Patient's privacy protection with anonymous access to medical services

Dasun Weerasinghe, Kalid Elmufti, Muttukrishnan Rajarajan and Veselin Rakocevic
Mobile Networks Research Group
School of Engineering and Mathematical Sciences
City University,
Northampton Square, London, EC1V 0HB, UK.
dasun.weerasinghe@city.ac.uk

***Abstract*—The Internet and mobile networks have penetrated the healthcare sector due to their increased functionality, low cost, high reliability and easy-to-use nature. However, in such healthcare environment the privacy and security of the transmitted information must be preserved. When dealing with health sensitive information at times it is vital to protect the patient's identity and their health sensitive information from third parties. In this paper we present a protocol that will authenticate and authorize patients to healthcare services without providing the patient's identification. The protocol protects patient's privacy with a secure anonymous authentication to healthcare services, where the patient has access to a complete set of healthcare services.**

I. Introduction

Electronic or mobile healthcare networks are established by connecting general practitioners, hospitals and national/private medical centres. This approach is an attractive solution for the already overstretched and under budgeted health sector since it reduces the current paper-based work, decreases waiting time, eliminates prior appointment requirements, enhances healthcare services with efficient, faster and more reliable methods, eliminates errors that can happen in the paper records and speeds up administrative procedures [11]. However, the development of such a working model in live medical environment will be subjected to an increase in the amount of sensitive medical information being transferred between different parties and the data transmission will take place over the Internet or the mobile network. The key problem in online/network media is the security and privacy of communication, especially the information about the health condition and medications. Our previous paper proposed the necessary security approaches to prevent eavesdropping, spoofing and modifications to the healthcare information over the network [12]. This paper proposes an approach to solve the problem of the patient's privacy using a novel anonymous access control technique.

There has been a number of research activities carried out in privacy as a social and legal issue [4]. Privacy may be understood as the right and desire of a person to control the disclosure of personal information [10]. This control can be passed to a third party in exchange for some services. A function of anonymity is a sub-section of the privacy protection. Anonymity protects user privacy by authenticating the user without identification. For example a patient who has registered with the National Health Service (NHS) should be able to receive healthcare advice from any medical centre without disclosing their identity.

The demand for user anonymity has been increased rapidly with the invention of electronic and mobile healthcare domains. An unauthorized access to a person's health sensitive data can be subjected to different type of misdemeanours. Some of the misdemeanours are as follows;

- The insurance companies are interested to know the undisclosure medical conditions of their clients to increase the insurance premium
- The access to addiction or mental sensitive health information of a patient will affect badly on his potential employment opportunities
- Banks will be reluctant to approve loans if they notice any serious health conditions of the account holder

So patients are reluctant to use online healthcare services due to the possibility of misusing the health sensitive data by third parties. In the past there have been incidents on disclosing the patient's medical information to external parties from various institutions such as healthcare providers, blood banks, pharmacies and adoption agencies [3] [8]. Some patients are too embarrassed to meet a doctor or a general practitioner face-to-face to discuss some private and sensitive healthcare issues. They prefer to use a remote media but again the identity of the patient shouldn't be disclosed. Therefore the anonymous access to medical services is one of the key requirements in electronic and mobile healthcare environments. This paper proposes a medical environment to access medical services without revealing the patient's identity to the medical services or third party service providers.

II. Related work and technology requirements

The research on anonymous authentication has been carried out by a number of research groups worldwide. A group of researchers from Tokai University, Japan have proposed an approach to access services based on user's authority but without identification at the service provider. This approach is based on Attribute certificate issued by the Attribute Authority [6]. Leszczyna has presented two un-traceability protocols for mobile agent environment as a solution for anonymous

PERVASIVEHEALTH 2008, 30 Jan - 1 Feb. Tampere, Finland / Copyright © 2008 ICST 978-963-9799-15-8
DOI 10.4108/ICST.PERVASIVEHEALTH2008.2509

access of IT services and its applications to an e-Health counselling scenario. Un-traceability is a subset of anonymity since the identity cannot be inferred by tracing the message [7]. Gritzalis et al. have discussed about the importance of privacy and confidentiality in electronic healthcare to the human psyche. They have used a real scenario implemented through a well-established distributed electronic environment in Greece that treats beta-thalassemia patient for more than five years [4]. One of our previous papers addresses authentication and privacy concern in electronic healthcare environment and ways to prevent it using the technologies such as Web services, Generic Authentication Architecture from 3GPP and Universal Mobile Telecommunications System (UMTS) [2]. A group of researchers from Aalborg University, Denmark have proposed a solution to protect user sensitive data with contextaware privacy protection mechanism by filtering the data before any disclosure in a medical environment [9].

