Password Authentication Key Exchange Mechanism using Identity Based System

R. A. Tijare, Prof. V. B. Gadicha

1) ME (CSE) Scholar, P.R.Pote College of Engg & Management, Amravati, India.

2) Head of Department (CSE), P.R.Pote College of Engg & Management, Amravati, India.

Abstract- In digital world various authentication techniques are used, password authentication is one of the traditional technique. Many improvements are made in password authentication techniques as only password authentication cannot withstand today's attack. One of the password authentication technique is two-server password authentication. In two-server password-authenticated key exchange (PAKE) protocol, a client splits its password and stores two shares of its password in the two servers, respectively, and the two servers then cooperate to authenticate the client without knowing the password of the client. In case one server is compromised by an adversary, the password of the client is required to remain secure. Research work proposed two servers that stores two shares of identity password in encrypted format. The two shares of passwords will be stored in such a way that identity password will be reformed with the help of any user defined algorithm. Along with password authentication, here idea is to implement identity based on encryption technique to encrypt the documents and messages. Proposed system will prevent dictionary, shoulder surfing, and key logger attacks.

Keywords:-*Password-authenticated, key exchange, identity-based encryption.*

*****

I. Introduction

To secure communications between two parties, an authenticated encryption key is required to agree on in advance. So far, two models have existed for authenticated key exchange. One model assumes that two parties already share some cryptographically-strong information: either a secret key which can be used for encryption/authentication of messages, or a public key which can be used for encryption/ signing of messages. These keys are random and hard to remember. In practice, a user often keeps his keys in a personal device protected by a password/PIN. Another model assumes that users, without help of personal devices, are only capable of storing "human-memorable" passwords. Bellovin and Merritt [4] were the first to introduce password-based authenticated key exchange (PAKE), where two parties, based only on their knowledge of a password, establish a cryptographic key by exchange of messages. A PAKE protocol has to be immune to on-line and off-line dictionary attacks.

In an off-line dictionary attack, an adversary exhaustively tries all possible passwords in a dictionary in order to determine the password of the client on the basis of the exchanged messages. In on-line dictionary attack, an adversary simply attempts to login repeatedly, trying each possible password. By cryptographic means only, none of PAKE protocols can prevent on-line dictionary attacks. Since Bellovin and Merritt [4] introduced the idea of PAKE, numerous PAKE protocols have been proposed. With the increased use and sharing of the information in today's world of networking, the security of this data has become a very serious problem. In the single-server setting, all the passwords necessary to authenticate clients are stored in a single server. If the server is compromised, due to, for example, hacking or even insider attacks, passwords stored in the server are all disclosed. This is also true to Kerberos [12], where a user authenticates against the authentication server with his username and password and obtains a token to authenticate against the service server. PAKE using identity based systems are used to counter the problem.

II. Literature Survey

Security of the user message and document without violating the secrecy of the information are the major requirements of the Password Authentication Key Exchange Mechanisms today. It is difficult to achieve security within the same network. This work focuses on maximizing security on identity basis. People pick bad password, and either forget, write down, or resent good ones.[4] Unfortunately, only password is not enough, it may lead to attack. Password-based encrypted key exchange protocols are design to provide security to a pair of user communicating on unreliable channel with a secure session key even when the secret key or password shared between two users is drawn from a small set of values. [2]

