International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 6, Issue 4, April 2017 **ISSN 2319 - 4847**

Survey on 3-PAKE Protocols in Cryptography

[#1]Gayathri Narayanan, [#2]Dr.Vince Paul and [#3]Dr.R.Satheesh Kumar

[#1]PG-Scholar, [#2] Professor and [#3]Associate Professor

Department of CSE, Sahrdaya College of Engineering and Technology, Kerala

Abstract

In crypography certain key exchange protocols are used for the secure exchange of secret and message.One such method is password authenticated key exchange protocol.This allows the user to easily remember the password which is selected from a small set than a random cryptographic key..3PAKE allow the user to rembember only one key and communicate with multiple users.We already have a number of key exchange protocols,each is developed as a enchanced version of previous protocol by solving its disadvantage.This paper gives a review on 3pake protocols .

Keywords— Three party,password,key exchange,authentication, reusability

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 in order to protect the data either by using Public key encryption schemes and signatures which might lead to higher cost for certain applications or by first establishing a common mystery key by means of a key trade convention and after that utilization this key to infer keys for symmetric encryption and message authentication.

Password based key exchange protocols assume a practical scenario in which the secret keys are selected from a small set of possible values,instead of distributed over a large space.

They also provide more convenience because human memorable passwords are simpler to use than irregular cryptographic keys which may require particular equipment for capacity or generating of keys.

THREE PARTY PASSWORD BASED KEY EXCHANGE

Three party password based key exchange is based on the concept that the passwords are easier to remember than high entropy keys.But here comes a problem in case of multiple communication.To make a communication between a user with multiple partners then this user want to remember seperate password for different partners.so inorder to reduce the number of passords directly proportional to the number of partners a three party model is introduced.Here each user shares a passsword with a trusted server which allow the user to communicate with multiple partners by remembering only one password.But this model not posess privacy with respect to server.but key privacy must be guarenteed by restricting the server from gaining the information about session key.

Initally a limited scope providing client-client model named 2PAKE is intoduced which then give way to 3PAKE client-client-server model more suitable for communicating environments.

2. REVIEW

I) ENHANCED PASSWORD-BASED SIMPLE THREE-PARTY KEY EXCHANGE PROTOCOL

In 2009, Hyun seok Kim and Jin young Choi [4] found out that S-3PAKE was still suffering from undetectable online dictionary attacks,against the claims of the authors. Analysis of protocols is done and found that the disadvantage is occur due to the improper translation of message to cipher text.

The authors also provided a detailed analysis of the S-3PAKE protocol and proved that any authorized client registered with the server can mount attacks. A new protocol is introduced as "STPKE", in which countermeasures are provided to resist the attacks,by keeping the advantages of the original protocol. The changes suggested are: to prevent the undetectable on-line guessing attacks, bitwise exclusive OR operation is introduced for calculation of X and Y. Also , for preventing 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.

II) Enhancement of a Three-Party Password-Based Authenticated Key Exchange Protocol

In 2013,shuhua wu,kefei chen,and yuefei zhu, found that a simple and efficient key exchange protocol proposed by Huang is still vulnerable to three kinds of attacks:
1).undetectable on-line dictionary attacks, and 2). key-compromise impersonation attack. Thereafter they have proposed an enhanced protocol that can defeat the attacks described and that was reasonably efficient.The enhanced protocol is as follows:

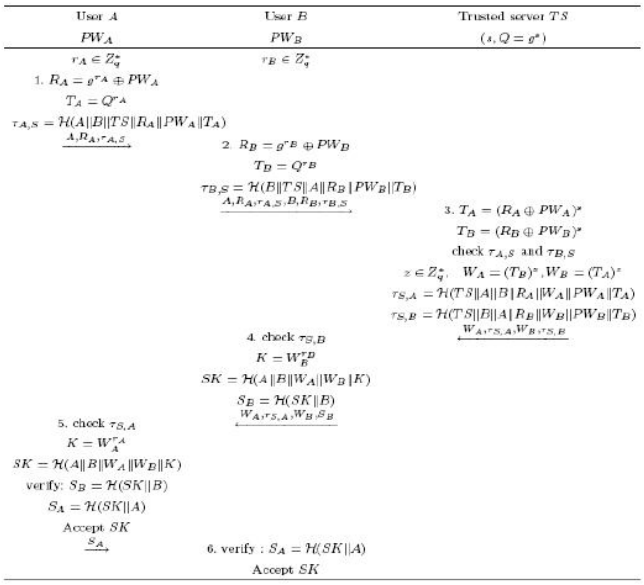


Fig. 1 Enhanced protocol

III) A Novel Three-Party Authenticated Key Exchange Protocol Using one time key

In 2013,Chao LV et al. proposed a low cost three party key exchange protocol named N-3PAKE protocol based on Diffie Hellman key exchange CDH assumption.the authors claimed that it to be secure and faster than some of the existing protocols.

