ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Privacy Preserving in Two Authenticated Servers by Key Exchange

Mr.P.Anji Babu, M.Tech
Asst prof,
Department of CSE,
TKR College of Engineering & Technology.

G.Tabitha
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

J.bhaskar
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

J.Soumya
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

Abstract:

Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm.Diffie–Hellman key exchange (D–H) is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle. D–H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel.

This key can then be used to encrypt subsequent communications using a symmetric key cipher.- Due to advances in technology and communication, it requires more effort to ensure security. It is essential that everyorganization has the right level of security. Authentication in security had emerged to be an essential factor in the keyestablishment over internet. The DIKE (Deniable Internet Key Exchange) protocols add novelty and new value to the IKEstandard. In recent communication systems, as there is more and more use of internet, the security services have becomeessential. Key-exchange in Diffie–Hellman key-exchange (DHKE) is among the core cryptographic mechanisms to ensurenetwork security.

Keywords:

Key exchange, Authentication, Cryptography, Dike, IKE

Introduction:

If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.

The key exchange problem:

The key exchange problem is how to exchange whatever keys or other information are needed so that no one else can obtain a copy. Historically, this required trusted couriers, diplomatic bags, or some other secure channel. With the advent of public key / private key cipher algorithms, the encrypting key (aka public key) could be made public, since (at least for high quality algorithms) no one without the decrypting key (aka, the private key) could decrypt the message.

Identification:

In principle, the only remaining problem was to be sure (or at least confident) that a public key actually belonged to its supposed owner. Because it is possible to 'spoof' another's identity in any of several ways, this is not a trivial or easily solved problem, particularly when the two users involved have never met and know nothing about each other.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Diffie–Hellman key exchange:

In 1976, Whitfield Diffie and Martin Hellman published a cryptographic protocol called the Diffie–Hellman key exchange (D–H) based on concepts developed by Hellman's PhD student Ralph Merkle. The protocol enables users to securely exchange secret keys even if an opponent is monitoring that communication channel. The D–H key exchange protocol, however, does not by itself address authentication (i.e. the problem of being sure of the actual identity of the person or 'entity' at the other end of the communication channel). Authentication is crucial when an opponent can both monitor and alter messages within the communication channel (aka man-in-the-middle or MITM attacks) and was addressed in the fourth section of the 1976 paper.

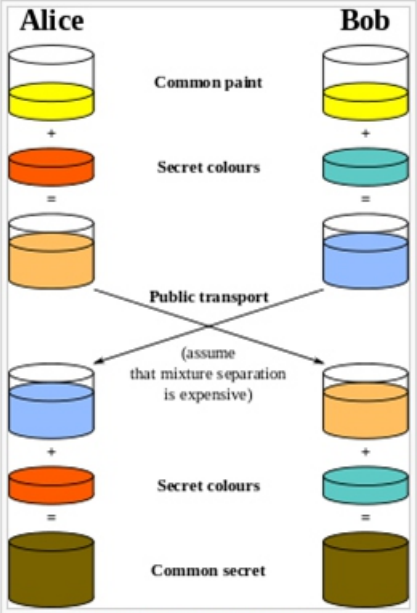


Illustration of the Diffie–Hellman Key Exchange

Public key infrastructure:

Public key infrastructures (PKIs) have been proposed as a way around this problem of identity authentication. In their most usual implementation, each user applies to a 'certificate authority' for a digital certificate which serves for other users as a non-tamperable authentication of identity, at the risk of compromising every user in case the CA itself is compromised. Several countries and other jurisdictions have passed legislation or issued regulations encouraging PKIs by giving (more or less) legal effect to these digital certificates. Several commercial firms, and a few government departments, have established such certificate authorities. VeriSign is the most prominent commercial firm.This does nothing to solve the problem though, as the trustworthiness of the CA itself is still not guaranteed from an individual's standpoint. It is a form of argument from authority fallacy. For actual trustworthiness, personal verification that the certificate belongs to the CA and establishment of trust in the CA are required. This is usually not possible.

For those new to such things, these arrangements are best thought of as electronic notary endorsements that "this public key belongs to this user". As with notary endorsements, there can be mistakes or misunderstandings in such vouchings. Additionally, the notary itself can be untrusted. There have been several high profile public failures by assorted certificate authorities.

