

Javassist

НА СЛУЖБЕ У JAVA-РАЗРАБОТЧИКА

JPoint 2015

Привет!

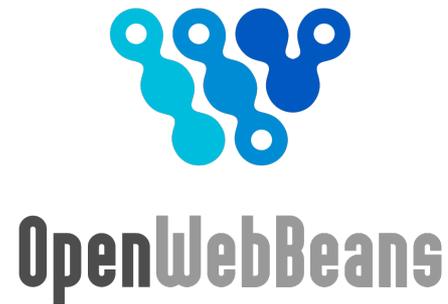


АНТОН АРХИПОВ

@antonarhipov

JRebel

XRebel



Инструментация байткода



ВЕЗДЕ!!!

```
@Entity
@Table(name = "owners")
public class Owner extends Person {
    @Column(name = "address")
    @NotEmpty
    private String address;

    @Column(name = "city")
    @NotEmpty
    private String city;

    @Column(name = "telephone")
    @NotEmpty
    @Digits(fraction = 0, integer = 10)
    private String telephone;

    @OneToMany(cascade = CascadeType.ALL,
              mappedBy = "owner")
    private Set<Pet> pets;
```

```
public class JavassistLazyInitializer
    extends BasicLazyInitializer
    implements MethodHandler {
```

```
final JavassistLazyInitializer instance
    = new JavassistLazyInitializer(...);
```

```
ProxyFactory factory = new ProxyFactory();
factory.setSuperclass(interfaces.length == 1?persistentClass:null);
factory.setInterfaces(interfaces);
factory.setFilter(FINALIZE_FILTER);
```

```
Class cl = factory.createClass();
final HibernateProxy proxy = (HibernateProxy) cl.newInstance();
((ProxyObject)proxy).setHandler(instance);
instance.constructed = true;
return proxy;
```

```
public class JavassistLazyInitializer
    extends BasicLazyInitializer
    implements MethodHandler {
```

генерируем проху!

```
final JavassistLazyInitializer instance
    = new JavassistLazyInitializer(...);
```

```
ProxyFactory factory = new ProxyFactory();
factory.setSuperclass(interfaces.length == 1?persistentClass:null);
factory.setInterfaces(interfaces);
factory.setFilter(FINALIZE_FILTER);
```



```
Class cl = factory.createClass();
final HibernateProxy proxy = (HibernateProxy) cl.newInstance();
((ProxyObject)proxy).setHandler(instance);
instance.constructed = true;
return proxy;
```

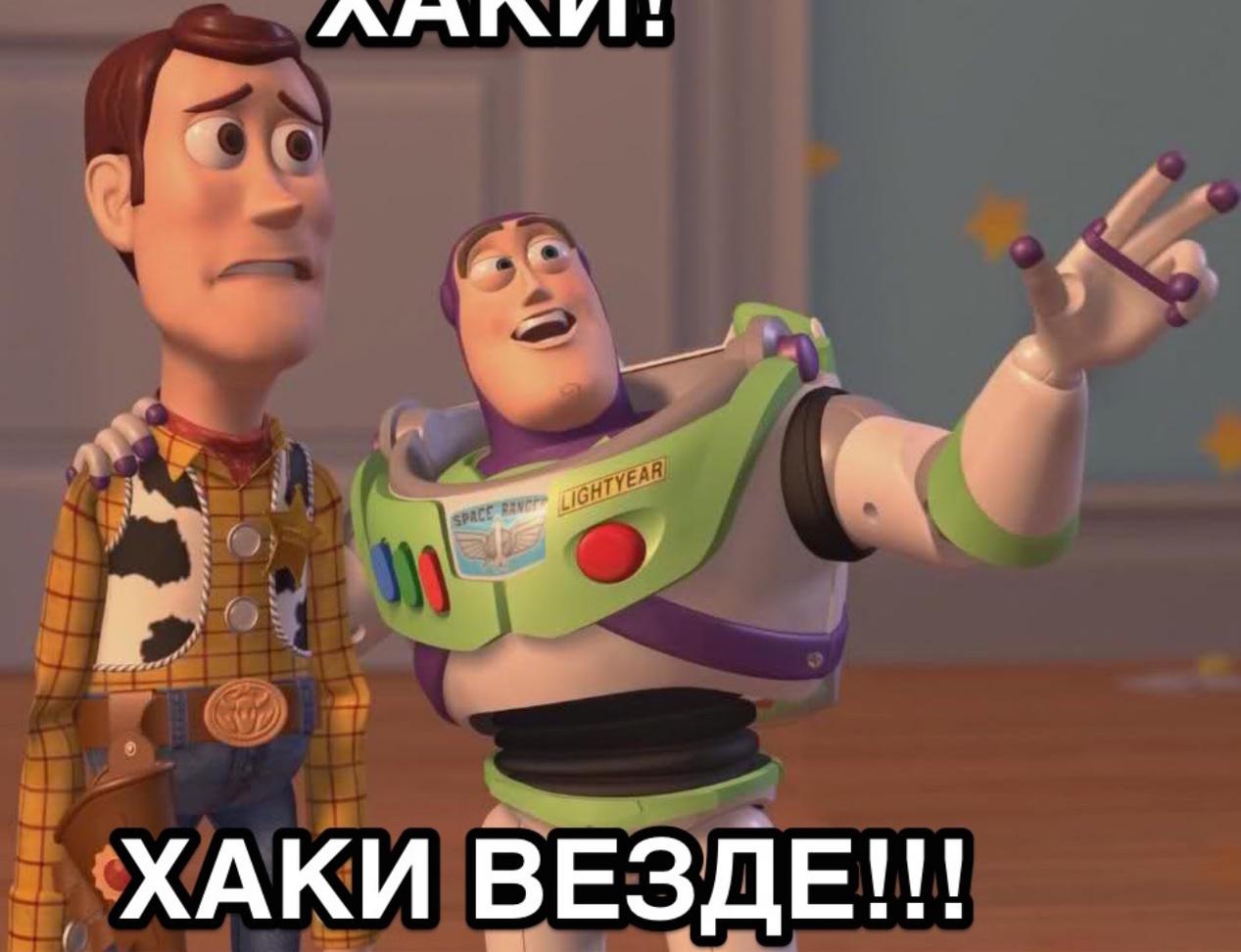
Основное применение
байткодо-генерирующих
библиотек в Java-фреймворках
- это генерация проху.

