International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Survey on Three-Party Password-Based Authenticated Key Exchange (3-PAKE) Protocols

Shivani Bhatia[1], Rekha Saraswat[2]

[1, 2] Centre for Development of Advanced Computing(CDAC), B-30, Sector-62, Institution Area, Noida –201307, Uttar Pradesh ,India

Abstract: ***Cryptographic protocols for key exchange have an aim of secure exchange of secret keys over the public network. Password based authenticated key exchange (PAKE) protocols are popularly used for communication purposes due to their convenience. As the name suggests, it involves sharing of a human-memorable password by each entity with a trusted third party. Three party PAKE (3-PAKE) protocols allow two parties to authenticate each other via the trusted third party and establish a session key between them for further communication. Various 3-PAKE protocols have been proposed over the years, each having its own weaknesses and strengths. This paper presents a review of few such 3-PAKE protocols and gives suggestions for future enhancements.***

Keywords: key-exchange, authentication, password**,** three-party

1. Introduction

For communicating securely over an adversary controlled public network, it is essential that secret keys are exchanged securely. Two parties can encrypt their messages and authenticate each other's identitiesin order to protect the information. Public key encryption schemes and signatures can be used but these schemes might lead to higher cost for certain applications. Another way of communicating securely is to first establish a common secret key via a key exchange protocol and then use this key to derive keys for symmetric encryption and message authentication schemes.[1]

Password based key exchange protocols assume a practical scenario in which the secret keys are not distributed over a large set but, chosen from a small set of possible values. They also provide more convenience because human-memorable passwords are easier to use than random cryptographic keys which might need specialized hardware for storage or generating of keys.[1]

1.1 Three party password based authenticated key exchange

Passwords are used mostly as they are easier to remember than high entropy secret keys. Moreover, users prefer to remember a few passwords only. In situations, where one user wants to communicate with multiple other users, he has to remember passwords directly proportional to the number of possible partners[1] In order to minimize the number of passwords each user has to remember, a3- party model is considered in which each user only shares a password with a trusted server. The main advantage of this solution is that it provides each user a capability to communicate securing with many other users while requiring to remember only one password. This provides a more realistic situation.

3-PAKEprotocols can be used for various applications which require mutual authentication and secure communication, like a buyer and seller in e-commerce where a trusted server helps in transactions etc.[7]

One disadvantage of a 3-party model is that the privacy of communication with respect to the server is not always guaranteed. The key exchange should take place in such a way that even though server participates in establishing a session key, it should not be able to gain any information on the value of that session key. Key privacy should be guaranteed.

The paper is organized as follows. In section 2, various security requirements for PAKE protocols are listed. Section 3 provides an overview of various protocols and their comparison. The paper ends with a conclusion in Section 4.

2. Security Requirements of PAKE

The key exchange protocols should satisfy various security requirements:[7]

- **Session key security**: The session key established by the protocol should only be known by the parties who are communicating with each other.
- **Perfect forward secrecy**: It is the property that a session key derived from a set of long term keys will not be compromised if one of the long term key is compromised in the future. Even if the password is disclosed, it doesn't reveal prior recorded information.

The common protocol attacks can be summarized as follows:[7]

- **Man in the middle attack**: The attacker makes independent connections with the victims and communicates with them, fooling them that they are talking to each other over a private connection,whereas their entire conversation is monitored by the attacker. The attacker impersonates as both the clients to the satisfaction of the other.
- **Replay attack**: The attacker simply takes a previously sent message and sends it again or can even delay the messages.
- **Offline dictionary attack**: The attacker eavesdrops the information, guesses the value of the password and verifies its correctness in an offline manner. There is no limitation on the number of guesses. Since no client/server participation is required, these attacks cannot be noticed.

- **Undetectable online dictionary attack**: The attacker tries to verify the guessed password in an online manner. But here, a failed guess is never noticed by the server and the client, hence the attacker can check many times to get sufficient information on the password.
- **Detectable online dictionary attack**: The attacker verifies the guessed password in an online manner using responses from the server, like above, but here the failed guess can be distinguished from an honest request.
- **Mutual Authentication**: The communicating parties should be authenticated by the server as well as authenticated among themselves.

