IMPERSONATION ATTACK ON EKE PROTOCOL

Shirisha Tallapally

Vaagdevi College of Engineering, Warangal, Andra Pradesh, India
Shirisha27@yahoo.co.in

ABSTRACT

The key exchange protocol is one of the most elegant ways of establishing secure communication between pair of users by using a session key. The passwords are of low entropy, hence the protocol should resist all types of password guessing attacks. Recently ECC-3PEKE protocol has been proposed by Chang and Chang. They claimed the protocol is secure, efficient and practical. Unless their claims Yoon and Yoo presented an Undetectable online password guessing attack on the above protocol. A key recovery attack was proved on ECC-3PEKE protocol using the Undetectable online password guessing attack proposed by Yoon and Yon. In the present paper an Impersonation attack on ECC-3PEKE protocol using the Undetectable online password guessing attack proposed by Yoon and Yon is demonstrated.

KEYWORDS

ECC-3PEKE protocol, Undetectable online password guessing attack, Impersonation attack.

1. INTRODUCTION

A session key can be exchanged between two users by using a key exchange protocol and assures a secure communication for later sessions. The first practical key exchange protocol is proposed by Diffie-Hellman [1]. Later improvements are made on this protocol. As it is simple for the users to remember the passwords, password based key exchange protocol achieved greater attention. Even though the protocol is simple and efficient, according to Ding and Horster [2], it should not be vulnerable to any type of off line, undetectable or detectable on line password guessing attacks, since the passwords are of low-entropy.

In general the password guessing attacks can be divided into three classes and they are listed below:

• Detectable on-line password guessing attacks: An attacker attempts to use a guessed password in an on-line transaction. He/She verifies the correctness of his/her guess using the response from server. A failed guess can be detected and logged by the server.

• Undetectable on-line password guessing attacks: Similar to Detectable on-line password guessing attack, an attacker tries to verify a password guess in an on-line transaction. However, a failed guess can not be detected and logged by server, as server is not able to distinguish an honest request from a malicious one.

• Off-line password guessing attacks: An attacker guesses a password and verifies his/her guess off-line. No participation of server is required, so the server does not notice the attack.

Bellovin and Merrit proposed Encrypted key exchange protocol [3]. Later many efficient key exchange protocols based on password have been developed [4, 5, 6, 7, 8]. Recently these two party key exchange protocols are extended to three party, in which, the two parties initially communicates the passwords with the trusted server securely. Later the server authenticates the clients when they want to agree upon a session key. Steiner et al proposed three party protocol[9]. Later Lin etal showed that STW-3 PEKE protocol falls to undetectable on-line password guessing attack, off-line password guessing attacks and proposed two versions of improved three party key exchange protocols [10]. Recently Chang and Chang [11] proposed a novel three party encrypted key exchange protocol (ECC-3PEKE protocol) without server

public key and claimed the protocol is secure, efficient and practical. Unlike their claims Yoon and Yoo [12] pointed out an Undetectable password guessing attack on their protocol, in which one party is able to know the other party's password and furthermore they presented an improved version of it to avoid the above attack. A key recovery attack [13] is also proved on ECC-3PEKE protocol using the Undetectable online password guessing attack proposed by Yoon and Yoo.

In this paper an impersonation attack on ECC-3 PEKE protocol is proposed using the Undetectable password guessing attack proposed by Yoon and Yon. A Client B can impersonate as Client A and communicate with Client C. While C is thinking that it is communicating with Client A but actually it is communicating with Client B. If a malicious party able to guess the password of another, then the same malicious party will impersonate as the client (the one whose password is guessed).

The paper is organized as follows: section 2 briefly reviews the ECC-3PEKE protocol, section 3 reviews undetectable password guessing attack on ECC-3PEKE protocol. Section 4 describes the impersonation attack on ECC-3PEKE protocol and the concluding remarks are made in section 5.

