ISSN No. 0976-5697

Volume 4, No. 11, Nov-Dec 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Weakness in 3pek Exchange Protocol using Parallel Message Transmission Technique

Archana Raghuvamshi
Assistant Professor
Department of Computer Science
Adikavi Nannaya University,
Rajahmundry,Andhra Pradesh
archana_raghuvamshir@yahoo.com

Prof.P.Premchand
Department of CSE
Osmania Univeristy
Hyderabad, Andhra Pradesh
University College of Engineering
profpremchand.p@gamil.com

Abstract: Three-party encrypted key (3pek) exchange protocol plays an obligatory role in area of the secure communication in which two users can agree a common session key based on a low entropy password. In 2002, a password authenticated key exchange protocol based on RSA proposed by Zhu et al.. Later, an undetectable password-guessing attacks has shown by Yeh et al. on this scheme and also has given solutions for improvement. Recently, Chang and Chang proposed a novel three party simple key exchange protocol. Later, an Undetectable online password guessing attack has shown on the above protocol by Yoon and Yoo. Recently, a password key exchange protocol PSRJ was proposed and also claimed to be in-vulnerable to Undetectable online password guessing attack proposed by Yoon and Yoo..A detectable online password guessing attack has shown on this scheme and has given solutions for improvement by Archana et al. in 2012.Later some other version of the 3pek exchange protocol using parallel message Trasmission Technique has been proposed and claimed to be vulnerable.In this paper, we review this protocol and analyze its robustness for security.

Keywords: 3pek exchange protocol, authentication, cryptanalysis, security, undetectable on-line dictionary attack.

I. INTRODUCTION

To achieve secure communication within intimidating network, 3Pek Exchange mechanism is widely set up on lots of remote user authentication system due to its simplicity and convenience of maintaining a human-memorable password at client side. In a normal 3PAKE protocol, each communication client shares an easy-to-remember password with a trusted server in advance. Once any two clients intend to establish a robust session key, both of them resort to the server and their shared passwords to authenticate each other. After that, only legitimate client can be authorized to derive the current session key.

Since Bellovin and Merrit [1] first proposed a two-party encrypted key exchange protocol based on user passwords, many two-party password-based authenticated key exchange (2PAKE) protocols have been investigated. However, the 2PAKE protocols are only suitable for client-server architecture [2]. This limitation inspires research community to extend 2PAKE protocols into 3PAKE schemes for three-party commu-nication environment, i.e. client-client-server model. The dictionary attack is a series of challenge-response malicious procedures in which adversary can iteratively try-and-guess the secret password of victim communication party until discovering the correct one. In general, the password guressing attacks are classified into three types [3].

1) ***Detectable on-line password guessing attacks:*** An intruder can use a guessed password in an on-line transaction. The correctness of the guessed password's can be verified by the intruder based on the server's response. With the failed logged procedure the attack would be detected by server.

2) ***Undetectable on-line password guessing attacks:*** This attack is similar to above attacks but the failed guessing procedure would not be detected by server. Hence, the server cannot distinguish an honest request from a malicious one.

3) ***Off-line password guessing attacks***: An intruder guesses a password and verifies his guess off-line. Server will not notice the attack; hence server participation is not required.

Inspite of many researchers [2-15] had focused on secure 3PAKE protocol most of them suffer from the different types of password guessing attacks. In 1995, an authentication protocol to improve the system efficiency of Bellovin and Merrit's mechanism by reducing the number of transmission rounds and cryptographic operation developed by Steiner et al. [4]. Unfortunately, the Y. Ding and P. Horster [5] and C.L. Lin, H.M. Sun and T. Hwang [6] had demonstrated that Steiner et al.'s scheme cannot resist against the undetectable on-line password guessing attack and off-line password guessing attack. To enhance its security, Lin et al. [6] adopted the public key cryptosystem technology to construct a remedy scheme. However, the computation cost of public key en/decryption is too high to be adopted in a 3PAKE protocol. Hence, Lee et al. [7] introduced two enhanced three-party en-crypted key exchange protocols to achieve mutual authentication and provide perfect forward secrecy in which the public key cryptosystem is not required. Later, Wen et al. [8] utilized weil pairing concept to establish a 3PAKE protocol with formal proof model. Nevertheless, Nam et al. [9] showed that Wen et al.'s protocol is vulnerable to a man-in-the-middle attack, and interpreted their proposed attack in the context of the formal proof model.

