

Managed Code Rootkits in Java

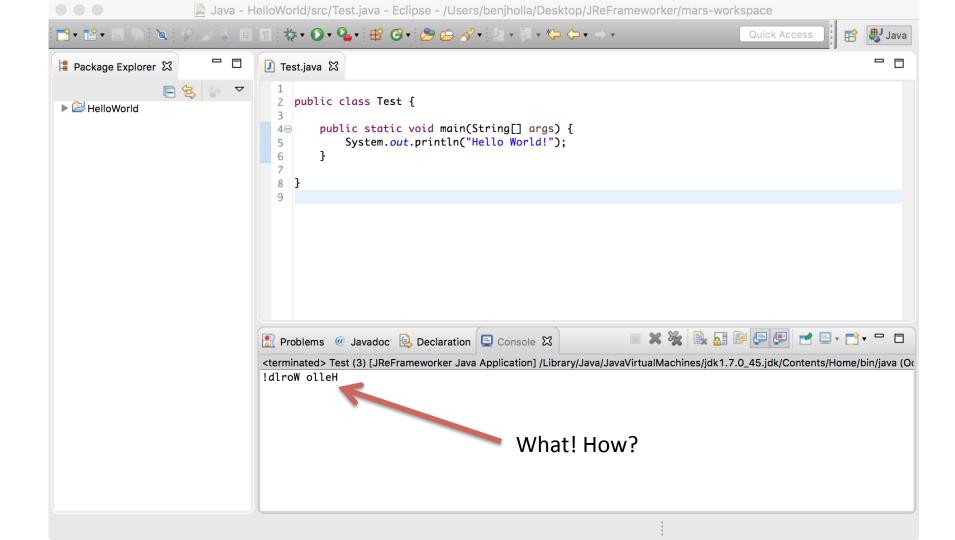
ben-holland.com

Agenda

- Managed Code Rootkits
- JReFrameworker Tool
- Demonstration
- Q/A + Pizza

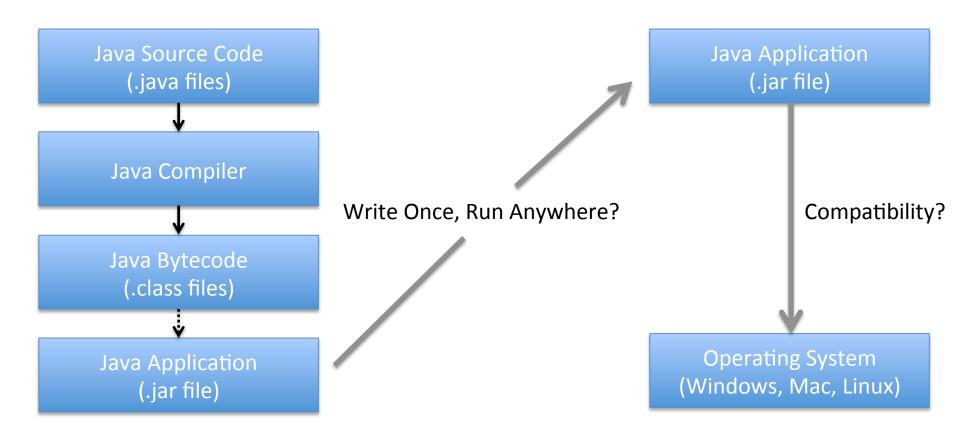
Hello World

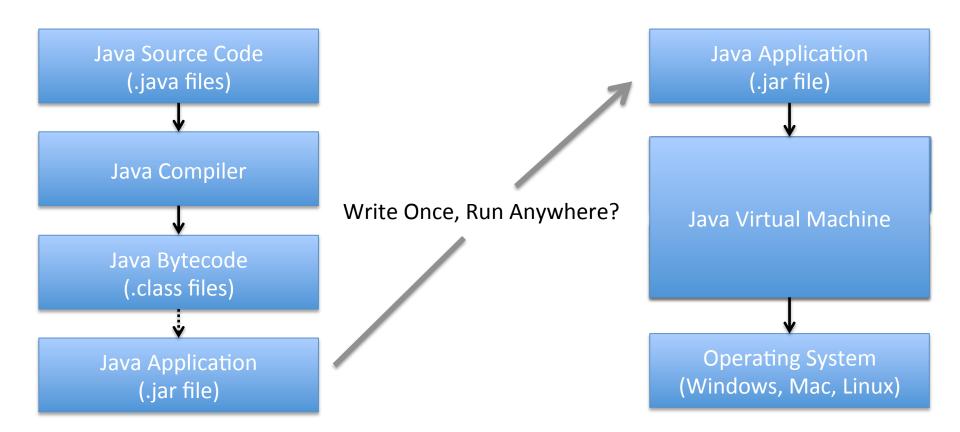
```
public class Test {
3
      public static void main(String[] args) {
4⊜
          System.out.println("Hello World!");
5
```