2. REVIEW OF ECC-3PEKE PROTOCOL

This section briefly explains the ECC-3PEKE protocol. The notations used in this protocol are listed below:
A,B : two communication parties
S: the trusted server
ID_A, ID_B, ID_S: the identities of A,B and S, respectively
PW_A, PW_B: the passwords securely shared by A with S and B
EPW(.):a symmetric encryption scheme with a password PW
r_A, r_B: the random numbers chosen by A and B, respectively
p: a large prime
g : a generator of order p - 1
R_A,R_B,R_S: the random exponents chosen by A,B and S, respectively
N_A,N_B :$N_A=g^{RA}$(mod p)and $N_B=g^{RB}$(mod p)
F_S(.):the one-way trapdoor hash function(TDF) where only S knows the trapdoor
f_K(.): the pseudo-random hash function (PRF) indexed by a key K
K_{AS},K_{AS}: a one time strong keys shared by A with S and B with S, respectively.
The procedure followed in ECC-3 PEKE protocol is given below:

Step 1: A → B : {ID_A, ID_B, ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$,f_{KAS} (N_A)} User A chooses a random integer number r_A and a random exponent $R_A \in_R Z^*_p$, and then computes $N_A = g^{RA}$ and $K_{AS} = N_A^{RA}$ .Then, A encrypts N_A by using his/her password PW_A like E_{PWA}, (N_A) and computes two hash values $F_S(r_A)$ and f_{KAS} (N_A). Finally, A sends {ID_A,ID_B,ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$, f_{KAS} (N_A) }to B.

Step2: B → S: {ID_A, ID_B, ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$, f_{KAS} (N_A),$E_{PWB}(N_B)$, $F_S(r_B)$, f_{KBS} (N_B)}. User B chooses a random integer r_B and a random exponent $R_B \in_R Z^*_p$, and then computes $N_B = g^{RB}$ and $K_{AB} = N_B^{RB}$. Then, B encrypts N_B by using his/her password PW_B like E_{PWB} , (N_B) and computes two hash values $F_S(r_B)$ and $f_{KAB}(N_B)$. Finally, B sends{ID_A, ID_B, ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$, f_{KAS} (N_A), $E_{PWB}(N_B)$, $F_S(r_B)$, f_{KBS} (N_B)} to S.

Step3: S → B:{ N_B^{RS}, $f_{KAS}(ID_A, ID_B,K_{AS},N_B^{RS})$, N_A^{RS}, $f_{KBS}(ID_A, ID_B,K_{BS},N_A^{RS})$} Server S decrypts $E_{PWA}(N_A)$ and $E_{PWB}(N_B)$ by using P_{WA} and P_{WB} to get N_A and N_B, respectively. Then, S gets r_A and r_B from $F_S(r_A)$ and $F_S(r_B)$ by using a trap door, respectively. To authenticate A and B, S computes $K_{AS} = N_A^{rA}$ and $K_{BS} = N_B^{rB}$ and then verifies f_{KAS} (N_A) and f_{KBS} (N_B), respectively. If successful, S chooses a random exponent $R_S \in_R Z^*_p$ and then computes N_A^{RS} and N_B^{RS}

respectively. Finally, S computes two hash values f_{KAS} (ID_A, ID_B,K_{AS},N_B^{RS})f_{KBS} (ID_A, ID_B,K_{BS}, ,N_A^{RS}), and sends {N_B^{RS} , f_{KAS} (ID_A, ID_B,K_{AS},N_B^{RS}),N_A^{RS} ,f_{KBS}(ID_A, ID_B,K_{BS},N_A^{RS})} to B.

