A Secure Architecture Based on Ubiquitous Computing for Medical Records Retrieval

Silvio E. Quincozes[*]
Universidade Federal do Pampa
Av. Tiarajú 810, Alegrete, RS, Brasil
silvioereno@alunos.unipampa.edu.br

Juliano F. Kazienko[†]
Universidade Federal do Pampa
Av. Tiarajú 810, Alegrete, RS, Brasil
kazienko@unipampa.edu.br

ABSTRACT

Electronic health record systems are important tools employed for accessing and maintaining patient data, such as the history of hospitalizations and medical exams. Nowadays, physicians, nurses and hospital staff need fast and secure access to medical records avoiding bureaucracy for patient information retrieval and imprecision in patient's data maintenance. Ubiquitous and pervasive computing can contribute to overcoming such challenges; however the device impersonation problem should be carefully addressed in this scenario. To deal with such problem, this paper presents a secure architecture based on ubiquitous and pervasive computing for medical records retrieval and maintenance. Such architecture relies on Near Field Communication (NFC) for message exchange between smartphones and tags. An authentication mechanism is presented and validated to ensure device authentication. Analytical results reveal that such mechanism is efficient in providing mutual authentication. Additionally, another important security properties are reached, as confidentiality, message anti-replay and device anti-tracking. Finally, as proof of concept, we present a medication delivery study case based on a developed prototype.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: General—*Medical Systems.*

General Terms

Medical Systems, Ubiquity, Security.

Keywords

Architecture, Security, Electronic Health Records Retrieval, Ubiquitous Computing, Near Field Communication.

1. INTRODUCTION

Electronic health record systems are relevant tools for supporting hospitals staff—physicians, nurses, technicians, and other professionals—to supply an efficient health management. According to the purpose and the system's operator, these systems can be grouped. One of them consists in Personal Health Records (PHR), where the patients can access and control who access their records. Another group consists in Electronic Health Records (EHR), where the health institution handles the system maintenance [1] [10] [11] [12].

Particularly, EHR systems demand by a more complex infrastructure [11]. Speediness in data retrieval, precision in insertion of new data in the system, application's penetration in the hospital environment are important items to public health management in a efficient way. In this sense, medical errors can be mitigated with information technology support, as indicated in [9].

Nowadays, ubiquitous computing and communication are provided by portable and miniaturized devices connected by a network. However, providing a secure access to patient information is a challenge in EHR systems driving many issues [8]. Specially, the device—laptops, smartphones and tags—impersonation problem should be addressed for avoiding that attackers, which may be, i.e., a hospital visitor or even the patient, get access granted to patient information stored in the system. Private information regarding the patient may be disclosed, as drugs involvement, sexually transmitted diseases, and many others, due to the impersonation caused by identity theft, as a social security number of a person or a device serial number, for example. Another concern is related to the data modification that should be carried out only by the hospital professionals. In this sense, the health institutions need keeping safe such data and avoid the unauthorized access.

Additionally, the devices have limited resources in ubiquitous computing and communication. Smartphones, for example, have their time of battery affected by several applications that run on them. Lower price Near Field Communication (NFC) tags are not capable of processing. Besides, such tags are very limited in terms of memory that can be used in read and write operations. NFC technology has been broadly applied to medical systems, where NFC tags are used for patient identification and medication control [6] [10]. Ultimately, a security solution should take into account such devices characteristics, which make the design even more challenging. To the best of our knowledge, a suitable treatment is not given to the device impersonation problem in the literature, considering particularly an ubiq-

[*]Bachelor in Software Engineering.

[†]Researcher Professor.

2016 8th Euro American Conference on Telematics and Information Systems (EATIS), Cartagena de Indias - Colombia, April 27-29.
978-1-5090-2435-3/16/$31.00 ©2016 IEEE.

uitous scenario [2] [6].

The main contribution of this work is to propose a secure architecture for medical records retrieval and maintenance. The proposed architecture is based on ubiquitous computing and communication relying on NFC and *Wi-Fi* technologies. We introduce an authentication mechanism to provide security and solve the device impersonation problem in this scenario, as the impersonation of NFC-capable smartphones and tags. Such mechanism is validated and analyzed so as to demonstrate its efficiency in reaching mutual authentication. In addition, a prototype is presented and discussed for medication delivery to patients as a study case.

The remaining of this work is organized as follows. In Section 2, the related works are discussed. Section 3 presents the architecture and the authentication mechanism proposed. In Section 4 is shown a security validation and analysis of such authentication mechanism. At the end, the Section 6 presents the conclusion and future works.

2. RELATED WORKS

In this section, we provide a discussion regarding the electronic health systems and the ubiquitous computing applied to them. The work presented in [1] proposes a PHR system, where the patient can access his own health records through a mobile device. Medical records are signed by the physician. The main concern is about the patient data's privacy. For authentication purposes, the patient holds a smart card in order to access his health records using a mobile device. However, in this system, physicians need to be enrolled in the patient's PHR system. Otherwise, a physician may access the system using the patient's smartphone where personal data as photos and e-mails are stored, exposing the patient's privacy.