Web of trust:

At the other end of the conceptual range is the web of trust system, which avoids central Certificate Authorities entirely. Each user is responsible for getting any certificate from another before using that certificate to communicate with, vet digital signatures from, ... the user claimed to be associated with the particular public key in a certificate. PGP (and GPG, an implementation of the OpenPGP Internet Standard) employ just such a web of trust mechanism. Together they are the most widely used high quality crypto system in the world. [citation needed]

Password-authenticated key agreement:

Password-authenticated key agreement algorithms can perform a cryptographic key exchange utilizing knowledge of a user's password.

Quantum key exchange:

The BB84 key exchange protocol—like any quantum key exchange protocol—exploits certain properties quantum physics to ensure its security. Since quantum mechanics ensures physical traces as a result of mere observation, it provides protection against man-in-the-middle attacks that cannot, as a matter of physical principle, be circumvented.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The Internet Key Exchange (IKE) is an IPsec (Internet Protocol Security) standard protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access. Specified in IETF Request for Comments (RFC) 2409, IKE defines an automatic means of negotiation and authentication for IPsec security associations (SA). Security associations are security policies defined for communication between two or more entities; the relationship between the entities is represented by a key. The IKE protocol ensures security for SA communication without the preconfiguration that would otherwise be required.

A hybrid protocol, IKE implements two earlier security protocols, Oakley and SKEME, within an ISAKMP (Internet Security Association and Key Management Protocol) TCP/IP-based framework. ISAKMP specifies the framework for key exchange and authentication; the Oakley protocol specifies a sequence of key exchanges and describes their services (such as identity protection and authentication); and SKEME specifies the actual method of key exchange. Although IKE is not required for IPsec configuration, it offers a number of benefits, including: automatic negotiation and authentication; anti-replay services (see anti-replay protocol); certification authority (CA) support; and the ability to change encryption keys during an IPsec session.

LITERATURE REVIEW:

Various authors describe various features in their techniques which they are used for the Internet key exchange ,all havetheir 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 providesecrecy and confidentiality to the sender as well as receiver. for that they use DHKE(Diffie hellman key exchange).With thehelp of DHKE they develop a family of privacy preserving authenticated DHKE protocols named deniable Internet keyexchange. 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 theunexposed 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 havethe same shared key but also the peer does know both the DH-exponent and the secret key corresponding to the DH-componentand 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 onehand traditional CNMSZK formulation considers a pair of players of fixed role, specifically one prover and one verifier. Onother hand , privacy preserving CNMSZK proposes additional privacy requirements for the session messages of DHKE beingexchanged 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 disadvantagesobserved in Yang,et al in 3PAKA protocols are get overcomes, especially in financial secure advantages, they have been verywidely deployed. This paper has been reviewed Yang, et al., provably secure 3PAKA protocol. By using smart cards theyshown that the protocol is weak against offline password guessing attack with lost smartcard and does not provideauthentication in the password updating phase. Furthermore, it is possible to be tracked by attacker. BY analysing that Yang, etal., 3PAKA protocol does not provide user anonymity. In order to solve the weaknesses in Yang, et al., 3PAKA protocol, thispaper proposed a privacy preserving 3PAKA (P_3PAKA) protocol using smart cards.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

P_3PAKAprotocol provides useranonymity and un-traceability by using dynamic identifier depending on each session's nonce. P_3PAKA protocol is moresecure 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 mostsecure 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 se-curityweaknesses in Yang, et al., protocol and the other is to propose a new 3PAKA protocol to solve the prob-lems in Yang, et al.,3PAKA protocol. Firstly, this paper review a security weakness against password guessing attack with lost smart card and lackof good properties for ubiquitous environment in Yang, et al., protocol. Then, this paper proposes a new privacy preserving3A-KA (P_3PAKA) protocol using smart cards to solve the security problems in Yang, et al., protocol. It provides useranonymity and un-traceability by adopting dynam-ic identifier depending on each session's nonce.

