ISSN: 2321-7782 (Online)
Volume 3, Issue 3, March 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Review Paper on Authentication Key Exchange by Using Privacy Preserving over the Internet

Priyanka A.Wankhade[1]
Computer science and Engineering
CBS college of Engineering and Management Amravati
Amravati, India

Dinesh Datar[2]
Information Technology
CBS college of Engineering and Management Amravati
Amravati, India

Abstract: ***Because of advances in technology and communication, it requires more hard facility to ensure security and privacy in communication network. There is very high need for every organization has the right level of security. In recent communication systems, as there is most use of Internet, the security services have become essential. Authentication in security had emerged to be an essential factor in the key establishment over Internet. It seems that recently Yang et.al propose provably secure 3PAKA protocol for secure exchange and similarly Key-exchange in Diffie–Hellman key-exchange (DHKE) is the valuable cryptographic mechanisms to ensure network security .The DIKE (Deniable Internet Key Exchange) was the family of privacy preserving authenticated DHKE protocol, both in the traditional PKI setting and in the identity based setting.***

There are lots of mechanism are provided for key exchange mechanism in recent year as given, but these mechanism only secure the message or key which is share by both trusted party over the Internet, but if the intruder authenticate the message which is send by the sender and when that message will receive by receiver without knowing that this message is already accessed by the intruder then what? There will be no use of that accessed message or key. So in this project there is a database in which the key sent by sender to receiver will be stored already, so that when receiver receives the valid key only that key will match with the key which is stored in the database and the message or the document which is sent by sender can be accessed by the receiver, as well as if the intruder knows the secret key then also he cannot accessed the message For that, the concept of Internet key exchange (IKE), and REA Algorithm are used.

Keyword: Authentication, DHKE, REA, Database.

I. INTRODUCTION

There are various ways are already given or mentioned for securing the key, and if the key will get secure then automatically message also gets secure, by analysing some recent techniques it seems that it may be possible to hide the key. [2]The basic of all technique are same, for hiding the key over the internet only the techniques are different, we can also say that all the emerging techniques are the phases of the Internet key change (IKE) [10]Internet protocol security (IP sec) and Internet Key-Exchange (IKE) protocols is also one of the technique for ensuring the internet security, which is given for key exchange mechanisms used to establish shared keys for use in the Internet Protocol Security (IPsec) standards . The IPsec and IKE are given for protecting messages communicated in the IP layer, i.e., “layer 3” of ISO-OSI. The transmission of messages using the network address possible with the ISO-OSI, by unknowing end-user peers’ identities. IKE and IPsec can be used to offer confidentiality, and privacy for communication protocols in the higher layers of ISO-OSI (note that many communication protocols including many authentication protocols which are invoked by end-users with explicit peer's identity information work at “layer 7" of ISO-OSI, i.e., the application layer[4] Authenticated Key Exchange (AKE) protocol is to enable both peer parties to establish a shared cryptographically strong key over an insecure network under the complete control of an opponent. AKE I s one of the most widely used and fundamental cryptographic primitives. For making AKE possible, the parties must

have authentication it means that they have their own keys, e.g. (public or secret) cryptographic keys, short (i.e., low-entropy) secret keys or credentials that satisfy a (public or secret) policy.[7]

All are the techniques are recently use for the key exchange methodology, by combining functions of all these techniques one new technique for analysing key which is sent by sender will get discover. Mainly the REA algorithm is used to make this possible.

II. LITERATURE REVIEW

Various authors describe various features in their techniques which they are used for the Internet key exchange ,all have their smart opinions and illustration for the key exchange mechanism.

Andrew Chi-Chao Yao and yunlei Zao(IEEE VOL. 9, NO. 1, JANUARY 2014) The Basic of this paper is to provide secrecy and confidentiality to the sender as well as receiver. for that they use DHKE(Diffie hellman key exchange).With the help of DHKE they develop a family of privacy preserving authenticated DHKE protocols named deniable Internet key exchange. They provide useful privacy protection to both protocol participants.

The security of DIKE is analysed in accordance with the various methods, some methods are as follows:

1. Canetti-Krawczyk framework (CK-framework) with post specified peers in the random oracle(RO)model.
2. Secure key exchange security(SK-security)
3. Concurrent Non- Malleable statistical Zero-Knowledge (CNMSZK) for DHKE
4. Concurrent knowledge of Exponent Assumption.

