Parameter Based Access Control Model for Mobile Handsets

Dasun Weerasinghe, Raj Muttukrishnan, 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 concept of mobile services is to provide the access to online content and services from anywhere, anytime and on any device. The mobile user is the consumer for the mobile services and the access to the services are enabled according to the user identification. Meanwhile, mobile device identity, SIM identity and location identity are some of the other identification parameters can be used by mobile service providers. The data and the services are delivered to the mobile device in encrypted format and the cryptographic key for the data decryption is derived using the identity parameters and key materials at the mobile. Therefore, the decryption key is not transmitted over the network and it is generated in the device before the service access. The generation of the decryption key in the mobile using the identity and attribute parameters will enable parameter based access control for mobile content. The data access rules are defined by service providers based on the availability of attributes and identities at the mobile handset.

Keywords: Parameter based Access Control, Security, Privacy, Mobile Devices.

1 Introduction

The security capsule [1] was introduced as a novel component to implement the security mechanisms in a mobile device and it enables secure consumption of mobile services in a mobile device. The security capsule is developed, deployed and distributed by the identity provider and it is assumed the identity provider is a trusted entity [2]. Therefore, the security capsule is considered as a trusted component in the mobile device. The Identity provider framework for mobile devices is presented in one of our previous publications [2]. The data and services in the mobile service environment are vulnerable to various security attacks during the distribution, consumption and storage phases. The security capsule is implemented to protect the data and services at the mobile handset and security protection for data distribution.

The security capsule establishes the mobile device communication with the identity provider and service providers. The service providers uniquely identify the mobile device for authentication and authorization to services. The unique identity is derived in the security capsule using the logical and physical identity parameters at the mobile

D. Weerasinghe (Ed.): ISDF 2009, LNICST 41, pp. 66–75, 2010.

device. The data and services are transmitted to the mobile device in encrypted format from the service providers. Meanwhile, a token is generated by the service provider and it is sent to the mobile device with the encrypted content. This token presents the mobile user's authorization to decrypt the encrypted content.

The service provider generates a unique token for each encrypted data item sent to the mobile device and each token is identified by its unique identity. Meanwhile, the token consists of a symmetric cryptographic key to derive the decryption key for the encrypted data. This decryption key is named as the data key and the key is generated in the mobile device with a number of static and dynamic input parameters. The parameter based key generation function enables the parameters based access control in a mobile handset. Meanwhile, the service provider controls the data access mechanism in real-time basis as the mobile handset requires a real-time cryptographic key for the data key generation process. The real-time key is sent to the mobile device during the decryption process.

The data key is generated in the mobile device rather than transmitting over the network from an external party. The key is generated using the mobile user dependent, the device dependent, the USIM dependent, the security capsule dependent, the service provider dependent and the token dependent parameters. The security capsule permanently deletes the decrypted data, cryptographic keys and tokens after the data access session by the mobile user. However, still encrypted keys and tokens are in the mobile device and only the real-time key has to be requested for data decryption process. The following are the identities are identified in the mobile device for the key generation process.

- IMPI (IP Multimedia Private Identity): The mobile operator assigned identity for the mobile user. This identity is stored in the USIM of the mobile device.
- 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.

2 Related Work

Online mobile applications for mobile devices have introduced new security and privacy risks beyond those that are found in online desktop systems. The articles [3] [4] discuss the security and privacy vulnerabilities on personalized data in mobile devices. The technical report from Perelson S. et al [5] investigates the data access control on mobile devices. They claimed that mobile manufacturers have spent most of their efforts designing security routines for the communication protocols rather than for the data and applications in mobile devices. Therefore, data security on mobile devices should have high priority in the future. An author [6] from IBM Global services presented the same view about security mechanisms in mobile devices. He emphasised that today's challenge is to implement resource intensive security measures on mobile devices.

