA	1.22 %	-0.1 %
15		Ruby	1.13 %	-0.1 %
16	↑↑	Rust	1.13 %	+0.5 %
17	↑↑↑↑↑↑	Ada	0.68 %	+0.4 %
18	↓	Visual Basic	0.67 %	-0.3 %
19	↓↓↓	Scala	0.66 %	-0.4 %
20	↑↑↑↑	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

1997	
2002	
2012	
2020	

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

Java

1997	
2002	
2012	
2020	

- 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

```java

public class HelloWorld {

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;
        }
    }
    return 1;
}


    public static void main(String[] args) {
        // Prints "Hello, World" to the terminal window.
        System.out.println("Hello, World");
    }

}
```

Java bytecode 2/3

```
00000000  ca fe ba be 00 00 00 37  00 25 0a 00 07 00 13 0a  |.......7.%......|
00000010  00 14 00 15 09 00 16 00  17 08 00 18 0a 00 19 00  |................|
00000020  1a 07 00 1b 07 00 1c 01  00 06 3c 69 6e 69 74 3e  |..........<init>|
00000030  01 00 03 28 29 56 01 00  04 43 6f 64 65 01 00 0f  |...()V...Code...|
00000040  4c 69 6e 65 4e 75 6d 62  65 72 54 61 62 6c 65 01  |LineNumberTable.|
00000050  00 03 67 63 64 01 00 05  28 4a 4a 29 4a 01 00 0d  |..gcd...(JJ)J...|
00000060  53 74 61 63 6b 4d 61 70  54 61 62 6c 65 01 00 04  |StackMapTable...|
00000070  6d 61 69 6e 01 00 16 28  5b 4c 6a 61 76 61 2f 6c  |main...([Ljava/l|
00000080  61 6e 67 2f 53 74 72 69  6e 67 3b 29 56 01 00 0a  |ang/String;)V...|
00000090  53 6f 75 72 63 65 46 69  6c 65 01 00 0f 48 65 6c  |SourceFile...Hel|
000000a0  6c 6f 57 6f 72 6c 64 2e  6a 61 76 61 0c 00 08 00  |loWorld.java....|
000000b0  09 07 00 1d 0c 00 1e 00  0d 07 00 1f 0c 00 20 00  |.............. .|
000000c0  21 01 00 0c 48 65 6c 6c  6f 2c 20 57 6f 72 6c 64  |!...Hello, World|
000000d0  07 00 22 0c 00 23 00 24  01 00 0a 48 65 6c 6c 6f  |.."..#.$...Hello|
000000e0  57 6f 72 6c 64 01 00 10  6a 61 76 61 2f 6c 61 6e  |World...java/lan|
000000f0  67 2f 4f 62 6a 65 63 74  01 00 0e 6a 61 76 61 2f  |g/Object...java/|
00000100  6c 61 6e 67 2f 4d 61 74  68 01 00 03 6d 69 6e 01  |lang/Math...min.|
00000110  00 10 6a 61 76 61 2f 6c  61 6e 67 2f 53 79 73 74  |..java/lang/Syst|
00000120  65 6d 01 00 03 6f 75 74  01 00 15 4c 6a 61 76 61  |em...out...Ljava|
00000130  2f 69 6f 2f 50 72 69 6e  74 53 74 72 65 61 6d 3b  |/io/PrintStream;|
00000140  01 00 13 6a 61 76 61 2f  69 6f 2f 50 72 69 6e 74  |...java/io/Print|
00000150  53 74 72 65 61 6d 01 00  07 70 72 69 6e 74 6c 6e  |Stream...println|
00000160  01 00 15 28 4c 6a 61 76  61 2f 6c 61 6e 67 2f 53  |...(Ljava/lang/S|
00000170  74 72 69 6e 67 3b 29 56  00 21 00 06 00 07 00 00  |tring;)V.!......|
00000180  00 00 00 03 00 01 00 08  00 09 00 01 00 0a 00 00  |................|
00000190  00 1d 00 01 00 01 00 00  00 05 2a b7 00 01 b1 00  |..........*.....|
000001a0  00 00 01 00 0b 00 00 00  06 00 01 00 00 00 02 00  |................|
000001b0  09 00 0c 00 0d 00 01 00  0a 00 00 00 6f 00 04 00  |............o...|
000001c0  08 00 00 00 32 1e 20 b8  00 02 37 04 16 04 37 06  |....2. ...7...7.|
000001d0  16 06 0a 94 9e 00 21 1e  16 06 71 09 94 9a 00 0f  |......!...q.....|
000001e0  20 16 06 71 09 94 9a 00  06 16 06 ad 16 06 0a 65  | ..q...........e|
000001f0  37 06 a7 ff de 0a ad 00  00 00 02 00 0b 00 00 00  |7...............|
00000200  1a 00 06 00 00 00 05 00  07 00 06 00 12 00 07 00  |................|
00000210  24 00 08 00 27 00 06 00  30 00 0b 00 0e 00 00 00  |$...'...0.......|
00000220  0b 00 03 fd 00 0b 04 04  1b fa 00 08 00 09 00 0f  |................|
00000230  00 10 00 01 00 0a 00 00  00 25 00 02 00 01 00 00  |.........%......|
00000240  00 09 b2 00 03 12 04 b6  00 05 b1 00 00 00 01 00  |................|
00000250  0b 00 00 00 0a 00 02 00  00 00 11 00 08 00 12 00  |................|
00000260  01 00 11 00 00 00 02 00  12                       |.........|
00000269
```

