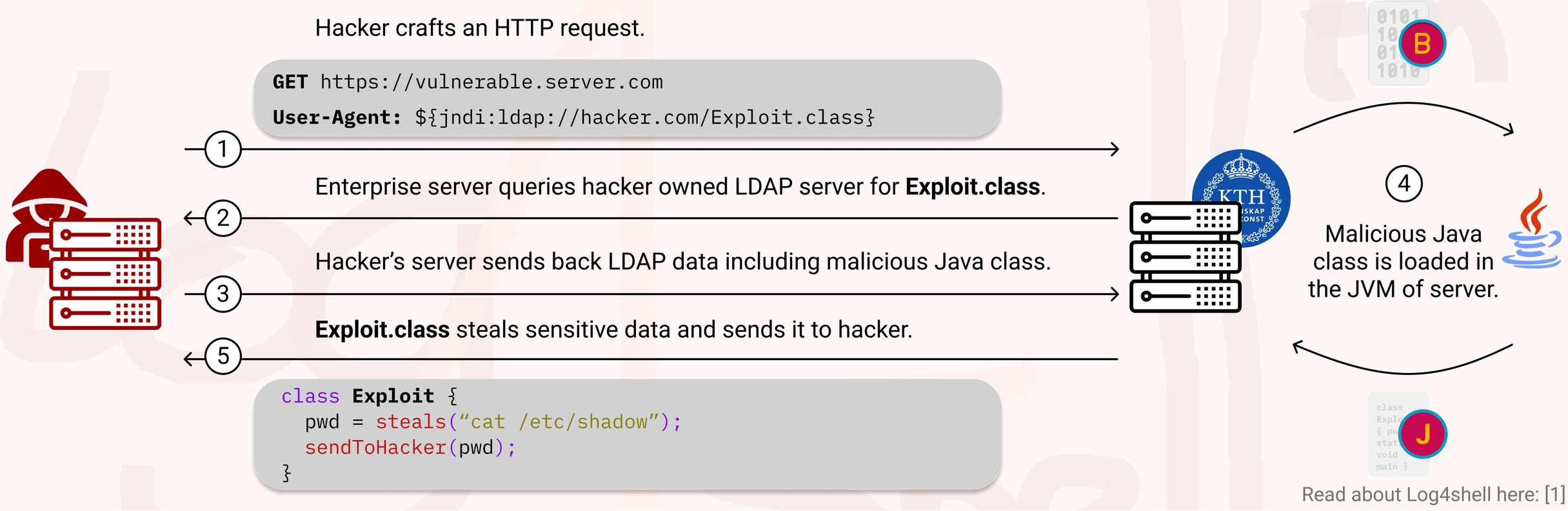
Runtime Integrity in Java Ecosystem

Aman Sharma
amansha@kth.se

Martin Wittlinger
marwit@kth.se

Research Group



Read about Log4shell here: [1]

⚠ Java can execute unknown classes at runtime!

Java software is composed of three kinds of classes

```java
package se.kth.app;

import org.apache.commons.Fraction;

public class Main {
    public static void main(String[] args) {
        System.out.println(new Fraction(1,2));
    }
}
```

Application classes

```xml
<dependency>
    <groupId>org.apache.commons</groupId>
    <artifactId>commons-lang3</artifactId>
    <version>3.13.0</version>
</dependency>
<dependency>
    <groupId>com.fasterxml.jackson.core</groupId>
    <artifactId>jackson-databind</artifactId>
    <version>2.15.2</version>
</dependency>
<dependency>
    <groupId>org.junit.jupiter</groupId>
    <artifactId>junit-jupiter-api</artifactId>
    <version>5.10.0</version>
    <scope>test</scope>
</dependency>
```

Third party library classes

```java
import java.io.IOException;
import java.io.InputStream;
import java.lang.reflect.Array;
import java.net.URL;
import java.util.List;
import java.util.Map;
import java.util.Set;
import jdk.internal.reflect.Reflection;
import sun.invoke.util.Wrapper;
```