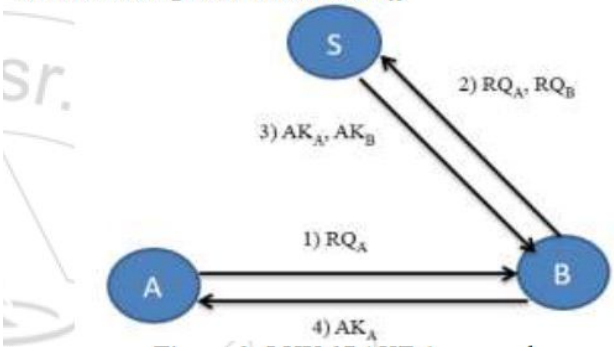
$$M1.\quad A \to B: \quad \underbrace{A, g^x, \{A, g^x\}_{H(A,g^x,pw_a)}}_{RQ_A}$$
$$M2.\quad B \to S: \quad \underbrace{B, g^y, \{B, g^y, N_b\}_{H(B,g^y,pw_b)}}_{RQ_B}, RQ_A$$
$$M3.\quad S \to A: \quad \underbrace{\{g^x, B, g^{yz}, N_b\}_{H(A,g^x,pw_a)}}_{AK_A}, \underbrace{\{g^y, A, g^{xz}\}_{H(B,g^y,pw_b)}}_{AK_B}$$
$$M4.\quad A \to B: \quad AK_B, \{A, N_b, g^x\}_K$$

This protocol fulfils the security requirements such as confidentiality of the secret key and the session key, mutual authentication between any two partners, and the freshness of the transmitted information or data and the session key with perfect forward secrecy.

IV)Strongly Password Based Three Party Authenticated Key Exchange Protocol

In 2013,Lin,Hou,Xu analysed the previous N-3PAKE protocol and he found that it is secure in case of passive adversaries but vulnerable in case of active adversaries.and also this N-3PAKE is failed to resist key impresonation attack,offline dictionary attack and unknown key sharing attack.so he proposed a new protocol that can overcome this attacks.

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.



he also provided experimental proofs and analysis for this procedure and also prove that it is a secure efficient and practical protocol and free from all well known attacks.

V) Session key Reusability Using 3PAKE in Symmetric Key Cryptography

In 2013, Shivani BhatiaRahul V. Anand proposed a system based on the LHX 3PAKE protocol.This protocol pose a disadvantage of costly an dtime consuming key generation.she suggested that since the session key is not travelling through the network even once and remains secure with the client so this key can be reused for consecutive session between same pair of clients.thus the user can have saving on time and reduce the complex modular exponential calculations for key generation.first phase protocol is similar to LHX 3PAKE protocol but a additional timestamp T is send from the server to client and second phase for reusability can be,

Step 1: A → B RQ_A=A, H(A, pw_a, T)

Step 2: B → S RQ_A, RQ_B=B, H(B, pw_b, T)

Step 3: S → B
AKB=A, H(A, B, pw_b, T), AK_A= B,H(B, A, pw_a,T)

Step 4: B → A AK_A

This protocol is free from most of the attacks like online and offline dictionary attacks,key compromise impersonation attack,forward security,man in the middle,unknown key sharing attack and database leakage.

3. CONCLUSIONS

Till now we have a number of a three party key exchange protocols for communicating securely with our partners.Each of them is proposed as a solution for its previous works .So by reusability of session key it is almost solved the issues o f multiple communication and reduced the time consuming and complex key calculations also.But that is also pose a drawback in the case of database access.So it is essential to develop a model that can reduce the database access time as well as reducing time for connecting to the database for the first time and storage of details.

References

[1] Shivani BhatiaRahul V. Anand, Session Key Reusability Using 3-Pake in symmetric key cryptography , iInternational Conference on Soft Computing Techniques and Implementations,2015
[2]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
[3] Chao Lv , Maode Mab, 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
[4] 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, May 2013
[5] Wejia Wang, Lei Hu, Three party password-based authenticated key establishment protocol resisting detectable ouline attacks, Advances in information sciences and service sciences(AISS), pp: 680-687,2013

[6] Hyun-Seok Kim , Jin-Young Choi, Enhanced password- based simplethree-party key exchange protocol, Elsevier, Computers and Electrical Engineering 35, pp: I 07-114,2009
[7] Alfred Menezes, BerkantUstaoglu, "On reusing ephemeral keys in Diffie Hellman key agreement protocol", International Journal of Applied Cryptography,ACM,pp. 154-158, 2010.
[8] 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.
[9] Whitefield Diffie, Martin E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, pp: 644-654, 1976