Java bytecode 3/3

```java

public class HelloWorld {

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;
      }
   }
   return 1;
}


    public static void main(String[] args) {
        // Prints "Hello, World" to the terminal window.
        System.out.println("Hello, World");
    }

}
```

```java
public class HelloWorld
{
  public static long gcd(long paramLong1, long paramLong2) {
    long l1 = Math.min(paramLong1, paramLong2); long l2;
    for (l2 = l1; l2 > 1L; l2--) {
      if (paramLong1 % l2 == 0L && paramLong2 % l2 == 0L) {
        return l2;
      }
    }
    return 1L;
  }



  public static void main(String[] paramArrayOfString) { System.out.println("Hello, World"); }
}
```

Example: Java in APK

Bytecode Viewer 2.9.22 - https://bytecodeviewer.com | https://the.bytecode.club - @Ko

File View Settings Plugins

Files

- android.apk
  - android
    - support
      - annotation
      - v4
      - v7
  - com
    - flareon
      - flare
        - BuildConfig.class
        - MainActivity.class
        - R$anim.class
        - R$attr.class
        - R$bool.class
        - R$color.class
        - R$dimen.class
        - R$drawable.class
        - R$id.class
        - R$integer.class
        - R$layout.class
        - R$menu.class
        - R$mipmap.class
        - R$string.class
        - R$style.class
        - R$styleable.class
        - R.class
        - ValidateActivity.class
  - Decoded Resources
  - lib
  - META-INF
  - res
    - anim
    - color
    - color-v11
    - drawable
    - drawable-hdpi-v4
    - drawable-ldrtl-hdpi-v4
    - drawable-ldrtl-mdpi-v4
    - drawable-ldrtl-xhdpi-v4
    - drawable-ldrtl-xxhdpi-v4
    - drawable-ldrtl-xxxhdpi-v4

Work Space

com/flareon/flare/MainActivity.class

Exact

Procyon Decompiler - Editable: true

```
1   package com.flareon.flare;
2
3   import android.support.v7.app.*;
4   import android.os.*;
5   import android.view.*;
6   import android.content.*;
7   import android.widget.*;
8
9   public class MainActivity extends ActionBarActivity
10  {
11      public static final String EXTRA_MESSAGE = "com.flare_on.flare.MESSAGE";
12
13      protected void onCreate(final Bundle bundle) {
14          super.onCreate(bundle);
15          this.setContentView(2130968601);
16      }
17
18      public void validateEmail(final View view) {
19          final Intent intent = new Intent((Context)this, (Class)ValidateActivity.class);
20          intent.putExtra("com.flare_on.flare.MESSAGE", ((EditText)this.findViewById(2131492994
21          this.startActivity(intent);
22      }
23  }
24
```

