Improve Your Software Quality Using Optional Type Systems

https://eisop.github.io/

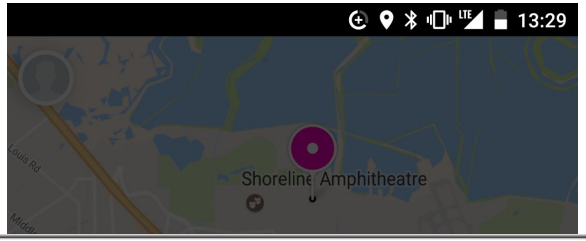
Live demo: http://eisop.uwaterloo.ca/live/

Werner Dietl, University of Waterloo

https://ece.uwaterloo.ca/~wdietl/

UNIVERSITY OF WATERLOO

Motivation



TREND MICRO InterScan™ Web Security Virtual Appliance

Log Off | --------Help---

Search

- System Status
- Dashboard
- + Application Control
- − HTTP
  - + HTTPS Decryption
  - + Advanced Threat Protection
  - + HTTP Inspection
  - + Data Loss Prevention
  - + Applets and ActiveX
  - − URL Filtering
    - Policies
    - Settings
- Reports
- + Updates
- Notifications
- + Administration

HTTP Status 500 - java.lang.NullPointerException

type Exception report

message java.lang.NullPointerException

description The server encountered an internal error that prevented it from fulfilling this request.

exception

```
org.apache.jasper.JasperException: java.lang.NullPointerException
        org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:432)
        org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
        org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
```

ter.java:73)
77)

java.lang.NullPointerException

```
        org.apache.jsp.urlf_005fsection_005fpolicy_005frule_jsp._jspService(urlf_005fsection_005fpolicy_005frule_jsp.java:742)
        org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
        org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:388)
        org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
        org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
        com.trend.iwss.servlets.filters.CSRFGuardFilter.doFilter(CSRFGuardFilter.java:73)
        com.trend.iwss.servlets.filters.AuthFilter.doFilter(AuthFilter.java:377)
```

java.lang.NullPointerException

Cost of software failures

$312 billion per year global cost of software bugs (2013)

$300 billion dealing with the Y2K problem

$440 million loss by Knight Capital Group Inc. in 30 minutes in August 2012

$650 million loss by NASA Mars missions in 1999; unit conversion bug

$500 million Ariane 5 maiden flight in 1996; 64-bit to 16-bit conversion bug

Software bugs can cost lives

1985-2000: **>8 deaths**: Radiation therapy
1991: **28 deaths**: Patriot missile guidance system
1997: **225 deaths**: jet crash caused by radar software
2003: **11 deaths**: blackout

2011: Software caused 25% of all medical device recalls

Java's type system is too weak

Type checking prevents many errors

```
int i = "hello";
```

Type checking doesn't prevent enough errors

```
System.console().readLine();
```

```
Collections.emptyList().add("one");
```


Java's type system is too weak

Type checking prevents many errors

```
int i = "hello";
```

Type checking doesn't prevent enough errors

NullPointerException

```
System.console().readLine();
```

```
Collections.emptyList().add("one");
```


Java's type system is too weak

Type checking prevents many errors

```
int i = "hello";
```

Type checking doesn't prevent enough errors

```
System
Collections.emptyList().add("one");
```

UnsupportedOperationException

Some errors are silent

```
Date date = new Date();
myMap.put(date, "now");
…
date.setSeconds(0);   // round to minute
…
myMap.get(date);
```


Some errors are silent

```
Date date = new Date();
myMap.put(date, "now");
…
date.setSeconds(0);   // round to minute
…
myMap.get(date);
```

Corrupted map

Some errors are silent

```
dbStatement.executeQuery(userInput);
```


Some errors are silent

```
dbStatement.executeQuery(userInput);
```

SQL injection attack

Initialization, data formatting, equality tests, …

Solution: Optional Type Checking

1. Design a type system to solve a specific problem
2. Write type qualifiers in code (or, use type inference)

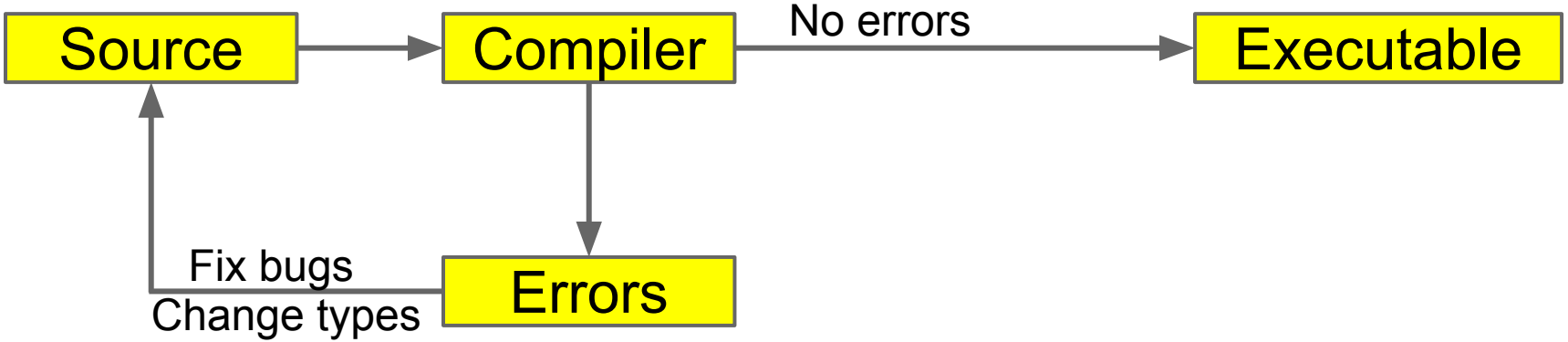
```
void foo (@Nullable Date date) {
  date.setSeconds(0); // compile-time error
```

