ESCOLA UNIVERSITÀRIA D'ENGINYERIA
TÈCNICA DE TELECOMUNICACIÓ LA SALLE

TREBALL FINAL DE MÀSTER

MÀSTER EN ENGINYERIA INFORMÀTICA I LA SEVA GESTIÓ

Arquitectura LogMeApp: Geo-localització com a mètode de seguretat en accessos a zones privades

ALUMNE

Jordi Massana Prats

PROFESSOR PONENT

Francesc Teixidó Navarro

ACTA DE L'EXAMEN
DEL TREBALL FINAL DE MÀSTER

Reunit el Tribunal qualificador en el dia de la data, l'alumne

D. Jordi Massana Prats

va exposar el seu Treball Final de Màster, el qual va tractar sobre el tema següent:

Arquitectura LogMeApp: Geo-localització com a mètode de seguretat
en accessos a zones privades.

Acabada l'exposició i contestades per part de l'alumne les objeccions formulades pels Srs. membres del tribunal, aquest valorà l'esmentat Treball amb la qualificació de

Barcelona,

VOCAL DEL TRIBUNAL VOCAL DEL TRIBUNAL

PRESIDENT DEL TRIBUNAL

Si has construït un castell a l'aire, no has perdut el temps, és allà on ha d'estar. Ara només has de construir-hi uns bons fonaments a sota.

George Bernard Shaw
1856-1950. Escriptor irlandès.

Agraïments

La realització d'aquest treball no hagués esta possible sense el recolzament de molta gent que desinteressadament m'ha donat suport durant tot el seu procés de realització.

En primer lloc, agrair al Xec la confiança que ha dipositat tant en mi com en la idea del treball, a l'Eva responsable del logotip de LogMeApp, la Mònica que ha supervisat la redacció de la memòria i a tot el cercle d'amics de Dublín que m'han portat al Pub a fer una pinta quan ha estat necessari desconnectar.

Finalment, agrair tot el suport rebut per part de la meva família durant tots aquests anys, que sempre ha respectat i confiat en les meves decisions i ha fet possible l'arribada a meta d'aquesta llarga cursa universitària. Sense ells, tot això no hagués estat possible.

A tots ells, moltes gràcies.

Abstract

El projecte LogMeApp es presenta com una arquitectura dissenyada per tal d'acreditar la presència d'un usuari en el moment que accedeix en alguna zona restringida que requereix d'autenticació per mitjà d'algun tipus de credencial única.

Per tal d'acreditar aquesta presència en el moment de l'accés, la tecnologia utilitza diverses tècniques de geo-localització on per mitjà del posicionament del telèfon mòbil de l'usuari propietari de la zona restringida i la posició de la zona accedida, porta a terme una comparació de posicions que defineix si realment és el propietari de l'espai qui està sol·licitant l'accés, o bé és un intrús que ha obtingut les seves credencials, cas en que es genera un avís instantani cap al telèfon de la víctima de la intrusió.

Paraules clau: geo-localització, *telèfon mòbil,*credencial,*posicionament, accés, zona restringida, autenticació.*

Resum

LogMeApp es presenta com a mètode de seguretat en accessos a zones restringides d'usuari. Per mitjà del posicionament de les dues parts participants en un accés a una zona privada, usuari i zona, acredita que realment és el propietari de l'espai restringit qui està sol·licitant l'accés i no un tercer subjecte a mode d'intrús.

Per tal de garantir la presència del propietari de la zona restringida a la qual s'està sol·licitant un accés, s'utilitzarà com a credencial d'identitat el posicionament del seu telèfon mòbil, i, per altra banda, també es posicionarà la zona accedida, duent a terme una comparació posterior de posicions per decidir si l'accés es vàlid o intrusiu. En cas que existeixi alguna sospita de que realment s'està intentant suplantar la identitat d'un usuari en la porta d'accés d'alguna de les seves zones privades, aquest serà avisat de forma instantània al seu telèfon mòbil.

L'objectiu s'aborda dissenyant i implementant els diferents components que composaran l'arquitectura per tal d'assolir el propòsit esmentat.

Aquesta arquitectura, batejada amb el nom de LogMeApp, es divideix principalment en dos grans blocs que composen el seu sistema central:

- **Nucli del sistema o capa d'autenticació:** S'encarrega de capturar la posició dels usuaris en el moment que se sol·licita un accés en una zona restringida i decideix si un accés és segur o no. En cas que no ho sigui, serà aquí des d'on es generi l'avís cap al telèfon del usuari propietari de la zona.
- **Capa de controladors d'espais:** Un controlador d'espai es defineix com el mòdul que treballa en la banda de l'espai que s'accedeix, i és l'encarregat d'obtenir la informació necessària per tal de geo-localitzar aquest espai. Un cop tingui aquesta posició, l'enviarà cap a la capa d'autenticació on es tramitarà la validació.
  En aquesta capa de l'arquitectura hi treballaran controladors d'espais diversos, que variaran el seu disseny i implementació depenent del tipus de zona restringida de la qual en siguin responsables.

Per altra banda, a part del sistema central d'autenticació, també és necessari un component en la banda del client, essencial per posar tot el sistema de validació en marxa.

- **Servei Mòbil d'actualització de posició:** Per tal que el sistema pugui disposar en tot moment de la geo-localització dels usuaris subscrits al tipus d'autenticació que es proposa, aquests hauran d'instal·lar una aplicació als seus dispositius mòbil que s'encarregarà de mantenir la posició del telèfon actualitzada en el servidor del sistema.

Finalment, amb l'objectiu d'obtenir un producte funcional, s'han dissenyat i implementat els components necessaris per abordar el control de **zones restringides de tipus web**, és a dir, accessos a pàgines personals com poden ser xarxes socials, serveis de webmail o comptes d'usuari en blogs o fòrums.

ÍNDEX DE CONTINGUTS

Índex de figures

1. Introducció

1.1 Motivació

La creació del projecte LogMeApp sorgeix de la idea de reduir el creixent problema de suplantació d'identitat que es produeix a diari en els diferents espais privats que requereixen d'una credencial d'usuari per accedir-hi.

En referència a zona privada, s'entén tot sistema d'informació o aparell, que requereixi d'una validació d'usuari per a fer-ne un ús legítim com ara poden ser comptes d'usuari en pàgines web, caixers automàtics, activacions i desactivacions d'alarmes domèstiques o inclús un vehicle propi, el qual també es posarà en marxa utilitzant una clau física que només el seu propietari posseeix. En definitiva, qualsevol espai abstracte o físic que estigui destinat exclusivament a un sol usuari o a una determinada comunitat.

"La contrasenya introduïda requereix de com a mínim 9 caràcters i ha de contenir xifres i lletres"

Si bé és cert que existeix ja molta investigació al voltant de la seguretat en la validació de credencials d'usuari quan s'accedeix a un espai privat, també és cert que els mètodes aplicats actualment no van més enllà dels algorismes d'encriptació de claus o l'ús de contrasenyes d'accés d'alta complexitat.

Les pretensions de LMA van més enllà d'obligar a un usuari a recordar una contrasenya de 10 caràcters que contingui xifres, lletres, majúscules i minúscules per assegurar la seguretat de la seva zona privada. LMA vol assegurar que quan usuari està accedint en un espai privat és ell, i no algú altre que ha obtingut les seves credencials.

L'arquitectura proposada pretén identificar a un usuari basant-se en la seva posició cada cop que accedeix a algun dels seus espais. Així doncs, actuarà com un sensor que s'activarà si una propietat privada ubicada a Matadepera és accedida de forma intrusiva quan el seu propietari està gaudint de *La Patum* de Berga.

"Anar a dormir sense posar el mòbil a carregar? Ara ja no".

Fent un cop d'ull a la situació tecnològica a l'abast de la societat actual, es comprova que una gran majoria de persones disposa ja d'un telèfon mòbil d'última generació capaç de detectar la seva pròpia geo-localització per mitjà de diverses tecnologies com ara GPS o antenes GPRS.

A més a més, considerant que el mòbil es un aparell quasi obligatori avui en dia, i que rarament aquest no acompanya al seu propietari allà on ell vagi, LMA suposarà que la posició d'una persona serà la mateixa que la del seu dispositiu mòbil i l'utilitzarà com a credencial de presència de l'usuari en una determinada posició.

"Ara que saps on sóc, que faràs tu perquè no utilitzin la targeta de crèdit que m'han robat?"

Efectivament, com el 99.9% de productes actuals que s'acompanyen del concepte "tecnològic" LMA fa ús d'Internet per posar en marxa el seu sistema de verificació. Però la qüestió és: què no està connectat a la xarxa avui en dia? Inclús el dispositiu més simple envia una petició a un servidor per obtenir o enregistrar informació.

Basant-se en aquesta realitat, i tenint en compte que actualment la tecnologia disponible fa possible que dispositiu amb Internet sigui sinònim de dispositiu localitzable, LMA intentarà que en el moment que es faci un accés a una zona privada, es dugui a terme una comparació entre la posició del propietari d'aquesta zona amb la posició de la zona en qüestió. En cas de no obtenir posicions similars d'ambdues bandes, LMA activarà una alarma en forma d'avís cap al telèfon mòbil de l'usuari, per què ell prengui les mesures necessàries envers l' intrusió del seu espai.

Resumint, es proposa una arquitectura molt ambiciosa i innovadora i transversal en el camp de les validacions de credencials, que si bé es cert que competeix amb d'altres tecnologies emergents en el mercat, proposa diferències molt interessants com ja es veurà al llarg d'aquest document.

1.2 Objectius

1.2.1 Objectius d'explotació

En el camp de batalla de les tecnologies no és feina fàcil competir amb una idea poc definida i abstracta. S'ha de tenir les coses clares i s'ha de saber exactament i de forma focalitzada quines necessitats del mercat actual es volen cobrir.

LMA vol penetrar al mercat de les a tecnologies de seguretat en accessos en zones privades, marcant un seguit de diferències sobre els mètodes ja implementats o els que estan en actual desenvolupament.

"No em facis masses canvis que el que tinc ja em va bé"

Qualsevol persona que hagi intentat vendre un nou producte tecnològic a un client ha sentit aquesta frase. Des del punt de vista de l'Enginyer es veu com que el client és un retrògrad tancat a canvis i millores, i es tendeix a pensar que aquest està cometent un error no implantat el meravellós sistema que se li està oferint. Però això no es així. El client sempre té la raó i en aquest cas més que mai. Ningú es vol exposar a un gran canvi si el que té satisfà les seves necessitats. Tot nou sistema requereix d'un temps

d'implantació que en molts casos i de forma comprensible, el client no està disposat a assumir.

Integració amb els productes ja existents

LMA vol evitar que es canviïn els productes que ja es troben en fase d'explotació. Des de la seva fase de disseny, pretén ser una tecnologia que ofereixi un alt grau d'integració amb el que ja està implementat actualment, oferint tot tipus de facilitats per a tal efecte.

El producte que es planteja és un servei a tercers que, tot i que no modifica el comportament ni els mètodes d'accés a un determinat espai protegit, li afegeix una propietat més en termes de seguretat: la geo-localització.

Per altra banda, es proposa un disseny d'arquitectura escalable i modular que permeti el creixement i la millora del producte per part de les diverses comunitats de desenvolupadors. D'aquesta manera s'aconsegueix descentralitzar tant el desenvolupament com la recerca envers les possibilitats de la pròpia tecnologia.

Verificació d'identitat en diversos àmbits.

De forma quotidiana tothom fa validacions d'identitat en diversos àmbits per mitjà de credencials que no necessàriament tenen que ser de la mateixa forma. Tant al accedir al nostre compte d'una xarxa social introduint usuari i contrasenya, com a l'obrir la porta de casa o del nostre vehicle per mitjà d'una clau, estem acreditant que estem autoritzats a accedir en un espai determinat.

LMA vol abordar l'acreditació de l'usuari en tants àmbits com sigui possible per mitjà de diferents mòduls dissenyats seguint un patró definit des de la pròpia arquitectura.

Registre d'accessos en espais privats de forma centralitzada

Actualment, és freqüent accedir a espais personals des de punts no segurs que probablement només s'utilitzaran un cop a la vida, com ara pot ser un accés al compte de correu electrònic des de l'ordinador d'una biblioteca pública.

Aquestes "portes" d'accés tenen un alt grau de perillositat per diverses raons, però bàsicament, pel fet de que s'han introduït credencials personals en un dispositiu del qual es té total desconeixença.

És per això que es vol deixar rastre d'aquests accessos. LMA ofereix un espai web als seus usuaris, on, per mitjà d'un registre, aquests podran fer un seguiment dels accessos als seus espais privats i comprovar si hi hagut alguna intrusió en algun d'ells.

Aquest espai web, com no podia ser d'altra manera, disposa de la protecció LMA per tal de protegir els comptes privats del usuaris

1.2.2 Objectius funcionals

Les entitats palpables que s'esperen obtenir en el moment de l'entrega del TFM LogMeApp són:

- **Nucli de validació LMA** i **mòdul** encarregat de gestionar la segureta d'accessos en comptes personals del tipus **web.**

- Disseny i implementació de **l'aplicació Web logmeapp.com** a l'abast dels usuaris LMA, per tal de controlar els seus comptes d'usuaris i obtenir informació sobre els accessos en les seves zones restringides.

- Disseny i implementació de **l'aplicació mòbil LMA per a la plataforma Android**, així com els serveis concurrents que s'executen en segon pla en el terminal.

2. Estat de l'art

A continuació s'exposa l'estat de l'art de les tecnologies, mètodes i procediments que de la mateixa manera que LMA, intenten vetllar per la seguretat dels espais privats dels usuaris per medi de tècniques que comparteixen punts en comú amb l'arquitectura que es proposa. A part d'una breu descripció sobre el funcionament d'aquests mètodes ja existents o bé en estat emergent, també es detalla en quins aspectes l'arquitectura LMA s'inspira en ells i en quins aspectes hi marca diferències a millor.

2.1 Geo-localització com a mètode de seguretat en accessos web.

Proveïdors de WebMail i xarxes socials.

Tant els principals proveïdors de webmail, com les xarxes socials més famoses ja apliquen actualment mètodes de geo-localització simples com a forma de seguretat a l'hora d'accedir a comptes personals, ja siguin de correu electrònic o pàgines de perfils diversos. Normalment, per mitjà de la localització IP es considera un accés sospitós el que es realitza des d'un país diferent des del que últimament s'ha accedit al compte.

Així doncs, quan un usuari marxa del seu país de residència i es connecta a un dels seus comptes des de l'estranger, aquest rep un avís d'aquest accés forà, que normalment serà en forma de correu electrònic.

Per altra banda, no es geo-localitza de cap manera a l'usuari que està accedint, així que aquestes tecnologies queden bastant per darrera de les pretensions de LMA.

2.2 Verificació d'identitat d'usuaris per mitjà de credencials físiques

NFC (Near Field Communication)

Near Field Communication es presenta com a una extensió de la tecnologia RFID que permet el intercanvi de dades per mitjà de camps electromagnètics entre dispositius que es trobin a menys de 10 cm de distància l'un de l'altre.

Diverses empreses bancàries han apostat ja per aquesta tecnologia, implementant receptors que permeten realitzar pagaments utilitzant telèfons mòbils dotats amb NFC com a mitjà de credencial. De la mateixa manera també és fa ús de NFC en diverses empreses per identificar als seus treballadors, els quals disposen d'un dispositiu únic dotat d'aquesta tecnologia per garantir la seva identitat.

La implantació d'aquest mètode, requereix de dos punts dotats de hardware NFC per realitzar aquest intercanvi de dades, així que el procés d'integració inclou una renovació tant de software com de hardware sobre els dispositius que s'implementa.

Com ja s'ha recalcat anteriorment, LMA té com objectiu integrar-se com a mètode d'autenticació sense realitzar grans canvis allà on s'implanti, i molt menys obligant a qui vulgui utilitzar el servei a fer una gran despesa en nova maquinària.

Tot i així, com a línia futura, no es descabellat pensar en una integració de NFC com a part de l'arquitectura LMA i així assegurar la presència d'un usuari en un determinat punt en àmbits d'autenticació que s'hi avinguin.

2.3 Serveis de seguiment per a telèfons mòbils i localitzadors GPS per a objectes de valor

Seguiment d'objectes per satèl·lit per medi de localitzadors GPS

Existeixen diversos proveïdors de serveis que ofereixen la possibilitat de fer el seguiment de qualsevol objecte per mitjà de localitzadors GPS adjunts al objecte a seguir. Aquestes empreses acostumen a actuar com intermediari entre aquest localitzador i l'objecte, i ofereixen al propietari de l'element a seguir, diverses interfícies per fer un seguiment en temps real del mateix.

Un altre propietat que aquests serveis acostumen a tenir, és un sistema d'alerta que detecta canvis inesperats de posició del localitzador GPS i avisa al propietari per mitjà de tecnologies cel·lulars com ara 3G o GPRS utilitzant protocols com SMS o correu electrònic.

La desavantatge d'aquests sistemes en comparació amb el servei que LMA vol oferir és que tenen una visió molt focalitzada del servei que ofereixen, limitant-se a protegir a un usuari de la pèrdua de l'objecte al que s'ha dotat amb el localitzador GPS, que, perquè no dir-ho, no acostumen a ser precisament barats.

Les pretensions de LMA no són les de protegir únicament propietats úniques d'usuaris, sinó que també es vol assegurar una identitat per mitjà de la geo-localització en accessos a espais comuns on diversos usuaris accedeixen per mitjà de credencials úniques, com pot ser el cas d'un caixer automàtic o la porta d'entrada a una empresa que requereix de credencials dels treballadors per donar accés.

Seguiment de telèfons mòbils com a forma de protecció del dispositiu i les dades del propietari.

