2009 Third International Conference on Network and System Security

Analysis of Two Pairing-based Three-party Password Authenticated Key Exchange Protocols

Raphael C.-W. Phan
Electronic and Electrical Engineering
Loughborough University
United Kingdom
r.phan@lboro.ac.uk

Wei-Chuen Yau, Bok-Min Goi
Faculty of Engineering
Multimedia University
Cyberjaya, Malaysia
wcyau@mmu.edu.my, bmgoi@mmu.edu.my

***Abstract*—Password-Authenticated Key Exchange (PAKE) protocols allow parties to share secret keys in an authentic manner based on an easily memorizable password. Recently, Nam et al. showed that a provably secure three-party password-based authenticated key exchange protocol using Weil pairing by Wen et al. is vulnerable to a man-in-the-middle attack. In doing so, Nam et al. showed the flaws in the proof of Wen et al. and described how to fix the problem so that their attack no longer works. In this paper, we show that both Wen et al. and Nam et al. variants fall to key compromise impersonation by any adversary. Our results underline the fact that although the provable security approach is necessary to designing PAKEs, gaps still exist between what can be proven and what are really secure in practice.**

***Keywords*-Password-authenticated key exchange; cryptanalysis; attacks; provable security; three-party; key compromise impersonation; Weil pairing**

I. Introduction

A 2-party password-based authenticated key exchange (PAKE) protocol [5] allows two parties to authenticate each other and to establish a common session key for securing a communication session using a low-entropy password. The first known PAKE is due to Bellovin and Merritt [6]. This concept has also been extended to 3 parties, e.g. two clients and a trusted server or key distribution center (KDC) [1], [2], [3], [10], [14], [17], [18], [19], [20], [35], [36], [22].

Recently, Wen et al. proposed a three-party password-based authenticated key exchange protocol using Weil pairing [37]. The protocol was formally proven secure in the random oracle model [4], [5]. Nam et al. [25] however showed that the security proof in [37] is flawed and pointed out that the protocol is vulnerable to unknown key-share attack (UKS) [16], [13], i.e. a client A (resp. B) thinking it is sharing a key with B (resp. A) when it is actually sharing with a malicious adversary C. Nam et al. proposed a way to prevent their attack, basically by including the identities of both clients into the generation of the secret session key shared by each client with the server.

The basic requirements of PAKEs can be found in literature, e.g. [24], [9]. In particular, they are as follows.

- **Dictionary attack resilience:** Originally, a dictionary attack is a password guessing technique in which the adversary attempts to determine a user's password by successively trying words from a dictionary (a compiled list of likely passwords) in the hope that one of these password guesses will be the user's actual password. This attack can be performed in *online mode* (trying successive passwords until a login is successful) or *off-line mode* (hashing or encrypting a dictionary of words and looking for any matches in a copied system file of hashed or encrypted user passwords). Informally, in the scenario of PAKE protocols, we say that a protocol is secure against *off-line dictionary attacks* if an adversary who obtains all the communication data between the client and the server is unable to carry out the dictionary attack to obtain the client's password. This can be achieved if and only if there is no verifiable ciphertext based on a human-memorizable password in the protocol run.
- **Unknown key-share attack (UKS) resilience:** UKS is an attack where a party A believes that he shares a key with another party B upon completion of a protocol run (this is in fact the case), but B falsely believes that the key is instead shared with a party $E \neq A$. A basic PAKE protocol should be resilient to this.
- **Perfect forward secrecy (PFS):** If long-term private keys or secrets of any party is compromised, the secrecy of previously established session keys should not be affected. This is an attempt to still offer some form of security guarantee in spite of the fact that the long-term secret has been leaked.
- **Key-compromise impersonation (KCI) resilience:** The compromise of any party's (client or server) long-term key or secret should not enable the adversary to impersonate any other parties.

