

Arquitectura e Integración de Aplicaciones Empresariales

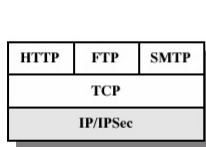
Novena Sesión Protocolos de Seguridad

Universidad Autónoma Metropolitana
Casa abierta al tiempo  Azcapotzalco

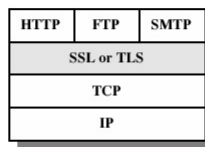
Dra. Maricela Bravo
Cubículo H-287-B
mari_clau_18@hotmail.com

¿Dónde ofrecer Seguridad?

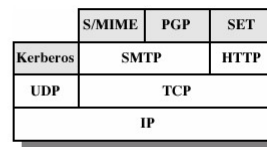
- Discusión bizantina sin respuesta final



(a) Network Level



(b) Transport Level



(c) Application Level



Conceptos generales

- ▶ Llaves pública/privada:
- ▶ Información encriptada con una llave solo puede ser desencriptada por su par.
- ▶ La base es mantener una llave guardada y distribuir la otra.
- ▶ El par de llaves está basado en un número primo.

Conceptos Generales

- ▶ Llave Simétrica:
- ▶ Usa la misma llave para encriptar y desencriptar (más práctico)
- ▶ Mucho más veloz que algoritmo asimétrico.
- ▶ Potencialmente inseguro.
- ▶ Transmitir llave simétrica con ayuda de algoritmos asimétricos.

Conceptos Generales

- ▶ Certificado Digital:
- ▶ Certifica que una persona o entidad es quien dice ser.
- ▶ Dirección de Correo, nombre, uso del certificado, ID de entidad que lo firma.
- ▶ CA almacenados en Navegador.
- ▶ Todo certificado es no confiable si no se ha firmado.

Protocolos de Seguridad

- ▶ HTTP no es un protocolo seguro
- ▶ Es simple y no se establece un estado cliente/servidor. Ejecuta sobre TCP/IP
- ▶ Es necesario instrumentar medidas de seguridad
 - ▶ SSL (Secure Socket Layer)
 - ▶ TLS (Transport Layer Security)
 - ▶ HTTPS
- ▶ Protocolo seguro HTTP
- ▶ El uso de SSL se aplica también a otras capas TCP/IP, por ejemplo,
- ▶ POP3, SMTP, FTP, SSH, etc.

- ▶ Transport Layer Security (TLS)
- ▶ Secure Sockets Layer (SSL)
- ▶ Son protocolos criptográficos, que proporcionan comunicaciones seguras por una red, comúnmente Internet.
- ▶

SSL

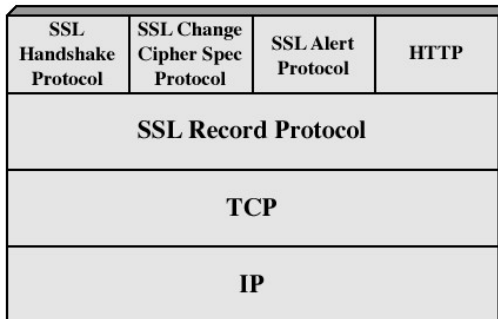
- ▶ SSL: Secure Sockets Layer, capa de sockets seguros.
- ▶ Establece un canal seguro en el nivel de transporte entre dos partes.
- ▶ Ofrece privacidad en las comunicaciones al utilizar cifrado con llave simétrica y usa códigos de autenticación de mensajes.

SSL

- ▶ SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, solo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.
- ▶ SSL implica una serie de fases básicas:
 - ▶ Negociar entre las partes el algoritmo que se usará en la comunicación
 - ▶ Intercambio de claves públicas y autenticación basada en certificados digitales.
 - ▶ Cifrado del tráfico basado en cifrado simétrico.
- ▶ Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:
 - ▶ Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza.
 - ▶ Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES y AES (Advanced Encryption Standard).
- ▶ Con funciones hash: MD5 o de la familia SHA.