3. Type checker warns about violations (bugs)

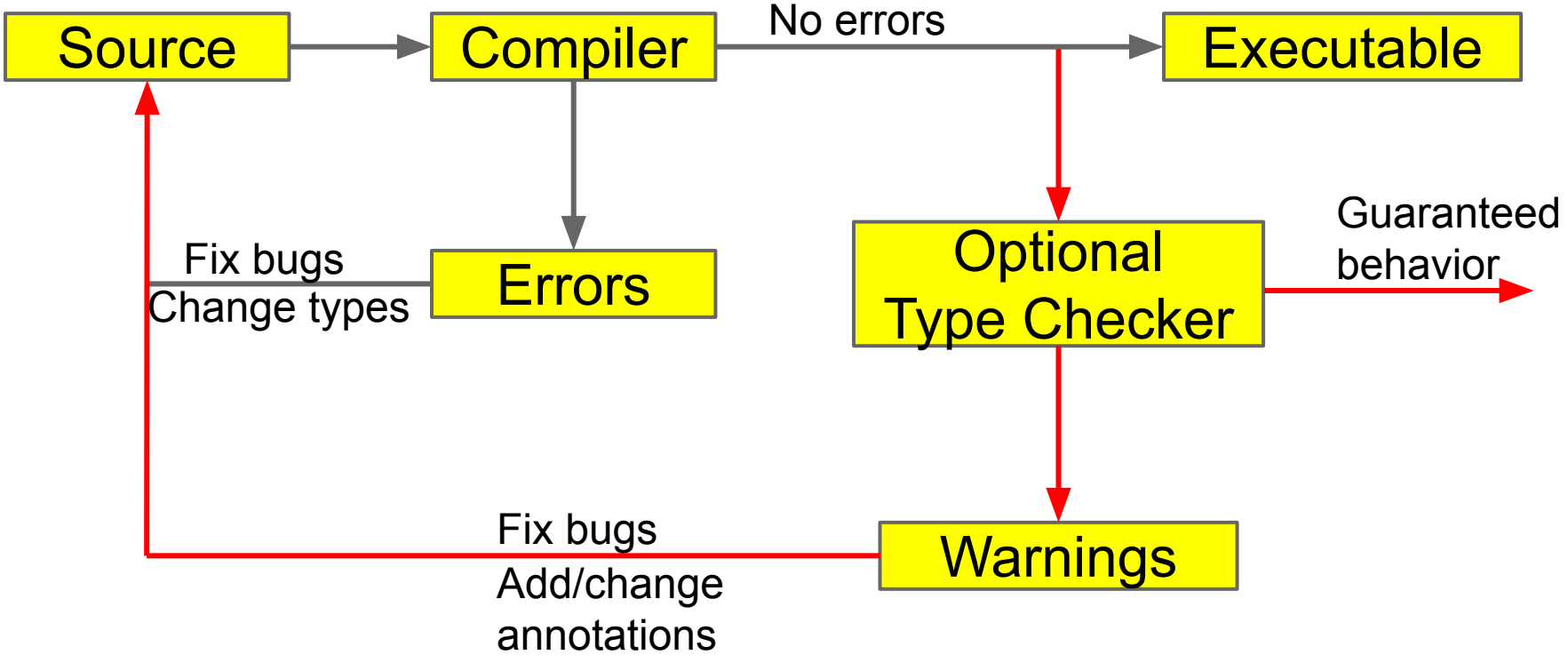
```
% javac -processor NullnessChecker MyFile.java

MyFile.java:149: dereference of possibly-null reference bb2
      allVars = bb2.vars;
                ^
```

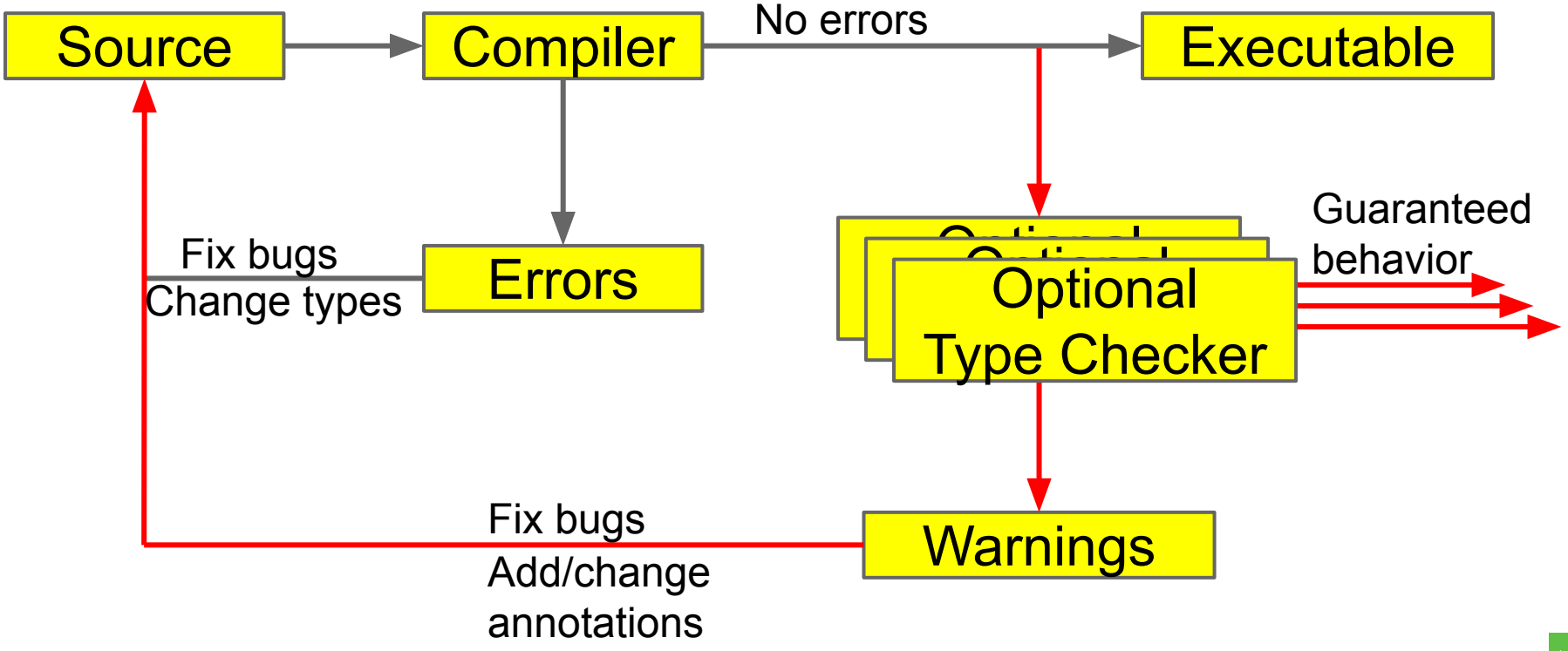

Type Checking



Optional Type Checking



Optional Type Checking



The Checker Framework

A framework for pluggable type checkers

“Plugs” into the OpenJDK or OracleJDK compiler

```
javac -processor MyChecker ...
```