The system proposed in this paper is based on the Single-Sign-On (SSO) and XML security technologies. SSO technology lets user authenticates to a single authentication authority once and allows accessing all the authentication protected resources and services without re-authentication [5]. The protocol developed in this study follows the SSO model based on Liberty Alliance standards and guidelines [1].

III. Anonymous Access in Medical Environment

A patient with a web browser/mobile device connects to the Healthcare Service Unit (HSU) over the Internet/mobile network in the proposed anonymously accessible medical environment. This HSU and medical environment is owned by a publicly trusted organisation for medical services. The healthcare Service Providers (HSP) such as private medical centres and General Practitioners provide healthcare services to patients. These services have to be registered using an offline methodology with the HSU before providing any services. The HSU authenticates and authorises patient with the mobile device for accessing service providers. The patient registers with healthcare service providers before accessing any services and registration process is performed through the HSU as shown in Figure 1. Once the registration process is completed the patient can access services with a hidden identity to the healthcare service provider. However the patient's identity is disclosed to HSU for the patient's authentication into the environment. Based on the identity and credentials the patient is authenticated and authorized to access healthcare service providers through HSU. However patient's identification is not disclosed to the healthcare service providers. The HSU acts as an anonymous identity provider, user authenticator and service access storage.

IV. Protocol

The protocol presented in this paper provides an anonymous authentication for patients to access healthcare service providers. Patients receive medications over the Intent/mobile network without revealing their true identity. The following conditions must be satisfied prior to the use of the protocol.

- Many healthcare service providers are registered with the HSU
- The HSU and healthcare service providers maintain an asymmetric key secure communication channel between them
- Each HSP has more than one registered patient through HSU for anonymous access

A. Patient registration with the HSP

The patient registers with the HSP using the authentication at HSU. The sequence of exchanged messages (Figure 1) are as follows:

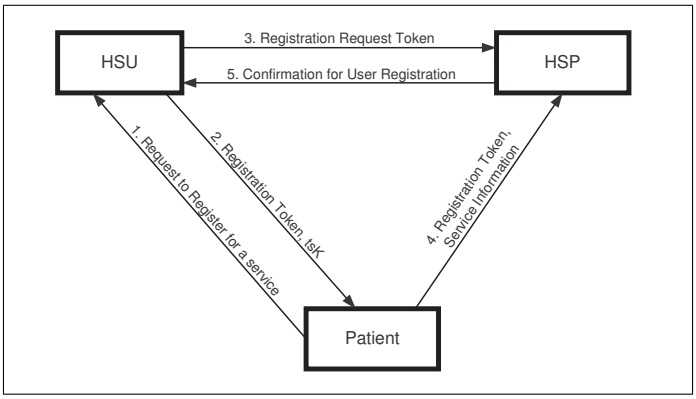

Fig. 1. Patient registration with HSP

1) Patient to HSU; the patient makes a request to register for an anonymous service access with healthcare service provider.
2) HSU to Patient; HSU generates and sends the registration token and a temporary session key (tsK). The temporary session key is used for the secure communication between the patient and the healthcare service provider.
3) HSU to HSP; the HSU sends the registration request token to HSP
4) Patient to HSP; the patient sends the registration token with HSP offline/online service access information to HSP. The service access information is an option filed in the message and it is encrypted using the tsK.
5) HSP to HSU; HSP sends the registration confirmation message to the HSU if the registration request token is validated successfully with patient's registration token. With the successful confirmation HSU records the identity of the patient with the healthcare service provider's identification.

B. Patient authorization and anonymous service access

The patient authorises to access services from HSP using the authorization provided by HSU. The sequence of exchanged messages (Figure 2) are as follows:

1) Patient to HSU; the patient requests to access a healthcare service provider anonymously by sending the healthcare service provider's identity.
2) HSU to Patient; the HSU generates a temporary user identity for the patient and it is a random number

