Security Protection on Trust Delegated Data in Public Mobile Networks

Dasun Weerasinghe, Muttukrishnan Rajarajan, and Veselin Rakocevic

School of Engineering and Mathematical Sciences
City University London
dasun.weerasinghe@city.ac.uk

Abstract. This paper provides detailed solutions for trust delegation and security protection for medical records in public mobile communication networks. The solutions presented in this paper enable the development of software for mobile devices that can be used by emergency medical units in urgent need of sensitive personal information about unconscious patients. In today's world, technical improvements in mobile communication systems mean that users can expect to have access to data at any time regardless of their location. This paper presents a token-based procedure for the data security at a mobile device and delegation of trust between a requesting mobile unit and secure medical data storage. The data security at the mobile device is enabled using identity based key generation methodology.

1 Introduction

In the modern world people are getting used to have access to a wide range of data and applications wherever they are and whenever they want, using public mobile communication networks. In such a ubiquitous communication environment, it is not a surprise that there is a growing need to enable the emergency medical teams to have a continuous and secure access to patient medical records. The added benefit of having person's medical record while providing emergency care is obvious, and has been highlighted in a number of publications [1][7][6].

This paper provides a detailed analysis of the above issues and provides solutions for secure authentication of data download and data protection following the download. In this respect, the first issue that requires attention is the secure authentication. This is achieved by careful distribution of trust between the key players in the process: the medical provider storing the medical records, the mobile network, and the mobile device requesting the data. Trust had to be negotiated and delegated between these players to enable them to feel confident to exchange data. The authors have presented the trust negotiation methodology in one of their previous publications[10].

With the emergence of electronic health solutions, the delegation and negotiation of trust from one healthcare service provider (HSP) to another is one of the main requirements for the secure provision of data and services [9]. The healthcare service providers can "in the extreme case" be mutually unknown and therefore not trusting each other. In our paper, the HSPs are classified in two categories; the 'relying healthcare service provider' and the 'requesting healthcare service provider'. The relying HSP is a medical

P. Kostkova (Ed.): eHealth 2009, LNICST 27, pp. 200–207, 2010.

center or a hospital which stores sensitive patient medical records - including patient's medical history, current diagnosis and medical treatments, known allergies, social history of the patient and patient personal information. The patients have the ownership of the patient medical records but they have granted the trust delegation on accessing these records to their HSP [8]. The requesting HSP is another medical center, hospital or mobile healthcare service unit with doctors and/or paramedics. This HSP requests access to patient medical records from the relying HSP in order to perform special or urgent diagnosis and medical treatment to patients. The access to the patient medical record is vital for a doctor at the requesting HSP to perform a correct diagnosis and/or treatment. This paper provides a detailed solution for securing this scenario.

2 Trust Negotiation in Mobile Services

During the recent past, initiatives have been taken both by the academia and by the industries towards improving the use of mobile communication for healthcare and safety of the public [4]. The m-health is an existing term representing an emerging set of healthcare applications and services that people can access from their web-enabled mobile devices [2]. Medical personnel having access to clinical data irrespective of the geographic location is an advantage of m-health. There are numerous examples of interesting applications. For example, real-time mobile telemedicine system is introduced to transmit video and patient bio-signals from a moving ambulance to a doctor in the hospital using wireless cellular phones [12]. Mobile device in the ambulance is connected to a Web service in the hospital to retrieve advices about transferring the patient there [5]. These approaches allow medical personnel to access patient medical records from a remote location but only if the patient medical records are at a centralized or distributed location for public access. Generally patient medical records are stored at patient's medical center and access to those records are restricted to protect the data confidentiality and patient privacy. Therefore mobile medical personnel at the disaster scene has to prove the legitimacy to access patient medical records from the patient's medical center [8].

A trust negotiation process should incorporate a trust negation algorithm to identify, verify and validate the trust level of the requestor party with respect to the requesting information. There are number of trust negotiation algorithms available and our framework will be able to use any of those to generate the trust level between the requestor party and relying party. Wu Z. et al describes an indirect trust establishment mechanism to bridge and build new trust relationships from extant trust relationships [11]. The trust evaluation algorithms output a trust level defined in the rage of Full to Minimal such as Full, High, Medium, Low, Minimal or the rage is in numerical numbers such as 1 to 10 [3].