Designing a 3PAKE protocol which possesses both of system security and compu-tation efficiency is particularly a challenge due to the difficult tradeoff among security robustness, system performance and computation cost. In 2007, Lu and Cao [10] developed an S-3PAKE protocol to pursue the security requirements and the efficiency criteria. However, their protocol suffers from man-in-the-middle attacks and undetectable on-line dictionary attack [11 and 12]. Later, Chung and Ku [2] proposed a security enhanced S-3PAKE mechanism which is based on Lu and Cao's protocol. Nevertheless, Chung and Ku's protocol is not without its flaws. In this paper, we find that the S-3PAKE scheme proposed by Chung and Ku is insecure against the unde-tectable on-line dictionary attack in the presence of an active attacker. A remedy mechanism is then introduced to eliminate the identified vulnerability.

The rest of this paper is organized as follows. Security analysis of 3pek Exchange Protocol Using Parallel Message Transmission Technique is demonstrated in Section 2. In Section 3 we have shown a Detectable on-line password guessing attack on the 3pek Exchange Protocol Using Parallel Message Transmission Technique.Finally, the concluding remarks are summarized in Section 4..

II. SECURITY ANALYSIS OF 3PEK EXCHANGE PROTOCOL USING PARALLEL MESSAGE TRANSMISSION TECHNIQUE

In this section, we briefly review 3pek Exchange Protocol Using Parallel Message Transmission Technique and analyze its robustness, i.e. the resistance to undetectable on-line dictionary attack. Before that, we define some notations which will be utilized in this paper in Figure 1.

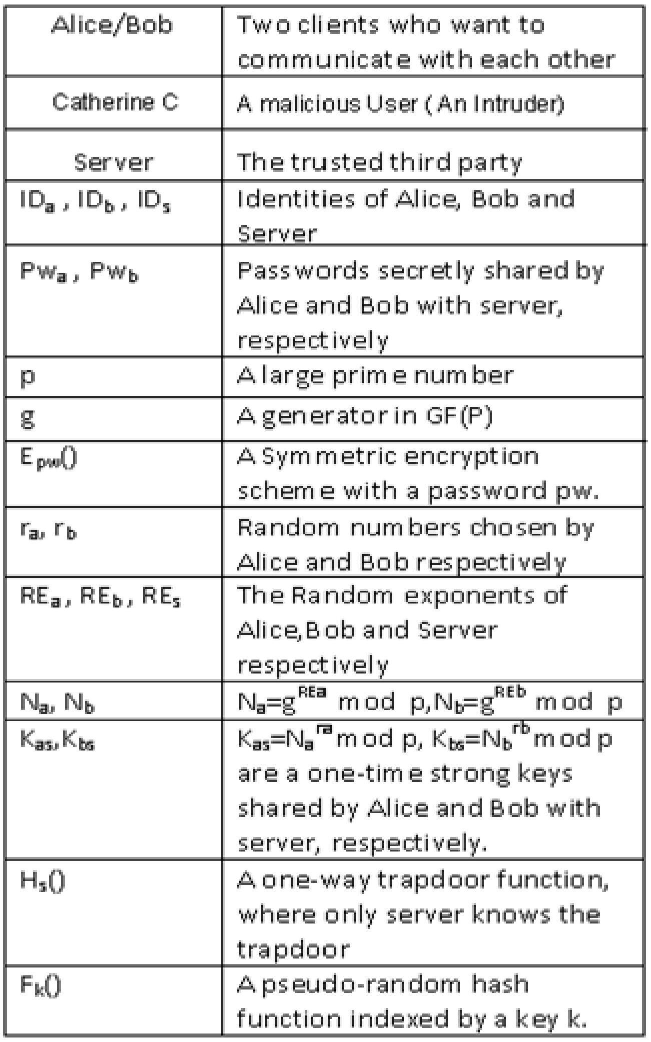
A 3pek exchange protocol using parallel message transmission technique is shown in Fig 2.The details are given below:

Step 1:
Alice A generates two random numbers r_a and RE_a and calculates E_{pwa} $(K_{AS}\oplus N_A)$, $H_S(N_A\oplus ID_a)$ and $F_{KAS}(N_A)$ $N_A=g^{REa}$(mod p) and $K_{as}=N_A^{ra}$ (mod p). Then Alice A sends {$ID_{a,}$ $ID_{b,}$ $ID_{s,}$ $E_{pwa}(K_{AS}\oplus N_A)$, $H_S(N_A\oplus ID_a)$,$F_{KAS}(N_a)$}To Server S.

Simultaniously, Bob B also generates $N_b=g^{REa}$(mod p), $K_{bs}=N_B^{\ rb}$ (mod p), $E_{pwb}(K_{BS}\oplus N_B)$, $H_S(N_B\oplus ID_b)$ and $F_{KBS}(N_b)$ Then, Bob B transmits {$ID_{a,}$ ID_b, $ID_{s,}$ $E_{pwb}(K_{BS}\oplus N_B)$, $H_S(N_B\oplus ID_b)$,$F_{KBS}(N_b)$} to Server S.
Here Clients Alice A and Bob B communicate with the server S parallely.

Step 2:
Once receiving the message sent from Clients Alice A and Bob B , Server S first utilizes a trapdoor to obtain $N_A\oplus ID_a$ and $N_B\oplus ID_b$ from $H_S(N_A\oplus ID_a)$ and $H_S(N_B\oplus ID_b)$ then retrieves $N_A =(N_A\oplus ID_a)\oplus ID_a$ and $N_B =(N_B\oplus ID_b)\oplus ID_b$ respectively.

Next it uses the passwords Pw_a and Pw_b and decrypts $E_{pwa}(K_{AS}\oplus N_A)$ and $E_{pwb}(K_{BS}\oplus N_B)$, respectively, and gets $K_{AS}\oplus N_A$ and $K_{BS}\oplus N_B$. Now, $K_{AS} = K_{AS}\oplus N_A\oplus\ N_A$ and $K_{BS} = K_{BS}\oplus N_B\oplus\ N_B$ will be determined. $F_{KAS}(N_a)$ and $F_{KBS}(N_b)$ are computed. S verifies whether computed value $F_{KAS}(N_a)$ (or $F_{KBS}(N_b)$) and received value $F_{KAS}(N_a)$ (or $F_{KBS}(N_b)$)) are identical or not. If this verification holds, S continues the residual procedures of this protocol.



Alice/Bob	Two clients who want to communicate with each other
Catherine C	A malicious User (An Intruder)
Server	The trusted third party
ID_a , ID_b , ID_s	Identities of Alice, Bob and Server
Pw_a , Pw_b	Passwords secretly shared by Alice and Bob with server, respectively
p	A large prime number
g	A generator in GF(P)
$E_{pw}()$	A Symmetric encryption scheme with a password pw.
r_a, r_b	Random numbers chosen by Alice and Bob respectively
RE_a , RE_b , RE_s	The Random exponents of Alice,Bob and Server respectively
N_a, N_b	$N_a=g^{REa}$ mod p,$N_b=g^{REb}$ mod p
K_{as},K_{bs}	$K_{as}=N_a^{\ ra}$mod p, $K_{bs}=N_b^{\ rb}$mod p are a one-time strong keys shared by Alice and Bob with server, respectively.
$H_s()$	A one-way trapdoor function, where only server knows the trapdoor
$F_k()$	A pseudo-random hash function indexed by a key k.