3. Review of 3-PAKE Protocols

The discovery of PAKE protocols started back in 1992 when the first two-party key exchange protocol was presented by Bellovin et al. After that, many two party protocols were discovered. But 2-PAKE protocols posed a disadvantage of the recollection of huge number of passwords by every client, hence offering a limited scope. 3-PAKE protocols overcame this limitation by introducing a trusted third party with which each user shares a password. Hence each user needs to remember only one password while communicating with any number of users. A number of 3-party protocols have been proposed but still some issues need to be addressed like secure authentication of clients when the password is low-entropy, believing that the trusted third party is not an attacker, dictionary attacks etc.

The following sub-section presents some notations and terminologies used for the protocols followed by a brief overview of some 3-PAKE protocols in the subsequent sub-sections.

3.1 Notations

A,B : Identity of clients A and B
S: Identity of server
p: a large prime number
g: a generator of order p
G: finite cyclic group with generator g
H(..), H'(..) : Secure one-way hash functions
M,N : two elements in G
s: private key of server
g^s: public key of server
pwa: password shared by A with S
pwb: password shared by B with S
$\{M\}_k$ or $E_k(M)$: Encryption of message M with key k

3.2 Simple three-party key exchange protocol

Lu and Cao [6], proposed a threeparty protocol in 2007, known as S-3PAKE based on chosen-based computational Diffie-Hellman (CCDH) assumption. It is a variation of the computational Diffie- Hellman (CDH) problem. The protocol is described as follows:

Step 1:
A1: A chooses a random number x∈Zq and computes $X=g^{x}.M^{pwa}$, then sends A||X to B.
B1: B also chooses a random number y∈Zp and computes $Y=g^{y}.N^{pwb}$, then sends A||X||B||Y to S.

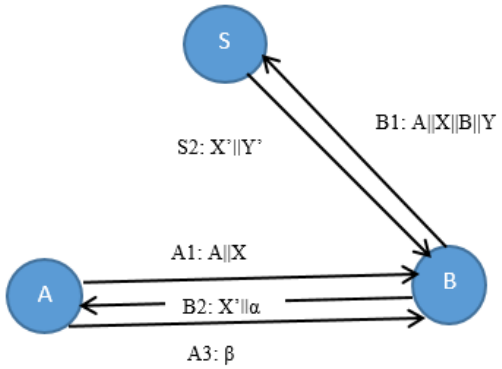

Figure 1: S-3PAKE protocol

Step 2:
S2: upon receiving A||X||B||Y, the server S first uses the passwords pwa and pwb to compute $g^{x}=X/M^{pwa}$ and $g^{y}=Y/N^{pwb}$, respectively. Then, she chooses another random number z∈Zp and computes g^{xz}, g^{yz}. Finally, she sends X'||Y' to B, where $X'=g^{yz}.H(A, S, g^{x})^{pwa}$and $Y'=g^{xz}.H(B,S,g^{y})^{pwb}$.
B2: when B receives X'||Y', he uses the password pwb to computeg^{xz}= Y'/ $H(B,S,g^{y})^{pwb}$ and uses the random number y to compute g^{xyz}. At last, he forwards X'||α to A, where α= $H(A,B,g^{xyz})$

Step 3:
A3: after A receives X||α , she first computes g^{yz}=X'/ H(A, S, $g^{x})^{pwa}$ and g^{xyz}. Then, she checks whether α= $H(A,B,g^{xyz})$ holds or not. If it does not hold, A terminates the protocol. Otherwise, she is convinced that $g^{xyz}$is valid. She can compute the session key $SK_A = H'(A,B,g^{xyz})$ and returns β= $H(B,A,g^{xyz})$ to B for validation.
B3: upon receiving β,B checks whether β= $H(B,A,g^{xyz})$ holds or not. If it holds, B can compute the session key SK_B= $H'(A,B,g^{xyz})$. Otherwise, he terminates the protocol.

The main design goal of S-3PAKE was to provide both security and efficiency without the use of server's public key. The authors discussed various security aspects which their protocol fulfills and proved that it resists online and offline dictionary attacks and replay attacks along with providing perfect forward secrecy. Comparison of S-3PAKE was done with Round-efficient 3-PAKE protocol proposed by Lee et.al in 2004 and it was concluded that S-3PAKE required lesser number of calculations than Lee's protocol.