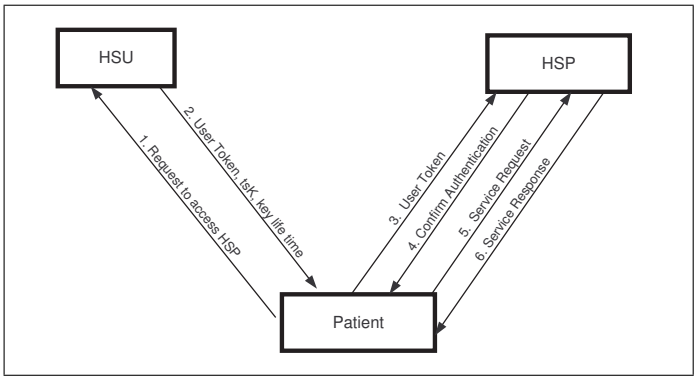

Fig. 2. Patient authorization and anonymous service access

for each service request. The temporary session key (tsK) is generated by the HSU to establish a secure communication channel between the patient and the healthcare service provider. The HSU sends the tsK, key life time and user token to the patient. HSU records the user identity, temporary user identity, service provider identity and timestamp in its database

3) Patient to HSP; the patient sends the user token as the login request to healthcare service provider. The patient will be an anonymous user to the HSP since the user token doesn't have any parameters to identify the true identity of the patient but it confirms that patient is a registered user at the HSP and he/she is authorized to access services.
4) HSP to Patient; the healthcare service provider validates user token and sends the confirm authentication message to the patient.
5) Patient to HSP; Patient sends the service request message to healthcare service provider and it is secured using the tsK.
6) HSP to Patient; The healthcare service provider responses to the message with encrypting the response using the tsK.

The patient can send many service requests to the same healthcare service providers until the temporary session key is expired. If it is expired or the patient wants to change the healthcare service provider then patient has to do a new service access request to the HSU. Then the HSU will generate a new temporary session key and temporary identification for the patient.

V. Security Tokens

The following are tokens deployed in the proposed schema and authors have reduced sizes and complexity of tokens as much as possible due to the processing power constrains of the mobile device and bandwidth constrains in the mobile networks;

- RegistrationToken (RT=$e_{HSP}(s_{HSU}$[UID|TS])); used by the healthcare service provider to identify and authenticate legitimate patient registration requests that are validated from the HSU. It consists with the user identification created by the HSU and the timestamp. The registration token is signed by the secret key of HSU and it is encrypted using the service provider's public key.

- RegistrationRequestToken (RRT=$e_{HSP}(s_{HSU}$[UID|TS|tsK|KeyLifeTime])); used by the healthcare service provider to identify legitimate patient registration requests from HSU. It consists with the user identification of patient, temporary session key, key life time and the timestamp. The RegistrationRequestToken token is signed by the HSU secret key and encrypted using the service provider's public key.

- UserToken (UT=$e_{HSP}(s_{HSU}$[TUID|TS|tsK|KeyLifeTime])); used by the healthcare service provider to authorize anonymous service access requests from patients. It consists with temporary user identity, timestamp and temporary session key and key life time. The UserToken token is signed by the HSU secrete key and encrypted using the service provider's public key.

Following are the implementation of tokens as XML objects. However these snapshots are taken before the XML encryption and XML signature are applied.

- RegistrationToken

```
<RegistrationToken>
    <UID>String</UID>
    <TimeStamp>Timestamp</TimeStamp>
</RegistrationToken>
```

- RegistrationRequestToken

```
<RegistrationRequestToken>
    <UID>String</UID>
    <TimeStamp>Timestamp</TimeStamp>
    <TempSessionKey>Key</TempSessionKey>
</RegistrationRequestToken>
```

- UserToken

```
<UserToken>
    <TempUID>String</TempUID>
    <TimeStamp>Timestamp</TimeStamp>
    <TempSessionKey>Key</TempSessionKey>
    <KeyLifeTime>Time<KeyLifeTime>
</UserToken>
```

VI. Risk Analysis

The above healthcare environment is proposed as a solution to the privacy and security threats in the electronic and mobile healthcare environments. This section will discuss the possible threats and solutions provided by the protocol defined in this study.

A. User anonymity

Patient's identity is only known by the Healthcare Service Unit which is a trusted organisation by all the users and healthcare service providers. The Healthcare Service Unit authenticates and authorizes patients at the healthcare service

provider with a temporary identification. The patient obtains distinct temporary identification for each service access request to the same healthcare service provider. The temporary identification is a random number and it doesn't have any relationship with the patient's true identification. There are no relationships between temporary identifications thou those are belong to the same patient or those are generated for the same healthcare service provider access. Therefore healthcare service providers are unable to trace back the temporary identity to the real identification of the patient. So the patient's identification is not disclosed to healthcare service providers and third parties who are interested to gather health sensitive information.