BORING

Давайте лучше патчить
чужой код! :)

ХАКИ!

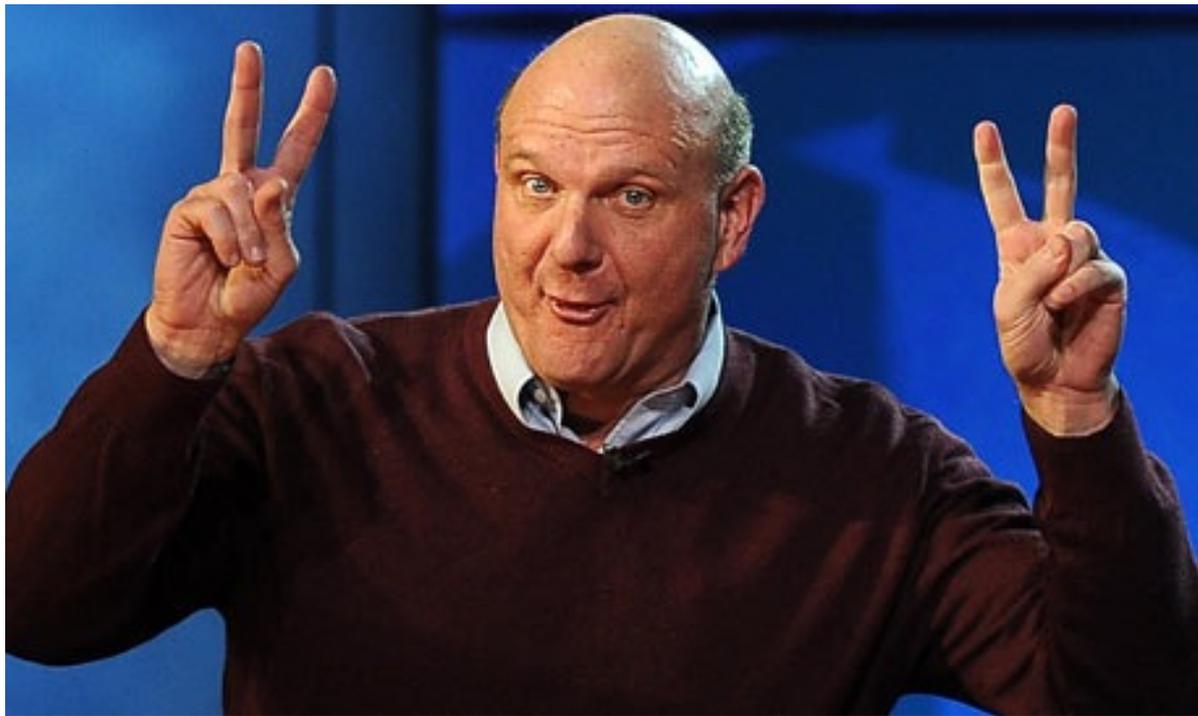
ХАКИ ВЕЗДЕ!!!



инструментация байткода?



инструментация байткода?



легко! бери Javassist!

План захвата галактики

базовые основы *Javassist*
-javaagent
немного о JRebel



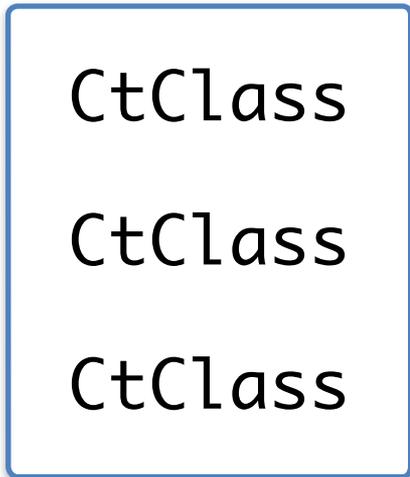
... и попробуем со всем этим хламом взлететь

Javassist

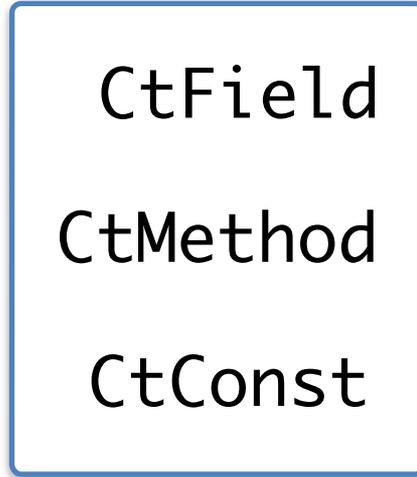
www.javassist.org



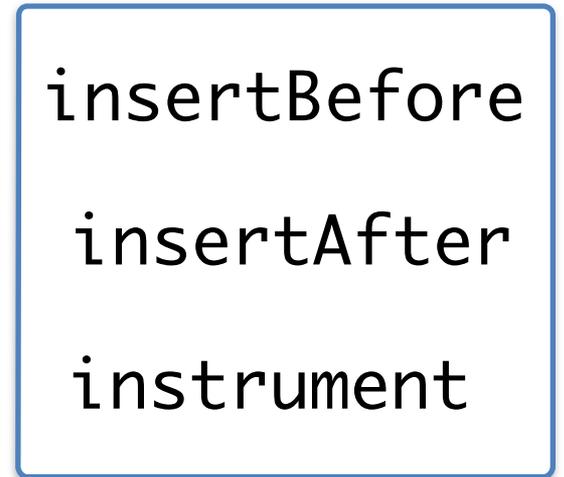
CtPool



CtClass



CtMethod



DEMO

<https://github.com/antonarhipov/jpoint>

Жаба-Агент



Java Agent

```
import java.lang.instrument.ClassFileTransformer;  
import java.lang.instrument.Instrumentation;
```

```
public class Agent {  
    public static void premain(String args, Instrumentation inst)  
        throws Exception {  
        inst.addTransformer(new ClassFileTransformer {  
            // тут будет код  
        });  
    }  
}
```

```
META-INF/MANIFEST.MF  
Premain-Class: Agent
```

```
$> java -javaagent:agent.jar application.Main
```