A Body Area Network based on sensors for ambient assisted living is proposed in [12]. The communication between a data collector device and the sensors is accomplished by *bluetooth* technology. As *bluetooth* is used, pairing between devices are necessary what implicates in communication delays. Besides, this proposal does not provide security in data exchange or device identification.

In [3], it is presented an adaptive synchronization approach that can be implemented by m-health applications to reduce the power consumption. For that, changes in the environment are captured battery level and network status. In this sense, the synchronization of collected data between biosensors end smartphones would be done at a low cost in terms of power consumption and communication delay. For communication, the 3G network, *Wi-Fi* technology or *bluetooth* can be used. However, the latter demands pairings between devices what causes extra delay in communications. Besides, this work does not address the information security. Traditionally, security causes overhead in power consumption and communication delay. As security is very relevant in ubiquitous health systems, an extended analysis would be important.

Recently, several works have highlighted the Near Field Communication (NFC) technology as a prominent tool for extend the ubiquitous computing and communication. NFC is a data communication technology that uses radio waves at high frequency of 13.56 MHz. The key to communication is proximate identification, usually limited to about 10cm [6]. It is important to notice that the short range of NFC transceiver does not totally avoid security attacks, as impersonation of devices. Among NFC-capable devices available, we can cite tags, smartphones, and laptops.

The work [10] presents a monitoring system of elderly and debilitated patients. The authors evaluate the system usability using practical experiments. NFC devices are used for user identification. Nevertheless, this work does not consider security issues as the authentication between devices, for example.

An EHR system is proposed in [13]. It is based on NFC-capable devices and *bluetooth*. In this proposal, the Secure Element (SE) is used to secure storage of credentials and to confidential data storage. The authors employ a Healthcard based on NFC devices with the aim at storing the patient health records. For reaching mutual authentication, the system is based on Public Key Infrastructure (PKI). However, such proposal depends on a Trusted Third Party (TTP) to generate, verify and store security keys, as mentioned by the authors. Another aspect consists in the high computational cost required by asymmetric encryption and operations related to certificates—specially for constrained resource devices, as tags and smartphones.

In the electronic payment world, security has been put on focus. The specification Europay, MasterCard and Visa (EMV) serves as a global specification for using of smart cards to credit and debit cards [7]. It prescribes authentication of cards by readers, in trading points. Authentication is obtained with *hashes* and off-line card authentication through public key cryptography. In EMV specification, there is no mutual authentication. That is, the card authenticity is ensured to the reader—or Point of Sale (POS)—but the POS authenticity is not ensured to the card. Hence, cards are vulnerable to the reading by a fake POS, which receives private information from the card.

In [5], some security issues of EMV are discussed. The authors specially discuss the electronic payment using the NFC technology and the possibility of information receiving by a fake POS. As the authors state, fake portable readers are cheap and even when turned off they can interact with an NFC-capable device. Due to such issues, the authors propose a mutual authentication protocol between a NFC phone and a POS, allowing them the sharing of a session key to perform secure transactions. However, such protocol depends on a Trusted Third Party (TTP) that shares particular symmetric keys with the devices. Therefore, TTP could personify the devices. Besides, this solution is not suitable for the ubiquitous scenario proposed in this paper that demands the communication and the identity verification of tags as well. Ultimately, the total number of exchanged messages in the protocol of [5] is seven as the total number of exchanged messages in the authentication mechanism presented in this paper, Section 3.2 is five. This feature is interesting from the point of view of the power consumption.

3. PROPOSED ARCHITECTURE

This section presents the proposed architecture. It aims at providing a secure and efficient access to medical records in a hospital environment. The components of such architecture are listed as follows:

- A *Server*. It stores the patient records, as exams, diagnostics, and medication prescriptions;
- *Smartphones*. They are used to retrieve data and system maintenance. Through these devices, physicians,

nurses and nursing technicians can modify and retrieve data from the Server;

- *An Access Point Wi-Fi.* In order to extend the system coverage area, we propose that communication between Smartphones and the Server takes place through the *Wi-Fi* technology [15]. Yet such communication is also possible using the NFC technology;

- *NFC Tags.* They store a *clue*—a hash—for leading to the patient identification, which is stored in the Server. For this proposal, the tags are attached to patient's bed. A possible extension to the system is to distribute tags to patients for outpatient treatment. In our proposal, we consider passive electronic read and write NFC tags. In passive tags, the transponder receives its power from the reader by magnetic induction. Thus, a tag can reply a reader device, for instance, a NFC-capable phone or a NFC-capable notebook;

- *A Desktop Application.* This application runs on the Server. It enables the patient hospitalization management and the system maintenance by a receptionist or physician;

- *An Application for Android Platform.* An application for android operating system that runs on Smartphones. It allows that a nursing technician, using her smartphone, take note regarding the delivery of prescribed medication to patients;

- *An Authentication Mechanism.* A last and important component of our proposed architecture consists of an Authentication Mechanism. It ensures mainly mutual authentication to avoid the device impersonation. The mechanism provides mutual authentication between the Server S and the Device M (Smartphone) based on a shared secret. Additionally, S also authenticates the tag (device T), identifying tags that do not belong to the system.

