Attacking JavaEE Application Servers

Martin Toshev

Bulgarian Java Users Group (BG JUG):

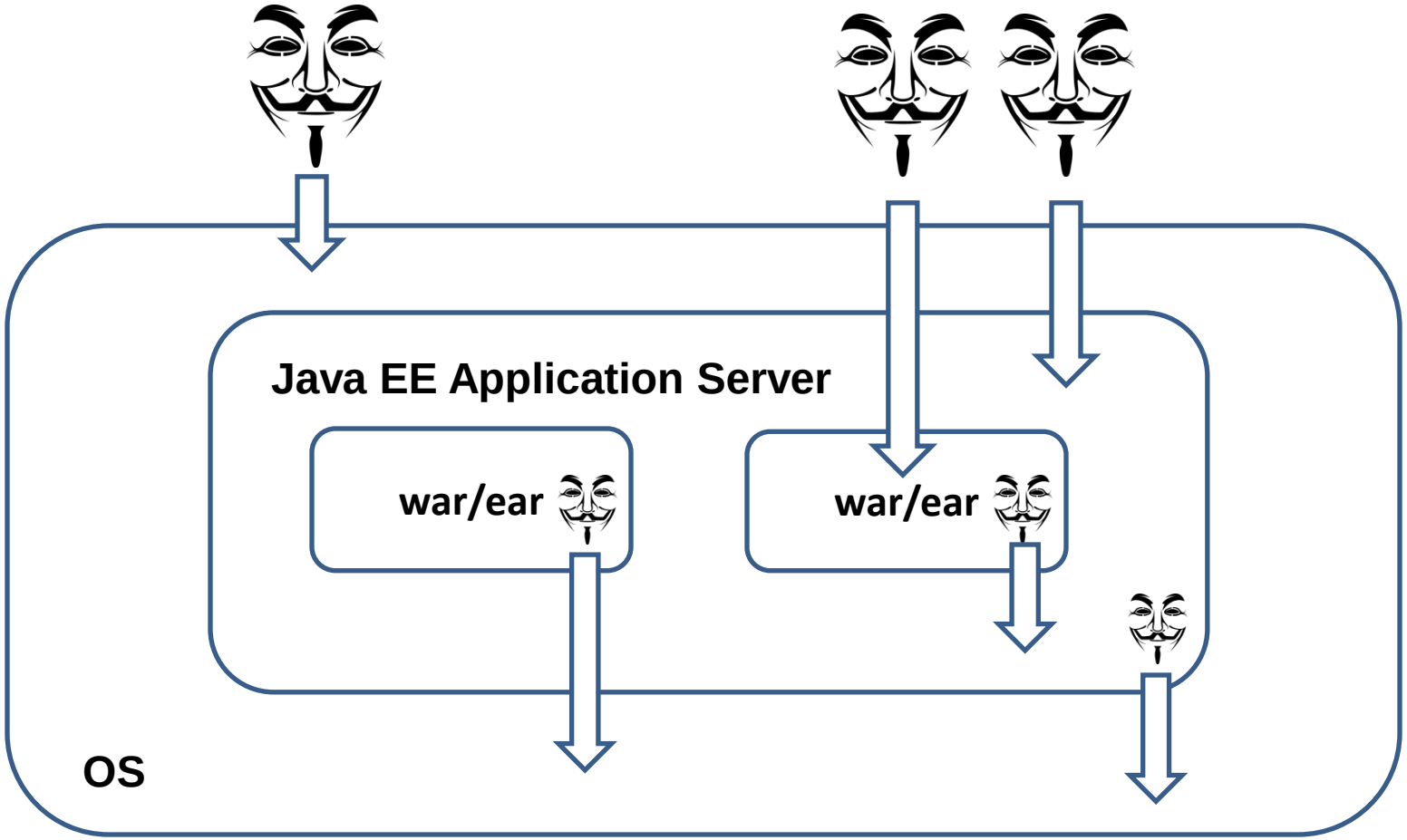
https://groups.google.com/forum/#!forum/bg-jug