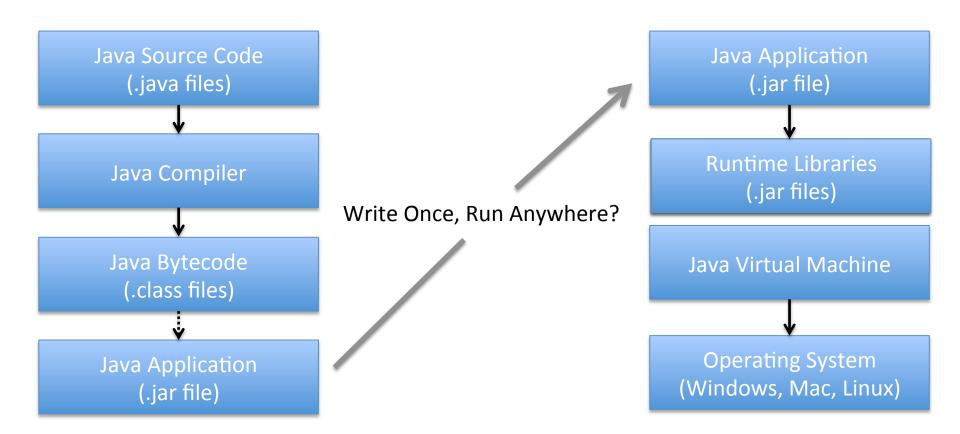


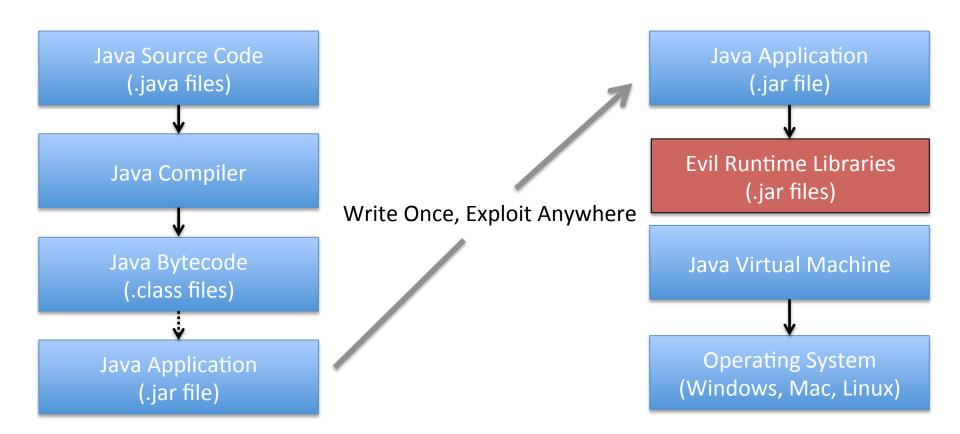
What happened?

- Nothing is wrong with the program...
- Something is wrong with Java itself!