ClassFileTransformer

```
new ClassFileTransformer() {  
    public byte[] transform(ClassLoader loader,  
                            String className,  
                            Class<?> classBeingRedefined,  
                            ProtectionDomain protectionDomain,  
                            byte[] classfileBuffer){  
  
        ClassPool cp = ClassPool.getDefault();  
        CtClass ct = cp.makeClass(new  
                                ByteArrayInputStream(classfileBuffer));  
  
        // тут можно сделать с ct что душе угодно  
  
        return ct.toBytecode();  
    }  
}
```

ClassFileTransformer

```
new ClassFileTransformer() {  
    public byte[] transform(ClassLoader loader,  
                            String className,  
                            Class<?> classBeingRedefined,  
                            ProtectionDomain protectionDomain,  
                            byte[] classfileBuffer){  
  
        ClassPool cp = ClassPool.getDefault();  
        CtClass ct = cp.makeClass(new  
                                ByteArrayInputStream(classfileBuffer));  
  
        // тут можно сделать с ct что душе угодно  
  
        return ct.toBytecode();  
    }  
}
```

ClassFileTransformer

```
new ClassFileTransformer() {  
    public byte[] transform(ClassLoader loader,  
                            String className,  
                            Class<?> classBeingRedefined,  
                            ProtectionDomain protectionDomain,  
                            byte[] classfileBuffer){  
        ClassPool cp = ClassPool.getDefault();  
        CtClass ct = cp.makeClass(new  
            ByteArrayInputStream(classfileBuffer));  
        // тут можно сделать с ct что душе угодно  
        return ct.toBytecode();  
    }  
}
```

ClassFileTransformer

```
new ClassFileTransformer() {  
    public byte[] transform(ClassLoader loader,  
                            String className,  
                            Class<?> classBeingRedefined,  
                            ProtectionDomain protectionDomain,  
                            byte[] classfileBuffer){  
  
        ClassPool cp = ClassPool.getDefault();  
        CtClass ct = cp.makeClass(new  
                                ByteArrayInputStream(classfileBuffer));  
  
        // тут можно сделать с ct что душе угодно  
        return ct.toBytecode();  
    }  
}
```

Instrumentation

Class loading

A white arrow pointing upwards, starting from the bottom right and ending at the top right of the green box.

