Device Data Protection in Mobile Healthcare Applications

Dasun Weerasinghe, Muttukrishnan Rajarajan, and Veselin Rakocevic

Mobile Networks Research Group
School of Engineering and Mathematical Sciences
City University London,
Northampton Square, London, EC1V 0HB, UK
dasun.weerasinghe@city.ac.uk

Abstract. The rapid growth in mobile technology makes the delivery of healthcare data and services on mobile phones a reality. However, the healthcare data is very sensitive and has to be protected against unauthorized access. While most of the development work on security of mobile healthcare today focuses on the data encryption and secure authentication in remote servers, protection of data on the mobile device itself has gained very little attention. This paper analyses the requirements and the architecture for a secure mobile capsule, specially designed to protect the data that is already on the device. The capsule is a downloadable software agent with additional functionalities to enable secure external communication with healthcare service providers, network operators and other relevant communication parties.

1 Introduction

The Internet and mobile networks have penetrated the healthcare sector due to their increased functionality, low cost, high reliability and easy-to-use nature. During the recent past, research activities have been focused on achieving portability of medical records, monitoring real-time health status of the patients, and enhancing the concept of online diagnosis and telemedicine. In a broader sense, such healthcare applications can be termed as "m-health". M-health is about an emerging set of applications and services that people can access from their web-enabled mobile devices. Even though the technology makes m-health possible many open issues still exist in the mobile healthcare environment such as security of electronic data transactions, mobile user authentication and secure data storage in a mobile device with protecting privacy. This paper presents a logical architecture for an on-the-phone security agent (a "Security Capsule"). This security agent can, in a single-sign-on mobile healthcare environment, rapidly improve the security by enabling authentication to healthcare service providers and also by protecting the privacy on the data storage on the phone.

The security capsule is owned by a trusted entity and it is securely downloaded and installed into the mobile device. The trusted entity can be a government body, National Health Service in UK or a mobile operator and this paper names

D. Weerasinghe (Ed.): eHealth 2008, LNICST 1, pp. 82–89, 2009.

the trusted entity as the authentication service. It is assumed that the mobile capsule itself is secured but the mobile device is considered to be an un-secured object and the communication between the mobile device and external parties is vulnerable to security attacks. Therefore, the security capsule is invented as a solution to protect sensitive medical data from security vulnerabilities during the transmission and to prevent losing or stealing the medical data stored in mobile devices. In the current mobile device technology, the encrypted sensitive information can be transmitted to a mobile device but decrypted plain information is stored in common storage area of the mobile device. So the sensitive information in a mobile device is vulnerable to un-authorized accesses. The application level password protection can be applied to sensitive information but the data can be retrieved in readable format from the hardware level. Therefore, if the mobile device is lost or stolen then an authorized party can acquire sensitive information from the mobile device. The proposed security capsule stores medical and sensitive data in encrypted format and those are decrypted only when the user wants to view the information. Meanwhile decrypted data is not stored inside the mobile capsule and is viewable to the user over a read-only interface of the mobile capsule. Therefore this data cannot be saved inside the mobile device or transmitted to another mobile user.

A number of publications [5,6,8] describe the use of the healthcare applications from a mobile device. According to the knowledge of authors none of those publications discuss an approach to secure the sensitive data that are stored within a mobile device. Meanwhile there are publications on security mobile agents but those publications fail to address the protection of the data security and privacy using token management systems and release of a read-only interface to the mobile users. In addition to the proposed, the mobile capsule can establish secure communications channels with external service providers and other security capsules. The Java Micro Edition, Symbian C++ and Python are some of the programming languages used to implement agents in mobile devices. Publications [4,11,12] discuss implementations of security mobile agent in Java and Telescript with addressing some of the existing security issues. In [2] Borselius discussed some security features and properties of agents and multi-agent systems. Picco in [9] presented evidence of benefits a mobile agent can potentially achieve and he illustrated architectural foundation for a mobile agent.

In addition to the data protection, the security capsule needs to provide at least two more functions: (1) to enable secure authentication to remote communication parties and (2) to enable secure encrypted communication channels from the mobile device to the remote communication parties. The security capsule authenticates and authorizes itself with the authentication service and the service providers before establishing any data transmission communications. The trust needs to be negotiated and established between the requestor party and the relying party through the capsule before sharing any sensitive information. The trust and authentication information is exchanged using security tokens. The security capsule will acquire security tokens from authentication service and healthcare service providers after each successful authentication, authorization or trust negotiation process. Following this, the data encryption is achieved through the message level security protection using XML security features for data transmission. The required secure protocols for this are defined in some of our previous publications [13,14].

