Java™
EVIL EDITION

Managed Code Rootkits in Java

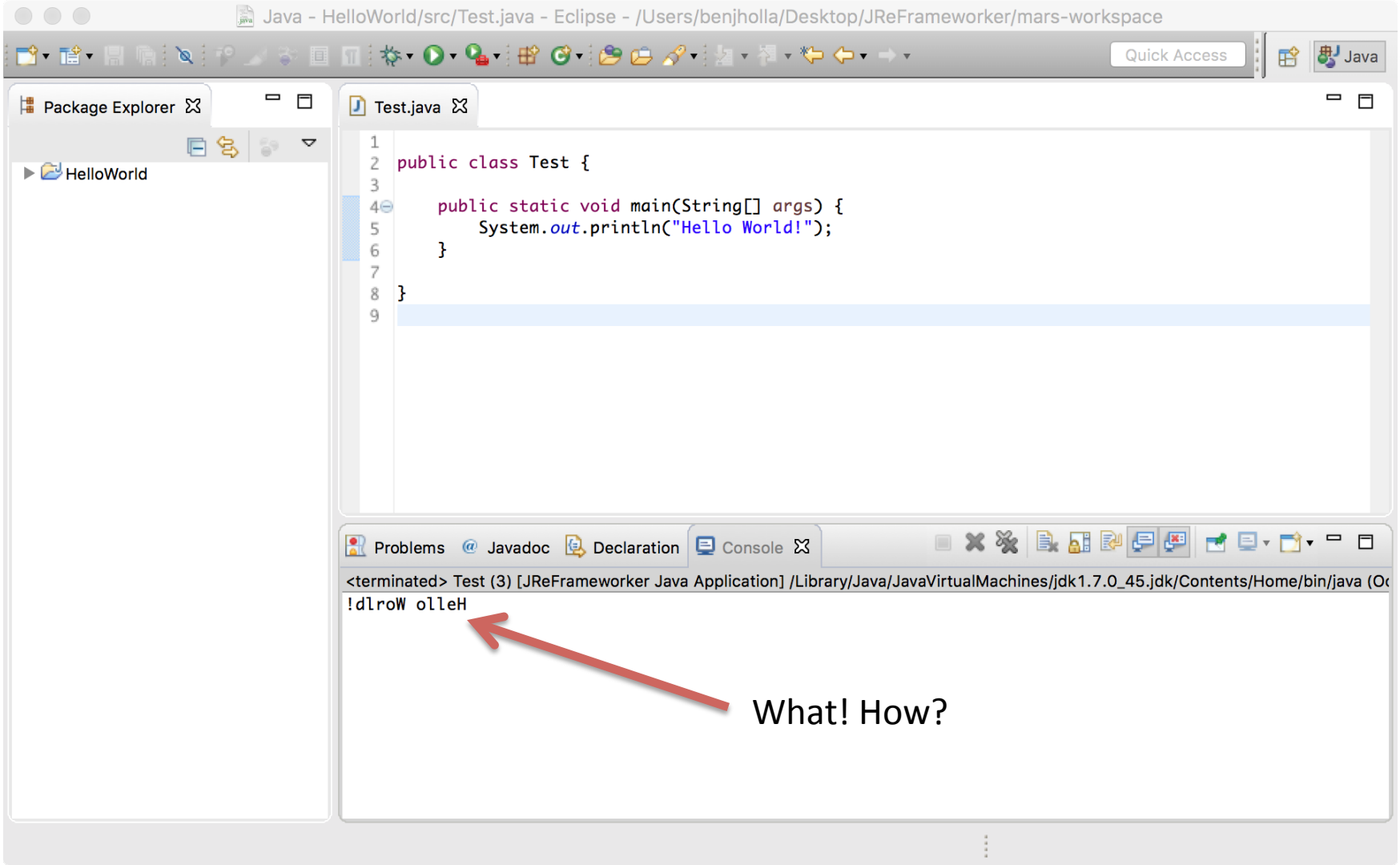
ben-holland.com

Agenda

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

Hello World

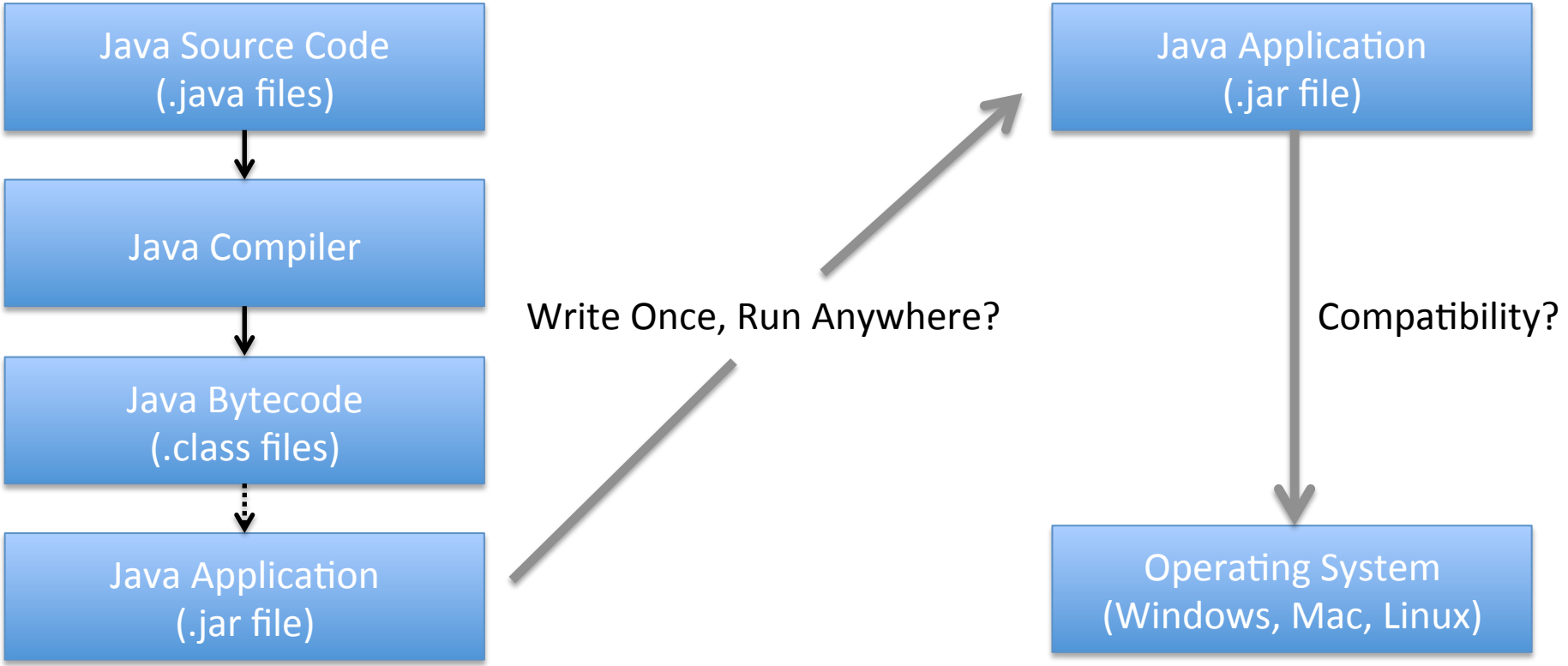
```
1
2 public class Test {
3
4     public static void main(String[] args) {
5         System.out.println("Hello World!");
6     }
7
8 }
9
```


Java - HelloWorld/src/Test.java - Eclipse - /Users/benjholla/Desktop/JReFrameworker/mars-workspace
Quick Access
Java
Package Explorer
HelloWorld
Test.java
1
2 public class Test {
3
4 public static void main(String[] args) {
5 System.out.println("Hello World!");
6 }
7
8 }
9
Problems
Javadoc
Declaration
Console
<terminated> Test (3) [JReFrameworker Java Application] /Library/Java/JavaVirtualMachines/jdk1.7.0_45.jdk/Contents/Home/bin/java (Oc
!dlroW olleH
What! How?