According to [14], systems may be categorized as local, remote and hybrid. The propose architecture presented in this section is local. It does not need connection to the Internet. Although it relies on a *Server* connected to the hospital network since the data is stored within the hospital dependencies. The hospital staff *Smartphones* are capable of sending and receiving information to this *Server* through a wireless access point using *Wi-Fi* technology [15].

3.1 Architecture's Overview

To start with, it is important to point out that the architecture proposed in this work is designed for an Electronic Health Records (EHR) system, where the health institution handles the system maintenance.

An overview of our proposed architecture is shown in Figure 1. In Step (1), a Receptionist retrieves the patient data and accomplishes the enrollment at the patient hospitalization. In this step, it takes place the binding between the patient and tag, which is attached to the patient bed. The Step (2) illustrates the storage of patient electronic health records in the server. Step (3) illustrates a tag attached to a patient bed. This tag stores a hash, which is used by the system to discover the patient identification. Afterward, in Step (4), the hospital professional put his mobile NFC-capable device—a smartphone or a tablet—close to a tag so as to read the hash from it through NFC technology. Soon after, such hash is sent to the server in Step (5) using *Wi-Fi* connection. The server, in turn, will check and recover the tag identification. It is important to emphasize that starting from Step (4) the mutual authentication mechanism is already working. It avoids the device impersonation even if an attacker device is present. This mechanism is explained in details in Section 3.2.

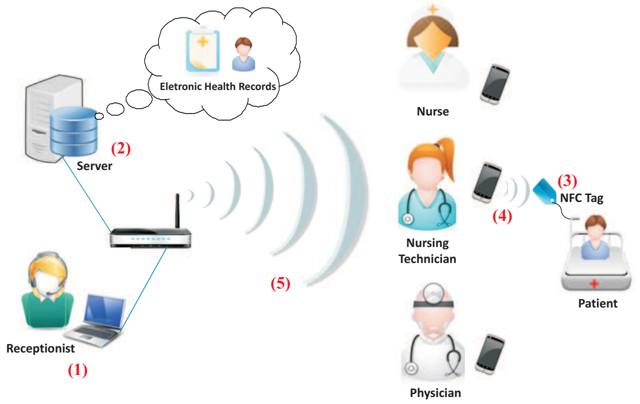


Figure 1: Architecture's overview.

3.2 Authentication Mechanism

For this work, we consider the use of NFC tags that does not accomplish processing. Such tags are cheaper than other tag types what facilitates its adoption. Nevertheless, these tags are enabled for reading and writing. As previously detailed in Section 3, such tags are powered by magnetic induction from the NFC-capable reader.

The Figure 2 presents the security mechanism proposed. The Device T represents a tag. It stores a hash that works as a *clue* for leading to the patient identification, which is stored in the Server. That is, H_1 is previously loaded in T, where $H_1 = hash(R||K_T)$. The key K_T is shared between the tag and the Server S. The random number R is generated by S.

In turn, S stores a database that contains information to support the authentication mechanism. For each *tag* enrolled to the system is stored an identification ID_T, the key K_T, the random number R and the *hash* from the concatenation of ID_T with K_T. Additionally, in regards to the Device M, a *smartphone*, S stores shared key K_M, a transaction counter C_1 and the hash of K_M concatenated with C_1.

The Device M, from Figure 2, represents the mobile device (*smartphone*) from a health professional. M holds the key K_M shared with S. Moreover, M holds a transaction counter C_2, which is increased after M authenticates S.

For access data from a certain patient, M must be close to T in order to retrieve H_1. The first message M_1 is just a reading request of T. Soon after, through the message M_2, T sends to M the hash H_1, which is stored within it.

Since any NFC-capable device can read H_1 without identity verification, S needs of an authentication mechanism so as to authenticate M avoiding that an illegitimate smartphone impersonates a legitimate one. For this reason, after the reading of H_1 from T, M computes $H_2 = hash(C_2||K_M)$.

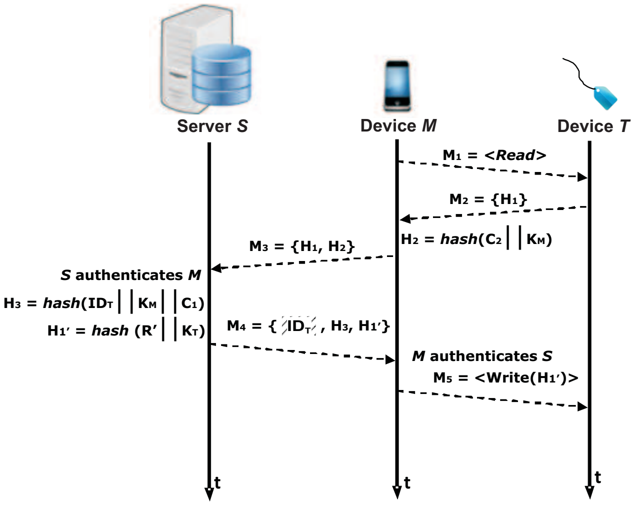


Figure 2: Authentication mechanism.