This paper presents the case for the security capsule and identifies the main requirements for the provision of the three main functions of the capsule: data protection on the device, secure authentication and data encryption. These three functions provide the necessary privacy and security for m-health application users. The rest of the paper is organized as follows. Section 2 presents the standard m-health communication architecture, identifies the main actors and their relationships. Sections 3 and 4 describe the logical architecture of the security capsule and the requirements for its most important units.

2 Mobile Healthcare Architecture

We observe an m-health architecture with three types of main actors; a mobile device with a secure capsule, authentication service and service provider as shown in figure 1. The patient or service provider staff with the mobile device accesses the services via a bandwidth-constrained mobile station, comprising the mobile device and the service-enabling SIM card connected to a mobile operator over the UMTS network. The authentication service is connected to the registered service providers such as healthcare service provider, private medical centre or insurance service providers to provide healthcare services to patients.

The mobile device authenticates with the authentication service by using credentials that are stored within the mobile capsule and SIM credentials at the mobile operator. Once successfully authenticated with the authentication service, the staff/patient with a mobile device can request access to the services at service providers. The authentication and authorization links between the mobile user and service providers are established based on Single-Sign-On [7] technology

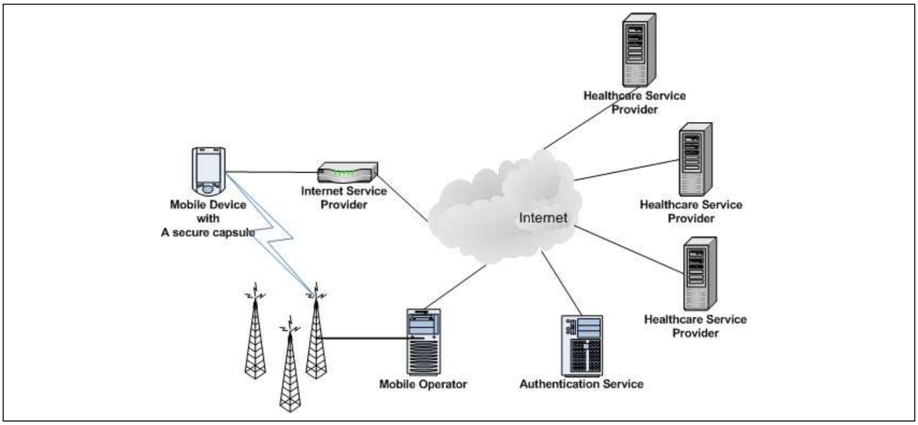
Healthcare Service Provider
Mobile Device with A secure capsule
Internet Service Provider
Internet
Healthcare Service Provider
Healthcare Service Provider
Mobile Operator
Authentication Service

Fig. 1. Mobile Healthcare Architecture

at the authentication service. Services and information sharing between a service provider staff and a relying service provider in distinguish security realms takes place after a trust negation between two service providers. The implementation of all the service providers and the authentication service are based on the Service Oriented Architecture [1,3]. Service providers communicate with the patient and the mobile operator using the Hypertext Transfer Protocol [10]. The message flow uses the latest XML encryption, XML signature and XML Key Management technologies that are much faster and consume less power for secure mobile applications.

3 Security Capsule Architecture

The logical architecture of the security capsule consists of storage and security units to preserve the data and message security. Figure 2 presents the main components, interfaces and the information flow in the security capsule.

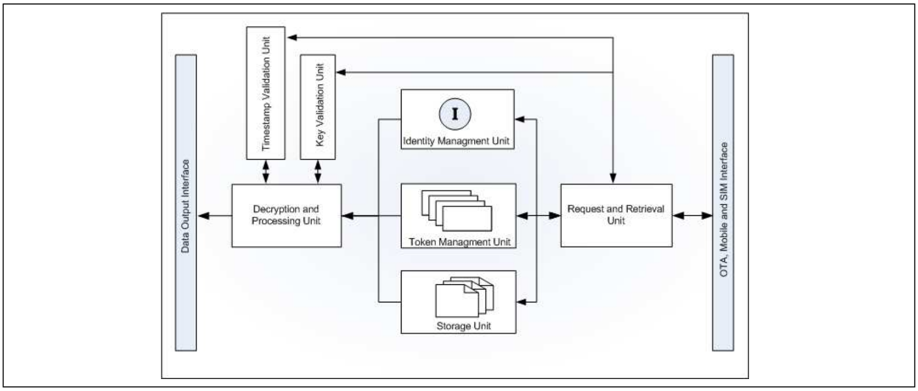
Data Output Interface
Timestamp Validation Unit
Key Validation Unit
I
Identity Managment Unit
Decryption and Processing Unit
Token Managment Unit
Request and Retrieval Unit
Storage Unit
OTA, Mobile and SIM Interface

Fig. 2. Security Capsule Architecture

Request and Retrieval unit establishes communication links with authentication providers, service providers, SIM/USIM and the mobile device over an interface. This interface is named as OTA, Mobile and SIM (OMS) interface and it supports connections to third party web services and OMS interfaces of other mobile capsules. Income data flow consists of identity objects, tokens and encrypted data and the data flow is respectively distributed to Identity Management Unit, Token Management Unit and Storage Unit. The Decryption and Processing Unit decrypts encrypted data and the input flows are shown in figure 1. This unit outputs the decrypted information over the data output interface to the mobile user. The security capsule provides read-only and un-savable interface to the mobile device and this data cant be saved in the mobile device or transmitted to another mobile device.

