UBICACIÓN CONSCIENTE DE LA PRIVACIDAD EN APLICACIONES DE E-SALUD

PRIVACY AWARE TRACKING SYSTEMS IN E-HEALTH

María de los Ángeles Cosío León[1] , Juan Iván Nieto Hipólito[1], Jesús Luna García[2]
al323592@uabc.mx / jnieto@uabc.mx / jluna@ac.upc.edu

Recibido: marzo 19, 2009 / Aceptado: mayo 1, 2009 / Publicado: noviembre 20, 2009

RESUMEN. Los sistemas de seguimiento a personas en los centros de trabajo son implantados con distintos objetivos: eficientar los servicios que ofrecen, generar condiciones que propicien la interacción entre los diferentes actores y dispositivos del contexto, así como generar espacios inteligentes para esa interacción. Los datos que proporcionan este tipo de sistemas permiten ubicar a una persona en todo momento, situación que agrede el derecho constitucional de las personas a la privacidad. En este contexto en el presente artículo se propone un mecanismo que permite armonizar estos objetivos que divergen por medio del uso de seudónimos, considerando las condiciones especiales que se dan en los ambientes de e-salud.

PALABRAS CLAVE: seudónimo, privacidad, e-salud.

ABSTRACT. Tracking systems are implemented in working spaces with several objectives: to provid quality services, to create conditions conducive for the interactions between different actors and devices in that context, and to generate smart spaces for interaction. This kinds of systems generate data that allows locate a person at all times, which violates people's privacy constitutional rights. In this context, we propose a mechanism to harmonize this controversy. Our proposal is based on pseudonyms, considering the special conditions that occur in environments of e-health.

KEYWORDS: Pseudonymous, privacy, e-health.

Introducción

Alan Westin define la privacidad como "El derecho de los individuos, grupos o instituciones a determinar por sí mismos, cuándo, cómo y hasta qué punto se pueden comunicar a terceras personas información referida a ellos" [4]. La Costitución en México, en los artículos 16 y 73 [5], legisla en materia de derecho de los individuos a la privacidad y la protección de datos personales en manos de particulares, y la información en manos de las instituciones gubernamentales es coordinada por medio del IFAI (Instituto Federal de Acceso a la Información) [6,7]. Los mecanismos de supervisión en los centros de trabajo deben ser dados a conocer de forma explícita para que no violenten la anterior reglamentación, por lo que la tarea principal es armonizar los derechos del trabajador y los derechos de la empresa a disponer de sus recursos de la manera que le sean más productivos.

El empleo de dispositivos móviles en los centros de trabajo para la ubicación de personas, puede ser considerado como un mecanismo de supervisión que ataca el derecho a la privacidad, aun cuando sus objetivos puedan no ser exclusivamente para ello. Esta interacción requiere ser ordenada para que los actores (empresa-personal) en una y otra posición convivan sin violentar sus derechos.

[1] Universidad Autónoma de Baja California, carretera Tijuana-Ensenada Km. #107, Ensenada, Baja California, México.
[2] Universidad Politécnica de Cataluña, Jordi Girona 1-3, 08034. Barcelona, España.

Las tecnologías, para proveer privacidad [8], se clasifican como sigue: Las que proveen total anonimato y se identifican como Tecnologías que Aumentan la Privacidad (privacy-enhancing Technologies, PETs), en ellas el origen de la comunicación es imposible de ubicar. En las Tecnologías Sensibles a la Privacidad (privacy-sympathetic technology, PSTs), cuyo ejemplo es el Seudónimo [3], una identidad lógica que relaciona a una identidad física por medio del uso de un alias, permitiéndole la interacción con otros servicios o identidades sin la posibilidad de una asociación directa con el dueño del seudónimo a menos que se trate de una persona autorizada. Una tercera clasificación se refiere a aquellas tecnologías sumamente intrusivas al derecho a la privacidad de las personas, referidas como Tecnologías Invasivas a la Privacidad (privacy-invasive technologies PITs), como los sistemas continuos de ubicación, problema para el cual en este articulo se presenta un mecanismo de ubicación conciente de privacidad en ambientes hospitalarios, usando seudónimos y técnicas de encriptamiento, cuya prueba de concepto fue desarrollada en el lenguaje de programación c#.