B. Message privacy

The patient's health sensitive information and patient's identification are not linked to each other at any parties at the proposed environment. For example the patient's identify is disclosed to the healthcare service unit but it doesn't receive any patient's health sensitive information. Meanwhile the healthcare service providers have access to patient's health sensitive information but they are unable to trace the patient's identity. Therefore the patient's privacy is protected in the proposed healthcare environment.

C. Message confidentiality

A secured confidential communication channel is established between the healthcare service unit and the patient's web browser/mobile device based on the asymmetric/symmetric encryption and the patient uses the secure channel for the authentication with the healthcare service unit. Therefore patient's authentication requests and tokens are protected from eavesdroppers. The communication between the patient and healthcare service providers are protected using the symmetric key encryption technology. Therefore all the patient's sensitive health records are protected from eavesdroppers and patient's privacy is protected.

D. User authentication and authorization

Patient authenticates to the Healthcare Service Unit by providing his/her identification details and password or relevant credentials. Once the authentication process is successful patient can request authorization to healthcare service providers from the healthcare service unit. The user token is generated by healthcare service unit and with the validity of the user token the healthcare service provider authorizes the patient for services.

E. Replay attacks

The authentication and authorization messages generate tokens and those tokens consist of timestamps to prevent replay attacks. An eavesdropper could capture login request message of a previous protocol between a patient and a healthcare service provider. The attacker might later replay that message to try to impersonate the patient to the healthcare service provider. The attack will not succeed if the healthcare service provider validates the timestamp of the request message. These tokens are integrity protected and attackers are unable to alter the timestamps before the attack.

VII. Conclusion

This paper described a medical environment that a patient can access without providing his/her identity. As the number of ageing population and patient's with chronic diseases increases there is an increasing pressure on the national and international healthcare communities to find alternative healthcare solutions to keep the quality of life of these people at the same levels as before. The online and mobile communication technologies have been introduced to health industry as a cost effective, faster, reliable and user-friendly solution. However, since the health sensitive information is transmitted in the network it is vital to protect patient's privacy against misdemeanours activities. The anonymous access control protocol defined in this paper will provide the way forward for secure future online/mobile healthcare systems.

References

[1] Liberty id-ff architecture overview. Technical report, Liberty Alliance, April 2003.

[2] Kalid Elmufti, Dasun Weerasinghe, M Rajarajan, Veselin Rakocevic, and Sanowar Khan. Privacy in mobile web services ehealth. In *Pervasive Health Conference and Workshops, 2006*, November 2006.

[3] Lisa N. Geller, Joseph S. Alper, Paul R. Billings, Carol I. Barash, Jonathan Beckwith, and Marvin R. Natowicz. Individual, family, and societal dimensions of genetic discrimination: A case study analysis. *Science and Engineering Ethics*, 2(1):71–88, 1996.

[4] S. Gritzalis, C. Lambrinoudakis, D. Lekkas, and S. Deftereos. Technical guidelines for enhancing privacy and data protection in modern electronic medical environments. *Information Technology in Biomedicine, IEEE Transactions on*, 9(3), September 2005.

[5] Markus Hillenbrand, Joachim Gotze, Jochen Muller, and Paul Mullar. A Single Sign-On Framework for Web-Services-based Distributed Applications. June 2005.

[6] Y Kakizaki, H Yamamoto, and H Tsuji. A method of an anonymous authentication for flat-rate service. *Journal of Computers)*, 1(8):36 – 42, 2006.

[7] Rafal Leszczyna. The solution for anonymous access of it services and its application to e-health counselling. In *1st 2005 IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS '05)*, September 2005.

[8] Weiss Alan M. Buying prescription drugs on the internet : Promises and pitfalls. *Cleveland Clinic journal of medicine (Clevel. Clin. j. med.)*, 73(3):282 – 288, 2006.

[9] Anelia Mitseva, Mohamad Imine, and Neeli R. Prasad. Context-aware privacy protection with profile management. In *WMASH '06: Proceedings of the 4th international workshop on Wireless mobile applications and services on WLAN hotspots*, pages 53–62, New York, NY, USA, 2006. ACM Press.

[10] Thomas C. Rindfleisch. Privacy, information technology, and health care. *Commun. ACM*, 40(8):92–100, 1997.

[11] Jin Wang and Hongwei Du. Setting up a wireless local area network (wlan) for a healthcare system. *International Journal of Electronic Healthcare*, 1(3):335 – 348, March 2005.

[12] Dasun Weerasinghe, Kalid Elmufti, M Rajarajan, and Veselin Rakocevic. Xml security based access control for healthcare information in mobile environment. In *Pervasive Health Conference and Workshops, 2006*, November 2006.