



NullSpy

Where did this null come from ?

SCG Bachelor Project

Lina Tran

20.12.2016



```
9 public class Ideone {
10
11     public static List<Integer> numbers;
12     public static BufferedReader reader;
13
14     public static void main(String[] args) {
15         makeReader();
16         readNumbers();
17         closeReader();
18         System.out.println(numbers);
19     }
20
21     private static void makeReader() {
22         try {
23             reader = new BufferedReader(new FileReader(new File("file.txt")));
24         } catch (FileNotFoundException e) {
25             reader = null;
26         }
27     }
28
29     private static List<Integer> readNumbers() {}
30
31     private static void closeReader() {
32         try {
33             reader.close();
34         } catch (IOException e) {
35             e.printStackTrace();
36         }
37     }
38 }
39 }
```



```
9 public class Ideone {  
10  
11     public static List<Integer> numbers;  
12     public static BufferedReader reader;  
13  
14*    public static void main(String[] args) {  
15        makeReader();  
16        readNumbers();  
17        closeReader();  
18        System.out.println(numbers);
```

Exception in thread "main" [java.lang.NullPointerException](#)
at Ideone.closeReader([Ideone.java:44](#))
at Ideone.main([Ideone.java:17](#))

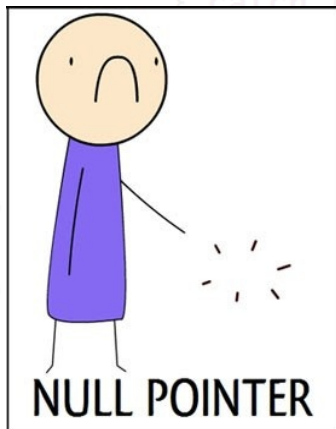
```
24        } catch (FileNotFoundException e) {  
25            reader = null;  
26        }  
27    }  
28  
29*    private static List<Integer> readNumbers() {  
41  
42*    private static void closeReader() {  
43        try {  
44            reader.close();  
45        } catch (IOException e) {  
46            e.printStackTrace();  
47        }  
48    }  
49 }
```



```
9 public class Ideone {
10
11     public static List<Integer> numbers;
12     public static BufferedReader reader;
13
14     public static void main(String[] args) {
15         makeReader();
16         readNumbers();
17         closeReader();
18         System.out.println(numbers);
19     }
20
21     private static void makeReader() {
22         try {
23             reader = new BufferedReader(new FileReader(new File("file.txt")));
24         } catch (FileNotFoundException e) {
25             reader = null;
26         }
27     }
28
29     private static List<Integer> readNumbers() {}
30
31     private static void closeReader() {
32         try {
33             reader.close();
34         } catch (IOException e) {
35             e.printStackTrace();
36         }
37     }
38 }
39 }
```

Where is the variable

reader



assigned null ?



```
9 public class Ideone {
10
11     public static List<Integer> numbers;
12     public static BufferedReader reader;
13
14     public static void main(String[] args) {
15         makeReader();
16         readNumbers();
17         closeReader();
18         System.out.println(numbers);
19     }
20
21     private static void makeReader() {
22         try {
23             reader = new BufferedReader(new FileReader(new File("file.txt")));
24         } catch (FileNotFoundException e) {
25             reader = null;
26         }
27     }
28
29     private static List<Integer> readNumbers() {
30
31     }
32
33     private static void closeReader() {
34         try {
35             reader.close();
36         } catch (IOException e) {
37             e.printStackTrace();
38         }
39     }
40
41 }
42 }
```

NullSpy



```
9 public class Ideone {
10
11     public static List<Integer> numbers;
12     public static BufferedReader reader;
13
14     public static void main(String[] args) {
15         makeReader();
16         readNumbers();
17         closeReader();
```

Field this.reader at line 25 is null: ([Ideone.java:25](#))