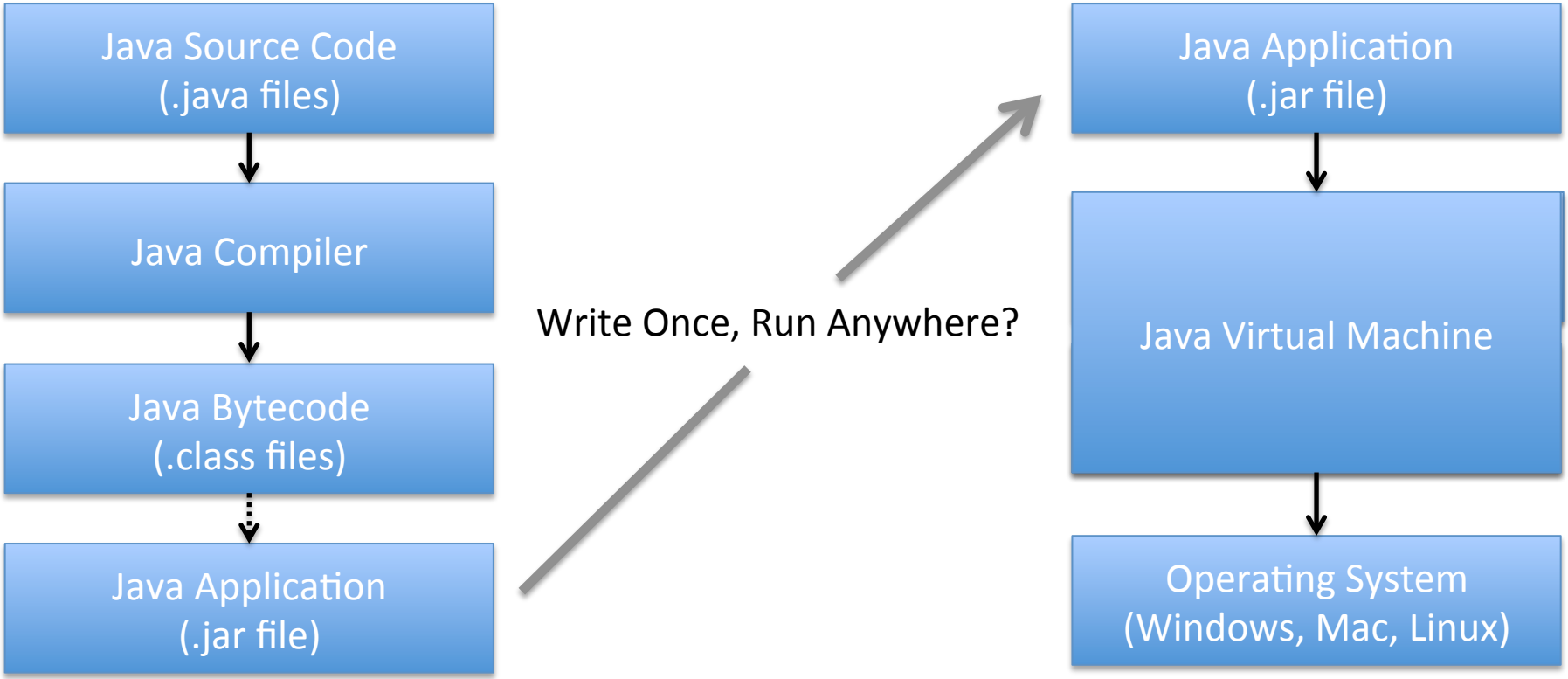
What happened?