(Fabrice Ben Hamouda Olivier Blazy, Celine Chevalier, David Point cheval and Damien Vergnaud)In this pa-per theypropose a new primitive that encompasses most of the previous notions of authenticated key ex-change. It is closely related toCAKE and the authors call it LAKE, for Language-Authenticated Key-Exchange, since parties establish a common key if andonly if they hold credentials that belong to specific languages. The definition of the primitive is more practice-oriented than thedefinition of CAKE from, but the two notions are very transparent. In particular, the new primitive enables privacy-preservingauthentication and key ex-change protocols by allowing two members of the same group to secretly and privately authenticate toeach 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 languagesthat permits to dissociate the public part of the policy, the private important information the users want to check and the secretvalues each user owns that assess the membership to the languages. They provide an ideal functionality for LAKE and giveefficient realiza-tions of the new primitive secure under classical mild assumptions, in the standard model with a common-reference string, with static corruptions. They signifi-cantly improve the efficiency of several CAKE protocol for specificlanguages and enlarge the set of languages for which they construct practical schemes. Notably, they obtain a very practicalrealization of Secret Hand-shakes and a Verifier-based Password-Authenticated Key Exchange.

Existing system:

Key-exchange, in particular Diffie–Hellman keyexchange(DHKE), is among the core cryptographic mechanismsfor ensuring network security. For key-ex-change over theInternet, both security and privacy are desired.

PROPOSED WORK/METHODOLOGY:

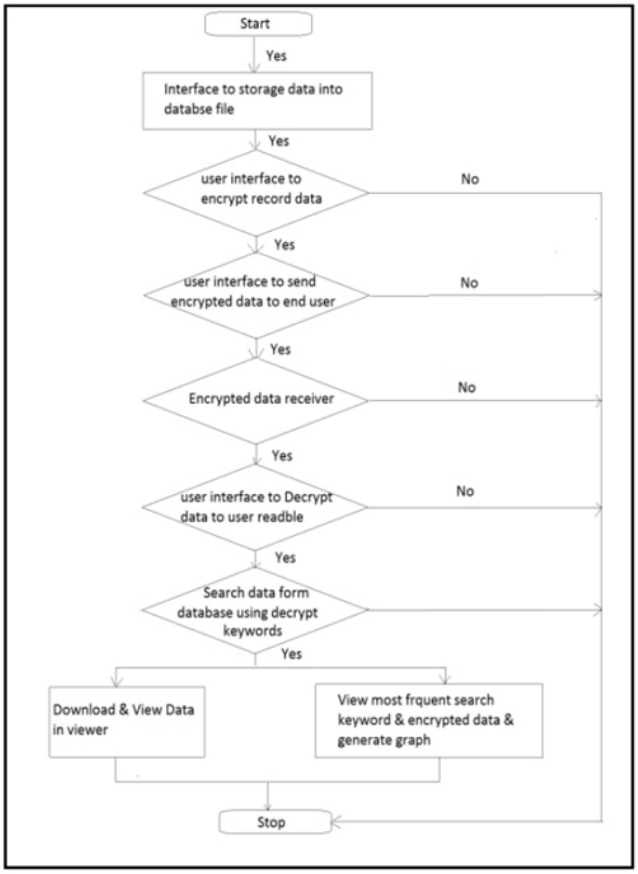
In this section we will see how to protect the key from the intruder and how to ensure privacy for both proto-col participants. The privacy preserving method is used for the security providing mechanism. In the Internet there is one storage media for store the data and that storage is used to store all 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 tech-nique 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. Basi-cally 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

Data Flow Diagram:



CONCLUSION:

The problem of key exchange has not yet been solved. In particular, it has not yet been solved for the modern situation of two previously unknown users attempting to communicate electronically, as, for instance, in electronic commerce. Some of the existing work-around designs work, more or less, but are not fully satisfactory.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 keyand both protocol participant.

References:

1. Andrew Chi-Chih Yao and Yunlei Zhao"Privacy-Preserving Authenticated Key-Exchange Over Internet" IEEE TRANSACTIONS ON INFORMATIONFORENSICS 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, TsinghuaUniversity, 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 forAlgebraic Languages" 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC '13) 1 March 2013, Nara, Japan) KaoruKurosawa 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 REAAlgorithm" 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 andInformation 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

11. C. J. F. Cremers, "Formally and practically relating the CK, CK-HMQV, and eCK security models for authenticated key exchange," IACR (TheInternational 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 SecurityProtocols", 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.