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

```
                    .method private hidebysig instance void InitializeComponent()
                                                          // CODE XREF: XXXXXXXXXXXXXXX.Form1__.ctor+7↑p
                    {
                      .maxstack 6
                      .locals init (class [System.Windows.Forms]System.Windows.Forms.Button V0)
02
73 19 00 00 0A        newobj   instance void [System.Windows.Forms]System.Windows.Forms.Label::.ctor()
7D 02 00 00 04        stfld    class [System.Windows.Forms]System.Windows.Forms.Label XXXXXXXXXXXXXXX.Form1::lbl_title
02
73 1A 00 00 0A        newobj   instance void [System.Windows.Forms]System.Windows.Forms.PictureBox::.ctor()
7D 03 00 00 04        stfld    class [System.Windows.Forms]System.Windows.Forms.PictureBox XXXXXXXXXXXXXXX.Form1::pbRoge
73 1B 00 00 0A        newobj   instance void [System.Windows.Forms]System.Windows.Forms.Button::.ctor()
0A                    stloc.0
02                    ldarg.0
7B 03 00 00 04        ldfld    class [System.Windows.Forms]System.Windows.Forms.PictureBox XXXXXXXXXXXXXXX.Form1::pbRoge
6F 1C 00 00 0A        callvirt instance void [System]System.ComponentModel.ISupportInitialize::BeginInit()
02                    ldarg.0
28 1D 00 00 0A        call     instance void [System.Windows.Forms]System.Windows.Forms.Control::SuspendLayout()
08                    ldloc.0
72 07 00 00 70        ldstr    aMicrosoftSansS            // "Microsoft Sans Serif"
22 00 00 80 41        ldc.r4   16.0
18                    ldc.i4.0
19                    ldc.i4.3
16                    ldc.i4.0
73 1E 00 00 0A        newobj   instance void [System.Drawing]System.Drawing.Font::.ctor(string, float32, valuetype [System.Drawing]System.Drawing.FontStyle, v
6F 1F 00 00 0A        callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set_Font(class [System.Drawing]System.Drawing.Font)
16                    ldc.i4.0
20 D2 00 00 00        ldc.i4   0xD2
20 83 01 00 00        ldc.i4   0x183
73 20 00 00 0A        newobj   instance void [System.Drawing]System.Drawing.Point::.ctor(int32, int32)
6F 21 00 00 0A        callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set_Location(valuetype [System.Drawing]System.Drawing.Point)
08                    ldloc.0
72 31 00 00 70        ldstr    aBtndecode                 // "btnDecode"
6F 22 00 00 0A        callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set_Name(string)
08                    ldloc.0
20 8B 00 00 00        ldc.i4   0x8B
1F 34                 ldc.i4.s 0x34
73 23 00 00 0A        newobj   instance void [System.Drawing]System.Drawing.Size::.ctor(int32, int32)
6F 24 00 00 0A        callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set_Size(valuetype [System.Drawing]System.Drawing.Size)
08                    ldloc.0
16                    ldc.i4.0
6F 25 00 00 0A        callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set_TabIndex(int32)
08                    ldloc.0
72 45 00 00 70        ldstr    aDecode                    // "DECODE!"
6F 16 00 00 0A        callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set_Text(string)
08                    ldloc.0
17                    ldc.i4.1
6F 26 00 00 0A        callvirt instance void [System.Windows.Forms]System.Windows.Forms.ButtonBase::set_UseVisualStyleBackColor(bool)
08                    ldloc.0
02                    ldarg.0
FE 06 02 00 00+       ldftn    instance void XXXXXXXXXXXXXXX.Form1::btnDecode_Click(object sender, class [mscorlib]System.EventArgs e)
08
73 27 00 00 0A        newobj   instance void [mscorlib]System.EventHandler::.ctor(object, native int)
6F 28 00 00 0A        callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::add_Click(class [mscorlib]System.EventHandler)
02                    ldarg.0
7B 02 00 00 04        ldfld    class [System.Windows.Forms]System.Windows.Forms.Label XXXXXXXXXXXXXXX.Form1::lbl_title
```

