FastTriaje: un asistente para la clasificación de víctimas en situaciones de emergencia con autenticación robusta

Candelaria Hernández Goya
Departamento de
Ingeniería Informática
Universidad de La Laguna
Email: mchgoya@ull.edu.es

Alexandra Rivero García
Departamento de
Ingeniería Informática
Universidad de La Laguna
Email: alexandra.rivero.00@ull.edu.es

Pino Caballero Gil
Departamento de
Ingeniería Informática
Universidad de La Laguna
Email: pcaballe@ull.edu.es

***Resumen*—Este trabajo describe el desarrollo de un sistema de clasificación de víctimas en situaciones de emergencia que consta de una plataforma web y una aplicación móvil. La sinergia entre estos elementos y la integración de diferentes tecnologías de comunicación (NFC y Wi-Fi) permite clasificar a las posibles víctimas de una forma rápida y confiable.**

La clasificación realizada para una víctima es guiada por el dispositivo móvil (la implementación se ha hecho para teléfonos inteligentes basados en Android) y una vez finalizada, el sistema ofrece la posibilidad de almacenarla en una tarjeta NFC que se asigna a la víctima. Además, el diagnóstico realizado se almacena en el dispositivo móvil, pudiéndose posteriormente remitir a un servidor central en caso de que las infraestructuras de comunicaciones estén disponibles.

Se han implementado métodos criptográficos robustos, concretamente se utilizan Demostraciones de Conocimiento Nulo para identificar a los usuarios que desarrollan los triajes, de manera que sean sólo los usuarios autorizados previamente por el servicio los que puedan hacer uso del sistema.

***Palabras clave*—Triaje, NFC, Android, Criptografía Ligera, Demostración de Conocimiento Nulo (Zero Knowledge Proof)**

I. Introducción

El sistema presentado en este trabajo se denomina FastTriaje y se basa en el método START (Simple Triage and Rapid Treatment) [1]. Este método persigue dos metas esenciales en situaciones de emergencia y/o desastres naturales: salvar el mayor número de vidas posible y, simultáneamente, optimizar el uso de los recursos materiales y humanos disponibles.

Un sistema tradicional de triaje facilita la toma de decisiones sobre la prioridad requerida para la atención de una víctima por medio de tres acciones principales: observación, evaluación y decisión. Con FastTriaje el proceso completo de diagnóstico de la gravedad del paciente es guiado por la aplicación. El sistema indicará al diagnosticador el resultado final de la evaluación, así como la decisión que debe tomarse.

Uno de los elementos del sistema es una aplicación móvil desarrollada para dispositivos Android. Dicha aplicación será la herramienta principal del personal a cargo de la evaluación del paciente, tanto a la hora de realizar su clasificación, como también para gestionar la información generada en cada triaje. Una de las posibilidades incluida en la aplicación es almacenar la información asociada al triaje en una etiqueta NFC que se asociará al paciente. Dicha información puede ser consultada posteriormente en cualquier momento a través de la misma aplicación.

El segundo pilar del sistema desarrollado es una plataforma web cuya función principal es centralizar la recogida de información generada por el uso de la aplicación móvil y facilitar la gestión de la misma, incluyendo la gestión de usuarios y sus privilegios

La aplicación móvil y la plataforma web interactúan a través de un servicio web REST, siendo el formato seleccionado para la comunicación mensajes JSON.

Se han incluido métodos de autenticación robusta basados en criptografía ligera para la comunicación de la aplicación con la etiqueta NFC y también con la plataforma web.

II. Descripción de los sistemas de triaje

El termino triaje es de origen francés y su raíz (trier) significa clasificar. Es en el entorno militar donde se comienza a utilizar en el ámbito de la clasificación de víctimas en función de la urgencia requerida para su atención.

Una definición ampliamente aceptada es la siguiente: proceso simple, completo, objetivo y rápido de obtener una evaluación clínica inicial de víctimas con el objetivo de evaluar sus capacidades inmediatas de supervivencia y priorizarlas según su gravedad.