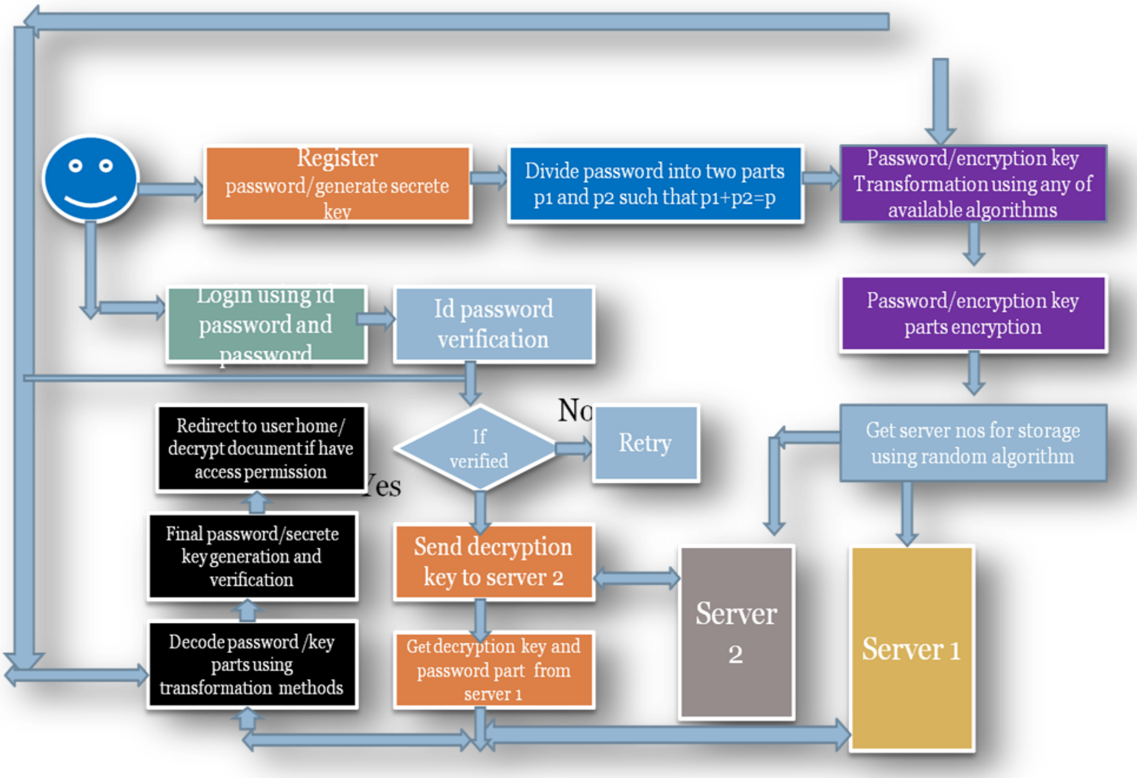
In the single-server setting, all the passwords necessary to authenticate clients are stored in a single server. If the server is compromised, passwords stored in the server are all disclosed. To counter the problem multi-server setting for PAKE was suggested where the password of the client is distributed in n servers. [14], [15]. A formal model of security for two-server

PAKE was given by Katz et al. [16]. Boneh and Franklin [7] defined chosen cipher text security for IBE under chosen identity attack.

Earlier password-based authentication systems transmitted a cryptographic hash of the password over a public channel which makes the hash value accessible to an attacker. When this is done, and it is very common, the attacker can work offline, rapidly testing possible password against the true password's hash value. Studies have consistently shown that a large fraction of user-chosen passwords are readily guessed automatically. Combining the two models, a model for ID PAKE protocol was given [18] and can be described as Participants, Initialization and Passwords.

III. Proposed work

Various techniques have been discussed based upon the comparison of schemes, proposed system has been developed that is PAKE using identity based system which overcomes the drawback of previous schemes. The detail working of Password Authentication Key Exchange using Identity Based System is shown in the figure


Register password/generate secrete key
Divide password into two parts p1 and p2 such that p1+p2=p
Password/encryption key Transformation using any of available algorithms
Login using id password and password
Id password verification
Password/encryption key parts encryption
Redirect to user home/ decrypt document if have access permission
If verified
No
Retry
Yes
Get server nos for storage using random algorithm
Final password/secrete key generation and verification
Send decryption key to server 2
Server 2
Server 1
Decode password /key parts using transformation methods
Get decryption key and password part from server 1

3.2.1: Working of PAKE

Working of proposed Identity Based System

STEP I: At the time of registration, user will get identity password, User have to specify id password at the time of file download.

STEP II: Identity password will be generated with the help of user's personal information

STEP III: Identity password will be automatically generated using user defined idpass generator algorithms.