.NET reversing 2/2

dnSpy v6.0.5 (64-bit)

File Edit View Debug Window Help C# Start

Assembly Explorer

- XXXXXXXXXXXXXXX (1.0.0.0)
  - XXXXXXXXXXXXXXXXXXX
    - PE
    - References
    - Resources
    - { } -
    - { } XXXXXXXXXXXXXXX
      - Form1 @02000002
        - Base Type and Interfaces
        - Derived Types
        - .ctor() : void @06000001
        - btnDecode_Click(object, EventArgs) : void @06000002
        - Dispose(bool) : void @06000003
        - InitializeComponent() : void @06000004
        - components : IContainer @04000001
        - lbl_title : Label @04000002
        - pbRoge : PictureBox @04000003
      - Program @02000003
    - { } 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)

InitializeComponent() : void

```
// XXXXXXXXXXXXXXX.Form1
// Token: 0x06000004 RID: 4 RVA: 0x00002180 File Offset: 0x00000380
private void InitializeComponent()
{
    this.lbl_title = new Label();
    this.pbRoge = new PictureBox();
    Button button = new Button();
    ((ISupportInitialize)this.pbRoge).BeginInit();
    base.SuspendLayout();
    button.Font = new Font("Microsoft Sans Serif", 16f, FontStyle.Regular, GraphicsUnit.Point, 0);
    button.Location = new Point(210, 387);
    button.Name = "btnDecode";
    button.Size = new Size(139, 52);
    button.TabIndex = 0;
    button.Text = "DECODE!";
    button.UseVisualStyleBackColor = true;
    button.Click += this.btnDecode_Click;
    this.lbl_title.AutoSize = true;
    this.lbl_title.Font = new Font("Microsoft Sans Serif", 20f, FontStyle.Regular, GraphicsUnit.Point, 0);
    this.lbl_title.Location = new Point(95, 18);
    this.lbl_title.Name = "lbl_title";
    this.lbl_title.Size = new Size(393, 31);
    this.lbl_title.TabIndex = 1;
    this.lbl_title.Text = "Let's start with something easy!";
    this.pbRoge.Image = Resources.bob_ross;
    this.pbRoge.Location = new Point(87, 65);
    this.pbRoge.Name = "pbRoge";
    this.pbRoge.Size = new Size(401, 316);
    this.pbRoge.TabIndex = 2;
    this.pbRoge.TabStop = false;
    base.AutoScaleDimensions = new SizeF(6f, 13f);
    base.AutoScaleMode = AutoScaleMode.Font;
    base.ClientSize = new Size(566, 444);
    base.Controls.Add(this.pbRoge);
    base.Controls.Add(this.lbl_title);
    base.Controls.Add(button);
    base.FormBorderStyle = FormBorderStyle.Fixed3D;
    base.Name = "Form1";
    this.Text = "Form1";
    ((ISupportInitialize)this.pbRoge).EndInit();
    base.ResumeLayout(false);
    base.PerformLayout();
```

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?

Sign Up!

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	c	200	
baby-cpp #2	cpp	200	
baby-go #3	go	200	
baby-rust #4	rust	300	
baby-swift #5	swift	300	
bandate #6	swift	400	
batsounds #7	go	300	
bitesize #8	c	100	
cardigan #9	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	
prime #16	c	100	
rootkit #17	c	100	
s2ring #18	rust	500	
streamy #19	cpp	400	
switcher #20	go	200	
toobz #21	rust	300	
unfair #22	cpp	200	
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`