Instrumentation

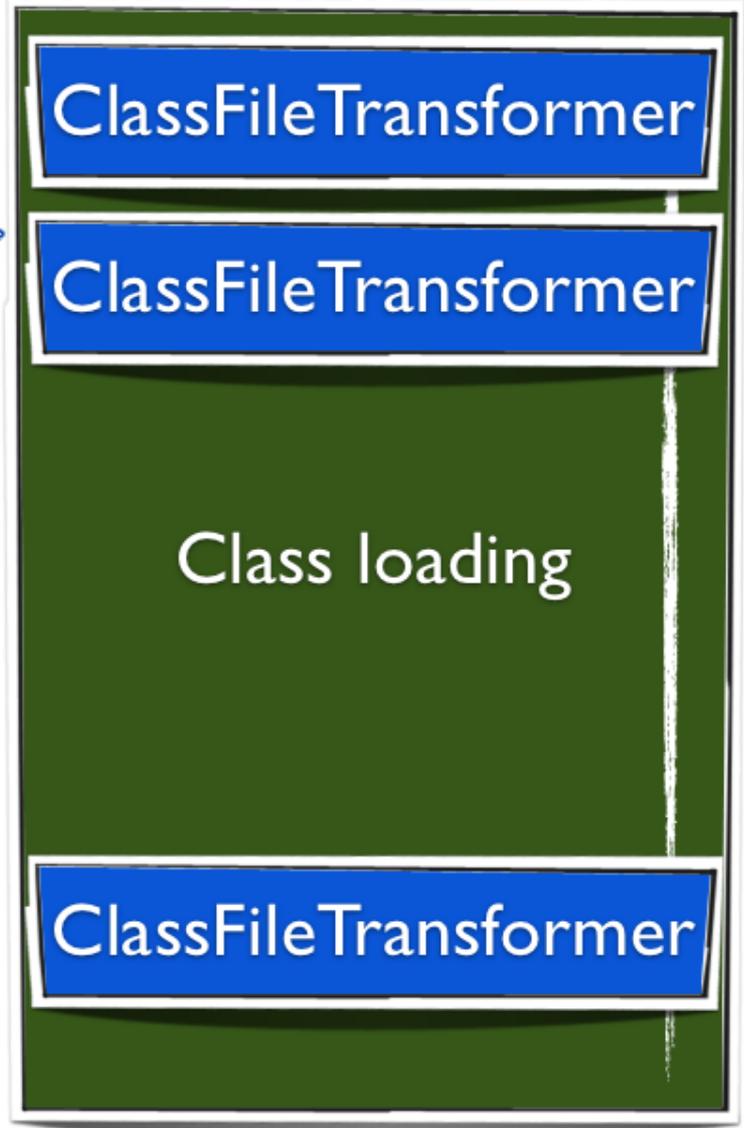
ClassFileTransformer

ClassFileTransformer

Class loading

ClassFileTransformer

Instrumentation

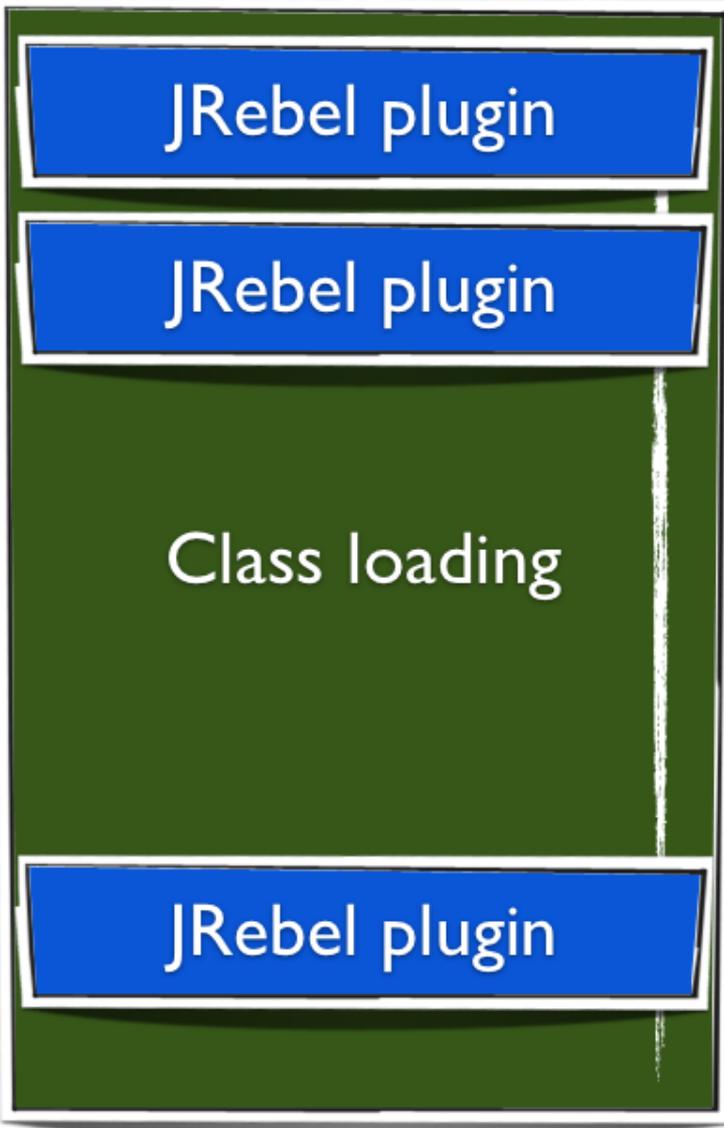


