Location Based Encryption using Message Authentication Code in Mobile Networks

[1] Swapna B Sasi, [2] Betsy K Abraham, [3] Jinil James, [4] Riya Jose

[1]Asst. Professor, Department of Computer Science and Engineering, Jyothi Engineering College, Cheruthuruthy
Thrissur, Kerala, India

[2, 3, 4] Department of Computer Science and Engineering, Jyothi Engineering College, Cheruthuruthy
Thrissur, Kerala, India

Abstract - The popularity of mobile devices increases the frequency of data transmission among mobile users. How to provide a secure and convenient protocol for data transmission is important. Secure communication is possible through encryption of data. The concept of "geoencryption" or "location-based encryption" is developed to restrict the location and time of data decryption. Location-based encryption or geo-encryption refers to an encryption method in which ciphertext can be decrypted only at a specified location. If someone attempts to decrypt the data at some other location, the decryption process fails ad reveals no details about the original plaintext information.

***Keywords* - Location based encryption, security, mobile networks, MAC.**

1. Introduction

Nowadays mobile communication has become an important part of our daily life. All the communications need security. Secure communication is possible through encryption of data. Geo-encryption builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It can be used with both fixed and mobile applications and supports a range of data sharing and distribution policies. It provides full protection against attempts to bypass the location feature. Depending on the implementation, it can also provide strong protection against location spoofing.

The term "location-based encryption" is used here to refer to any method of encryption wherein the cipher text can only be decrypted at a specified location. If an attempt is made to decrypt the data at another location, the decryption process fails and reveals no information about the plaintext. The device performing the decryption determines its location using some sort of location sensor, for example, a GPS receiver or some other satellite or radio frequency positioning system.

Location-based encryption can be used to ensure that data cannot be decrypted outside a particular facility, for example, at a particular theatre, the headquarters of a government agency or corporation, or an individual's office or home. Alternatively, it may be used to confine access to a broad geographic region. Time as well as space constraints may be placed on the decryption location.

2. Related work

The growing interest in location based encryption and the continual emergence of new encryption techniques inspired some previous efforts for surveying the characteristics, applications and drawbacks of such an area . In this subsection we highlight the features that distinguish our survey and hint the difference in scope. The goal of [1] is to make a method of encryption wherein the cipher text can only be decrypted at a specified location.

The existing system uses geoencryption algorithm with a PVT-mapping function. On the encrypting side, a GeoLock is computed based on the intended recipient's Position, Velocity, and Time. The PVT block defines where the recipient needs to be in terms of position, velocity & time for decryption to be successful. The GeoLock is then XORed with the session key to form a GeoLocked session key. The resultant is then encrypted using an asymmetric algorithm and conveyed to the recipient. On the decryption side, GeoLocks are computed using an AntiSpoof GPS receiver for PVT input into the PVT-GeoLock mapping function. If the PVT values are correct, then the resultant GeoLock will XOR with the GeoLocked key to provide the correct session key.That

Paper is a good introductory for readers interested in the broad area.

In [2] a location-dependent approach is proposed for mobile information system. This approach can meet the confidentiality, authentication, simplicity, and practicability of security issues. An information system which provides services for mobile clients is called mobile information system. Data encryption techniques are used for ensuring the data transmission security between information server and mobile clients.

The mobile client transmits a target latitude/longitude coordinate for data encryption to information server. Then, the server encrypts the message and sends the ciphertext back to the mobile client. The client can only decrypt the ciphertext when the coordinate acquired form GPS receiver matches with the target coordinate. The process of communication is divided into register phase and operation phase. Traditional encryption technology cannot restrict the location of mobile clients for data decryption. In order to meet the demand of mobile information system in the future, a location-dependent data encryption is proposed in this paper. The approach provides a novel function by using the latitude/longitude coordinate as the key of data encryption.

A location-dependent approach, called location-dependent data encryption algorithm (LDEA), is proposed in [3]. A target latitude/longitude coordinate is determined firstly. The coordinate is incorporated with a random key for data encryption. The receiver can only decrypt the ciphertext when the coordinate acquired from GPS receiver is matched with the target coordinate. The purpose of LDEA is mainly to include the latitude/longitude coordinate in the data encryption and thus to restrict the location of data decryption. When the target coordinate and TD (toleration distance) is given by the sender on the left-hand side, an LDEA-key is generated from latitude/longitude coordinate and TD. If the acquired coordinate is matched with the target coordinate within the range of TD, the ciphertext can be decrypted back to the original plaintext. Otherwise, the result is indiscriminate and meaningless.