These various methods are get compared with each other.

a) *SK-security vs. CNMSZK for DHKE*

According to Sk-security if the session is uncorrupted then the session key is unknown to anyone expect this peer and if the unexposed peer completes a matching session then the two parties have the same shared key.

Now according to CNMSZK if the possibly malicious peer completes a matching session then not only the two parties have the same shared key but also the peer does know both the DH-exponent and the secret key corresponding to the DH-component and public key send alleged by it in the test-session.

b) CNMSZK for DHKE vs. traditional CNMSZK based approaches.

CNMSZK formulation for DHKE is based on the traditional CNMSZK formulation but some essential differences. On one hand traditional CNMSZK formulation considers a pair of players of fixed role, specifically one prover and one verifier. On other hand , privacy preserving CNMSZK proposes additional privacy requirements for the session messages of DHKE being exchanged concurrently over internet.

Suyeon Park and Hee-Joo Park(IJSIA Vol.8, No.4 (2014), pp.307-320 ISSN: 1738-9976) In this paper the disadvantages observed in Yang,et al in 3PAKA protocols are get overcomes, especially in financial secure advantages, they have been very widely deployed. This paper has been reviewed Yang, *et al.*, provably secure 3PAKA protocol. By using smart cards they shown that the protocol is weak against offline password guessing attack with lost smartcard and does not provide authentication in the password updating phase. Furthermore, it is possible to be tracked by attacker. BY analysing that Yang, *et al.*, 3PAKA protocol does not provide user anonymity. In order to solve the weaknesses in Yang, *et al.*, 3PAKA protocol, this paper proposed a privacy preserving 3PAKA (P_3PAKA) protocol using smart cards. P_3PAKAprotocol provides user anonymity and un-traceability by using dynamic identifier depending on each session's nonce. P_3PAKA protocol is more secure while maintaining efficiency than the other previous protocols. In this paper total 12 criteria is given, those criteria has

some required features, if those features is get satisfied by the method then the comparison can be done that which is the most secure method for the user Yang, *et al.*, 3PAKA protocol is consist with four phases, Basically four phases are given.

1) Registration Phase

2) Login Phase

3) Password updating Phase

4) Key agreement Phase

And these phases are also taken in P_3PAKA protocol there are two purpose of this paper: one is to show security weaknesses in Yang, *et al.*, protocol and the other is to propose a new 3PAKA protocol to solve the problems in Yang, *et al.*, 3PAKA protocol. Firstly, this paper review a security weakness against password guessing attack with lost smart card and lack of good properties for ubiquitous environment in Yang, *et al.*, protocol. Then, this paper proposes a new privacy preserving 3AKA (P_3PAKA) protocol using smart cards to solve the security problems in Yang, *et al.*, protocol. It provides user anonymity and un-traceability by adopting dynamic identifier depending on each session's nonce.

(Fabrice Ben Hamouda Olivier Blazy, Celine Chevalier, David Point cheval and Damien Vergnaud)In this paper they propose a new primitive that encompasses most of the previous notions of authenticated key exchange. It is closely related to CAKE and the authors call it LAKE, for Language-Authenticated Key-Exchange, since parties establish a common key if and only if they hold credentials that belong to specific languages. The definition of the primitive is more practice-oriented than the definition of CAKE from, but the two notions are very transparent. In particular, the new primitive enables privacy-preserving authentication and key exchange protocols by allowing two members of the same group to secretly and privately authenticate to each other without revealing this group beforehand.

In order to define the security of this framework, they use the UC framework and an appropriate definition for languages that permits to dissociate the public part of the policy, the private important information the users want to check and the secret values each user owns that assess the membership to the languages. They provide an ideal functionality for LAKE and give efficient realizations of the new primitive secure under classical mild assumptions, in the standard model with a common reference string, with static corruptions. They significantly improve the efficiency of several CAKE protocol for specific languages and enlarge the set of languages for which they construct practical schemes. Notably, they obtain a very practical realization of Secret Handshakes and a Verifier-based Password-Authenticated Key Exchange.