Modifying the Runtime

How can modify the runtime for good evil purposes?

```
0 CAFFRARE 00000033 022D0000 25012700 00250128 04005001 20000041 01240000
  32 A1012B09 002E012C 0A009B01 2D09002E 012E0701 2F0A0009 012D0801 300A0060
  96 3301380A 00490139 07013A08 013B0A00 15013C0A 0049013D 08013E0A 0049013F
 128 08014004 00600141 08014204 00490143 08014404 00490145 08014604 0049014
 160 98914804 99499149 98914404 91339148 99992591 40949969 91409499 69914594
 192 9060014F 04006001 50040060 01510400 2F015207 01530400 2F015404 01330155
 224 84813301 5604902F 81570400 2F015807 81590801 54040034 813C0401 33015804
 256 002F015C 08015D0A 0060015E 07015F0A 003B012D 0A003B01 600A003B 01610A00
 320 01680A00 2E014908 01690701 6A0A0049 016B0701 6C07016D 0A004C01 6E0A016F
 384 04013301 78040171 01790401 33017404 0178017C 04013301 7004002F 017F0701
 416 7F94995R 012D9R91 8091810R 01820183 0R918201 84070185 0R918201 86070187
 448 04002F01 8804005R 01830400 5R018404 005R0186 0701890R 0184018R 04013301
 480 SCR4002F 01800400 25018504 0025018F 04002501 0004002F 01910401 33019208
 640 914F9899 459491B
 672 R801R904 013301R
 832 75730100 194C6061 76612F69 6F2F4669 6C652450 61746853 74617475 733B0100
 864 9C707265 6669784C 656E6774 68010001 49010000 73657061 7261746E 72436861
                                                                             prefixlenath I separatorCha
 896 72919991 43919999 73657961 7261746F 72919911 79617468 53657961 7261746F
 928 72436861 7201000D 70617468 53657061 7261746F 72010010 73657269 616C5665 rChar pathSeparator serialVe
                                                                            rsionUID
 992 450E0DE4 FF010008 66696C65 50617468 0100144C 6A617661 2F6E696F 2F66696C
1024 652E5061 74683B01 00132461 73736572 74608E6E 73446073 61626C65 64010001
                                                                            e/Path:
1056 5A010009 6973496E 76616C69 64010003 28295A01 0004436F 64650100 0F4C696E Z isInvalid ()Z Code Lin
 1888 654F756D 62657254 61626C65 01000D53 7461636B 4D617054 61626C65 07015307
                                                                            eNumberTable
1120 01C50100 0F676574 50726566 69784C65 6E677468 01000328 29490100 063C696E
                                                                             # getPrefixLength ()I sin
1152 69743F01 0016284C 64617661 2F6C616F 672F5374 72696F67 3R492956 01002328
                                                                                  (Ljava/lang/Strina:I)V
1184 4C6A6176 612F6C61 6E672F53 7472696E 673B4C6A 6176612F 696F2F46 696C653B
1216 29560701 85010015 284C6A61 76612F6C 616E672F 53747269 6E673B29 56010027
1248 284C6A61 76612F6C 616E672F 53747269 6E673B4C 6A617661 2F6C616E 672F5374
                                                                            (Ljava/lang/String;Ljava/lang/St
1280 72696E67 3B295601 0023284C 6A617661 2F696F2F 46696C65 3B4C6A61 76612F6C | ring: \V #(Ligyg/io/File:Ligyg/l
          ○ big ○ (select some data)
```

```
1 public class java.io.File extends java.lang.Object implements java.io.Ser;
     private static java.io.FileSystem fs;
     private java.lang.String path;
     private transient java.io.File$PathStatus status:
     private transient int prefixLength;
     public static final char separatorChar;
     public static final java.lang.String separator;
     public static final char pathSeparatorChar;
     public static final java.lang.String pathSeparator;
    private static final long serialVersionUID;
     private transient volatile java.nio.file.Path filePath;
     static final boolean $assertionsDisabled;
                        14. 57. 5T STICKY
        $r1 = r0.<iqva.io.File: jqva.io.File$PqthStqtus stqtus>:
        if $r1 != null goto label3;
        $r4 = r0.<java.io.File: java.lang.String path>;
        $i0 = virtualinvoke $r4.<java.lang.String: int indexOf(int)>(0);
        if $i0 >= 0 goto label1;
        $r5 = <java.io.File$PathStatus: java.io.File$PathStatus CHECKED>;
```



Bytecode

Intermediate Representations

Decompiled Source

JReFrameworker

- ben-holland.com/JReFrameworker
 - Develop and debug attacks in Eclipse
- Allows you to write new source code that...
 - Inserts Logic
 - Replaces Logic
 - Merges Logic
- Targets any platform
 - Write once, exploit anywhere!

Demonstration



Questions?

- Thanks for coming!
- Pizza...yum ©