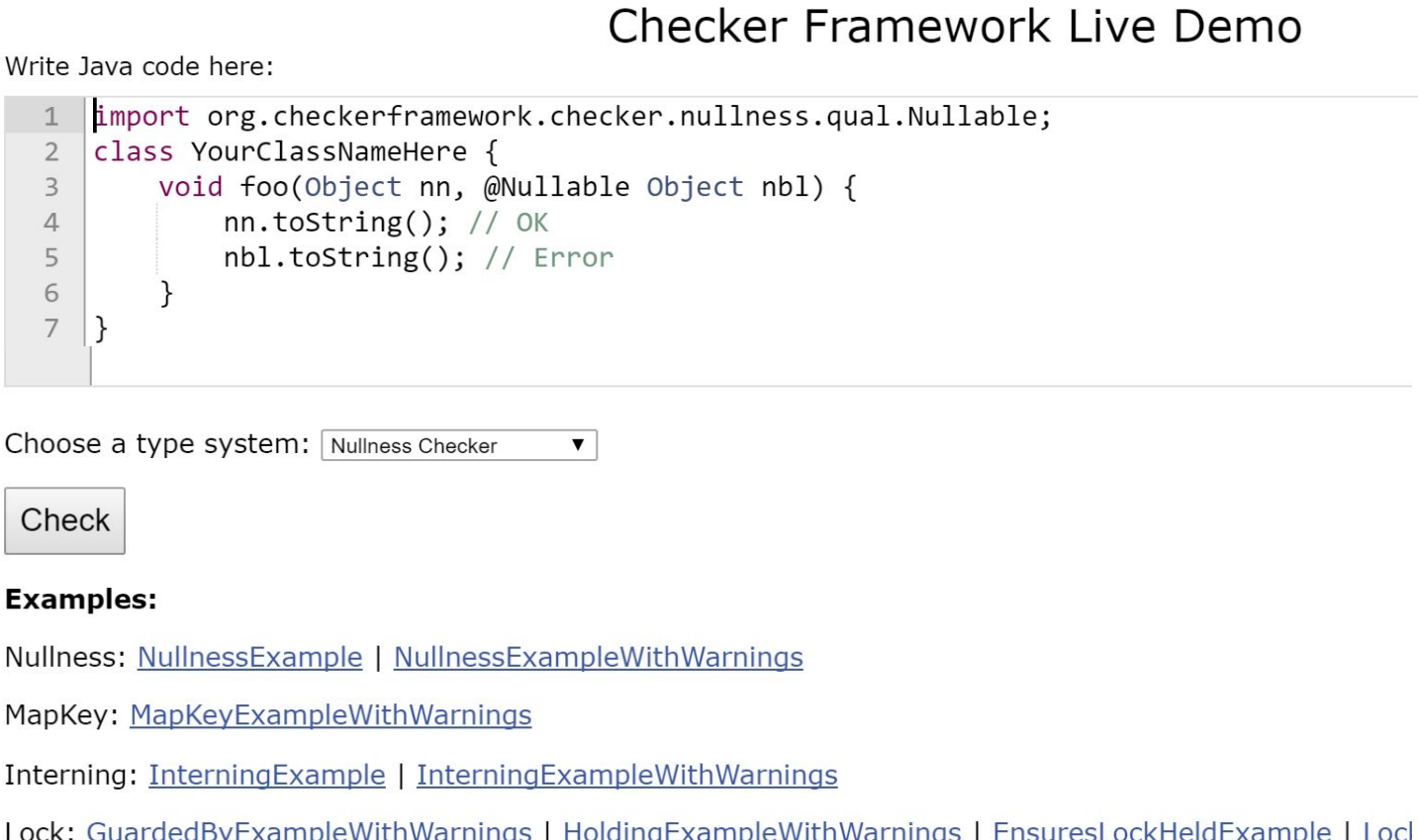
Standard error format allows tool integration

Ant, Maven, Gradle integration

```
<presetdef name="jsr308.javac">
  <javac fork="yes"
    executable="${checkerframework}/checker/bin/${cfJavac}" >
    <!-- JSR-308-related compiler arguments -->
    <compilerarg value="-version"/>
    <compilerarg value="-implicit:class"/>
  </javac>
</presetdef>
```

```
<dependencies>
  ... existing <dependency> items ...
  <!-- annotations from the Checker Framework:
          nullness, interning, locking, ... -->
    <dependency>
      <groupId>io.github.eisop</groupId>
      <artifactId>checker-qual</artifactId>
      <version>3.34.0-eisop1</version>
    </dependency>
</dependencies>
```

Live demo: http://eisop.uwaterloo.ca/live/



Prevent null pointer exceptions

Java 8 introduces the `Optional<T>` type

- Wrapper; content may be *present* or *absent*
- Constructor: `of(T value)`
- Methods: `boolean isPresent()`, `T get()`

```
Optional<String> maidenName;
```


`Optional` reminds you to check

Without `Optional`:

```
String mName;
mName.equals(...);

if (mName != null) {
    mName.equals(...);
}
```

possible NullPointerException

With `Optional`:

```
Optional<String> omName;
omName.get().equals(...);

if (omName.isPresent()) {
    omName.get().equals(...);
}
```

possible NoSuchElementException

possible NullPointerException

Complex rules for using `Optional` correctly!

How not to use Optional

Other gu
Stephen
Dalorzo,
Brian Go
Olszewsl
Oleg She

Stuart Marks's rules:

1. Never, ever, use null for an Optional variable or return value.
2. Never use Optional.get() unless you can prove that the Optional is present.
3. Prefer alternative APIs over Optional.isPresent() and Optional.get().
4. It's generally nal for the specific purpose of chaining met
5. If an Optiona chain, or has an intermediate result of Opt ex.
6. Avoid using Optional in fields, method parameters, and collections.
7. Don't use an Optional to wrap any collection type (List, Set, Map). Instead, use an empty collection to represent the absence of values.

Let's enforce the rules with a tool.

Which rules to enforce with a tool

Stuart Marks's rules:

1. **Never**, ever, use null for an Optional variable or return value.
2. **Never** use Optional.get() unless you can prove that the Optional is present.
3. *Prefer* alternative APIs over Optional.isPresent() and Optional.get().
4. It's *generally a bad idea* to create an Optional for the specific purpose of chaining methods from it to get a value.
5. If an Optional chain has a nested Optional chain, or has an intermediate result of Optional, it's *probably too complex*.
6. *Avoid* using Optional in fields, method parameters, and collections.
7. **Don't** use an Optional to wrap any collection type (List, Set, Map). Instead, use an empty collection to represent the absence of values.

Which rules to enforce with a tool

Stuart Marks's rules:

1. **Never**, ever, use null for an Optional variable or return value.
2. **Never** use Optional.get() unless you can prove that the Optional is present.
3. *Prefer* alternative APIs over Optional.isPresent() and Optional.get().
4. It's *generally* ... specific purpose of chaining met...
5. If an Optiona... as an intermediate result of Opt...
6. *Avoid* using Optional in fields, method parameters, and collections.
7. **Don't** use an Optional to wrap any collection type (List, Set, Map). Instead, use an empty collection to represent the absence of values.

These are *type system* properties.

