Seguridad 101 JavaEE - OWASP Top 10

Víctor Orozco - @tuxtor

11 de mayo de 2018

Nabenik

Víctor Orozco

- Developer (JVM/Open Source Advocate)
- Ex-becario OEA-GCUB
- Consultor @ Nabenik
- Speaker @ JavaOne, DevNexus, FISL, etc.
- @tuxtor
- http://vorozco.com
- http://tuxtor.shekalug.org

Principios básicos

- No existe un framework generico para hacer ”seguridad 360”
- Seguridad = Balance entre necesidad de negocio/tecnología
- En Java hay n formas de hacer lo mismo
- Requerimientos -> Cifrado, firmas digitales, autenticación, autorización
- Herramientas

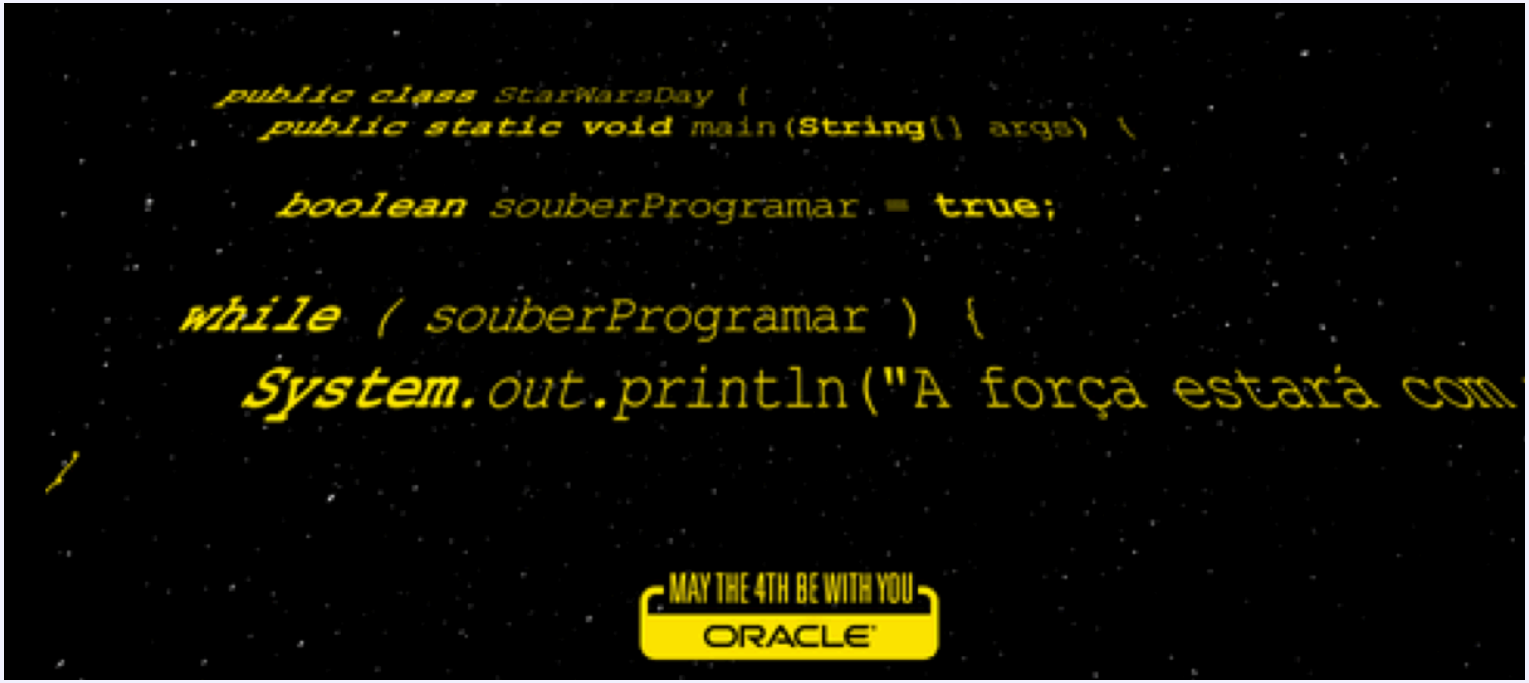
Definiciones básicas

We use cookies to analyse our traffic and to show ads. By using our website, you agree to our use of cookies.