En la mateixa línia de protecció per geo-localització, en el mercat actual es troben proveïdors de serveis que per mitjà de la instal·lació d'una aplicació al telèfon mòbil, permeten fer un ús remot d'aquest utilitzant un ordinador domèstic com a mitjà d'accés.

Entre les propietats remotes amb que es doten al dispositiu gràcies a l'aplicació instal·lada i normalment una aplicació web, es troben la del posicionament del cel·lular en temps real sobre un mapa, l'eliminació de dades sensibles com ara contrasenyes i fitxers privats en cas de robatori, o bloqueig total del dispositiu per evitar-ne l'ús de forma temporal o permanent.

Tot i que inicialment aquestes funcionalitats no es van incloure en els plans de LMA, més endavant s'ha vist que tractant el dispositiu mòbil com a credencial d'un usuari, és important oferir protecció sobre aquest. Així doncs, per mitjà de les interfícies web ofertes per l'arquitectura LMA, també es proporcionen els serveis esmentats anteriorment per actuar de forma remota sobre els telèfons mòbils dels usuaris. Aquestes funcionalitats es detallen en l'apartat que descriu les interfícies web de l'arquitectura.

2.4 Single sign-on. Instancia única d'identificació per accedir a diversos sistemes

Existeixen diversos procediments d'autenticació que permeten a un usuari accedir a diversos sistemes i/o aplicacions amb una única instancia d'identificació, incrementant així el grau de seguretat envers la captura de credencials que viatgen per la xarxa, i reduint l'error humà a l'hora d'autenticar la seva identitat per mitjà de credencials diferents en cada un dels sistemes que vol accedir.

[Font: http://es.wikipedia.org/wiki/Single_sign_on - Wikipedia]

Aquest tipus de procediments es coneixen com a mètodes Single sign-on (SSO) i principalment n'hi han de 5 tipus:

- *Enterprise single sign-on (I-SSO),* porta a terme una autenticació primària de l'usuari, interceptant els requeriments de login presentats per les aplicacions secundàries per a completar els mateixos amb l'usuari i contrasenya. Els sistemes I-SSO permeten interactuar amb sistemes que poden inhabilitar la presentació de la pantalla de login en terceres aplicacions.

- *Web single sign-on (Web-SSO)*,treballa només amb aplicacions i recursos accedits via web. Els accessos són interceptats amb l'ajuda d'un servidor proxy o

d'un component instal·lat en el servidor web destí. Els usuaris no autenticats que tracten d'accedir són redirigits a un servidor d'autenticació i tornen únicament després d'haver assolit un accés vàlid. S'utilitzen *cookies*, per a reconèixer aquells usuaris que accedeixen, així com el seu estat d'autenticació.

- *Kerberos* és un mètode que externalitza l'autenticació dels usuaris. Els usuaris es registren en el servidor Kerberos i reben un "tiquet" que després les aplicacions client presenten per a obtenir accés.

- *Identitat federada* és una nova manera de concebre aquest tema, també per a aplicacions Web. Utilitza protocols basats en estàndards per a habilitar que les aplicacions puguin identificar els clients sense necessitat d'autenticació redundant.

- *OpenID* és un procés de SSO distribuït i descentralitzat on la identitat es compila en una url que qualsevol aplicació o servidor pot verificar.

Inspiració de LMA en els mètodes SSO

Tot i que LMA no vol modificar els mètodes d'autenticació d'usuaris emprats per els diferents sistemes existents, si es cert que capta la essència d'aquests mètodes en quant a monitoritzar des d'un únic punt l'accés a diferents sistemes i aplicacions.

A més a més, l'arquitectura que es proposa basa part del seu funcionament en una assignació única d'identificador per cada un dels espais privats dels usuaris, i en el cas del mòdul d'autenticació WebNet de LMA que controla els accessos a la xarxa dels usuaris, com en el procediment Web Single sign-on, és farà ús de *cookies* per identificar i localitzar la màquina que està accedint a qualsevol dels espais web restringits com ja es veurà en la descripció detallada d'aquest mòdul controlador.

3. Metodologia: Anàlisi i plantejament de LogMeApp

La idea original de LMA de forma molt bàsica es va basar en comparar la posició d'un usuari amb la del espai restringit al que està accedint per garantir la seva presència en aquest espai en el moment de l'accés.

LMA com a protecció dels comptes web d'un usuari

Inicialment es pensa en espai restringit d'usuari, únicament com a referència als espais Web personals dels que un usuari disposa com poden ser perfils en xarxes socials, comptes de correu electrònic, blogs o comerços virtuals i e-banks.

Partint d'aquesta idea es comença dibuixar una arquitectura que intenta que en el moment que un usuari accedeix a algun dels seus comptes web, s'obtingui la seva posició (la del seu telèfon mòbil) i la posició de la màquina des on aquest usuari està accedint a la xarxa. Un cop es tenen ambdues posicions, aquestes es comparen i s'activa una alarma en cas de que no coincideixin, disposant d'un servei que avisa a l'usuari de l'existència de intrusos en alguna de les seves zones restringides.

Però com passa sovint en la entrada a la fase de disseny d'una idea de la qual no es té més que un esbós mental del que es vol fer, cada instant que passa fa que s'obrin noves portes envers aquesta idea inicial i l'ambició del projecte creix de forma exponencial.

Està molt bé fer saber a un usuari que algú esta envaint la privacitat d'algun dels seus comptes web. És innovador i necessari. Però per què no pujar un graó més i intentar buscar un punt comú als diversos àmbits on un usuari acredita la seva identitat més enllà de la web?

Maduració de la idea i plantejament d'una arquitectura per capes: Autenticació d'usuari i Controladors d'espais

Donant-hi voltes a la idea es conclou que no necessàriament ha de ser un accés web el que quedi sota la protecció de LMA, sinó que amb un bon disseny modular de l'arquitectura es poden abordar i protegir infinitat d'àmbits on un usuari acrediti la seva presència per mitjà de credencials.

Es aquí on apareix el plantejament d'una arquitectura de dues capes:

- **Capa d'autenticació:** Compara la posició de l'usuari, la qual s'obté en aquesta mateixa capa, amb la de l'espai que aquest està accedint, informació que es rep per part de la capa superior de controladors d'espais.
- **Capa de controladors d'espais**: Un controlador d'espai encapsula en forma de mòdul un seguit de funcions específiques per localitzar l'espai en el qual l'usuari està accedint. D'aquesta manera es pot disposar de mòduls que treballin amb la infinitat de zones restringides on un usuari sol·licita un accés per mitjà de credencials úniques; des de la pàgina de perfil d'una xarxa social d'aquest usuari, la retirada de diners del seu compte

en un caixer automàtic, i inclús, si cal, acreditar la seva presència en el procés desactivació de la seva alarma domèstica.

Amb aquest plantejament, el control d'accessos web ara passa a ser un controlador LMA específic per a tal efecte, que enviarà la informació de posicionament del dispositiu des del qual s'accedeix a l'espai web a la capa d'autenticació, on es comparará amb la posició de l'usuari.

L'objectiu final de l'arquitectura, des d'un punt de vista funcional, es reflexa de forma gràfica en la figura següent on es mostra amb un exemple com LMA detecta i processa accessos intrusius en zones personals privades.

En el cas concret de l'esquema següent, es reflexa com actua el sistema de seguretat LMA quan en Batman, que ha aconseguit les credencials de l'Spiderman per entrar a una determinada zona restringida, intenta suplantar la seva identitat en la porta d'entrada de la zona.

De dreta a esquerra, es veu tot el procés d'actuació de LMA, des del moment que es captura en la capa de controladors la posició del terminal des d'on en Batman accedeix al compte del Spiderman, fins al moment que l'Spiderman rep l'avís de la intrusió després que la capa d'autenticació dugui a terme la comparació de posicions.

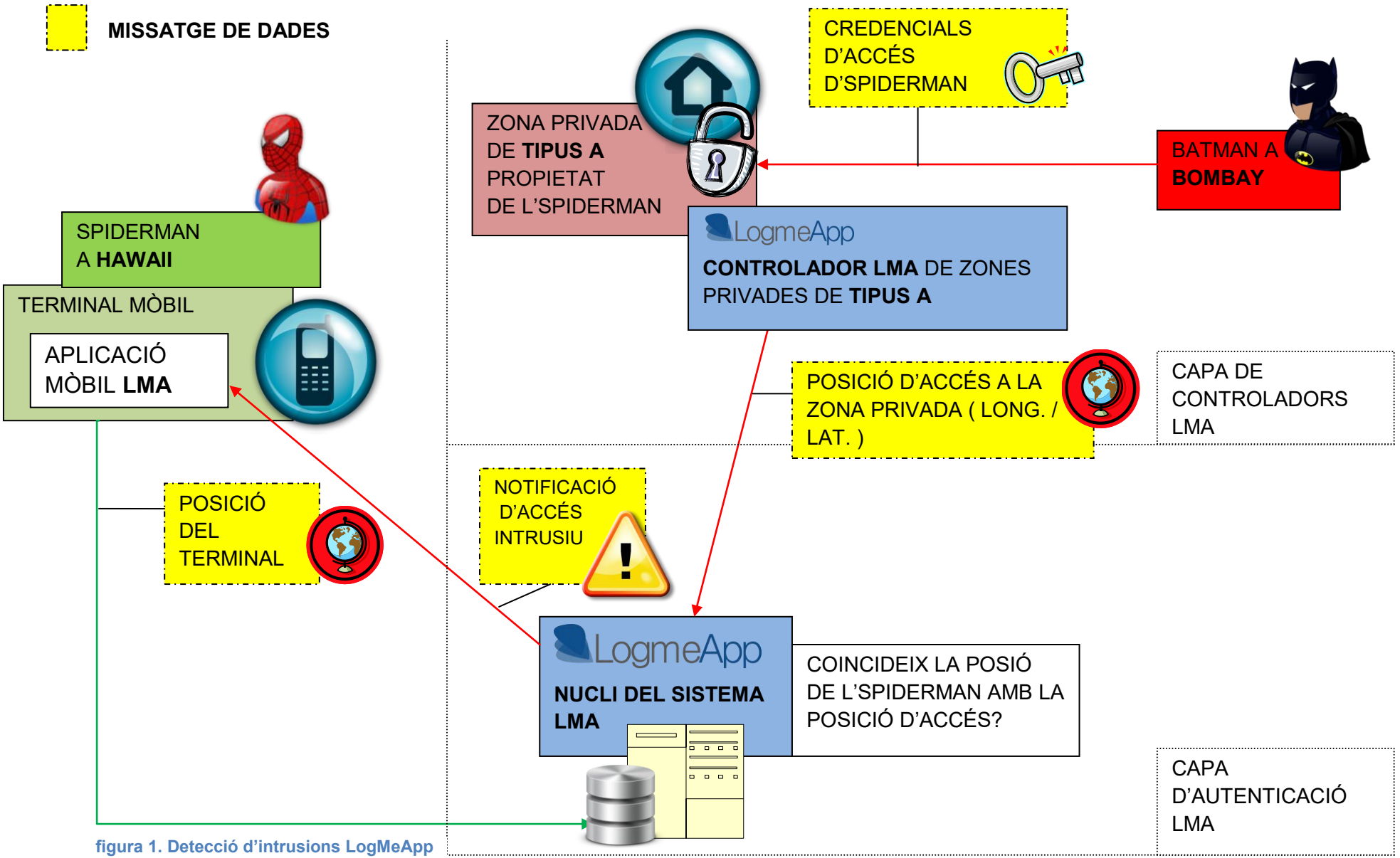

figura 1. Detecció d'intrusions LogMeApp

4. Arquitectura LogMeApp

A continuació s'exposa el procés de creació de l'arquitectura LMA. Es descriuen la fase de disseny del producte, les tecnologies emprades per a posar el sistema de validació en funcionament i la fase d'implementació.

4.1 Model conceptual de l'arquitectura LMA

El concepte bàsic de LMA és interceptar el procés d'accés dels usuaris a la seves zones privades per dur-hi a terme una validació. Exactament, vol comparar la posició d'aquest usuari (la del seu dispositiu mòbil) amb la posició de l'espai que està accedint, activant una alarma en cas de que no coincideixin.

El sistema s'organitza en dues capes diferenciades amb responsabilitats diferents. La primera és la d'autenticació que únicament emmagatzema els usuaris LMA i manté les seves posicions actualitzades per dur a terme la validació de posicions quan sigui necessari.

La segona és la capa de controladors d'espai, on diversos mòduls cobriran els diferents àmbits on un usuari pot disposar de zones privades, i serà en aquest nivell on es tractarà de forma específica la captació de la posició d'accés en cada un dels diferents tipus de zones restringides.

4.1.1 Capa d'autenticació

L' usuari LMA.

Com tota tecnologia que disposa d'accions úniques i exclusives per a cada un dels seus usuaris, cal pensar quina informació es necessitarà per poder actuar de forma personalitzada.

En primera instància, dels usuaris de LMA es requereix:

Credencials d'usuari (Identificador i contrasenya)	Identificador únic i contrasenya com a credencials úniques per a cada usuari dins dels sistema LMA. S'especifica un compte de correu electrònic per cobrir el camp identificador; no tan sols per la seva naturalesa única sinó també per a fer-lo servir com a via de contacte en determinats casos. Amb aquestes credencials l'usuari accedeix a les diverses interfícies web o mòbils que LMA proporciona als usuaris per a realitzar el seguiment dels accessos en els seus espais privats.
Geo-posició	Longitud i latitud constantment actualitzada d'aquests usuaris.

	Imprescindible per dur a terme la validació de presència d'usuari quan aquest realitza un procés d'accés a zona privada. L'aplicació mòbil corrent en els terminals dels usuaris s'encarregarà de mantenir aquesta geo-localització actualitzada en el servidor LMA.
Dispositiu mòbil	Bloc d'informació referent al dispositiu mòbil d'aquest usuari, per poder contactar-lo instantàniament en cas que sigui necessari i per tenir una referència única de les actualitzacions de posició. El tipus de dades d'aquest apartat varien en funció del tipus de dispositiu que l'usuari declara.

La part d'usuari queda doncs resolta. Ara queda veure amb quins altres blocs d'informació es relacionaran aquests per anar donant forma al sistema plantejat.

4.1.2 Capa de controladors d'espais

Per sobre de la capa d'autenticació, l'arquitectura té un seguit de mòduls treballant per tal d'obtenir la posició exacta del mitjà d'accés en cada un dels espais privats en que l'usuari està accedint.

Aquests mòduls treballaran en un nivell anomenat capa de controladors d'espais, i és per mitjà d'aquests que s'obtenen les dades necessàries sobre el posicionament dels accessos en els espais restringits. Un cop les posicions són extretes, es transmetent a la capa d'autenticació on es porta a terme la validació de presència d'usuari.

Zones privades d'usuari sota la vigilància de LMA

L'arquitectura planteja aquest aspecte de manera que tot espai accedit per un usuari disposa d'un mitjà físic per dur a terme aquest accés. Si bé es cert que aquest mitjà serà diferent per als diferents àmbits on un usuari acredita la seva presència, i que la informació que es requerirà d'aquests espais variarà en funció de la seva naturalesa, tots disposaran de la següent informació comú:

Identificador únic	Identificador únic alfanumèric que identifica la zona privada accedida
Geo-posició	Posició de la zona accedida o del mitjà des del qual s'hi accedeix en cas de ser una zona d'accés remot.

La informació sobre la posició d'un accés és bastant abstracte, i s'ha d'enfocar des de diferents punts de vista en funció de en quin àmbit s'està parlant.

Exemples

A continuació s'exposen un seguit d'exemples de com es tractarien algun dels hipotètics àmbits que LMA podria cobrir.

Cas 1: Protecció envers intrusions en espais web

Es vol protegir a un usuari de les intrusions que pugui tenir en algun dels seus comptes web, ja siguin xarxes socials, webmail o perfils d'usuari en blogs diversos.

L'espai accedit en aquest cas és abstracte, doncs la ubicació física de la zona serà la posició del servidor web que mostri la pàgina, informació que de forma clara no és rellevant per als propòsits de LMA.

Així doncs, cal traslladar el concepte de posició de zona, a la ubicació de la màquina des de on accedeix aquest espai web.

La informació que s'emmagatzemarà en casos de zones del tipus web serà:

Propietari	Identificador	Descripció	Geo-posició		
Jordi	P1	Pc a casa	Longitud: 50	-	Latitud: 30
Jordi	P2	Pc a la feina	Longitud: 10	-	Latitud: 60
Jordi	P3	Pc a la universitat	Longitud: 25	-	Latitud: 40

Serà després en la capa de controladors d'espai de LMA on, un mòdul dissenyat de forma específica per a tal efecte, obtindrà la informació sobre la posició de l'origen de l'accés en el moment que un usuari accedeixi a un compte web.

D'aquesta manera si LMA detecta que en Jordi accedeix a un dels seus comptes web des del "PC de casa" quan ell es troba a la feina, activarà les seves alertes. De la mateixa manera, com mesura de seguretat preventiva activarà una alerta en cas que la capa de controladors per a espais web no sigui capaç de localitzar l'origen de l'accés.

Cas 2: Protecció envers ús de targetes de crèdit de forma il·legítima en caixers automàtics

En aquest cas la protecció va dirigida als comptes corrents de l'usuari LMA. Exactament, es vol generar una alerta si es detecta que una targeta bancària és utilitzada per algú altre que no sigui el seu propietari en un caixer automàtic.

L'espai accedit és més evident en aquesta situació. La posició física del caixer en el moment de retirar-hi diners, serà més que suficient per validar la presència de l'usuari i el bloc d'informació necessari per identificar la zona restringida quedarà de la següent manera:

Propietari	Identificador	Descripció	Geo-posició
LaCaixa	C1	Caixer C/Calàbria 12	Longitud: 50 - Latitud: 30
LaCaixa	C2	Caixer C/Entença 23	Longitud: 10 - Latitud: 60
LaCaixa	C3	Caixer Pl/Orfila 2	Longitud: 25 - Latitud: 40

D'aquesta manera l'arquitectura podrà detectar, en el moment que s'accedeixi a la targeta de forma il·legítima la posició del propietari de la mateixa i actuar en conseqüència.