Define a type system

$$
\begin{array}{rcll}
\mathtt{h} & \in & \mathtt{Heap} & = \mathtt{Addr} \rightarrow \mathtt{Obj} \\
\iota & \in & \mathtt{Addr} & = \text{Set of Addresses} \cup \{\mathtt{null}_a\} \\
\mathtt{o} & \in & \mathtt{Obj} & = {}^{\mathtt{r}}\mathtt{Type},\ \mathtt{Fields} \\
{}^{\mathtt{r}}\mathtt{T} & \in & {}^{\mathtt{r}}\mathtt{Type} & = \mathtt{OwnerAddr}\ \mathtt{ClassId}\langle\overline{{}^{\mathtt{r}}\mathtt{Type}}\rangle \\
\mathtt{Fs} & \in & \mathtt{Fields} & = \mathtt{FieldId} \rightarrow \mathtt{Addr} \\
\iota & \in & \mathtt{OwnerAddr} & = \mathtt{Addr} \cup \{\mathtt{any}_a\} \\
{}^{\mathtt{r}}\Gamma & \in & {}^{\mathtt{r}}\mathtt{Env} & = \overline{\mathtt{TVarId}\ {}^{\mathtt{r}}\mathtt{Type}};\ \overline{\mathtt{ParId}\ \mathtt{Addr}}
\end{array}
$$

$$
\begin{array}{rcll}
\mathtt{P} & \in & \mathtt{Program} & ::= \overline{\mathtt{Class}}, \mathtt{ClassId}, \mathtt{Expr} \\
\mathtt{Cls} & \in & \mathtt{Class} & ::= \mathtt{class}\ \mathtt{ClassId}\langle\overline{\mathtt{TVarI}}\rangle \\
 & & & \mathtt{extends}\ \mathtt{ClassId}\langle\overline{{}^{\mathtt{s}}\mathtt{Ty}}\rangle \\
 & & & \{\ \overline{\mathtt{FieldId}\ {}^{\mathtt{s}}\mathtt{Type}};\ \overline{\mathtt{Met}} \\
{}^{\mathtt{s}}\mathtt{T} & \in & {}^{\mathtt{s}}\mathtt{Type} & ::= {}^{\mathtt{s}}\mathtt{NType} \mid \mathtt{TVarId} \\
{}^{\mathtt{s}}\mathtt{N} & \in & {}^{\mathtt{s}}\mathtt{NType} & ::= \mathtt{OM}\ \mathtt{ClassId}\langle\overline{{}^{\mathtt{s}}\mathtt{Type}}\rangle \\
\mathtt{u} & \in & \mathtt{OM} & ::= \\
\mathtt{mt} & \in & \mathtt{Meth} & ::= \\
 & & \mathtt{MethSig} & ::= \\
\mathtt{w} & \in & \mathtt{Purity} & ::= \\
\mathtt{e} & \in & \mathtt{Expr} & ::= \\
 & & & \mathtt{Expr.MethId}\langle{}^{\mathtt{s}}\mathtt{Type}\rangle(\mathtt{Expr}) \mid \\
 & & & \mathtt{new}\ {}^{\mathtt{s}}\mathtt{Type} \mid ({}^{\mathtt{s}}\mathtt{Type})\ \mathtt{Expr} \\
 & & & \overline{\mathtt{TVarId}\ {}^{\mathtt{s}}\mathtt{NType}};\ \overline{\mathtt{ParId}\ {}^{\mathtt{s}}\mathtt{Type}} \\
{}^{\mathtt{s}}\Gamma & \in & {}^{\mathtt{s}}\mathtt{Env} & ::= \overline{\mathtt{TVarId}\ {}^{\mathtt{s}}\mathtt{NType}};\ \overline{\mathtt{ParId}\ {}^{\mathtt{s}}\mathtt{Type}}
\end{array}
$$

$$\text{OS-Upd}\ \frac{\mathtt{h}, {}^{\mathtt{r}}\Gamma, \mathtt{e}_0 \rightsquigarrow \mathtt{h}_0, \iota_0 \quad \iota_0 \neq \mathtt{null}_a \quad \mathtt{h}_0, {}^{\mathtt{r}}\Gamma, \mathtt{e}_2 \rightsquigarrow \mathtt{h}_2, \iota \quad \mathtt{h}' = \mathtt{h}_2[\iota_0.\mathtt{f} := \iota]}{\mathtt{h}, {}^{\mathtt{r}}\Gamma, \mathtt{e}_0.\mathtt{f} = \mathtt{e}_2 \rightsquigarrow \mathtt{h}',}$$

$$\text{OS-Read}\ \frac{\mathtt{h}, {}^{\mathtt{r}}\Gamma, \mathtt{e}_0 \rightsquigarrow \mathtt{h}', \iota_0 \quad \iota_0 \neq \mathtt{null}_a \quad \iota = \mathtt{h}'(\iota_0)\downarrow_2(\mathtt{f})}{\mathtt{h}, {}^{\mathtt{r}}\Gamma, \mathtt{e}_0.\mathtt{f} \rightsquigarrow \mathtt{h}', \iota}$$

$$\text{GT-Read}\ \frac{\Gamma \vdash \mathtt{e}_0 : \mathtt{N}_0 \quad \mathtt{N}_0 = \_\ \langle \quad \ldots}{\Gamma \vdash \mathtt{e}_0.\mathtt{f} : \mathtt{N}_0 \rhd fType(\mathtt{C}_0, \mathtt{f})}$$

$$\text{GT-Upd}\ \frac{\Gamma \vdash \mathtt{e}_0 : \mathtt{N}_0 \quad \mathtt{N}_0 = \mathtt{u}_0\ \mathtt{C}_0\langle\_\rangle \quad \mathtt{T}_1 = fType(\mathtt{C}_0, \mathtt{f}) \quad \Gamma \vdash \mathtt{e}_2 : \mathtt{N}_0 \rhd \mathtt{T}_1 \quad \mathtt{u}_0 \neq \mathtt{any} \quad rp(\mathtt{u}_0, \mathtt{T}_1)}{\Gamma \vdash \mathtt{e}_0.\mathtt{f} = \mathtt{e}_2 : \mathtt{N}_0 \rhd \mathtt{T}_1}$$