Figure 1. Notations used in this paper

Otherwise, S terminates this protocol at current session. Next, S computes N_A^{RES} mod p and N_B^{RES} mod p, and corresponding hashed credential $F_{KAS}(ID_{a,}\ ID_b,\ K_{AS,}\ N_B^{RES})$and $F_{KBS}(ID_{a,}\ ID_{b,}\ K_{BS,}\ N_A^{RES})$. Finally, S sends{ N_B^{RES}, ,$F_{KAS}(ID_{a,}\ ID_{b,}\ K_{AS,}\ N_B^{RES})$} to A and { N_A^{RES}, ,$F_{KBS}(ID_{a,} ID_{b,} K_{BS,} N_A^{RES})$} to B simultaneously.

i.e., S → A: { N_B^{RES}, ,$F_{KAS}(ID_{a,} ID_{b,} K_{AS,} N_B^{RES})$},
S → B: { N_A^{RES}, ,$F_{KBS}(ID_{a,} ID_{b,} K_{BS,} N_A^{RES})$}.

.

Step 3:
Upon receiving the transmitted messages sent from S, B first verifies $F_{KBS}(ID_{a,}\ ID_{b,}\ K_{BS,}\ N_A^{RES})$ to authenticate S. If this verification is passed, B believes the received N_A^{RES} is valid and then computes the session key K=(N_A^{RES}) ^{REB} (mod p) and $F_K(ID_b$, K). Otherwise, B terminates this protocol.B →

A: $F_K(ID_b, K)$ B sends the $F_K(ID_b, K)$ to A. Note that $F_K(ID_b, K)$ will be used by client A to verify the legality of client B and the established session key K. At the same time, A verifies $F_{KAS}(ID_{a,} ID_b, K_{AS,} N_B^{RES})$ to authenticate S. If this verification does not hold, A terminates this protocol. Otherwise, A computes the session key K= $(N_B^{RES})^{REA}$ (mod p) and $F_K(ID_a, K)$.

Step 4:
A → B: $F_K(ID_a, K)$.
Finally, A sends the $F_K(ID_a, K)$ to B. After A and B successfully examine the validation of the incoming messages fK(IDB, K) and fK(IDA, K), both of them can ensure that they actually share the secret session key K= $(N_B^{RES})^{REA}$ (mod p)= $(N_A^{RES})^{REB}$ (mod p) at present. Otherwise, the protocol will be terminated.

