Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-2, February 10, 2012

Delegation-Based in On-Line and Off-Line Authentication Over Wireless Communication

Saravanan D
Lecturer, Dept of Computer Applications
Sathayabama University, Chennai 119.

JothiVenkateshK N
Lecturer, Dept of Computer Applications
Sathayabama University, Chennai 119.
E-mail: jothivengatesh@gmail.com

Abstract - Portable communication system provides mobile users with global roaming services. Localized authentication protocol is presented for inter-network roaming across wireless LANS. Private authentication protocol is presented to prevent the home location register. The concept of delegation in wireless communication is used to solve the problems of data security, user privacy and efficiency in PCSs. Authentication protocol contains on-line and off-line authentication processes. In the on-line authentication process, VLR connects with HLR when MS accesses the network through VLR and demands authentication. HLR also leaves secure authentication tokens with MS and VLR in this process. The off-line authentication process means that VLR need not contact HLR frequently and can rapidly authenticate MS by verifying the secure token when MS accesses the network VLR again.

Delegation is used to increase the communicational efficiency, and save the authentication time. Their protocol employs off-line authentication processes, such that VLR does not need to contact HLR frequently, and can rapidly re-authenticate MS. The protocol exhibits non-repudiation in on-line authentication process, it still has a weakness in off-line authentication processes. Without the non-repudiation property, a protocol may inspire a mobile user to deny that was used its services and to pay, or inspire a service provider to over charge a mobile user for services that wont request.

Keywords: *Authentications, Protocol, Encryption, Decryption, Re-Authenticated, Cryptography.*

I. INTRODUCTION

As technology advances from analogue systems to digital systems, personal communication system (PCSs) will soon provide broadband services in addition to the traditional voice and data communications. Wireless communication suffers from threats inherited from wide networks and those which are specified in the wireless environment for the lack of physical association between the subscriber and the wired network and easy access, proper authentication is necessary to protect the communication against illegal usage. Such protection is elaborated in terms of security services to be provided in the authentication protocols. During the authentication process, some secret information must be mutually agreed upon so the following communication can proceed efficiently in protected mode to achieve desired confidentiality. With modern digital and cryptographic techniques, protocols have been proposed to provide secure services to its subscribers which are comparable to those provided by traditional wireline networks.

In this project, the logic of these protocols is examine from various aspects, which include security services provided, constructing mechanisms, placement of trust, efficiency, influence of security disasters, and applicability of implementation. Various attacks are also considered to find out weaknesses associated with these protocols.

Note that authentication in this project is intended for the two parties on both ends of the wireless link. A subscriber and the mobile unit operated on his behalf will be treated as an integral part unless explicitly addressed, though they are two different entities and some sort of authentication is involved in between, either by PIN, password or through the complicated zero-knowledge proof identification procedure. The mobile end will be called mobile station (MS), portable unit (PU); the fixed end will be called network, service provided (or) operator.

1.1 Existing System

This investigation addresses the weakness of the delegation based authentication protocol. Although, the authentication protocol tries to achieve the non-repudiation property, and a malicious Visited location registerstill can forge authentication messages in the off-line authentication processes without the help of mobile station.

However, these forged messages are verifiable, such that home location *register* believes that *MS* generates the messages with the problem of data security, user privacy, computational loads and communicational efficiency in PCSs.

1.1.1 Disadvantages

- Security will not be provided for the messages obtained by the user.
- For that purpose It can’t find out the weakness provided in offline authentication
- It does not have the property of non-repudiation in off-line authentication.

II. PROPOSED SYSTEM

This investigation discusses the weakness of the authentication protocol and presents an enhanced protocol. The enhanced protocol uses a backward hash chain to ensure that the authentication messages in off-line authentication process cannot be forged.

In other words, the enhanced protocol achieves non-repudiation in both on-line and off-line authentication processes, and thus avoids the weakness described above. The remainder of this investigation is organized with the concept of the delegation-based authentication protocol and describes its weakness. It presents the enhanced protocol and discusses its security attributes.

Advantages

- It can easily identify the weakness occurred in off-line authentication with the help of web application.
- The proposed system fulfills the security attributes.
- Enhanced protocol achieves non-repudiation in both on-line and off-line authentication.

So we go for advanced encryption standard algorithm**.**

III. SYSTEM IMPLEMENTATION

Roaming Authentication Methods

3.1 On-Line Authentication
3.2 Off-Line Authentication

Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is workable and effective. Implementation of a modified application to replace an existing one. This type of conversation is relatively easy to handle, provide there are no major changes in the system.

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly.

Initially as a first step the executable form of the application is to be created and loaded in the common server machine which is accessible to the entire user and the server is to be connected to a network. The final stage is to document the entire system which provides components and the operating procedures of the system. Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

IV. IMPLEMNTATION FUNCTIONS

4.1 AUTHENTICATION
4.2 ENCRYPTION
4.3 DECRYPTION

4.1 Authentication

There are three types of techniques for doing this.