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

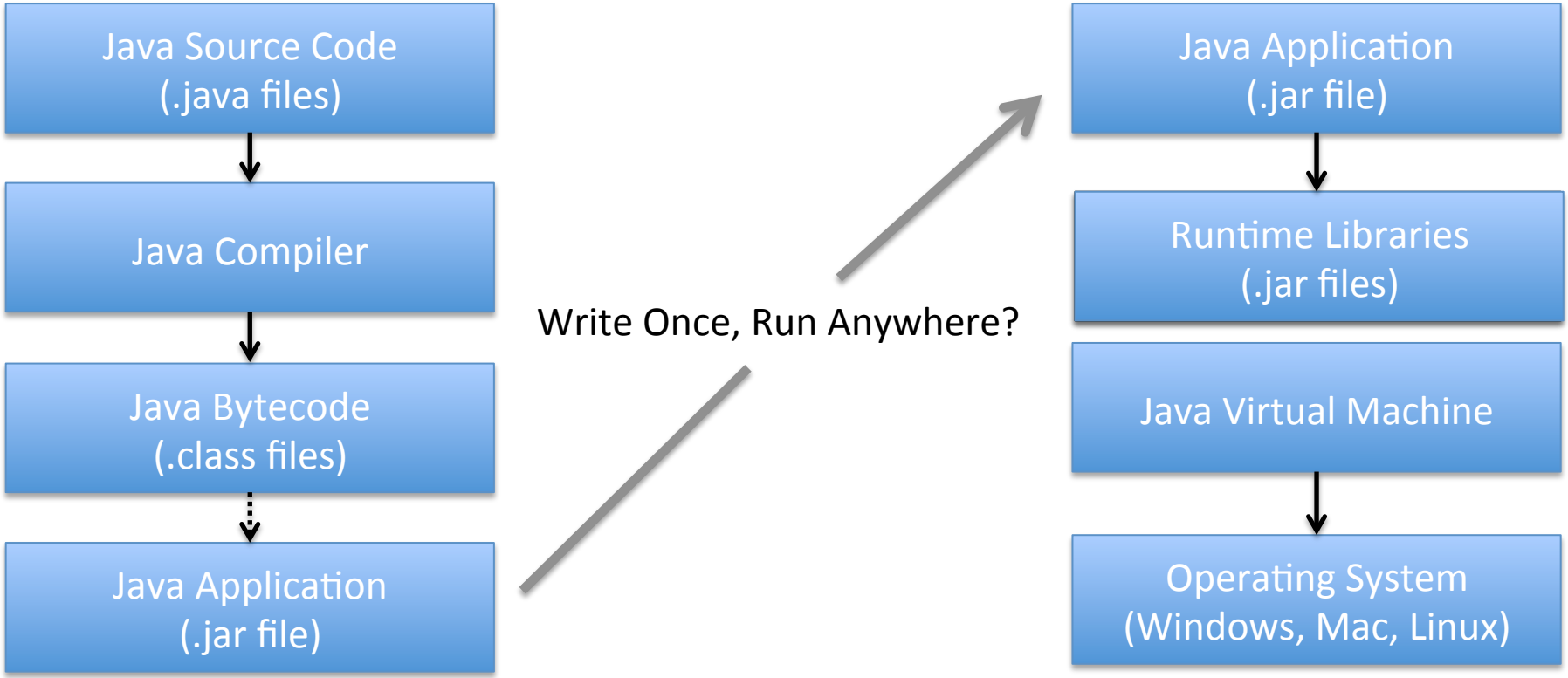
Java Runtime



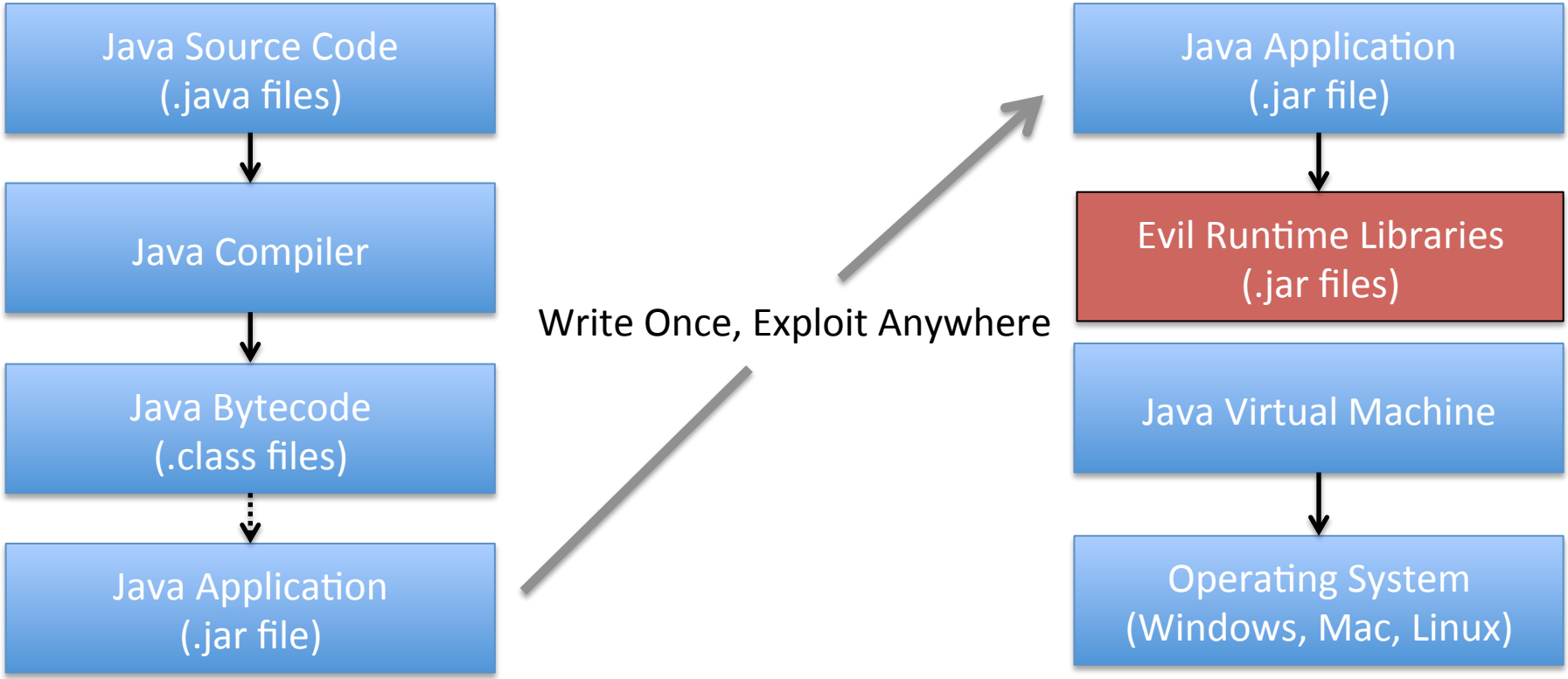
Java Runtime



Java Runtime

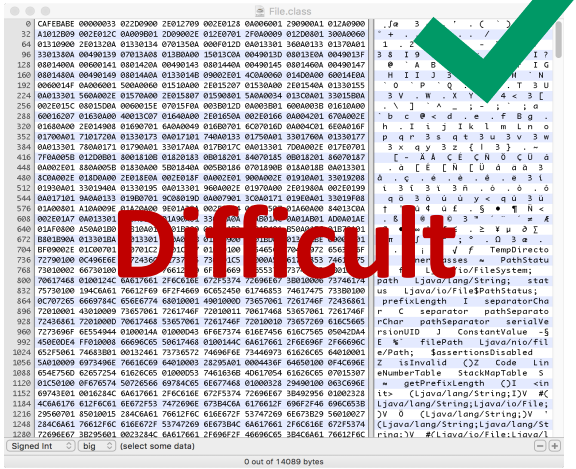