The security key management in a mobile device has been a top research topic due to the requirements of end-to-end security infrastructure for the mobile service environment. The key exchange schema in [7] allows mobile devices to dynamically agree on session keys with a server. Meanwhile the mobile device is able to perform public key computations in this schema. However, Dodis et al. [8] highlighted threats to cryptography when installing a private key in a device and especially when a user carries the mobile device which allows remote access from public or foreign domains. It recommended having a key as an output from a combination of different types of physical and logical cryptographic inputs. In public key infrastructure, the private key has to be distributed to the mobile device to use asymmetric key encryption technology. However, the publication [9] emphasized the drawbacks in transmitting the private key to a remote device even though the key is encrypted before transmission. However, the mobile device is able to validate public key certificates of service providers before starting any sensitive communication. The publications [10] [11] proposed light weight public key certificate evaluation techniques for mobile devices.

The article [12] emphasized the importance of mobile user authentication without exposing passwords on the network as a future approach. The authors of that article also suggested generating secret encryption keys in mobile devices and then sharing them with the mutually trusted parties. Storing the cryptographic keys in mobile devices is an open research question. Dodis Y. et al [13] proposed a key insulated security approach to protect cryptographic keys in mobile devices. Transmitting long term secrets between entities is vulnerable to the credential sniffing attacks and replay attacks [14].

3 Security Design

This section discusses the functional design of the security capsule to enable the parameter based access control in a mobile device. The design is categorized into the registration process, data transmission and the data access processes. During the registration, the security capsule registers with the identity provider and the service providers. The security capsule consists of identities and credentials for the secure communication with external parties. A secret key is generated at the service provider for the data encryption and then the encrypted data is transmitted to the service provider. The same secret key is generated at the mobile device for the data decryption and it is an output from the identity parameters and the attributes at the mobile device. The successful secret key generation enables the mobile user to access data from the service provider.

As a pre-requisite to the security capsule installation at the mobile device, the identity provider and service providers should agree to a publicly available hash function and a symmetric key encryption algorithm.

3.1 Registration Process

The registration process categorizes into two phases such as registration with the identity provider and the registration with the service provider.

Phase 1: Registration with the Identity Provider

This phase starts when the mobile device requests to download the security capsule from the identity provider. The security capsule will be downloaded using the over-the-air or the wired techniques. The following are the main steps in the registration process.

(1) The mobile device requests to download security capsule from the identity provider.

(2) The security capsule is downloaded to the mobile device.

(3) The mobile user verifies the authentication of the identity provider and the integrity of the downloaded security capsule using the following steps;
   - The public key certificate of the identity provider is used to authenticate the identity provider.
   - The calculated hash value of the security capsule binary installation is compared with the hash value at the identity provider for the security capsule integrity.

(4) The security capsule is installed in to the mobile device as a mobile application. The downloaded security capsule is uniquely identified using the UID. The UID is saved in the security capsule compilation and it will be used to present the security capsule identification to the identity provider during the future communications. The UID is an alphanumeric value in the security capsule and it is un-accessible to the device users.

(5) The security capsule accesses the IMPI and IMEI values from the mobile device and it generates the K_{IMPI} and K_{IMEI} using the inbuilt hash function.

$$HASH\ (\ IMPI\ ) = K_{IMPI}$$
$$HASH\ (\ IMEI\ ) = K_{IMEI}$$

(6) The K_{IMPI} and the K_{IMEI} are transmitted to the identity provider by encrypting them using the identity provider's public key.

(7) The identity provider records the $_{KIMPI}$ and $_{KIMEI}$ values with the UID of the security capsule.

Phase 2: Registration with the Service provider

The security capsule registers with the service provider for services during this phase and the following are the pre-requisites for the registration.

(1) The mobile user should have a unique identification with the service provider.

(2) The mobile device authenticates with the identity provider and both parties share a secret key (Ks) for the communication.

(3) The identity provider and the service provider share a secure communication channel and Service Provider has a Public Key Infrastructure.
Let's assume that SPUID is the mobile user identity at the service provider.

The following are the steps in the registration process with the service provider.

(1) The security capsule sends the registration request to the identity provider with the service provider identity and the SPUID.