http://java-bg.org/

Agenda

- Attack vectors
- Strategies and tools
- Secure coding and deployment

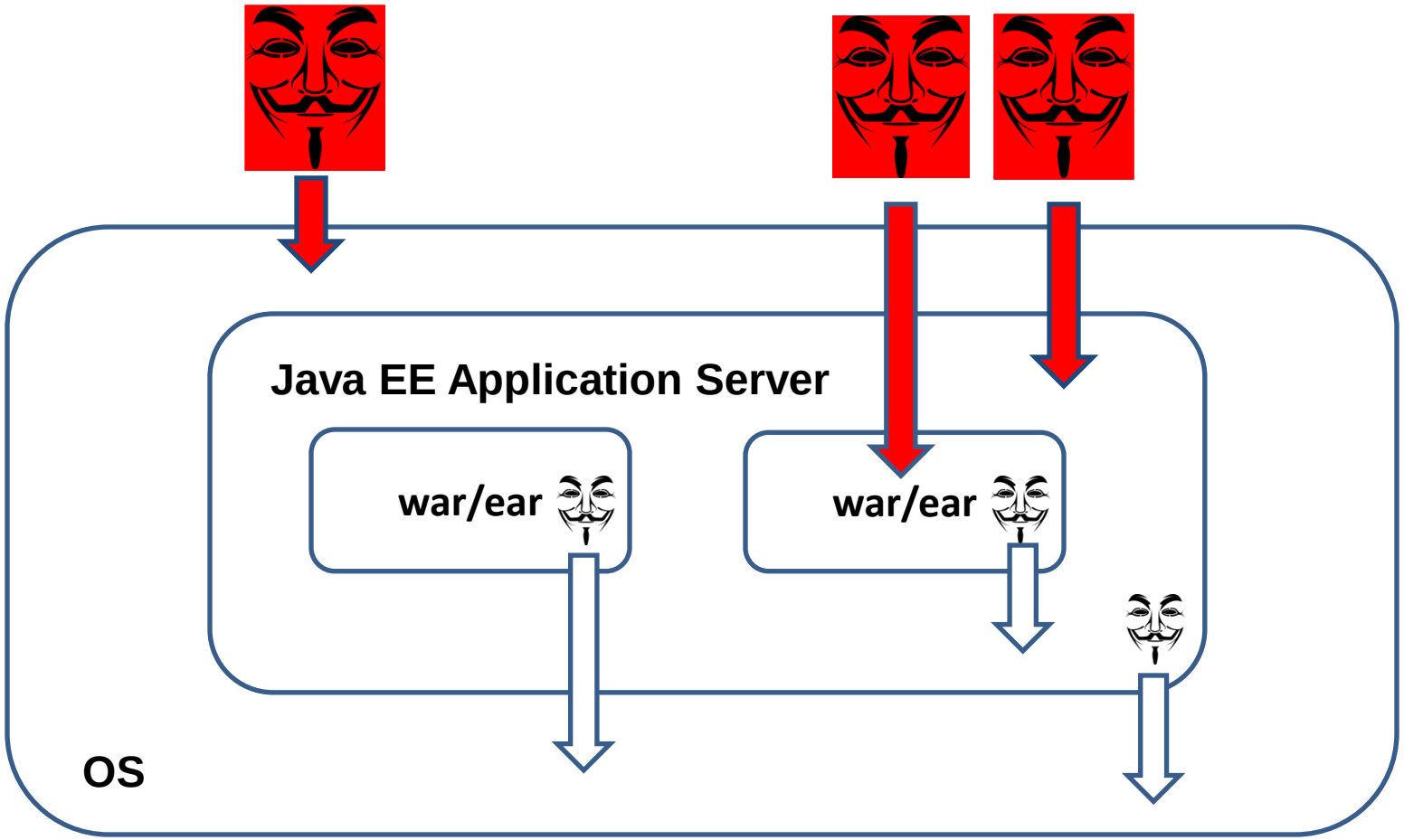
Attack Vectors



Attack Vectors

- An attack could be originating:
  - externally
  - from the application server itself
  - from an application