Thus, M sends the message $M_3 = \{H_1, H_2\}$ to the Server S.

Based on the shared key K_M and the counters C_1 and C_2, S can compute $H_2' = hash(C_1||K_M)$ and verify if $H_2 = H_2'$. If these values are the same, then S believes that it is communicating with a legitimate M. This processing takes place as described in the Algorithm 1. Since M is authentic, S authenticates T using $H_1 = hash(R||K_T)$ received in M_1, a list of known tags by the Server and $H_1' = hash(R||K_T)$, which is compared to H_1. Moreover, the value of C_1 is increased. Due to the comparison of C_1 and C_2, S knows that the message M_3 is fresh preventing the replay attack.

To prove its legitimacy, S computes the following hash: $H_3 = hash(ID_T||K_M||C_1)$. This hash will be checked by M later. Additionally, for providing anti-tracking feature, S refreshes the value stored within the tag—that was transmitted in M_2—by the generating of a new random number R' and a new hash value, as follows: $H_1' = hash(R'||K_T)$. So, M_4 is sent to the Device M, where $M_4 = \{E_{KM}(ID_T), H_3, H_1'\}$. It is important to notice that ID_T is encrypted with the shared key K_M. To denote it, ID_T appears striped in Figure 2.

Later, the mobile device M computes the hash H_3' so as to verify the identity of S. Such hash is computed from the shared key K_M, the C_2 controlled by M, and the ID_T received in M_4. That is, $H_3' = hash(ID_T||K_M||C_2)$. Soon after, H_3 is compared to H_3', as shown in Algorithm 2. If these hashes are the same, then S is authentic. Thus, the counter C_2 is increased so as to be synchronized with C_1, which is controlled by S.

Finally, in M_5, the hash value H_1' is sent to T. Such hash overwrites the old value stored within the tag, that is, value is refreshed. In this sense, the new hash value will be sent to a device M at the next time in which the tag be read, mitigating the tag tracking. At this moment, the mobile device M can retrieve or modify information regarding the patient. Hence, before every information retrieval or modification, the messages presented in Figure 2 are exchanged to avoid the impersonation and the unauthorized access.

Algorithm 1 S authenticates M

```
M is composed of $C_1, K_M, H_2'$
T is composed of $ID_T, K_T, H_1'$
List of M $L_M[\,] = \{M_1, M_2, ..., M_n\}$
List of T $L_T[\,] = \{T_1, T_2, ..., T_n\}$
String $H_1$, $H_2$, $H_3$, $H_M$, $H_T$
$H_1 = ReceiveH_1()$
$H_2 = ReceiveH_2()$
for $i = 0$ to $|L_M|$ do
    if $M_{[i]}.H_2' = H_2$ then
        Successful authentication of M
        $M = M_{[i]}$
        for $i = 0$ to $|L_T|$ do
            if $T_{[i]}.H_1' = H_1$ then
                $T = T_{[i]}$
                Successful Authentication of T
                $H_3 = $ hash $(ID_T||M.K_M||C_1)$
                $M.C_1 = M.C_1 + 1$
                $H_1' = $ hash $(R'||T.K_T)$
                $Send(E_{KM}(ID_T), H_3, H_1')$
            end if
        end for
    end if
end for
if $M = $ null then
    Send "Mobile Device Authentication Fail."
end if
if $T = $ null then
    Send "Tag Authentication Fail."
end if
```

Algorithm 2 M authenticates S

```
String $C_2$, $K_M$, $ID_T$, $H_1$, $H_2$, $H_3$, $H_1'$
$H_3 = ReceiveH_3()$
$H_1' = ReceiveH_1'()$
if $H_3 = H_3'$ then
    Successful Authentication
    $C_2 = C_2 + 1$
    $TagWritten(H_1')$
end if
if $H_3 \neq H_3'$ then
    Authentication Fail
end if
```

4. SECURITY VALIDATION AND ANALYSIS

In this section, we present a validation and an analysis of our authentication mechanism. The validation is based on *Burrows-Abadi-Needham* (BAN) Logic so as to evaluate the security in the proposed architecture. BAN Logic was originally proposed in [4], where the authors intend to verify and validate the security of protocols to demonstrate their effectiveness in reaching the proposed aims.

For this evaluation, we focus mainly on the authentication mechanism, presented in Section 3. The validation—through the BAN logic—is composed of three steps as follows: *Idealization*, where the messages are described according to this logic; *Assumptions*, with the raising and definitions of assumptions, which must to respect BAN logic sintaxe; and *Validation*, that consists in the rules application in order to conclude regarding the protocol effectiveness.

4.1 BAN Notation

Table 1 describes the logic expressions used in this work. We distinguish three objects through of the basic notation of BAN: T, for tag; M, for mobile device; and S, for the server. Besides, we distinguish the symmetric keys K_M and K_T, and the counters C_1 and C_2.