It is important for a security protocol, as is a PAKE protocol, to be secure not only against known types of attacks [14], [13], [15], [16], [28], [29], [30], [33], [34] including those listed above, but also be designed to resist any kind of

978-0-7695-3838-9/09 $26.00 © 2009 IEEE
DOI 10.1109/NSS.2009.56

attack by an adversary of some defined adversarial power. Indeed, provably secure protocols take the latter approach and provide a reasonable measure of security in the protocol design. Nevertheless, the fact that a protocol is provably secure does not preclude [11], [12], [26], [27], [31], [32] weaknesses or flaws in proofs due to oversights or subtleties in security model definitions. Thus, it is vital that even provably secure protocols are carefully analyzed to ensure they do not miss capturing resistance against any kinds of attacks.

In this paper, we contribute to this direction by showing that both the Nam et al. variant and provably secure Wen et al. variant are susceptible to key compromise impersonation (KCI) attacks [15], [9].

II. Nam et al. and Wen et al. Protocols

We will use the notations given in Table I. Unless otherwise mentioned, all described operations are done modulo p, except operations in the exponents, and all protocols are based on Diffie-Hellman (DH) type assumptions.

Table I
Notations

A, B	The clients
ID_i	The identity of party i
S	The server who stores the identity (ID_i) and password (pw_i) of client i
s	Long-term private key of S
P_S	Equals sP; this is the public key of S
pw_i	Client i's human-memorizable password shared with S
$\mathcal{E}_k(\cdot)$	Symmetric encryption using the secret key, k
$\mathcal{D}_k(\cdot)$	Symmetric decryption using the secret key, k
p	Sufficiently large prime
H	Cryptographic hash function
G	Hash function $\{0,1\}^* \rightarrow G_1$
$x \in_R Z_p^*$	Randomly choosing an element x of Z_p^*

Throughout this paper, $(G_1, +)$ and $(G_2, \cdot)$ denote two cyclic groups of prime order q. A bilinear map [23], $\hat{e} : G_1 \times G_1 \rightarrow G_2$ satisfies the following properties:

- Bilinearity: For all P, $Q \in G_1$ and all a, $b \in Z$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
- Non-degeneracy: There exists a $P \in G_1$ such that $\hat{e}(P, P) \neq 1$.
- Computability: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any P, $Q \in G_1$.

Since the Nam et al. protocol is an improvement of the Wen et al. one, for the rest of this paper our descriptions are based on Nam et al. though all results equally to the Wen et al. variant.

The security of the Nam et al. protocol is based on Weil Diffie-Hellman (WDH) assumption [7], [8]. This assumption states that given groups G_1, G_2 ,a pairing $\hat{e} : G_1 \times G_1 \rightarrow G_2$, and $aP, bP, cP \in G_1$ for random $a, b, c \in Z_p$, it is computationally intractable to compute $\hat{e}(P, P)^{abc} \in G_2$.

Basically, the protocol involves the following five steps (see Fig. 1):