Javassist

ASM



Instrumentation

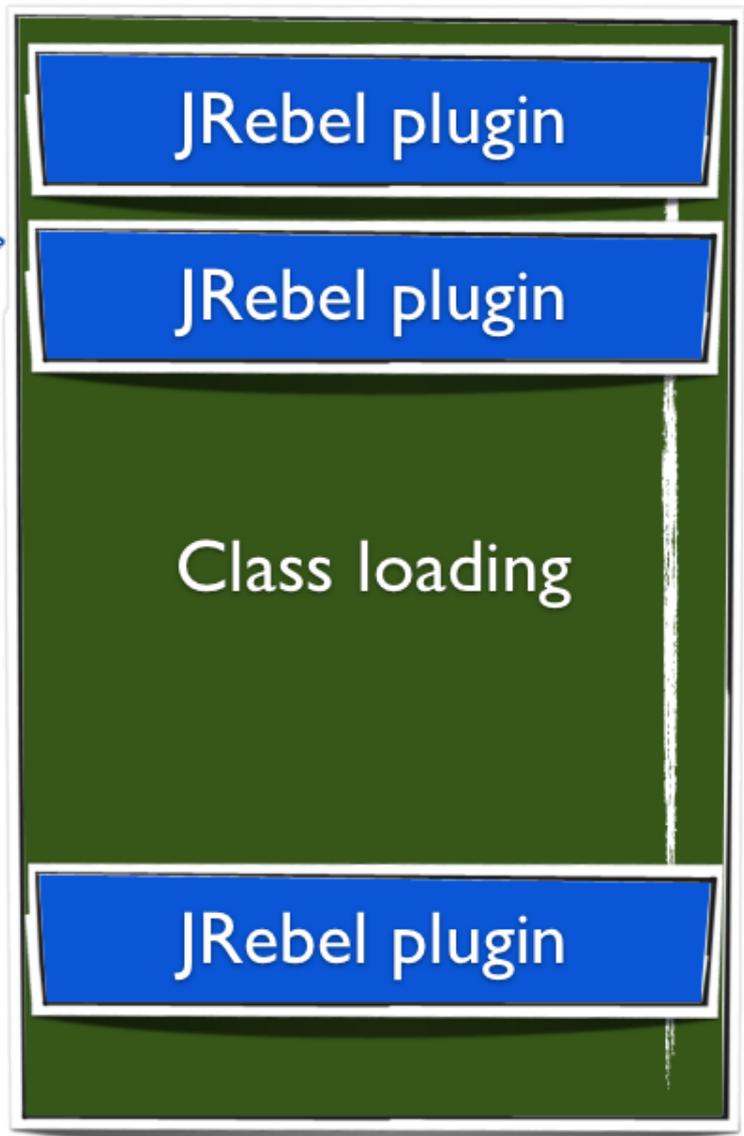


Javassist

ASM



Instrumentation



Javassist

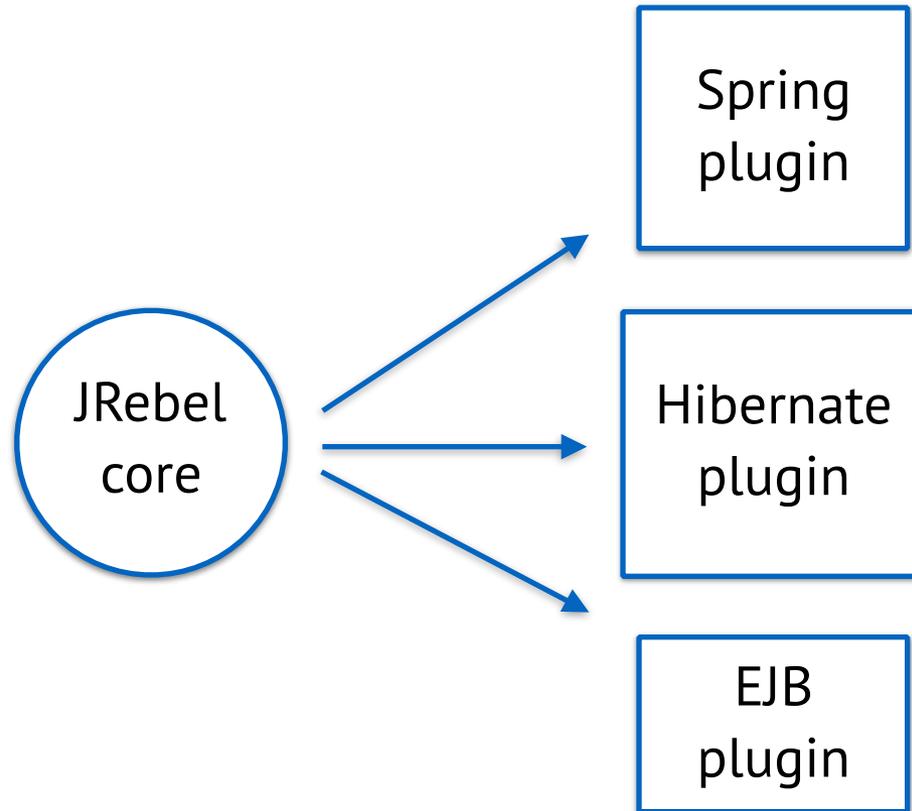