Un cop més, serà en la capa de servei, des d'on un mòdul que treballi en aquesta capa tramitarà la detecció de l'accés al caixer, i enviarà a la capa d'autenticació la informació necessària per validar la presència de l'usuari.

Cas 3: Protecció envers al robatori de vehicles.

No és ja cap novetat que els vehicles incorporin localitzadors GPS com a mesura de seguretat o mòduls de comunicació 3g per obtenir o enviar dades cap a la xarxa.

LMA té com a línea futura incloure aquest camp en un dels seus àmbits de protecció, i es per això que també es té en compte a l'hora de dissenyar l'arquitectura.

Un vehicle no és més que un espai restringit per a un usuari, on aquest utilitzarà en la majoria dels casos, una clau física per acreditar la propietat del vehicle en qüestió.

Per al cas específic de vehicles, el registre d'informació emmagatzemat en el sistema d'informació LMA podria ser:

Propietari	Identificador	Descripció	Geo-posició
Jordi	V1	El cotxe petit	Longitud: 50 - Latitud: 30
Jordi	V2	Furgoneta de la feina	Longitud: 10 - Latitud: 60
Jordi	V3	El cotxe gran	Longitud: 25 - Latitud: 40

A diferència de la resta de casos l'espai restringit vehicle tindrà una posició variable en funció de on es trobi en un determinat moment.

Abstracció de propietats comuns per a tots els espais privats d'un usuari.

Tant en el cas d'una web, el d'un caixer automàtic o el d'un vehicle propi, es comprova com tot i tractar-se d'àmbits totalment diferents, s'aconsegueix abstreure la seva part comú que serà útil per a realitzar el procés de validació de LMA.

Per altra banda, es veu com el concepte "espai privat" es totalment abstracte i té un significat molt variable en funció de l'àmbit que estiguem tractant en la capa de Serveis de l'arquitectura.

4.1.2.1 Controladors d'espai LMA. Responsabilitats, conceptes i directrius de disseny

Degut al gran ventall d'àmbits d'autenticació que LMA pretén abordar, es fa impossible definir un disseny únic per als controlador que treballen per sobre de la capa d'autenticació i és per això que el que es fa des de l'arquitectura, és definir un seguit de directrius per implementar aquests mòduls.

Responsabilitats d'un controlador d'espais LMA

El primer que es necessita per a començar el disseny d'un controlador d'espais LMA, és entendre quines són les responsabilitats que se li adjudiquen i les dades de sortida necessàries per a que sigui integrable amb la resta de l'arquitectura. A continuació, es mostra un llistat d'aquestes responsabilitats:

- Interceptar les dades d'accés d'un usuari en l'instant que aquest està accedint en algun dels seus espais restringits coberts pel controlador.
- Detectar la posició de l'espai on l'usuari està accedint o la posició del mitjà que està utilitzant en cas d'accés es remot.
- Relacionar l'usuari que està realitzant l'accés amb el compte LMA d'aquest usuari.
- Independentment de les tecnologies o mètodes específics que es facin servir en cada mòdul, enviar a la capa d'autenticació la següent informació quan es produeixi un accés en l'àmbit que cobreixen:
    - Posició de l'espai accedit.
    - Usuari LMA que està accedint a aquest espai.
    - Usuari LMA propietari de l'entitat a la que pertany l'espai accedit.

Conceptes sobre un controlador d'espai

Arribats a aquest punt de la memòria, cal definir un parell de conceptes dels quals es parla en aquest mòdul, per tal d'entendre des de quin punt de vista s'ha enfocat aquesta part de l'arquitectura. Així doncs, a continuació es descriuen un seguit de termes que es repeteixen al llarg dels següent apartats.

CONCEPTE	DESCRIPCIÓ
ENTITAT LMA	La majoria dels espais restringits on un usuari accedeix, formen part d'una tercera entitat que proveeix d' aquests espais als seus usuaris. Així doncs, cada un dels controladors d'espais implementats per a LMA, cobrirà els grups d'entitats que tinguin propietats comuns en quan a la forma d'accés que els usuaris fan servir per acreditar la seva identitat envers la zona privada. Cada una d'aquests proveïdors de serveis que ja disposen d'usuaris propis es defineix com a ENTITAT. Per exemple, accessos a clients web de correu electrònic i accessos a pàgines personals de perfil en xarxes socials, quedaran sota la tutela del mateix servei i, el proveïdor del servei de correu o el proveïdor de la xarxa social seran entitats diferents. En canvi, serà un altre servei el que tracti la monitorització de l'ús de targes de crèdit com a forma de pagament i en aquest cas, les entitats seran les diferents entitats bancàries responsables de les targes en qüestió.
POSICIÓ D'ACCÉS	Quan es parla de posició d'accés, s'entén que es parla de la posició on es troba o bé la zona accedida físicament, o bé quin és l'origen d'un accés remot en algun espai restringit. Aquesta dualitat de concepte anirà en funció de l'àmbit que s'estigui parlant en un determinat moment.

Directrius de disseny d'un controlador d'espai LMA

Per tal de poder crear un controlador d'espai LMA, s'han de generar certs blocs d'informació que han d'existir en el sistema persistent de dades del controlador per poder generar les dades de sortida necessàries per dur a terme la validació de presència en la capa d'autenticació.

A continuació, es descriuen quines són aquestes entitats de dades imprescindibles:

Relació usuari LMA- usuari espai restringit

Per tal que la capa d'autenticació pugui relacionar una zona restringida amb un determinat usuari per dur a terme la comparació de posicions, el controlador haurà de disposar d'una

relació entre els noms d'usuaris de les ENTITATS LMA que cobreix i els seus respectius usuaris LMA.

D'aquesta manera, es tindrà constància en tot moment de quin usuari LMA s'està protegint, independentment del nom d'usuari que aquest utilitzi com a credencial per a un determinat espai privat.

Entitats d'un servei LMA.

Cada una de les entitats que integrin un controlador LMA han de pertànyer a la vegada a un usuari LMA, per tal de poder controlar les accions d'aquesta entitat LMA des de l'arquitectura.

Per altra banda,LMA ofereix interfícies específiques per a cada un dels diferents serveis implementats, on l'usuari propietari de l'entitat podrà consultar diferents dades, tant del servei que se li està oferint, com dels usuaris LMA que s'estan beneficiant de la validació LMA en les zones restringides que ofereix.

Detecció de la posició de la zona accedida o del mitjà utilitzat per accedir a aquesta zona.

Segurament aquesta és la part on cada un dels serveis distaran més en quant a disseny i implementació. No es pot definir un forma específica de com un servei ha de captar la posició de la zona que un usuari accedeix, doncs dependrà totalment tant del tipus de zona que s'estigui accedint com del mitjà o credencials que es facin servir per accedir-hi.

La única restricció per al disseny d'aquesta part del servei són les dades de sortida que s'han d'enviar cap a la capa d'autenticació.

La taula següent mostra la informació de sortida que un servei LMA ha de tenir i la forma en que aquesta informació es requerida per part de la capa d'autenticació:

Dada	Forma
Posició d'accés	Longitud i latitud de la posició de la zona accedida (o mitjà d'accés a la zona)
Marge d'error de posició d'accés	Des del controlador, s'envia un marge d'error en quant a la posició de l'accés, per tal de que la capa d'autenticació estableixi un llindar de tolerància a l'hora de dur a terme la comparació de posicions.
Entitat propietària de la zona d'accés	Nom d'usuari LMA de l'entitat propietària de la zona d'accés
usuari LMA	Nom d'usuari LMA que està realitzant l'accés.

4.2 Nucli LMA. Capa d'autenticació del sistema

Perseguint el repte de crear una arquitectura transversal en l'àmbit de la seguretat en espais personals, s'ha dut a terme un disseny molt acurat de cada un dels components que la composen, i s'ha fet una recerca acurada de quines són les tecnologies a fer servir com a base de la implementació del sistema que acompleixen en propietats els propòsits del sistema.

Així doncs, és hora de posar fil a l'agulla i veure quin ha estat el procés de convertir la idea LMA en un producte real i funcional.

4.2.1 Selecció de tecnologies per donar vida al nucli o capa d'autenticació de LMA

El nucli de l'arquitectura LMA, també com a capa d'autenticació del sistema, es basa en un servidor web Apache on es reben les peticions de validació per part dels diversos mòduls perifèrics que controlaran les diferents zones contemplades on un usuari LMA pot accedir.

En aquest servidor es realitzen les comprovacions de posició dels usuaris respecte a l'espai que estan accedint. Així doncs, en aquesta banda del sistema es troben en tot moment les posicions actualitzades dels usuaris, per poder autenticar l'accés en qualsevol moment.

Servidor Apache com a nucli central de LMA

La tria de la tecnologia Apache ha estat, principalment, per raons de suport de les principals tecnologies de desenvolupament web que treballen en la banda del servidor. Aquest, s'integra de forma nativa tant amb diversos motors de bases de dades com amb el llenguatge de programació PHP, tecnologia que a la vegada proporciona infinitat de frameworks integrables que serveixen com a plataforma d'accés als serveis web dels principals proveïdors de serveis de la xarxa, com ara Motors de cerca o xarxes socials.

En primera instància es podria pensar en un seguit de desavantatges d'aquest tipus de servidor, respecte als coneguts servidor d'aplicacions com ara JBoss o Glassfish en quant a la seva capacitat de procés, ja que aquests disposen de la possibilitat de llançar aplicacions independents dins del propi servidor. Però, res més lluny de la realitat, Apache proporciona per mitjà de PHP, la possibilitat de controlar tant la capacitat de procés del sistema, com la seva concurrència de processos comunicant directament amb fils de procés implementats amb llenguatges d'alta eficiència com ara C o C++, equiparant així les seves propietats a les del tipus de servidors esmentats anteriorment.

A més a més, grans proveïdors de serveis com ara importants entitats proveïdores de xarxes socials o els principals motors de cerca existents a la xarxa, utilitzen aquesta tecnologia per a

servir als seus usuaris. Aquests avals, són una de les millors garanties d'estar treballant amb una tecnologia estable, eficient i 100% integrable.

MySQL. Sistema persistent de dades de LMA

Gairebé de forma automàtica, després de seleccionar la tecnologia Apache per alimentar el nucli de l'arquitectura, s'escull MySQL com a gestor de Bases de Dades per a donar forma al sistema de persistència de dades de LMA.

[Font: http://www.mysql.com/]

MySQL es famós per ser el gestor escollit per totes les aplicacions web que no requereixen ni d'un gran volum de dades ni d'un elevat nombre de peticions de forma concurrent. D'entrada això no agrada massa tenint en compte les ambicions de LMA, però, fent una mica de recerca sobre aquesta tecnologia, es descobreix que les coses han millorat molt per a MySQL en els últims temps. Aquest gestor ja suporta per mitjà de diferents línies del producte com ara MySQL Cluster, tant la possibilitat de distribuir el processament de peticions en diferents punts com la de distribuir les dades i replicar-les en diferents servidors, incrementant així de forma considerable la seguretat del sistema amb que es treballa.

La versió inicial de LMA que es presenta actualment, no fa ús de totes aquestes propietats de distribució de Base de dades, però, es bo saber que en un futur es disposa d'elles en cas de que creixi el sistema de forma considerable.

PHP. Principal eina de programació de LMA

Apache y MySQL, en la majoria dels casos, van de la mà del llenguatge PHP per gestionar i desenvolupar les aplicacions que es beneficiaran d'aquestes dues tecnologies.

PHP, gràcies als diferents frameworks que s'han anat desenvolupant per aquest llenguatge al llarg dels anys per part de diferents entitats o comunitats, s'ha convertit en un eix central capaç d'integrar qualsevol aplicació web que s'implementi, amb els diferents serveis web oferts pels principals proveïdors de serveis que governen la xarxa avui en dia, com ara proveïdors de motors de cerca, xarxes socials o famosos CMS.

Un bon exemple d'algun d'aquests frameworks és el que es coneix com a Zend Framework, utilitzat també per LMA, i que inclou un alt nombre de llibreries que proporcionen capacitat d'integració amb d'altres tecnologies i arquitectures corrent a la xarxa.

Per altra banda, PHP pot treballar com a llenguatge orientat a objectes tal i com es coneixen en d'altres llenguatges com ara Java o C++, fet molt important quan s'implementa una arquitectura des d'una perspectiva modular i escalable.

Plataforma mòbil. Android com a plataforma inaugural de l'aplicació mòbil LMA.

La joia de la corona en quan a funcionament de tot el sistema LMA, probablement siguin els dispositius mòbils que els usuaris LMA utilitzen per a mantenir la seva posició actualitzada en el servidor. Es per això que cal fer un bon anàlisis dels mètodes i tecnologies a fer servir per tal que el procés d'actualització sigui el més eficient possible, però a la vegada usable i transparent per a l'usuari.

Tot i que entra dins dels plans a curt termini de LMA , el fet de portar l'aplicació mòbil de geo-localització d'usuaris a les principals plataformes mòbils com ara IOS (Iphone) , Blackberry OS, Windows Phone (Microsoft) o WebOs (HP), la que inaugura la posada en marxa del sistema és la plataforma de l'empresa Google coneguda com a Android.

A continuació s'exposen les principals raons per les quals s'ha fet la tria d'aquesta plataforma:

- Plataforma mòbil capdavantera per a *smartphones* a nivell mundial en quant a volum d'usuaris i quantitat de dispositius que l'utilitzen. *[Font: Gartner – Maig 2011]*
- Suportada per la companya Google una de les més prestigioses existents en el mercat actual.
- Publicació d'actualitzacions de la plataforma de forma periòdica que solucionen errors de versions anteriors del sistema i/o hi aporten millores visuals o funcionals.
- Multitud de comunitats de desenvolupadors que suporten l'arquitectura i serveixen de gran ajuda a l'hora de desenvolupar aplicacions per a la plataforma.
- Capacitat multi tasca que permet l'execució de serveis de forma transparent a l'usuari.
- Llicència de codi lliure i baix nivell de restriccions per part de la companyia propietària a l'hora de publicar aplicacions per a la plataforma.
- Conegut i més que provat llenguatge Java com a principal eina de desenvolupament.
- Capacitat per a rebre missatges instantanis de tipus "push", que poden ser processats per mitjà d'aplicacions mòbils (des de la versió 2.2 del sistema operatiu).

Tecnologia "PUSH Messages" com a forma de comunicació entre el nucli de l'arquitectura i els terminals Android dels usuaris LMA.

LMA vol avisar directament als dispositius mòbils dels usuaris quan es detecti una anomalia en els accessos a alguna de les seves zones privades.

Per a fer-ho s'han avaluat les diverses tecnologies que existeixen per dur a terme aquesta comunicació entre el servidor LMA i els dispositius dels seus usuaris:

- *Missatge curt SMS/MMS*: Aquesta metodologia, tenint en compte que un dels prerequisits per utilitzar els serveis de LMA és disposar d'un dispositiu mòbil amb connexió de dades, queda descarta d'arrel, degut a les seves limitacions en quant a

volum d'informació per missatge, i pel fet de que es facturin de forma individual fora de les tarifes de dades que ofereixen les operadores.

- *Email*: Aquesta va ser la idea inicial per a dur a terme el sistema d'avisos de LMA. Qualsevol dispositiu amb connexió de dades, en la majoria dels casos, té assignat per part de l'usuari un dels seus comptes de correu. Així doncs en el moment que aquest rep un nou correu electrònic el dispositiu avisa d'aquest nou element a la bústia d'entrada per mitjà d'una notificació. Per altra banda, la recepció d'aquest tipus de missatges queda inclosa dins de les tarifes de dades dels dispositius mòbils, fet important també per tal de no influir de forma negativa en la factura telefònica de l'usuari.

La tecnologia mail, acompleix quasi completament els objectius de LMA en quant a fer saber a un usuari de forma instantània que un intrús està accedint a un dels seus espais privats, però ben aviat, es detecta una limitació important en aquesta tecnologia. Els missatges email, no poden ser processats per una aplicació corrent en el dispositiu mòbil com a missatge de dades amb diferents paràmetres d'informació. El format és estàndard i es limita a un títol i un cos de missatge, és a dir no és personalitzable en quant a forma.

És per això que, indagant una mica més en la matèria, es descobreix el sistema de missatgeria de tipus PUSH proporcionat per el servei de Google "Cloud to Message Device" (C2DM).

Les propietats d'aquests tipus de missatges, queden molt per davant de les tecnologies esmentades anteriorment, tenint en compte els propòsits de LMA.

Aquests són totalment personalitzables en forma, i permeten incloure tants camps com es desitgi amb tipus de dades de format text. A més a més, es poden processar a mode d'interrupció per part d'una aplicació mòbil corrent en un terminal Android, fet que farà l'aplicació per a mòbils LMA molt més atractiva i útil per als usuaris.

Estàndard JSON . Protocol per a la missatgeria interna de l'arquitectura LMA.

En el moment que és planteja la definició d'una arquitectura que es composi de diversos mòduls, s'ha de fixar un "idioma" comú per a tots aquests mòduls, tant per a comunicar-se entre ells, com perquè aquests siguin capaços de parlar amb el nucli del sistema, en aquest cas, la capa d'autenticació LMA.

És per això que, tenint en compte que el tipus de informació que ha de fluir entre els diferents components de LMA no són grans volums de dades binàries, sinó que es tracta de trames de dades de tipus text en la seva majoria, s'ha escollit el protocol de comunicació JSON ((JavaScript Object Notation) com a tecnologia principal per a comunicar els diferents mòduls que composen l'arquitectura.