(2) The identity provider calculates the key values: K_{IMPI_SPUID}, K_{IMEI_SPUID} and K_{APP_SPUID} using the hash function. Then the key values are sent to the service provider with the SPUID and these key values are distinct to each service provider. These key values will be used to establish a secure communication between the mobile device and the service provider.

$$HASH\ (K_{IMPI,}\ SPUID) = K_{IMPI\_SPUID}$$
$$HASH\ (K_{IMEI},\ SPUID\ ) = K_{IMEI\_SPUID}$$
$$HASH\ (HASH(UID),\ SPUID) = K_{APP\_SPUID}$$

(3) The service provider saves the key values with the SPUID. Then it acknowledges the identity provider by sending a User PIN derivation request to the mobile device. The request consists of the public key certificate of the service provider.

(4) The User PIN derivation request is transmitted from the identity provider to the mobile device.

(5) Finally the mobile device and service provider share a User PIN (4 digits).The User PIN is transmitted from the mobile device to the service provider over a secure channel using the service provider public key. The User PIN is obtained from the mobile user and it is obtained over the device keypad. The derivation of the User PIN is an optional step for extra security at the security capsule.

During the registration phase the mobile device shares unique key values (K_{IMPI_SPUID}, K_{IMEI_SPUID} and K_{APP_SPUID}) with the service provider for the future secure communication. The service provider and the mobile device generate the secret key for the communication using these key values and the User PIN. The key values are generated using the hardware (mobile device) dependent, SIM dependent and the capsule dependent parameters. However, these parameters are not sent outside the mobile device and the parameters cannot be derived using the key values due to the irreversible property of the hash function. The key values are transmitted in a secure communication link between the identity provider and the service provider and the attackers are unable to access them. Meanwhile, these values are only transmitted once in the network to the service provider and then these key values are utilized many times for the data key generation process.

3.2 Data Transmission

The data is transmitted to the mobile device in an encrypted format from the service providers to preserve the data confidentiality and the data is encrypted using the data key at the service provider. The service providers generate and send Data token to the mobile device before the data transmission and the data token presents the mobile device's authorization to access the data. The transmitted tokens consist of secret cryptographic key and this key will be used to generate the data key to decrypt the data from service providers. This key is named as 'Token key' and a unique token is generated for each encrypted data element. The tokens are uniquely identified by the service provider with the token ID. The service provider maintains a link between the token ID and the encrypted data in its domain.

The data transmission phase starts with generating the shared secret key for the data encryption at the service provider. The security capsule and the service provider share the symmetric key algorithm for the data encryption and the data decryption as a pre-request to the data transmission process.

Phase 1: Key Generation at Service provider

The Data key is generated at the service provider using the hash function and the Data key is a 192 bit (64 bit X 3) cryptographic key. The service provider generates a Real-Time key before the data key generation and this key will be an input to the Data key generation function. This Real-Time key enables the real-time security/authentication protection at the security capsule and it is linked with the Token ID at the service provider. The security capsule has to send the Token ID to retrieve the correct Real-Time key from the service provider. Depending on the required security level for the data, the service provider will be able to configure the Real-Time key as a single key at the service provider or a unique key for each encrypted data segment. The generated Real-Time key is saved at the service provider with the Token ID. The following is the Data key generation hash function with the input parameters.

Function (Real-Time Key, Token Key, K_{IMPI_SPUID}, K_{IMEI_SPUID}, K_{APP_SPUID}) = Data Key

Phase 2: Data encryption at the service provider
The generated Data key is used to encrypt the requested data. The symmetric encryption algorithm is used for the data encryption functionality. Finally, the encrypted data is transmitted to the mobile device. The data will be sent to the security capsule. Meanwhile, the related Data Token for the encrypted data should be at the security capsule; otherwise the security capsule requests the token from the service provider.

3.3 Data Access at the Security Capsule

The security capsule obtains the request for the data decryption from the mobile user and it retrieves relevant Data Token from the memory. The Data key is generated as the initial step for accessing data at the mobile device. Then the encrypted data will be decrypted using the decryption algorithm.

Phase 1: Key generation at the Security Capsule
The following are the key generation steps at the security capsule.