The contents of the paper are given as follows:-

a) **Definitions**

1. Universal Compensability
2. Commitment
3. Smooth Projective Hash Function

b) Double linear Cramer-Shoup Encryption (DLCS)

c) SPHF for implicit proofs of membership

1. commitments of signature
2. linear pairing product equation

d) **Language Authentication Key Exchange**

1. The ideal functionality

2. A generic UC-secure LAKE construction

e) **Concrete Instantiation and comparison**

1. Possible languages

2. concrete instantiation

(Ayman Mousa, Elsayed Nigm, Sayed El-Rabaie, Osama Faragallah IJNIS Vol.14, No.5, PP.280-288, Sept. 2012) There is a lot of very important data in the database, which need to be protected from attack. Cryptographic support is an important mechanism of securing them. People, however, must trade off performance to ensure the security because the operation of encryption and decryption greatly degrades query performance. For the query types that require extra query processing over encrypted database, the cost differentials of query processing between non encrypted and encrypted database increase linearly in the size of relations. To solve such a problem, the proposed encryption algorithm REA can implement SQL query over the encrypted database.

In this paper, They introduced a new encryption algorithm, which they called "Reverse Encryption Algorithm (REA)", restating its benefits and functions over other similar encryption algorithms. REA algorithm limits the added time cost for encryption and decryption so as to not degrade the performance of a database system. They also provide a thorough description of the proposed algorithm and its processes. This paper examines a method for evaluating query processing performance over encrypted database with the new encryption algorithm (REA) and with the most used encryption algorithm AES. The measuring performance of query processing will be conducted in terms of query execution time. The results of a set of experiments show the superiority of the proposed encryption algorithm REA over other encryption algorithm AES with regards to the query execution time. Their new encryption algorithm REA can reduce the cost time of the encryption/decryption operations and improve the performance.

The new encryption algorithm, "Reverse Encryption Algorithm (REA)", because of its simplicity and efficiency it can outperform for competing the algorithms. REA algorithm is limiting the added time cost for encryption and decryption to so as to not degrade the performance of a database system, they gives a general analysis of the functioning of these structures.

(Dexin Yang, Bo Yang) In this paper, a new multi-factor authenticated key exchange scheme is get introduced, which combines with biometrics, password and the smart card, is get proposed. Compared with the previous schemes, this scheme has higher security in remote authentication and preserves privacy of biometrics, and most of the previous schemes rely on the smart card to verify biometrics.

The advantage of these approaches is that the user's biometrics is not shared with the remote server, which can resist insider's attack and preserve the privacy of the biometrics. The disadvantage is that the given remote server must trust the smart card to perform authentication, which guide to various vulnerabilities. To achieve multifactor authentication, a new and fresh function called one-way function with distance-keeping, which is used to preserve privacy of user's biometrics, is proposed. This scheme has advantages as multi-factor authentication, privacy preserving and lower communication complexity etc. It is proven secure under the random oracle and is suitable to the environment which lacked communication resource and needed higher security.

Biometric authentication has some advantages over traditional authentication methods: biometric information cannot be acquired by direct convert observation, it is impossible to share and difficult to reproduce and it is convenient for user by alleviating the need to memorize long and random passwords. Moreover, biometrics is one of the rare techniques that can be used for negative recognition through which the system determines whether the person is who he or she denies to be. But biometrics is easily obtained and cannot be changed, which makes biometric features unreliable as encryption keys. The server cannot verify the device captures a person's biometrics who is alive because the biometric capture devices are remotely located.

III. PROPOSED WORK/METHODOLOGY

In this section we will see how to protect the key from the intruder and how to ensure privacy for both protocol participants. The privacy preserving method is used for the security providing mechanism. In the Internet there is one storage media for store the data and that storage is used to store all the search word. Whatever data user want to send, that data get encrypted and the storage media also used by the user, and if the user cannot be able to send data with the encryption technique then the process will get stop. The data will be send to the end user by using key and encryption technique, and the end user will be access that data by decryption technique and the key. Basically there is one database is already created, because the key which is sent by the sender will be stored in the database. sender and receiver both have their email ID, and sender knows the e-mail id of receiver and receiver knows the sender. So that they will the authenticate and true user of the key and the message. The log in and password are also plays most important role in this process. Without the registration the key will not accessed by the receiver as well as sender. For accessing the message or any document or any type of data ,the key which is sent by sender have to match with the key which is stored in the database, if the key will not match then receiver get message "Wrong matching data". And if the key will match then search document from encrypted key and Getting Most Encrypted