Són moltes les avantatges d'utilitzar protocols de comunicació dels quals es disposa d'una especificació formal que els avali com a estàndard, ja que això fa que existeixin llibreries per a tot tipus de tecnologia, fet que garanteix poder tractar amb el protocol de forma eficient sigui quina sigui la tecnologia implementada en un determinat punt o component de l'arquitectura.

Per altra banda, JSON facilita molt la feina quan es treballa amb la tecnologia web AJAX per a implementar qualsevol capa de presentació web, tal i com és el cas del site LMA que ofereix una pagina personal a cada un dels seus usuaris on es mostra informació sobre l'estat dels comptes LMA.

En definitiva, es tracta d'un idioma que tota tecnologia sigui del tipus que sigui entén i implementa, convertint el seu ús en una garantia més de integrabilitat i escalabilitat de l'arquitectura.

4.2.2 Procés de validació d'un usuari per part del nucli LMA

En aquesta capa del sistema, la d'autenticació, és on es decideix l'autenticitat d'identitat d'un usuari en el moment que aquest accedeix a alguna de les seves zones restringides.

Per a fer-ho, en si mateixa únicament disposa de la posició actualitzada dels usuaris LMA, i seran els mòduls que treballen en la capa de controladors de l'arquitectura, els que proveiran de la informació necessària per detectar la posició de l'accés.

Un cop es tenen ambdues posicions, es porta a terme una comparació de geo-localitzacions la qual defineix un accés com a vàlid o sospitós.

En cas de que es detecti un accés sospitós, aquesta mateixa capa d'autenticació envia un avís instantani al dispositiu android de l'usuari LMA propietari de l'espai accedit, fent ús del servei *Cloud to Message Device* que Google posa a l'abast de forma gratuïta (versió limitada) per tal d'enviar missatges del tipus PUSH des de la xarxa a terminals Android amb connexió de dades.

Aquesta comparació és configurable per part de cada un dels mòduls controladors en quant a precisió de posicions exigida, doncs, depenent del tipus de zona accedida amb que es tracti, s'exigirà un radi de seguretat més o menys ampli respecte la posició del dispositiu mòbil de l'usuari. La informació sobre aquest marge de seguretat forma part del paquet d'informació enviat des de la capa de controladors quan demana processar una autenticació d'usuari.

Per acabar d'entendre com es porta a terme aquesta validació d'usuari per part de la capa d'autenticació del sistema, a continuació es mostra un diagrama de seqüència de tot el procediment.

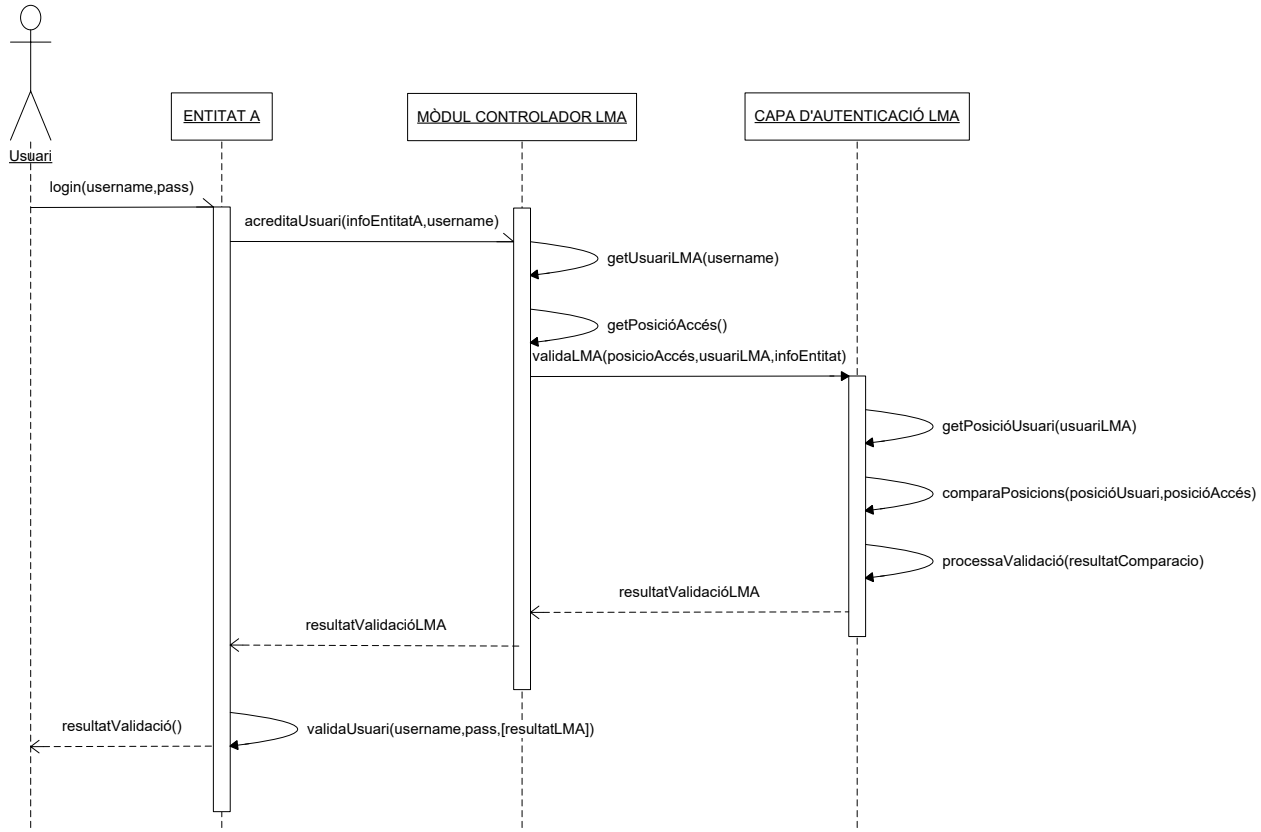

figura 2. Diagrama de seqüència: Validació d'usuari en la capa d'autenticació LMA

Tal i com s'aprecia en el diagrama, aquesta validació duta a terme per el sistema LMA, no és intrusiva en quant a permetre l'accés o no a una zona privada, sinó que senzillament vol ser un servei a tercers que aporti aquest grau addicional de seguretat alhora d'acreditar a un usuari.

Serà la funció de validació independent de LMA que l'entitat A faci servir per autoritzar als seus usuaris en els seus espais restringits, la que opcionalment podrà utilitzar el resultat de la validació LMA com a criteri de decisió a l'hora de permetre o restringir l'accés.

4.2.3 LMA Groups. Autoritzacions d'accés en un espai per a múltiples usuaris LMA

Analitzant la usabilitat del producte LogMeApp s'arriba a la conclusió de que sovint un mateix grup d'usuaris poden accedir a un espai restringit utilitzant les mateixes credencials d'accés.

És per això que es defineix el concepte LMA Groups, el qual permet crear grups d'usuaris autoritzats per accedir a una determinada zona privada.

D'aquesta manera, establint aquests grups d'usuaris de confiança, en el moment que arribi una petició de validació per part d'un controlador d'espais cap a la capa d'autenticació, aquesta no tan sols comparerà la posició de l'accés amb l'usuari que està accedint, sinó que si troba algun usuari del seu grup de confiança en la posició de l'accés, LMA considerarà l'accés com a segur.

Tot i així, tenint en compte que la confiança entre les persones és un concepte alterable amb el temps, és deixarà constància d'aquest accés en el registre d'accessos de l'usuari del qual s'ha tramitat l'accés.

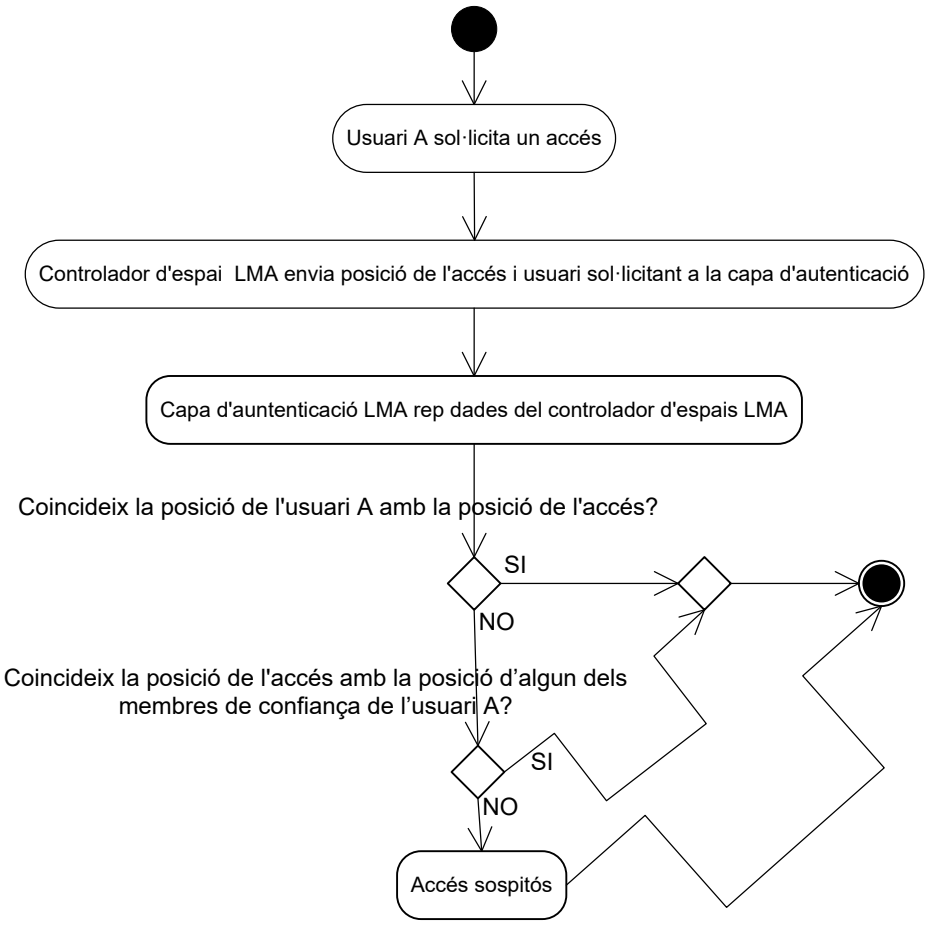

figura 3. Diagrama d'activitat: validació d'un usuari amb LMA Groups

La definició i modificació d'aquests grups de confiança entre els usuaris LMA, és una de les funcionalitats de l'espai web que LMA proporciona a cada un dels seus usuaris.

4.3 Controlador d'espais LogMeApp WebNet

El nucli del sistema LMA manté un sistema de dades actualitzat amb les posicions en temps real de tots els seus usuaris, però, en si mateix, no pot dur a terme capa procés de validació de no ser per la informació que rep dels mòduls controladors de les zones accedides, els quals li proporcionen la posició dels accessos a aquestes quan és necessària.

És per això, que per tal d'inaugurar l'arquitectura com a producte complet i funcional, s'ha dissenyat i implementat un dels mòduls que probablement abordi l'àmbit on un usuari disposa de més zones restringides avui en dia: La xarxa

4.3.1 Objectius del mòdul LMA WebNet

Durant tot el document s'ha parlat del fet de localitzar la zona on accedeix un usuari per tal de dur a terme una validació de presència. Des d'un punt de vista abstracte, aquest plantejament és correcte, doncs si es vol accedir a "A" d'una forma o altre l'usuari que està realitzant l'accés s'ha de trobar, almenys, amb predisposició per accedir a aquest espai "A"; altrament, vol dir que algú altre està intentant accedir a una zona restringida en la qual no està autoritzat.

Bé doncs, en el cas dels comptes d'usuari que es creen de forma personal en els diversos proveïdors de serveis com a ara webmail o xarxes socials, el concepte de "posició de zona restringida" s'ha d'extrapolar cap a la posició del mitjà que s'empra per a dur a terme aquest accés. Es considera que la porta d'entrada a aquest tipus d'espais privats se situa en cada un dels terminals des d'on un usuari accedeix als seus comptes, és a dir a la banda del client, i no pas en el propi servidor que allotja la pàgina on s'accedeix.

4.3.2 Components del mòdul LMA WebNet

4.3.2.1 Identificació de terminals amb accés a la xarxa

En el cas del mòdul web, la idea es que cada un dels usuaris LMA disposa d'una col·lecció de punts d'accés identificats de forma única per part del sistema LMA dels quals es disposa de la geo-localització exacta a on es troben aquests terminals.

Aquests identificadors únics es fan accessibles des de la banda del servidor, gràcies als navegadors web dels usuaris, els quals, per mitjà de la implementació de plugins específics per a tal efecte, els fan visibles a les pàgines web subscrites a LMA per mitjà d'una *cookie*.

Gràcies a aquesta metodologia, un usuari por indicar en tot moment on es troba el seu terminal d'accés, per tal de fer efectiva la validació d'identitat LMA en les diferents pàgines web on aquest accedeixi .

A part, de la forma que s'ha implementat aquesta part del sistema, un usuari rebrà un avís en el seu navegar, en quan es detecti un moviment del terminal des del qual s'està connectant, per tal de que aquest afegeixi nou punt d'accés en el servidor LMA WebNet.

4.3.2.2 Geo-localització W3C definida en el nou estàndard HTML5

Aquesta detecció del canvi de posició d'un terminal per part del plugin del navegador, es duu a terme utilitzant la col·lecció de funcions de geo-localització W3C que s'ha especificat en el nou estàndard web HTML 5 i que implementen les últimes versions dels navegadors existents en el mercat com ara Mozilla Firefox 4, Chrome 8.5+ o el nou Internet Explorer 9 de la firma Microsoft.

El mètode més precís que existia abans de l'especificació d'aquest nou estàndard per tal de localitzar un terminal amb accés a la xarxa, era per mitjà de l'adreça IP externa amb que aquest terminal accedia a Internet.

La precisió d'aquesta metodologia sempre ha deixat bastant que desitjar, doncs la localització IP és du terme, o bé per mitjà de base de dades que emmagatzemen la localització d'ips estàtiques (sovint poc actualitzades) , o bé per dades que proporcionen les diferents operadores sobre les ips dinàmiques i/o estàtiques que assignen als seus clients per zones, fet que fa que la geo-localització d'aquestes IPS siguin amb un marge d'error, sovint inclús de kilòmetres de distància.

Res a veure doncs amb la precisió que HTML5 ha aconseguit a l'hora de geo-localitzar un navegador d'Internet, doncs pot arribar a afinar, i sovint ho fa, fins a la porta de qualsevol domicili que es trobi en una zona mínimament poblada.

No es pretén descriure en aquest document, com HTML5 posiciona a un navegador web amb tanta precisió, però com a dada curiosa, només indicar que entre els seus mètodes de posicionament, es troba el de fer un seguiment dels noms assignats a les xarxes sense fils que es troben al voltant del terminal en qüestió, les quals han estat prèviament localitzades per els vehicles encarregats de fer la captura d'imatges del famós sistema Google Street View.

Com a resultat d'aquesta identificació única de cada un dels punt d'accés d'un usuari, el mòdul controlador LMA és capaç de identificar i relacionar amb una posició concreta el mitjà d'accés que aquest està utilitzant.

Finalment, el procés que ha de seguir un usuari, un cop tingui instal·lat en el navegador el plugin pertinent serà:

- Acreditació al compte d'usuari LMA per mitjà d'usuari i contrasenya.

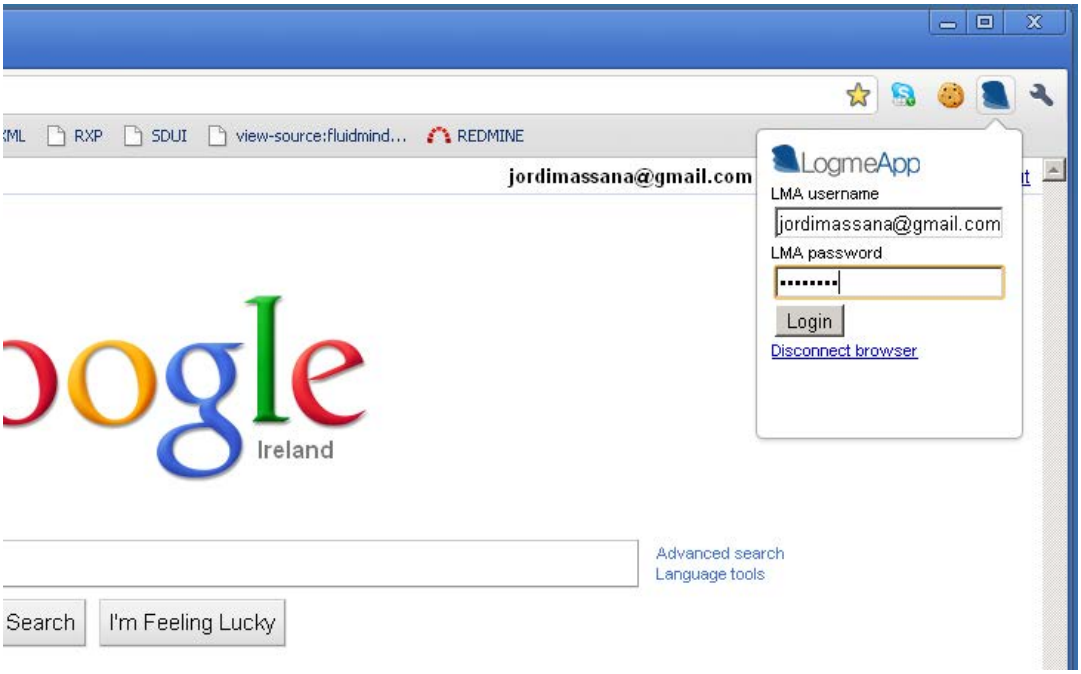

figura 4. Login en el plugin d'identificador de terminal per al navegador

-Selecció de terminal o inclusió d'un nou punt de connexió.

