FastTriaje: A Mobile System for Victim Classification in Emergency Situations

Alexandra Rivero-García, Candelaria Hernández-Goya, Iván Santos-González and Pino Caballero-Gil
Department of Computer Engineering, Universidad de La Laguna, Tenerife, Spain

Keywords: Triaje, FastTriaje, NFC, Android, Elliptic Curves, Lightweight Cryptography, Internet of Things, Zero Knowledge Proofs.

Abstract: The high penetration of communication technologies and smartphones may help in many complex scenarios. This work presents a system to perform victim diagnosis in emergency situation and/or natural disasters. The implementation include a web platform, a web service and a mobile application. The synergy among these three elements and different communication technologies such as NFC and Wi-Fi allows to classify potential casualties in a fast, useful and reliable way. Robust cryptographic methods are used to ensure the access only to legitimate users.

1 INTRODUCTION

The system proposed in this paper is called FastTriaje and it is based on the method START (Simple Triage and Rapid Treatment) (Iserson and Moskop, 2007). This method allows to obtain two essential aims in an emergency situation and/or a natural disaster: saving as many lives as possible and optimizing the available resources, both material and human ones (Raúl Sánchez Bermejo, 2011), (no,).

A traditional triage helps to decide on patient's attention priority by means of three actions: Inspection, Evaluation and Decision. With FastTriaje the disgnosis process is completely guided by the application. The system itself will indicate to the diagnostician the result of the evaluation and the decision to be carried out.

One of the system elements is a mobile application for Android devices. The application will be the diagnosticians tool to classify the victims and storing the information of each triage in an NFC tag that will be attached to the victim. The tag generated may be accessed at any time afterwards through the same application.

The second pillar in the system is a web platform whose main objectives are centralizing the triage information and easing user management.

The mobile application and the web platform interacts by means of a REST web service, through the transmission of different messages in JSON format.

Important security measures, based on lightweight cryptography and zero knowledge proofs have also been included improving reliability.

2 VICTIM CLASSIFICATION: TRIAJE SYSTEMS

The word TRIAGE is a term recently coined by the scientific community referring to patient classification. A commonly accepted definition follows: a simple, completed, objective and fast process to obtain an initial clinical assessment of people with the objective of evaluate their immediate survival capacities and prioritizing them according their severity.

An efficient method for casualty classification in a hostile situation is crucial. In order to achieve the classification, all triage systems distinguish two steps:

- First triage or simple triage. It is carried out in the hostile zone with fast methods like SHORT, START (Simple Triage and Rapid Treatment) or MRCC (Método Rápido de Clasificación en Catástrofes). Here, the diagnostician will not spend more than a minute, evaluating the survival capabilities of victims and sorting them depending on their seriousness.
- Second triage. It is made in a medical station or in a hospital. At this point, medical staff analyze each patient state: bruises, wounds and injuries. The Andorran Triage Model (MAT), Spanish Triage System (SET) and Manchester Emer-

Rivero-García A., Hernández-Goya C., Santos-González I. and Caballero-Gil P..
FastTriaje: A Mobile System for Victim Classification in Emergency Situations.
DOI: 10.5220/0004981502380242
In *Proceedings of the 10th International Conference on Web Information Systems and Technologies* (WEBIST-2014), pages 238-242
ISBN: 978-989-758-023-9

gency Triage System (METS) are methods widely used during this stage.

Note that two types of triages are defined but they are not mutually exclusive, both should be carried out. The first triage gives important information about priorities for evacuation to hospitals where medical staff will do the second triage.

A more detailed description of the START method (Simple Triage and Rapid Treatment) has been included bellow because is the one used by FastTriaje, (see figure 1).

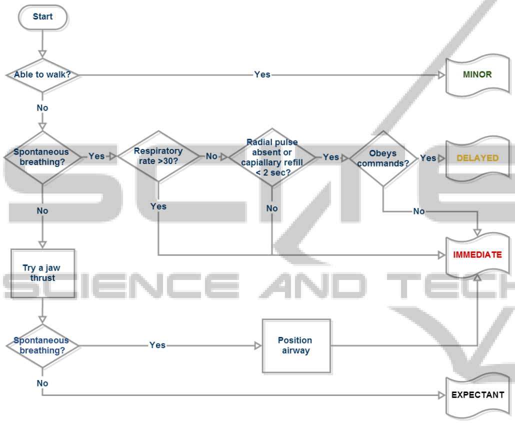

Figure 1: Simple Triage and Rapid Treatment Algorithm.