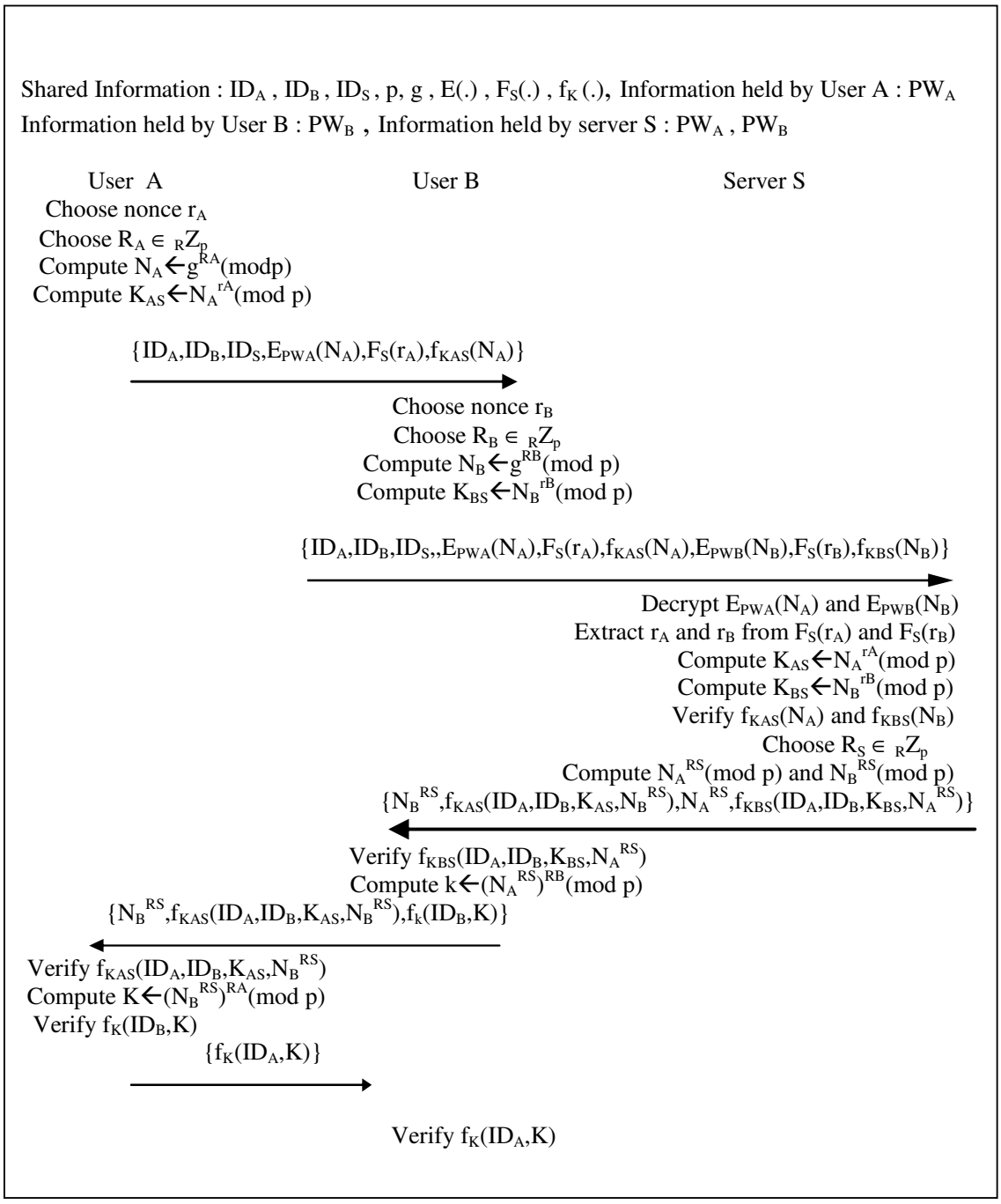

Figure 1: ECC-3PEKE protocol

Step 4: B → A: { N_B^{RS} , f_{KAS} (ID_A, ID_B,K_{AS},N_B^{RS}),f_k(ID_B,K)} By using $K_{BS} = N_B^{rB}$, B authenticates S by checking f_{BS}(ID_A, ID_B,K_{BS},N_A^{RS}).If successful, B computes the session key $K = (N_A^{RS})^{RB} = g^{RS\ RARB}$ and hash value f_K(ID_B,K), and then sends {N_B^{RS} , f_{KAS} (ID_A, ID_B,K_{AS},N_B^{RS}), f_K(ID_B,K)} to A.

Step5: A → B:{f_K(ID_A,K)} By using $K_{AS} = N_A^{rA}$, A authenticates S by checking f_{KAS} (ID_A, ID_B,K_{AS},N_B^{RS}). If successful A computes the session key $K = (N_B^{RS})^{RA} = g^{RSRARB}$,and authenticates B by checking f_K(ID_B,K). If authenticates is passed, A computes and sends f_K(ID_A,K).