Table 1: BAN Logic Notation.

Representation	*Meaning*
A $\mid\equiv$ B	A believes in B: For A, B is true
A $\triangleleft$ X	A receives X: A has received a message which contains M
P $\mid\sim$ X	P said X: P has sent a message that contains X
P $\mid\Rightarrow$ X	P has complete control over X; P is responsible for X
#(X)	*New* X: X is fresh, and it has not been used before
$\{X\}_K$	Formula X is encrypted with K key
$A \overset{K}{\leftrightarrow} B$	The key K is shared only between A and B
$\frac{F}{F'}$	It can infer Formula F' from Formula F

4.2 BAN Workflow

As described in Section 3, the messages used in the authentication mechanism are the following:

M1. $M \rightarrow T : Reading$

M2. $T \rightarrow M : hash(R||K_T)$

M3. $M \rightarrow S : hash(R||K_T), hash(C_2||K_M)$

M4. $S \rightarrow M : K_M(ID_T), hash(ID_T||K_E||C_1), hash(R||K_T)$

M5. $M \rightarrow T : hash(R||K_T)$

It is important to point out that the symbol → denotes the sending of a message. Therefore, e.g., the expression A → B: M is used for denoting a message M sent from A to B.

4.2.1 Idealization

M2. $T \rightarrow M : H(\#(R)||K_T)$

M3. $M \rightarrow S : H(\#(R)||K_T), H(\#(C_2)||K_M)$

M4. $S \rightarrow M : K_M\{ID_T\}, H(ID_T||K_M||\#(C_1)),$
$H(\#(R)||K_T)$

4.2.2 Assumptions

1. $S \mid\Rightarrow K_T$
2. $S \mid\equiv S \overset{K_M}{\leftrightarrow} M$
3. $S \mid\equiv ID_T$
4. $S \mid\Rightarrow C_1$
5. $S \mid\Rightarrow R$
6. $S \mid\equiv T$
7. $S \mid\equiv M$
8. $S \mid\equiv M \mid\equiv K_M$
9. $S \mid\equiv M \mid\equiv T \mid\equiv H(R||K_T)$
10. $T \mid\equiv H(R||K_T)$
11. $T \mid\sim M\ H(R||K_T)$
12. $M \triangleleft S\ \{ID_T\}K_M$
13. $M \mid\equiv M \overset{K_M}{\leftrightarrow} S$
14. $M \mid\Rightarrow C_2$
15. $M \triangleleft ID_T$
16. $M \mid\equiv S$
17. $M \mid\equiv T$
18. $M \mid\equiv T \mid\equiv H(R||K_T)$
19. $M \mid\equiv S \mid\equiv ID_T$
20. $M \mid\equiv S \mid\equiv K_T$
21. $M \mid\equiv S \mid\equiv K_M$
22. $M \mid\equiv S \mid\equiv C_1$
23. $M \mid\sim S\ H(R||K_T)$
24. $M \mid\sim S\ H(\#\{C_2\}||K_M)$

4.2.3 Validation and Conclusion

M2:

25. As M does not know K_T, the information regarding this message is not enough to state that M believes in T. That is, such message is still not enough to M authenticate T, however it proves that T believes in the transmitted information. Besides, although M does not know R, M believes that $\#(H(R||K_T))$ because the $\#(R)$ what ensures anti-tracking. A formal description is presented as follows:

$$\frac{T|\sim H(\#(R)||K_T)M}{M|\equiv T|\equiv H(R||K_T)} \text{ and } \frac{\#(R)}{\#(H(R||K_T))}$$

Therefore,

$$\frac{T|\sim H(\#(R)||K_T)M}{M|\equiv \#(H(R||K_T))}$$

M3:

26. Based on the premise in which S has complete control over C_1 and since S believes in the shared key K_M, at the moment in which S receives $H(\#(C_2)||K_M)$, we can infer that S trusts M has knowledge of C_2 and K_M. Hence, S believes that M is authentic. Additionally, given that the counter C_1 must be equal to counter C_2—that is a fresh value—S is safe against message replay attacks, as follows:

$$\frac{S|\Rightarrow C_1, S \overset{K_M}{\leftrightarrow} M, S \triangleleft H(\#(C_2)||K_M)}{S|\equiv M}$$

27. M sends data from T to S. As $H(R||K_T)$ verification takes place, S believes that M believes that T knows the value of this *hash*. Since K_T is controlled by S, hence S believes in T authenticity.

$$\frac{T|\sim\#(H(R||K_T))M, M|\sim\#(H(R||K_T))S, S|\Rightarrow H(R||K_T)}{S|\equiv T}$$

M4.