Antecedentes

La privacidad se puede ofrecer en las diferentes capas del modelo OSI dependiendo del escenario que se requiere proteger, Marco Gruteser y Dirk Grunwald [9] ofrecen privacidad a nivel de capa 2 al anonimizar la dirección del dispositivo (dirección MAC). Los autores aplican su propuesta en la tecnología de WiFi (estándar IEEE802.11), modificando la dirección MAC mediante el uso de la técnica de encriptamiento MD5.

Los sistemas de seguimiento y ubicación del personal se basan mayormente en sistemas inalámbricos (por ejemplo WiFi). Desarrollar aplicaciones para estos ambientes conlleva grandes retos: consideraciones del modelo de movilidad, el modelado del canal de radio y el control de topología para la optimización de recursos [1]. Estos parámetros deben ser analizados con detenimiento, ya que en el contexto de aplicaciones e-salud demanda alta disponibilidad de los enlaces y confiabilidad en los datos que se transportan. Ante esto, es necesario implementar mecanismos de encriptación, que permitan ofrecer un canal seguro de comunicación debido a la particularidad de los datos que se transportan. Para tal efecto, en este artículo se propone la implementación de un esquema de llaves simétricas elegidas sobre el esquema de llaves asimétricas debido a que tienen la ventaja de ser ligeras en su implementación, lo cual facilita su uso en dispositivos móviles con recursos limitados tanto de memoria como de capacidad de procesamiento. Sin embargo, presentan desventajas como la administración de intercambio de llaves y cómo reducir la probabilidad de que lleguen al dispositivo equivocado para evitar que sean utilizadas de forma inadecuada. Para solucionar esto, en este trabajo se consideró intercambiar llaves y seudónimos en un espacio controlado y, por el dinamismo del contexto, realizar la actualización de llaves en intervalos de tiempo prefijados.

El uso de seudónimos y los mecanismos de seguridad propuestos en las diferentes capas del modelo OSI ofrecen una solución a las aplicaciones de e-salud en materia de privacidad. La integración de estas técnicas tiene varios enfoques: para el envío de información de ubicación protegida, para la interacción de los pacientes y los diferentes servicios de salud [10], y orientada al uso de diversos servicios [3]. Existen otras propuestas que incluyen ubicación, pero no consideran privacidad o mecanismos de seguridad, aun cuando transportan datos de pacientes en situaciones críticas.

Escenarios

Para integrar conciencia de privacidad al escenario de nuestro interés, obtuvimos las condiciones iníciales bajo las cuales nuestra propuesta se desarrollaría y cómo sería su comportamiento ante una situación que considerara al mayor número de actores y parámetros en el ambiente analizado [2]. A continuación se describe en detalle.

Consideraciones Iniciales.
El Hospital Carmelitas II instaló un sistema de ubicación de su personal con cobertura al interior de sus instalaciones, cuyo objetivo es contar con información en tiempo real del número de personas por servicio y del personal que lo cubre. Así mismo, pretende propiciar un ambiente de cooperación entre colegas, conociendo la proximidad de ellos, puesto que las pantallas inteligentes son sensibles a la presencia del dispositivo de seguimiento y se usan para desplegar mensajes o documentos que apoyan sus actividades. En lo que respecta a los datos de infraestructura, de personal y de pacientes, éstos se almacenan en una base de datos que contiene tablas con información de: 1) Expedientes de pacientes (se actualiza en visitas al médico y a petición del paciente); 2) Personal (actualizada por el sistema de localización y por el área recursos humanos); 3) Salas de reuniones (su estado de ocupación, ubicación y tipo de reunión); 4) Dispositivos involucrados en el sistema (ubicación y direcciones IP).

Conociendo las consideraciones iníciales, en seguida se describen cóomo éstas afectan al evento de interés, el cual incluye los puntos considerados críticos al implementar la solución propuesta.

Escenario “A” (llamada de emergencia sin el uso de seudónimos).
Se recibe una llamada de la Sra. Juanita en el conmutador de hospital. Su número está registrado en el sistema, por lo que despliega la información a quien le atiende. El despliegue incluye su médico y su ubicación y, en caso necesario, quién está ahora atendiendo el servicio en lugar del titular. La operadora pregunta al paciente su estado y le informa cómo se procederá para su atención. En este punto el sistema infiere la actividad del médico para decidir el flujo de la llamada y se asegura que se le notifique a la persona adecuada, así como queel expediente de Juanita le está siendo enviado a su terminal. Si el médico requerido se encuentra en rondas, le piden aproximarse a una pantalla, la cual al detectar su presencia, desplegará el expediente.

