

Location Based Authentication: A New Approach towards Providing Security

Shraddha D. Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil

Computer Department, Rajarshi Shahu College of Engg
Pune, India

Abstract- Identifying communicating entities i.e. “users” is today’s need. The process of identifying these entities accurately is known as authentication. The conventional authentication mechanisms are based on three factors: knowledge, possession and biometrics. The geographical position of a user is an important attribute that can be used to authenticate a user. In this paper, we are trying to explain 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.

Index Terms- communicating entities; credentials; legitimate users information security; location- based authentication

I. INTRODUCTION

Authentication is the process of identifying correct entities and giving access to legitimate users. Location-based authentication is a new approach towards providing higher security.

With the growth of wireless technologies in sectors like the military, aviation, etc, there is a need to determine the authenticity of a genuine user. The location-based authentication is a quite new direction in the information security. The direction gains in importance nowadays due to mobile devices coming to wireless network environment.

Authentication is one of the three main processes of AAA systems (Authentication Authorization Accounting) [2]. Generic AAA system is in Figure 1.

AAA system consists of three main factors:

- Authenticator
- Authority and
- Accounting

As shown in Figure 1, if a user wants to get access to restricted area, he has to give request to authenticator (1). However authority (2) will decide whether or not to grant access to that user. If the user is legitimate then controller (3) will establish connection between user and restricted area. Information related to user’s actions is recorded by Accounting (4).

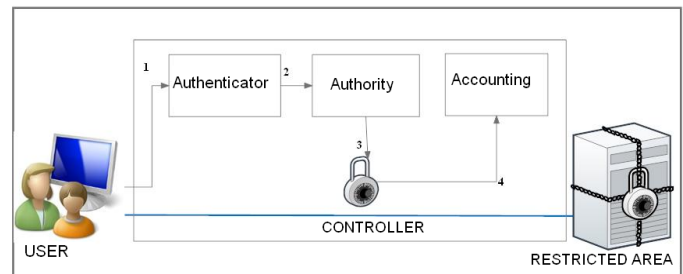


Figure 1: AAA System

The existing authentication models are most prevalent authentication models and have been used for decades. In order to authenticate a particular user, there is wide range of aspects. These aspects possess any of the following factors:

- Something you know: a password
- Something you have: a digital certificate
- Something you are: a biometric

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. In this paper, we are introducing a relatively new technique which will provide a higher level of security to an application.

The user gets access to his mail account only after evaluation of following credentials:

- User id and Password
- IP address
- Biometric Data
- Location

Thus after this we can decide whether the user is legitimate or not. In this way we can provide a higher level of security to an application.

Consider the example of any social networking site or an E-Mail application; the important information about users such as username, password, personal details, etc. is stored in the database. This database is mostly placed on the server(s) which are located at a particular location(s). So, the information stored on the servers might get accessed by the providers for some reasons like security. Access to this should be granted only when the person is at the geographic position where the particular server is located. Or else the access must be denied. In other words the information should not be allowed to be taken away outside that premise. In such cases, existing security controls are

insufficient to provide the level of security that this kind of growing computing system want.

The solution to this problem would be Location Based Authentication that will take into account not only the user id and password but also geographical location and biometric template; thus leading to higher level security. After successful authentication, the data that is to be sent and received would be encrypted. To achieve this Advanced Encryption Standard algorithm will be used.

II. RELATED WORK

Authentication is accepting proof of identity given by a credible person who has evidence on the said identity or on the originator and the object under assessment as his artifact respectively. Traditional authentication technique generally requires an id and password to verify the identity of user. By nature, user is looking for a password that is easy to remember and secured from any attack. However, remembering many complicated passwords, especially when user has different accounts, is not an easy task. Earlier two factor authentication technique is common in use. In the two factor authentication individual can be identified by his user name and password. If username and password is matched then process of authentication is done and user can access the data. But in this technique anyone can hack password and access information. In many cases, users' passwords are stored in plain-text form on the server machine. Anyone who can gain access to the server's database has access to enough information to impersonate any authenticable user. In cases in which users' passwords are stored in encrypted form on the server machine, plain-text passwords are still sent across a possibly-insecure network from the client to the server. Anyone with access to the intervening network may be able to "snoop" pairs out of conversations and replay them to forge authentication to the system. Each separate system must carry its own copy of each user's authentication information. As a result, users must maintain passwords on each system to which they authenticate, and so are likely to choose less-than-secure passwords for convenience. Knowledge based authentication uses secret information. When user provides some information to authenticate himself as a legitimate user, the system processes this information and suggests whether the user is legitimate or not