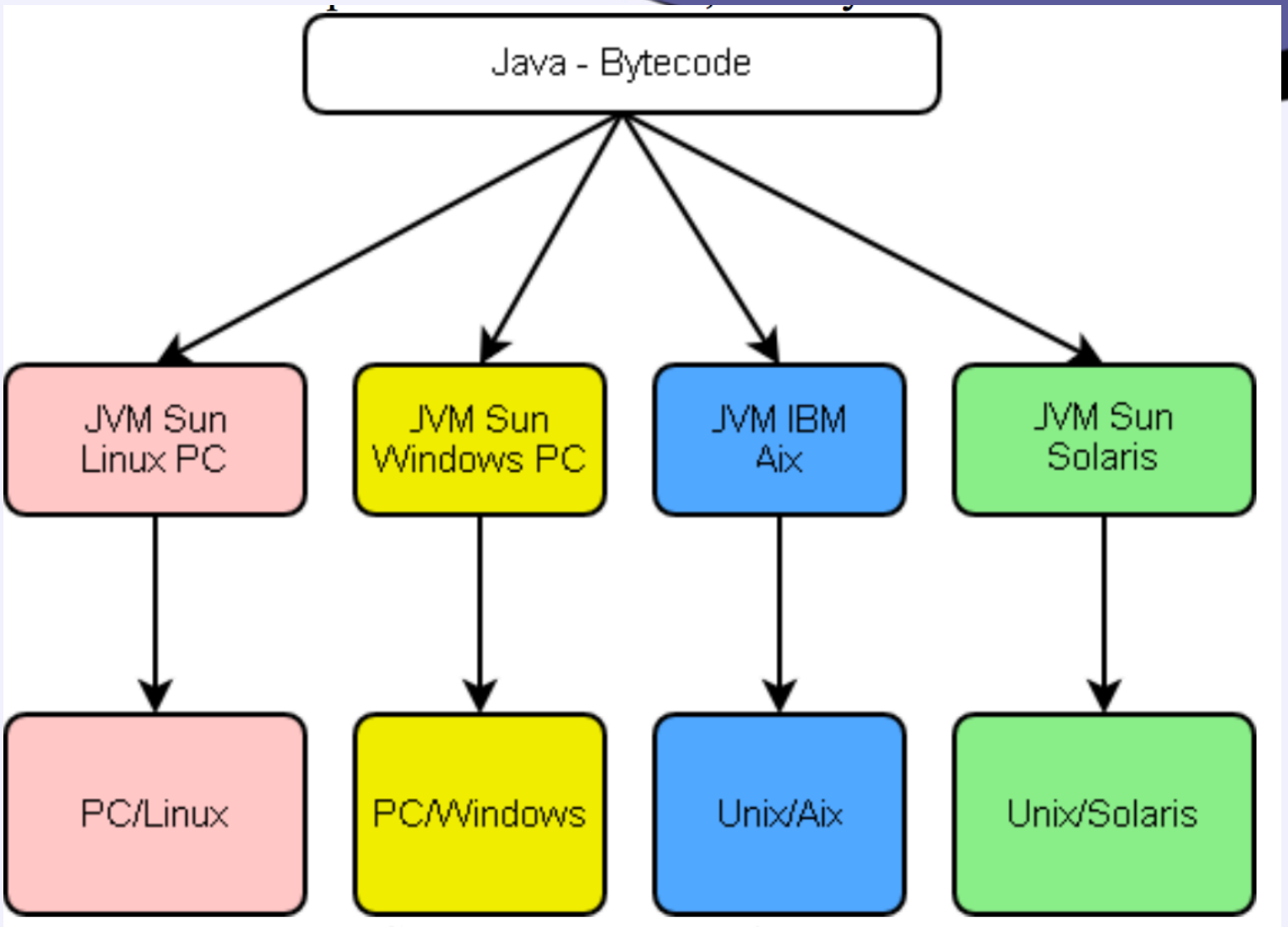
1	1		Java
2	2		C
3	3		C++
4	5	^	C#
5	8	^	Python
6	7	^	PHP
7	6	v	JavaScript
8	12	^^	Perl
9	18	^^	Ruby
10	10		Visual Basic .NET

¿Que es Java?