Integrar la conciencia de privacidad a este escenario requirió hacer una serie de reflexiones previas:
• ¿Qué actividades de los empleados son privadas en escenarios normales y en escenarios de emergencia?
• Restringir tiempos de ubicación para colaboración entre colegas, ¿reduce la utilidad del sistema?
• ¿Es significativo que los datos de ubicación de un médico en el hospital puedan estar expuestos a ser capturados mientras son transmitidos por un canal de comunicaciones?
• ¿Es una forma segura de operar para la organización, contar con un sistema de localización de su personal sin consideraciones de privacidad?

Estas reflexiones permiten plantear el escenario B que se describe en la siguiente subsección.

Escenario “B” (llamada de emergencia con el uso de seudónimos).
En el Hospital Carmelitas II se recibe una petición de servicio en el centro de llamadas de la Sra. Juanita, y, por ser ella paciente de este hospital, su número está registrado en el sistema. Una vez que su llamada se clasifica como de emergencia, el sistema advierte que un mensaje de petición de servicio fue enviado. Se

espera una respuesta afirmativa de atención, en tanto que la operadora informa cómo se procederá con la atención al paciente. Esta primera etapa del escenario B se muestra en la figura 1.

El sistema infiere la actividad del médico y toma decisiones sobre el curso del mensaje de petición de servicio. Si no se logra respuesta, se activa el envío de mensajes en el sistema de audio del hospital y mensajes de advertencia son enviados al personal autorizado para verificar la eventualidad. Este personal autorizado decidirá sí se registra como falla del personal o la no respuesta fue normal ante saturación de trabajo del personal. En todas estas transacciones de información se debe considerar la privacidad del personal involucrado y de sus colegas cercanos, en caso de haberlos.

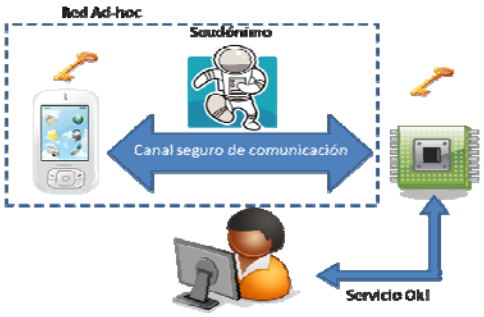

Figura 1. Diagrama global del sistema

Arquitectura implementada

Generación de seudónimos.
En cada dispositivo móvil se integró una rutina para la generación de seudónimos por medio de codificación MD5. Los parámetros para esta rutina son 3: nombre del usuario, tiempo en el que ocurre la transferencia de llaves simétricas y un valor aleatorio. Este valor aleatorio tiene el propósito de romper posibilidades de duplicidad. El sistema entrega la llave simétrica y el dispositivo móvil el seudónimo generado en un canal seguro.

Servidor de atención a pacientes.
Este módulo integra servicios y mecanismos que interactúan con el sistema de seguimiento. Mecanismos ligeros de deducción de actividad basados en agendas y ubicación actual del personal deben ser considerados en este módulo, consciente del uso de seudónimos. Además, este módulo interactúa con los servicios de vídeo conferencia, considerando espacios seguros y políticas de privacidad fijadas por el propietario de la información.

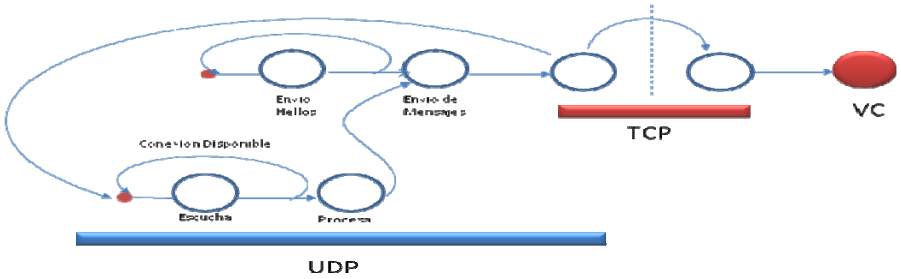

Figura 2. Sistema de sockets del modulo servidor de atención a pacientes

El sistema de sockets TCP, mostrado en la figura 2, habilita la comunicación entre el dispositivo móvil y el servidor de atención a pacientes, e inicia los servicios de vídeo conferencia y envío de imágenes. Además, dos sockets UDP permiten el servicio de Videoconferencia en su modalidad de cliente.