Attack Vectors



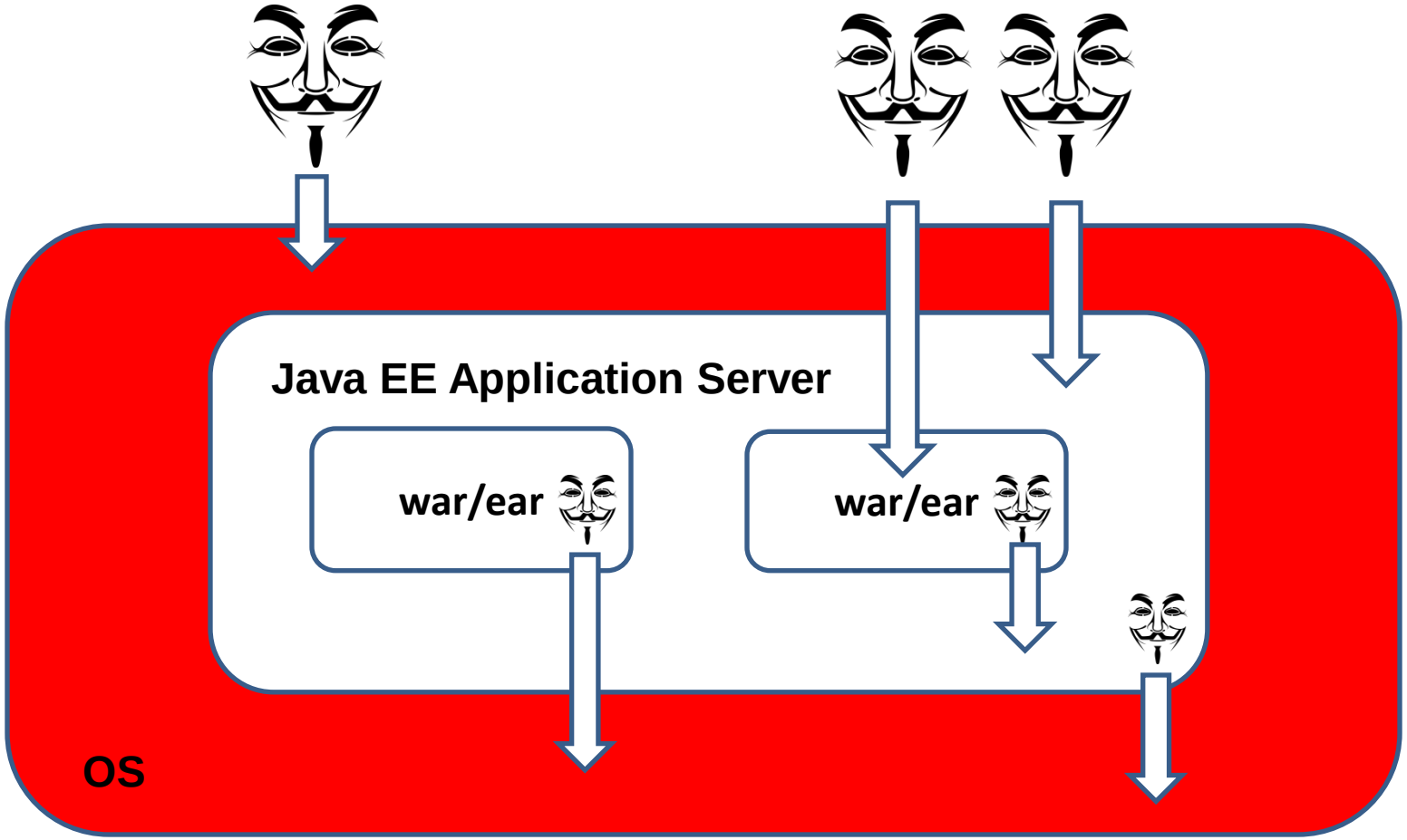
Attack Vectors

- An external attack can:
  - exploit directly remote services exposed by the JavaEE application server
  - exploit another remotely accessible process running in the OS

Attack Vectors

- An external attack can:
  - exploit input for applications deployed in the Java EE Server (such as input validation attacks, SQL injection, XSS …)