Transferring trust delegation for accessing patient medical records between healthcare service providers is one of the vital requirements in healthcare industry and specially accessing patient medical records over a mobile device in emergency situations. According to the knowledge of authors most publications haven't considered the security and privacy aspects in trust negotiation techniques for mobile healthcare environment. Therefore the novelty and the research contribution of this paper compared to the other publications is; 'Token based trust negotiation and delegation framework for healthcare service providers with a security and privacy protection on trust delegated data'.

3 Proposed Schema

The solution for trust negotiation in mobile web services is designed using the token based trust negotiation framework. The TGS is the facilitator for the trust negotiation between healthcare service providers. It generates and issues tokens for authentication and trust negotiation process. These tokens are designed in XML format and those are categorized into security tokens and trust tokens. The mobile device is unlikely to be trusted by the schema but the security capsule is a trusted entity. So patient medical records and obtained tokens are stored in the security capsule. The patient medical records are stored in the encrypted format and security capsule can decrypt those only if valid security and trust tokens are present.

The use case for trust delegation on patient medical records begins when MHP attempts to access patient medical record from a healthcare service provider. The patient medical records are saved at the relying healthcare service provider and TGS bridges the trust negotiation between two parties. The scheme for transferring trust delegation to access patient medical records is summarized with the reference to Figure 1.

1. The MHP authenticates with TGS to access patient medical records. The TGS issues the security token to the MHP's mobile device
2. The MHP requests the access to patient medical record from TGS by specifying the patient identity
3. The TGS locates the relying healthcare service provider for the patient medical records and sends the trust negotiation request
4. The patient medical record and trust tokens are sent to the mobile device of MHP from the patient's healthcare service provider
5. The mobile device decrypts the patient medical records utilizing the tokens records.

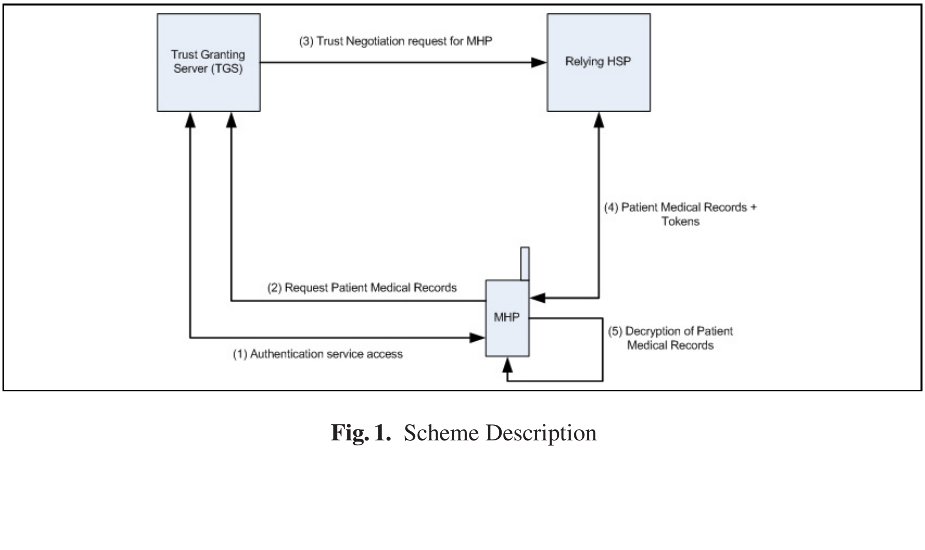
Trust Granting Server (TGS)
(3) Trust Negotiation request for MHP
Relying HSP
(4) Patient Medical Records + Tokens
(2) Request Patient Medical Records
MHP
(5) Decryption of Patient Medical Records
(1) Authentication service access

Fig. 1. Scheme Description

4 Implementation

The paper presents both specific protocol exchanges and the structure and syntax of security and trust tokens.