Un cop l'usuari s'ha loguejat al servidor LMA, té l'opció de seleccionar un punt de connexió ja conegut pel sistema, o be introduir-ne un de nou. Automàticament el plugin ens detectarà la posició del punt d'accés per mitjà d'HTML5 i l'estàndard de geo-localització definit per W3C.

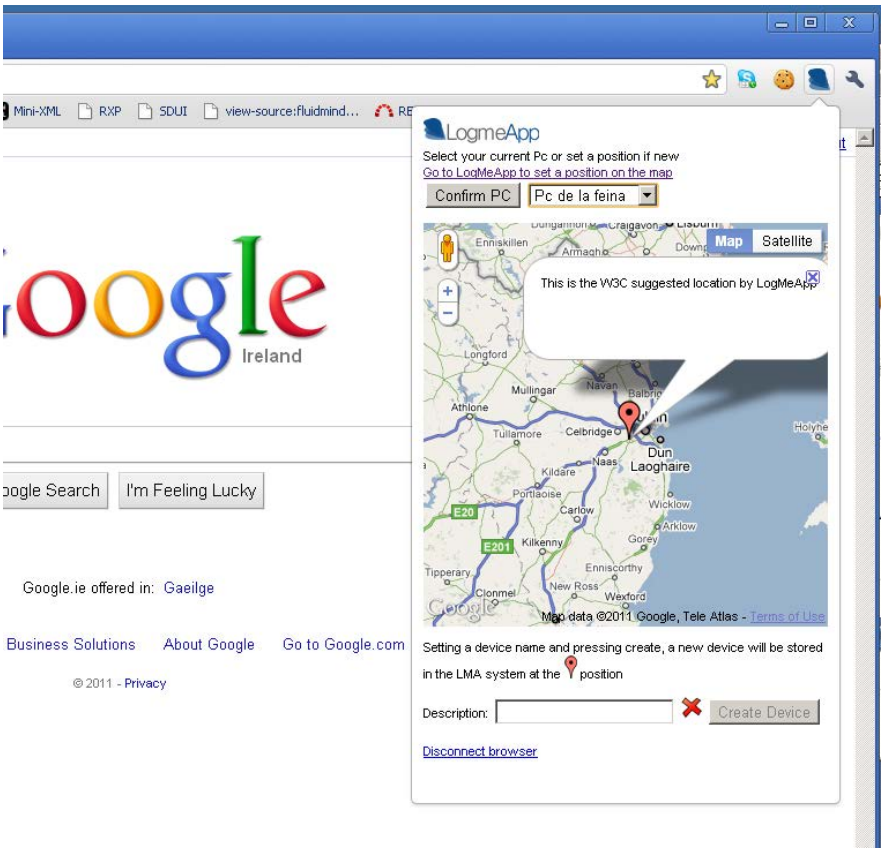

figura 5. Selecció de terminal en el plugin d'identificador de terminal per al navegador

- Finalment, el navegador indicarà que el terminal des del que s'està accedint a la xarxa, serà identificable per part de les webs que implementin la seguretat LMA.

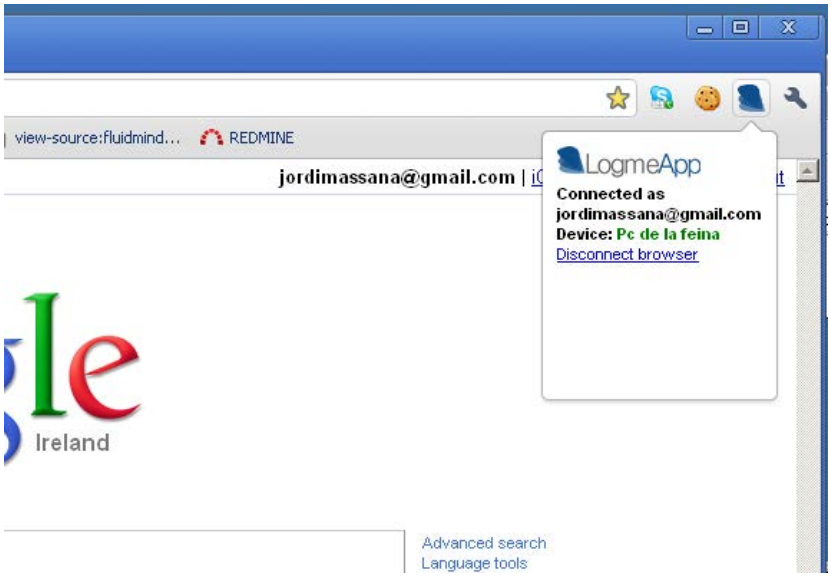

figura 6. Navegador connectat al servidor LMA

4.3.2.3 Entitats LMA subscrites al mòdul LMA WebNet

Com s'ha comentat anteriorment en la proposta de directrius de disseny a l'hora de crear un mòdul controlador per a LMA, aquest haurà de tenir en compte i mantenir de forma persistent dins del seu sistema de dades, la informació relativa a les ENTITATS a qui pertanyen les zones restringides que aquests usuaris LMA accedeixen. En aquest cas, aquestes entitats seran les diferents webs que ofereixin una espai personal dins del seu entorn web.

Així doncs, el mòdul controlador disposarà de la següent informació en seu sistema persistent de dades per a cada una d'aquestes entitats LMA.

Hosting Server	Adreça on s'ubica el servidor de hosting que allotja la pàgina web entitat
Domain	Domini únic d'accés a la pàgina web entitat.
API_KEY	Clau proporcionada pel sistema com a credencial de entitat LMA
owner	Usuari LMA propietari de la Web Entitat

Extrapolant el diagrama de seqüència anterior, on es feien referències genèriques al mòdul controlador i les entitats LMA sota el seu control, tindrem el següent per al cas específic del controlador d'espai LMA WebNet.

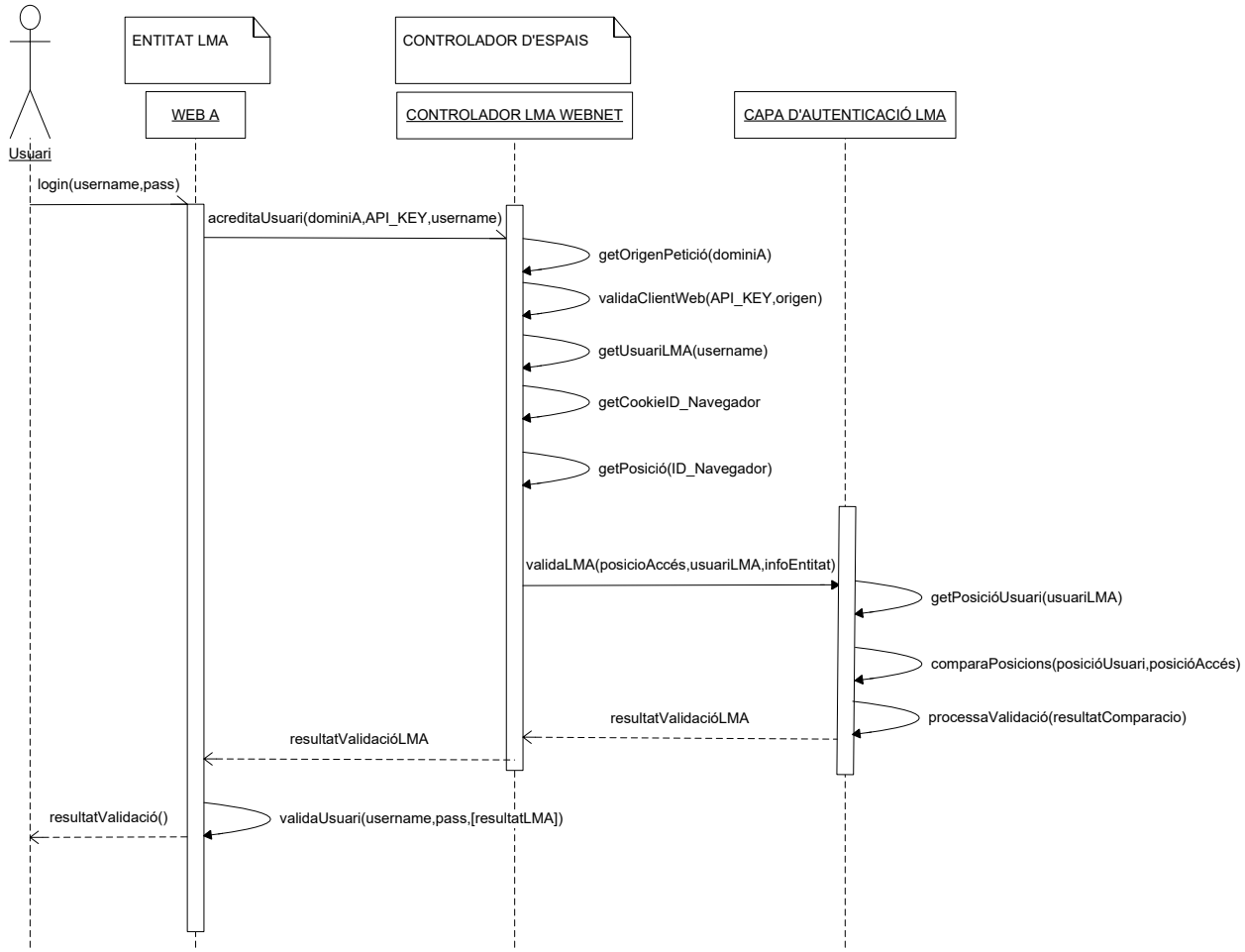

figura 7. Diagrama de seqüència: Validació d'usuari en la capa d'autenticació LMA i el controlador WebNet

4.3.2.4 API LMA WebNet. Comunicació controlador LMA WebNet - nucli LMA

Per a cada una de les entitats subscrites al mòdul LMA web, es proporciona als administradors de les pàgines una API que facilita les funcions necessàries per comunicar amb la capa d'autenticació per tal de dur a terme una verificació d'identitat d'algun dels seus usuaris.

Concepte API KEY

Per tal de que aquesta API tingui una distribució controlada i no es pugui sol·licitar una validació al nucli LMA des de qualsevol implementació realitzada fora de un mòdul verificat per LMA, els administradors web tenen assignada una API KEY única que els permet fer ús de forma exclusiva d'aquestes funcions de comunicació/validació.

La obtenció d'aquesta API KEY per part d'un administrador Web es porta a terme per mitjà del següent procediment descrit en forma de diagrama de seqüència.

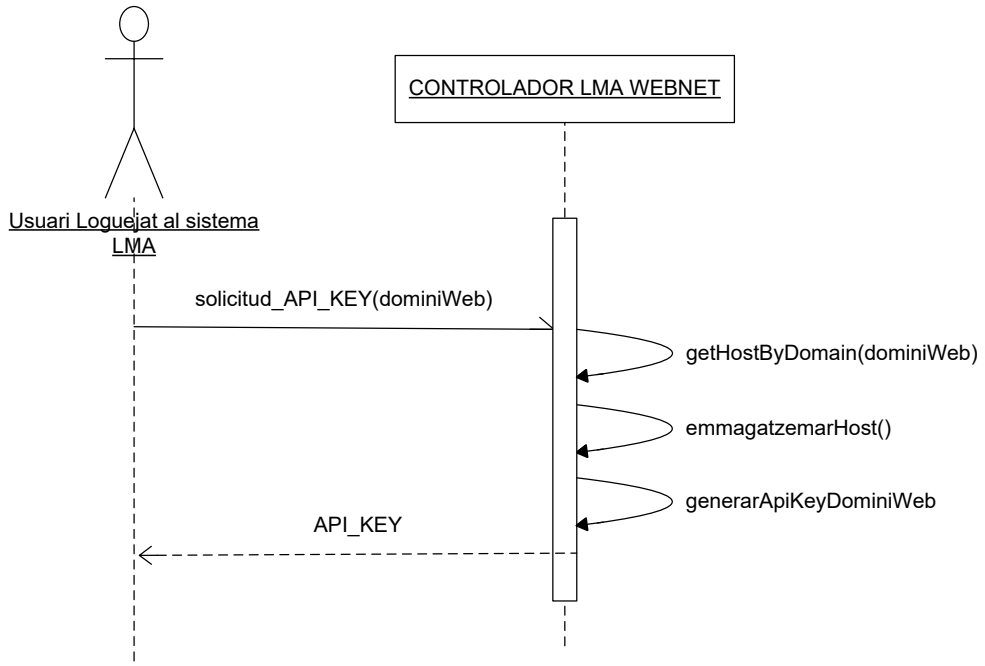

figura 8. Diagrama de seqüència: Procés de sol·licitud d'una nova API KEY LMA

D'aquesta manera, si un web sol·licita una validació d'usuari al nucli LMA però la petició no prové del l'adreça de Host enregistrada en el moment de la sol·licitud de la API_KEY per al domini de la pàgina demandant, la petició de validació serà ignorada.

4.3.3 Integració del mòdul LMA Webnet

4.3.3.1 Integració de la API LMA WebNet en una web de forma programàtica

Seguint la filosofia de crear un producte fàcilment integrable amb els sistemes en actual funcionament, la API LMA WEB s'ha dissenyat pensant en que qualsevol propietari d'una web que disposi d'una zona restringida per a usuaris registrats en pugui fer ús, ja sigui un programador web avançat o un administrador web sense nocions de programació.

Crida a la funció de validació LMA WEB des de una Web Programada

En el moment que s'administra una web programada d'arrel, sense fer ús de cap CMS, (Content Management System) se sobreentén que si aquesta disposa d'espais personals per als seus usuaris, darrera d'aquesta pàgina hi ha un programador amb unes mínimes nocions sobre el que és una llibreria i alguna línia de codi.

Per aquests casos, el programador web només haurà d'afegir una línia de codi dins la funció que valida als seus usuaris per mitjà del nom i la contrasenya, per tal de que aquests es beneficiïn de la protecció de LMA.

De forma genèrica, considerant un formulari típic d'autenticació web, i un script php de validació de credencials, la crida a la funció de validació LMA es farà de la següent manera:

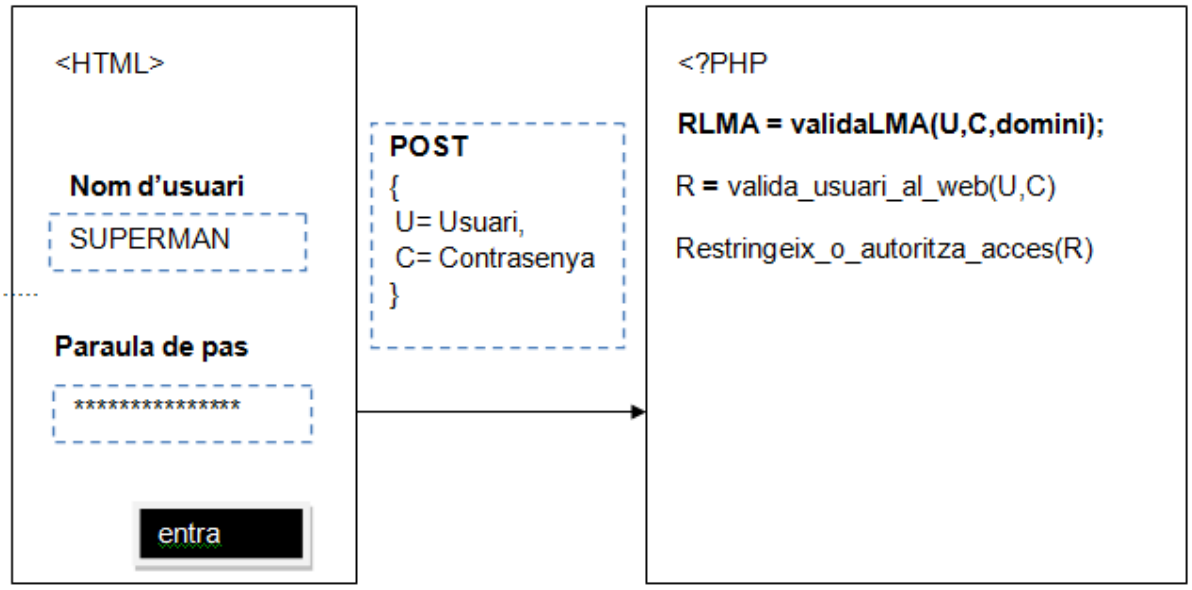

figura 9. Integració de la API LMA WebNet en una pàgina web

Les tasques que aquesta funció de validació realitza (“validaLMA()”) de forma transparent tant per a l’usuari com per al administrador web són:

- Obtenció del usuari LMA corresponent al usuari WEB que està accedint a l’espai restringit.
- Obtenció de l’identificador únic de terminal, que el plugin instal·lat en el navegador de l’usuari fa accessible.
- Consulta a la base de dades LMA WEB sobre la posició assignada al identificador de terminal obtingut.
- Enviament de les dades obtingudes sobre el posicionament, el corresponent usuari LMA, i el domini que sol·licita l’autenticació cap a la capa d’autenticació.

L’exemple anterior, també mostra que la funció de validació LMA pot tenir o no efecte en el moment de decidir si s’autoritza o no l’accés a una pàgina web. Serà el programador de la web qui decidirà si utilitza o no el resultat de la validació LMA per a prendre aquesta decisió.

Relació entre els usuaris subscrits a una web amb el seu corresponent usuari LMA

Per tal de poder realitzar l’acreditació de presència LMA, la capa d’autenticació, la qual recordem que només disposa de la informació relativa a la geo-localització dels usuaris LMA, necessita saber a quin usuari LMA correspon el usuari que s’està *loguejant* a la web.