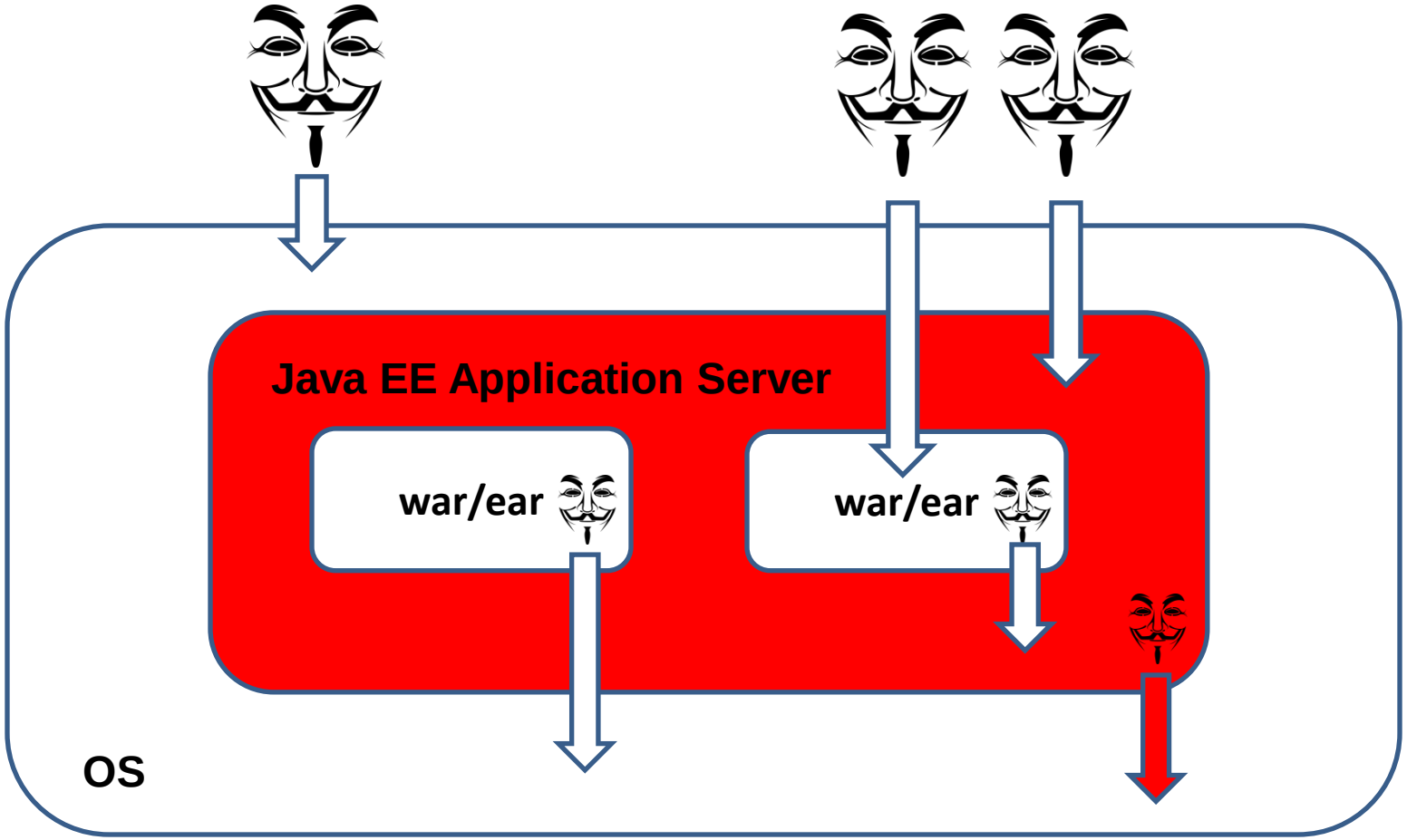
Attack Vectors



Attack Vectors

- An attack can:
  - originate from a malicious application running in the same OS
- Administrators do not always install from trusted sources or check against MD5 checksums …

Attack Vectors



Attack Vectors

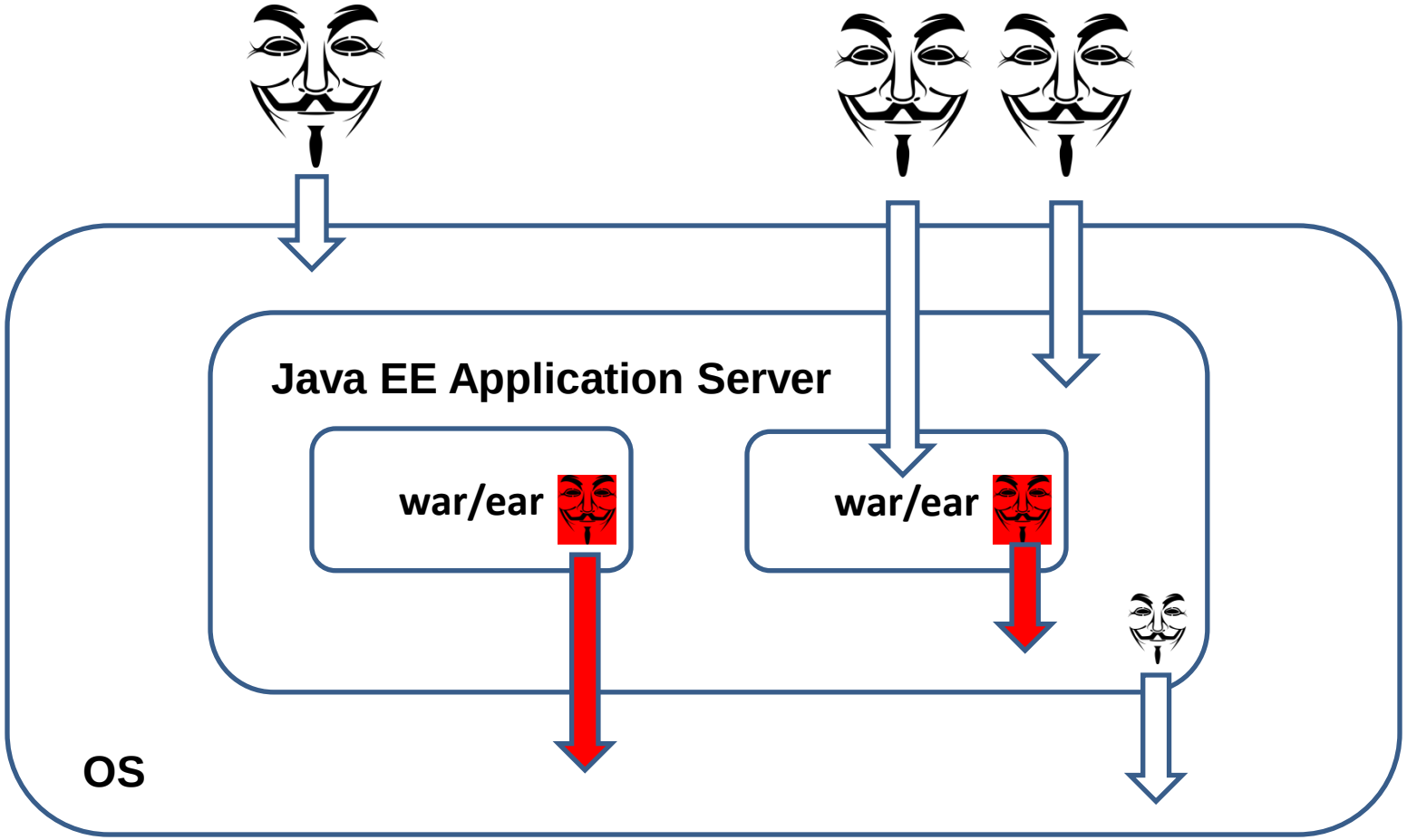
- An attack originating from the application server can:
  - be crafted by modifying the codebase and rebuilding the application server
  - be achieved more easily by targeting open-source application servers such as Glassfish and Wildfly