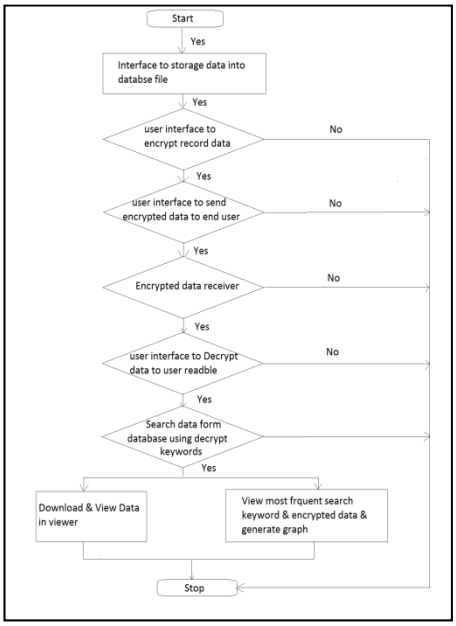

Fig.1.Data flow diagram

IV. CONCLUSION

In this paper we have pointed out various techniques used for key exchange by authenticate way. such as DHKE, DIKE, P_3PAKA protocol, CAKE, LAKE, Biometric way. All these techniques are used to ensure confidentiality and privacy for key and both protocol participant

References

1. Andrew Chi-Chih Yao and Yunlei Zhao"Privacy-Preserving Authenticated Key-Exchange Over Internet" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014
2. Miss. Pooja P. Taral Prof. Vijay B. Gadicha, "Secure Key Exchange over Internet" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 2014, pg. 545-548 ISSN 2320–088X
3. Suyeon Park and Hee-Joo Park, "Privacy Preserving Three-party Authenticated Key Agreement Protocol using Smart Cards" IJSIA Vol.8, No.4 (2014), pp.307-320
4. Andrew C. Yao Frances F. Yao Yunlei Zhao Bin Zhu, "Deniable Internet Key Exchange" Institute for Theoretical Computer Science, Tsinghua University, Beijing, China., Vol.10, 3 March 2013
5. Fabrice Ben Hamouda Olivier Blaze C_eline Chevalier David Pointcheval and Damien Vergnaud "Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages" 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC '13) 1 March 2013, Nara, Japan) Kaoru Kurosawa Ed., Springer-Verlag, 2013.

6. A. P. Sarr and P. E. Vincent, "A complementary analysis of the (s)YZ and DIKE Protocols," in Proc. Africacrypt 2012, pp. 203–220.
7. Ayman Mousa Elsayed Nigm Sayed El-Rabaie Osama Faragallas," Query Processing Performance on Encrypted Databases by Using the REA Algorithm" IJNS Vol.14, No.5, PP.280-288, Sept. 2012
8. Dexin Yang Bo Yang," A Novel Multi-factor Authenticated Key Exchange Scheme With Privacy Preserving", Journal of Internet Services and Information Security, volume: 1,2011 number: 2/3, pp. 44-56
9. A. C. Yao and Y. Zhao, "Deniable Internet key-exchange," IACR (The International Association for Cryptologic Research), San Diego, CA, USA, Tech. Rep. 2011/035, Jan. 2011.
10. J. Camenisch, N. Casati, T. Gross, and V. Shoup, "Credential authenticated identification and key exchange," in Proc. CRYPTO 2010, pp. 255–276.
11. C. J. F. Cremers, "Formally and practically relating the CK, CK-HMQV, and eCK security models for authenticated key exchange," IACR (The International Association for Cryptologic Research), San Diego, CA, USA, Tech. Rep. 2009/253, 2009.
12. L. Harn, W.-J. Hsin and M. Mehta, "Authenticated Diffie–Hellman key agreement protocol using a single cryptographic asumption", IEEE Proc.-Commun., Vol. 152, No. 4, August 2005.
13. Boyd C., Mao, W., Paterson, K.G., "Deniable Authenticated Key Establishment for Internet Protocols, 11th International Workshop on Security Protocols", LNCS, vol. 3364, pp. 255-271 (2003).
14. M.S. Borella, "Methods and protocols for secure key negotiation using IKE," IEEE Network, (2000), 18-29.