$$\text{DYN}\ \frac{\begin{array}{l}\mathtt{h} \vdash {}^{\mathtt{r}}\Gamma : {}^{\mathtt{s}}\Gamma \\ \mathtt{h} \vdash \iota_1 : dyn({}^{\mathtt{s}}\mathtt{N}, \mathtt{h}, {}^{\mathtt{r}}\iota_1) \\ \mathtt{h} \vdash \iota_2 : dyn({}^{\mathtt{s}}\mathtt{T}, \iota_1, \mathtt{h}(\iota_1)\downarrow_1) \\ {}^{\mathtt{s}}\mathtt{N} = \mathtt{u}_N\ \mathtt{C}_N\langle\_\rangle \\ \mathtt{u}_N = \mathtt{this}_u \Rightarrow {}^{\mathtt{r}}\Gamma(\mathtt{this}) \\ free({}^{\mathtt{s}}\mathtt{T}) \subseteq dom(\mathtt{C}_N)\end{array} \quad \left.\begin{array}{l}\\ \\ \\ \\ \\ \\ \end{array}\right\} \Longrightarrow \mathtt{h} \vdash \iota_2 : dyn({}^{\mathtt{s}}\mathtt{N} \rhd {}^{\mathtt{s}}\mathtt{T}, \mathtt{h}, {}^{\mathtt{r}}\Gamma) \quad {}^{\mathtt{r}}\mathtt{T} = \iota'\ \_\langle\_\rangle \quad \iota \vdash {}^{\mathtt{r}}\mathtt{T}\ {}^{\mathtt{r}}{<:}\ \iota'\ \mathtt{C}\langle\overline{{}^{\mathtt{r}}\mathtt{T}}\rangle \quad \iota \vdash {}^{\mathtt{r}}\mathtt{T}\ {}^{\mathtt{r}}{<:}\ \iota'\ \mathtt{C}\langle\overline{{}^{\mathtt{r}}\mathtt{T}_a}\rangle \Rightarrow \iota \vdash \overline{{}^{\mathtt{r}}\mathtt{T}}\ {}^{\mathtt{r}}{<:}\ \overline{{}^{\mathtt{r}}\mathtt{T}_a} \quad \mathrm{dom}(\mathtt{C}) = \overline{\mathtt{X}} \quad \mathrm{free}({}^{\mathtt{s}}\mathtt{T}) \subseteq \overline{\mathtt{X}} \circ \overline{\mathtt{X}'}}{dyn({}^{\mathtt{s}}\mathtt{T}, \iota, {}^{\mathtt{r}}\mathtt{T}, (\overline{\mathtt{X}'\ {}^{\mathtt{r}}\mathtt{T}'}; \_)) = {}^{\mathtt{s}}\mathtt{T}[\iota'/\mathtt{this}, \iota'/\mathtt{peer}, \iota/\mathtt{rep}, \mathtt{any}_a/\mathtt{any}_u, \overline{{}^{\mathtt{r}}\mathtt{T}/\mathtt{X}}, \overline{{}^{\mathtt{r}}\mathtt{T}'/\mathtt{X}'}]}$$

Define a type system

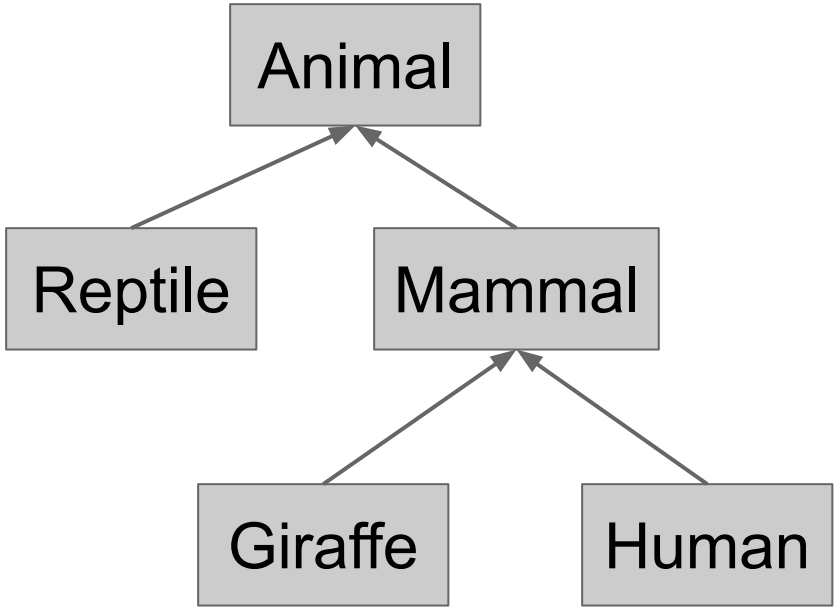
1. **Type hierarchy** (subtyping)
2. **Type rules** (what operations are illegal)
3. **Type introduction** (what types for literals, …)
4. **Dataflow** (run-time tests)

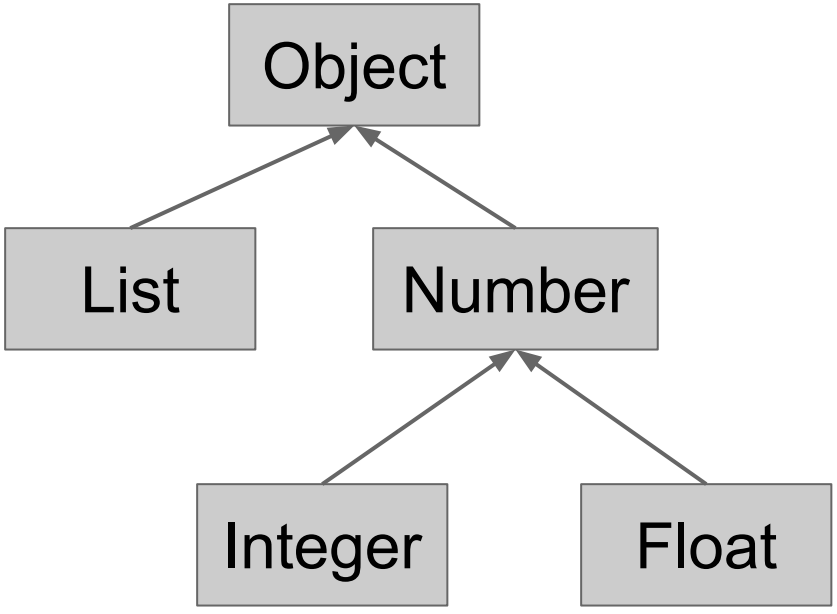
We will define two type systems:
Nullness and Optional

Define a type system

1. **Type hierarchy (subtyping)**
2. Type rules (what operations are illegal)
3. Type introduction (what types for literals, …)
4. Dataflow (run-time tests)

1. Type hierarchy



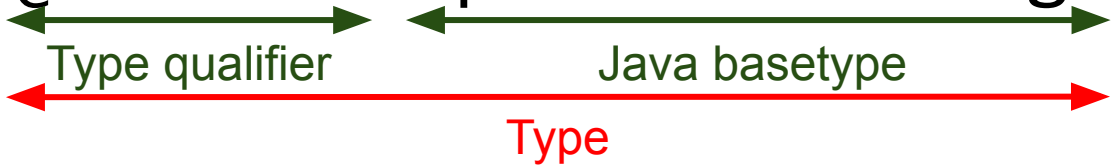


2 pieces of information:

- the types
- their relationships (lower = fewer values, more properties)

Type = type qualifier + Java basetype

```
@Present Optional<String> maidenName;
```



Null pointer exception

```
String op(Data in) {
  return "transform: " + in.getF();
}
…
String s = op(null);
```


Null pointer exception

Where is the defect?

```
String op(Data in) {
  return "transform: " + in.getF();
}
…
String s = op(null);
```


Null pointer exception

Where is the defect?

```
String op(Data in) {
  return "transform: " + in.getF();
}
…
String s = op(null);
```


Null pointer exception

Where is the defect?

```
String op(Data in) {
  return "transform: " + in.getF();
}
...
String s = op(null);
```

Can’t decide without specification!