START method consists of answering a few simple questions to evaluate possible casualties. The answers are just “Yes” or “No” and depending on the answer given, the method will make another question or establish a classification. The questions are related to:

- mobility,
- breathing,
- perfusion, and
- state of mind.

START uses colored tags in the classification, each color stands for a different seriousness level:

- Black: dead or irrecoverable victims.
- Red: victims requiring immediate care.
- Yellow: victims requiring urgent care, but can wait for treatment from half an hour to one hour.
- Green: victims who are not seriously injured. They can wait for treatment more than an hour.

The traditional colored tags, are substituted by NFC tags. Next this technology and its security countermeasures are introduced.

3 NEAR FIELD COMMUNICATION TECHNOLOGY

Near Field Communications or NFC (nfc, b) is a short-range high frequency wireless communication technology. It may be defined as an extension of Radio Frequency Identification (RFID) since it combines the interface between tags and reader into a single device. It allows users to share content between digital devices in a peer to peer mode what makes it a promising paradigm in mobile technology.

In 2003 NFC was approved as ISO standard and nowadays is a technology used in many applications like car keys, ID cards, tickets, smartphones and so on. Contrary to other technologies as RFID, Bluetooth, ZigBee or Wi-Fi, NFC is not designed to send information continuously. Communication between devices requires that devices touch each other to exchange the information quickly and timely.

Some key features of NFC are:

- Its frequency range is 16.56MHz, this is a free frequency.
- Different communication rates are allowed: 106kb/s, 212kb/s or 424kb/s.
- High proximity between devices is needed: 10cm or less.
- It is an open technology based on standards.
- It may be considered a simple and reliable technology.
- Two communication modes are supported: active and passive mode. The first one allows communication between devices that can generate their own magnetic camp. The second is devoted to the interaction with NFC tags.

One of the main advantages of NFC when comparing it with other technologies is its inherent security. Due to its short communication range and the need of user involvement when an action is performed, NFC provides a higher security level.

A comparison among different technologies has ben included in Table I ((nfc, a)).

4 FastTriaje SYSTEM

FastTriaje main scenario is an emergency situation or natural disaster. Its goal is to speed up the classifications of victims. The modules that compose the whole system may be appreciated in figure 2: a mobile application and a web platform.

Table 1: Comparison of some short range technologies.

	Technology			
Feature	NFC	Bluetooth	RFID	ZigBee
Connection set	0.1s or less	6s	0.1s or less	30ms
Speed	424-848kbps	24Mbps (version 3.0)	424kbps	250kbps
Range	10cm	10m	3m	70m
Battery consumption	Low	High	Low	Low
Security	High	High	Vulnerable	Vulnerable
User experience	Touch	Need configuration	No configuration	No configuration

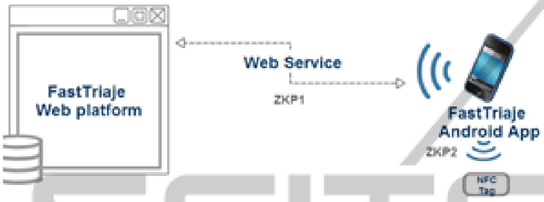

Figure 2: FastTriaje modules.

A mobile application is included. The main goal of this Android application is implementing the START triage method in mobile devices as a simple, usable and intuitive tool that facilitate the traditional triage process. All the triages generated are sent to a web platform, where every user has access to the information associated to the triages made by him/her. Additionally, the application allows to store each triage on an NFC tag to label victims.

Only legitimate users can exchange information with the web platform since a robust authentication protocol (see ZKP1 in next section) is used before transferring triages. All users who want to use the mobile application must be registered in advance on the web platform. User's privileges are set by the system administrator on this platform. Thus, it makes possible to distinguish between users with permissions to only read tags from those who may write on it, as well.

The web platform communicates with the mobile application by means of a web services. Before writing information on a NFC tag, the authorized user executes another authentication protocol (ZKP2) that associates the triage to be stored there with his/her credentials.