En situaciones críticas, el disponer de un método fiable y eficiente para la clasificación de víctimas es crucial. Generalmente los sistemas de triaje distinguen dos etapas:

- Primer triaje. Se lleva a cabo en la misma zona hostil. El personal a cargo del diagnóstico no debe pasar más de un minuto evaluando las capacidades de supervivencia de la víctima, ordenándolas finalmente de acuerdo a su gravedad. Algunos métodos en esta categoría son SHORT, START o MRCC.
- Segundo triaje. Esta etapa se desarrolla en una instalación sanitaria o un hospital. Aquí es el personal médico el que analizará el estado de la víctima: contusiones, heridas y lesiones. Algunos de los métodos aplicados en esta

ISBN: 978-84-9717-323-0

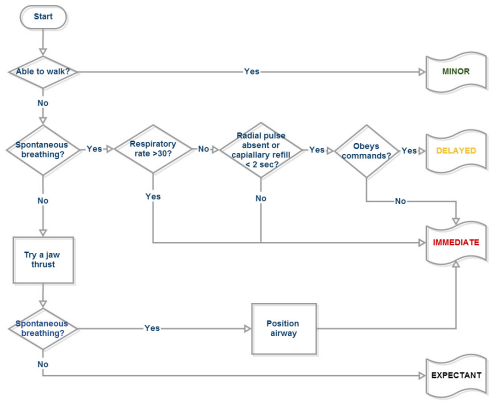

Figura 1. Algoritmo START

etapa son el Modelo Andorrano de Triaje (MAT), Spanish Triage System (SET) y Manchester Emergency Triage System (METS).

A pesar de realizar la distinción previa, estos métodos no son excluyentes sino complementarios. Los triajes correspondientes a la primera etapa proporcionan información indispensable para realizar la evacuación a las instalaciones sanitarias donde personal médico realizará la segunda etapa.

Se incluye en la figura 1 una descripción gráfica del método START. Éste es el método que se ha implementado en el sistema FastTriaje.

START utiliza etiquetas con cierto color para indicar el resultado de la clasificación, cada color representa un estado de gravedad diferente:

- negro: víctima mortal o irrecuperable.
- rojo: víctimas que requieren atención médica inmediata.
- amarillo: víctimas que requieren cuidados urgentes, pero su estado permite un retraso en la atención de entre media a una hora.
- verde: víctimas que no están seriamente heridas. Su tratamiento puede retrasarse más de una hora.

En el sistema propuesto en este trabajo las etiquetas tradicionales se sustituyen por etiquetas NFC ya que facilitan el tratamiento automático de la información generada en las valoraciones, permitiendo además que dicha información sea procesada fuera del lugar del suceso. En la sección siguiente se especifican algunas de las características que posee esta tecnología y que la hacen especialmente interesante para el sistema desarrollado.

III. Tecnología NFC

Near Field Communications (NFC) es es una tecnología de comunicación inalámbrica de alta frecuencia de corto alcance. En cierto modo se puede entender como una extensión de la tecnología RFID puesto que posibilita la coexistencia de los papeles de lector y tarjeta en un mismo dispositivo. Su principal funcionalidad es la de permitir la transferencia de contenido entre dispositivos móviles en modo punto a punto.

Una caraterística diferenciadora de esta tecnología frente a otras tales como RFID, Bluetooth, ZigBee o Wi-Fi, es que la transmisión de información en NFC no es continua, se requiere el contacto entre los dispositivos para el intercambio de información. Sin embargo dicha transferencia se realiza de manera rápida y oportuna.

Una de las principales ventajas de NFC cuando se compara con otras tecnologías es su seguridad inherente. Debido a su corto rango de comunicación y la necesidad de participación de los usuarios cuando se realiza una acción, NFC ofrece un nivel de seguridad más alto.

La tabla I recoge una comparación entre NFC y algunas tecnologías inalámbricas de comunicación.

Tabla II
Parámetros del campo de curvas elípticas en las ZKPs.