Java Development Kit classes

Contribution 1: Generating an allow-list of classes

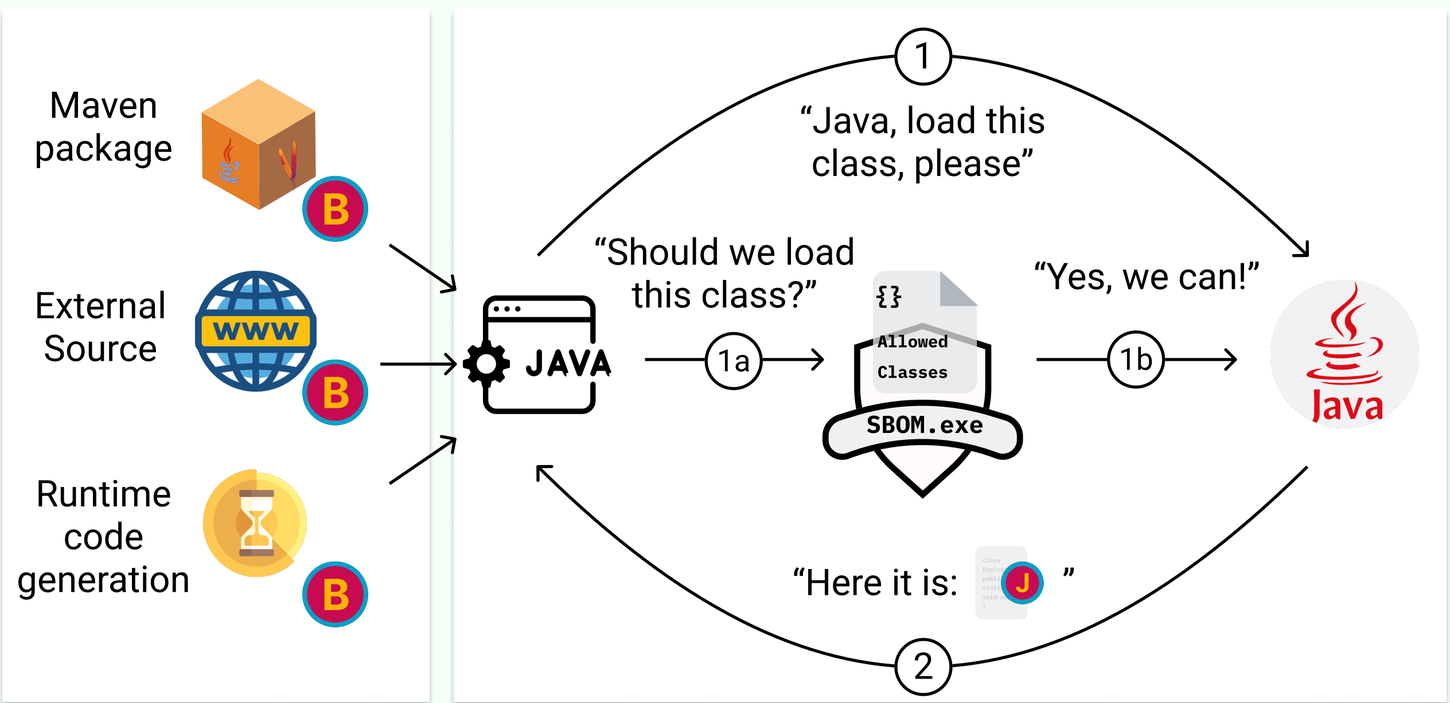
Run the tests and get all the classes that are being executed.

Get all classes from a Software Bill of Materials.

Scan all classes inside the Java Development Kit.

```
// allowed_classes.json
{
  "application": [
    "se.kth.app.Main"
  ],
  "library": [
    "org.apache.commons.Fraction"
  ],
  "jdk": [
    "java.lang.String"
  ]
}
```

Contribution 2: Creating an agent that checks for class provenance



1. '*Log4Shell: The Log4j Vulnerability Emergency Clearly Explained | UpGuard*'. Available: https://www.upguard.com/blog/apache-log4j-vulnerability
2. M. Balliu et al., *'Challenges of Producing Software Bill of Materials for Java'*, IEEE Security & Privacy 2023.
3. S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff, *'A sense of self for Unix processes'*, in Proceedings 1996 IEEE Symposium on Security and Privacy.
4. M. Ohm, T. Pohl, and F. Boes, '*You Can Run But You Can't Hide: Runtime Protection Against Malicious Package Updates For Node.js*'. arXiv, May 31, 2023. doi: 10.48550/arXiv.2305.19760.

Personal Webpage