5 LIGHT WEIGHT CRYPTOGRAPHY AND ZERO KNOWLEDGE PROOFS

Nowadays mobile applications are designed for almost any field: business activities, transport management, social sharing and so on. In all of them guarantying information security is a must. Traditional solutions generally need specific infrastructure, transferring these solutions to the environment under study here is non-viable (Babar et al., 2010).

We have used lightweight cryptography in order to guarantee legitimate access to the information associated to the triage system. Concretely, we use Elliptic Curve Cryptography (ECC) (Hankerson et al., 2003) since:

- it provides with problems with higher computational complexity, and
- key length to achieve certain security level is shorter.

When using ECC there is certain notation related to the curves used that should be defined. This notation is included in table II.

$$E(F_p) = \{(x,y) \in F_p x F_p : y^2 = x^3 + ax + b\} \cup \{O\} \quad (1)$$

where

$$a, b \in F_p, 4a^3 + 27b^2 \neq 0$$

Table 2: Elliptic curve domain parameters in ZKPs.

Parameter	Description
p	prime number defining the field F_p
a, b	coefficients in the equation of elliptic curve E
P	a base point (a generator of a cyclic subgroup of $E(F_p)$)
m	order of P in $E(F_p)$

This election is justified by the restrictions on the computational and communication capabilities defined on the devices involved, smartphones mainly. The solutions developed are based on Zero Knowledge Proofs (ZKP) which stand out as a promising solution to the authentication problem in the Internet of Things (Martínez et al., 2009), (Ramzy and Arora, 2011), (Alpár et al., 2012).

These protocols allow a party A to convince another party B, about the knowledge of certain secret information without sending anything related to it. These demonstrations may be extended to solve the authentication problem as it isincluded in the ISO standard 9798-5 dedicated to entity authentication.

ZKPs use three main elements:

- Witness (w): the prover selects a random item from a predefined set, keeping it secret. This value is called compromise (x). From it, the prover generates a value called witness, and then, sends it to the verifier.
- Challenge (e): In the second step, the verifier selects a random question that must be answered by the prover correctly, provided that he/she knows the secret information. This question is related to x and with the secret associated to the credentials of the prover.
- Answer (y): Finally the prover sends a response to the challenge and it is now when the verifier analyzes that response and checks if it is correct, in this case the authentication is accepted.

6 AUTHENTICATION METHODS IN FastTriaje

This section describes the authentication protocols implemented in FastTriaje to guarantee access control only to legitimate users. The two first protocols share certain features, for example both protocols are interactive (two parties, the prober A and the verifier B takes part) and the bootstrapping stage consists of defining an elliptic curve E and a base point P on it. Apart from that, the credentials associated to A are defined in the same way: the secret identification is an integer randomly selected in Zp, while the public one is a point on the curve E generated by multiplying the secret integer by the base point.

6.1 ZKP1 One-way Authentication: First Proposal

This protocol is devoted to authenticate mobile devices (A) against the web platform (B). A detailed description is included in Table III. It makes use of a hash function to define the challenge in each execution. This feature does not corresponds with the original definition of ZKPs but allows to reduce the number of iterations to just one in each authentication interaction.

Table 3: ZKP1.

Stages	Actions
Bootstrapping	p prime number E elliptic curve in Z_p $P \in E$
A's secret identification	$a \in Z_p$
A's public identification: PuidA	$a * P \in E$
Compromise: A's secret	$x \in_r {}^1 Z_p$
Witness: $A \rightarrow B$	$w = x * P \in E$
Challenge: $A \leftarrow B$	$e = hash(P, a * P, x * P)$
Answer: $A \rightarrow B$	$y = x + a * e \in Z_p$
Verification: B checks	$y * P - e * PuidA = w$

6.2 ZKP2 One-way Authentication: Second Proposal

The protocol described here is used to authenticate a user (A) against an NFC tag (B) prior to storing a triage on it.

Table 4: ZKP2.