Per tal d’enregistrar aquesta relació dins del mòdul web de LMA, les pàgines subscrites al servei hauran de fer una crida a una funció de la API amb els dos noms d’usuari: l’usuari web i l’usuari LMA.

Per tal de cridar aquesta funció específica, es facilita una interfície web (també inclosa dins de la API LMA) on per mitjà d’una caixa de text i un botó de subscripció els usuaris registrats d’una web podran introduir quin es el seu usuari LMA per tal que el controlador d’espais realitzi la relació USUARI WEB – USUARI LMA

4.3.3.2 Integració de la API LMA WebNet amb els principals Gestors de Continguts

En els temps que corren, gràcies als famosos gestors de continguts, tothom , i cal emfatitzar en la paraula tothom, pot disposar de la seva pàgina web personal amb zones restringides per a usuaris registrats.

Aquests gestors, un cop el CMS s’ha instal·lat en el servidor, proporcionen una interfície al administrador, per mitjà de la qual aquest és capaç de gestionar els continguts de la web en quant al tipus, els menús mostrats, els elements de cada un dels menús, la aparença de la web, etc. Tot de forma molt senzilla, usable i intuïtiva.

Una altra propietat d'aquests coneguts CMS és la possibilitat que ofereixen per instal·lar-hi mòduls de tercers que dotin la pàgina web que gestionen de funcionalitats addicionals.

Aquí és on entra LMA WEB creant una versió de la API a mode de mòdul instal·lable per als tres gestors de continguts més emprats actualment:

- Joomla
- Blooper
- Wordpress

Gràcies a aquests mòduls, els administradors seran capaços per mitjà de simples menús navegables, de mostrar als seus usuaris el formulari de subscripció de la web al seu compte LMA per tal d'enviar la relació "usuari web-usuari LMA".

Per altra banda, el mòdul també ofereix la possibilitat de substituir el formulari de logueig a la pàgina per als usuaris que porten els CMS per defecte, per un que implementa la funcionalitat d'enviar la petició de validació a la capa d'autenticació LMA.

A continuació és mostra un exemple de funcionament per al CMS Joomla.

La interfície següent és el panell de configuració estàndard per a extensions del CMS.

La banda dreta, mostra els paràmetres de la extensió, on l'usuari introduirà el domini de la pàgina i la api key que ha obtingut en subscriure-la al servidor LMA.

Com es veu, integrar LMA en una web és d'allò mes senzill, ja que aquest plugin modifica el mòdul de Login que Joomla porta per defecte, afegint la característica d'enviar la petició de validació LMA quan usuari accedeix a la seva zona restringida dins de la pàgina.

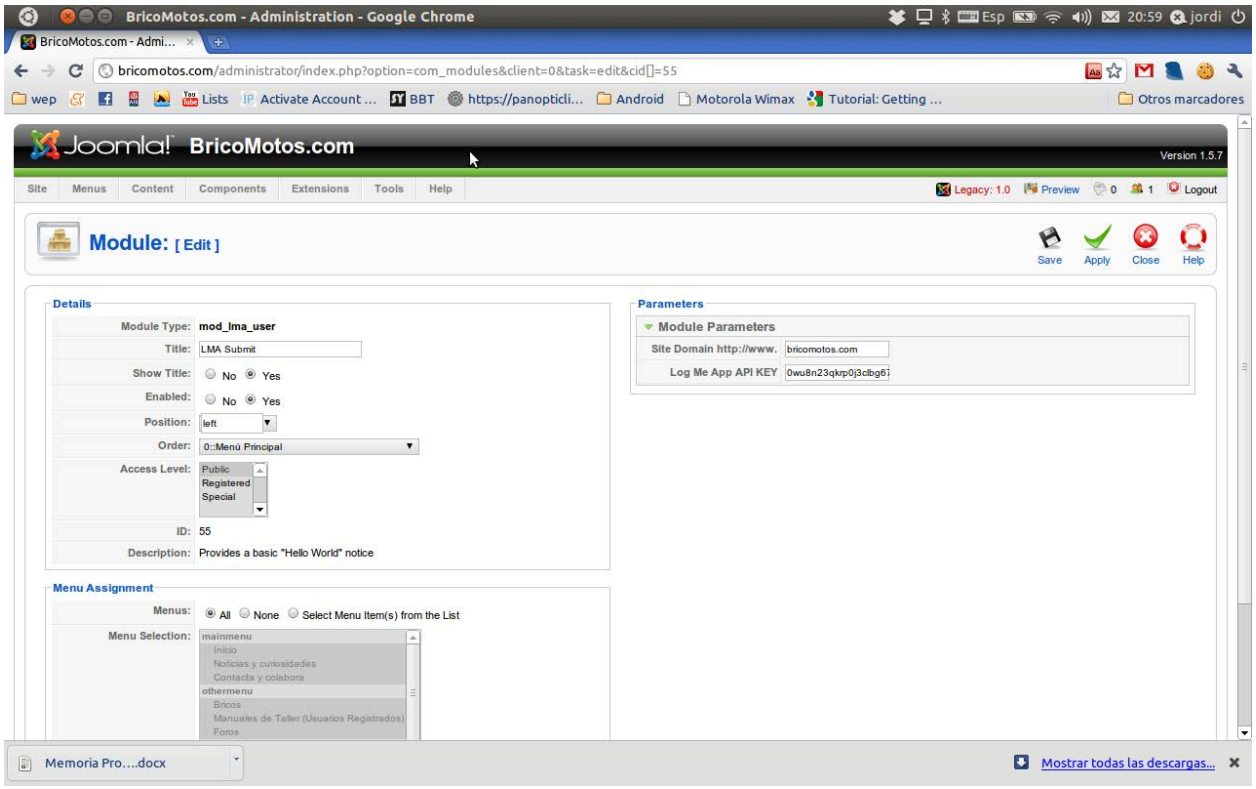

figura 10. Integració de la API LMA WebNet en el CMS Joomla

[Font: www.bricomotos.com – panell d'administració]

5. Interfícies d'usuari LogMeApp

Una part d'important de tota l'arquitectura LMA, i potser de la qual depengui l'èxit o fracàs del producte que es planteja, és la manera amb que aquest es presenta, tant als seus usuaris, com a les entitats que ofereixen els serveis a una determinada comunitat.

És per això que s'han tingut en compte tots els factors possibles, de cara a crear una capa de presentació útil, intuïtiva i usable de tota l'arquitectura.

5.1 logmeapp.com: espai web d'administració per a comptes d'usuari

LMA ofereix un espai personal per a cada un dels seus usuaris, des de on aquests poden donar-se d'alta com a usuaris del servei i gaudir d'un registre de tots els accessos realitzats a les seves zones restringides subscrites a LMA.

Així doncs, es defineix una zona restringida d'usuari del tipus web, per a que aquests puguin dur a terme el control dels seus comptes LMA. Com no podia ser d'altre manera, aquestes zones restringides LMA són controlades a la vegada pel mòdul controlador LMA WebNet. LogMeApp es realimenta!

5.1.1 Registre d'accessos a zones restringides

Per a cada un dels accessos detectats per LMA els usuaris en poden consultar els següents detalls:

- Entitat proveïdora de la zona accedida
- Posició de la zona o del mitjà d'accés a aquesta zona.
- Posició del propi usuari en el moment que s'ha realitzat l'accés.
- Nivell de seguretat de l'accés en funció dels resultats de la comparació entre la posició de l'usuari i la posició de la porta d'accés a la zona accedida.

A continuació es mostra un exemple de pàgina personal LMA mostrant la informació sobre un accés sospitós en un dels seus espais.

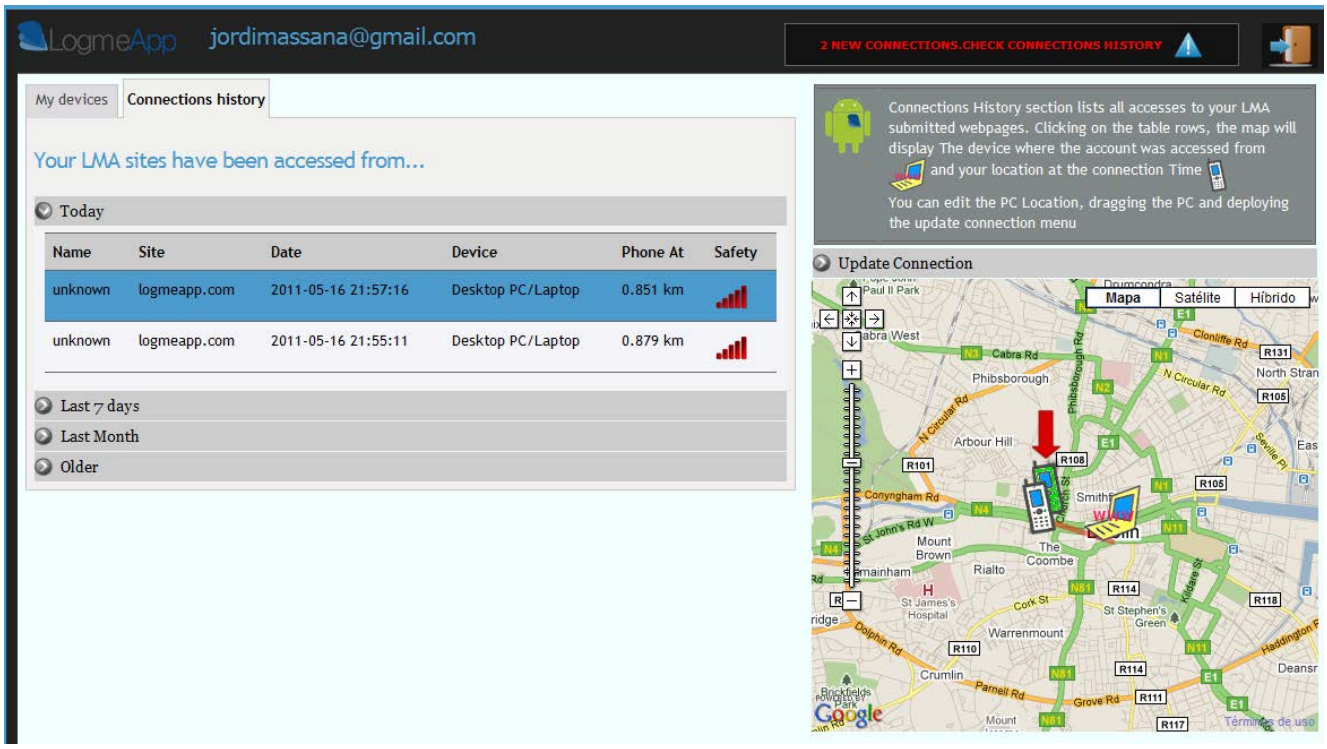

figura 11. logmeapp.com : Visualització d' un accés sospitós

- El mòbil verd indica la posició actual de l'usuari.
- El mòbil blanc indica la posició on es trobava l'usuari en el moment de l'accés.
- El portàtil groc representa l'origen de l'accés a la zona privada.

Per altra banda, aprofitant les propietats del conegut fenomen Web 2.0, l'aplicació WEB de LMA permet instal·lar mòduls addicionals des de la pròpia pàgina, per tal de que els usuaris LMA puguin beneficiar-se dels detalls proporcionats també per cada un dels mòduls controladors de LMA.

Així doncs, un usuari disposarà d'un llistat de mòduls a instal·lar, que aquest podrà seleccionar o no en funció de si té algun espai controlat pel mòdul controlador en qüestió.

Mòdul LMA WebNet per a l'aplicació Web de LMA.

LMA WebNet disposa d'un mòdul instal·lable per a l'aplicació Web de LMA, que proporciona detalls concrets sobre l'ús dels serveis Webnet per part d'aquests usuaris, com ara el llistat de Pàgines web en les quals disposen de zones restringides controlades per el sistema LMA.

Per altra banda, aquest mòdul també proporciona les eines necessàries per als administradors web que desitgin proporcionar per als usuaris de la seva pàgina la seguretat LMA.

D'aquesta manera, per mitjà de la mateixa aplicació LMA WEB, es permet realitzar procés de subscripció de pàgines web als serveis de WebNet i l'obtenció de la API LMA Webnet descrita anteriorment.

Finalment, un usuari que instal·li aquest mòdul en la seva pàgina personal de LMA obtindrà la següent interfície:

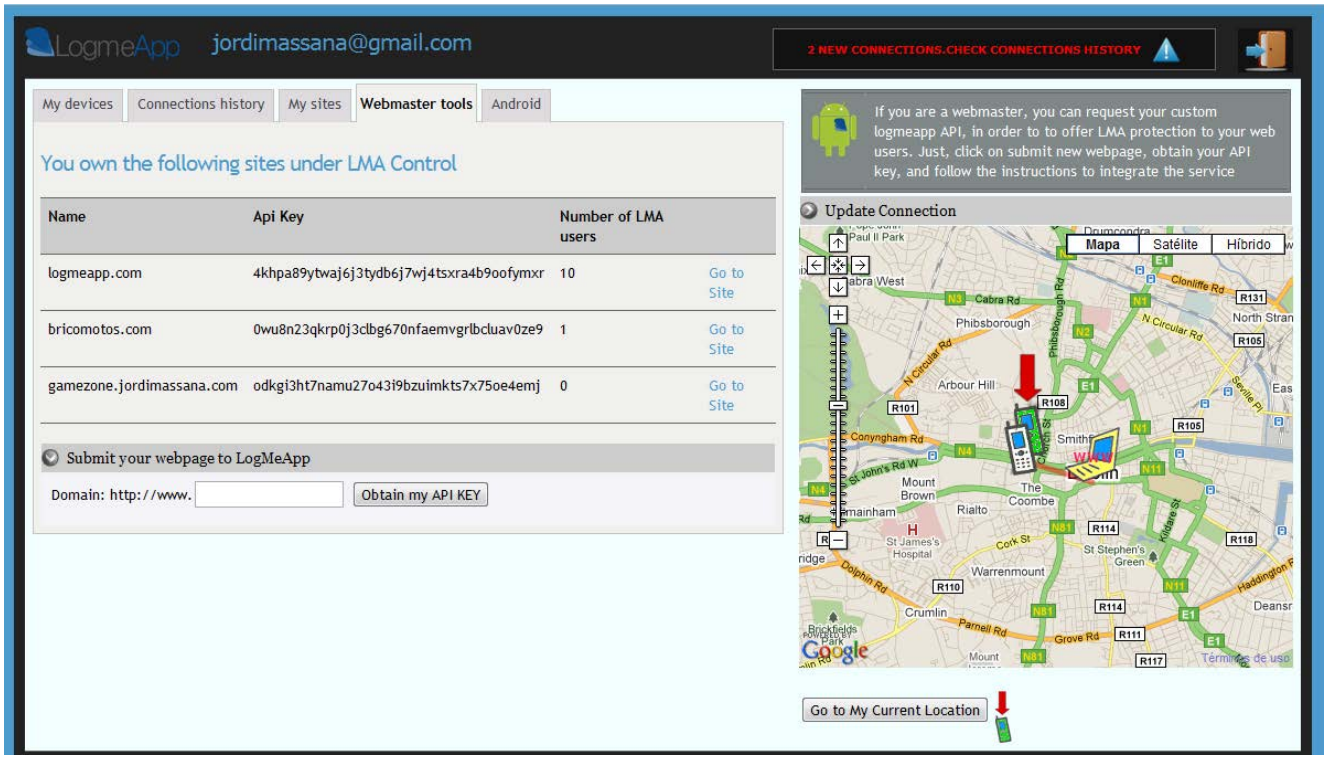

figura 12. logmeapp.com: Mòdul WebNet

En aquest apartat "webmaster tools", un administrador web pot veure en quines pàgines integra al controlador d'espais LMA WebNet per tal d'oferir la protecció LMA als seus usuaris.

També s'observa la interfície que es proporciona des del site per tal d'obtenir una nova API KEY per a un nou domini.

5.1.2 Gestió de LMA Groups. Relacions de confiança entre usuaris LMA

Una altra funcionalitat que el site de LMA ofereix als seus usuaris es la de gestionar els seus grups de confiança. Per a fer-ho es disposa d'un cercador d'usuaris LMA que permetrà anar incloent aquests usuaris dins dels diferents grups que es vagin creant.

Ara bé, aquesta relació ha de ser recíproca. Cada cop que s'afegeixi un usuari LMA dins d'un grup de confiança , aquest rebrà una petició de confiança que haurà d'acceptar i no s'establirà la relació fins que no ho faci.

5.1.3 Control remot del dispositiu mòbil de l'usuari LMA

Aquesta funcionalitat pot ser una de les que faci més atractiu el producte de LMA als ulls d'un usuari, més enllà de l'àmbit de seguretat en accessos que es promulga al llarg de tot aquest document.

LogMeApp inclou en el *site* personal par a cada usuari, una interfície per realitzar certes accions de forma remota sobre els seus dispositius mòbils que tinguin instal·lada l'aplicació mòbil LMA.

Les accions que es permeten realitzar des del site LMA són:

- Bloqueig del terminal.
- Fer sonar el dispositiu per tal de localitzar-lo en un recinte.
- Posicionar el dispositiu en un Mapa.
- Esborrat complet de dades personals del dispositiu.
- Mostrar en pantalla un telèfon de contacte a on trucar en cas de pèrdua.

5.2 LogmeApp: aplicació de control LMA per a dispositius mòbils

Per tal de posar el sistema en funcionament, és crucial que per part dels usuaris LMA s'instal·li l'aplicació mòbil que es proporciona des de l'arquitectura.

La finalitat principal de l'aplicació mòbil LMA és detectar i actualitzar en el nucli del sistema les posicions exactes on es troben cada un dels seus usuaris per mitjà d'un "servei" llançat el primer cop que s'executa l'aplicació i que es deixa corrent de forma permanent i transparent en els terminals dels usuaris, tot i que aquest aturi l'aplicació visual LMA.