3.3 Enhanced Password-Based Simple Three-Party Key Exchange Protocol

In 2009, Kim and Choi [4] found out that S-3PAKE was still suffering from undetectable online dictionary attacks, contradicting the claims of the authors. They analyzed the protocol in a formal model and pointed out that the weakness occurs because messages of the communicants are not properly encrypted into the exchanged cryptographic messages.

The authors have illustrated a detailed analysis of the S-3PAKE protocol and proved that any legitimate client registered with the server can mount attacks. A new protocol is formulated, STPKE', in which countermeasures are

provided to resist the attacks, while retaining the advantages of the original protocol. The changes suggested are: For preventing the undetectable on-line guessing attacks, bit-wise exclusive OR operation is introduced for calculation of X and Y. Also ,to prevent man-in-the-middle attack, generator element is introduced for disguising the identifiers ID_A and ID_B, which are introduced as input parameters for computing X' and Y' respectively as :

$X = (g^x \oplus g^a) .M^{pwa}$
$ID'_A = ID_A . g^a$
$Y = (g^y \oplus g^b) .N^{pwb}$
$ID'_B = ID_B . g^b$
$X' = g^{yz} .H(ID'_A, ID'_B, ID_S, g^x)^{pwa}$
$Y' = g^{xz} .H(ID'_B, ID'_A, ID_S, g^y)^{pwb}$

Though the suggested changes succeed in removing the attacks, they also increase the computational complexity of the protocol.

3.4 A Novel Three-Party Authenticated Key Exchange Protocol Using One-Time Key

Chao Lv et al. [7] proposed N-3PAKE protocolin 2013 without using server's public key. This protocol was on the lines of Diffie-Hellman key exchange. Compared to the above mentioned two protocols, this protocol is simpler in terms of cryptographic operations. The protocol description is as follows:
$RQ_a = A, g^x, \{A, g^x\}_{H(A, g^x, pwa)}$
$RQ_b = B, g^y, \{B, g^y, N_b\}_{H(B, g^y, pwb)}$
$AK_a = \{g^x, B, g^{yz}, N_b\}_{H(A, g^x, pwa)}$
$AK_b = \{g^y, A, g^{xz}\}_{H(B, g^y, pwb)}$

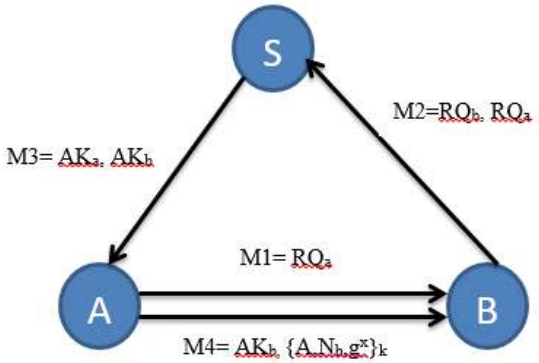

Figure 2: N-3PAKE protocol

The value of key k is calculated as $k = g^{xyz}$ for further communication between A and B.The authors claimed that protocol satisfies the properties of mutual authentication, perfect forward secrecy and session key security. It also resists attacks like replay attacks, man in the middle attack, online and offline dictionary attacks.The authors claimed that protocol has the properties of mutual authentication, perfect forward secrecy and session key security. It also resists attacks like replay attacks, man in the middle attack, online and offline dictionary attacks.

Formal verification of the protocol was shown using AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. The protocol was compared to four other existing schemes on the basis of various performance parameters.

3.5 Strongly Password Based Three Party Authenticated Key Exchange Protocol

Lin, Hou and Xu [5] analyzed the N-3PAKE protocol mentioned above and found it to be secure in case of passive adversary, but when active adversary was present, it was vulnerable to offline dictionary attacks, key compromise impersonation attacks and unknown key sharing attacks.

The authors proposed an improved protocol LHX-3PAKE-1 whose description is as follows:
$RQ_A = A, g^x, H(A, g^{xs}, pw_a)$
$RQ_B = B, g^y, H(B, g^{ys}, pw_b)$
$AK_A = B, g^y, H(A, B, g^y, g^{xs}, pw_a)$
$AK_B = A, g^x, H(B, A, g^x, g^{ys}, pw_b)$
B verifies AK_B and A verifies AK_A.

