BString:
A String-based Framework to Improve Application Security

MSc Thesis
(final presentation)

19 January 2022

Christian Zürcher

Two major problems of our time

Data leaks

Remote Code Execution (RCE)

Important:

These threats usually originate from String values.

Two major problems of our time

https://owasp.org/www-project-top-ten/

Security measures for strings already exist…

Restrictive data types

Data encryption

Taint and data flow analyses

…, but they lack fundamental features

- limited interoperability between different tools
- no shared configuration
- no standardized set up
- limited automation

Our idea: a generalizable security framework for String

Step 1: ***Improving*** the String class of OpenJDK

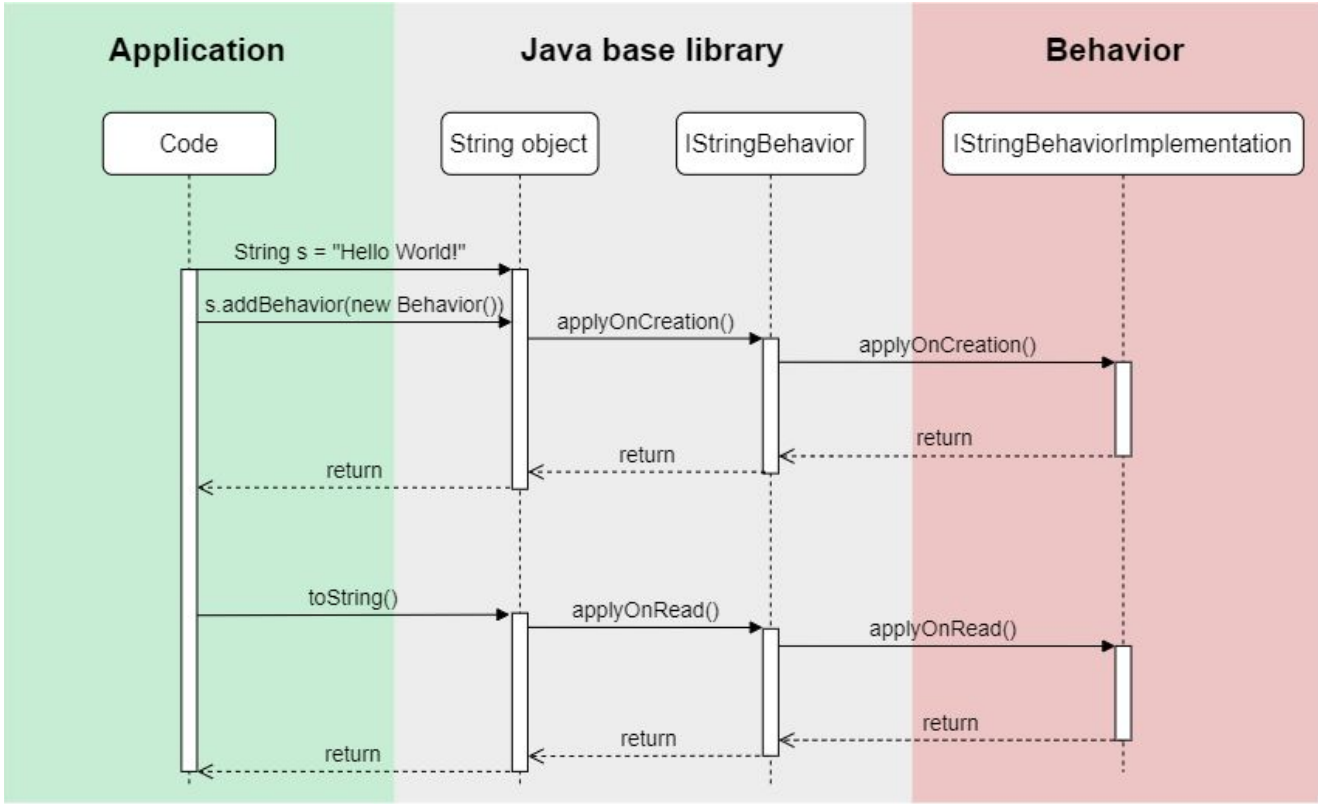
Step 2: ***Compiling*** the modified JDK/JRE

Step 3: ***Using*** the additional functionality without sacrificing any compatibility

Provided API

```
public interface IStringBehavior {

    public String applyOnCreation(String s);

    public String applyOnRead(String s);

    public boolean attachToChild();

    public boolean recordHistory();

    …

}
```

Behind the scenes



Challenges

Don’t break the system:

- String is used throughout the Java VM
- Changes must not alter the existing behavior
- Recursions are very easy to introduce