Step 6: B authenticates A by checking f_K(ID_A,K).If successful, B confirms A's knowledge of the session key $K = g^{RSRARB}$.
Figure 1 illustrates ECC-3PEKE protocol

3. UNDETECTABLE ONLINE PASSWORD GUESSING ATTACK ON CHANG AND CHANG PROTOCOL

This section demonstrates the undetectable password guessing attack on Chang-Chang protocol as proposed by Yoon and Yoo [7] with the assumption of B as malicious party. The procedure of the above attack is given below:

Step1: A → B: {ID_A, ID_B, ID_S,E_{PWA}(N_A), F_S(r_A),f_{KAS} (N_A)}

Step2: B recordsmessage {ID_A, ID_B, ID_S,E_{PWA}(N_A), F_S(r_A), f_{KAS} (N_A)} from A

Step3: B guesses a password PW_A' from password dictionary and gets N'_A

Step4: B chooses a random integer r_B and then computes $K_{BS} = N'^{rB}_A$. Then, B encrypts N'_A by using his/her password PWB like E_{PWB} (N'_A) and computes two hash values F_S(r_B) and f_{KBS} (N'_A).

Step5: B → S: {ID_A, ID_B, ID_S,E_{PWA}(N_A), F_S(r_A), f_{KAS} (N_A), E_{PWB}(N'_A), F_S(r_B), f_{KBS} (N'_A)} B transmits {ID_A, ID_B, ID_S,E_{PWA}(N_A), F_S(r_A), f_{KAS} (N_A),E_{PWB}(N_B), F_S(r_B), f_{KBS} (N_B)}

Step6: S → B:{ N'^{RS}_A , f_{KAS} (ID_A, ID_B,K_{AS},N'^{RS}_A), N_A^{RS} , f_{KBS}(ID_A, ID_B,K_{BS},N_A^{RS})} After receiving the message S can authenticate A and B by verifying f_{KAS} (N_A) and f_{KBS} (N'_A), respectively. S will compute f_{KAS} (ID_A, ID_B, K_{AS}, N'^{RS}_A) and f_{KBS}(ID_A, ID_B,K_{BS},N_A^{RS}) to B.

Step7: After receiving the message B simply compares $N'^{RS}_A = N_A^{RS}$. If $N'^{RS}_A = N_A^{RS}$, it follows that PWA′ = PWA.
Figure 2 illustrates Undetectable online password guessing attack on Chang and Chang protocol.