Java Runtime

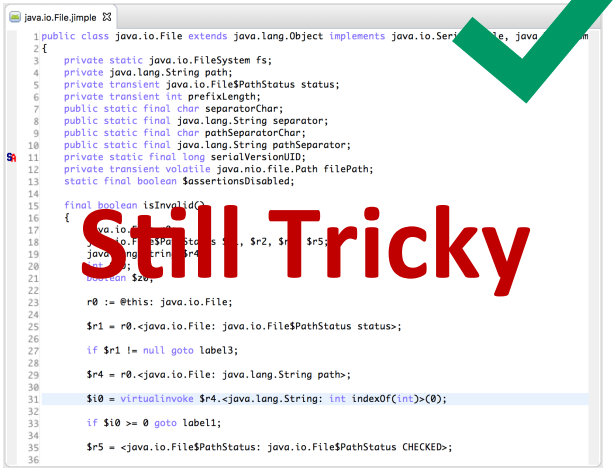


Modifying the Runtime

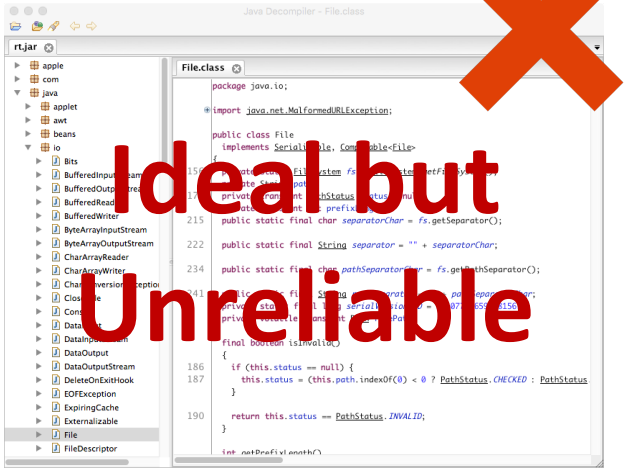
How can modify the runtime for ~~good~~ evil purposes?



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 ☺