Vídeo Chat (terminales de uso en consultorios y pantallas inteligentes).
Este módulo genera un vídeo chat con la funcionalidad de grabado en modo AVI. Ofrece la posibilidad de ver la reproducción desde otro dispositivo en la red de comunicaciones vía reproductor de Windows Media o enviando fotografías a dispositivos móviles para que un usuario remoto pueda tener acceso al escenario de interés, aun cuando no pueda o no sea necesario tener un servicio de vídeo conferencia.

Nodo Móvil (usuarios móviles, instalado en el dispositivo de ubicación).
En este módulo se desarrolló un "click-chat". Mediante alarmas audibles, se informa de la llegada de mensajes al usuario móvil. Esta notificación se realiza de forma diferenciada, dependiendo si el usuario que recibe el mensaje es el destinatario o si es algún otro nodo móvil del mismo servicio. La respuesta esperada por el sistema es un *click* a alguna de las opciones que ofrece, las cuales se modifican dependiendo de los servicios activos. Si el servicio no es atendido por la persona definida *a priori*, el sistema considera otras alternativas obtenidas de la base de datos y puede aceptar la respuesta de otro actor. La figura 3 muestra el diagrama de flujo que se sigue para dar respuesta a un evento.

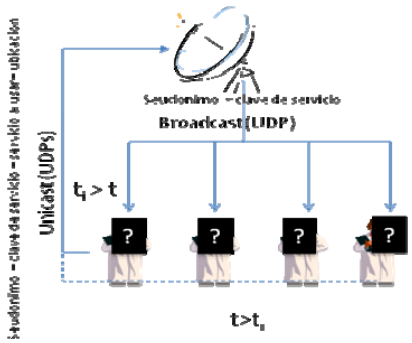

Figura 3. Consideraciones de respuesta a un evento

Las transmisiones de actualización de estado del sistema, el expediente del paciente y los parámetros obtenidos por el personal del hospital se protegen mediante el uso de llaves simétricas.

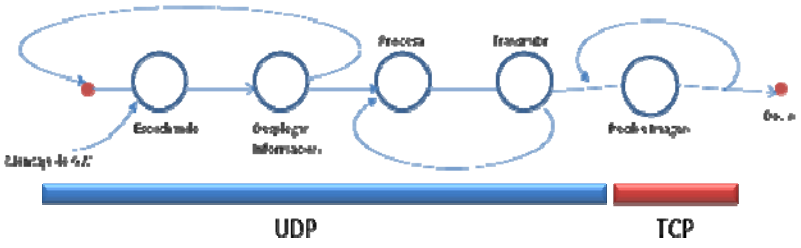

Figura 4. Sistemas de Sockets en el dispositivo móvil

La figura 4 muestra la integración de tres sockets habilitados mediante dos hilos en el dispositivo móvil. Este sistema se activa cuando se solicita la recepción de imágenes y se desactivaban los dos sockets UDP para dar servicio completo al Socket TCP. El sistema inicialmente abre dos socket: uno para el envío de mensajes y un segundo para la recepción de los mismos. No se envían paquetes sí no son motivados por paquetes de petición de servicio que deban ser atendidos por el nodo móvil, por consideraciones de ahorro de energía en el dispositivo. Además, se consideran mecanismos de verificación de recepción de paquetes, para después volver al estado de sólo escucha. Dicho estado de reposo sólo será modificado por un mensaje de emergencia o el vencimiento del temporizador de información ubicación.