1) A selects a random number $a \in_R Z_p^*$ and computes aP, $Q = G(ID_S)$, and $k_a = H(ID_A, ID_B, aP, P_S, Q, \hat{e}(P_S, aQ))$. Then, A computes $c_a = \mathcal{E}_{k_a}(PW_A)$ and sends $\langle ID_A, aP, c_a \rangle$ to B.
2) B selects a random number $b \in_R Z_p^*$ and computes bP, $Q = G(ID_S)$, $k_b = H(ID_B, ID_A, bP, P_S, Q, \hat{e}(P_S, bQ))$, $R = G(ID_A, ID_B)$, and $K = \hat{e}(aP, bR)$. Then, B computes $c_b = \mathcal{E}_{k_b}(PW_B)$ and $\mu_b = H(ID_B, K)$. B sends $\langle ID_A, aP, c_a, ID_B, bP, c_b, \mu_b \rangle$ to S.
3) Based on ID_A, ID_B from the received message, the server S can retrieve the passwords PW_A, PW_B from the database. S first computes $k_a = H(ID_A, ID_B, aP, P_S, Q, \hat{e}(aP, sQ))$ and $k_b = H(ID_B, ID_A, bP, P_S, Q, \hat{e}(P_S, bQ))$. Then, S checks if $PW_A = \mathcal{D}_{k_a}(c_a)$ and $PW_B = \mathcal{D}_{k_b}(c_b)$ respectively. If not, S stops executing the protocol. Otherwise, S, computes $\sigma_a = H(k_b, aP)$ and $\sigma_b = H(k_a, bP)$, and sends $\langle bP, \mu_b, \sigma_b, \sigma_a \rangle$ to A.
4) A first computes $R = G(ID_A, ID_B)$ and $K = \hat{e}(bP, aR)$. Then, A computes and checks if σ_b and μ_b equal to $H(k_a, bP)$ and $H(ID_B, K)$ respectively. If not, A stops executing the protocol. Otherwise, A computes $\mu_a = H(ID_A, K)$ and the session key $SK = H(aP, bP, R, K)$. Finally, A sends $\langle \mu_a, \sigma_a \rangle$ to B.
5) B checks if $\sigma_a = H(k_b, aP)$ and $\mu_a = H(ID_A, K)$. If not, it terminates the protocol. Otherwise, B computes the session key $SK = H(aP, bP, R, K)$.

With this description, then the Wen et al. protocol is similar except in step (1) where A computes $k_a = H(aP, P_S, Q, \hat{e}(P_S, aQ))$; step (2) where B computes $k_b = H(bP, P_S, Q, \hat{e}(P_S, bQ))$; step (3) where S computes $k_a = H(aP, P_S, Q, \hat{e}(aP, sQ))$ and $k_b = H(bP, P_S, Q, \hat{e}(P_S, bQ))$.

III. On the Security of Both Protocols

Recall the definition of key compromise impersonation (KCI) resilience. In more detail, when an adversary learns the long-term key s of the server S, obviously then the server can be impersonated trivially. Resilience against KCI attacks is formulated so that some sort of security guarantee can still be afforded even when this long-term key is leaked. In particular, though it is clear that the server can be impersonated, yet KCI resilience offers the guarantee that this is the most an adversary could do, and that the adversary cannot impersonate anyone else to S.

We show a key compromise impersonation (KCI) attack on both Nam et al. and Wen et al. protocols that can be mounted by any adversary. In particular, when an adversary learns the long-term key s of the server S, the adversary can impersonate anyone else to S, thus contradicting the KCI resilience requirement. It works as follows:

1) The message $\langle ID_A, aP, c_a \rangle$ from A to B, and similarly the message $\langle ID_B, bP, c_b, \mu_b \rangle$ from B to S are