ASM

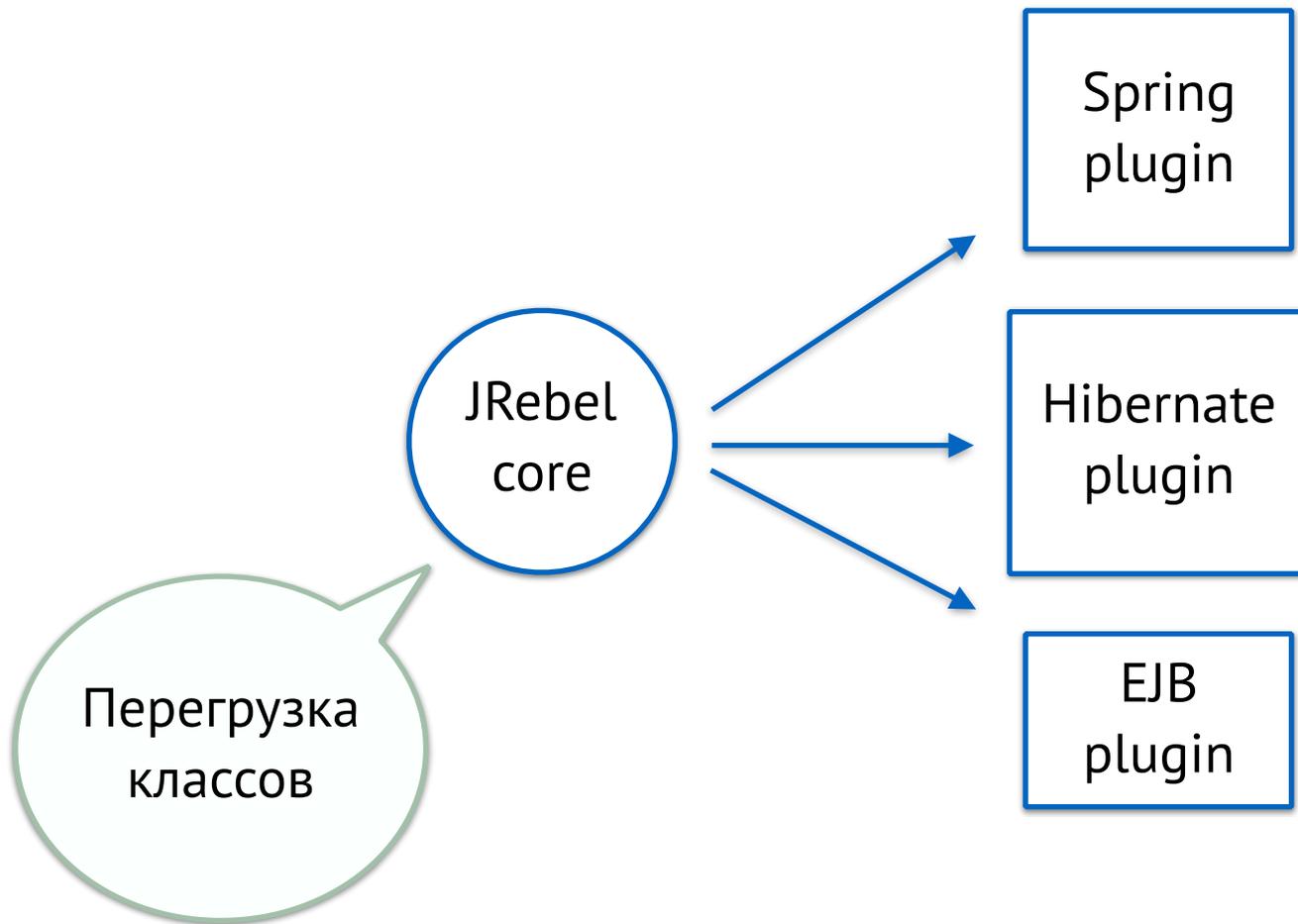


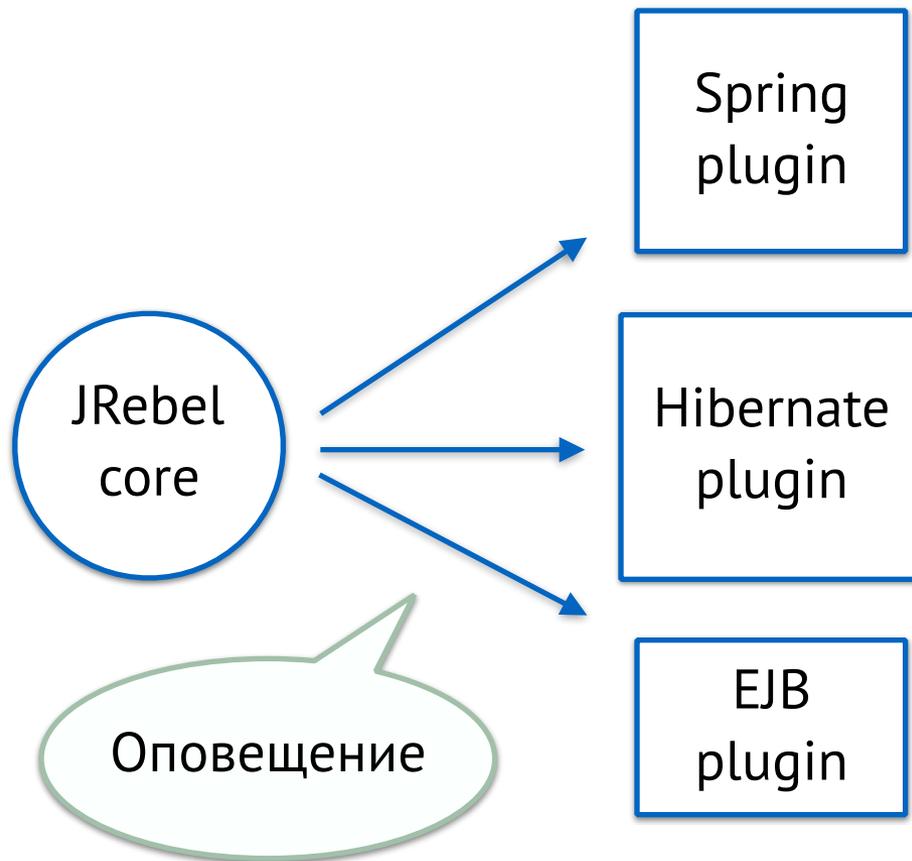
DEMO

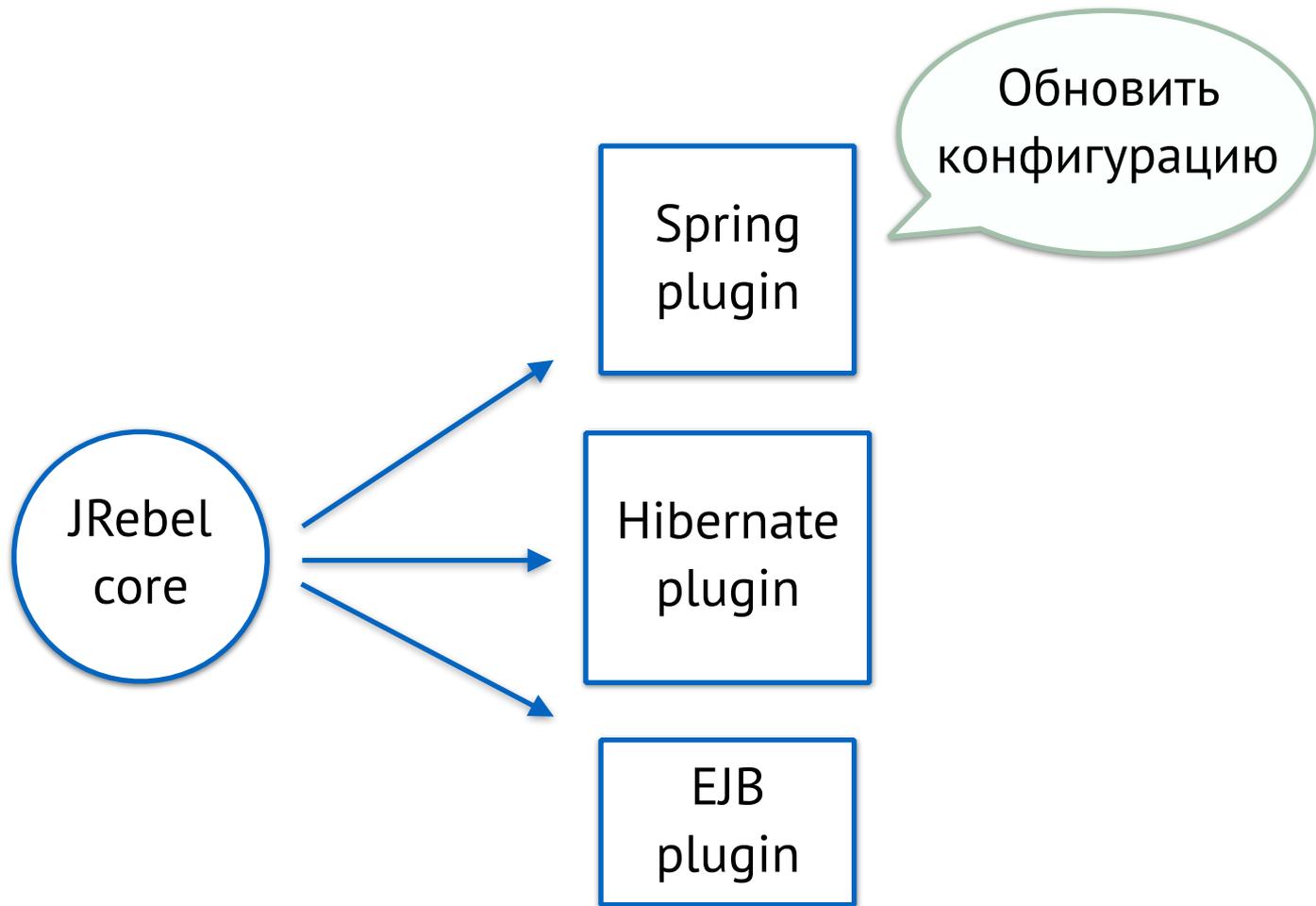
<https://github.com/zeroturnaround/callspy>

