



Факультет компьютерных наук

Системное программирование

Москва 2024

Расширение статического анализа кода Java на основе пользовательских аннотаций

Extending Static Analysis of Java Code Based on User Annotations

Выполнил:

Пасилецкий Даниил Олегович

Руководитель:

Профессор Базовая кафедра
«Системное программирование» ИСП
РАН, факультета компьютерных наук,
Белеванцев Андрей Андреевич

Консультант:

Старший лаборант ИСП РАН,
Афанасьев Виталий Олегович



Основные термины, понятия и определения

Статический анализ кода – анализ исходного кода на предмет ошибок и недочётов без непосредственного выполнения анализируемых программ.

Java – анализ исходного кода на предмет ошибок и недочётов без непосредственного выполнения анализируемых программ.

Svace – анализ исходного кода на предмет ошибок и недочётов без непосредственного выполнения анализируемых программ.

Java Annotations – это специальная форма синтаксических метаданных, которая может быть добавлена в исходный код.

Моделирование – это специальный подход при котором исходный класс заменяется на его упрощенную модель, с которой умеет работать анализатор



Проблема

Анализатор не всегда может верно работать, иногда из-за ограничений на потребляемые время и память приходится что-то упрощать, а иногда код очень непонятный (либо вообще исходники отсутствуют). И одно из решений - это предоставить пользователю механизм, который подсказывает что-то анализатору.

```
1 public class SalaryCalculator {  
2  
3     public static double calculateAverageDailySalary(double totalSalary, int totalDays) {  
4         return totalSalary / totalDays;  
5     }  
6  
7     public static void main(String[] args) {  
8         double dailySalary = calculateAverageDailySalary(50000, Calendar.getWorkingDays());  
9     }  
10 }
```



Постановка задачи

Необходимо расширить возможности статического анализатора Svace, таким образом чтобы пользователи могли предоставлять дополнительную информацию анализатору, путем добавления специальных аннотаций в исходном коде анализируемой программы.

```
public class SalaryCalculator {  
    public static double calculateAverageInDaySalary(@Range(min = 28, max = 31) int dayInMonths, double salary) {  
        return salary / dayInMonths;  
    }  
}
```



Моделирование

Используется специальный класс
который перекрывает настоящую
реализацию Calendar

```
1 public class Calendar {  
2     public static int getWorkinkDays() {  
3         int number = Spec.getAnyInt();  
4         number.range(28, 31);  
5         return number;  
6     }  
7 }
```



Основные проблемы

```
1 public class SalaryCalculator {  
2  
3     public static double calculateAverageDailySalary(double totalSalary, @Range(min=28, max=32) int totalDays) {  
4         return totalSalary / totalDays;  
5     }  
6  
7     public static void main(String[] args) {  
8         double dailySalary = calculateAverageDailySalary(50000, 0);  
9     }  
10 }
```



План

- ☐ Определить набор аннотаций, которые могут быть использованы пользователями
- ☐ Улучшить работу статического анализатора с аннотациями
- ☐ Разработать пакет с набором аннотаций, которые используются для расширения информации анализатора.
- ☐ Доработать статический анализатор для реагирования на эти аннотации и учитывать их при анализе кода.



Набор аннотаций

29

аннотаций без учета перегрузок

Можно помечать аннотациями:

- Параметры функций
- Поля
- Методы

@Sensitive

@Tainted

@FunHash

@Leaked

@NotNull

@FunPrintfLike



Как измерить результат

- Количество замененных спецификации на пользовательский код
- Количество использований аннотаций пользователями
- Время затрачиваемое на добавление новой аннотации



Факультет компьютерных наук

Системное программирование

Москва 2024

Расширение статического анализа кода Java на основе пользовательских аннотаций

Extending Static Analysis of Java Code Based on User Annotations

Выполнил:

Пасилецкий Даниил Олегович

Руководитель:

**Профессор Базовая кафедра
«Системное программирование» ИСП
РАН, факультета компьютерных наук,
Белеванцев Андрей Андреевич**

Консультант:

**Старший лаборант ИСП РАН,
Афанасьев Виталий Олегович**