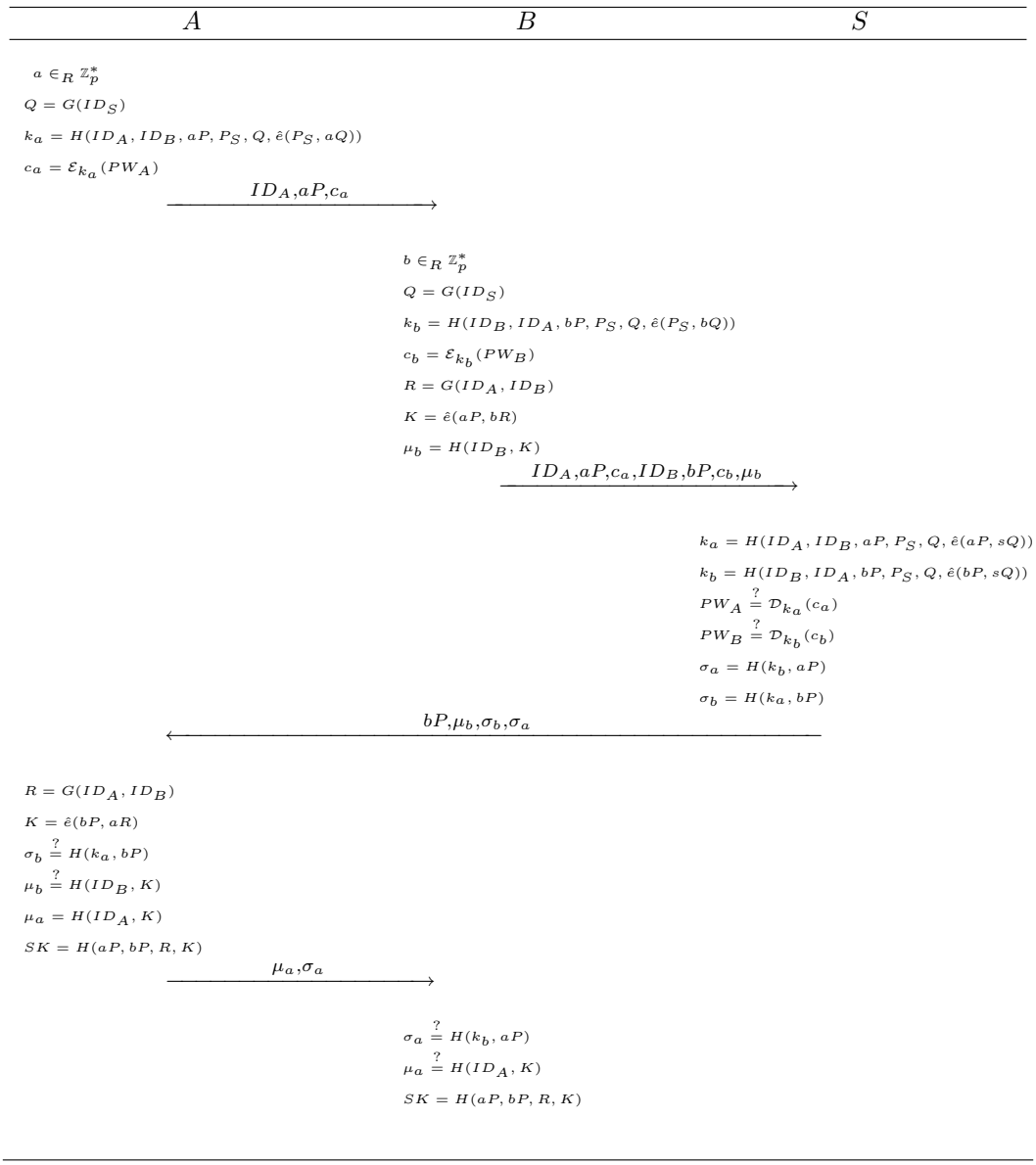

Figure 1. Nam et al. Protocol

easily attainable by a passive eavesdropping adversary C.

2) Upon compromising the long-term key s of the server S, the adversary C is thus able to compute $k_a = H(ID_A, ID_B, aP, Ps, Q, \hat{e}(P_S, aQ))$ and $k_b = H(ID_B, ID_A, bP, Ps, Q, \hat{e}(P_S, bQ))$ ($k_a = H(aP, Ps, Q, \hat{e}(P_S, aQ))$ and $k_b = H(bP, Ps, Q, \hat{e}(P_S, bQ))$ for Wen et al. protocol.), since the only secret input to the computation of k_a and k_b is s.
3) Decrypt c_a and c_b with k_a and k_b respectively. Thus, C can obtain PW_A and PW_B.
4) C can now impersonate A (resp. B) to S because authentication of A (resp. B) to S just depends on PW_A (resp. PW_B).

IV. Conclusion

Wen et al. proposed three-party password-based authenticated key exchange protocol using Weil pairing [37], with security proof in the random oracle model. Nam et al. [25] showed the insecurity of the Wen et al. protocol, and proposed an improvement to counter their attack. Nevertheless, we have demonstrated that the Nam et al. improvement and the original Wen et al. protocol, both do not provide resilience to key-compromise impersonation (KCI) [9] which is nowadays commonly expected of key exchange protocols.

