Alumne: Javier Díaz Espejo
Consultora: Cristina Pérez Solà
Data: 11 de gener de 2015

JAVIER DIAZ ESPEJO

Firmado digitalmente por JAVIER DIAZ ESPEJO
Fecha: 2016.01.26 17:21:23 +01'00'

Segon cicle d'enginyeria informàtica

Àrea – Seguretat informàtica

SportsTrackerSegur

Estructura de la presentació

1. Introducció
2. Possibles models d'atacants
3. Disseny
4. Implementació
5. Entorn de proves
6. Conclusions

1. Introducció

El projecte tracta sobre el desenvolupament d'una aplicació web segura per gestionar activitats esportives anomenada *Sports Tracker Segur*. En l'actualitat la pràctica d'esports és un hàbit molt comú per moltes persones que volen mantenir un estil de vida saludable.

Aquests tipus d'aplicacions treballen amb **dades sensibles** dels usuaris, i una pèrdua d'informació per part d'una aplicació pot generar un gran perjudici a una persona.

1.1 Objectiu

- Desenvolupament d'una aplicació web per gestionar activitats esportives d'una forma segura.

1.2 Estat de l'art

En l'actualitat en el mercat hi ha una gran diversitat d'aplicacions *sports tracker*, a causa del gran volum de dispositius mòbils intel·ligents apareguts en els últims anys.

Exemples d'aplicacions existents al mercat són: Connect de Garmin, Polar Flow de Polar, Runtastic, Endomondo, Runkeeper i un llarg etc.

La majoria d'aquestes aplicacions en la seva política de privacitat especifiquen el seu compromís de prendre les mesures adients per impedir un accés no autoritzat a les dades personals dels usuaris, però sense especificar quines tècniques apliquen.

2. Possibles models d'atacants

Abans d'iniciar el disseny de l'aplicació s'ha realitzat un estudi i anàlisi d'un conjunt de possibles tècniques conegudes que un possible atacant pot utilitzar en contra de l'aplicació.

2.1 Escolta de xarxa

L'escolta de xarxa consisteix a què un atacant és capaç d'interceptar tot el tràfic de dades que es produeix entre la víctima i el servidor de l'aplicació.

El protocol SSL (*Security Socket Layer*) i el TLS (*Transport Layer Security*) són els protocols criptogràfics de seguretat d'ús comú per a connexions amb pàgines web.

2.2 Suplantació de lloc web (*Web Spoofing*)

Un atacant es podria plantejar realitzar una clonació de pàgines web de la nostra aplicació, amb l'únic objectiu de fer creure a la víctima que està interactuant amb l'aplicació vertadera. En l'actualitat és un tipus d'atac bastant perillós i difícilment detectable, tot i què es poden prendre algunes mesures de prevenció.

2.3 Accés no autoritzat a la BD

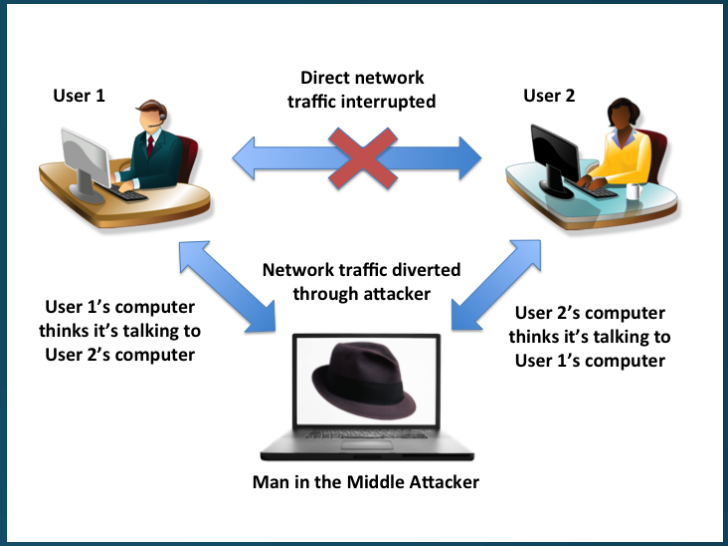
Evitar un possible accés a la BD per part de terceres persones des de la xarxa d'Internet, però també de les pròpies persones que puguin gestionar o tindre accés directe al servidor de la BD.

2.4 Enginyeria social

El concepte fa referència als atacs que es basen en intentar fer creure alguna cosa a l'usuari per a què aquest de forma voluntària li faciliti les pròpies credencials a l'atacant.