Stages	Actions
Bootstrapping	p prime number E elliptic curve in Z_p $P \in E$
A's secret identification	$a \in Z_p$
A's public identification: PuidA	$a * P \in E$
Compromise: A's secret	$\{x_1 * P, x_2 * P, \cdots, x_n * P\}$ $\in E$, with $x_i \in_r Zp$
Witness: $A \rightarrow B$	$w = hash(x_j * P + x_k * P)$, with $j, k \in_r \{1, 2, \cdots, n\}$
Challenge: $A \leftarrow B$	$e \in_r Zp$
Answer: $A \rightarrow B$	$y = x_j + x_k - a * e \in Z_p$
Verification: B checks	$hash(y * P - e * PuidA)$ $= w$

However this protocol cannot be used directly on the NFC tags since they are totally passive, making it impossible for them to generate challenges. That is the reason why the the Fiat-Shamir Paradigm (Fiat and Shamir, 1987) has been used to transform the interactive ZKP2 into a non-interactive ZKP. The new protocol is described in Table 5.

Applying this paradigm requires the definition of the challenge by using a hash function. We have opted by using the new standard SHA3 (Bertoni et al.,).

Table 5: ZKP2 Non interactive.

Stages	Actions
Bootstrapping	p prime number E elliptic curve in Z_p $P \in E$
A's secret identification	$a \in Z_p$
A's public identification: PuidA	$a * P \in E$
Compromise: A's secret	$\{x_1 * P, x_2 * P, \cdots, x_n * P\}$ $\in E$, with $x_i \in_r Zp$
Witness: $A \rightarrow B$	$w = SHA3(x_j * P + x_k * P)$, with $j,k \in_r \{1,2,\cdots,n\}$
Challenge: $A \leftarrow B$	$e = SHA3(w) \in Z_p$
Answer: $A \rightarrow B$	$y = x_j + x_k - a * e \in Z_p$
Verification: B checks	$SHA3(y * P - e * PuidA)$ $= w$

7 CONCLUSIONS AND FUTURE WORK

A system that may improve logistics, the classification and attention of casualties in hostile situations such as natural disasters or accidents have been developed. The tool consists of a mobile application and a web service. The mobile application performs the triages and allows to store the results on NFC tags, that may be attached to victims. It is also possible to transfer them through a web service to a centralized web platform where the information may be processed according different user profiles.

Since the services provided are critical, security on data communication and reliability requirements have been taken into account.

There are still some points in the system than can be improved, such as:

- Adding statistical functionalities to the web platform.
- Integrating it with patient's clinical records.
- Extending the application to perform the second kind of triage.

ACKNOWLEDGEMENTS

This research has been partially supported by the Spanish Ministry of Economy and Competitiveness and Ministry of Science and Innovation under grants IPT-2012-0585-370000: DEPHISIT and TIN2011-25452: TUERI.

REFERENCES

NFC and Contactless Technologies. http://www.nfc-forum.org/aboutnfc/nfc_and_contactless/.

NFC Forum Official Page. http://www.nfcforum.org/home/.

Alpár, G., Batina, L., and Verdult, R. (2012). Using NFC phones for proving credentials. In *Proceedings of the 16th international GI/ITG conference on Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance*, MMB'12/DFT'12, pages 317--330, Berlin, Heidelberg. SpringerVerlag.

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

Bertoni, G., Daemen, J., Peeters, M., and Assche, G. V. The Keccak sponge function family . http://keccak.noekeon.org/papers.html.

Fiat, A. and Shamir, A. (1987). How to prove yourself: Practical solutions to identification and signature problems. pages 186--194. Springer-Verlag.

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

Iserson, K. V. and Moskop, J. C. (2007). Triage in medicine, part i: Concept, history, and types. *Annals of Emergency Medicine*, 49(3):275 – 281.

Martínez, S., Valls, M., Roig, C., Miret, J., and Giné, F. (2009). A Secure Elliptic Curve-Based RFID Protocol. *Journal of Computer Science and Technology*, 24(2):309–318.

no, J. A. M. C. El triaje. http://www.dit.upm.es/ jantonio/personal/cruzroja/.

Ramzy, I. and Arora, A. (2011). Using zero knowledge to share a little knowledge: Bootstrapping trust in device networks. In *Stabilization, Safety, and Security of Distributed Systems*, volume 6976 of *LNCS*, pages 371–385. Springer Berlin Heidelberg.

Raúl Sánchez Bermejo, Carmen Cortés Fadrique, B. R. F. (2011). El triaje en urgencias en los hospitales españoles. Unidad de Urgencias, Hospital General Nuestra Señora del Prado, Toledo, España.