The problem with both protocols lies in that the client password is encapsulated with a function where the only unknown secret input is the long-term private key of the server. KCI attacks can be prevented for instance by having the password encapsulation (in this case c_a or c_b) be a function of not only the long-term private key of the server but also a function of some ephemeral (short-term) unknown variables that are never sent in the clear to another party but instead only used locally within the context of a protocol run.

Nevertheless, we caution against adhocly fixing a protocol without a thorough re-analysis in the provable security model, thus both protocols should not be used in practical applications. Instead, we suggest to use the three-party PAKEs rigorously proven secure in the formal sense, e.g. [1], [3].

ACKNOWLEDGMENT

This research was supported by the Malaysia e-Science Fund (01-02-01-SF0048).

REFERENCES

[1] M. Abdalla, P.-A. Fouque, and D. Pointcheval. Password-Based Authenticated Key Exchange in the Three-Party Setting. *Proc. PKC '05*, LNCS 3386, pp. 65-84, 2005.

[2] M. Abdalla and D. Pointcheval. Interactive Diffie-Hellman Assumptions with Applications to Password-Based Authentication. *Proc. FC '05*, LNCS 3570, pp. 341-356, 2005.

[3] M. Abdalla and D. Pointcheval. Interactive Diffie-Hellman Assumptions with Applications to Password-Based Authentication. Full version of [2], available online at `http://www.di.ens.fr/~pointche/pub.php?reference=AbPo05`.

[4] M. Bellare and P. Rogaway. Provably Secure Session Key Distribution: the Three Party Case. *Proc. ACM Symposium on the Theory of Computing (STOC '95)*, pp. 57–66, 1995.

[5] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated Key Exchange Secure against Dictionary Attacks. *Advances in Cryptology - Eurocrypt '00*, LNCS 1807, pp. 139-155, 2000.

[6] S. Bellovin and M. Merritt. Encrypted Key Exchange: Passwords based Protocols Secure against Dictionary Attacks. *Proc. IEEE Symposium on Security & Privacy '92*, pp. 72-84, 1992.

[7] D. Boneh and M. Franklin. Identity Based Encryption from the Weil Pairing. *Advances in Cryptology - Crypto '01*, LNCS 2139, pp. 231-229, 2001.

[8] D. Boneh and M. Franklin. Identity Based Encryption from the Weil Pairing. *SIAM Journal on Computing*, Vol. 32, No. 3, pp. 586-615, 2003.

[9] C. Boyd and A. Mathuria. *Protocols for Authentication and Key Establishment*. Springer-Verlag, 2003.

[10] C-C. Chang and Y-F. Chang. A Novel Three-party Encrypted Key Exchange Protocol. *Computer Standards and Interfaces* Vol 26, No. 5, pp.471-476, 2004.

[11] K.-K.R. Choo, C. Boyd and Y. Hitchcock. Examining Indistinguishability-based Proof Models for Key Establishment Protocols. *Advances in Cryptology - ASIACRYPT '05*, LNCS 3788, pp. 585-604, 2005.

[12] K.-K.R. Choo, C. Boyd and Y. Hitchcock. Errors in Computational Complexity Proofs for Protocols. *Advances in Cryptology - ASIACRYPT '05*, LNCS 3788, pp. 624-643, 2005.

[13] W. Diffie, P.C. van Oorschot and M.J. Wiener, Authentication and Authenticated Key Exchanges. *Design, Codes and Cryptography*, Vol. 2, No. 2, pp. 107-125, 1992.

[14] Y. Ding and P. Horster. Undetectable On-line Password Guessing Attacks. *ACM Operating Systems Review*, Vol. 29, No. 4, pp.77-86, 1995.