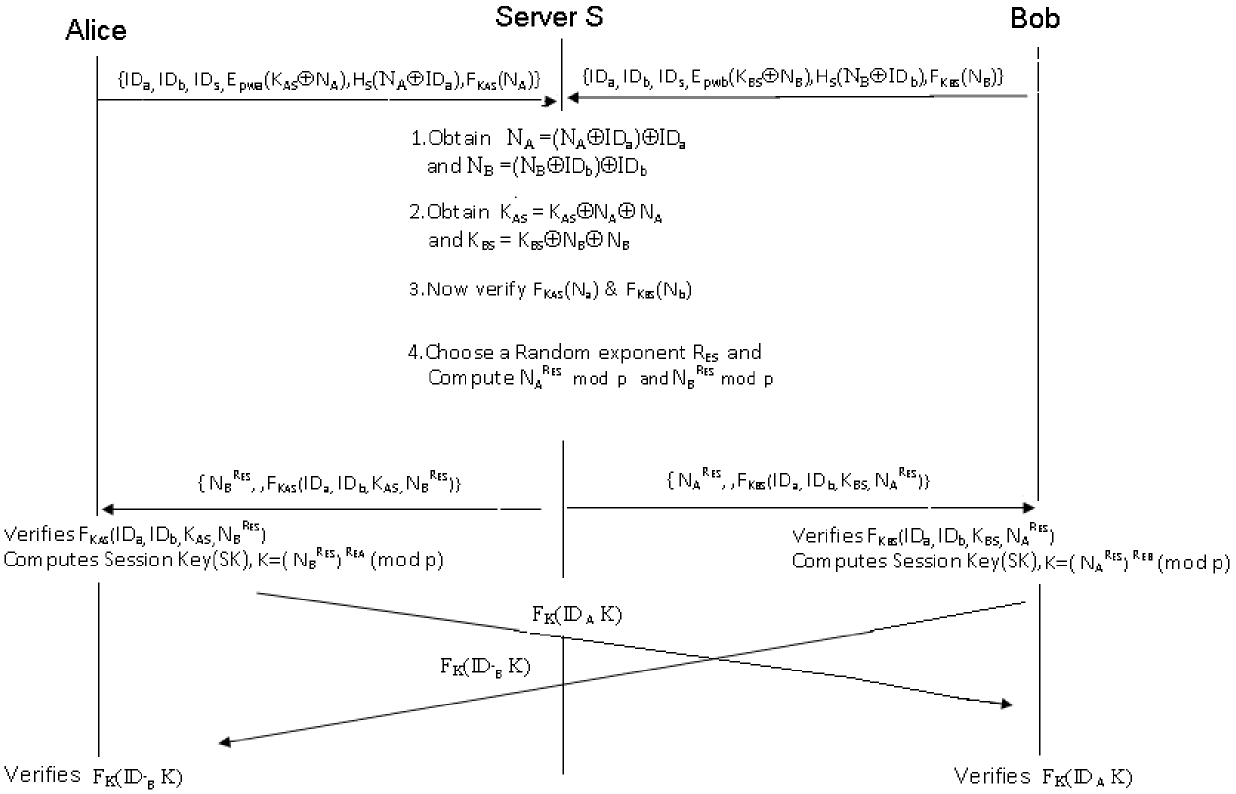

Alice
Server S
Bob
$\{ID_a, ID_b, ID_s, E_{pwa}(K_{AS}\oplus N_A), H_S(N_A\oplus ID_a), F_{KAS}(N_A)\}$
$\{ID_a, ID_b, ID_s, E_{pwb}(K_{BS}\oplus N_B), H_S(N_B\oplus ID_b), F_{KBS}(N_B)\}$
1.Obtain $N_A=(N_A\oplus ID_a)\oplus ID_a$
and $N_B=(N_B\oplus ID_b)\oplus ID_b$
2.Obtain $K_{AS}=K_{AS}\oplus N_A\oplus N_A$
and $K_{BS}=K_{BS}\oplus N_B\oplus N_B$
3.Now verify $F_{KAS}(N_a)$ & $F_{KBS}(N_b)$
4.Choose a Random exponent R_{ES} and
Compute N_A^{RES} mod p and N_B^{RES} mod p
$\{N_B^{RES}, ,F_{KAS}(ID_a, ID_b, K_{AS}, N_B^{RES})\}$
$\{N_A^{RES}, ,F_{KBS}(ID_a, ID_b, K_{BS}, N_A^{RES})\}$
Verifies $F_{KAS}(ID_a, ID_b, K_{AS}, N_B^{RES})$
Computes Session Key(SK), K=$(N_B^{RES})^{REA}$ (mod p)
Verifies $F_{KBS}(ID_a, ID_b, K_{BS}, N_A^{RES})$
Computes Session Key(SK), K=$(N_A^{RES})^{REB}$ (mod p)
$F_K(ID_A K)$
$F_K(ID_B K)$
Verifies $F_K(ID_B K)$
Verifies $F_K(ID_A K)$

Figure 2.The 3pek Exchange Protocol Using Parallel Message Transmission Technique

III. DETECTABLE ON-LINE PASSWORD GUESSING ATTACKS

This section demonstrates the Detectable password guessing attack on 3pek Exchange Protocol using parallel message tranmission technique, in which one party is able to know the other party's password.