[4] Explains how location can be used as one of the credentials to give access to data only to legitimate user. This technique is relatively new approach towards information security. Location Based Authentication is a technique that will take into account the geographical location of the user; which is latitude, longitude of the person who is trying to authenticate his identity. Location information is captured at that instance when he is trying to access his mail account. This paper, we are introducing a relatively new technique which will provide a higher level of security to an application. Location based authentication is an additional factor in providing strong authentication as a location characteristic can never be stolen or spoofed. It has provided a supplementary dimension in network security. It gives the owner the complete control of the information that only he has access to.

A navel approach to identify Geo-Encryption with GPS and different parameters such as locations And time is proposed in [5]. The use of location information can be used for enhancing the security of an application. Geo-encryption is the use of position navigation and time (PVT) information as means to enhance the security of a traditional cryptographic system. It allows data to be encrypted for a specific place or board geographic area and supports constraints in time as well as space. It can be used with both fixed and mobile applications and supports a range of data sharing and distribution policies. This paper describes how the traditional cryptographic system can be extended to incorporate the notion of location and other parameters (Time).

Our work is a dedicated study of secure communication using location dependent encryption technique. In addition, we are making use of the unique id of the device and MAC concept which adds an extra level of security by optimizing the access to the message only to a specific machine located at a predefined geographical area.

3. Implementation

Geoencryption is an enhancement to traditional encryption that makes use of physical location or time as a mean to produce additional security and security features. It limits the access (decryption) of information content to specified locations and/or times. The algorithm does not replace any of the conventional cryptographic algorithms, but instead adds an additional layer of security. Any attempts to access the secure information at an unauthorized location will result in a failure of the decryption process fails. We try to present a modified Geo protocol and improve its efficiency and applicability. The idea of location based encryption can be implemented as an android app. The app is used by two users, the sender and the receiver to transfer data securely between them. The message to be send is encrypted into cipher text by the sender and it is decrypted at the receiver side to get the plain text. Receiver can only decrypt the ciphertext when he is at the specified location.

The components of the proposed system are:

A. Login and registration
B. Location retrieval
C. Encryption and decryption
D. Error validation

A) Login and registration

In this module user first register in to the app by giving their simple personal details like username ,password ,e-mail id etc and by using the username and password the user login in to the application. In this module we use database to store the registered user details. To create the database in android we use sqlite.**SQLite** is a relational database management system contained in a small C programming library. In contrast to other database management systems, SQLite is not a separate process that is accessed from the client application, but an integral part of it. SQLite is a popular choice as embedded database for local/client storage in application software such as web browsers. SQLite implements most of the SQL-92 standard for SQL but it lacks some features. For example it has partial support for triggers, and it can't write to views (however it supports INSTEAD OF triggers that provide this functionality). While it supports complex queries, it still has limited ALTER TABLE support, as it can't modify or delete columns.

B) Location retrieval

In this module the latitude and longitude of the user is getting from the device by using either GPS or by using PROVIDER (Location manager is the class used to get the location in android).

In android by using these steps the user location is located

1.Start application.
2.Sometimes later, start listening for updates from desired location providers.
3.Maintain a "current best estimate" of location by filtering out new, but less accurate fixes.
4.Stop listening for location updates.
5.Take advantage of the last best location estimate.

Two providers are used in android to get the user location. GPS provider and .NETWORK provider. GPS location provider. determines location using satellites. Depending on conditions, this provider may take a while to return a location fix. Requires the permission android.permission.ACCESS_FINE_ LOCATION. The GPS provider will only work correctlly and more efficently in places where we can see the sky. .NETWORK provider determines location based on availability of cell tower and WiFi access points. Results are retrieved by means of a network lookup. Requires either of the permissions android.permission.ACCESS_COARSE_LOCATION or android.permission.ACCESS_FINE_ LOCATION.