Specification 1: non-null parameter

```
String op(@NonNull Data in) {
  return "transform: " + in.getF();
}
…
String s = op(null);
```


Specification 1: non-null parameter

```
String op(@NonNull Data in) {
  return "transform: " + in.getF();
}
…
String s = op(null);      // error
```

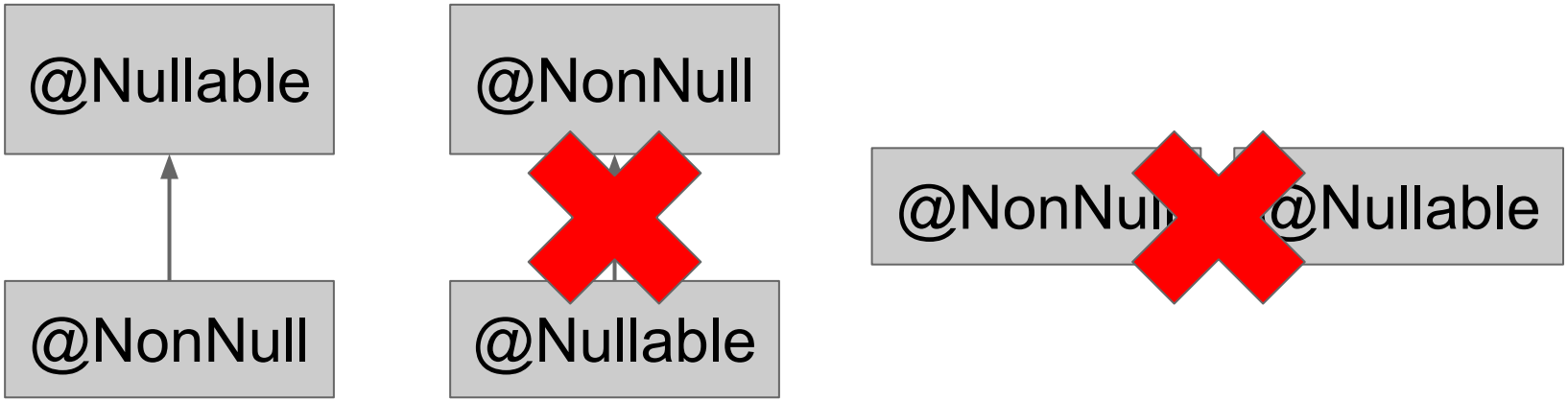

Specification 2: nullable parameter

```
String op(@Nullable Data in) {
  return "transform: " + in.getF();
}
…
String s = op(null);
```


Specification 2: nullable parameter

```
String op(@Nullable Data in) {
  return "transform: " + in.getF();
}                                  // error
…
String s = op(null);
```

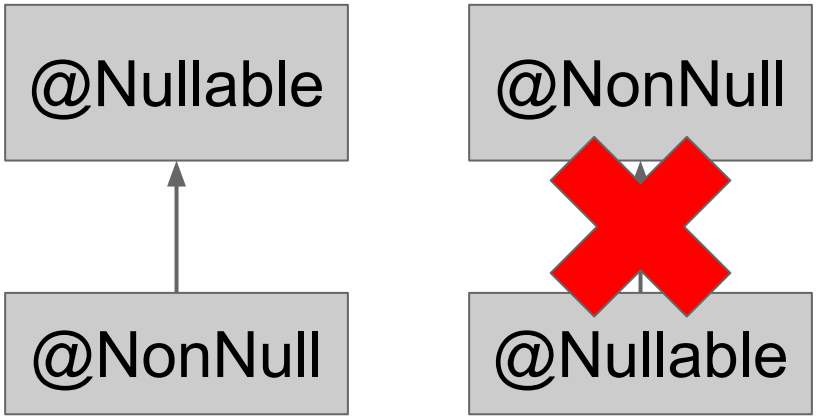

Type hierarchy for nullness

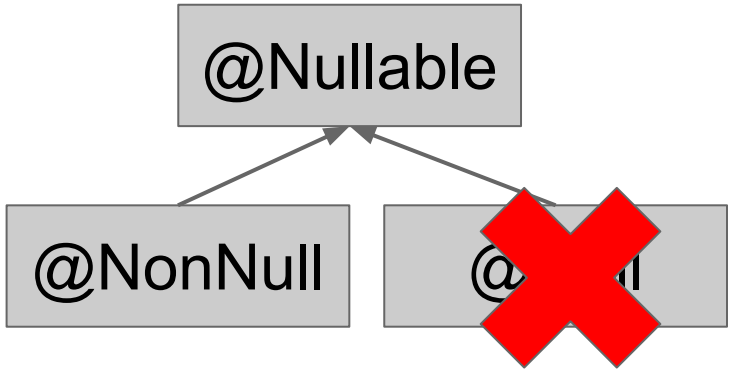


2 pieces of information:

- the types
- their relationships

Type hierarchy for nullness





2 pieces of information:

- the types
- their relationships

Type hierarchy for Optional

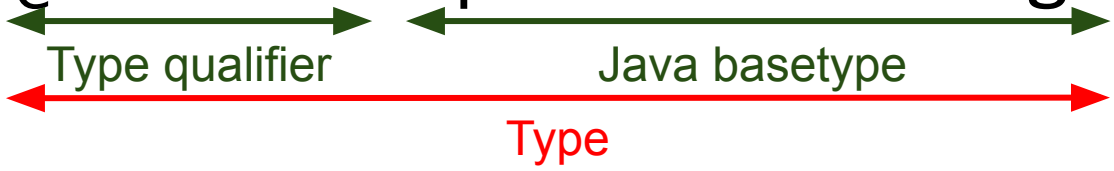
“Never use Optional.get() unless you can prove that the Optional is present.”

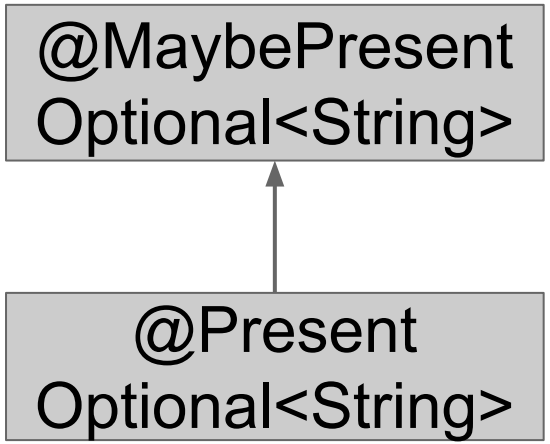
2 pieces of information:

- the types
- their relationships

Type = type qualifier + Java basetype

```
@Present Optional<String> maidenName;
```





Default qualifier = `@MaybePresent`

- `@MaybePresent Optional<String>`
- `Optional<String>`

equivalent

Define a type system

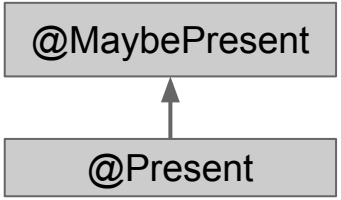
1. Type hierarchy (subtyping)
2. **Type rules (what operations are illegal)**
3. Type introduction (what types for literals, …)
4. Dataflow (run-time tests)

2. Type rules

To prevent null pointer exceptions:

- `expr.field`
  `expr.getValue()`
  receiver must be non-null
- `synchronized (expr) { … }`
  monitor must be non-null
- …

Type rules for Optional



"Never use Optional.get() unless you can prove that the Optional is present."