(1) Validates the Data Token integrity and the Data Token freshness. If the token is not valid then it is deleted from the capsule and a new token is requested from the service provider.
  - The XML signature of the token is verified with the token issuer's public key for the token integrity
  - The timestamp of the token and the token lifetime are compared with the present timestamp from the identity provider for the token freshness.

(2) The Token ID and the Token key are extracted from the token.

(3) The security capsule sends the Real-Time key request message to the service provider while specifying the Token ID

(4) The service provider replies with a challenge request. The communication between the service provider and the mobile device is secured using a shared session key generated during the authentication process.

(5) The challenge response is generated by the security capsule as follows;

$F_{challenge}$ (User PIN, Challenge Request) = Challenge Response

(6) The challenge response is sent to the service provider

(7) The service provider executes the same function ($F_{challenge}$) and generates the Challenge Response. Then it compares the generated Challenge Response with the response sent by the security capsule. The service provider sends the Real-Time key to the mobile device if both challenge responses are the same.

(8) The security capsule obtains the IMPI and IMEI from the mobile device and the UID from the internal data storage.

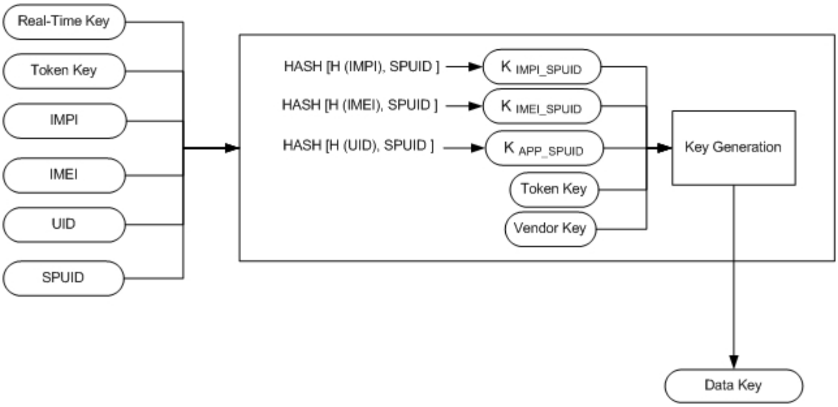

Fig. 2. Key generation at the Security Capsule

(9) The data key for the decryption is generated using the key generation algorithm as shown in Figure 2. The key generation algorithm is designed using the hash functions.

(10) Real-Time key, Token key, IMPI, IMEI, UID, K_{IMPI_SPUID}, K_{IMEI_SPUID} and K_{APP_SPUID} values are in the phone memory after the Data Key generation process. These values should be removed from the memory after the key is generated to prevent security attacks. Therefore, the security capsule discards those values for the memory location.

(11) The security capsule decrypts the data using the data key and symmetric decryption algorithm in the capsule. Then Data key is permanently deleted from the device memory.

Phase 3: Data access and data deletion

The security capsule presents the data in a viewable format to the mobile user and the data content or the data memory location details are not accessible to the mobile users. Therefore, the mobile user will not be able to save the data in a different memory location or send it to another mobile device. The security capsule controls the user interaction with the decrypted data during the utilization. The user will only be able to view the data and other functionalities such as save, edit, copy, delete, etc are disabled from the user interface. Once the data utilization session is completed, the capsule permanently deletes the decrypted data from the memory.

The key generation, data decryption, data access and data deletion functionalities of the security capsule are summarized in the Figure 3. The hash function for the key generation is implemented using the SHA-1 algorithm and it generates a 192 bit cryptographic key as the Data key. The Token key and Real-Time key are 64 bit cryptographic keys. The symmetric key encryption and decryption functionalities are implemented using the Triple DES / Electric Code Book / No Padding algorithm. The hash function and the encryption/decryption algorithms are publicly available. The operational data from the capsule is saved on the Random Access Memory of the mobile device. These memory locations are accessed from the security capsule to delete the memory contents permanently by making data bits to zero.