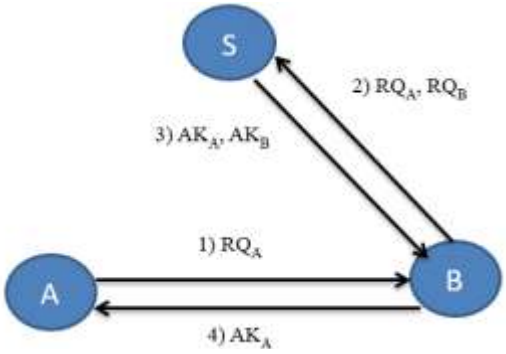

Figure 3: LHX-3PAKE-1 protocol

The session key value calculated = g^{xy}.The protocol exhibits advantages of resisting online dictionary attacks, offline dictionary attacks, man in the middle attack, replay attack, key compromise impersonation attacks, unknown key sharing attacks and ensures perfect forward security and known session key security.

The authors also give suggestions for resisting denial-of-service attacks by pre-calculating challenge response pairs(x, g^x), and storing the value of password as encrypted with the secret key $\{pw\}_s$ in case of server database compromise. If the server was to store the transformation of passwords f(pw) such as g^{pw}or H(pw), LHX-3PAKE-1 would give way to a variant LHX-3PAKE-2 in which 'pw' parameter in the arguments of RQ_A, RQ_B,AK_A,AK_B would be replaced by f(pw).

3.6Three Party Password Based Authenticated Key Establishment Protocol Resisting Detectable Online Attacks

CAPTCHA (Completely Automated public Turing test to tell Computers and Humans Apart) is a program that can grade tests that most humans can pass but current computer program cannot do. Many internet companies like Yahoo, Microsoft have also used captcha schemes to prevent free accounts from being registered by machine alone. [10]

This protocol follows a different approach than other schemes mentioned above. The protocol is WH-3PAKE whose security is based on both the difficulties of the computational Diffie-Hellman problem and a hard artificial

intelligence problem. In the protocol, ψ(r,t) is a distorted picture function and specific CAPTCHA scheme wherer € Ωn, Ω is the set of all 52 upper case and lower case characters and 10 digits, Ωn is the set of all strings of symbols in Ω of length n, and t is a random integer to generate a random distorted picture function of r such that people can recognize r from the picture but machines cannot. ψ(r,t1) and ψ(r,t2) are different to machines due to different values of t1 and t2,but to humans they are the same string.[10]

The description of the protocol is as follows:

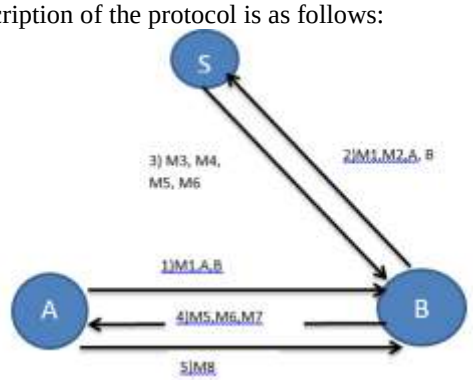

Figure 4: WH-3PAKE protocol

M1= Epwa(g^x)
M2= Epwb(g^y)
K_{AS}= g^{xs1}, K_{BS}= g^{ys2}, M3= E_{KBS}(ψ(r,t1)),
M4= E_{pwb} (g^{s2}), M5=E_{KAS} (ψ(r, t2)),
M6= E_{pwa} (g^{s1})
M7= H (1||r||B||A)
M8= H (1||r||A||B)

Value of session key is calculated as sk=H (2||r||A||B). The advantages of protocol is that it resists the continual detectable and undetectable online attacks on the clients as well as trusted serverbeing participators ,the complexities of client side computing and communication are reduced largely. So this protocol is well suited for mobile or light-weight clients. Also the perfect forward secrecy is ensured.

The authors concluded the paper by comparing the protocol with some existing schemes of three-party setting and stating that none of the schemes proposed take into account the human being's abilities different from machines which have an impact on the efficiency and security of the protocol.