Parámetro	Descripción
p	número primo que define el campo F_p
a, b	coeficientes de la ecuación de la curva elíptica E
P	un punto base (un generador de un subgrupo cíclico de $E(F_p)$)
m	orden de P en $E(F_p)$

IV. Criptografía ligera y demostraciones de conocimiento nulo

Actualmente se diseñan aplicaciones móviles para casi cualquier ámbito de aplicación: negocios, gestión de transporte, redes sociales y muchos otros. En todos ellos el garantizar la seguridad de la información es una obligación. Las soluciones tradicionales generalmente requieren infraestructura específica, por lo que transferir estas soluciones al entorno aquí analizado no es viable [2].

En el sistema desarrollado se ha hecho uso de la criptografía ligera para garantizar el acceso legítimo a la información asociada a los triajes. Esta elección queda justificada por las restricciones sobre las capacidades computacionales y de comunicación definidas sobre los dispositivos que participan, generalmente teléfonos inteligentes. Concretamente, se usa criptografía de curvas elípticas (Elliptic Curve Cryptography, ECC) [3] debido a que:

- proporciona problemas con una complejidad computacional superior, y
- la longitud de clave que se necesita para alcanzar un nivel de seguridad concreto es más corta.

La tabla II describe la notación relacionada con las curvas necesaria para describir los protocolos implementados.

Las ZKPs permiten a un participante (el probador, A) convencer a otro (el verificador, B), sobre la veracidad de un hecho sin proporcionar más información que la validez de dicha demostración. Estas demostraciones se pueden extender para resolver el problema de autenticación tal y como se describe en el estándar ISO 9798-5 dedicado a autenticación de entidades.

Los elementos principales de las ZKPs son los siguientes tres:

Tabla I
COMPARACIÓN DE TECNOLOGÍAS INALÁMBRICAS DE CORTO ALCANCE.

	Tecnología			
Característica	NFC	Bluetooth	RFID	ZigBee
Establecimiento de conexión	0.1s o menos	6s	0.1s o menos	30ms
Velocidad	424-848kbps	24Mbps (versión 3.0)	424kbps	250kbps
Rango	10cm	10m	3m	70m
Consumo de batería	Bajo	Alto	Bajo	Bajo
Seguridad	Alta	Alta	Vulnerable	Vulnerable
Intervención de usuario	Tocar	Requiere configuración	Sin configuración	Sin configuración

Figura 2. Módulos de FastTriaje

- Testigo (w): el probador selecciona aleatoriamente un elemento de un conjunto predefinido manteniendo dicha elección en secreto. Este valor se denomina compromiso (x). A partir del mismo, se genera otro valor denominado testigo (w), siendo dicho valor remitido al verificador.
- Reto (e): En el segundo paso, el verificador selecciona aleatoriamente una pregunta que el probador debe responder correctamente, siempre y cuando realmente conozca la información secreta asociada al proceso de autenticación. Esta pregunta está relacionada con x y con las credenciales que deben ser verificadas.
- Respuesta (y): Finalmente el probador envía la respuesta al reto que será comprobada por el verificador. En caso de que la verificación sea correcta la autenticación se acepta.

V. EL SISTEMA DESARROLLADO: FASTTRIAJE

El principal escenario para el despliege de FastTriaje es una situación de emergencia o desastre natural. Su objetivo es agilizar la clasificación de víctimas y la gestión de la información generada durante ese proceso. La figura 2 ilustra los módulos que componen el sistema: la aplicación móvil y la plataforma web.

El objetivo principal de la aplicación Android es implementar el método de triaje START en dispositivos móviles como una herramienta simple, usable e intuitiva que facilita el proceso de triaje tradicional. Con dicha aplicación es posible enviar a una plataforma web los triajes realizados cuando el estado de las comunicaciones lo permitan. Actualmente la implementación desarrollada transfiere los triajes realizados haciendo uso de infraestructura Wi-Fi, pero es posible adaptarla para que use comunicaciones Wi-Fi Direct [4]. De esta manera, la transferencia de información se puede realizar directamente entre los dispositivos que forman parte de una red desplegada en la zona del desastre. Los usuarios registrados en el sistema podrán consultar posteriormente los triajes realizados. Además, cada triaje se puede almacenar en una etiqueta NFC que se anexa a la víctima para su clasificación "in situ". En cualquier caso la información asociada a cada triaje queda también registrada en el dispositivo móvil utilizado.