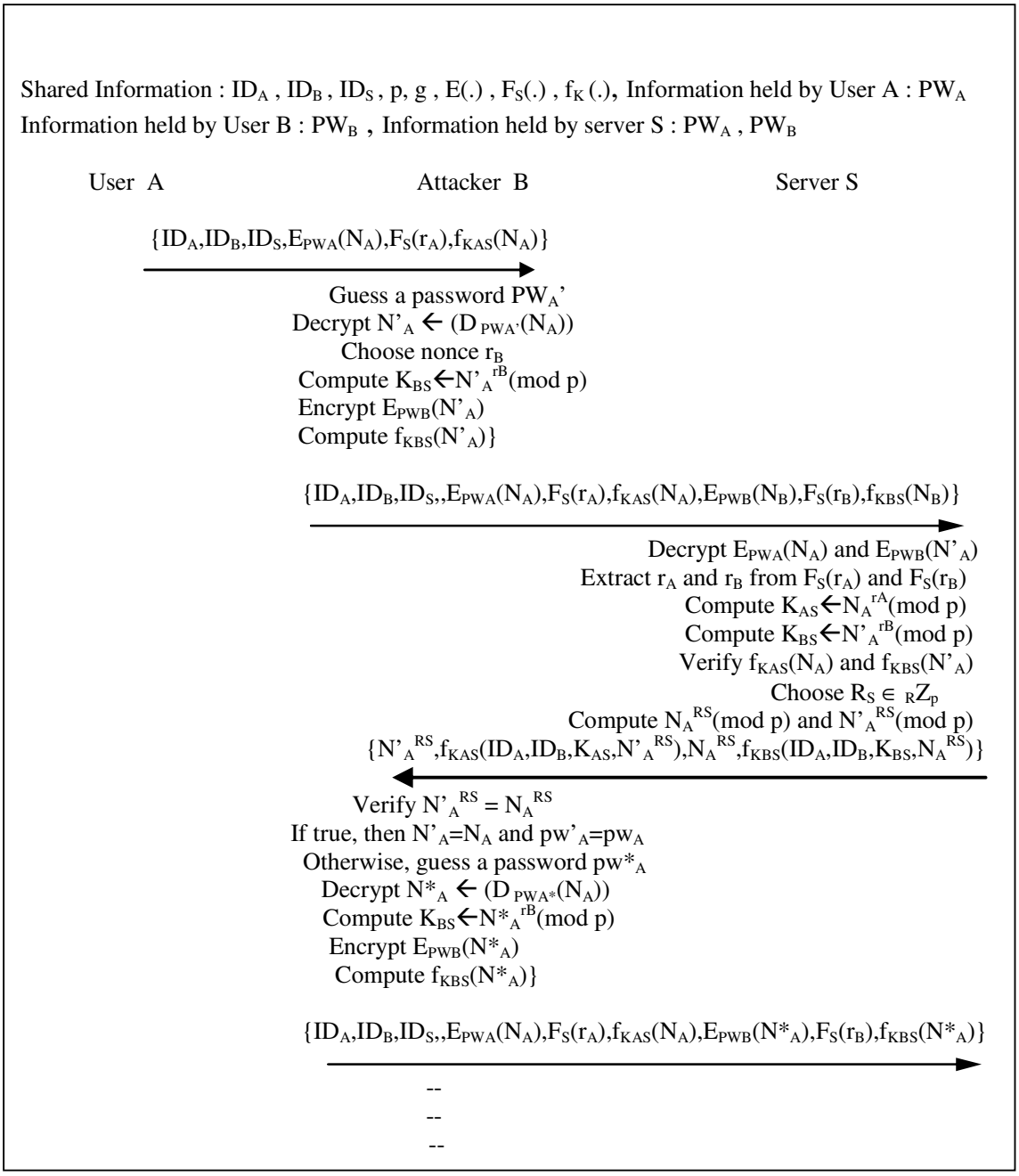

Figure 2: Undetectable online password guessing attack on Chang and Chang protocol

4. IMPERSONATION ATTACK ON ECC-3PEKE PROTOCOL

Shared Information : ID_A , ID_C , ID_S , p, g , E(.) , $F_S(.)$, $f_K(.)$, Information held by User B : PW_A
Information held by User C : PW_C , Information held by server S : PW_A , PW_C

User B		User C		Server
Choose nonce r_A				
Choose $R_A \in {}_RZ_p$				
Compute $N_A \leftarrow g^{RA}(\text{mod} p)$				
Compute $K_{AS} \leftarrow N_A{}^{rA}(\text{mod p})$				
B encrypts N_A by using password of A i.e. PW_A (this is already obtained as shown in figure 2)				
$\{ID_A, ID_C, ID_S, E_{PWA}(N_A), F_S(r_A), f_{KAS}(N_A)\}$	$\rightarrow$			
		Choose nonce r_c		
		Choose $R_C \in {}_RZ_p$		
		Compute $N_C \leftarrow g^{RC}(\text{mod p})$		
		Compute $K_{CS} \leftarrow N_C{}^{rC}(\text{mod p})$		
		$\{ID_A, ID_C, ID_S, E_{PWA}(N_A), F_S(r_A), f_{KAS}(N_A), E_{PWC}(N_C), F_S(r_C), f_{KCS}(N_C)\}$	$\rightarrow$	
				(As S believes that A & C wants to establish a session)
				Decrypt $E_{PWA}(N_A)$ and $E_{PWC}(N_C)$
				Extract r_A and r_C from $F_S(r_A)$ and $F_S(r_C)$
				Compute $K_{AS} \leftarrow N_A{}^{rA}(\text{mod p})$
				Compute $K_{CS} \leftarrow N_C{}^{rC}(\text{mod p})$
				Verify $f_{KAS}(N_A)$ and $f_{KCS}(N_C)$
				Choose $R_S \in {}_RZ_p$
				Compute $N_A{}^{RS}(\text{mod p})$ and $N_C{}^{RS}(\text{mod p})$
		$\{N_C{}^{RS}, f_{KAS}(ID_A, ID_C, K_{AS}, N_C{}^{RS}), N_A{}^{RS}, f_{KCS}(ID_A, ID_C, K_{CS}, N_A{}^{RS})\}$	$\leftarrow$	
		Verify $f_{KCS}(ID_A, ID_C, K_{CS}, N_A{}^{RS})$		
		Compute $k \leftarrow (N_A{}^{RS})^{RC}(\text{mod p})$		
$\{N_C{}^{RS}, f_{KAS}(ID_A, ID_C, K_{AS}, N_C{}^{RS}), f_K(ID_C, K)\}$	$\leftarrow$			
Verify $f_{KAS}(ID_A, ID_C, K_{AS}, N_C{}^{RS})$				
Compute $K \leftarrow (N_C{}^{RS})^{RA}(\text{mod p})$				
B uses ID_A to make believe that it is A and computes $f_K(ID_A, K)$}				
Verify $f_K(ID_C, K)$				
$\{f_K(ID_A, K)\}$	$\rightarrow$			
		Verify $f_K(ID_A, K)$		