Native code complications:

- The string pooling uses native code
- Translation between different data types

RQ1:

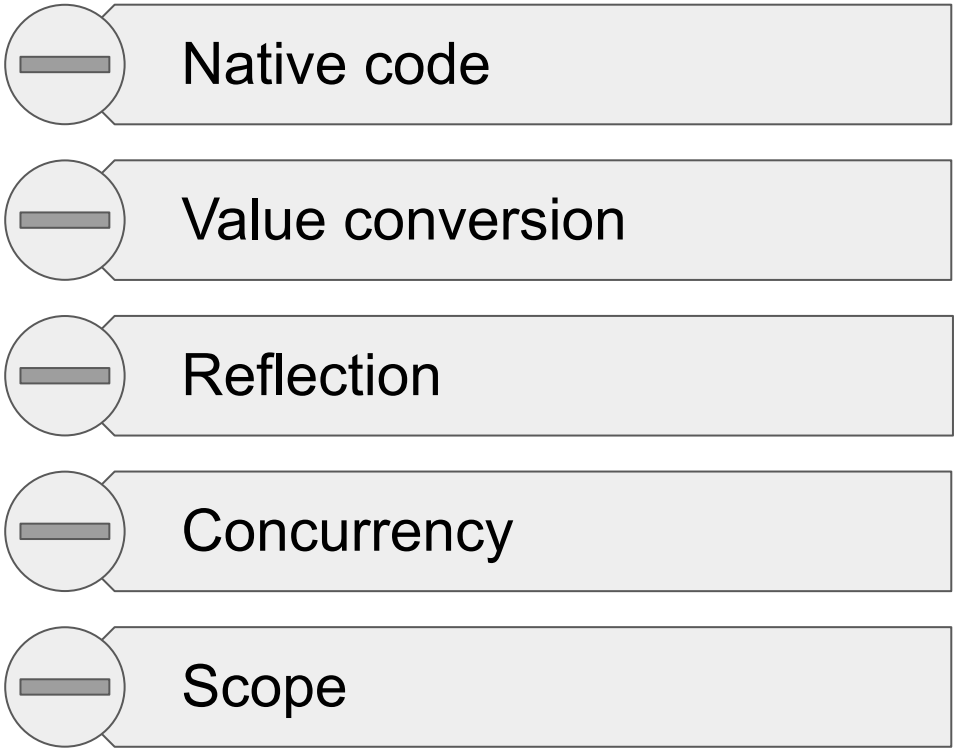
What are the restrictions when used with existing Java code?

Compatibility

Project Name	Package	Version	Compatible?
Apache Comons (IO)	Commons-io	2.8.0	✓
Apache Commons (Logging)	Commons-logging	1.2	✓
Apache HttpClient	Org.apache.httpcomponents	4.5.13	✓
Gson	Com.google.code.gson	2.8.5	× (reflection)
JavaMail	Com.sun.mail	1.6.0	✓
Log4J (core)	Org.apache.logging.log4j	2.14.1	✓
Logback (classic)	Ch.qos.logback	1.3.0-alpha5	✓
SLF4J	Slf4j-simple	2.0.0-alpha1	× (custom byte buffer)
SLF4J (API)	Org.slf4j	2.0.0-alpha1	✓
Spring	Org.springframework	5.3.6	✓
Square Okhttp	Com.squareup.okhttp3	5.0.0-alpha.2	✓
Square Okio	Com.squareup.okhokio	2.10.0	✓
Square Retrofit	Com.squareup.okhretrofit	2.9.0	✓

Table 4.1: Evaluation of popular Java libraries

Restrictions



RQ2:

What are the security gains and threats?