Attack Vectors

… Administrators do not always install JavaEE application servers from trusted sources or check against MD5 checksums …

… which makes this type of attacks a real scenario

Attack Vectors



Attack Vectors

- An attack originating from an application can be performed due to:
  - misconfigured security during deployment
  - intentional malicious code inside the application

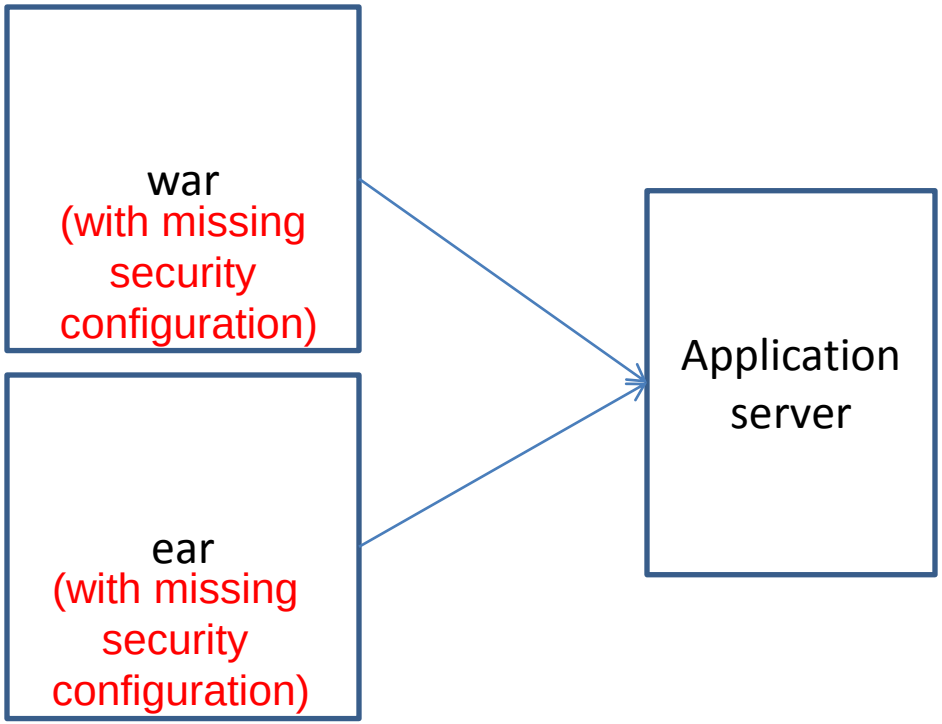
Attack Vectors

(scenario 1: misconfigured security in the app)