The first type authentication is accepting proof of identity given by a credible person which has evidence on the said identity or on the originator and the object under assessment as his artifact respectively.

The second type authentication is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph.

The third type authentication relies on documentation or other external affirmations. For example, the rules of evidence in criminal courts often require establishing the chain of custody of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it.

4.2 Encryption

Encryption is the manipulation of data, based on a password (also known as a key), for security purposes. Once your data has been encrypted, a person can not make sense of your data without knowing the password. Encryption is a process of coding information which could either be a file or mail message into text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading the data. The most widely used symmetric key cryptographic method is the Data Encryption Standard (DES) is used in this process. The algorithm is best suited to implementation in hardware, probably to discourage implementations in software, which tend to be slow by comparison. The key used in encryption is known as public key.

4.3 Decryption

In Decryption User can get Encryption Text automatically when he is giving In Encryption Id and Secret key. With the help of public key he can select the encrypted file and automatically decrypt a particular file. In a symmetric cryptosystem the same key used in encryption is also been used in decryption. The decryption key is known as private key.

V. CONCLUSIONS

Security is one of the important requirements to the wide acceptance of personal communication systems and authentication is the most essential procedure to ensure that the service is properly used. In this paper we examine some well-known protocols for the universal mobile telecommunication service from various aspects, including techniques used, system architecture, placement of trust, efficiency, influence of security disasters, feasibility of recover, and applicability of implementation. With advancement of hardware and software techniques, applications intended for data, voice, image, or their combinations can all be incorporated into this wireless environment in the future. As new services emerged, requirements for the security would be different depending on the applications. Compatibility with existing services and interoperability among different service providers should also be considered. All of these complicate the design of a proper authentication protocol and its still waiting for us to solve.

VI. FUTURE ENHANCEMENTS

Most subscribers roam among multiple base stations, but not into Foreign Service domains. That is, inter-domain roaming is not frequent. A common secret established between the subscriber and the network could be used to authenticate each other repeatedly for several sessions. It would be worthwhile using public-key techniques to establish the common secret, and then more desired services, which include non-repudiation and end-to-end encryption etc., can be improved.