4. Performance Comparison

Considering the efficiency and security of the protocols, the steps required for execution and the complexity of cryptographic operations are used to measure the performance of the proposed schemes. The higher the computation cost, the greater the time required by the two parties to establish secure communication, which is a drawback. Thus, developing a low cost 3-PAKE protocol needs to take into account the computation complexity, number of steps and security properties. Table 1,summarizes the various the protocols on the parameters such as modular exponentiations, no. of times hash function needs to be calculated, no. of XOR operations, communication steps, random numbers, encryptions and decryptions for public key and private key.

5. Conclusion

The various three party methods of key exchange allow the two clients to establish a symmetric key between them. This key can be used to encrypt and decrypt further communication between the clients.

Table 1: Performance comparison

Parameter → Protocol ↓	Modular exponentiations	Hash functions	Pseudorandom numbers	Public key en/decryption	Private key en/decryption	XOR operations	No.of steps
S-3PAKE	10	8	3	0	0	0	5
STPKE'	12	10	5	0	0	4	5
N-3PAKE	6	4	4	0	10	0	4
LHX-3-PAKE-1	8	8	3	0	0	0	4
WH-PAKE	8	6	7	0	16	0	5

Though the methods provide security and efficiency but also pose a disadvantage in case of multiple communication sessions between the same pair of clients. Every time the complex process of key generation is carried out while communication. Like during communication on SSL, abbreviated handshake with previous session resume can save resources.Since the secret key value calculated is not travelling through the network even once and remains secure with the clients (assuming personal secrecy), the efficiency of key exchange algorithm can be increased by reusing the value of the key for subsequent sessions and providing authentication during each session establishment. This would reduce the number of complex and costly calculations to be performed at the client and server side.Hence a mechanism needs to be developed which allows for the reuse of the secret key in a particular time interval yet ensuring authenticity of the clients.

References

[1] Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval, "Password-Based Authenticated Key Exchange in the Three-Party Setting", IEEE Proceedings on InformationSecurity, Volume 153, number 1, March 2006 , pp. 27-39.
[2] Whitefield Diffie, Martin E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, pp. 644-654,1976.

[3] Behrouz A. Forouzan, Cryptography and network security, Tata McGraw-Hill, 2007.
[4] Hyun-SeokKim ,Jin-Young Choi, "Enhanced password-based simple three-party key exchange protocol", Elsevier, Computers and Electrical Engineering, 35, pp.107–114,2009.
[5] Yuanhui Lin, MengboHou, Qiuliang Xu, "Strongly password based three party authenticated key exchange protocol", Ninth International conference on Computational Intelligence and security, IEEE, pp. 555-558,2013.
[6] Rongxing Lu, Zhenfu Cao, "Simple three-party key exchange protocol", Elsevier, computers & security 26, pp. 94-97,2007.
[7] Chao Lv , MaodeMab, Hui Li, JianfengMaa, Yaoyu Zhang, "An novel three-party authenticated key exchange protocol using one-time key", Elsevier, Journal of Network and Computer Applications (36), pp. 498–503,2013.
[8] Alfred Menezes, BerkantUstaoglu, "On reusing ephemeral keys in Diffie Hellman key agreement protocol",International Journal of Applied Cryptography,ACM,pp. 154-158, 2010.
[9] Tang, Wen, "A simple three party password based key exchange protocol", International Conference on Mechanical and Electrical Technology, IEEE, pp. 730-732, 2010.
[10] Wejia Wang, Lei Hu, "Three party password-based authenticated key establishment protocol resisting detectable online attack", Advances in information sciences and service sciences (AISS), pp. 680-687, 2013.
[11] Shuhua Wu, Kefei Chen, and Yuefei Zhu, "Enhancements of a Three-Party Password-Based Authenticated Key Exchange Protocol", The International Arab Journal of Information Technology, Vol. 10, No. 3, pp. 215-221,2013.

Author Profile

Ms. RekhaSaraswatreceived her MCA degree from Uttar Pradesh Technical University in 2004. She joined CDAC Noida in 2006 and then completed her MS degree from BITS,Pilani in 2010. She currently works as an Assistant Professor in CDAC, Noida. Her research interests include network security, information security and image processing.

Shivani Bhatia completed her B.Tech in Electronics & Communication from Maharishi Dayanand University, Rohtak in 2013. She is currently pursuing M. Tech in Information Technology from CDAC Noida. Her research interests include cryptography and network security.