… leads to opening holes in the Java EE security model

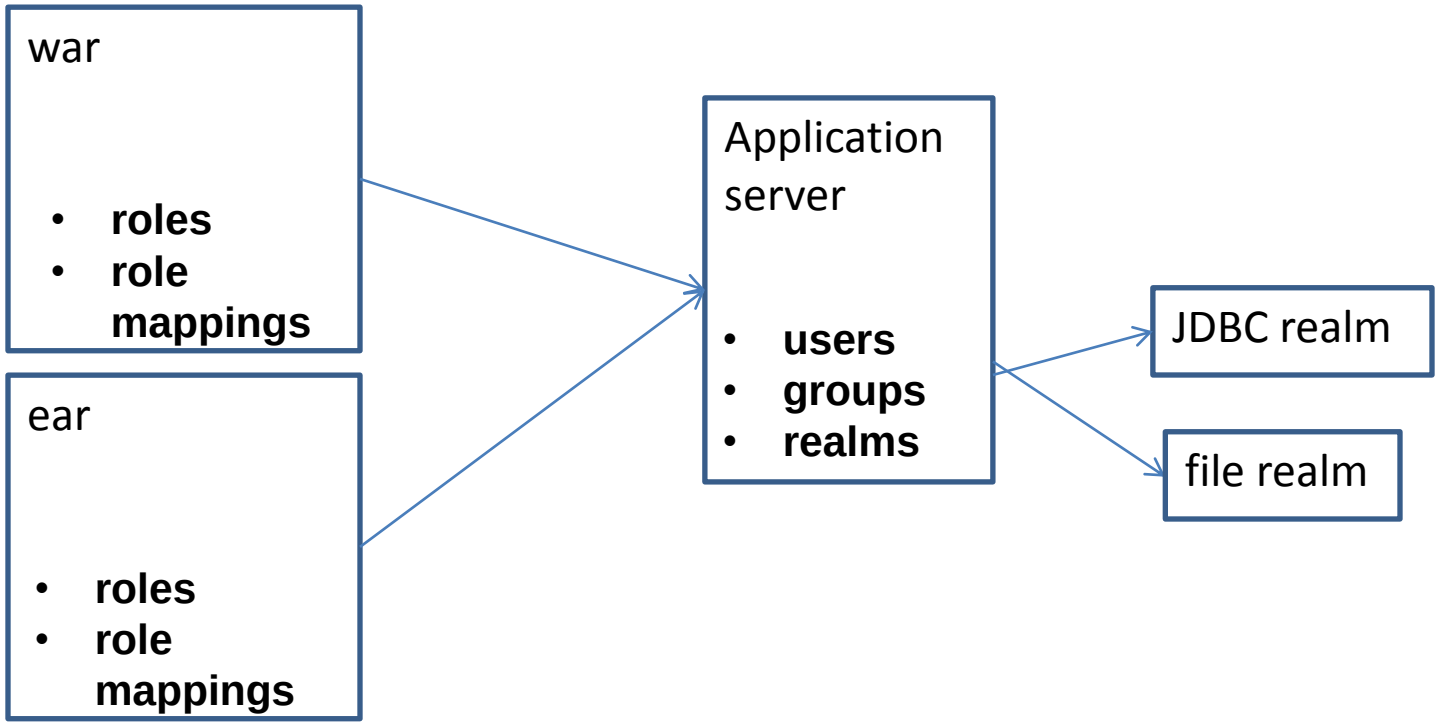
Attack Vectors

(scenario 1: misconfigured security in the app)



Attack Vectors

Java EE Security Model in a nutshell:



Attack Vectors

Java EE Security Model in a nutshell:

1. initial request is made

2. server authenticates the client using an authentication mechanism

3. URL authorization based on info from deployment descriptors or from annotations in source code is done

4. In case an EJB method is invoked the EJB container checks the appropriate permissions based on user roles
(the web container delegates information about the user and its roles to the EJB container)

Attack Vectors

Example:

```
import javax.annotation.security.DeclareRoles;
import javax.annotation.security.RolesAllowed;
...
@DeclareRoles({"MANAGER", "EMPLOYEE", "ADMIN"})
@Stateless
public class PaymentServiceImpl implements PaymentService {

// Jim: temporarily commented for testing purposes
// TODO: uncomment before  deployment on PROD
// @RolesAllowed("MANAGER")
public void increaseSalary(User employee, int ammount) {
        …
}
```

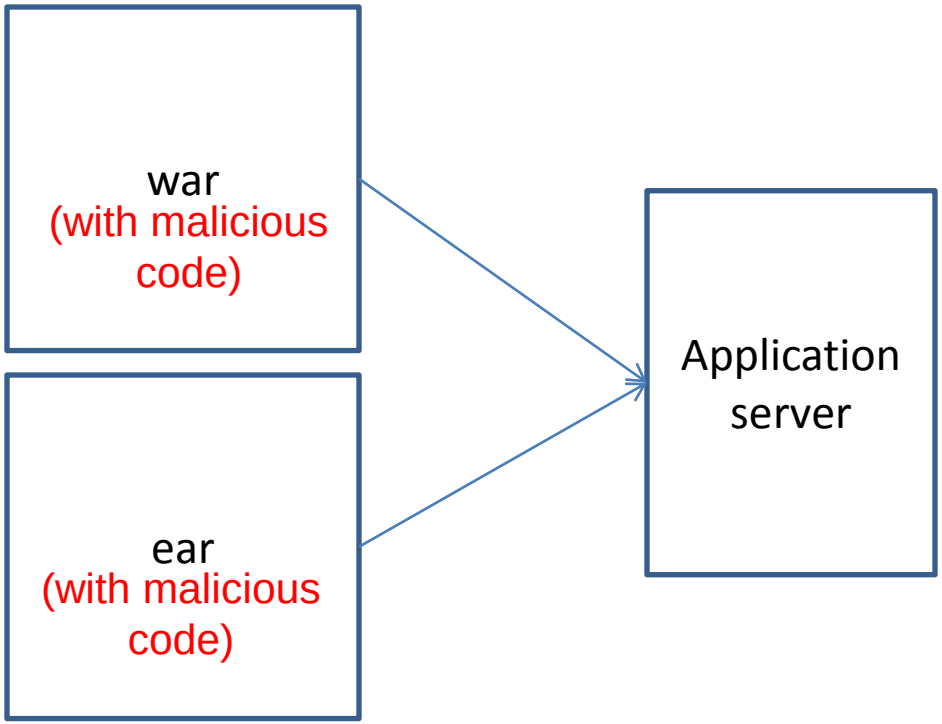
Attack Vectors

(scenario 2: malicious code in the app)