4.1 Protocol

This section describes the critical protocol exchanges to address the threat model with the consideration of authentication, confidentiality and integrity. The protocol consists of 2 phases:

1. MHP authenticates with TGS
2. Trust negotiation between relying healthcare service provider and MHP

The following additional notations are adapted for the protocol explanation:

- RelHSP= Relying healthcare service provider
- ReqHSP= Requesting healthcare service provider

Phase 1: MHP authenticates with the TGS
Phase 1 initiates with MHP going to a disaster scene. The mobile device of MHP had the Login Token that was generated by the healthcare service provider. Following are the steps to get the MHP authenticated with the TGS:

1. MHP to TGS [Login Token]; The login token is the authentication request to the TGS from MHP. The token consists of information about the healthcare service provider and mobile healthcare personal.
2. The TGS decrypts the message using its private key and verifies the signature of the token against the public key certificate of ReqHSP. If the verification is successful then the ReqHSP and MHP identification are checked in the Trust Mapping Database.
3. TGS to MHP [Authentication Token]; Once the trust level is obtained, the TGS generates the Authentication Token for MHP.

Phase 2: Trust Negotiation between MHP and Relying Healthcare Service provider
Phase 2 startes with MHP approaching a patient at a disaster situation. The patient needs urgent medical attention and MHP has to view the patient medical records for effective treatments. It is assumed that MHP has found an identification of the patient.

Following are the steps on trust negotiation between the healthcare service provider and the MHP:

1. MHP to TGS: [RecordAccess(PatientID, Authentication Token)]; The MHP identifies the patient and makes the request to access patient medical records.
2. The TGS verifies the authentication token and then identifies the relying healthcare service provider (RelHSP) of the patient. The RelHSP holds the patient medical records. Then TGS locates the previous trust negotiation and trust decline records between the requesting parties (MHP and ReqHSP) and the relying party (RelHSP) in the trust mapping database. The Trust Evaluation Engine generates the recommended trust level for MHP to access patient medical records from RelHSP.

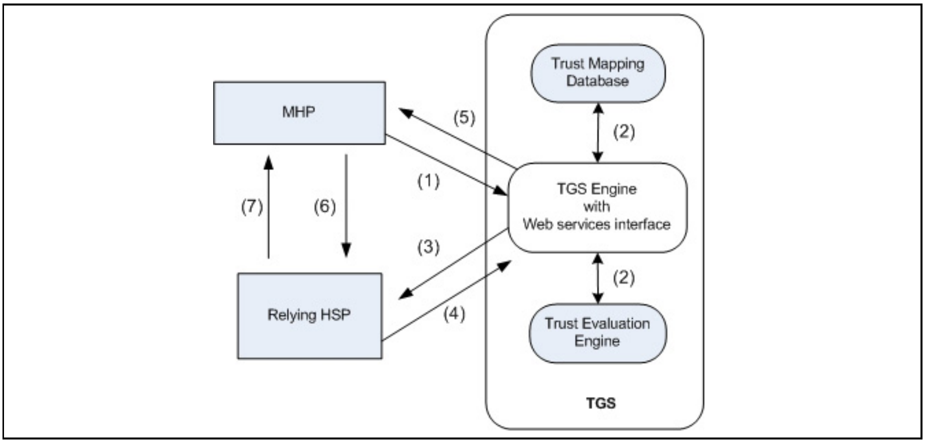

Fig. 2. Phase 2 message flow

3. TGS to RelHSP [TrustRecommendation Token]; The Trust Recommendation Token is generated by the TGS.
4. RelHSP to TGS [TrustChallenge, Confirmation, Assigned Trust Level]; The RelHSP verifies the Trust Recommendation Token against the TGS signature and obtains the information about the requesting party and patient identification. The finalized trust level for MHP is named as ’Assigned Trust Level’ and then the trust challenge token is generated by RelHSP.
5. TGS to MHP [TrustChallenge Token]. The TGS sends the Trust Challenge Token to the MHP.
6. MHP to RelHSP [TrustChallengeResponse]. The MHP retrieves the RAND from the trust challenge token and generates the trust challenge response using its private key for integrity.
7. RelHSP to MHP [Trust Token]. The RelHSP validates the trust challenge response against the RAND and public key certificate of MHP. If the validation is successful then the Trust Token is generated as trust delegation object.