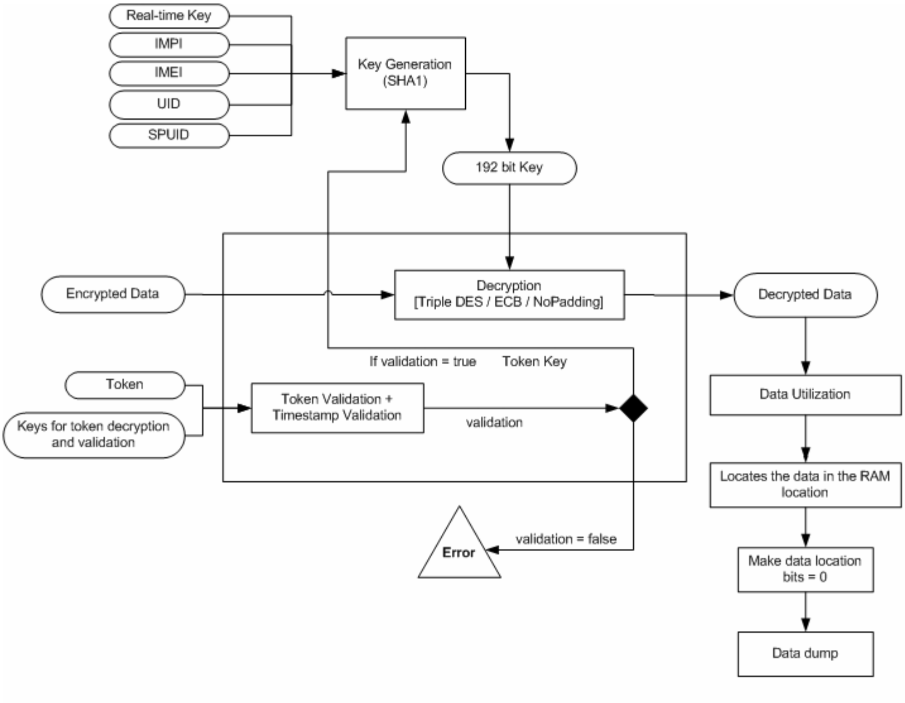
Real-time Key
IMPI
IMEI
UID
SPUID
Key Generation (SHA1)
192 bit Key
Encrypted Data
Decryption [Triple DES / ECB / NoPadding]
Decrypted Data
If validation = true
Token Key
Token
Keys for token decryption and validation
Token Validation + Timestamp Validation
validation
Data Utilization
Locates the data in the RAM location
Error
validation = false
Make data location bits = 0
Data dump

Fig. 3. Security Capsule Functionality

4 Parameter Based Access Control

The generation of the Data key at the mobile device enables the mobile user to access data from the service provider. The Data key is distinct to each encrypted data set and it is generated using the following types of inputs.

(1) Mobile User dependent: **User PIN;** the data cannot be access without the presence of the user

(2) Mobile device (Hardware) dependent: **IMEI;** the data can only be accessed in the specified mobile device. The mobile device identification is specified to the service provider during the registration.

(3) Mobile SIM dependent: **IMPI;** the data can only be accessed if the specified SIM card is in the mobile device. The SIM card identification is specified to the service provider during the registration.

(4) Security Capsule dependent: **UID;** the data can only be accessed in the specified security capsule. The security capsule identification is specified to the service provider during the registration.

(5) Service Provider dependent: **Real-Time key;** the data can only be accessed if the real-time authorization is granted by the service provider. The Real-Time key presents the real time access rights to the sensitive data.

(6) Service Provider and Identity Provider dependent: **Token key;** The Data or Trust token presents the mobile user authorization to access data. The authorization is obtained using the mobile device authentication with the identity provider. The Token key is granted to the mobile device only if the mobile user access is authorized by the identity provider and service provider during the authentication phases.

The Data key will not be generated if any of the input is not presented at the key generation process.

The mobile service environment transmits different levels of sensitive data from the service providers. The security protection with the full range of the above input types is not required for the data levels. The service provider generates the Data key for the encryption process and the service provider has the ownership of the data. Therefore, the service provider decides the required security levels of the data and the required input parameters for the Data key generation. For an example, the less number of input parameters will be used to generate the data key for less sensitive data and the higher number of input parameters will be used to generate the Data key for the more sensitive data. The service provider specified input parameters should be presented at the mobile device to access the data from the service provider. Therefore, the generation of the Data key using the different types of parameters at the mobile device enables the novel parameter based access control concept for data security in mobile devices.

