Breaking provably secure SAKE-C authenticated key exchange protocol with Extended Key Compromise Impersonation (E-KCI) Attack

Ali Mackvandi
Pishgaman International Enterprise
Security & Privacy Department
Yazd-Iran
Mackvandi@pishgaman.com

Maryam Saeed
Iran University of Science & Technology
Department of ICT
Tehran-Iran
M_saeed@vu.iust.ac.ir

Mansour Naddafiun
Pishgaman International Enterprise
Security & Privacy Department
Yazd-Iran
Naddafiun@pishgaman.com

***Abstract*— *Authenticated* Key Exchange (AKE) protocols are those protocols that allow two or more entities to concur with a common session key in an authentic manner in which this key is used to encrypt the proceeding communications. In 2010, Zhao et al. proposed Provably Secure Authenticated Key Exchange Protocol under the CDH Assumption (referred to as SAKE and SAKE-C). Despite the fact that the security of the proposed protocol is proved in the formal model, due to not considering all the prerequisite queries in defining and designing formal security model, in this paper it is shown that the so-called secure protocol is vulnerable to Extended Key Compromise Impersonation (E-KCI) attack so that this attack is a practicable flaw that was signaled by Tang et al. for the first time in 2011. It is furthermore worth mentioning that Tang et al. applied E-KCI attack to the famous 3-pass HMQV protocol. It is also noteworthy that the E-KCI attack is verified by D. Pointcheval in Tang et al.'s paper.**

Index Terms*— *AKE (Authenticated Key Exchange), Cryptographic protocols, Extended KCI attack, Security Analysis.

I. INTRODUCTION

THE indispensable need for maintaining the security, privacy, and reliability of transmitting data over the Internet made many researchers propose and devise different methods based on the cryptographic approaches. To the best of our knowledge, the first practical step in preserving the privacy and security of the vital transmitting data is to establish a common symmetric encryption session key in a secure manner between two or more intended entities. Another burning issue is key authentication that should be achieved between the corresponding parties in an authentic way. In other words, key authentication is achieved successfully when communicating parties assure that they are the only ones who are cognizant of the fresh agreed-upon session key. If a KE protocol provides mutual authentication, it is called authenticated Key Exchange (AKE) protocol. Consequently, numerous Key Exchange protocols (KE) have been proposed and studied over the past years to provide a diversity of security needs, the most secure and efficient of which are surveyed in [1,2]. Also, the most recent studies on KE protocols can be referred to the seminal work of Diffie-Hellman and Needham-Schroeder in [3,4]. Furthermore, the standardization associations including IEEE and ISO have proposed several key establishment standards in the literature [5,6,7].

While we are encountering with new attacks and threats on the Internet day in and day out, it is perspicuous that designing and proposing a secure protocol, being able to resist these ongoing vulnerabilities, is not a trivial task. Consequently, it is incumbent on the protocol designers to take into consideration all the imperative security attributes throughout designing their protocols since, in case of any negligence in designing such protocols, ineluctable and irreparable losses will be brought about.

It is also worth mentioning that analyzing the security of the proposed protocols is commonly achieved in the formal models, but defining a proper model is not a inconsequential task, because not taking account of some types of queries, e.g. the *Corrupt Query* [8,9], or malapropos defining the adversarial game [10] may prompt a security proof that fails to capture valid attacks, and this matter disproves the belief that a security proof in the Random Oracle Model means that there are no structural flaws in the scheme [11].

It is essential for AKEs to provide the following desirable security attributes [13,15,16,17,18]:

- **Forward secrecy:** The forward secrecy is provided if the secrecy of previously established session keys is not divulged by compromising any entity's password or long-term private keys.
- **Known session key security:** Compromising the one session key should not jeopardize the security of other session keys.
- **Resilience to Unknown Key Share attack (UKS):** User $\mathcal{A}$ should not be compelled into sharing a session key with an adversary E after the completion of a protocol run, while $\mathcal{A}$ falsely thinks that his/her key is shared with user B.
- **Resilience to password compromise impersonation attack:** Disclosure of any user $\mathcal{A}$'s password should not allow an adversary to share any session key with $\mathcal{A}$ by masquerading him- or herself as any other entity.
- **Resilience to ephemeral key compromise impersonation attacks:** Some protocols deploy some random parameters as the ephemeral keys. Disclosure of any user $\mathcal{A}$'s ephemeral

key should not enable an adversary to establish a session key with $\mathcal{A}$ by impersonating him- or herself as any other participant.