Sólo los dispositivos autorizados pueden intercambiar información con la plataforma web. Para garantizarlo se ha implementado una demostración de conocimiento nulo (Zero Knowledge Proof, ZKP) como protocolo de autenticación (ver ZKP1 en la siguiente sección). Aquellos usuarios que utilicen la aplicación deben estar registrados previamente en la plataforma web. Los privilegios de los usuarios, los establece el administrador de dicha plataforma. De este modo, se distinguirá entre usuarios con permiso sólo para consultar las etiquetas, de aquellos que pueden realizar los triajes y almacenarlos en las etiquetas NFC.

La plataforma web se comunica con la aplicación móvil a través de un servicio web. Antes de almacenar el triaje en la etiqueta NFC, el usuario autorizado ejecuta otra demostración de conocimiento nulo (ZKP2) que asocia el triaje con sus credenciales.

VI. MÉTODOS DE AUTENTICACIÓN EN FASTTRIAJE

Esta sección describe los protocolos de autenticación implementados en FastTriaje para garantizar el acceso sólo a los usuarios legítimos. Los dos protocolos comparten algunas características, principalmente en la etapa de inicialización. En ambos casos dicha etapa consiste en fijar una curva elíptica (E) y un punto base de la misma (P). Además las credenciales asociadas a A se definen de la misma manera: la identificación secreta es un entero seleccionado aleatoriamente del conjunto $\mathbb{Z}_p$, mientras que la pública es un punto de la curva E generado al multiplicar el entero asociado a la información secreta por el punto base.

VI-A. ZKP1: Autenticación del dispositivo móvil frente a la plataforma web

Este protocolo se utiliza para la autenticación del dispositivo móvil (A) frente a la plataforma web (B). Se incluye una descripción detallada del mismo en la tabla III. El reto definido en cada ejecución se genera a través de la aplicación de una función hash. Esta manera de proceder no se corresponde con la definición tradicional de las demostraciones de conocimiento nulo pero permite reducir el número de iteraciones del protocolo a sólo una.

Tabla III
ZKP1: AUTENTICACIÓN EL DISPOSITIVO MÓVIL FRENTE A LA PLATAFORMA WEB

Etapas	Accciones
Inicialización	número primo p E curva elíptica $\mathbb{Z}_p$ $P \in E$
Identificación secreta de A	$a \in \mathbb{Z}_p$
Identificación pública de A: $Puid_A$	$a * P \in E$
Compromiso:	$x \in_r \mathbb{Z}_p$
Testigo: $A \rightarrow B$	$w = x * P \in E$
Reto: $A \leftarrow B$	$e = hash(P, a * P, x * P)$
Respuesta: $A \rightarrow B$	$y = x + a * e \in \mathbb{Z}_p$
Verificación: B comprueba	$y * P - e * Puid_A = w$

Tabla IV
ZKP2: AUTENTICACIÓN DEL DISPOSITIVO MÓVIL FRENTE A LA ETIQUETA NFC.

Etapas	Acciones
Inicialización	p número primo E curva elíptica en $\mathbb{Z}_p$ $P \in E$
Identificación secreta de A	$a \in \mathbb{Z}_p$
Identificación pública de A: $Puid_A$	$a * P \in E$
Compromiso:	$\{x_1 * P, x_2 * P, \cdots, x_n * P\}$ $\in E$, con $x_i \in_r \mathbb{Z}_p$
Testigo: $A \rightarrow B$	$w = hash(x_j * P + x_k * P)$, con $j, k \in_r \{1, 2, \cdots, n\}$
Reto: $A \leftarrow B$	$e \in_r \mathbb{Z}_p$
Respuesta: $A \rightarrow B$	$y = x_j + x_k - a * e \in \mathbb{Z}_p$
Verificación: B comprueba	$hash(y * P - e * Puid_A)$ $= w$

VI-B. ZKP2: Autenticación del dispositivo móvil frente a la etiqueta NFC

El protocolo se destina a la autenticación del dispositivo móvil (A) frente a la etiqueta NFC antes de almacenar el triaje en ella.