Arquitectura SSL

- Utiliza TCP (transferencia de datos confiable)

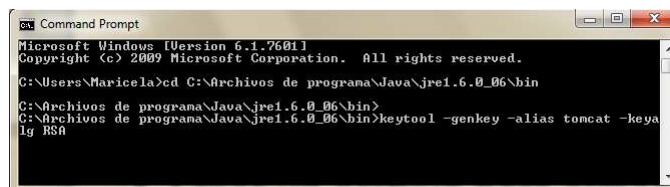


Instalación y configuración de SSL en Tomcat 8

Creación de la llave para el servidor

- ▶ Crear un archivo para almacenar la llave privada del servidor y un certificado auto-firmado (esto normalmente se solicita a una certificadora)

```
%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA
```



```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Maricela>cd C:\Archivos de programa\Java\jre1.6.0_06\bin
C:\Archivos de programa\Java\jre1.6.0_06\bin>
C:\Archivos de programa\Java\jre1.6.0_06\bin>keytool -genkey -alias tomcat -keyalg RSA
```

Proporcionar los datos para crear la clave

- ▶ La contraseña del almacén de claves (6 dígitos)
- ▶ Nombre y apellido
- ▶ Nombre de la unidad: Azcapotzalco
- ▶ Nombre de la organización: UAM
- ▶ Nombre de la ciudad o localidad
- ▶ Nombre del estado o provincia
- ▶ Código del país con dos letras

Buscar el archivo *.keystore

```

Command Prompt - keytool -genkey -alias tomcat -keyalg RSA
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

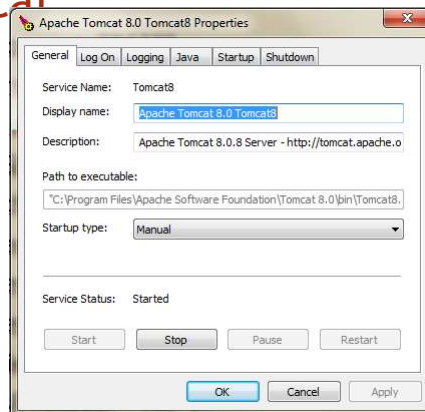
C:\Users\Maricela>cd G:\Archivos de programa\Java\jre1.6.0_06\bin
C:\Archivos de programa\Java\jre1.6.0_06\bin>keytool -genkey -alias tomcat -keyalg RSA
Escriba la contraseña del almacén de claves:
Desea o escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  Unknown: Maricela Bravo
¿Cuál es el nombre de su unidad de organización?
  Unknown: UAM
¿Cuál es el nombre de su organización?
  Unknown: Azcapotzalco
¿Cuál es el nombre de su ciudad o localidad?
  Unknown: Distrito Federal
¿Cuál es el nombre de su estado o provincia?
  Unknown: Distrito Federal
¿Cuál es el código de país de dos letras de la unidad?
  Unknown: MX
¿Es correcto C:\Users\Maricela\Bravo, OU=UAM, O=Azcapotzalco, L=Distrito Federal, ST=Distrito Federal, C=MX?
  Unknown:
  (no):
  
```

- ▶ Tomcat solamente opera con formatos de llave JKS, PKCS11 o PKCS12.
- ▶ El formato de JKS es el estándar de java “Java Keystore”, y es el formato creado por el comando keytool.

Abrir, modificar y guardar el archivo de configuración del servidor conf/server.xml

```
<Connector port="8443"  
  protocol="org.apache.coyote.http11.Http11NioProtocol"  
  maxThreads="200"  
  SSLEnabled="true"  
  scheme="https"  
  secure="true"  
  keystoreFile="C:/Users/Maricela/.keystore"  
  keystorePass="123456"  
  clientAuth="false"  
  sslProtocol="TLS" />
```

Detener y reiniciar el servicio de Tomcat



Probar en el navegador con: https://localhost:8443



This Connection is Untrusted

You have asked Firefox to connect securely to **localhost:8443**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

Agregar la excepción



This Connection is Untrusted

You have asked Firefox to connect securely to **localhost:8443**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

[Add Exception...](#)

Agregar la excepción



Finalmente