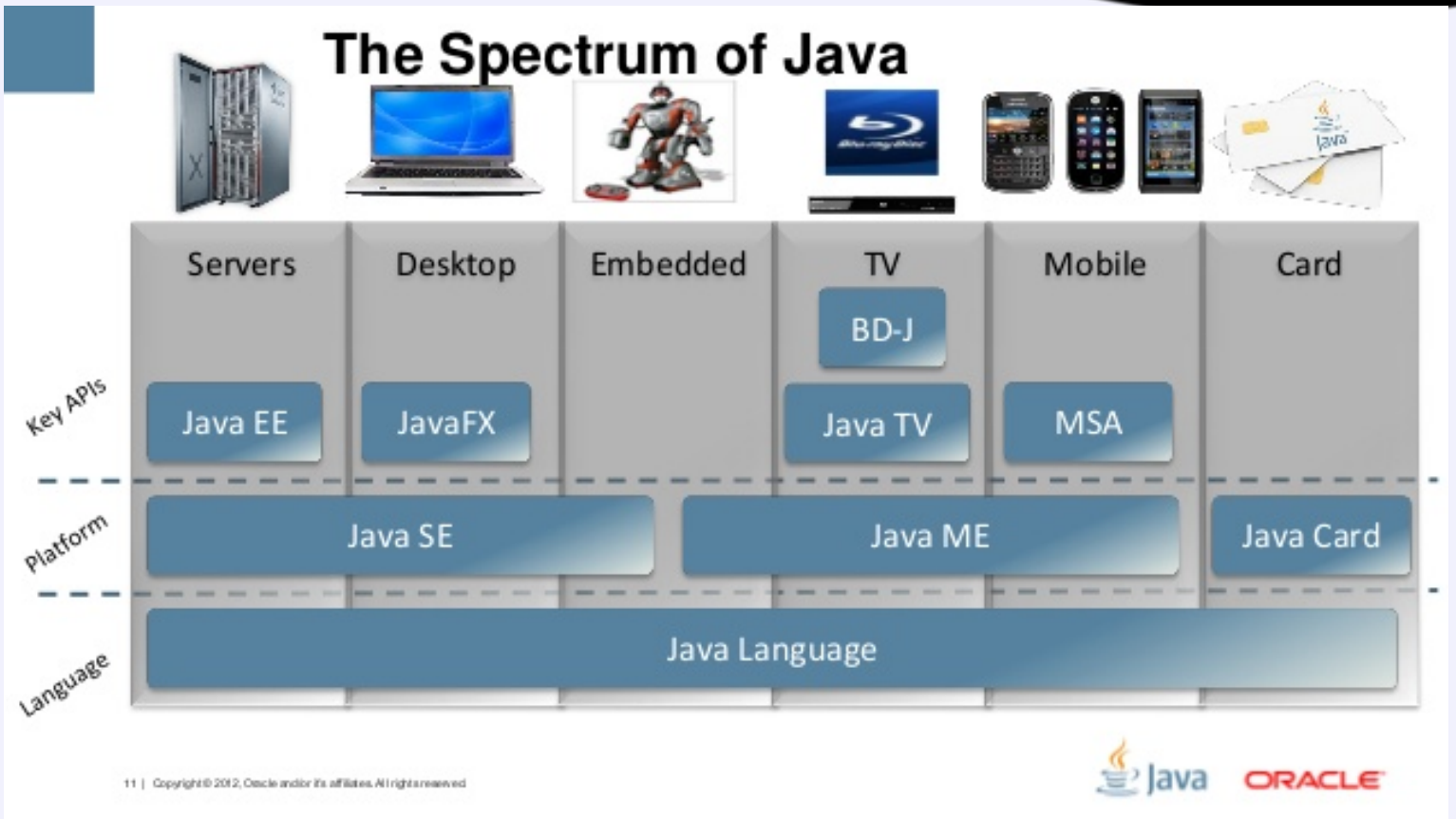
Lenguaje


public class StarWarsDay {
public static void main(String[] args) {
boolean souberProgramar = true;
while (souberProgramar) {
System.out.println("A força estará com
}
MAY THE 4TH BE WITH YOU
ORACLE