Finally the RelHSP encrypts the patient medical records using the session key of the trust token and transmits it to the MHP. The data is signed by the RelHSP private key for integrity and encrypted by the MHP public key for confidentiality.

4.2 Token Generation and Management

This section describes the token structures for the proposed schemas and the below abbreviations are used for token representation.

$$\begin{aligned} TS &= \text{Time stamp} \\ s_{N_K}(\text{X}) &= \text{The signature of data X using secret key K of N} \\ e_{N_K}(\text{X}) &= \text{The encryption of data X using secret key K of N} \end{aligned}$$

- Authentication Token (AT)
  (AT = $e_{TGS_{S1}}(s_{TGS_{S2}}$[ReqHSPID | MHPID | GTL | Token Life Time | TS]));
  The Authentication Token is issues by the TGS for authenticated mobile healthcare personals. This token is belonged to the TGS and this can only be viewed and verified by the TGS. Therefore the token is signed by TGS integrity key (TGS2) and then encrypted by the confidentiality key of TGS (TGS1). This token specifies the General Trust Level (GTL) of the MHP.

- Trust Token(TT)
  (TT = $e_{MHP_{public}}(s_{RelHSP_{private}}$[TTID | MHPID | ATL | PatientID | Token Life Time | TS | tsK]));
  The trust token is the trust granted object for MHP to access the requested patient medical record. The trust token identification (TTID) is assigned to each trust token for unique identification. The tsK is the session key is used to decrypt the encrypted patient medical records.

4.3 Security Capsule Implementation

The security capsule has been developed to enable security of the healthcare data in a mobile device and it is a application for a mobile device that can be installed using OTA technique. The patient medical records are sent to the mobile device in encrypted format and the encrypted data is saved in the security capsule. The data decryption and protect the security and privacy on patient medical records are the main functionalities of it.

The logical architecture of the security capsule consists of six functional and storage units as shown in Figure 3. The Service Manager establishes Web services communication with the Trust Granting Server and Healthcare Service providers. It establishes the communication with the external parties. Meanwhile it communicates with the mobile device display API and data storage units. The Data Manager, Token Manager and Key Manager maintain storage spaces respectively for encrypted data, tokens and cryptographic keys. The Service Manager filters the incoming data stream and then dispatch it to the correct storage area. The incoming encrypted medical records from the service providers are decrypted by the process manager.

The data decryption process executes when the mobile personal requests to view the data from the mobile device. Then the Process Manager retrieves the encrypted data from the Data Manager and the relevant tokens from the Token Manager storage. The token validation and public key certificate validation functions are performed to verify the legitimacy of the tokens and cryptographic keys. Finally the Process Manager generates the decryption key and then decrypts the encrypted data. The decrypted data is displayed in the mobile device through the Service Manager and after the session the decrypted data and cryptographic keys are sent to the Data Dump Manager. The Data Dump Manger discards used data, tokens and keys from the device and USIM memory. The decryption key generation process and the permanent data deletion process in the security capsule protect the patient medical records from privacy and security vulnerabilities.

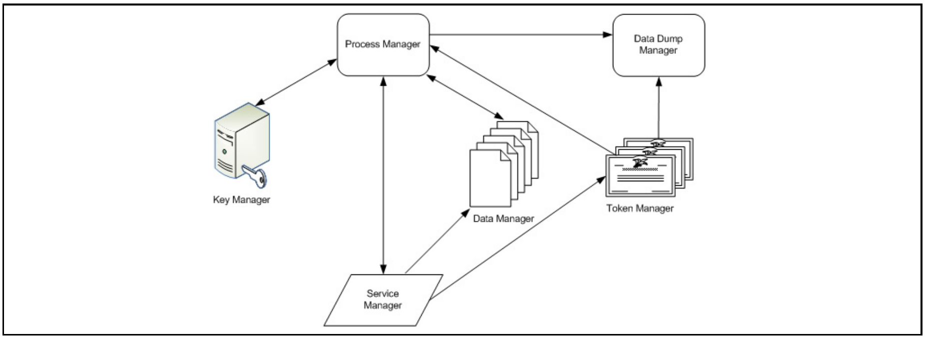

Fig. 3. Security Capsule Architecture

The novel key generation algorithm in the Process Manger generates the data key to decrypt encrypted patient medical records from the service providers. Following are the input types for the key generation algorithm.