… can be made possible due to misconfiguration of the Java SE security model of the application server

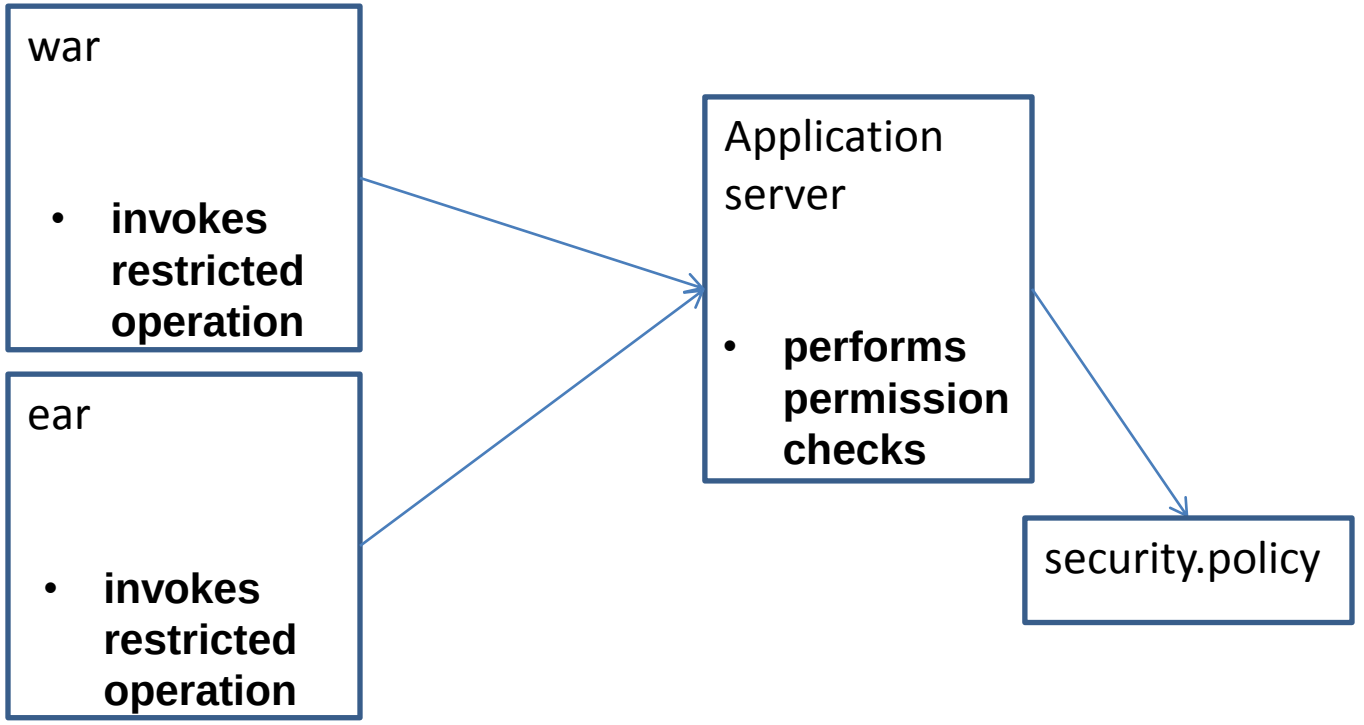
Attack Vectors

(scenario 2: malicious code in the app)



Attack Vectors

Java SE Security Model in a nutshell:



Strategies and Tools

(external)

Try to exploit services exposed by the OS or the application server (such as JMX)

Vulnerability databases such as **SecurityFocus**, **osvdb** and **nvd** and application server changelogs are valuable sources of information

Strategies and Tools

Tools:

- **network scanners** - Nmap, SATAN, Nessus, GFI LANguard, TripWire, SuperScan
- **remote system administration** - Back Office, ProRat
- **vulnerability scanners** - metasploit, w3af, Nexpose
- **MITM on the local network** - Ettercap

Strategies and Tools

… This Security Alert addresses the security issue CVE-2008-3257, a vulnerability in the Apache Connector component (mod_weblogic) of the Oracle Weblogic Server (formerly BEA WebLogic Server). This vulnerability may be remotely exploitable without authentication, i.e. it may be exploited over a network without the need for a username and password …

Strategies and Tools

… Unfortunately, the person(s) who published this vulnerability and associated exploit codes didn't contact Oracle before publicly disclosing this issue. This means that the vulnerability was made public before providing Oracle an opportunity to develop an appropriate fix for this issue and notify its customers …