Maquina virtual



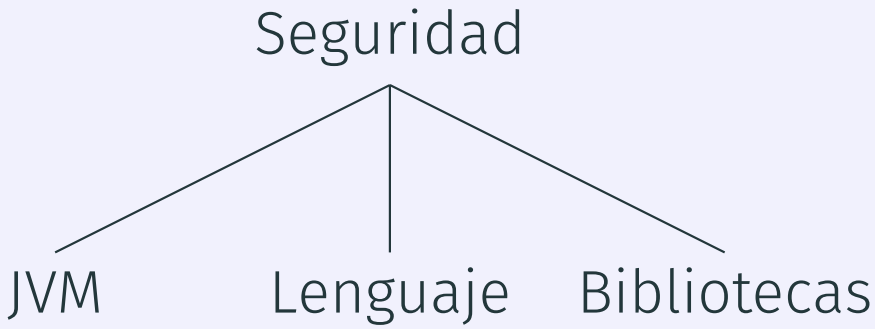
Muchas plataformas



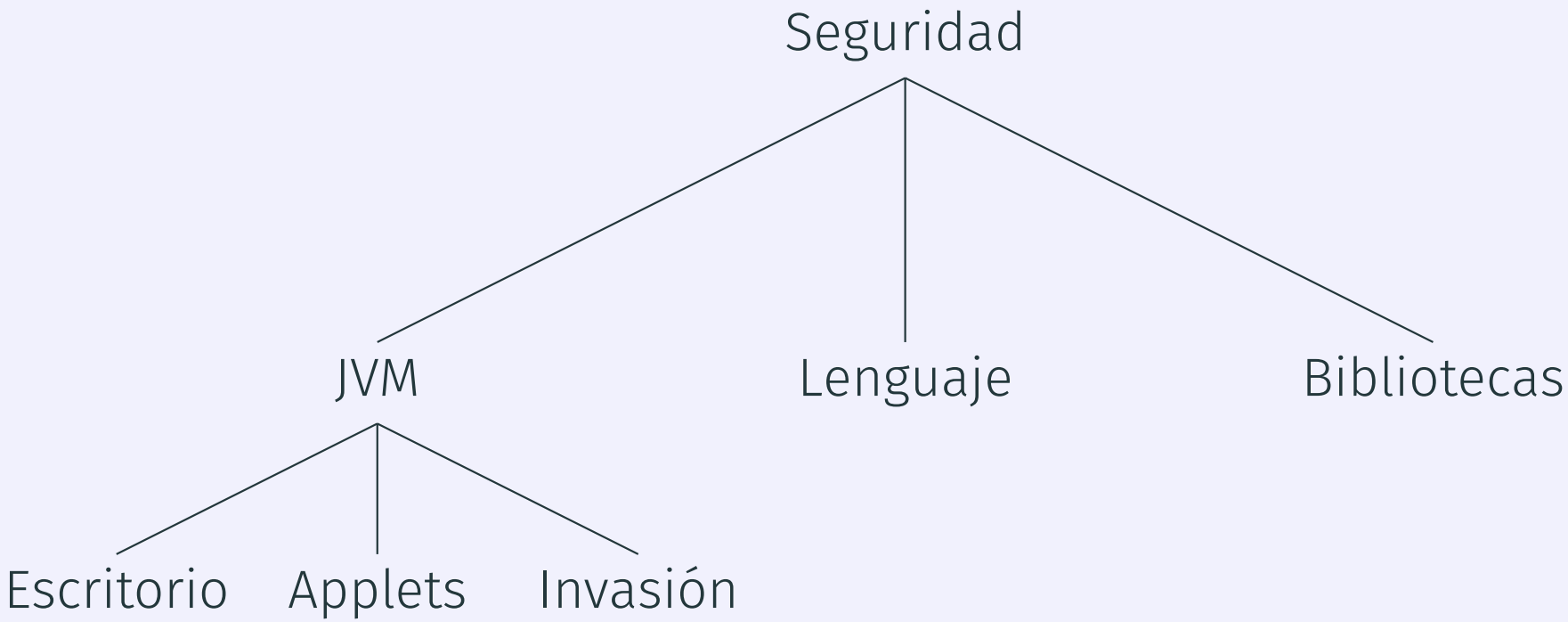
Seguridad en Java

Infosec

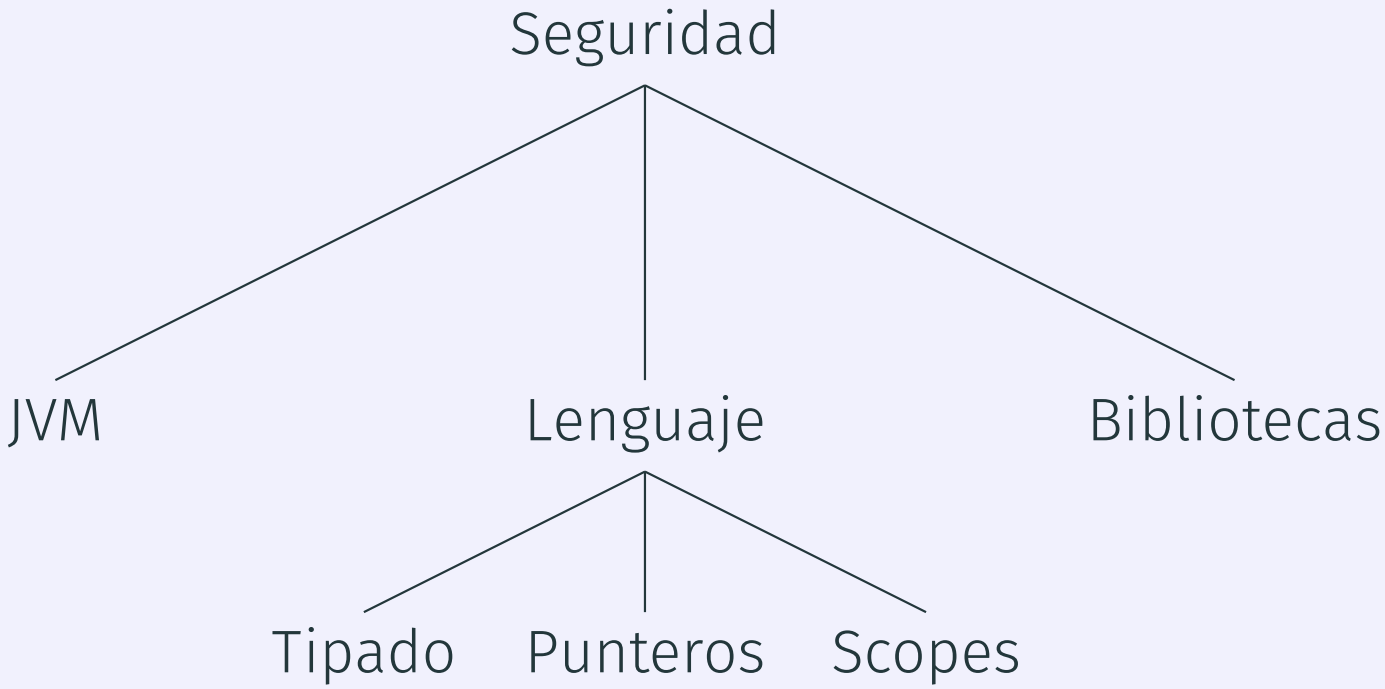
Seguridad



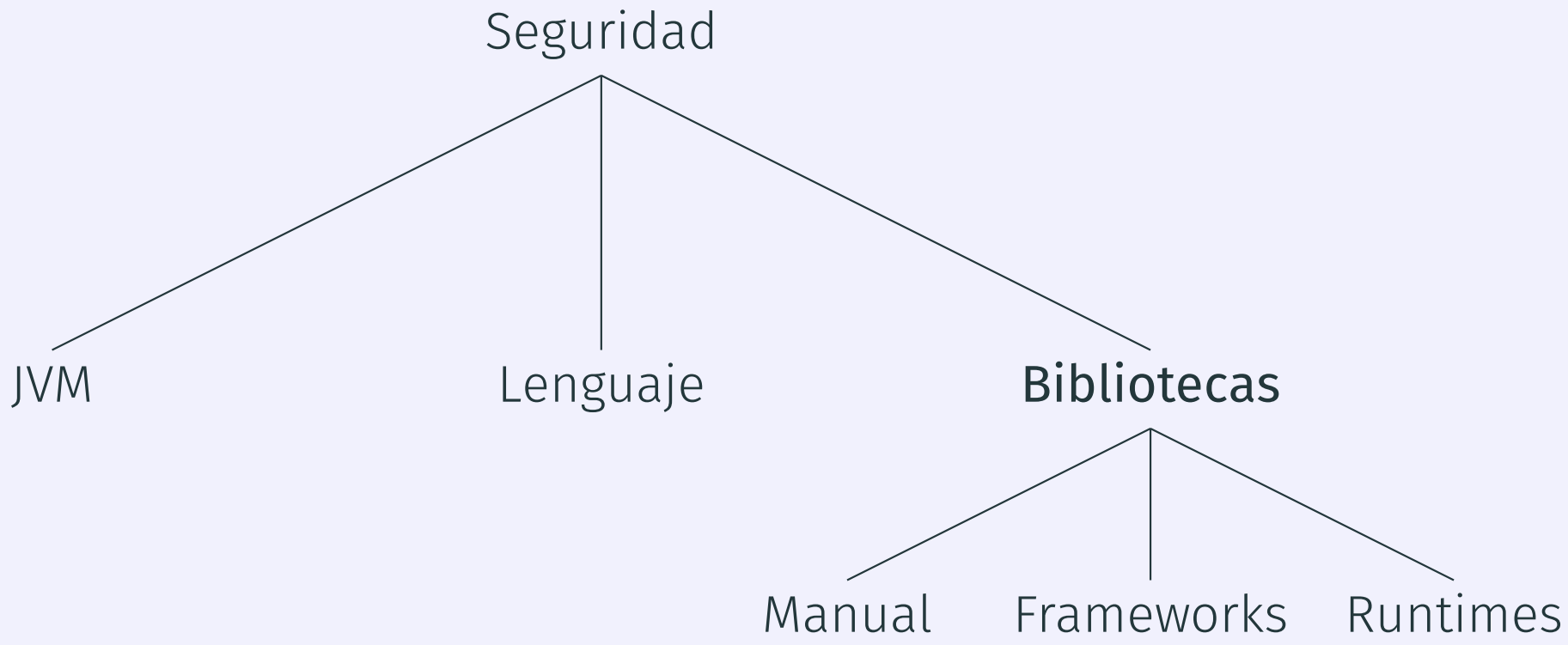
Seguridad


Seguridad
JVM
Lenguaje
Bibliotecas
Escritorio
Applets
Invasión

Seguridad


Seguridad
JVM
Lenguaje
Bibliotecas
Tipado
Punteros
Scopes

Seguridad


Seguridad
JVM
Lenguaje
Bibliotecas
Manual
Frameworks
Runtimes

Bibliotecas

¿Cual?

- Apache Shiro
- Spring Security
- OACC
- Picketlink
- Keycloak
- JGuard
- JACC
- SoteriaRI

. . .

Tecnologias Web

Render en servidor

- JSF (Icefaces, Primefaces)
- GWT
- JSP
- Servlets
- Vaadin
- Struts
- Spring MVC

Tecnologias Web

Render en servidor

- JSF (Icefaces, Primefaces)
- GWT
- JSP
- Servlets
- Vaadin
- Struts
- Spring MVC

Render en cliente

- Angular
- React
- Knockout (Oracle JET)
- Vue

Tecnologias Web

Render en servidor

- JSF (Icefaces, Primefaces)
- GWT
- JSP
- Servlets
- Vaadin
- Struts
- Spring MVC