Exception in thread "main" [java.lang.NullPointerException](#)
at Ideone.closeReader([Ideone.java:44](#))
at Ideone.main([Ideone.java:17](#))

```
25         reader = null;
26     }
27 }
28
29     private static List<Integer> readNumbers() {
41
42     private static void closeReader() {
43         try {
44             reader.close();
45         } catch (IOException e) {
46             e.printStackTrace();
47         }
48     }
49 }
```

```
9 public class Ideone {
10
11     public static List<Integer> numbers;
12     public static BufferedReader reader;
13
14     public static void main(String[] args) {
15         makeReader();
16         readNumbers();
17         closeReader();
18         System.out.println(numbers);
19     }
20
21     private static void makeReader() {
22         try {
23             reader = new BufferedReader(new FileReader(new File("file.txt")));
24         } catch (FileNotFoundException e) {
25             reader = null;
26         }
27     }
28
29     private static List<Integer> readNumbers() {}
30
31     private static void closeReader() {
32         try {
33             reader.close();
34         } catch (IOException e) {
35             e.printStackTrace();
36         }
37     }
38 }
39 }
```



- Bytecode
- High level overview
- Process flow
- Validation
- Demo





■ Bytecode

- High level overview
- Process flow
- Validation
- Demo



```
4 public void say() {  
5     String result = hello;  
6     System.out.println(result);  
7 }
```

public void say();

```
0  aload_0 [this]  
1  getfield HelloWorld.hello : java.lang.String [14]  
4  astore_1 [result]  
5  getstatic java.lang.System.out : java.io.PrintStream [21]  
8  aload_1 [result]  
9  invokevirtual java.io.PrintStream.println(java.lang.String) :  
   void [27]  
12 return
```

Line numbers:

```
[pc: 0, line: 5]  
[pc: 5, line: 6]  
[pc: 12, line: 7]
```

Local variable table:

```
[pc: 0, pc: 13] local: this index: 0 type: HelloWorld  
[pc: 5, pc: 13] local: result index: 1 type: java.lang.  
String
```