Aquesta aplicació es composa de tres components ben diferenciats: servei d'actualització de posició, servei de recepció de missatges push i interfície d'usuari.

5.2.1 Servei d'actualització de posició mòbil

L'aplicació LMA llança un servei que s'executa en segon pla i es deixa funcionant de forma permanent en els aparells mòbils dels usuaris LMA. Aquest servei, un cop l'usuari s'hagi

autenticat en l'aplicació i aquesta hagi obtingut el seu identificador únic dins del sistema,actualitzarà la posició d'aquest en el servidor LMA per mitjà d'un missatge JSON, cada vegada que es detecti un moviment de més de 25 metres del terminal. Aquest llindar de distància, s'estableix per evitar una sobrecàrrega de tràfic de dades degut al moviment de l'usuari dins d'un límits concrets com ara casa seva o el seu lloc de treball.

5.2.2 Servei de gestió de missatges "push"

Per tal de poder rebre els avisos push emesos per part de la capa d'autenticació de LMA, en el moment que es detecten accessos d'origen sospitós, es requereix d'un servei mòbil que serveixi com a porta d'accés per aquest tipus de missatges i implementi les funcions necessàries per tractar aquest protocol.

Aquest servei, com en el cas anterior, s'executa en segon pla de forma transparent a l'usuari la primera vegada que aquest executa l'aplicació LMA en el seu terminal. Cal dir també que la unica part que ha calgut implementar d'aquest component en concret, ha estat una interfície d'alt nivell per gestionar el servei de rebuda de missatges, el qual es proporciona de forma nativa en el sistema operatiu Android des de la seva versió 2.2.

5.2.3 Interfície d'usuari LMA per a dispositius mòbils

La part visual de l'aplicació mòbil LMA permet als usuaris realitzar les mateixes accions que proporciona la interfície WEB LMA. Però a part de poder consultar el registre d'accessos a zones restringides, aquesta interfície visual, la qual es comunica amb els altres dos components serveis anunciats, també proporciona a l'usuari informació sobre els accessos sospitosos que l'arquitectura detecti en temps real.

Les funcionalitats principals de l'aplicació són:

- Rebuda de noves notificacions d'accessos sospitosos en espais restringits.
- Consulta del històric d'accessos realitzats als espais restringits d'un usuari.

Aquesta aplicació s'ha orientat al mòdul LMA WebNet de l'arquitectura, així que també proporciona funcionalitats directament relacionades amb el control d'accessos en espais web:

- Visualització sobre un mapa de l'origen de l'accés per a cada un dels accessos registrats.
- Modificació de la posició d'un terminal d'usuari d'accés a la xarxa conegut pel sistema LMA.

Finalment,passejant un mica per les pantalles principals de l'aplicació es contempla el següent:

- **Pantalla login de l'aplicació al servidor LMA** i selecció de compte de correu de Google que es vol associar al **servei C2DM de Google**, per tal de rebre les notificacions push generades per la capa d'autenticació LMA en cas de detecció d'accessos sospitosos en espais privats.

figura 14. Aplicació Android: Pantalla de login

figura 13. Aplicació Android: Servei C2DM per a notificacions push

- **Pantalla principal de l'aplicació**. Mostra en un mapa la posició actual a on es detecta el nostre terminal. A la banda superior dreta, es disposa de la informació sobre el nombre de **notificacions sobre accessos sospitosos** que s'han detectat.

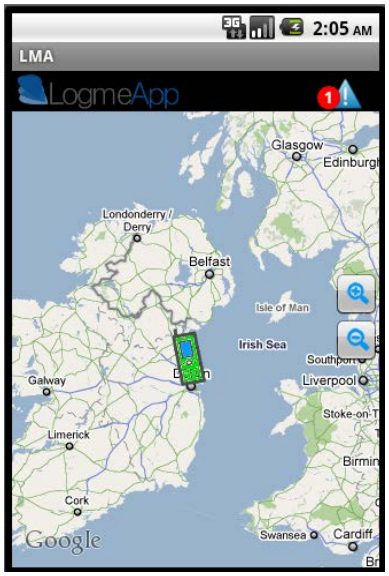

figura 15. Aplicació Android: Pantalla principal

- **Notificacions d'accessos sospitosos**. Pitjant la icona notificacions de la pantalla anterior, es mostra un llistat dels accessos no garantits per LMA que s'han detectat. Aquests es poden seleccionar, i es mostrarà sobre el mapa la següent informació:

    - Origen de l'accés i espai accedit (la posició de l'origen és aproximat en cas de no ser un accés des d'un navegador amb el plugin LMA instal·lat).
    - Posició de l'usuari en el moment de l'accés.

figura 17. Aplicació Android: Llistat de notificacions

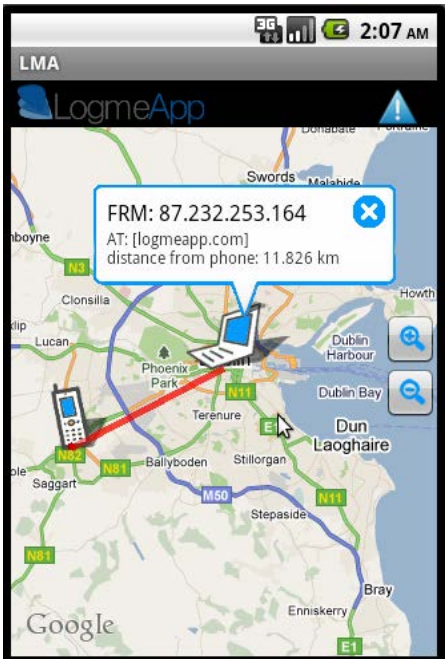

figura 16. Aplicació Android: Notificació plasmada en el mapa

- **Històric d'accessos en espais restringits de l'usuari.** S'ofereix la possibilitat de consultar quins han estat els accessos que s'han realitzat a les zones privades d'un usuari ja siguin sospitosos o no. A part de la informació bàsica que es llista d'aquests accessos es pot consultar informació detallada de cada un d'ells.

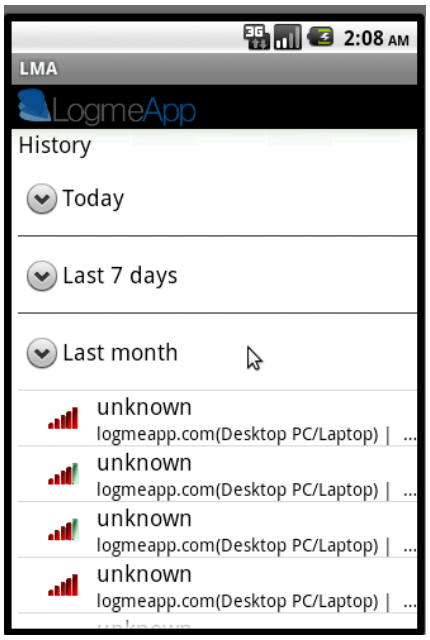

figura 19. Aplicació Android: Històric d'accessos

figura 18. Aplicació Android. Informació detallada sobre un accés

En el cas de la captura de pantalla anterior s'indica que s'ha detectat un accés en algun dels espais restringits de l'usuari, en el que l'origen s'ha registrat a 12 km de la posició de l'usuari. Per altra banda es mostra que el PC des del qual s'ha accedit no disposava del plugin LMA en el navegador (LMA authenticated).

- **Avisos instantanis push d'accessos sospitosos**., Es mostres les notificacions pertinents en el moment que es rep un missatge d'avís per part del servidor LMA. Aquesta notificació redirecciona a l'usuari a l'aplicació LMA on pot consultar informació detallada sobre la incidència

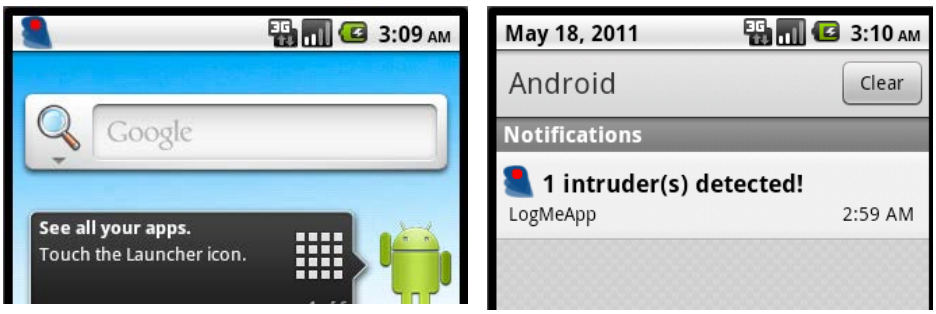

figura 20. Aplicació Android: Avís d'intrusió

- **Gestió de terminals LMA WebNet**. Des de l'aplicació mòbil es permet a l'usuari, tant modificar la posició d'algun dels terminals d'accés a la xarxa coneguts en el sistema LMA, com inserir-ne de nous, els quals es podran seleccionar des del plugin LMA del navegador web, com a origen d'accés.

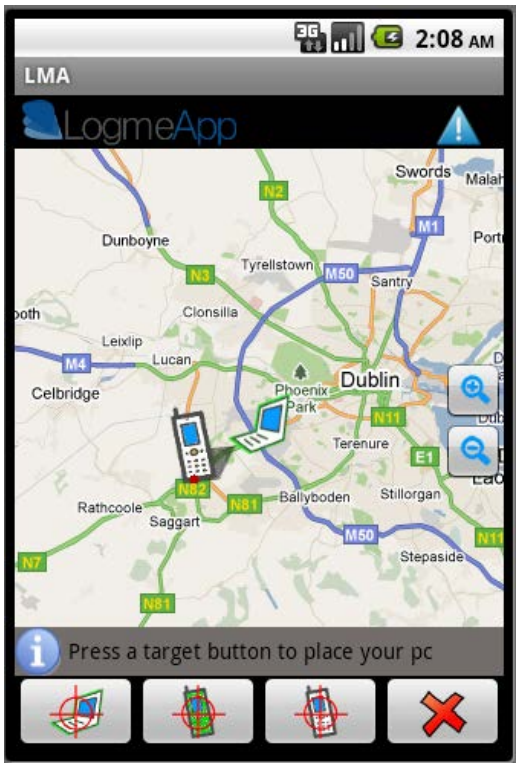

figura 21. Aplicació Android: Posicionament d'un terminal WebNet

6. Línies de futur

Com s'ha anat transmetent al llarg del document, les projeccions i expectatives de LogMeApp són elevades. És un projecte molt ambiciós que vol entrar de forma contundent en el mercat de les tecnologies que vetllen per la seguretat de les validacions per credencials.

Les fites que fins ara s'han aconseguit, és crear un nucli estable per a l'arquitectura, capaç de rebre peticions de validació per part de mòduls controladors d'accés WebNet integrats en diversos websites que disposen de zones privades per a usuaris registrats.

Per altra banda també és disposa de la identificació única per a terminals amb accés a la xarxa, gràcies als plugins per als diferents navegadors web que s'han implementat.

Així doncs, tot i que el producte per ara té carències en aspectes de seguretat i robustesa envers a un gran volum de concurrència i usuaris, es presenta una arquitectura 100% funcional respecte als seus propòsits inicials.

6.1 Supressió de les principals carències del sistema LMA

6.1.1 Seguretat de l'arquitectura envers atacs maliciosos

Durant totes les etapes de creació de LogMeApp s'ha tingut en compte la seguretat del servidor i les interfícies d'usuari, en quant a fer ús de comunicacions segures amb certificats SSL i encriptació de informació sensible a la base de dades.

També s'han programat els scripts del servidor que entreguen informació de la base de dades a peticions AJAX, de tal manera que només acceptin peticions de determinats orígens coneguts.

En definitiva, la seguretat ha estat en el punt de mira durant tot el procés de disseny i implementació de l'arquitectura.

Tot i així, qualsevol persona que hagi dissenyat sistemes accessibles des de la xarxa i amb un alt volum de comunicacions per mitjà d'aquesta, sap perfectament que no existeix el sistema perfecte i requereix d'un anàlisi acurat fet per professionals en el camp, de tots els forats que l'arquitectura pugui tenir per a atacs maliciosos.

Així que, com a primer punt a tractar en quant al futur de LogMeApp, és convertir aquesta arquitectura, funcional ara per ara, en una arquitectura a la vegada 100% segura.

6.1.2 Robustesa envers un gran creixement del volum d'usuaris

Aquest és potser el punt més dèbil que actualment es pot trobar en el producte LogMeApp. Tot i que la intenció d'aquest treball és exposar una idea innovadora i ambiciosa acompanyada d'un prototip funcional que li dona forma, a curt termini aquest ha de ser, junt amb l'aspecte de la seguretat, el punt principal a abordar de tot el sistema.

S'han de realitzar probes d'estres del sistema amb un gran volum d'usuaris i concurrència de peticions de validació en el servidor. Caldrà cert redisseny de la base de dades en quant a fragmentació de taules, sintaxis de crides SQL, i distribució de punts de càrrega de peticions en diversos processadors.

Per sort, existeixen molts patrons de disseny per a tal efecte, i només caldrà aplicar un patró que garanteixi la robustesa que necessita un producte amb les expectatives de LogMeApp.

Un cop més, com en l'apartat anterior: "Zapatero a tus zapatos"; existeixen experts en la matèria de la concurrència i la persistència de dades que poden aportar molt més en aquest àmbit que no pas el dissenyador d'aquesta arquitectura i escriptor d'aquest document.

6.2 Portabilitat de l'aplicació mòbil LMA a les principals plataformes mòbils

Si es vol fer arribar la seguretat LMA a la majoria d'usuaris possibles, el fet que l'aplicació mòbil sigui multi plataforma és un punt crucial per aconseguir el propòsit, ja que aquesta és la credencial de presència dels usuaris de l'arquitectura.

Les principals plataformes mòbils que LMA té en el punt de mira per portar la seva aplicació considerant principalment el volum d'usuaris que les fan servir són:

[Font: Gartner – Maig 2011]

Plataforma	Companya	Cuota de mercat
IOS	Apple	16.8 %
BlackBerry OS	RIM	12.9 %
Windows 7 Phone	Microsoft	3.6 %
Symbian	Nokia	27 %
Android	Google	36 %

Indicar que totes les plataformes llistades a la taula anterior, disposen del seu propi Kit de desenvolupament (SDK) els quals faciliten molt la feina a l'hora d'implementar aplicacions per a les plataformes indicades.

6.3 Portabilitat del identificador de terminals del controlador d'espais LMA WebNet als principals navegadors web

El controlador d'espais WebNet, té com a eix de funcionament la detecció de la posició del terminal des del que s'està accedint a un determinat espai restringit web, identificació que es recorda es emesa per el navegador d'internet utilitzat per accedir a la xarxa.

6.3.1 Navegadors d'escriptori

Però, actualment, la emissió d'aquesta identificació per part del navegador només està disponible per al navegador Chrome de Google, fet que fa impossible determinar la posició dels terminals que accedeixin a la xarxa per mitjà d'un altre navegador.

És per això que existeix la necessitat d'implementar ,en forma de plugin, aquesta funcionalitat per als principals navegadors web que es troben al mercat.

A curt termini, es pretén portar el plugin d'identificació els següents navegadors:

[Font: Net Applications – Gener 2011]

Navegador	Companyia	Cuota de mercat
Firefox 4+	Mozilla	21.74 %
Internet Explorer 9+	Microsoft	56.77 %
Opera	Opera Software	2.15%
Safari	Apple	6.36 %
Chrome	Google	10.93 %

6.3.2 Navegadors per a plataformes mòbils

La idea actual del plugin d'identificació, la qual es basa en que un usuari selecciona d'un llistat de terminals registrats en el sistema, el terminal des del qual està sortint a la xarxa, no és aplicable quan es parla de navegadors mòbils.

Aquest procediment manual de selecció de terminal queda invalidat en aquests casos, doncs l'usuari no enregistrarà una posició diferent per al terminal cada cop que vulgui utilitzar el navegador web del seu dispositiu mòbil des de qualsevol lloc.

Aquest punt s'ha tingut en compte, i la idea per tal d'identificar i localitzar aquests terminals mòbils per part del controlador d'espais WebNet és connectar l'aplicació mòbil LMA amb el propi navegador del dispositiu utilitzant directament l'identificador d'usuari LMA per sortir a la xarxa i les funcions ja implementades per detectar la posició mòbil de l'usuari.

Es contempla aquest punt com a línia de futur prioritària per a guanyar una major integració del mòdul WebNet amb els diferents dispositius mòbils del mercat. .

6.4 Cobertura de l'arquitectura: Controladors d'espais LMA

LMA es presenta com a producte de seguretat multi àmbit en quant al tipus de zones privades en que vol aportar la tecnologia de seguretat per posicionament que ofereix.

És per això que la seva expansió en els diferents àmbits resideix en la implementació de diferents mòduls controladors d'espais, que s'encarreguin de gestionar conjunts de zones privades diverses depenen del tipus d'aquestes en quant a la manera que acrediten a les persones o entitats que hi accedeixen.

A continuació s'exposen els plans de LMA més immediats en quant a la implementació de nous controladors d'espais.

6.4.1 Seguretat en transaccions bancàries

La copia de targetes de crèdit de forma fraudulenta, i la seva posterior utilització en caixers automàtics o diferents punts de pagament, és una pràctica habitual que acostuma a portar molts mals de cap a la víctima del frau, ja que sovint aquesta no percep la utilització fraudulenta de la targeta per part de tercers usuaris fins que no fa un cop d'ull al seu compte corrent.

LMA vol abordar aquest problema. Partint de la base que tant els caixers automàtics, com els punts de pagament amb targeta utilitzats per diverses entitats com comerços, peatges i d'altres institucions són fàcilment localitzables, LMA, de la manera que es presenta pot abordar perfectament la detecció del frau mencionat anteriorment.