For more security new factor is added. Humans have specific physical attributes that are unique to specific individuals. Humans are conditioned to recognize these characteristics and use them for authentication. A user enrolls in a biometric system by providing a sample of the physical characteristic measured by the system. In biometry techniques like facial recognition, finger print analysis, retina, voice recognition is done. Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. A biometric system can operate in the following two modes. In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps involved in person verification. . In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor

scores and calculate the threshold. Third step is the testing step. In Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. To prevent identity theft, biometric data is usually encrypted when it's gathered. How biometric verification works on the back end: To convert the biometric input, a software application is used to identify specific points of data as match points. The match points in the database are processed using an algorithm that translates that information into a numeric value. The database value is compared with the biometric input the end user has entered into the scanner and authentication is either approved or denied.

The STAT II technique uses active infrastructure to provide space-time information. It uses the proprietary communication technology IQRF to determine the possible location. This technique needs a new entity of the system for position determination. A new entity in the system is an anchor point.

The anchor point is a transceiver with short signal range and with the exactly known position. The transceiver of anchor point is based on proprietary communication technology IQRF. IQMESH is a network protocol implemented on IQRF devices enabling them to communicate to each other. IQRF is a complete modular platform for wireless peer-to-peer or network connectivity.

Authentication terminal sends space-time information to server AAA in order to authenticate.

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. In order to easily recover the contents of an encrypted signal, the correct decryption key is required.

However, we can increase the reliability and security of the authentication mechanism by combining multiple authentication factors into a single model.

III. PROPOSED SYSTEM

The principal behind the system is to provide access to only those who have been identified correctly. To authenticate users, following credentials will be used:

1. Location

Location of a specific user is highly sensitive information. This can be used for efficient authentication. This can be used as one of the key attribute to authenticate a person. In this model we will be using GPS device, specifically GPS receiver for tracking the geographic position of a particular user. The task of GPS device is to track the latitude and longitude co-ordinates of a user who is trying to get authenticated. Once the location sent by the user is process by local server, he will be able to access his mail account. One user can have multiple locations depicted.

2. Biometric

A physical feature or behavior is another distinct aspect, which is exclusive to an individual being authenticated. A finely designed biometric system accepts readings from an individual and precisely carries out the authentication. A fingerprint scanner, Digital Persona is used to manage and enroll fingerprints on notebooks/laptops running on 32-bit operating systems.

3. Encryption

The process of converting plain text to cipher text is known as encryption. In this system the data that a legitimate user will send or receive will be in encrypted form. To achieve this we will be using AES (Advanced Encryption Standard) algorithm which is advanced version of DES (Data Encryption Standard). The main advantages of AES are that its resistance against all known attacks; speed and code compactness on a wide range of platforms; design simplicity.

4. Key Generation

Key generation is the process of generating keys of cryptography. A key is used to encrypt and decrypt whatever data is being encrypted /decrypted. Symmetric –key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both encryption of plain text and decryption of cipher text.

System Description:

Figure (2) shows the overall working of the system. The proposed location-based authentication can be easily applied on a Mail system. Initially, the user will connect with local server wirelessly. The Local Server then will send a Connection Request to Mail Server. An acknowledgement will be sent by Mail Server to Local Server on successful connection establishment. After this process, if the user is not registered, he will begin the (1) Register. Here, the user will provide details like username, password; will scan his fingerprint impression and select a location from the list provided as per his preference. Furthermore, he would also submit information like address, email id, contact no, etc. The Local Server will send acknowledgement signal (2) Successful, once the user has registered successfully.