Figure 3 : Impersonation attack on ECC-3PEKE protocol

A malicious party B guesses the password of A using Undetectable password guessing attack as proposed by Yoon and Yoo. B uses the password of A for impersonating A, when A and C wants to communicate. The following procedure presents the attack in detail.

Step 1: B → C: $\{ID_A, ID_C, ID_S, E_{PWA}(N_A), F_S(r_A), f_{KAS}(N_A)\}$ User B chooses a random integer number r_A and a random exponent $R_A \in_R Z^*_p$, and then computes $N_A = g^{RA}$ and $K_{AS} = N_A^{RA}$ .Then, **B encrypts N_A by using password of A i.e. PW_A like E_{PWA} (N_A)** and computes two hash values $F_S(r_A)$ and $f_{KAS}(N_A)$. Finally, B sends $\{ID_A, ID_B, ID_S, E_{PWA}(N_A), F_S(r_A), f_{KAS}(N_A)\}$ to C.

Step2: C → S: $\{ID_A, ID_C, ID_S, E_{PWA}(N_A), F_S(r_A), f_{KAS}(N_A), E_{PWC}(N_C), F_S(r_C), f_{KCS}(N_C)\}$. User C chooses a random integer r_C and a random exponent $R_C \in_R Z^*_p$, and then computes $N_C = g^{RC}$ and $K_{cs} = N_C^{RC}$. Then, C encrypts N_C by using his/her password PW_C like $E_{PWC}(N_C)$ and computes two hash values $F_S(r_C)$ and $f_{KCS}(N_C)$. Finally, C sends$\{ID_A, ID_C, ID_S, E_{PWA}(N_A), F_S(r_A), f_{KAS}(N_A), E_{PWC}(N_C), F_S(r_C), f_{KCS}(N_C)\}$ to S.

Step3: S → C:$\{ N_C^{RS}, f_{KAS}(ID_A, ID_C, K_{AS}, N_C^{RS}), N_C^{RS}, f_{KCS}(ID_A, ID_C, K_{CS}, N_A^{RS})\}$ Server S decrypts $E_{PWA}(N_A)$ and $E_{PWC}(N_C)$ by using P_{WA} and P_{WC} **(As S believes that A & C wants to establish a session)** to get N_A and N_C, respectively. Then, S gets r_A and r_C from $F_S(r_A)$ and $F_S(r_C)$ by using a trap door, respectively. To authenticate A and C, S computes $K_{AS} = N_A^{rA}$ and $K_{CS} = N_C^{rC}$ and then verifies $f_{KAS}(N_A)$ and $f_{KCS}(N_C)$, respectively. If successful, S chooses a random exponent $R_S \in_R Z^*_p$ and then computes N_A^{RS} and N_C^{RS} respectively. Finally, S computes two hash values $f_{KAS}(ID_A, ID_C, K_{AS}, N_C^{RS})$, $f_{KCS}(ID_A, ID_C, K_{CS}, , N_A^{RS})$, and sends $\{N_C^{RS}, f_{KAS}(ID_A, ID_C, K_{AS}, N_C^{RS}), N_A^{RS}, f_{KCS}(ID_A, ID_C, K_{CS}, N_A^{RS})\}$ to C.

Step 4: C → B: $\{ N_C^{RS}, f_{KAS}(ID_A, ID_C, K_{AS}, N_C^{RS}), f_k(ID_C, K)\}$. By using $K_{CS} = N_C^{rC}$, C authenticates S by checking $f_{KCS}(ID_A, ID_C, K_{CS}, N_A^{RS})$.If successful, C computes the session key $K = (N_A^{RS})^{RC} = g^{RS\ RARC}$ and hash value $f_K(ID_C, K)$, and then sends $\{N_C^{RS}, f_{KAS}(ID_A, ID_C, K_{CS}, N_A^{RS}), f_K(ID_C, K)\}$ to B **(thinking B as A)**.