Security gains


Date type emulation

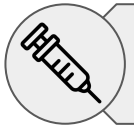

In-memory encryption


Off-memory encryption


Taint analysis


Data flow analysis

Security threats



String or application hijacking

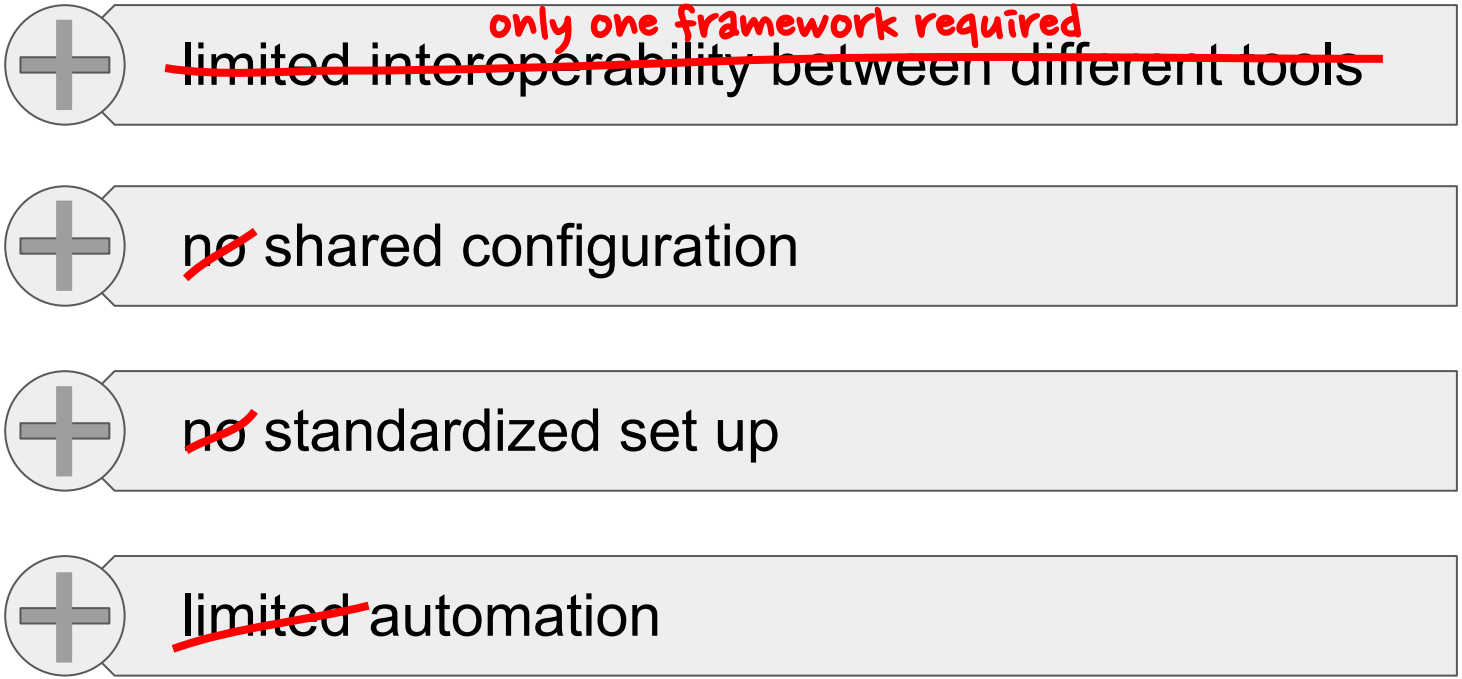
Developer confusion

Performance evaluation

[milliseconds]	String initialization	Read value	Attaching behavior to new String
baseline	4	166	11
without behavior	13	171	20
with empty behavior	16	193	22
with behavior attachment	16	191	32
with history	59	213	87
with encryption on read in IO	2,388	9,331	19
with encryption and decryption	5,112	7,982	timeout

DEMO

Conclusion


only one framework required
limited interoperability between different tools
no shared configuration
no standardized set up
limited automation

Summary

Two major problems of our time

Data leaks

Remote Code Execution (RCE)

Important:
These threats usually originate from String values.

2

Provided API

```
public interface IStringBehavior {

    public String applyOnCreation(String s);

    public boolean applyOnRead(String s);

    public boolean inheritToChild();

    public boolean recordHistory();

    …

}
```

7

Compatibility

Project Name	Package	Version	Compatible?
Apache Comons (IO)	Commons-io	2.8.0	✓
Apache Commons (Logging)	Commons-logging	1.2	✓
Apache HttpClient	Org.apache.httpcomponents	4.5.13	✓
Gson	Com.google.code.gson	2.8.5	× (reflection)
JavaMail	Com.sun.mail	1.6.0	✓
Log4J (core)	Org.apache.logging.log4j	2.14.1	✓
Logback (classic)	Ch.qos.logback	1.3.0-alpha5	✓
SLF4J	Slf4j-simple	2.0.0-alpha1	× (custom byte buffer)
SLF4J (API)	Org.slf4j	2.0.0-alpha1	✓
Spring	Org.springframework	5.3.6	✓
Square Okhttp	Com.squareup.okhttp3	5.0.0-alpha.2	✓
Square Okio	Com.squareup.okhokio	2.10.0	✓
Square Retrofit	Com.squareup.okhretrofit	2.9.0	✓

Table 4.1: Evaluation of popular Java libraries

11

Security gains

- Date type emulation
- In-memory encryption
- Off-memory encryption
- Taint analysis
- Data flow analysis

14