Now, the next step is (3) Login. Whenever the user wants to login to his account, he will first, open the application, enter his username and password and will submit it to Local Server. These details are then given to the Mail Server. These credentials will be validated by the Mail Server and if are correct, user will be asked to scan his thumb. This all is done in step (5) Username and password Authentication. The next step is to (6) Scan Thumb. This fingerprint impression is validated locally by the Local Server and then the location of the user is traced out. This location is sent to Local Server via (7) Send Location where it is checked if the location is valid. To accomplish this task, the system will make use of GPS enabled device that is connected to user machine via which user's location will be traced out. This device provides user's space-time information i.e. latitude & longitude to Local Server. The Local Server stores all information about user such as username, password, fingerprint template, his preferred location's latitude and longitude and range of that location.

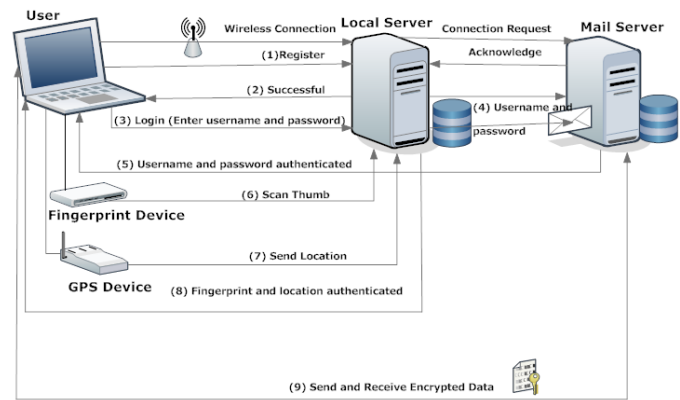


Figure 2 : System Description

The Fingerprint and location authentication is done at stage (8). After successful login, the Local server will establish connection between the User and the Mail Server, after which the user can compose mails, send mails and check inbox. All these details (such as username, password, e-mail details) of user are stored on the Server in encrypted format. Also the sending and receiving signals are encrypted by using AES algorithm.

The coverage area is specified for users. If a user goes out of that area after successful login, the access to his account will be prohibited.

The major advantage of the system is that the level of confidentiality is very high which leads to higher level of security. However, GPS Device's capacity to catch the signals appropriately is a sensitive issue.

IV. ALGORITHMS

As mentioned earlier, this scheme revolves around the idea about using location as one of the attributes to provide more security. To accomplish this task, following algorithms are being used:

1. Registration

This will focus on registering user to the system. Steps for this are as follows:

1. Enter user's personnel information
2. Enter USER ID and PASSWORD
3. Scan fingerprint
4. Select possible locations from database
5. Validate and store data

2. Log in: Go to login page

This is to provide login facility to the user. Steps are:

1. Enter USER ID and PASSWORD and validate it.
2. If success then go to step 3, else go to step 5.
3. Scan Fingerprint if match then proceed, else go to step 5.
4. Implicitly check location if valid go to step 6, else go to step 5.
5. Ask to enter again if attempts less than 3 else, go to step 7.
6. Grant access to user's account and show inbox.
7. Stop.

3. Fingerprint algorithm

When the user provides valid username and password, the next step is to ask him to scan his fingerprint and validate it. So in

order to add new Fingerprint Impression(if user is in registration phase) or to check if it is valid, following is the algorithm:

1. Create an object enroller of DPFPEnrollment by using method called createEnrollment() from getEnrollmentFactory().
2. Process the sample and create a feature set for the enrollment purpose using extractFeature (sample, DPFPDataPurpose.DATA_PURPOSE_ENROLLMENT).
3. Check quality of the sample and add to enroller if it's good.
4. Add feature set to template.
5. Check if template has been created. If yes, report success and stop capturing. If not, report failure and restart capturing.

To verify the fingerprint while logging in:

1. Create an object verifier of DPFPVerification by using createVerification() method of getVerificationFactory().
2. Collect the sample from the user.
3. Process sample and create a feature set for verification. Again use extractFeature (sample, DPFPDataPurpose.DATA_PURPOSE_VERIFICATION) for this.
4. Compare the feature set with stored template.
5. If match found, proceed to next step; location validation.
6. If no match found and no of attempts are less than 3, ask to scan fingerprint again.
7. Else deny access to the email account.