Only call `Optional.get()` on a receiver of type `@Present Optional`.

```
class Optional<T> {
  T get() { … }
}
```

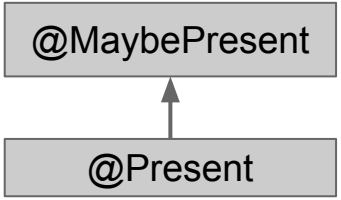
example call:

```
myOptional.get()
```

example call:

```
a.equals(b)
```


Type rules for Optional



"Never use Optional.get() unless you can prove that the Optional is present."

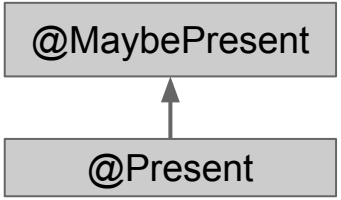
Only call `Optional.get()` on a receiver of type `@Present Optional`.

example call:

`myOptional.get()`

```
class Optional<T> {
  T get(Optional<T> this) { … }
}
```


Type rules for Optional



"Never use Optional.get() unless you can prove that the Optional is present."

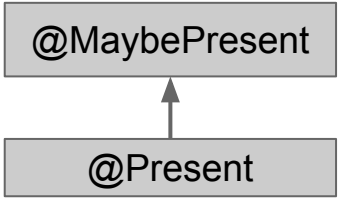
Only call `Optional.get()` on a receiver of type `@Present Optional`.

example call:

`myOptional.get()`

```
class Optional<T> {
  T get(@Present Optional<T> this) {...}
}
```


Type rules for Optional



"Never use Optional.get() unless you can prove that the Optional is present."

Only call `Optional.get()` on a receiver of type `@Present Optional`.

example call:

`myOptional.get()`

```
class Optional<T> {
  T get(@Present Optional<T> this) {…}
  T orElseThrow(@Present O… this, …) {…}
}
```


Define a type system

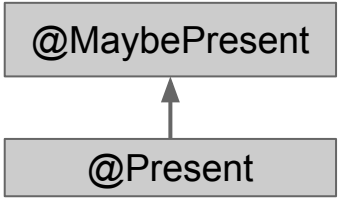
1. Type hierarchy (subtyping)
2. Type rules (what operations are illegal)
3. **Type introduction (what types for literals…)**
4. Dataflow (run-time tests)

Type introduction rules

For Nullness type system:

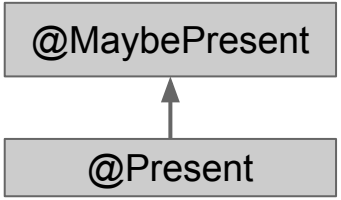
- `null : @Nullable`
- `"Hello World" : @NonNull`

Type introduction for Optional




```
Optional<T> of(T value) {...}
Optional<T> ofNullable(T value){...}
```


Type introduction for Optional




```
@Present Optional<T> of(T value) {...}
Optional<T> ofNullable(@Nullable T value){...}
```


Define a type system

1. Type hierarchy (subtyping)
2. Type rules (what operations are illegal)
3. Type introduction (what types for literals, …)
4. **Dataflow (run-time tests)**

Flow-sensitive type refinement

After an operation, give an expression a more specific type

```
@Nullable Object x;
if (x != null) {
   ...
}
...
```

x is @NonNull here

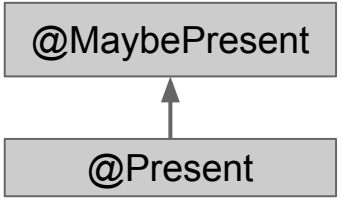
x is @Nullable again

```
@Nullable Object y;
y = new SomeType();
...
y = unknownValue;
...
```

y is @NonNull here

y is @Nullable again

Type refinement for Optional



"Never use Optional.get() unless you can prove that the Optional is present."

After `receiver.isPresent()` returns true, the receiver's type is `@Present`

```
@MaybePresent Optional<String> x;
if (x.isPresent()) {
   …
}
…
```

x is @Present here

x is @MaybePresent again

Let’s look at the Optional Checker

https://github.com/eisop/checker-framework/tree/master/checker/src/main/java/org/checkerframework/checker/optional

https://github.com/eisop/checker-framework/tree/master/checker-qual/src/main/java/org/checkerframework/checker/optional/qual

Design the type system first

Before you start coding, first write the user manual.

What problem are you solving?

What qualifiers will you need?

What rules do you need to enforce?

Implement type qualifiers and hierarchy

```
@Documented
@Retention(RetentionPolicy.RUNTIME)
@Target({ElementType.TYPE_USE,
        ElementType.TYPE_PARAMETER})
@SubtypeOf({MaybePresent.class})
public @interface Present {}
```

https://github.com/eisop/checker-framework/tree/master/checker-qual/src/main/java/org/checkerframework/checker/optional/qual

Use the Subtyping Checker

Experiment with the type qualifiers using the Subtyping Checker:

```
javac -processor ...SubtypingChecker \
  -Aquals=...Present,...MaybePresent \
  SubtypeCheck.java
```


Name your checker

Simplify usage by adding a main class:

```
public class OptionalChecker
      extends BaseTypeChecker {}
```


Annotate parts of the JDK

Add `jdk.astub` JDK specifications

```
class Optional<T extends Object> {
   static <T extends Object> @Present Optional<T> of(T value) …
   T get(@Present Optional<T> this) …
   …
}
```

https://github.com/eisop/jdk/blob/master/src/java.base/share/classes/java/util/Optional.java

Type rules and type introductions

No additional rules needed for the Optional Checker — everything can be specified declaratively and use Checker Framework rules.