3.1 Request and Retrieval Unit

This is the communication unit of the security capsule and this unit establishes secure communication links with service providers and authentication services over XML messages or web service invokes. Meanwhile communication between two secure mobile capsules is established by the request and retrieval unit. This unit validates incoming data flow and protects out going data flow using XML security features [13].

3.2 Identity Management Unit

The security capsule acquires an identification object from the authentication service during the download and registration phase. This identification object is used as a security credential for authentication and authorization with authentication service. Meanwhile service providers from different realms should authenticate and authorize the mobile capsule before disclosing any services. The service provider issues an identification object to the mobile capsule after a successful authentication and authorization to services. These identification objects are named as service provider identification objects and those are saved and managed by the Identity Management Unit. Meanwhile public key infrastructure (PKI) information of the mobile capsule is saved with the Identity Management Unit.

3.3 Token Management Unit

Various types of tokens are utilized during the communications between the mobile capsule and the service providers such as registration, authorization, authentication and trust tokens. Format and the structure of these tokens are discussed in the token management section. These tokens grant authority to the mobile capsule to acquire services and data from service providers. The decryption and processing unit doesn't process encrypted data unless the valid token is present for the encrypted content. Tokens and encrypted data are sent to the mobile device at two different instances and the capsule save those tokens in the Token Management Unit. Tokens are indexed in the Token Management Unit with reference to the service provider identity and timestamp. It provides tokens to the Decryption and Processing Unit for data decryption process. Meanwhile tokens are expired after the specified token lifetime. The expired tokens are automatically achieved or deleted to save the storage space and the processing power of the mobile device.

3.4 Storage Unit

Encrypted data from service provider are saved in the storage unit of the mobile capsule. These encrypted data are indexed with service provider id and those are automatically deleted or archived after the decryption to save the storage space of the mobile device.

3.5 Decryption and Processing Unit

This is one of the main units in the security capsule. This unit represents a decryption algorithm to decrypt encrypted data from service providers. Each encrypted data is linked with one or more security tokens to prove the mobile capsule's authorization to decrypt the encrypted data. Therefore Decryption and Processing Unit is linked with the Token management unit to fetch the necessary tokens for the decryption process. The token generated timestamp and the token lifetime are concatenated to each token. This algorithm verifies the freshness of the tokens and encrypted data before decryption. Present timestamp is acquired using the Time Stamp Validation unit. Tokens and encrypted data are signed by the secrete keys to protected the integrity. The public key certificates and other key information are retrieved over the Key Validation Unit. The decrypted data is transferred through the data output interface to the mobile device. The output of the interface is in read-only format and decrypted data is not saved with in security capsule at any instance. The decrypted information can't be saved within the mobile device or can't be transmitted to outside the mobile device since the Data Output interface provides and read-only and un-savable interface.

4 Token Management

Different types of tokens are utilized in this proposed mobile security capsule and these tokens provide authorization to successful data decryption. Tokens are issued by authentication service and service providers to register and authenticate the mobile user to use sensitive data and services. The token management unit is one of the main functional units in the mobile security capsule since it stores and manages these tokens. These tokens basically consist of issuer's identification, token identification, session key information, timestamp and token lifetime. The token will be deleted or archived after the token life time is expired. However token management unit can request for a new token from the service provider for expired tokens. All the tokens are constructed in XML format and tokens are integrity protected by signing the contents using the issuer's private key. Meanwhile token is encrypted to protect the confidentiality using a session key or the public key of the mobile capsule. Following sub sections describe some of the tokens in the token management unit with their XML structures. The below abbreviations are used for token representation.

- SMC = Secure Mobile Capsule;
- SP= Service Provider
- AS = Authentication Service
- TS = Time stamp
- tsK = Session Key
- s_{N_K}(X) = The signature of data X using secret key K of entity N
- e_{N_K}(X) = The encryption of data X using public key K of entity N

4.1 Registration Token

(RT=$e_{MSC_{public}}(s_{AS_{private}}$[UID||Lifetime||TS])) The registration token is used by the authentication service to identify and authenticate legitimate mobile devices before establishing communications with service providers. The registration token is issued by the authentication service during the download and installation phase of the security capsule. The security capsule should have a valid registration token for communication. The mobile security capsule sends the registration token to authentication service and the authentication service verifies it before disclosing access service providers. This token belongs to the authentication service and this verified by the authentication service. Therefore the token is signed by the private key of the authentication service and encrypted using the public key/session key of the security capsule.