Working of proposed Password Authentication Key Exchange Protocol

STEP 1: In PAKE, user's password and encryption keys will be stored on two servers System will split out the given password in two shares

STEP 2: The separated shares will be transformed using any of user defined algorithms

STEP 3: Transformed shares will be encrypted using users identity and then stored on two servers

STEP 4: When user comes for authentication, user have to specify his identity password along with his password

STEP 5: If identity password is correct, server 1 will send key token to decrypt part of password stored on server 2 and vice versa

STEP 6: The decrypted password parts then decoded using transformation method used previously

STEP 7: Then the two parts will be combined to get single password

STEP 8: If the password matches with user specified password, user will be considered as authenticated

STEP 9: user have to specify correct id password and password within 3 attempts, otherwise the account will get locked.

IV. Conclusion

The internet has become most important medium now a day for performing almost everyday tasks. Therefore huge amount of Data Lake are being created every day. Multinational companies are using technologies like cloud computing for their business. So management of information has been difficult by traditional security. With the use of PAKE using IBS security management has become easy. Huge amount of data handling can be done without worrying about intruders, both from inside and outside. By implementing PAKE using IBS improvement in security management can be done.

References

[1] M. Abdalla, P. A. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In Proc. PKC’05, pages 65-84, 2005.

[2] M. Abdalla and D. Pointcheval. Simple password-based encrypted key exchange protocols. In Proc. CT-RSA 2005, pages 191-208, 2005..

[3] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Proc. Eurocrypt’00, pages 139-155, 2000.

[4] S. M. Bellovin and M. Merritt. Encrypted key exchange: Passwordbased protocol secure against dictionary attack. In Proc. 1992 IEEE Symposium on Research in Security and Privacy, pages 72-84, 1992.

[5] J. Bender, M. Fischlin, and D. Kugler. Security analysis of the PACE key-agreement protocol. In Proc. ISC’09, pages 33-48, 2009.

[6] J. Bender, M. Fischlin, and D. Kugler. The PACEjCA protocol for machine readable travel documents. In INTRUST’13, pages 17-35, 2013.

[7] D. Boneh and M. Franklin. Identity based encryption from theWeil pairing. In Proc. Crypto’01, pages 213-229, 2001.

[8] V. Boyko, P. Mackenzie, and S. Patel. Provably secure passwordauthenticated key exchange using Diffie-Hellman. In Proc. Eurocrypt’ 00, pages 156-171, 2000.

[9] J. Brainard, A. Juels, B. Kaliski, and M. Szydlo. Nightingale: A new two-server approach for authentication with short secrets. InProc. 12th USENIX Security Symp., pages 201-213, 2003.

[10] E. Bresson, O. Chevassut, and D. Pointcheval. Security proofs for an efficient password-based key exchange. In Proc. CCS’03, pages 241-250, 2003.

[11] E. Bresson, O. Chevassut, and D. Pointcheval. New security results on encrypted key exchange. In Proc. PKC’04, pages 145-158, 2004.

[12] B. Clifford Neuman and Theodore Ts’o. Kerberos: An authentication service for computer networks. IEEE Communications, 32 (9): 33-38, 1994.

[13] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Proc.Crypto’98, pages 13-25, 1998.

[14] W. Diffie and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 32(2): 644-654, 1976.

[15] W. Ford and B. S. Kaliski. Server-assisted generation of a strong secret from a password. In Proc. 5th IEEE Intl. Workshop on Enterprise Security, 2000.

[16] D. Jablon. Password authentication using multiple servers. In Proc. CT-RSA’01, pages 344-360, 2001.

[17] J. Katz, P. MacKenzie, G. Taban, and V. Gligor. Two-server password-only authenticated key exchange. In Proc. ACNS’05, pages 1-16, 2005.

[18] X. Yi, R. Tso and E. Okamoto. ID-based group password authenticated key exchange. In Proc. IWSEC’09, pages 192-211, 2009.

[19] X. Yi, F. Hao and E. Bertino. ID-based two-server password authenticated key exchange. In ESORICS’14, pages 257-276, 2014.