- **Resilience to extended Key Compromise Impersonation (KCI) attack**: Exposure of any participant $\mathcal{A}$'s long-term and ephemeral secrets should not allow an adversary to share any session key with $\mathcal{A}$ by masquerading him- or herself as any other entity.

In 2010, Zhao et al. [12] proposed Provably Secure Authenticated Key Exchange Protocol under the CDH Assumption (referred to as SAKE-C). In spite of the fact that the security and efficiency of the SAKE-C protocol is proved in the formal model and that it is asserted that one of the expected and desirable security attributes of a secure AKE protocol is resistance to KCI attack, but the designers of [12] did not take into consideration all the fundamental security features in defining their formal security model, causing their proposed protocol to be vulnerable to the Extended KCI attack. The E-KCI attack is a feasible threat in the real world since an adversary can easily gain access to the confidential information of users by exploiting different malwares which can be installed on the victim's system platform or the adversary can utilize the imperfectness of the pseudo-random number generator in practice [13]. It is also notable that the E-KCI attack is upheld by D. Pointcheval in [13].

The rest of the paper is organized as follows. Section 2 explicates the notation used hereinafter and reviews the SAKE-C protocol [12] in brief, while its security vulnerability is elucidated in Section 3. Finally, the conclusion is drawn in Section 4.

II. A Brief Review On SAKE-c Protocol

In this section, in concise, we scrutinize SAKE-C protocol [12] in Fig.1. It is noteworthy that SAKE protocols consist of two versions, namely SAKE and SAKE-C. There is a slight difference between these two proposed versions in which the former requires two communication rounds without providing Perfect forward Secrecy(PFS) and key confirmation whereas the latter requires three rounds of communications that satisfies PFS and key confirmation. For the sake of simplicity, we will zero in on the SAKE-C protocol, since it is asserted that this version is more secure and robust in comparison with the other one. The notations applied in this protocol are listed in Table1.

The running steps of the SAKE-C protocol, which is depicted in Fig.1, proceed as follows:

(1) The participant $\mathcal{A}$ selects an ephemeral key $x' \in_{\mathcal{R}} \mathbb{Z}_q$ and computes $x = H_1(x', a)$, $X = g^x$, $e_A = H_2(X, ID_B)$, $S_A = (x - a.e_A)$, $\alpha_A = g^{S_A}$, respectively and sends α_A, e_A to $\mathcal{B}$.

(2) Upon receiving α_A, e_A from $\mathcal{A}$, $\mathcal{B}$ verifies the validation of e_A by computing $X' = \alpha_A.A^{e_A}$ and $e'_A = H_2(X', ID_A)$. If $e_A = e'_A$, it means $X = X'$. Then, $\mathcal{B}$ chooses an ephemeral key $y' \in_{\mathcal{R}} \mathbb{Z}_q$ and calculates $y = H_1(y', b)$, $Y = g^y$, $S_B = (y - b.e_B)$, $\alpha_B = g^{S_B}$, $\mathcal{Z}_1 = X^{y+b}$, $\mathcal{Z}_2 = (XA)^y$, $SK = H(\mathcal{Z}_1, \mathcal{Z}_2, ID_A, ID_B)$, $\sigma = (1, \alpha_A, \alpha_B, ID_A, ID_B)$, $MAC_{SK}(\sigma)$, respectively, and sends $\alpha_B, e_B, MAC_{SK}(\sigma)$ to $\mathcal{A}$.

Table 1. Deployed Notations

Notation	Definition
ID_A, ID_B	Identities of users $\mathcal{A}$ and $\mathcal{B}$, respectively.
P, q, g	Two large primes p and q with q|(p−1), and a generator g of group G with order q.
A, a	Long-term key pair of $\mathcal{A}$, in which $A = g^a$ modp.
B, b	Long-term key pair of $\mathcal{B}$, in which $B = g^b$ modp.
x', y'	Ephemeral keys of $\mathcal{A}$ and $\mathcal{B}$, respectively.
$H_1, H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q$	Two collision-free one-way hash functions modeled as random oracles.
$H: \{0,1\}^* \rightarrow \{0,1\}^{\lambda}$	Collision-free one-way hash function modeled as a random oracle, where λ is a security parameter.
SK	Session key established by the users.