Render en cliente

- Angular
- React
- Knockout (Oracle JET)
- Vue

Servicios

- SOAP
- Rest
- RMI

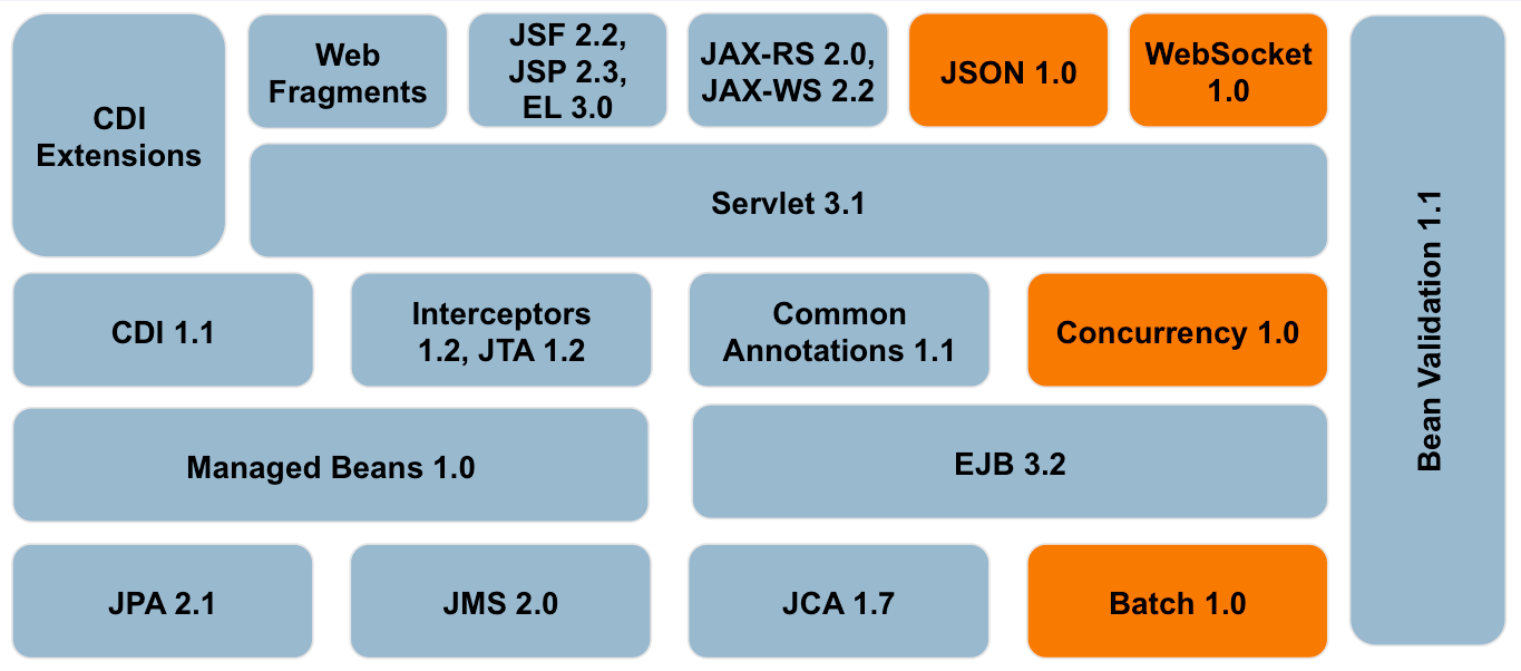
Tecnología


solaris
redhat
ORACLE
LINUX
debian
CentOS
ORACLE
PostgreSQL
MySQL
mongoDB
Java
ENTERPRISE
EDITION
JBoss
by Red Hat
GlassFish
WildFly
payara

JavaEE 7

- API Rest - JAX-RS 2.0
- WebSocket - WebSocket 1.0, Servlet 3.1
- JSON - JSON API 1.0
- SOA, Microservices