28. Given that S has sent the $E_{KM}(ID_T)$ and the hash $H(ID_T||K_M||C_1)$—or H_3 as explained in Section 3.2—to M, we can infer that S is authenticated by M. It is important to notice that C_1 is fresh, that is, $\#(C_1)$. Such reasoning is strongly based on the fact that only S and M have knowledge of the shared secret key K_M.

$$\frac{M \overset{K_M}{\leftrightarrow} S, M\Rightarrow C_2, S|\sim\{ID_T\}K_M M, S|\sim H(ID_T||\#(C_1)||K_M)M}{M|\equiv S}$$

Since S believes in T and M believes in S, we can infer that M believes in T.

$$\frac{M|\equiv S, S|\equiv T}{M|\equiv T}$$

Hence, we demonstrate that the authentication mechanism reaches mutual authentication. Additionally, such mechanism improves the system security, avoiding the tracking of devices and the replay of messages. Through the evaluation of the exchanged messages, we argue that the protocol reaches its purpose.

4.3 Security Analysis

In this section, we discuss the security features of the proposed mechanism.

4.3.1 *Mutual Authentication*

The authentication mechanism provides authentication of the Device M and the Server S. It is reached due to the secret K_M shared between both. In addition, the tag identity is verified by the Server S. That is, the Server verifies if the tag is enrolled—or legitimate—by getting its ID from the H_1 in M_3.

4.3.2 *Confidentiality*

After performing the authentication mechanism, all information exchanged between S and M is encrypted with K_M.

4.3.3 *Anti-Tracking*

The information stored in a tag is refreshed every time the authentication mechanism runs. This characteristic avoids the device tracking.

4.3.4 *Anti-Replay*

Counters are used to prevent the message replay. The values of C_1 and C_2 are increased according to received messages. Thus, M and S recognize replayed messages.

4.3.5 *Anti-Cloning*

In our work, the Server authenticates the tags. In other words, it identifies tags that do not belong to the system. However, a tag cloning attack remains possible [6] [13]. A solution to this problem is not presented in this paper and we plan to address this issue in a future work.

5. PRACTICAL EVALUATION

In this section, as a first study case of the proposed architecture, we present and discuss a developed prototype to the medication delivery to patients. Such system's module demands a precise and secure access for avoiding delivering mistakes. Our aim is to evaluate—in laboratory environment—the system functionality and communication delay. In Section 5.1, the prototype details are presented. Section 5.2 discuss our findings.

5.1 Prototype

In order to evaluate the proposed architecture, we have implemented a prototype. It is important to point out that before the medication delivery takes place it is necessary the medication prescription by a physician. In the medication prescription module, a physician may include new prescriptions in the electronic health records during the patient hospital stays. For that, as described in Section 3, each hospital bed contains a NFC tag impregnated. Thus, a physician can accomplish medication prescription to patients closing his smartphone to the tag during a visit to the patient's room. Such tag contains information that enables the patient identification.

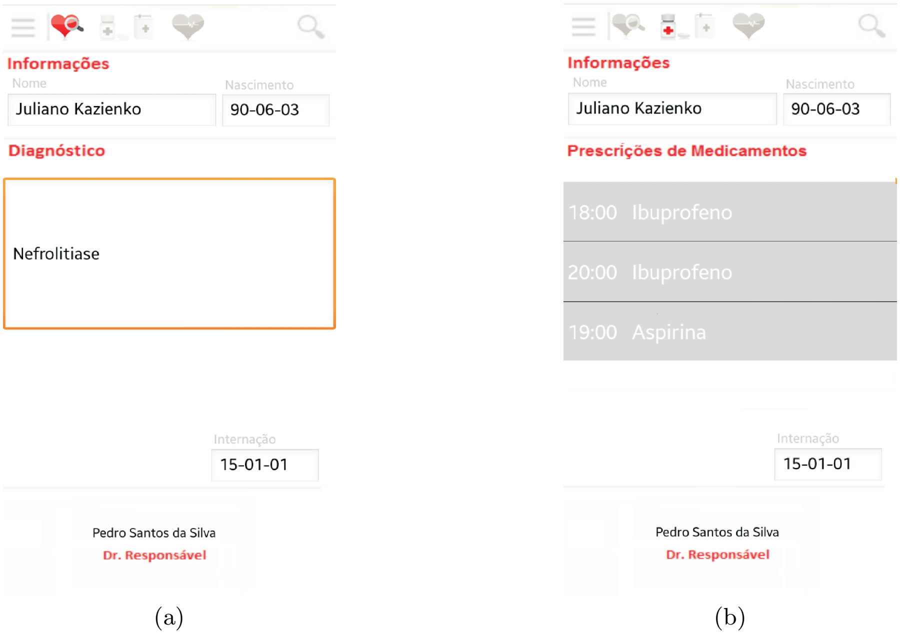
For the implementation of the medication delivery prototype, we have relied on the *Hospital de Caridade de Jaguari* (HCJ), placed in Jaguari city, Brazil. In this institution, the medication delivery is typically carried out by a nursing technician. Thus, the prototype of medication delivery presented in this work should be performed by such professional using her smartphone.

The prototype is implemented in C Sharp language. For experimental purposes, it is used the Message Digest 5 (MD5) algorithm for hash computation. However, any other algorithm could be used. Additionally, the following materials are used for this evaluation:

- A smartphone Galaxy S4 Zoom Android platform 4.4.2;
- A notebook Sony Vaio svf15213cbw, OS Windows 8;
- An access point D-Link, DI524;
- A NFC tag Mifare DESFire 4k.