Sin embargo, este protocolo no puede utilizarse directamente con las etiquetas NFC puesto que las etiquetas utilizadas en la implementación son totalmente pasivas. Esta elección se debe a intentar reducir costos de implementación lo que imposibilitaba la generación de retos por parte de la etiqueta. Por este motivo se optó por utilizar el paradigma de Fiat-Shamir [5] para transformar el protocolo propuesto generando una versión no interactiva.

De acuerdo con este paradigma se usa una función hash para la generación de los retos. En la implementación realizada se ha usado el nuevo estándar de función hash, SHA3 [6].

VII. CONCLUSIONES Y CUESTIONES FUTURAS

Este trabajo presenta un sistema que mejora la logística, clasificación y atención de víctimas en situaciones hostiles como pueden ser desastres naturales o accidentes. La herramienta está compuesta por una aplicación móvil y una plataforma web. La aplicación móvil sirve como asistente durante el desarrollo de los triajes y permite almacenar los resultados en etiquetas NFC que se asocian a las víctimas. Además es posible transferir el resultado de los triajes, a través de un servicio web, a una plataforma web donde la información generada puede procesarse de acuerdo con los perfiles de usuarios definidos.

Debido a que los servicios proporcionados se entienden como críticos, en la implementación realizada se ha tenido en cuenta la robustez del proceso de autenticación de entidades, así como la eficiencia del sistema.

Puesto que este trabajo está en desarrollo quedan algunas cuestiones importantes por solventar. Quizás una de las más significativas es dotar al sistema del servicio de confidencialidad. También caben mejoras a la hora de facilitar la coordinación e integración de los diferentes cuerpos de emergencia que pueden participar en la resolución de la misma. En este sentido, con la versión actual del sistema en el caso de que intervinieran diferentes cuerpos sanitarios habría que realizar la etapa de registro "in situ".

Otras cuestiones que se esperan incluir son las siguientes:

- Añadir funcionalidades estadísticas a la plataforma web.
- Integrar el sistema con las historias clínicas de los pacientes.
- Extender la aplicación para que posibilite la realización del segundo tipo de triajes.
- Se espera además ampliar la aplicación desarrollada completando el sistema de clasificación con extensiones específicas para grupos concretos de víctimas, tales como pacientes pediátricos y también con la implementación de sistemas de triajes pertenecientes a la categoría de segundo triaje.

AGRADECIMIENTOS

Este trabajo ha sido financiado parcialmente por el Ministerio de Economía y Competitividad y el Ministerio de Ciencia e Innovación bajo los proyectos IPT-2012-0585-370000: DEPHISIT y TIN2011-25452: TUERI.

REFERENCIAS

[1] K. V. Iserson and J. C. Moskop, "Triage in medicine, part i: Concept, history, and types," *Annals of Emergency Medicine*, vol. 49, no. 3, pp. 275 – 281, 2007.

[2] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (IoT)," in *Recent Trends in Network Security and Applications*, ser. Communications in Computer and Information Science. Springer Berlin Heidelberg, 2010, vol. 89, pp. 420–429.

[3] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

[4] J. I. S. González, "Implementación de algoritmos seguros en dispositivos wi-fi direct," 2013.

[5] A. Fiat and A. Shamir, “How to prove yourself: Practical solutions to identification and signature problems,” in *Advances in Cryptology - CRYPTO 86*. Springer-Verlag, 1987, pp. 186–194.
[6] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, “ The Keccak sponge function family ,” Sooft.es, http://keccak.noekeon.org/papers.html.