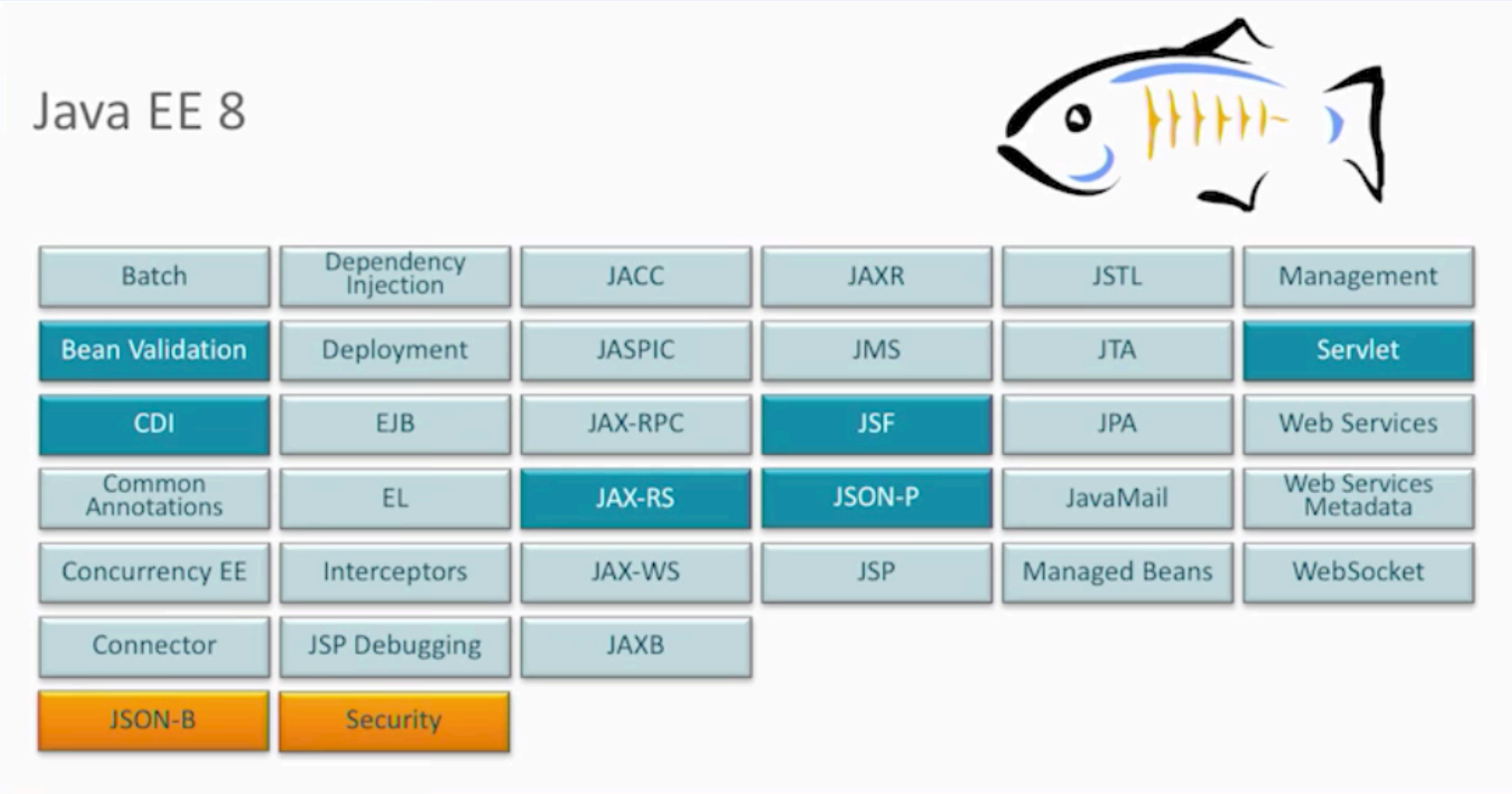
JavaEE 7


CDI Extensions
Web Fragments
JSF 2.2, JSP 2.3, EL 3.0
JAX-RS 2.0, JAX-WS 2.2
JSON 1.0
WebSocket 1.0
Servlet 3.1
CDI 1.1
Interceptors 1.2, JTA 1.2
Common Annotations 1.1
Concurrency 1.0
Managed Beans 1.0
EJB 3.2
JPA 2.1
JMS 2.0
JCA 1.7
Batch 1.0
Bean Validation 1.1

JavaEE 8

- Mejor integración de JSF con CDI
- Mejor integración de JMS con CDI
- HTTP/2
- JSON-B
- Security
- JAX-RS Reactivo

JavaEE 8


Java EE 8
Batch
Dependency Injection
JACC
JAXR
JSTL
Management
Bean Validation
Deployment
JASPIC
JMS
JTA
Servlet
CDI
EJB
JAX-RPC
JSF
JPA
Web Services
Common Annotations
EL
JAX-RS
JSON-P
JavaMail
Web Services Metadata
Concurrency EE
Interceptors
JAX-WS
JSP
Managed Beans
WebSocket
Connector
JSP Debugging
JAXB
JSON-B
Security

EE vs OWASP Top 10

Advertencia

- Visto en N desarrollos
- Un punto de inicio
- Informar

JavaEE

- A1-Injection
- A2-Broken Authentication and Session Management
- A3-Sensitive Data Exposure
- A4-XML External Entities
- A5-Broken Access Control
- A6-Security Misconfiguration
- A7-Cross-Site Scripting (XSS)
- A8-Insecure deserialization
- A9-Using Components with Known Vulnerabilities
- A10-Insufficient Logging y Monitoring

`https://www.owasp.org/index.php/Top_10_2017-Top_10`

JavaEE

- A1-Injection
- A2-Broken Authentication and Session Management
- A3-Sensitive Data Exposure
- A4-XML External Entities
- A5-Broken Access Control
- A6-Security Misconfiguration
- A7-Cross-Site Scripting (XSS)
- A8-Insecure deserialization
- A9-Using Components with Known Vulnerabilities
- A10-Insufficient Logging y Monitoring

`https://www.owasp.org/index.php/Top_10_2017-Top_10`

JavaEE - A1 - Injection

Problemas y causas comunes

- Concatenación de Strings en SQL
- Datos mal intencionados a aplicaciones
- Manipulación data stores
- Escalar privilegios

Sugerencias

- JAMAS y NUNCA concatenar parametros
- Siempre utilizar mecanismos de `sanitizing`
- Parchar con OWASP ESAPI
- JDBC y JPA soportan de serie sanitizing si no se concatena
- Bean Validation en parametros

JavaEE - A2-Broken Authentication and Session Management

Problemas y causas comunes

- Implementación de solución manual vs frameworks
- Falta de políticas
- Entrenamiento en la plataforma
- Comunicación y/o autenticación via http