A client Catherine C (Intruder) can impersonate client Alice and communicate with client Bob. While Bob is thinking that it is communicating with client Alice but actually it is communicating with client Catherine. If a malicious party able to guess the password of another, then the same malicious party will impersonate as the actual client. Detectable on-line password guessing attacks on on 3pek Exchange Protocol using parallel message tranmission technique is shown in Figure.3.The details are shown below.

Step 0: Alice and Bob share passwords pwa and pwb secretly with server respectively. An intruder Catherine C impersonate Alice to guess Alice's password.

Step 1: Alice A generates two random numbers r_a and RE_a and calculates $E_{pwa}(K_{AS}\oplus N_A)$, $H_S(N_A\oplus ID_a)$ and $F_{KAS}(N_A)$ where $N_A=g^{REa}$(mod p) and $K_{as}=N_A^{ra}$ (mod p). Then Alice A sends { $ID_{a,} ID_{b,} ID_{s,} E_{pwa} (K_{AS} \oplus N_A)$, $H_S(N_A\oplus ID_a)$,$F_{KAS}(N_a)$} to Server S.

Step 2: A client Catherine C an intruder intercepts this message i.e{$ID_{a,}$ $ID_{b,}$ $ID_{s,}E_{pwa}(K_{AS}\oplus N_A)$, $H_S(N_A\oplus ID_a)$,$F_{KAS}(N_a)$}.

Now Client Catherine C generates her own two random number ra'& REa' to computes$N_{A'}$ = g $^{REa'}$ (mod p) and $K_{AS'}$= $N_{A'}{}^{ra'}$(mod p). Now Client Catherine C guess Alice's password as Pwa' to encrypt $(K_{AS'}\oplus N_{A'})$.Again Catherince C also computes the another two credentials $H_S(N_{A'} \oplus ID_a)$, $FK_{AS'}(N_{A'})$ by its own because the IDs are not secret. Then she sends {$ID_{a,}$ $ID_{b,}$ $ID_{s,}$ $Epw_{a'}(K_{AS'}\oplus N_{A'})$, $H_S(N_{A'} \oplus ID_a)$, $FK_{AS'}(N_{A'})$} to Server S.

Step 3: Upon receiving {$ID_{a,}$ $ID_{b,}$ $ID_{s,}$ $Epw_{a'}(K_{AS'}\oplus N_{A'})$, $H_S(N_{A'}\oplus ID_a)$, $FK_{AS'}(N_{A'})$}, Server S Decrypts

$Epw_{a'}(K_{AS'} \oplus N_{A'})$ to get $(K_{AS'} \oplus N_{A'})$. Then it retrieves $N_{A'} \oplus ID_a$ from $H_S(N_{A'} \oplus ID_a)$ by using trapdoor. Now server computes $N_A^{э} = (N_A^{э} \oplus ID_a) \oplus ID_a$ and obtains $K_{AS'} = K_{AS'} \oplus N_{A'} \oplus N_{A'}$.Now Server S verifies whether computed $FK_{AS'}(N_{A'})$ and received $FK_{AS'}(N_{A'})$ are equal or not.if both FKas(Na) and FKas'(Na') are equal then the guessed password is correct and server will continue the residual procedure of the protocol. Hence the attack can be detectable by Server the Server terminates this protocol at current session if not equal. An intruder never sits idle. After some time she repeats the same process. She will continue this until she hits the successful password. In this way a malicious client can impersonate the actual client by successfully getting the secrete session key.