2.5 Atac d'home en el mig (MITM)

Un atacant és capaç de desviar el tràfic de la víctima per a què passi pel seu propi ordinador, i tornar a redirigir-lo al seu destí original.



2.6 Atac de denegació de servei (DoS)

Té com objectiu principal un sistema de computadors o xarxa per a què els seus serveis siguin inaccessibles als usuaris legítims.

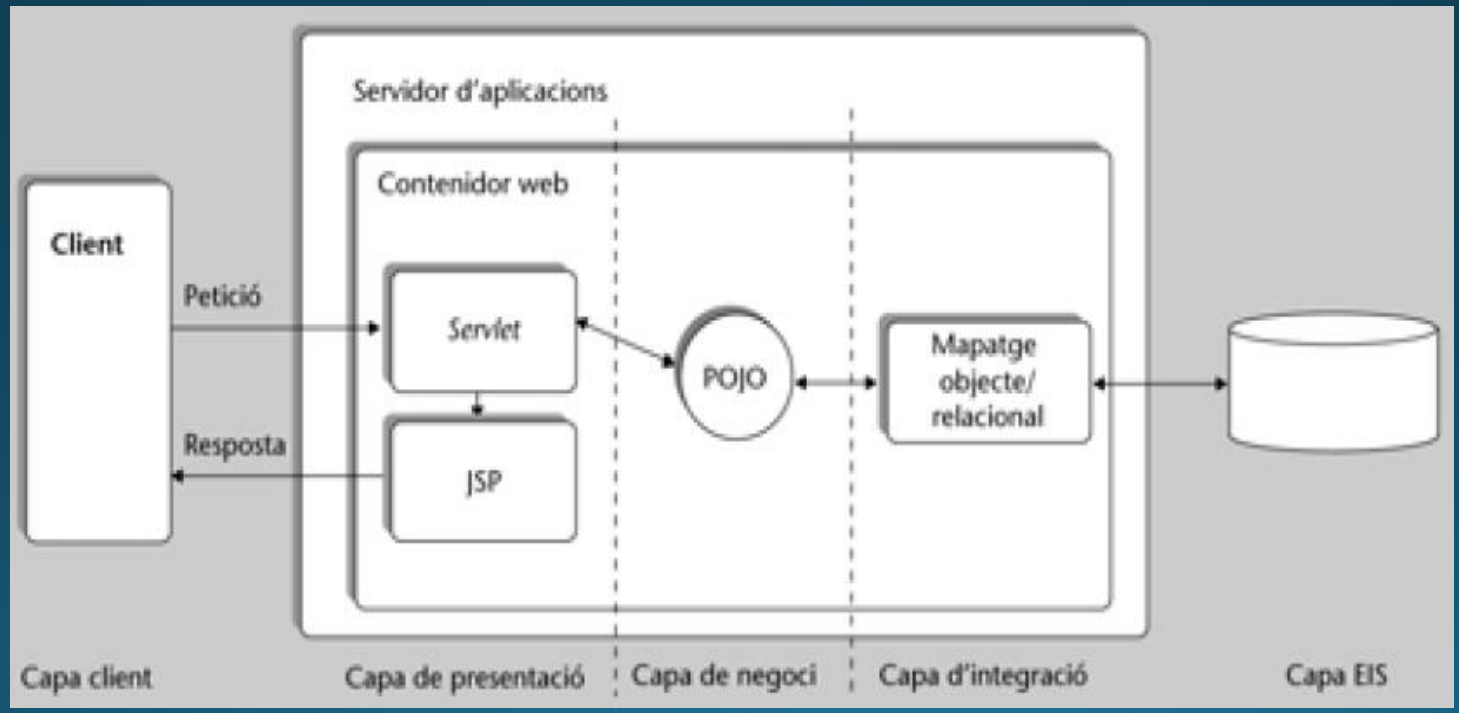
3. Disseny

3.1 Disseny: Tecnologia web

- Llenguatge de programació Java (plataforma Java EE).
- Framework JSF (*JavaServer Faces*).
- HTML5 , CSS i JavaScript.
- Base de dades *MySQL*.
- Servidor d'aplicacions *GlassFish Server*.

3.2 Disseny: Arquitectura

- Arquitectura híbrida (per capes i client-servidor)
- Patrons de disseny.
- Agents.



3.3 Disseny: Protocols criptogràfics

3.3.1 Connexions segures

L'assegurament de les connexions entre el client i el servidor de l'aplicació és fonamental per tal d'evitar certs atacs d'un possible atacant, entre altres destaquem l'escolta de xarxa, la suplantació web o un MITM.