4. GPS algorithm

After successful validation of fingerprint, the location is to be tracked out with the help of GPS device, for that following are the steps:

1. Initialize GPS Device
2. Listen to a port by using GPSTDriver() function at specific port and with finite baudRate.
3. Setup GPS.
4. Retrieve available Port list and baud rate list by using two main functions getPortList() and getBaudRateList().
5. Start auto detection of GPS Driver by following steps:
 - a. Create an object OBJ of GPSTDriver.
 - b. Make use of GPSTDriver.detect() to detect GPSTDriver.
 - c. Open the GPSTDriver.
 - d. Add GPS listener to the object OBJ by using addGPSListener().
6. As soon as the GPS Driver is successfully initialized, the location of the user is to be traced out. To accomplish this task, a method called gpsEvent() is defined which has object of GPSInfo as a parameter.
 - a. Extract Latitude and Longitude of the location specified by the user.
 - b. Check the distance of the same.
 - c. If the distance of the location specified by the user is within valid range, proceed further.

- d. If invalid, deny the access to his account.
7. When the user is accessing his account, keep on tracing out his location continuously. For this isAlive() is used. This will check if user is within the coverage area. If user goes out of this stipulated area, cut down the access to his account.

V. CONCLUSION AND FUTURE WORK

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.

The avenues for future work on this application are:

- Monitoring behavior of the user
- Implementation on a PDA
- Besides latitude and longitude fields, an altitude field can also be added.

REFERENCES

- [1] David Jaros and Radek Kuchta, "New Location-based Authentication Techniques in the Access Management", Sixth International Conference on Wireless and Mobile xCommunications, 2010
- [2] H. Rui, Y. Man, H. Janping, K. Zhigang, and M. Jian, "A novel Service oriented AAA Architecture", In Personal Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on, 2003, pp. 2833-2837 vol. 3.
- [3] Karaoguz and Jeyhan, "Location-based authentication of wireless terminal," US Patent, 2011.
- [4] D. E. Denning and P. F. MacDoran, "Location based authentication: Grounding cyberspace for better security," Computer Fraud & Security, vol. 1996, pp.12-16, 1996.
- [6] Rajerwari Mukesh, Dr. A. Damodaram "A Robust Finger Print based Two-Server Authentication and key exchange system, IEEE 2009.
- [7] David Jaros, Radek Kuchta, Radimir Vrba, "The Location-based Authentication with The Active Infrastructure", The Sixth International Conference on Internet and Web Applications and Services, 2011
- [8] Authentication: From Passwords to Public Keys by Richard E. Smith
- [9] Mohammad Musa, Edward Schaefer, and Stephen Wedig,
- [10] A simplified AES algorithm and its linear and differential cryptanalyses, Cryptologia 27 (April 2003), no. 2, 148-177.
- [12] YounSun Cho, Michael Goodrich and Lichun Bao, "Secure Access Control for Location-Based Application in WLAN Systems", Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on Oct. 2006
- [13] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit Authentication for Mobile Devices", Hotsec, 2009
- [14] G. Lenzini, M. Bargh, and B. Hulsebosch, "Trust-enhanced Security in Location-based Adaptive Authentication," Electronic Notes in Theoretical Computer Science, vol. 197, pp. 105-119, 2008.

AUTHORS

First Author – Shraddha D. Ghogare, Computer Department
Rajarshi Shahu College of Engg, Pune, India
Email id - shraddhaghogare@gmail.com

Second Author – Swati P. Jadhav, Computer Department
Rajarshi Shahu College of Engg, Pune, India
Email id - jadhav.swati001@gmail.com

Third Author – Ankita R. Chadha, Computer Department
Rajarshi Shahu College of Engg, Pune, India
Email id - chadha.ankita@gmail.com

Fourth Author – Hima C. Patil, Computer Department, Rajarshi
Shahu College of Engg, Pune, India
Email id - patilhimac@gmail.com