Sugerencias

- Forzar https
- Utilizar adecuadamente los ciclos de vida de la plataforma (singleton != stateless != statefull) y cache
- No implementar en base a interceptores

JavaEE - A3-Sensitive data exposure

Problemas y causas comunes

- Guardar datos sin cifrar
- Datos con cifrado ”debil”, AKA cifrado propio
- Transmitir credenciales via http
- Transmisión de excepciones completas a front-end

Sugerencias

- Identificar con un checklist los datos sensitivos
- Evitar cifrado de dos vías a menos que sea necesario
- Evitar transmisión de llaves
- Verificar código auto generado (excepciones)

JavaEE - A5-Broken Access Control

Problemas y causas comunes

- Implementación de solución manual vs frameworks
- Falta de políticas
- Escalar privilegios
- Comunicación y/o autenticación via http

Sugerencias

- Forzar https
- Implementación RBAC de application server
- Implementación RBAC de framework
- Entender el modelo de JAAS y SoteriaRI

JavaEE - A6-Security Misconfiguration

Problemas y causas comunes

- Configuración por defecto de applicaction server
- Configuración por defecto de SO
- Configuración `relajada` de capa de transporte

Sugerencias

- Configurar siempre el SO destino
- Proteger Glassfish
- Firewall
- RBAC
- Evitar certificados autofirmados en entornos no controlados
- JVM tipo `server`

JavaEE - A8-Insecure deserialization

Problemas y causas comunes

- Self made frameworks
- No validation

Sugerencias

- Evaluar si no vale la pena utilizar un software listo
- Bean validation

JavaEE - A9-Using components with known vulnerabilities

Problemas y causas comunes

- Difícil dar seguimiento a los lanzamientos
- Frameworks muy nuevos o muy viejos
- No seguir las notas del lanzamiento

Sugerencias

- Actualizar el app server con el calendario de lanzamiento
- Suscripción a mailing list/foros
- Servicios tipo Bintray
- Servicios de análisis estático (Sonar)

JavaEE - Bonus-APIs sin proteger

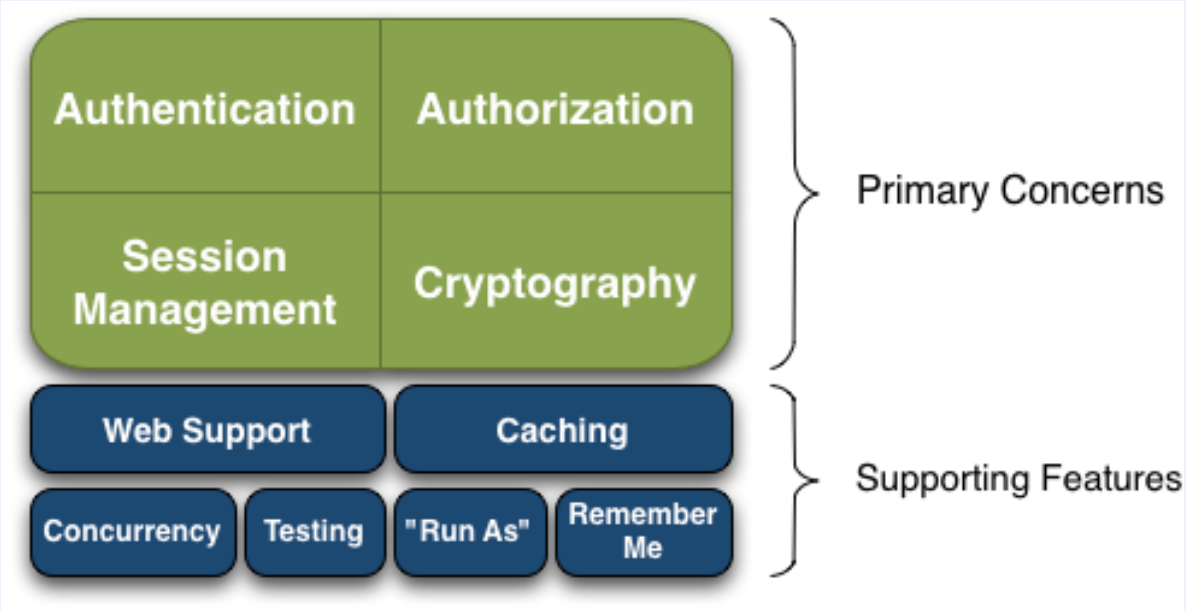
Problemas y causas comunes

- Combinación de broken auth, broken access control o security misconfiguration
- No hay nada
- Especialmente grave en rich clients

Sugerencias

- Verificar código auto generado
- Programar en modo `deny all`

Apache Shiro



Apache Shiro

- Java Authentication and Authorization Service - JAAS
- RBAC
- Autenticación
- Autorización
- Cifrado

Apache Shiro - Taxonomia

- Permission
- Principal (generic attribute)
- Subject (user)
- Credential
- Realm
- Role
- Session

Fin

Gracias

- me@vorozco.com vorozco@nabenik.com
- http://vorozco.com
- http://github.com/tuxtor/slides