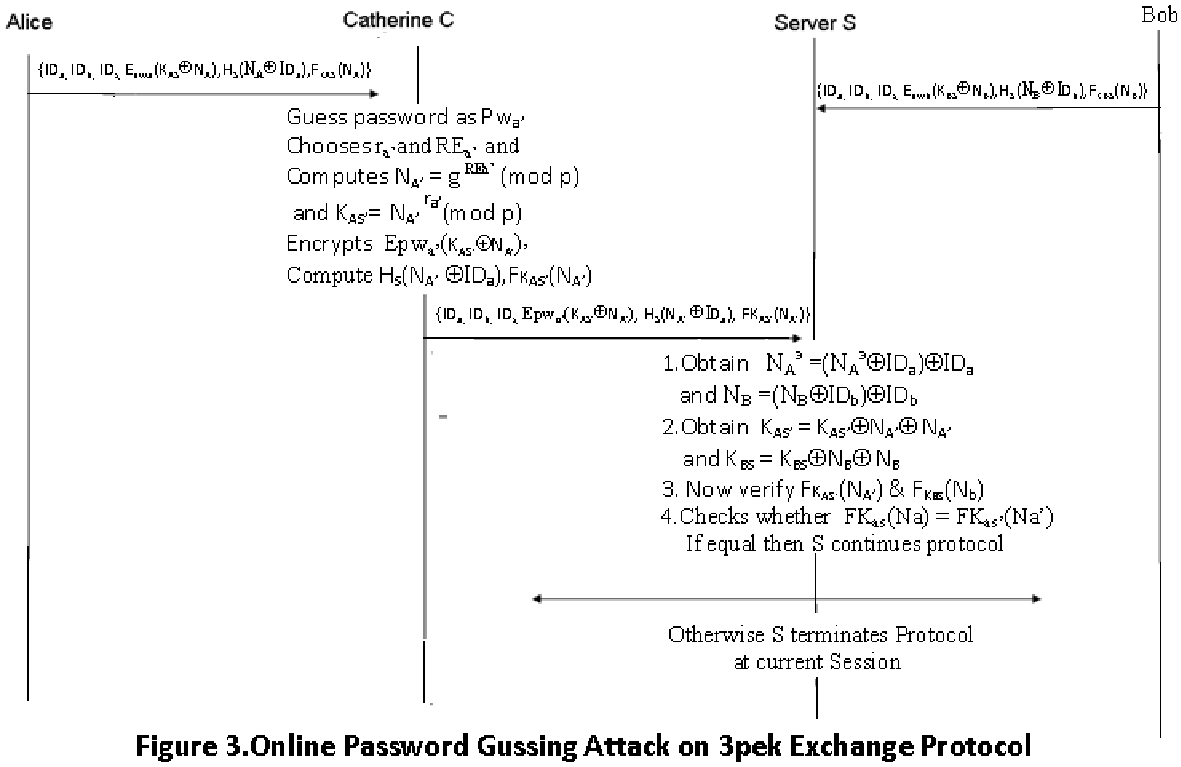

Alice
Catherine C
Server S
Bob
$\{ID_a, ID_b, ID_c, E_{pwa}(K_{AS} \oplus N_A), H_S(N_A \oplus ID_a), F_{KAS}(N_A)\}$
$\{ID_a, ID_b, ID_c, E_{pwb}(K_{BS} \oplus N_B), H_S(N_B \oplus ID_b), F_{KBS}(N_B)\}$
Guess password as $Pw_{a'}$
Chooses $r_{a'}$ and $RE_{a'}$ and
Computes $N_{A'} = g^{RE_{a'}}$ (mod p)
and $K_{AS'} = N_{A'}^{r_{a'}}$ (mod p)
Encrypts $Epw_{a'}(K_{AS'} \oplus N_{A'})$,
Compute $H_S(N_{A'} \oplus ID_a), FK_{AS'}(N_{A'})$
$\{ID_a, ID_b, ID_c, Epw_{a'}(K_{AS'} \oplus N_{A'}), H_S(N_{A'} \oplus ID_a), FK_{AS'}(N_{A'})\}$
1.Obtain $N_A^{э} = (N_A^{э} \oplus ID_a) \oplus ID_a$
and $N_B = (N_B \oplus ID_b) \oplus ID_b$
2.Obtain $K_{AS'} = K_{AS'} \oplus N_{A'} \oplus N_{A'}$
and $K_{BS} = K_{BS} \oplus N_B \oplus N_B$
3. Now verify $F_{KAS'}(N_{A'})$ & $F_{KBS}(N_b)$
4.Checks whether $FK_{as}(Na) = FK_{as'}(Na')$
If equal then S continues protocol
Otherwise S terminates Protocol
at current Session

Figure 3.Online Password Gussing Attack on 3pek Exchange Protocol Using Parallel Message Transmission Technique

IV. CONCLUSION

In this paper, we have demonstrated that a 3pek Exchange Protocol Using Parallel Message Transmission Technique is insecure against the detectable on-line password guessing attack. To eliminate the identified authentication weakness, we suggest that there should be some proper synchronization is needed between the credentials passed between clients and server.