Depending on the environment where your application is used or the desired level of accuracy, you might choose to use only the Network Location Provider or only GPS, instead of both. Interacting with only one of the services reduces battery usage at a potential cost of accuracy. By using this we can get the lattitude and logitude ie, geo-coordinates of the users location. This geo-coordinates can be converted in to location by using geocoding.Geocoding is the convertion of geo-coordinates in to the place name.

C) Encryption and decryption

The process of encryption and decryption is done by using the DES algorithm. And the key used in this algorithm is generated from the geolocation and the unique id that we get from the device. The encrypted text is then send to the receiver. The receiver needs to get its location details and only using those it can decrypt and obtain a meaningful text.

For geting the unique ID (ANDROID DEVICE ID), TelephonyManager.getDeviceId() is required to return the IMEI of the phone, which is unique to that piece of hardware. Android Device ID is the specific alpha-numeric Identification code associated with your mobile device. This is a 64-bit quantity that is generated and stored when the device first boots. It is unique for each device. To get the Android Device ID we have the to use the permission. android.permission.READ_PHONE_STATE.thease permissions are added in the manifest file when the app is created. Manifest file is where all the permission are added. In manifest file we are also giving the supporting version details. In the app we are not using the MAC id because in android for getting the Mac id from one Device to another we need Wi-fi connectity. In some phones there is no wifi connectivity so we are using another unique id like MAC id to give more security to the data sent through the application.

Advantages of using Android_ID as Device ID:
•It is unique identifier for all type of devices (smart phones and tablets).
•No need only a single permission.
•It will remain unique in all the devices and it works on phones without Simcard slot
Android device id have also some disadvantages
•If Android OS version is upgraded by the user then this may get changed.
•The ID gets changed if device is rooted or factory reset is done on the device.
•Also there is a known problem with a Chinese manufacturer of android device that some devices have same Android_ID.
4) Data error validation

Here we are using a unique header(which is an id created for each file at the time of sending) and it is sent along with the data. During the decryption time it is checked by the receiver and the integrity of the data can be verified.

4. Applications

Traditional encryption technology cannot restrict the location of mobile clients for data decryption. In order to meet the demand of mobile information system in the future, a modified location-dependent data encryption algorithm is proposed in this paper. Geo-encryption can support both fixed and mobile applications, and a variety of data sharing and distribution policies[7]. It provides strong protection against location spoofing, depending on the implementation. Secure and confidential data transfer can be established through this approach. It can be used in banking applications where data such as account details are to be securely transferred. Also confidential data sharing between business firms can be accomplished. Geoencryption can be applied in military purposes where security really matters. This location based encryption technology can be extended to employ more applications like digital film distribution[6] etc.

5. Conclusion

Location based encryption enhances security by integrating position and time into encryption and decryption processes. The described geo-encryption approach builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific location(s)[8] or for specific area(s), e.g. a corporation's campus area. Constraints in time as well as location can also be enforced. Geo-encryption can be used with both fixed and mobile applications and supports a wide range of data sharing and distribution policies.

References

[1] L. Scott, D. Denning, "A Location Based Encryption Technique and Some of Its Applications", Proceedings of ION NTM 2003.

[2] H.Liao, P.Lee, Y.Chao, C.Chen, "A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security", In The 9th International Conference on Advanced Communicate Technology, pp. 625-626, Feb. 2007.

[3] L.Hsien-Chou, C.Yun-Hsiang, "A New Data Encryption Algorithm Based on the Location of Mobile Users", Info. Tech. J., 2008.

[4] Shraddha D. Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil, "Location Based Authentication: A New Approach towards providing Security", International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012.

[5] V. Rajeswari, V. Murali, A.V.S. Anil, "A Navel Approach to Identify Geo-Encryption with GPS and Different Parameters (Locations And Time)", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (4), 2012.

[6] L. Scott, D. Denning, "Location Based Encryption & Its Role In Digital Cinema Distribution", Proceedings of ION GPS/GNSS 2003.

[7] H.Hamad, S.Elkourd, "Data encryption using the dynamic location and speed of mobile node", Journal Media and Communication Studies Vol. 2, pp.67-75, March 2010.

[8] H. C. Liao, Y H. Chao, and C. Y Hsu, "A Novel Approach for Data Encryption Depending on User Location," The Tenth Pacific Asia Conference on Information Systems (PACIS 2006), July 2006.