When a nursing technician closes her smartphone to the tag, the patient's identification is captured and transmitted by *Wi-Fi* Technology to an access point and, in turn, to a server. Afterwards, the patient's diagnosis is displayed on the smartphone's screen of the professional, as shown in Figure 3(a). The diagnosis works as a summarized report supplying information regarding the patient disease and patient history. The knowledge of the disease helps the professional in the prevention of mistakes in medication delivery. At the moment in which the technician desires to view the list of remaining medications to deliver, she may touch on the third button at the top of the screen. We highlight that the language adopted for the prototype screens is Portuguese—as shown in Figures 3(a), 3(b), 4(a) and 4(b)—because we intend to extend and deploy the prototype in HCJ, as aforementioned.

Figure 3(b) shows the list of remaining medications to deliver. As previously detailed, the technician may view this screen by touching on the third button at the top of Figure 3(a). In Figure 3(b), the system shows the description of the



Informações
Nome: Juliano Kazienko
Nascimento: 90-06-03
Diagnóstico
Nefrolitiase
Internação: 15-01-01
Pedro Santos da Silva
Dr. Responsável

(a)

Informações
Nome: Juliano Kazienko
Nascimento: 90-06-03
Prescrições de Medicamentos
18:00 Ibuprofeno
20:00 Ibuprofeno
19:00 Aspirina
Internação: 15-01-01
Pedro Santos da Silva
Dr. Responsável

(b)

Figure 3: The Figure (a) illustrates the summarized report with diagnosis shown to the nursing technician. Figure (b) depicts the list of remaining medications for delivering.

medication, delivery time and the frequency of delivery for each medication. Notice that at any time, a nursing technician can consult the electronic health records of a patient for checking if there are new medications by pressing the third button at the top of smartphone's screen.

The Figure 4(a) illustrates the confirmation screen. It appears after the technician select what medications she has delivered. Hence, the previously selected medications—the first one shown in the screen—are removed from the list of pending medications. The Figure 4(b) shows the screen with the remaining medications for delivering.

5.2 Results and Discussion

In our experiments, we consider two metrics: (i) prototype functionality and (ii) communication delay. Basically, we focus on the medication delivery module for the prototype implementation. The experiments were performed in laboratory environment.

The prototype footprint is 1320.96 kB. Thus, it fits well within the smartphone's memory used—described in Section 5.1—which is capable of storage 8 gB.

For practical evaluation, 20 experimentation runs were carried out, capturing the time demanded to perform a medication delivery—from the receiving of tag data to the message of medication removal sent to the server—for 20 times. It is important to point out that the time spent by the technician for removal confirmation (Figure 4(a)) was not considered. A server side application was installed in the notebook described in Section 5.1.

Considering a list of three medications prescribed to a patient, the average communication delay for medication delivery is 198.95 ms. Such time includes the authentication mechanism execution described in Section 3.2. Hence, the practical experiments reveal a low average communication delay and the prototype functionality enabling the conclusion of a medication delivery in less than a minute technically. We do not consider the time to select the medication delivered and to confirm the medication removal because it depends on the user skills. However, we argue the increased time into medication delay is low for a trained operator.

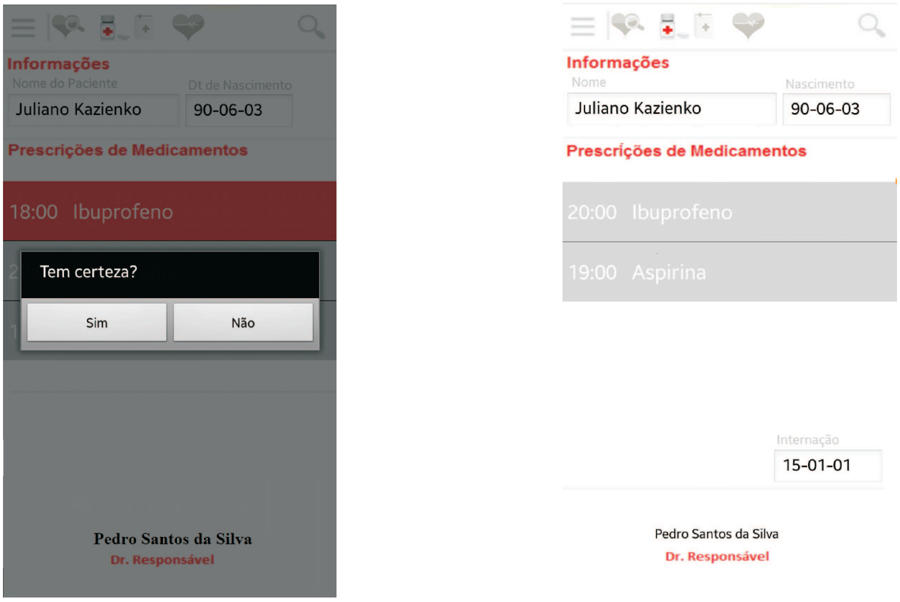
6. CONCLUSION AND FUTURE WORKS

In this work, we propose a secure architecture for medical records retrieval and maintenance. In order to increase speediness, precision and hospital penetration, such architecture is based on ubiquitous computing relying mainly on the intensive use of NFC-capable devices including passive electronic read and write NFC tags.