V. ACKNOWLEDGMENTS

The research reported in this paper is the result of a unremitting effort that has started lately in this area.Dozens of researchers from all over the world published many papers on this subject, and we have greatly benefited from their imaginative ideas and gorgeous insights. They are too numerous to list here, but we are gratefully acknowledge the contribution of all.

VI. REFERENCES

[1] S.M. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against password guessing attacks," *in Proc. of 1992 IEEE Symposium on Research in Se-curity and Privacy*, pp.72–84, 1992.

[2] H.R. Chung and W.C. Ku, "Three weaknesses in a simple three-party key exchange proto-col," *Information Science*, vol.178, no.1, pp.220-229, 2008.

[3] Y. Ding and P. Horster, "Undetectable on-line password guessing attacks," *ACM Operat-ing Systems Review*, vol.29, no.4, pp.77-86, 1995.

[4] M. Steiner, G. Tsudik and M. Waidner, "Refinement and extension of encrypted key exchange," *ACM Operating Systems Review*, vol.29, no.3, pp.22-30, 1995.

[5] Y. Ding and P. Horster, "Undetectable on-line password guessing attacks," *ACM Operat-ing Systems Review*, vol.29, no.4, pp.77-86, 1995.

[6] C.L. Lin, H.M. Sun and T. Hwang, "Three party-encrypted key exchange: attacks and a solution," *ACM Operating Systems Review*, vol.34, no.4, pp.12-20, 2000.

[7] T.F. Lee, T. Hwang and C.L. Lin, "Enhanced three-party encrypted key exchange without server public keys," *Computers and Security*, vol.23, no.7, pp.571-577, 2004.

[8] H.A. Wen, T.F. Lee and T. Hwang, "Provably secure three-party password-based authen-ticated key exchange protocol using Weil pairing," *IEE Proceedings – Communications*, vol.152, no.2, pp.138-143, 2005.

[9] J. Nam, Y. Lee, S. Kim and D. Won, "Security weakness in a three-party pairing-based protocol for password authenticated key exchange," *Information Sciences*, vol.177, no.6, pp.1364-1375, 2007.

[10] R.X. Lu and Z.F. Cao, "Simple three-party key exchange protocol," *Computers and Secu-rity*, vol.26, no.1, pp.94-97, 2007.

[11] H. Guo, Z. Li, Y. Mu and X. Zhang, "Cryptanalysis of simple three-party key exchange protocol," *Computers and Security*, vol.27, no.1-2, pp.16-21, 2008.

[12] C.W. Phan Raphael, W.C. Yau and B.M. Goi, "Cryptanalysis of simple three-party key exchange protocol (S-3PAKE)," *Information Sciences*, vol.178, no.13, pp.2849-2856, 2008.

[13] C.L. Lin, H.M. Sun, M. Steiner and T. Hwang, "Three-party encrypted key exchange without server public-keys," *IEEE Communication Letters*, vol.5, no.12, pp.497-499, 2001.

[14] H.M. Sun, B.C. Chen and T. Hwang, "Secure key agreement protocols for three-party against guessing attacks," *Journal of Systems and Software*, vol.75, pp.63-68, 2005.

[15] H.A. Wen, T.F. Lee and T. Hwang, "Provably secure three-party password-based authen-ticated key exchange protocol using Weil pairing," *IEE Proceedings – Communications*, vol.152, no.2, pp.138-143, 2005.