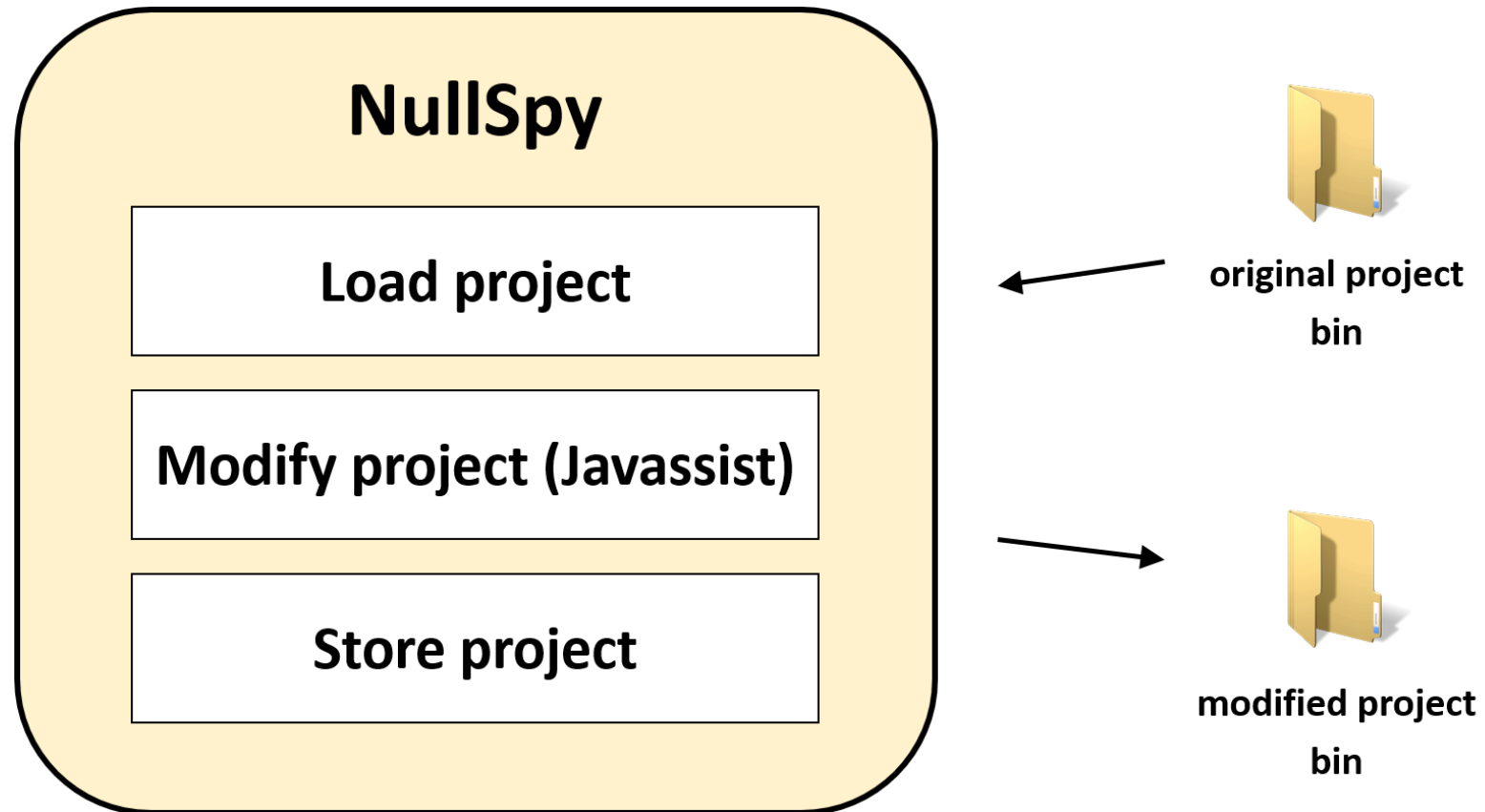
- Bytecode
- **High level overview**

- Process flow
- Validation
- Demo





High level overview



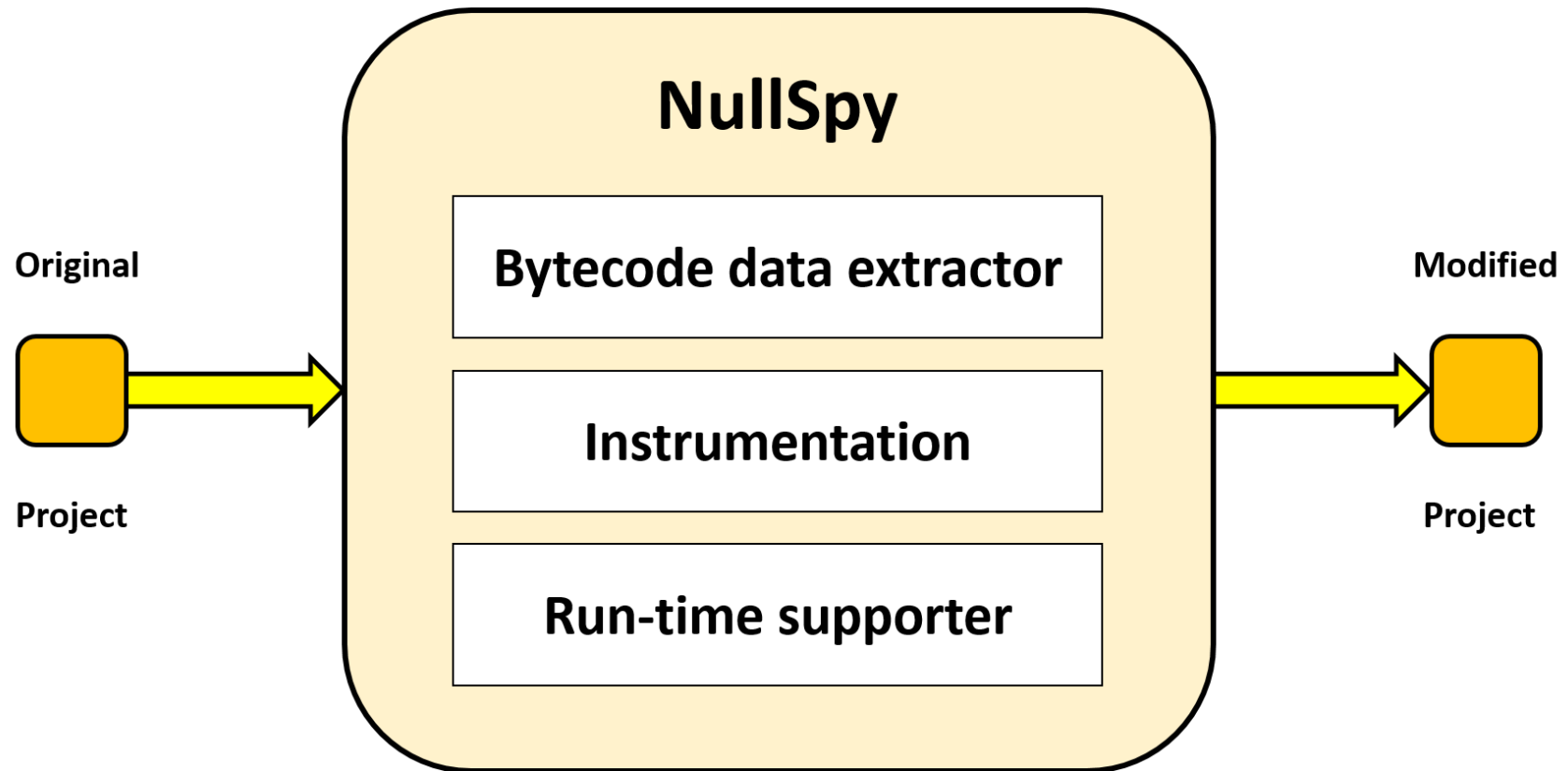


- Bytecode
- High level overview
- **Process flow**
- Validation
- Demo





Process flow





1. Extract information about

1. Target variable
2. Variable assignment

2. Instrumentation

1. Variable assignment
2. Wrap «Main()» method with *try-catch-block*

3. Add run-time supporter package



“Target variable”

```
public class DrawApplication {  
  
    private ToolButton fToolButton;  
  
    protected void open(final DrawingView newDrawingView) {  
        ...  
        fToolButton.tool();           // field access  
        fToolButton.myIcon.toString(); // field access  
  
        JPanel activePanel = ...;  
        activePanel.add((Component) getDesktop(), BorderLayout.CENTER);  
        // local variable as a target variable  
        ...  
    }  
}
```



- **Insert our bytecode after each variable assignment**

```
JPanel activePanel = ...;  
activePanel.add( (Component) getDesktop(), BorderLayout.CENTER);  
    DrawApplication", "open", "(Lorg/jhotdraw/framework/  
    DrawingView;)V", "localVariable_3", "activePanel", "Ljavax/  
    swing/JPanel;", activePanel, 3, 254, 136, 143, 144);  
activePanel.add( (Component) getDesktop(), BorderLayout.CENTER);
```



- **Catch-block of «Main()» method:**
 - Extract information from NPE stack trace
 - Identifier comparisons
 - Adds direct “link” to null assignment of NPE culprit variable

Field this.reader at line 25 is null: ([Ideone.java:25](#))

Exception in thread "main" [java.lang.NullPointerException](#)
at Ideone.closeReader([Ideone.java:44](#))
at Ideone.main([Ideone.java:17](#))