VII. EXPERIMENTAL RESULTS

Type 1: ONLINE AUTHENTICATION

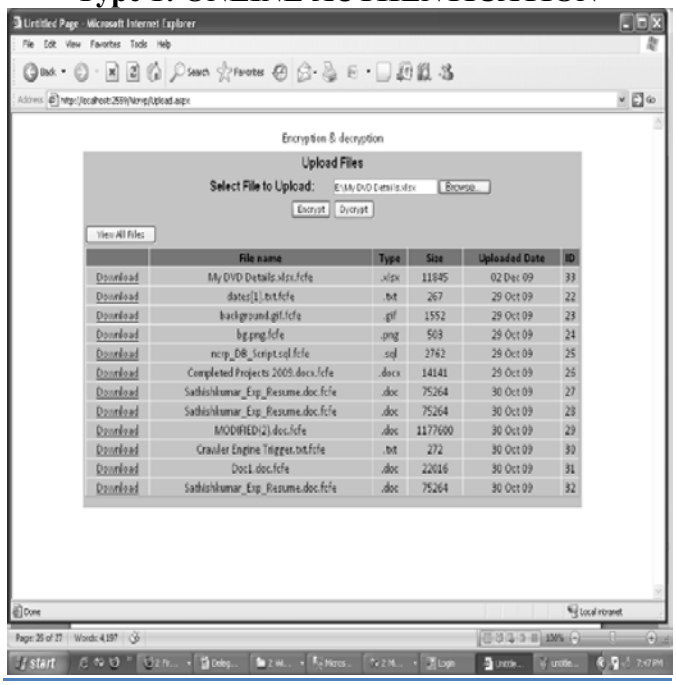

Figure1: Uploading File

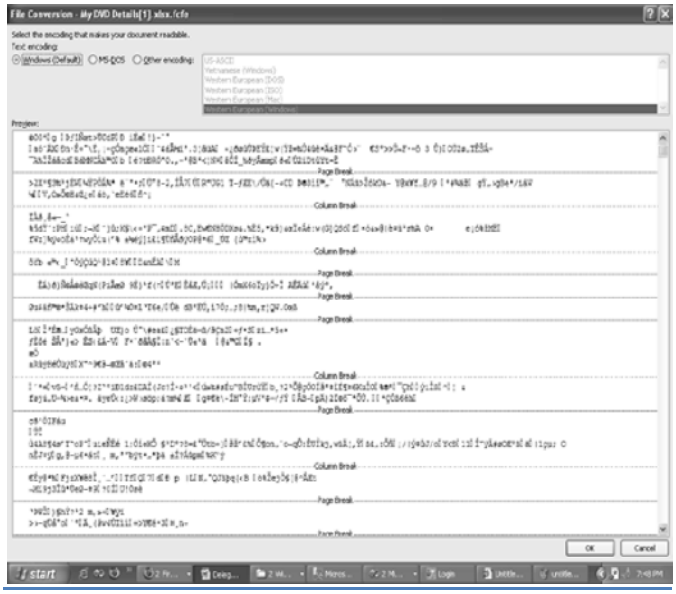

Figure2:Encrypted File

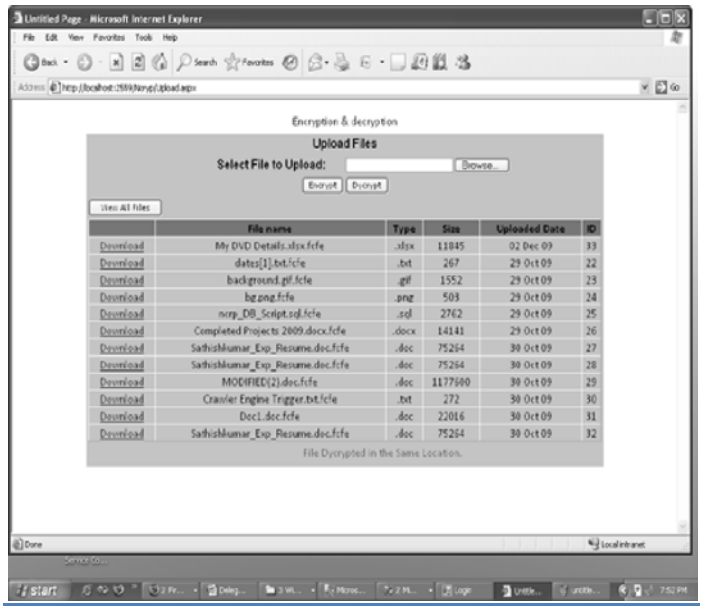

Figure 3: Viewing the Upload File

Type 2: OFFLINE AUTHENTICATION

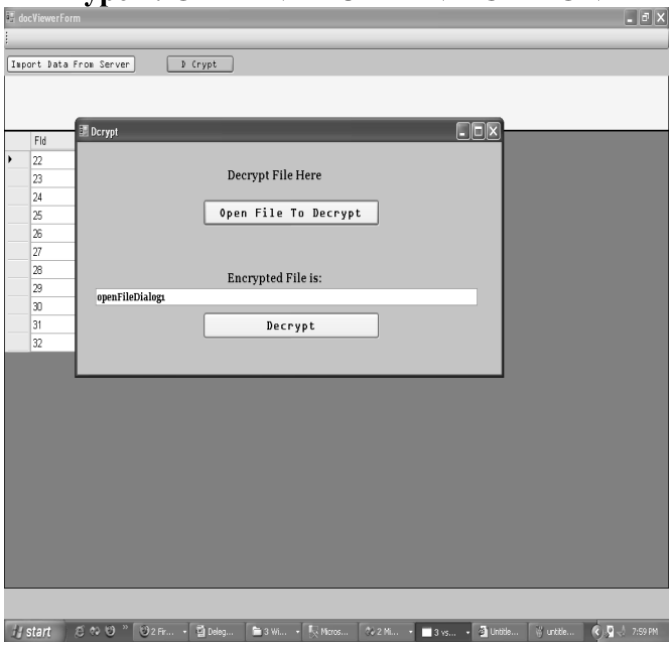

Figure4:Selecting Encrypted File

Figure5:File Decrypted

REFERENCES

1. Lynn Landes. Scrap the secret ballot - return to open voting, November 2005. http://www.opednews.com-/articles/opednelynnlan 051104 scrap the secret b.htm.
2. Ben Adida, “Advances in Cryptographic Voting Systems”, August 2006, www.vote. caltech.edu/media-/documents/wps/vtp_wp51.pdf

3. R.Mercuri. "Physical Verifiability of Computer Systems," 5th International Computer Virusand Security Conference, March, 1992.
4. David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24(2):84–90, 1981. http://doi.acm.Org/10.1145/35854- 9.358563.
5. M.Jakobsson, A.Juels and R.Rivest., "Making mix nets robust for electronic voting by randomized partial checking", February 1, 2002. http://www.vote.caltech.
6. T.-F. Lee, C.-C. Chang, and T. Hwang, "Private authentication techniques for the global mobility network," Wireless Personal Commun., vol. 35, no. 4, pp. 329-33336, Dec. 2005
7. W.-B. Lee and C.-K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," IEEE Trans. Wireless Commun., vol. 4, no. 1, pp. 57-64, Jan. 2005.
8. M. Rahnema, "Overview of the GSM system and protocol architecture," IEEE Commun. Mag., pp. 92-100, Apr. 1993.