The extra parameters can be introduced to the concept depending on the mobile service environment such as location ID verifies the user location before the data decryption. The service provider defines the access control level for the data based on the parameters. Then the required parameters should be available at the mobile device for the data access. The Data token is enhanced as follows with an extra XML element to present the parameter based access control level for the encrypted data.

XML element:

<p_access>User PIN, IMEI, IMPI, UID, Real-Time key, Token Key </p_access>

Explanation:

If the parameter is required then it is presented with ‘1’ and else ‘0’

Example:

<p_access>1, 1, 1, 1, 1, 1 </p_access>: Highest access level and all the parameters are required for the data access

<p_access>0,0,0,0,0,0 </p_access>: lowest access level and the data access is allowed without verifying the presence of the parameters at the mobile device.

5 Conclusion

This paper presents the functionality and the architectural implementation of the security capsule to protect the data and services at the mobile devices. The novel key generation approach is introduced using the different types of input parameters. The parameter based access control methodology is process to configure the security for the mobile data.

References

1. Weerasinghe, D., Rajarajan, M., Rakocevic, V.: Device Data Protection in Mobile Healthcare Applications. In: The First International Conference on Electronic Healthcare in the 21st century, London, September 8 (2008)
2. Weerasinghe, D., Rajarajan, M., Rakocevic, V.: Federated Trust Negotiation for Mobile Services. In: International Conference on Security and Identity Management (SIM), Ahmedabad, India, May 10-11 (2009)
3. Villate, Y., Illarramendi, A., Pitoura, E.: Data Lockers: Mobile-Agent Based Middleware for the Security and Availability of Roaming Users Data. In: Scheuermann, P., Etzion, O. (eds.) CoopIS 2000. LNCS, vol. 1901, Springer, Heidelberg (2000)
4. Lankhorst, M.M., van Kranenburg, H., Salden, A., Peddemors, A.J.H.: Enabling technology for personalizing mobile services. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences, HICSS, January 7-10, pp. 1107–1114 (2002)
5. Perelson, S., Botha, R.: An investigation into access control for mobile devices. Departmentof Business Information Systems, Port Elizabeth Technikon, South Africa (July 2004)
6. Keely, D.: A Security Strategy for Mobile E-business. Tech. Rep. GSOEE213, IBM Global Services (2001)
7. Bresson, E., Chevassut, O., Essiari, A., Pointcheval, D.: Mutual Athentication and Group Key Agreement for Low-Power Mobile Devices. In: 5th IEEE International Conference on Mobile and Wireless Communications Networks (2003)
8. Dodis, Y., Katz, J., Xu, S., Yung, M.: Key-insulated public key cryptosystems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 65–82. Springer, Heidelberg (2002)
9. Sander, T., Tschudin, C.: Towards mobile cryptography. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, pp. 215–224. IEEE Computer Society Press, Los Alamitos (1998)
10. Berbecaru, D., Lioy, A., Marian, M.: On the complexity of public-key certificate validation. In: Davida, G.I., Frankel, Y. (eds.) ISC 2001. LNCS, vol. 2200, p. 183. Springer, Heidelberg (2001)
11. Umezawa, K., Susaki, S., Tezuka, S., Hirasawa, S.: Development and Evaluation of a Certificate Validation System in Mobile Environments. IEEJ Transactions on Electrical and Electronic Engineering 1, 84–93 (2007)
12. Forman, G.H., Zahorjan, J.: The Challenges of Mobile Computing. IEEE Computer 27(4), 38–47 (1994)
13. Dodis, Y., Katz, J., Xu, S., Yung, M.: Key-insulated public key cryptosystems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 65–82. Springer, Heidelberg (2002)
14. Oprea, A., Balfanz, D., Durfee, G., Smetters, D.: Securing a remote terminal application with a mobile trusted device. In: ACSAC (2004)