- Bytecode
- High level overview
- Process flow
- **Validation**
- Demo



- **JHotDraw**
 - GUI framework for technical and structured Graphics
- **Execution time difference**
 - JHotDraw tests
 - Time: ~7.20s → ~7.57s

~5%



- Bytecode
- High level overview
- Process flow
- Validation
- **Demo**



Summarize

1. Load original class files



Original class files

2. Extract information about

1. Target variable
2. Variable assignment

```
public void say() {
  0  aload 0 [this]
  1  getfield HelloWorld.hello : java.lang.String [14]
  4  astore_1 [result]
  5  getstatic java.lang.System.out : java.io.PrintStream [21]
  8  aload 1 [result]
  9  invokevirtual java.io.PrintStream.println(java.lang.String) :
    void [27]
  12 return
  Line numbers:
    [pc: 0, line: 5]
    [pc: 5, line: 6]
    [pc: 12, line: 7]
  Local variable table:
    [pc: 0, pc: 13] local: this index: 0 type: HelloWorld
    [pc: 5, pc: 13] local: result index: 1 type: java.lang.
      String
}
```

3. Instrumentation

1. Variable assignment
2. Wrap «Main()» method with *try-catch-block*

```
JPanel activePanel = ...;
activePanel.add((Component) getDesktop(), BorderLayout.CENTER);
DrawApplication", "open", "(Lorg/jhotdraw/framework/
DrawingView;)V", "localVariable_3", "activePanel", "Ljavaw/
swing/JPanel;", activePanel, 3, 254, 136, 143, 144);
activePanel.add((Component) getDesktop(), BorderLayout.CENTER);
```

Javassist

4. Add run-time supporter package



Run-time supporter

5. Store modified class files



Modified class files

Field this.reader at line 25 is null: ([Ideone.java:25](#))

Exception in thread "main" [java.lang.NullPointerException](#)
at Ideone.closeReader([Ideone.java:44](#))
at Ideone.main([Ideone.java:17](#))