- User PIN: 4 digit PIN agreed between mobile healthcare personal and the healthcare service provider
- IMPI (IP Multimedia Private Identity): The mobile operator assigned identity for the mobile healthcare personal with the USIM
- IMEI (International Mobile Equipment Identity): The unique identity for the mobile device and this is issued by the mobile device manufacturer.
- UID: The Identity provider issued unique identity for the security capsule
- Token Key: The cryptographic key in the token that provides mobile device authentication to the decrypt data
- Vendor Key: the cryptographic key is sent by the healthcare service provider during the decryption process. This key provides a real time authentication of the mobile healthcare personal with the User PIN.

Therefore the mobile device dependent, mobile SIM dependent, Mobile personal dependent, TGS dependent and the Healthcare service provider dependent identification parameters are required in the key generation process. This will protect transmitting patient medical records to other mobile devices or stealing mobile devices to access sensitive data inside.

5 Conclusion

The paper has introduced a scheme for the trust negotiation between healthcare service providers to retrieve and access patient medical records using mobile devices during an emergency scene. The main contribution of the paper can be summarized as; ’Trust negotiation and data protection at a mobile device’. The contribution of system architecture, scheme and protocol will form a new business model for healthcare industry to efficiently and securely share data and services between unknown healthcare service providers.

References

1. Belsis, M.A.: Dwivedi A.N. Providing secure maccess to medical information. Int. J. Electronic Healthcare 3(1), 51–57 (2007)
2. 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)
3. Jung, D.I., Avolio, B.J.: Opening the black box: an experimental investigation of the mediating effects of trust and value congruence on transformational and transactional leadership. Journal of Organizational Behavior 21(8), 949–964 (2000)
4. Moran, E.B., Tentori, M., Gonzalez, V.M., Favela, J., Martinez-Garcia, A.I.: Mobility in hospital work: towards a pervasive computing hospital environment. International Journal of Electronic Healthcare 3(1), 72–89 (2007)
5. Motta, E., Domingue, J., Cabral, L., Gaspari, M.: Irs-ii: A framework and infrastructure for semantic web services. In: Fensel, D., Sycara, K., Mylopoulos, J. (eds.) ISWC 2003. LNCS, vol. 2870, pp. 306–318. Springer, Heidelberg (2003)
6. Mu, M.A., Rodrguez, M., Favela, J., Martinez-Garcia, A.I., Gonzlez, V.M.: Context-aware mobile communication in hospitals. Computer 36(9), 38–46 (2003)
7. Rodriguez, M.D., Favela, J., Martinez, E.A., Munoz, M.A.: Location-aware access to hospital information and services. IEEE Transactions on Information Technology in Biomedicine 8(4), 448–455 (2004)
8. Schoenberg, R., Safran, C.: Internet based repository of medical records that retains patient confidentiality. British Med. J. 321, 1199–1203 (2000)
9. Vawdrey, D.K., Sundelin, T.L., Seamons, K.E., Knutson, C.D.: Trust negotiation for authentication and authorization in healthcare information systems. In: Proceedings of the 25th Annual International Conference of the IEEE (September 2003)
10. Weerasinghe, D., Rajarajan, M., Rakocevic, V.: Trust delegation for medical records access using public mobile networks. In: Proceedings of the 3rd International Conference on Pervasive Computing Technologies for Healthcare (April 2009)
11. Wu, Z., Weaver, A.C.: Bridging trust relationships with web service enhancements. In: ICWS 2006: Proceedings of the IEEE International Conference on Web Services, pp. 163–169 (2006)
12. Xiao, Y., Gagliano, D., LaMonte, M., Hu, P., Gaasch, W., Gunawadane, R., Mackenzie, C.: Design and evaluation of a real-time mobile telemedicine system for ambulance transport. J. High Speed Netw. 9(1), 47–56 (2000)