Només cal la implementació d'un controlador LMA que s'integri en el software d'aquests punts a on es llegeix la targeta, i informi a la capa de validació del sistema de l'usuari que suposadament està realitzant la transacció, i la posició des d'on aquesta s'està portant a terme.

A més a més, el cost de integració d'aquest controlador en els diversos software dels lectors seria bastant baix, doncs el pes d'informació necessari per a realitzar l'acreditació de presència de l'usuari LMA, com ara la posició dels diversos punts de pagament o la relació entre l'usuari de la targeta i el seu corresponent usuari LMA, residiria en el sistema persistent de dades del mòdul controlador d'espais.

Així doncs, un petit esbós del que podria ser un control de presència en aquest àmbit, representat en forma de diagrama de seqüència podria ser:

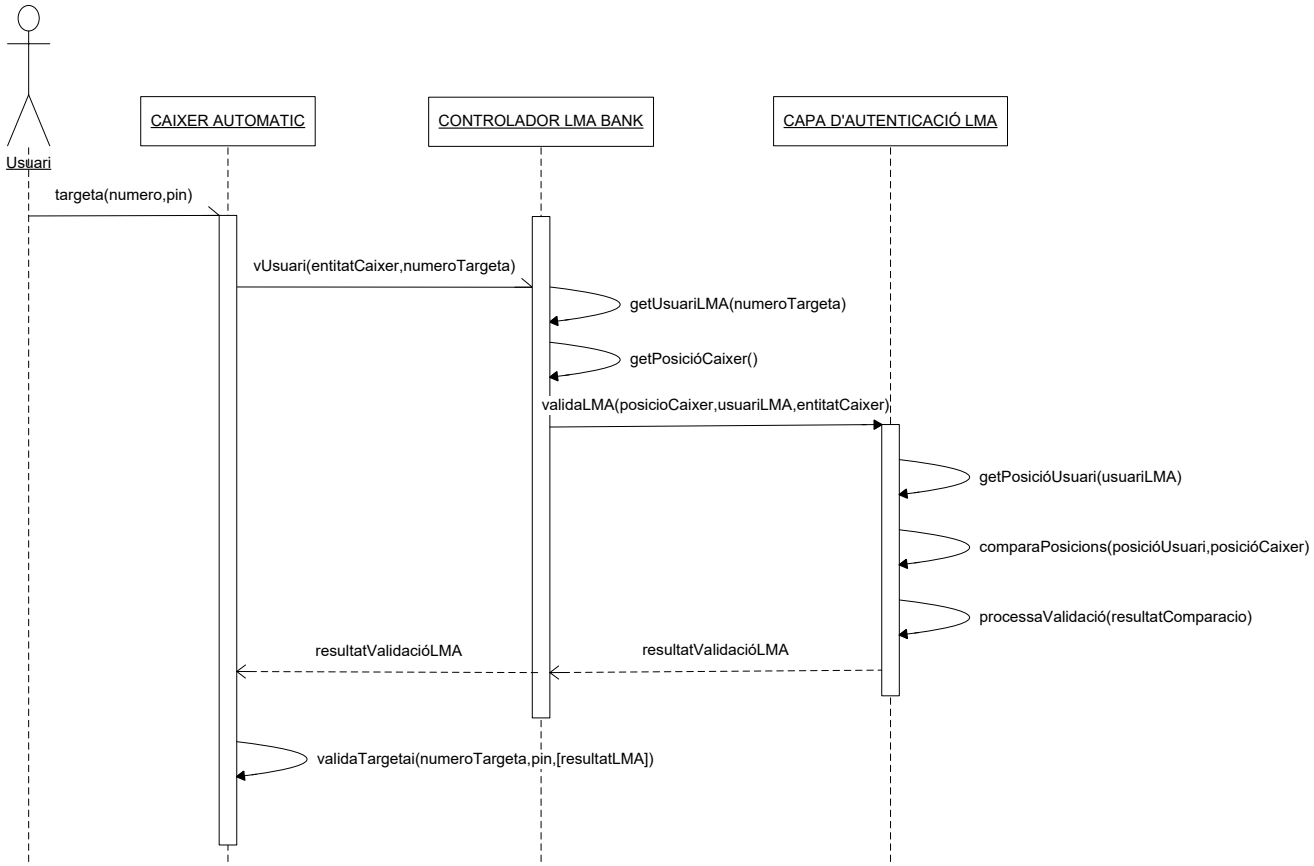

figura 22. Diagrama de seqüència: Validació LMA per a usuaris de caixers automàtics

6.4.2 Acreditació de presència en vehicles equipats amb sistemes 3G

Un fenomen en creixement en la industria de l'automoció, és el d'equipar els vehicles amb sistemes de navegació amb accés a la xarxa gràcies a mòdems 3G per a tal efecte.

Aprofitant que LMA s'alimenta d'aquesta tecnologia 3G per a localitzar al seus usuaris, el que es planteja és utilitzar aquesta tecnologia de localització dels dispositius mòbils també per a les zones accedides, en aquest cas el propi vehicle.

Així doncs, en aquest cas el mòdul controlador d'espais s'incorporaria en el software de navegació de cada un dels vehicles dels usuaris, i actualitzaria la posició d'aquests al servidor LMA, igual que ho fa l'aplicació mòbil LMA per Android en actual funcionament.

D'aquesta manera, en el moment que un subjecte no propietari intentés accedir de forma intrusiva en el nostre vehicle, junt amb l'alarma habitual de la qual ja disposen, es podria activar un avís cap al propietari, en detectar una diferència de posicions amb el vehicle en qüestió.

6.4.3 Integració LMA amb els sistemes d'alarma de recintes

Són molts els recintes privats, ja siguin domicilis, comerços o edificis de diverses entitats o institucions, que disposen d'una alarma de seguretat dotada de sensors per detectar la presència d'intrusos durant l'absència dels propietaris, que aquests activaran i desactivaran introduint un codi concret en aquest mòdul d'alarma.

La finalitat d'aquests tipus d'alarmes, és donar constància al responsable del recinte protegit d'aquestes intrusions comunicant la presència intrusa a la centraleta de la empresa responsable de l'alarma, que posteriorment es posarà en contacte amb la víctima de la intrusió.

Així doncs, LMA pot aportar poc en aquest àmbit en concret de generar avisos cap al responsable del recinte, doncs el sistema d'alarma està implementat precisament per aquest efecte.

Però, es pot garantir d'alguna manera que qui introdueix el codi de desactivació de l'alarma és una persona acreditada per a fer-ho? Precisament aquí és on LMA es vol filtrar, un cop més, en la captura de credencials. Per mitjà de l'arquitectura que es planteja, es viable que, coneixent la posició on s'ubica aquest panell de desactivació de l'alarma, detectar si es un usuari pertanyent al grup d'usuaris acreditats el que està portant a terme la desactivació.

Aquí podria entrar en joc l'eina LMA Groups que s'ha explicat anteriorment, permetent així assignar un grup familiar, o el conjunt dels treballadors d'una empresa com a usuaris autoritzats a realitzar la desactivació de l'alarma en qüestió.

6.5 SDK obert per a la implementació de controladors d'espais

Un dels projectes de futur més ambiciosos i atractius de l'arquitectura LMA, és oferir de forma oberta i gratuïta un SDK per a desenvolupadors, per mitjà del qual puguin implementar un controlador d'espais en l'àmbit que desitgin, oferint de forma segura, el nucli LMA a terceres entitats implementades de forma totalment independent.

La idea de implementar un SDK sorgeix del plantejament que qualsevol punt d'accés que disposi d'una interfície programable amb connexió a la xarxa pot integrar un controlador d'espai LMA.

Així doncs, aquest SDK vol oferir:

- Funcions de comunicació amb el nucli LMA o capa d'autenticació.
- Creació d'aplicacions web JavaScript instal·lables en el site logmeapp.com.
- Generació de bases de dades genèriques en base a les directrius de disseny d'un model relacional de controlador d'espai.
- Llibreries PHP per al control del servidor del controlador d'espais LMA.

7. Conclusions

Les sensacions que s'obtenen del fet de convertir una idea inexistent al terreny de la realitat palpable i funcional, són realment bones.

No és tan sols el fet de descobrir que realment una persona que ha estudiat una enginyeria és vàlida i capaç d'afrontar la creació de qualsevol producte que imagini, sinó que és també el increment d'esperit de superació i les ganes emprenedores que el desenvolupament d'un producte com LogMeApp proporciona.

Intentar conèixer els propis límits d'un mateix, així com els de la tecnologia a l'abast actual, i adonar-se que ni uns ni altres són encara definibles, aporta a nivell personal garanties d'un futur carregat de reptes i fronts obertes on oferir-hi una dedicació agraïda i agradable.

Aquest projecte, ha resultat tot un mèrit tant personal com professional per a l'autor d'aquest document, ja que el seguit de tecnologies i conceptes que s'han afegit dins del seu camp de coneixement durant el procés de creació, li han servit, a part de per a obtenir la titulació d'Enginyer Informàtic, per a fer-lo créixer dins del seu àmbit professional: el disseny, l'anàlisi i el desenvolupament de software.

Quan es comencen a definir els primers fonaments de l'arquitectura que s'ha exposat, l'autor del projecte no té més que un seguit de nocions molt limitades sobre certs àmbits que l'arquitectura ha abordat, finalment, de forma favorable, com ara la implementació d'aplicacions mòbils d'un cert grau de complexitat, o la programació d'aplicacions web utilitzant tecnologies JavaScript com AJAX.

S'ha estudiat, s'han après noves tecnologies, s'han emprat recursos tecnològics que ni tan sols es tenia constància de la seva existència i, el més important, s'han aconseguit els objectius prefixats per al projecte i inclús s'ha fet créixer la idea amb noves metes que han anat apareixent al llarg de la creació del producte.

Situació actual de LMA: un bon punt de partida.

El punt actual on es troba l'arquitectura LogMeApp, no és més que la línia de sortida, del que s'espera que sigui un procediment habitual a l'hora de validar usuaris en espais restringits per credencials. El tret de sortida d'un producte innovador i amb un alt grau d'integració amb tota la resta de tecnologies existents en aquest camp.

Es juga amb l'avantatge que ara mateix, LogMeApp no té competència directa. Encara no s'ha trobat cap producte al mercat que intenti cobrir exactament els mateixos objectius de l'arquitectura que aquí és defineix. Per tant, amb un bon procés de venta que proporcioni l'acceptació necessària per part d'usuaris i empreses, s'espera una entrada favorable i trencadora de l'arquitectura en el mercat de les tecnologies de seguretat.

Per altra banda, es presenta un producte adaptable a infinitat d'àmbits, on de segur a diari es trobaran nous *targets* a on vendre i on afegir-hi les funcionalitats que LMA proporciona, fet que

augmenta les possibilitats d'èxit de la tecnologia. Si no és a un lloc, serà a un altre, però es dipositen un bon grapat d' esperances en que LMA serà un triomf tant de l'autor i creador de la tecnologia, com de l'escola Universitària que l'ha format per tal de tenir la perspectiva d'Enginyeria necessària per a posar-la en marxa.

Inimaginables els plans futurs que aquesta arquitectura por arribar tenir. Els que es llisten a l'apartat de línies futures no són més que les idees més immediates de creixement per a LMA, però qualsevol persona amb una mica d'esperit creador i emprenedor, de segur que a mesura que ha anat llegint aquest document ha anat trobant possibles aplicacions de la tecnologia que ni tan sols l'autor ha contemplat. Estem davant doncs de les arrels d'un fenomen, que si es processa bé en totes les etapes prèvies a la seva posada en marxa, pot donar molt joc en el panorama tecnològic actual.

Objectius assolits

Objectius acomplerts.

L'objectiu d'aquest TFM des del seu origen fins a dia d'avui ha estat la **definició d'una arquitectura que permeti acreditar la presència d'una persona determinada en el moment que aquesta du a terme una validació en un espai personal per mitjà de credencials úniques**.

Per altra banda, també entra dins de la llista d'objectius inicials, el disseny y la implementació d'un prototip de software que plasmi aquesta idea abstracte al mon real, amb tot el que això ha suposat:

- Disseny i implementació del **nucli de validació LMA** i el seu model relacional de base de dades.
    - Classes necessàries per a gestionar tot el procediment d'actualitzacions de posició dels usuaris LMA a la base de dades.
    - Mòdul de comunicació amb la capa superior de controladors d'espais per tal de dur a terme les acreditacions de presència dels usuaris.
    - Mòdul per a la generació d'avisos per mitjà de missatges de tipus PUSH als terminals mòbils dels usuaris utilitzant la tecnologia C2DM de Google.
- Disseny i implementació del **controlador d'espais WebNet** i el seu model relacional de base de dades.
    - Implementació del plugin per al navegador GoogleChrome com a identificador dels terminal amb accés ala xarxa dels usuaris.
    - Implementació de la API LMA WebNet integrable amb els espais webs existents, encarregada de gestionar la captura de la posició dels terminals que accedeixen a un determinat espai web.
    - Generació, a partir de la API LMA WebNet, de mòduls instal·lables en els gestors de continguts web més estesos: Joomla, Blooper i Wordpress.

- Disseny i implementació de **l'aplicació Web logmeapp.com** a l'abast dels usuaris LMA, per tal de controlar els seus comptes d'usuaris i obtenir informació sobre els accessos en les seves zones restringides.
    - Implementació del Frontend HTML i Javascript.
    - Implementació del Backend composat principalment per PHP i AJAX.
        - Mòdul de comunicació amb la BBDD del nucli LMA.
        - Mòdul de control remot per als dispositius mòbils dels usuaris.

- Disseny i implementació de **l'aplicació mòbil LMA per a la plataforma Android**, això com els serveis concurrents que s'executen en segon pla en el terminal.

En conclusió, des de l'humil punt de vista de l'autor: "s'han fet el deures".

8. Bibliografia

Manuals [des de Gener 2010]:

The Busy Coder's Guide to Advanced Android Development
Mark L. Murphy
Copyright © 2009-10 CommonsWare, LLC. All Rights Reserved
Sep 2010:Version 1.9.1 ISBN: 978-0-9816780-1-6

Formació tècnica i recursos a la xarxa [des de Desembre 2010]:

MySQL Connector/C++: how to build a client on Linux using NetBeans 6.5
Internet Super Hero
Disponible a Internet: http://blog.ulf-wendel.de/?p=216#installation

Creating Web Services using Apache Axis-C++
Linux.com
Disponible a Internet: http://www.linux.com/archive/articles/113947

Google Chrome Extensions
Google Code
Disponible a Internet: http://code.google.com/chrome/extensions/index.html

Android Api
Android Developers
Disponible a Internet: http://developer.android.com/reference/packages.html

Manual de jQuery
Desarrollo Web
Disponible a Internet: http://www.desarrolloweb.com/manuales/manual-jquery.html

Google Map Custom Marker Maker
powerhut.co.uk
Disponible a Internet: http://www.powerhut.co.uk/googlemaps/custom_markers.php

Google Maps API Signup
Google Maps API Family
Disponible a Internet: http://code.google.com/intl/es/apis/maps/signup.html

Android C2DM Messaging (Server Push for Android Phones)
AdvanTej
Disponible a Internet: http://techtej.blogspot.com/2010/10/android-c2dm-messaging-server-push-for.html

Push service from Google
My Life with Android
Disponible a Internet: http://techtej.blogspot.com/2010/10/android-c2dm-messaging-server-push-for.html

Zend Framework
Zend, The PHP company
http://www.zend.com/en/resources/zend-documentation/

Android C2DM with PHP and Zend Framework
Mike WillBanks. Getting inside the mind of a php developer.
Disponible a Internet: http://blog.digitalstruct.com/2010/11/21/android-c2dm-with-php-and-zend-framework/

Free IP address geolocation tools
IpInfoDb
Disponible a Internet:
http://www.ipinfodb.com/activate.php?username=jordimassana&code=a18eb83acac890bcf4c375e9fcdee9f1

Papers i articles relacionats amb l'estat de l'art [des de Desembre 2010]:

How Unique Is Your Web Browser?
Peter Eckersley. Electronic Frontier Foundation,
Disponible a Internet: https://panopticlick.eff.org/browser-uniqueness.pdf

The Mobile Phone as a Multi OTP Device Using Trusted Computing
Mohamed Alsomai, Audun Josang
Publicat a: NSS '10 Proceedings of the 2010 Fourth International Conference on Network and System Security
IEEE Computer Society Washington, DC, USA ©2010
ISBN: 978-0-7695-4159-4

Mobile Identity Management Revisited
Emin Islam Tatli, Stefan Lucks
Publicat a: Electronic Notes in Theoretical Computer Science (ENTCS) Volume 244, August, 2009
Elsevier Science Publishers B. V. Amsterdam, The Netherlands, The Netherlands

An agent-oriented mobile payment system secured using a biometrics approach
Huigi Lu, Frederic Claret-Tournir, Chris R. Chatwin, Rupert C.D.Young, Zhongming Liu
Publicat a: International Journal of Agent-Oriented Software Engineering, Volume 3 Issue 2/3, March 2009
Inderscience Publishers, Geneva, SWITZERLAND

A learning-based approach for IP geolocation
Brian Eriksson, Paul Barford, Joel Sommers, Robert Nowak
Publicat a: PAM'10 Proceedings of the 11th international conference on Passive and active measurement
Springer-Verlag Berlin, Heidelberg ©2010
ISBN:3-642-12333-3 978-3-642-12333-7

Geolocation privacy and application platforms
Nick Doty, Erick Wilde
Publicat a: SPRINGL '10: Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS. November 2010
ISBN: 978-1-4503-0435-1

Privacy issues in location-aware browsing
Maria Luisa Damiani, Pierluigi Perri
Publicat a: Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS. November 2010
ISBN: 978-1-4503-0435-1