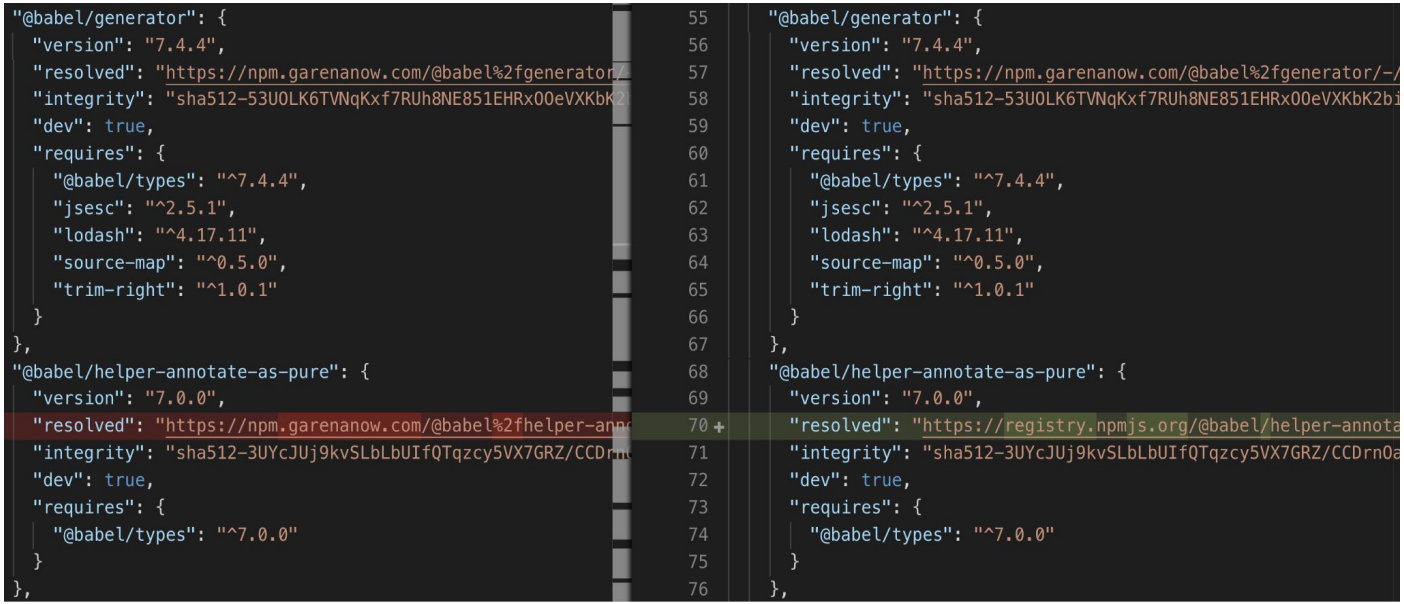
Maven-lockfile

3rd KTH Workshop on the Software Supply Chains

Presented by **Yogya Gamage**

The role of lockfiles

- Deterministic builds
- Integrity
- Dependency tree visualisation
- Code diffs



But we don't have lockfiles for maven.

```xml
<?xml version="1.0" encoding="UTF-8"?>

<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <groupId>com.mycompany.app</groupId>
  <artifactId>my-app</artifactId>
  <version>1.0-SNAPSHOT</version>
  <name>my-app</name>
  <!-- FIXME change it to the project's website -->
  <url>http://www.example.com</url>
  <properties>
    <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
    <maven.compiler.source>1.7</maven.compiler.source>
    <maven.compiler.target>1.7</maven.compiler.target>
  </properties>
  <dependencies>
    <dependency>
      <groupId>junit</groupId>
      <artifactId>juni</artifactId>
      <version>4.1</version>
      <scope>test</scope>
    </dependency>
  </dependencies>
</project>
```

Maven-lockfile

- **Generate** - generates a lock file
- **Validate** - validates the repository against the lockfile
- **Freeze** - dumps the state of the dependencies saved in the lockfile into a pom file

Demo

Thank you!

GitHub **Project**

GitHub **Action**