Step5: B → C:$\{f_K(ID_A, K)\}$ By using $K_{AS} = N_A^{rA}$, A authenticates S by checking $f_{KAS}(ID_A, ID_C, K_{AS}, N_C^{RS})$. If successful B computes the session key $K = (N_C^{RS})^{RA} = g^{RSRARC}$ and authenticates C by checking $f_K(ID_C, K)$. If authentication is passed, B computes and sends $f_K(ID_A, K)$ (**B uses ID_A to make C believe that it is A**).

Step 6: C authenticates A(**C is thinking B as A**) by checking $f_K(ID_A, K)$.If successful, C confirms A's knowledge of the session key $K = g^{RSRARB}$.
Figure 3 illustrates impersonation attack on ECC-3PEKE protocol. Similarly impersonation of the responder works on the same protocol.

5. CONCLUSIONS

Recently Chang and Chang proposed a novel three party simple key exchange protocol. They claimed the protocol is secure, efficient and practical. Unless their claims Yoon and Yoo, presented an Undetectable online password guessing attack on the above protocol. A key recovery attack is also proved on Chang and Chang protocol using the Undetectable online password guessing attack proposed by Yoon and Yoo. In the similar line, an impersonation of initiator attack is demonstrated on ECC-3PEKE protocol. An impersonation of the responder attack also equally applies to the above protocol.

ACKNOWLEDGEMENTS

The author gratefully acknowledges Ms.R.Padmavathy, Assistant Professor, National Institute of technology, Warangal for her guidance and motivation which helped in the completion of this work. The author also would like to thank management of Vaagdevi College of Engineering, Warangal for their encouragement

REFERENCES

[1] W. Diffie and M. Hellman, "New Directions in cryptography", *IEEE Transactions on Information theory*, Vol 22 ,no. 6 , pp 644-54, (1976).

[2] Y. Ding and P. Hoster, "Undetectable Online password guessing attacks", *ACM operatinf system review*, vol 29, no. 4,pp 77-86 (1995).

[3] SM. Bellovin and M. Merrit, " Encrypted key exchange: password-based protocols secure against dictionary attacks". *In: Proceedings of IEEE sysmposium on re-search in security and privacy, IEEE Computer society press* :72-84,(1992).

[4] K. Kobara and H. Imai. Pretty-simple password-authenticated key exchange under standard assumptions. *IEICE Transactions*, E85-A (10):2229-2237, Oct. 2002. Also available at http://eprint.iacr.org/2003/038/.

[5] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks. *Proceedings of the 2000 Advances in Cryptology (EUROCRYPT'2000)*. Berlin, Germany:Springer-Verlag, 2000: 139-155.

[6] E. Bresson, O. Chevassut, and D. Pointcheval. New security results on encrypted key exchange. *Proc. PKC 2004*, LNCS 2947, pp. 145-158. Springer-Verlag, Mar. 2004.

[7] M. Abdalla and D. Pointcheval. Simple Password-Based Encrypted Key Exchange Protocols. *Proc. of Topics in Cryptology - CT-RSA 2005*, LNCS 3376, pp. 191-208, Springer-Verlag.

[8] M. Abdalla, O. Chevassut, and D. Pointcheval. One-time verifier-based encrypted key exchange. *Proc. of PKC '05*, LNCS 3386, pp. 47–64. Springer-Verlag, 2005.

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

[10] CL. Lin, HM. Sun, M. Steiner, T. Hwang " Three-party excrypted key exchange without server public Keys" *IEEE Communication letters*, vol 5, no.12,pp 497- 9 , (2001).

[11] CC. Chang and YF. Chang, "A novel three party encrypted key exchange protocol", *Computer Standards and Interfaces*, vol 26 , no 5, (pp 471-6),(2004).

[12] EJ. Yoon and KY. Yoo, "Improving the novel three-party encrypted key exchange protocol", *Computer Standards and Interfaces*, 30:309-314 , (2008).

[13] R. Padmavathy, Chakravarthy Bhagvati. "A Key Recovery Attack on Chang and Chang Password Key Exchange Protocol" *ICCNT*, World science press, 2009.

.