[15] M. Just and S. Vaudenay. Authenticated Multi-Party Key Agreement. *Advances in Cryptology - Asiacrypt '96*, LNCS 1163, pp. 36-49, 1996.

[16] B.S. Kaliski Jr, An Unknown Key-Share Attack on the MQV Key Agreement Protocol. *ACM TISSEC*, Vol. 4, No. 3, pp. 275-288, 2001.

[17] 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.

[18] 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

[19] 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.

[20] S.W. Lee, H.S. Kim, and K.Y. Yoo. Efficient Verifier-based Key Agreement Protocol for Three Parties without Servers Public Key. *Applied Mathematics and Computation* Vol 167, No. 2, pp. 996-1003, 2005.

[21] X.-J. Lin, C.-K. Wu, and F. Liu. Analysis of an Authenticated Identity-based Multicast Scheme. *IET Communications* Vol. 2, No. 7, pp. 935?37, 2008.

[22] R. Lu and Z. Cao. Simple Three-party Key Exchange Protocol. *Computers & Security*, Vol. 26, pp. 94-97, 2007.

[23] A. Menezes, T. Okamoto, and S. Vanstone. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transaction on Information Theory*, Vol. 39, pp. 1639-1646, 1993.

[24] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. *Handbook of Applied Cryptography*, CRC Press, 1997.

[25] 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, pp. 1364-1375, 2007.

[26] K. Ouafi, and R.C.-W. Phan. Privacy of Recent RFID Authentication Protocols. In *Proc. ISPEC '08*, LNCS 4991, pp. 263-277, Springer-Verlag, 2008.

[27] K. Ouafi, and R.C.-W. Phan. Traceable Privacy of Recent Provably-Secure RFID Protocols. In *Proc. ACNS '08*, LNCS 5037, pp. 479-489, Springer-Verlag, 2008.

[28] R.C.-W. Phan. Security Limitations of Authorized Anonymous ID-based Authentication Scheme for Mobile Communication. *IEEE Communications*, Vol. 43, No. 5, pp. 149-153, 2005.

[29] R.C.-W. Phan. Fixing the Integrated Diffie-Hellman-DSA Key Exchange Protocol. *IEEE Communications Letters*, Vol. 9, No. 6, pp. 570-572, 2005.

[30] R.C.-W. Phan, and B.-M. Goi. Cryptanalysis of an Improved Client-to-Client Password-Authenticated Key Exchange (C2C-PAKE) Scheme. In *Proc. ACNS '05*, LNCS 3531, pp. 33-39, Springer-Verlag, 2005.

[31] R.C.-W. Phan, and B.-M. Goi. Cryptanalysis of the N-Party Encrypted Diffie-Hellman Key Exchange using Different Passwords. In *Proc. ACNS '06*, LNCS 3989, pp. 226-238, Springer-Verlag, 2006.

[32] R.C.-W. Phan, and B.-M. Goi. Cryptanalysis of Two Provably Secure Cross-Realm C2C-PAKE Protocols. In *Progress in Cryptology - Indocrypt '06*, LNCS 4329, pp. 104-117, Springer-Verlag, 2006.

[33] R.C.-W. Phan, B.-M. Goi, and K.-H. Wong. Cryptanalysis of Some Improved Password-Authenticated Key Exchange (PAKE) Schemes. *Computer Communications*, Vol. 29, No. 15, pp. 2822-2829, 2006.

[34] R.C.-W. Phan, 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.

[35] H-M. Sun, B-C. Chen, and T. Hwang. Secure Key Agreement Protocols for Three-party against Guessing Attacks. *The Journal of Systems and Software* Vol 75, pp.63-68, 2005.

[36] 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.

[37] H.-A. Wen, T.-F. Lee, and T. Hwang. Provably Secure Three-party Password-based Authenticated Key Exchange Protocol using Weil Pairing. *IEE Proceedings - Communications* Vol. 152 No. 2 pp. 138-143, 2005.