Implement dataflow refinement

Declarative specification possible:

```
@EnsuresQualifierIf(result = true,
   expression = "this",
   qualifier  = Present.class)
public boolean isPresent() {
    return value != null;
}
```

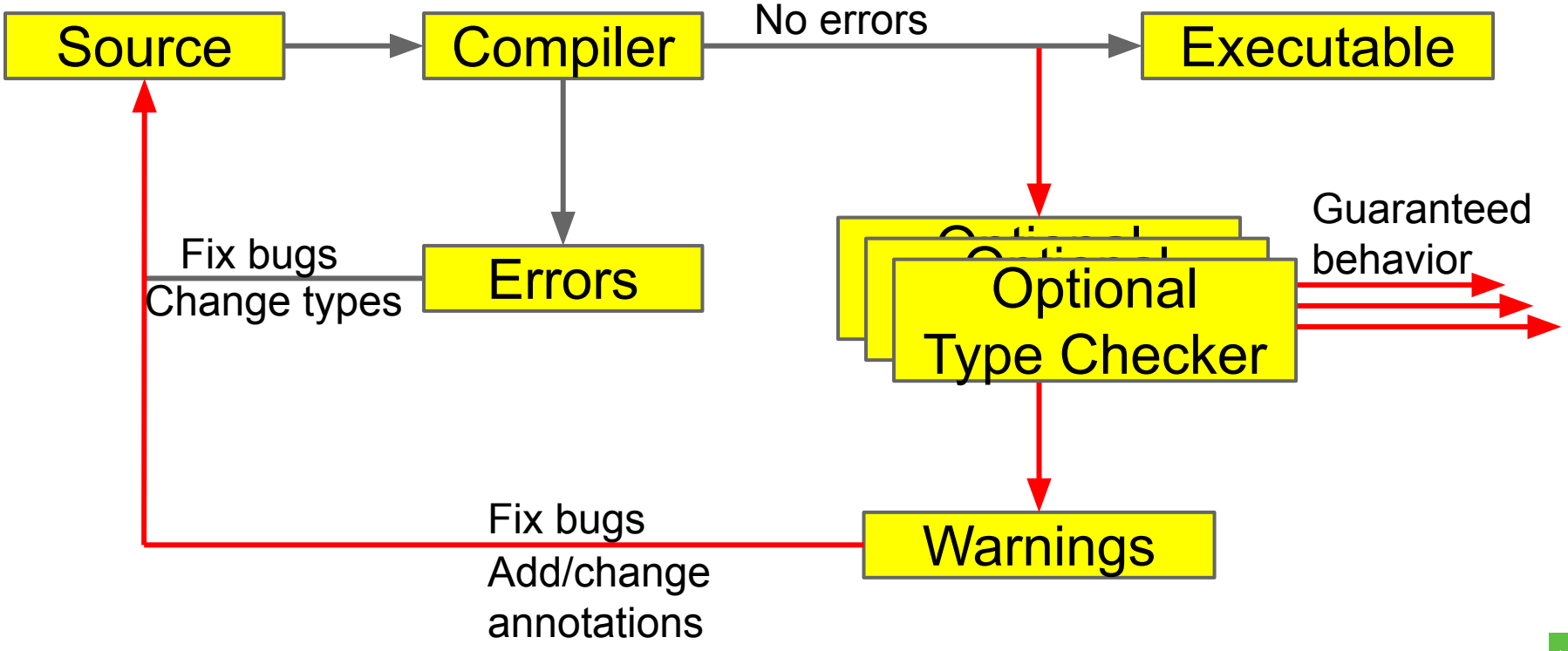

You can use the Optional Checker

Distributed with the Checker Framework

Checks 6 of the 7 rules for using `Optional`

https://eisop.github.io/cf/manual/#optional-checker

Optional Type Checking



Benefits of type systems

- **Find bugs** in programs
  - Guarantee the **absence of errors**
- **Improve documentation**
  - Improve code structure & maintainability
- Aid compilers, optimizers, and analysis tools
  - E.g., could reduce number of run-time checks

- Possible negatives:
  - Must write the types (or use type inference)
  - False positives are possible (can be suppressed)

Checker Framework facilities

- Full type systems: inheritance, overriding, ...
- Generics (type polymorphism)
  - Also qualifier polymorphism
- Qualifier defaults
- Pre-/post-conditions
- Warning suppression

Example type systems

Null dereferences (`@Nullable`)

>200 errors in Google Collections, javac, ...

Equality tests (`@Interned`)

>200 problems in Xerces, Lucene, ...

Concurrency / locking (`@GuardedBy`)

>500 errors in BitcoinJ, Derby, Guava, Tomcat, ...

Fake enumerations / typedefs (`@Fenum`)

problems in Swing, JabRef

String type systems

Regular expression syntax (`@Regex`)
    56 errors in Apache, etc.; 200 annos required
printf format strings (`@Format`)
    104 errors, only 107 annotations required
Method signature format (`@FullyQualified`)
    28 errors in OpenJDK, ASM, AFU
Compiler messages (`@CompilerMessageKey`)
    8 wrong keys in Checker Framework

Security type systems

Command injection vulnerabilities (`@OsTrusted`)

5 missing validations in Hadoop

Information flow privacy (`@Source`)

SPARTA detected malware in Android apps

It’s easy to write your own type system!

What a checker guarantees

The program satisfies the type property. There are:

- no bugs (of particular varieties)
- no wrong annotations

- Caveat 1: only for code that is checked
  - Native methods (handles reflection!)
  - Code compiled without the pluggable type checker
  - Suppressed warnings
    - Indicates what code a human should analyze

  Checking part of a program is still useful
- Caveat 2: The checker itself might contain an error

Verification

- **Goal**:
  prove that no bug exists
- **Specifications**:
  user provides
- **False negatives**:
  none
- **False positives**:
  user suppresses warnings
- **Downside**: user burden

Bug-finding

- **Goal**:
  find some bugs at low cost
- **Specifications**:
  infer likely specs
- **False negatives:**
  acceptable
- **False positives**:
  heuristics focus on most important bugs
- **Downside**: missed bugs

Neither is “better”; each is appropriate in certain circumstances.

Checkers are usable

- Type-checking is familiar to programmers
- Modular: fast, incremental, partial programs
- Annotations are not too verbose
  - **`@Nullable`**: 1 per 75 lines
  - **`@Interned`**: 124 annotations in 220 KLOC revealed 11 bugs
  - **`@Format`**: 107 annotations in 2.8 MLOC revealed 104 bugs
  - Possible to annotate part of program
  - Fewer annotations in new code
- Few false positives
- First-year CS majors preferred using checkers to not
- **Practical**: in use in Silicon Valley, on Wall Street, etc.

Tips

- Start by type-checking part of your code
- Only type-check properties that matter to you
- Use subclasses (not type qualifiers) if possible
- Write the spec first (and think of it as a spec)
- Avoid warning suppressions when possible
- Avoid raw types such as `List`; use `List<String>`

More at JAX 2023

Null Pointer Exceptions: the Problems, Current Approaches, and Ongoing Efforts

Donnerstag, 11. Mai 2023

16:45 - 17:45

Raum: Kongresssaal

Pluggable type-checking improves code

Checker Framework for creating type checkers

- Featureful, effective, easy to use, scalable

Prevent bugs at compile time

Create custom type-checkers

Improve your code!

`https://eisop.github.io/`

Acknowledgement: Slides developed with Michael Ernst, University of Washington.