Affected versions: 6.1, 7.0, 8.1, 9.0, 9.1, 9.2, 10.0

Strategies and Tools

… Earlier community editions of JBoss allow you to use default authentication to the JMX server running on the server (shutting down the server via JMX is made possible to attackers) - CVE-2013-4810 …

Affected versions: 4x, 5x

Strategies and Tools

(ear/war)

- craft malicious code that bypasses code reviews and code analysis tools (and possibly open a "back-door" in the application server)

Strategies and Tools

(ear/war)

- make use of techniques for:
  - initialization of classes based on loadable services or configuration files
  - AOP weaving
  - servlet filters
  - annotation processors

Strategies and Tools

Tools:

… write your own …

Secure Coding and Deployment

- The OS:
  - secure the environment of your application server
  - always patch your OS with latest updates

Secure Coding and Deployment

- The application server:
  - check that application server comes from a trusted source (compare against true MD5 checksum)
  - disable unused services when installing application servers

Secure Coding and Deployment

- The application server:
  - always enable encryption for the remote services exposed by the application server
  - check the documentation of your application server on the default security manager and security policy enabled by the application server

Secure Coding and Deployment

- The application server:
  - if necessary define proper security policy and define additional access control checks for the applications being deployed
  - always apply security patches to your application server installation

Secure Coding and Deployment

- The ear/war:
  - allow minimum set of permissions to roles in the application context
  - follow best security practices as defined by the Secure Coding Guidelines for Java SE

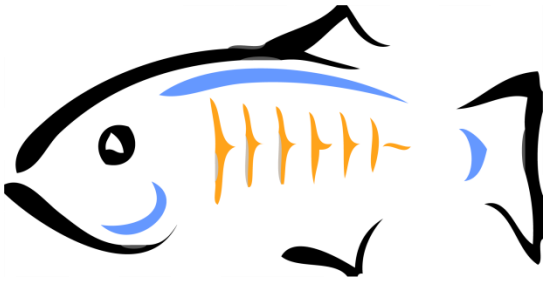
Secure Coding and Deployment

- The ear/war:
  - perform static & dynamic code analysis in order to find possible bugs or resource leaks (that may lead to implicit DoS)
  - do not leave behind test/unused URLs

Secure Coding and Deployment

- The ear/war:
  - perform in-container security policy tests (e.g. using Cactus or Arquillian frameworks …)
  - perform in-container resource consumption tests

Go ahead and try to find leaks …



9.0.0.Alpha1 **4.1** **12.1.3**


DAYS
CLOUD Days
mobile day
3 CONFERENCES
2 DAYS
1 PLACE
17-19 NOVEMBER 2014
INTER EXPO CENTER (IEC), SOFIA

Thank you

References

Java EE 7 tutorial part X: Security

https://docs.oracle.com/javaee/7/tutorial/doc/

Java Platform, Enterprise Edition (JavaEE) Specification, v7

http://download.oracle.com/otndocs/jcp/java_ee-7-fr-eval-spec/index.html

References

Back door into JavaEE application servers
macaron.googlecode.com/files/en-macaron.pdf

OWASP Top 10 for JavaEE
https://www.owasp.org/images/8/89/OWASP_Top_10_2007_for_JEE.pdf

Attacking Jboss like a boss
https://www.defcon.org/images/defcon-18/dc-18-presentations/Krpata/DEFCON-18-Krpata-Attacking-JBoss.pdf

References

Oracle Security Alert for CVE-2008-3257
http://www.oracle.com/technetwork/middleware/ias/downloads/alert-cve2008-3257-088842.html

Securing a WebLogic Server deployment
https://docs.oracle.com/cd/E13222_01/wls/docs61/security/lockdown.html

Whitepaper on Jboss exploitation
http://securityxploded.com/JBoss%20Whitepaper.pdf

References

Java Security Overview (white paper)

http://www.oracle.com/technetwork/java/js-white-paper-149932.pdf

Java SE Platform Security Architecture Spec

http://docs.oracle.com/javase/7/docs/technotes/guides/security/spec/security-spec.doc.html

Inside Java 2 Platform Security, 2nd edition

http://www.amazon.com/Inside-Java%C2%BF-Platform-Security-Implementation/dp/0201787911

References

Java Security, 2nd edition, Scott Oaks

http://shop.oreilly.com/product/9780596001575.do

Securing Java, Gary McGraw, Ed Felden

http://www.securingjava.com

Secure Coding Guidelines for Java SE

http://www.oracle.com/technetwork/java/seccodeguide-139067.html#0

References

Java 2 Network Security

http://www.amazon.com/JAVA-Network-Security-2nd-Edition/dp/0130155926

Java Security Documentation

http://docs.oracle.com/javase/8/docs/technotes/guides/security/index.html

References

Core Java Security: Class Loaders, Security Managers and Encryption

http://www.informit.com/articles/article.aspx?p=1187967

Overview of Java Security Models

http://docs.oracle.com/cd/E12839_01/core.1111/e10043/introjps.htm#CHDCEJGH