4.2 Authorization Token

(AT=$e_{MSC_{public}}(s_{AS_{private}}$[UID||SID||tsK||KeyLifetime||Lifetime||TS])) The authorization token is used to authorize the mobile device to access services from the service provider. This token is issued by the service provider and it consists of user identity, session identity, time stamp and session key and key life time. The authorization token is signed by the service provider private key to protect the data integrity and the token is encrypted using the public key of the mobile security capsule. Authorization tokens are linked with the encrypted data from service providers and a valid token has to be present for a successful data decryption.

4.3 Trust Token

(TT=$e_{MSC_{public}}(s_{SP_{private}}$[TTID||SPID||ALT||Lifetime||tsK||TS]))The trust token can be considered as the trust agreement between the mobile device and the service provider. The trust tokens are generated using some trust evaluation algorithms in the trust federated environment by service providers or authentication service. The trust token represents the trust acquired by the mobile user to view some sensitive data from a service provider. The service provider generates the trust level which is named as assigned trust level (ATL) and it is concatenated to the trust token. This token should be presented to Decryption and Processing unit for data decryption functionality. The trust token is singed by service provider private key and the confidentiality is protected by encrypting the token by the public key of the mobile security capsule. The trust token will expire after the token lifetime and the Trust Management Unit can request a new trust token from the service provider.

5 Conclusion

The mobile communication technologies have been introduced to health industry as a cost effective, faster, reliable and user-friendly solution. Since health sensitive information is transmitted in the network it is vital to protect patient's privacy against misdemeanours activities. This paper proposes a security capsule with token management architecture to enable the secure transmission and storage in a mobile device.

References

1. Beznosova, K., Flinnb, D.J., Kawamotoc, S., Hartmand, B.: Introduction to web services and their security. Information Security Technical Report 10(1), 2–14 (2005)
2. Borselius, N.: Mobile agent security. Electronics & Communication Engineering Journal 14(5), 211–218 (2002)
3. Damiani, E., De Capitani di Vimercati, S., Samarati, P.: Towards securing xml web services. In: XMLSEC 2002: Proceedings of the 2002 ACM workshop on XML security, pp. 90–96. ACM, New York (2002)
4. Dean, D., Felten, E.W., Wallach, D.S.: Java security: from HotJava to Netscape and beyond. In: IEEE (ed.) 1996 IEEE Symposium on Security and Privacy, Oakland, California, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, May 6-8, 1996, pp. 190–200. IEEE Computer Society Press, Los Alamitos (1996)
5. Dwivedi, A., Wickramasinghe, N., Bali, R.K., Naguib, R.N.G., Goldberg, S.: Critical success factors for achieving superior m-health success. International Journal of Electronic Healthcare 3(2), 261–278 (2007)
6. Istepanian, R.S.H., Jovanov, E., Zhang, Y.T.: Guest editorial introduction to the special section on m-health: Beyond seamless mobility and global wireless health- care connectivity. IEEE Transactions on Information Technology in Biomedicine 8(4), 405–414 (2004)
7. Hillenbrand, J.M.M., Gotze, J., Mullar, P.: A Single- Sign-On Framework forWeb-Services-based Distributed Applications. In: Proceedings of the 8th International Conference on Telecommunications, 2005. ConTEL 2005, vol. (1), pp. 273–279 (2005)
8. Moran, E.B., Tentori, M., Gonzalez, V.M., Favela, J., Martinez-Garcia, A.I.: Mobility in hospital work: towards a pervasive computing hospital environment. Intl. J. Electronic Healthcare 3(7), 72–89 (2007)
9. Picco, P.: Mobile agents: an introduction. Microprocessors and Microsystems 25(2), 65–74 (2001)
10. Sun Microsystems, Wireless Toolkit, Version 2.1 (2003), `http://java.sun.com/products`
11. Tardo, J., Valente, L.: Mobile agent security and Telescript. In: IEEE CompCon 1996, pp. 58–63 (1996)
12. Varadharajan, V.: Security enhanced mobile agents. In: CCS 2000: Proceedings of the 7th ACM conference on Computer and communications security, pp. 200–209. ACM Press, New York (2000)
13. Weerasinghe, D., Elmufti, K., Rajarajan, M., Rakocevic, V.: Securing electronic health records with novel mobile encryption schemes. International Journal of Electronic Healthcare 3(4), 395–416 (2007)
14. Weerasinghe, D., Rajarajan, M., Elmufti, K., Rakocevic, V.: Patient privacy protection using anonymous access control techniques. Methods of Information in Medicine 47(3), 235–240 (2008)