Pruebas de concepto

El prototipo se ejecutó en un dispositivo móvil (PDA HP iPAQ hx2400 Pocket PC) y 5 computadoras portátiles HP Pavillion dv-5 1160us. Estos equipos se desplegaron en un área de 15 m^2. De las 5 computadoras portátiles, una realizó las funciones de Gateway y los 4 equipos restantes generaban tráfico con el fin de emular un ambiente de aplicación real. En la primera prueba, debido a la saturación del canal de comunicaciones que provocaban las 4 computadoras portátiles, no fue posible lograr conectividad entre el dispositivo móvil y el Gateway. En una segunda prueba se dejaron 3 equipos portátiles, una de ellos haciendo la función de Gateway, y el dispositivo móvil; en esta topología se logró ejecutar todos los módulos, teniendo un tiempo de respuesta promedio de 9 segundos. Se realizó una tercera prueba con 2 equipos (una haciendo las funciones del Gateway y la otra generando tráfico); con esta topología se ejecutó el prototipo de la aplicación en múltiples ocasiones funcionando sin retardos. El Gateway realizaba las tareas descritas en la sección de *Servidor de atención a pacientes* y el nodo móvil realizo las funciones descritas en la sección *Nodo móvil*. En cuanto a la usabilidad de la aplicación en el dispositivo móvil, el prototipo tuvo una buena aceptación por parte de los usuarios que la utilizaban por primera vez. Esta aceptación se debió a que la aplicación cuenta sólo con 4 botones para todas las funciones que realiza.

Conclusiones y trabajo a futuro

Asegurar la privacidad sólo por medio de seudónimos no es una solución absoluta; es necesario hacer uso de herramientas que los apoyen y actúen en las capas inferiores del modelo OSI. El uso de técnicas de encriptamiento ayuda a tener un canal de comunicación seguro, tal y como se sugiere en esta propuesta. Consideraciones especiales deben ser tomadas en cuenta en los sistemas cuyo propósito sean las áreas de salud. La más importante es que, ante una situación de emergencia, el modelo de privacidad debe ser desactivado y reforzar otras medidas de seguridad físicas, entendiendo como "emergencia" como un caso crítico en el que la integridad del paciente y del personal del hospital esté en riesgo.

Como trabajo a futuro se contempla: 1) Hacer consideraciones de privacidad a la información a la que los médicos acceden con conciencia de contexto, situación que es crítica cuando se usan pantallas inteligentes; ejemplo de esta controversia es la presentación de imágenes de personas atacadas por enfermedades raras o infecto contagiosas. 2) En el sistema no se hace referencia al concepto de reputación que bien podría ser abordado desde las advertencias generadas por las identidades autorizadas.

Referencias

1. Rappaport Theodore S. (1996) *Wireless Communications*. Chapter 4, Mobile Radio Propagation: Small-Scale Fading and Multipath. Prentice Hall, 139-196. New Jersey.
2. Rodríguez M. D., Favela, J., Preciado, A., and Vizcaíno, A. (2005) *Agent-based ambient intelligence for healthcare*. AI Common. 18(3): 201-216.
3. Yuan Yuan-Chu Hwang and Soe-Tsyr, (2007) *A Privacy-Aware Identity Design for Exploring Ubiquitous Collaborative Wisdom*. Computational Science – ICCS 2007. (4490/2007): 433-440.
4. Westin, Alan F. (1967) *Privacy and Freedom*. New York, NY: Atheneum
5. IFAI, Instituto Federal de Acceso a la Información: *Protección a datos personales* [online] <http://www.ifai.org.mx> Consultado: Febrero-2009.
6. IFAI, Instituto Federal de Acceso a la Información, *Recomendaciones sobre las políticas generales para el manejo, mantenimiento, seguridad y protección de datos personales*, [online] <http://www.ifai.org.mx> Consultado: Febrero -2009.
7. IFAI, Instituto Federal de Acceso a la Información: *Lineamientos de protección a datos personales* [online] <http://www.ifai.org.mx> Consultado: Febrero -2009.
8. Clarke Roger. (12 Abril 1999) *The Legal Context of Privacy-Enhancing and Privacy-Sympathetic Technologies* [online] <http://www.rogerclarke.com>, ACN: 002360456. Consultado: 15 de enero de 2009.
9. Gruteser Marco, Grunwald Dirk. (2005), *Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis, Mobile Networks and Applications* (10): 315–325, 2005 Springer Science + Business Media, Inc. Manufactured in The Netherlands.
10. Au Richard, Peter Croll. (2008) *Consumer-Centric and Privacy Identity Management for Distributed e-Health Systems*, Proceedings of the 41st Annual: 234 – 234, IEEE.