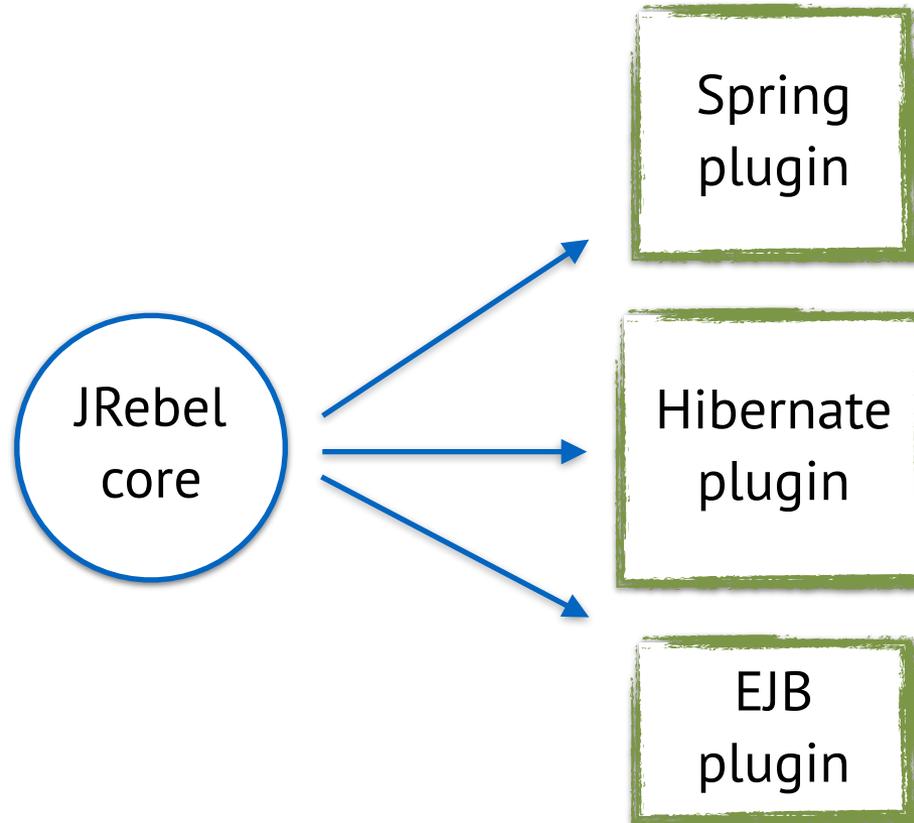
Javassist B **JRebel**





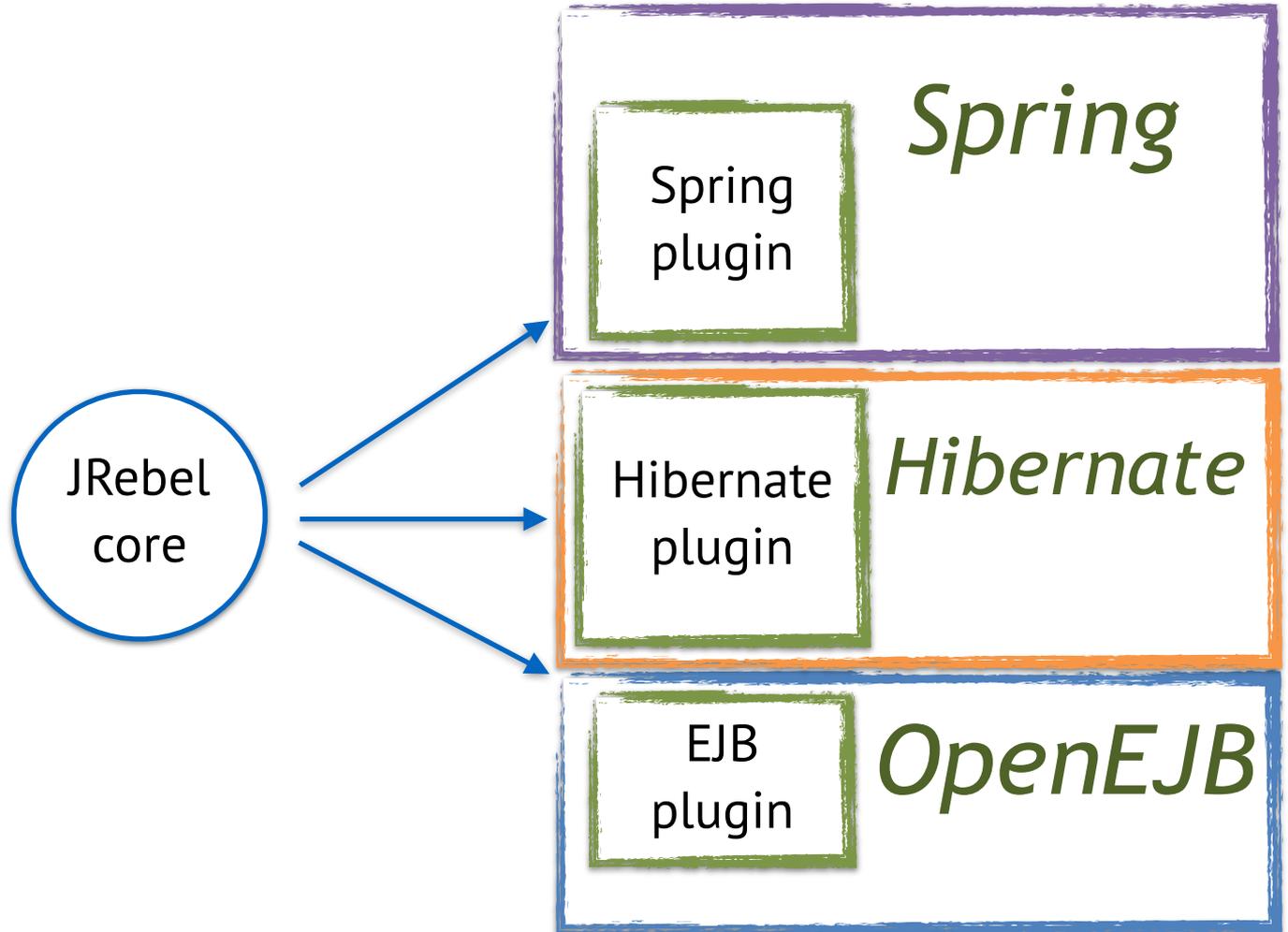






Здесь живёт Javassist



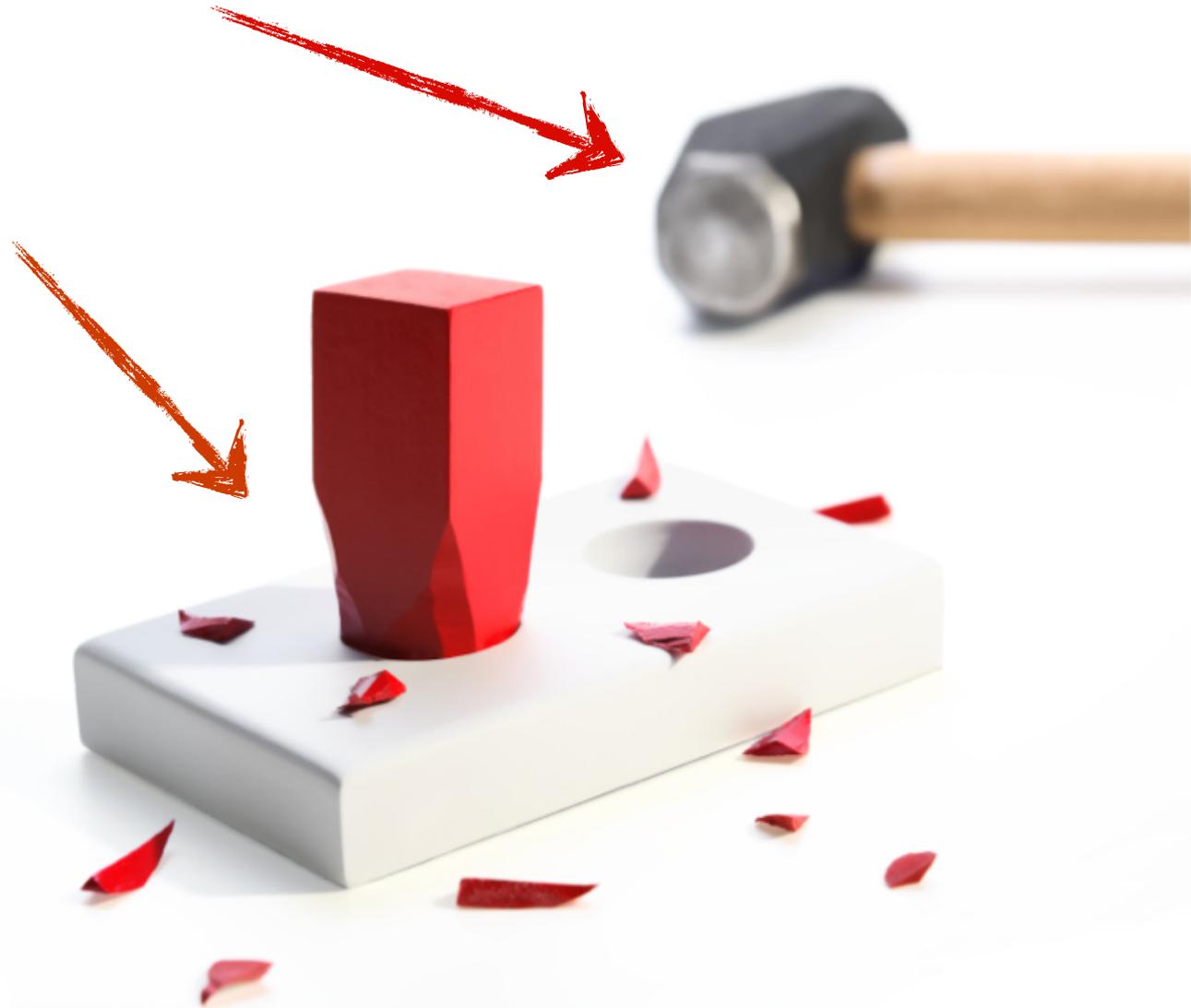


DEMO

<https://github.com/antonarhipov/jpoint>

Javassist

Задача





@antonarhipov

anton@zeroturnaround.com

<https://speakerdeck.com/antonarhipov>

<http://www.slideshare.net/arhan>