Forward secrecy: propietat que garanteix que una clau de sessió derivada d'un conjunt de claus públiques i privades no es veurà compromesa si una de les claus privades es veu compromesa en un futur.

Suite recomanada a utilitzar:

DHE_RSA_WITH_AES_CBC_SHA.

3.3 Disseny: Protocols criptogràfics

3.3.2 Autenticació d'usuaris

El protocol SRP (*Secure Remote Password*) permet que un usuari demostri el coneixement d'una contrasenya sense que en cap moment qui la comprova tingui coneixement de la mateixa o d'un valor derivat de la mateixa després de l'aplicació d'una funció resum.

L'usuari pot demostrar al servidor el coneixement de la contrasenya sense revelar-la. En el món de la criptografia aquest fet se'l coneix com a "*proves de coneixement nul o de coneixement zero*".

3.3 Disseny: Protocols criptogràfics

3.3.3 Confidencialitat de les dades

A part de protegir les dades d'atacants aliens al sistema, també s'ha de protegir contra les mateixes persones que tenen un accés autoritzat a la gestió (*insider*) o a l'ús de l'aplicació web com els usuaris.

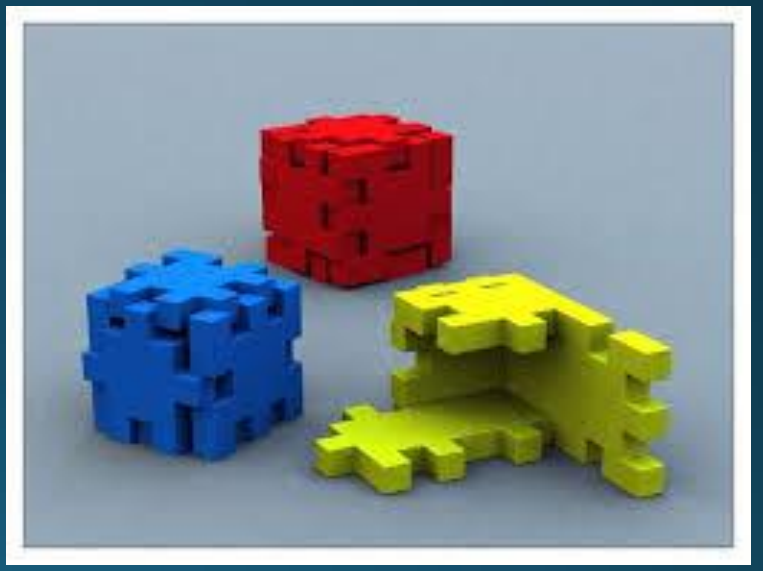
En aquest apartat s'han desenvolupat els següents punts:

- *La gestió de permisos de la BD*
- *Xifratge de les dades*
- *Gestió de claus*
- *Privacitat de les dades*

4. Implementació

4.1 Entorn de desenvolupament i proves

Per al desenvolupament inicial del prototip s'ha preparat l'entorn d'explotació a nivell local, en una única màquina física. Instal·lació de la BD *MySQL*, del servidor *GlassFish* i de l'entorn de desenvolupament d'aplicacions *NetBeans*.



4.2 Implementació dels protocols criptogràfics

- Connexions segures:
  - Generació de dos certificats (CA i servidor).
  - El camp CN (*common name*) dels certificats.
- Autenticació dels usuaris:
  - Ús d'un mètode d'autenticació feble (les claus dels usuaris es guarden resumides en el servidor).
- Confidencialitat de les dades:
  - És imperatiu l'ús del mateix ordinador amb el mateix navegador web que l'usuari va utilitzar per donar-se d'alta en l'aplicació.

5. Entorn de proves

5.1 Desplegament del prototip en servidor extern

- Alta en AWS (*Amazon Web Services*).
- Creació d'una instancia d'un servidor Windows Server.
- Configuració i preparació de l'entorn de la mateixa forma que a nivell local.
- Ús dels mateixos certificats que en l'entorn local.
- Direcció pública d'accés https://52.34.38.80

5.1 Demostració de funcionament del prototip

6. Conclusions finals

L'objectiu principal del projecte és desenvolupar una aplicació web segura per gestionar les activitats esportives que practiquen els usuaris. En el disseny com en la implementació s'ha utilitzat les eines adequades per poder assegurar aquest objectiu, i per tant es pot dir que l'objectiu principal s'ha assolit amb èxit.

5.1 Línies de treball futur

Millores i ampliació de l'ecosistema d'ús.

Fi de la presentació

11 de gener de 2015

Alumne:
Javier Díaz Espejo
Consultora:
Cristina Pérez Solà

Moltes gràcies per l'atenció