Additionally, a lightweight authentication mechanism was introduced. Using a short number of messages, its aim is to cope with the device impersonation problem by attackers. It provides mutual authentication between the Server S and the Device M (Smartphone) based on a shared secret, without the need of a Trusted Third Party (TTP). Moreover, S also authenticates the tag (device T), identifying tags that do not belong to the system. Such mechanism is validated and analyzed so as to demonstrate its efficiency in reaching mutual authentication and other security features.

Experimental practical evaluation reveals that the architecture is partly functional covering an important system module: medication delivery. Although the low average communication delay, it is necessary to extend the experimentation specially related to wireless communications peculiarities, as interference.

For future works, we intend to implement and to deploy a full prototype of the proposed architecture in the HCJ. Hence, an extended experimental evaluation will be carried out in order to reach new findings specially in terms of security, speediness and the precision.



Informações

Nome do Paciente: Juliano Kazienko

Dt de Nascimento: 90-06-03

Prescrições de Medicamentos

18:00 Ibuprofeno

Tem certeza?

Sim Não

Pedro Santos da Silva

Dr. Responsável

(a)

Informações

Nome: Juliano Kazienko

Nascimento: 90-06-03

Prescrições de Medicamentos

20:00 Ibuprofeno

19:00 Aspirina

Internação: 15-01-01

Pedro Santos da Silva

Dr. Responsável

(b)

Figure 4: The Figure (a) illustrates the medications removal confirmation screen. The Figure (b) depicts the refreshed list of remaining medications.

Acknowledgment

The authors would like to thank the *Universidade Federal do Pampa*, Brazil, for the support in their activities and the *Hospital de Caridade de Jaguari*, Brazil, for the partnership in this research effort.

7. REFERENCES

[1] M. H. Aboelfotoh, P. Martin, and H. S. Hassanein. A mobile-based architecture for integrating personal health record data. In *16th IEEE International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 216–221, 2014.

[2] A. Alzahrani, A. Alqhtani, H. Elmiligi, F. Gebali, and M. S. Yasein. NFC Security Analysis and Vulnerabilities in Healthcare Applications. In *IEEE Pacific Rim Conference on Communications, Computers & Signal Processing*, pages 302–305, 2013.

[3] A. Benharref, M. A. Serhani, and R. M. Khalifa. Smart Data Synchronization in m-Health Monitoring Applications. In *16th IEEE International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 78–83, 2014.

[4] M. Burrows, M. Abadi, and R. M. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, 1990.

[5] U. B. Ceipidor, C. M. Medaglia, A. Marino, S. Sposato, and A. Moroni. KerNeeS: A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions. In *9th International ISC Conf. on Information Security and Cryptology*, pages 115–120, 2012.

[6] V. Coskun, B. Ozdenizci, and K. Ok. A Survey on Near Field Communication (NFC) Technology. *Wireless Personal Communications*, 71:2259–2294, Dec. 2013.

[7] EMVCo. EMV Contactless Specifications for Payment Systems. Technical Report Book C-2, v. 2.4, Feb. 2014.

[8] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval. Security and Privacy in Electronic Health Records: A Systematic Literature Review. *Journal of Biomedical Informatics*, 46:541–562, 2013.

[9] M. Z. Hydari, R. Telang, and W. M. Marella. Electronic health records and patient safety. *Communications of the ACM*, 58(11):30–32, 2015.

[10] R. Iglesias, J. Parra, C. Cruces, and N. G. de Segura. Experiencing NFC-based touch for home healthcare. In *2nd International Conference on Pervasive Technologies Related to Assistive Environments*, page 27, 2009.

[11] J. Magnuson and P. C. Fu. *Public Health Informatics and Information Systems*. Springer, 2014.

[12] D. F. M. Rodrigues, E. T. Horta, F. D. M. Guedes, and J. J. P. C. Rodrigues. A Mobile Healthcare Solution for Ambient Assisted Living Environments. In *16th IEEE International Conference on E-health Networking, Application and Services (Healthcom)*, pages 115–120, 2014.

[13] D. Sethia, D. Gupta, T. Mittal, U. Arora, and H. Saran. NFC based secure mobile healthcare system. In *6th International Conference on Communication Systems and Networks*, pages 1–6, 2014.

[14] R. Steele, K. Min, and A. Lo. Personal health record architectures: technology infrastructure implications and dependencies. *Journal of the American Society for Inf. Science and Technology*, 63(6):1079–1091, 2012.

[15] Wifi. IEEE 802.11 Wireless Local Area Networks. Available in: `http://www.ieee802.org/11/`, 2015. Access on: April, 2015.