(3) Likewise, upon receiving $\alpha_B, e_B, MAC_{SK}(\sigma)$ from $\mathcal{B}$, $\mathcal{A}$ also verifies the authenticity of e_B by computing $Y' = \alpha_B.B^{e_B}$ and $e'_B = H_2(Y', ID_A)$. If $e_B = e'_B$, it means $Y' = Y$. Then, $\mathcal{A}$ computes $\mathcal{Z}_1 = (YB)^x$, $\mathcal{Z}_2 = Y^{x+a}$, $SK = H(\mathcal{Z}_1, \mathcal{Z}_2, ID_A, ID_B)$, $\sigma' = (0, \alpha_A, \alpha_B, ID_A, ID_B)$, and $MAC_{SK}(\sigma')$. Also, $\mathcal{A}$ checks the validity of $MAC_{SK}(\sigma')$=$MAC_{SK}(\sigma)$. If it holds, then $\mathcal{A}$ sends $MAC_{SK}(\sigma')$ to $\mathcal{B}$.

(4) As soon as $\mathcal{B}$ revieves $MAC_{SK}(\sigma')$, s/he checks if $MAC_{SK}(\sigma')$=$MAC_{SK}(\sigma)$. If the equality holds, $\mathcal{B}$ assures of the legitimacy of $\mathcal{A}$.

At this stage, both entities share their common session key and verify the validity of the exchanged key *SK*.

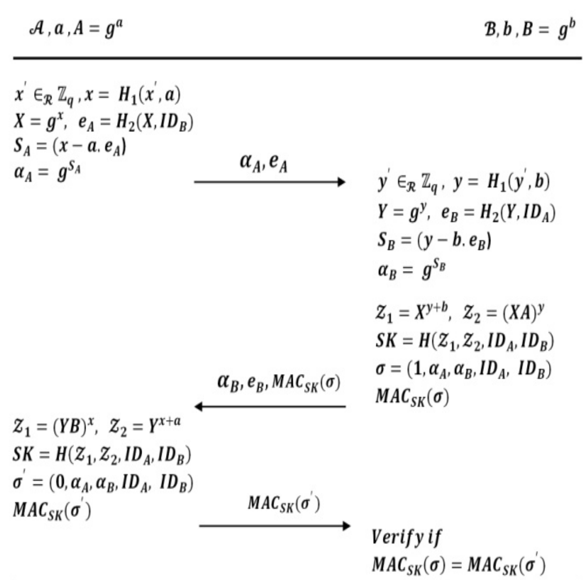

Fig.1. The 3-pass SAKE-C protocol.

III. Security Analysis of SAKE-C protocol

Vulnerability to Extended Key Compromise Impersonation (E-KCI) attack:

In this section, it is shown that the proposed protocol [12] is subject to E-KCI attack. As it is mentioned, the E-KCI attack is demonstrated for the first time by [13] and they proved that this attack is a feasible threat in the real world, because an adversary can easily gain access to the confidential information of users by exploiting different malwares which can be installed on victim's system platform or the adversary can misuse of the imperfectness of the pseudo-random number generator in use [13]. Into the bargain, it is noteworthy that the E-KCI attack is confirmed by D. Pointcheval in Tang et al.'s paper.

The E-KCI attack is reasonably straightforward and can proceed as follows:

(1) The adversary initiates the E-KCI attack against Alice by compromising Alice's long-term private key a and the Diffie-Hellman ephemeral key x', respectively. Then, s/he can pose himself/herself as the opposite party, Bob, and carry on the protocol steps.

(2) Upon receiving α_A, e_A from Alice, the adversary sequentially selects $y' \in_{\mathcal{R}} \mathbb{Z}_q$, and computes $y = H_1(y', b), Y = g^y,\ e_B = H_2(Y, ID_A), S_B = (y - b.e_B)$, $\alpha_B = g^{S_B}$, $\mathcal{Z}_1 = X^{y+b},\ \mathcal{Z}_2 = (XA)^y$, $SK = H(\mathcal{Z}_1, \mathcal{Z}_2, ID_A, ID_B)$, $\sigma = (1, \alpha_A, \alpha_B, ID_A,\ ID_B)$, and $MAC_{SK}(\sigma)$. Then, the adversary sends $\alpha_B, e_B, MAC_{SK}(\sigma)$ to Alice.

(3) After receiving $\alpha_B, e_B, MAC_{SK}(\sigma)$, Alice first verified the validity of e_B by computing $Y' = \alpha_B . B^{e_B}$ and $e'_B = H_2(Y', ID_A)$. If $e_B = e'_B$, it means $Y' = Y$. Then, $\mathcal{A}$ computes $\mathcal{Z}_1 = (YB)^x,\ \mathcal{Z}_2 = Y^{x+a}$, $SK = H(\mathcal{Z}_1, \mathcal{Z}_2, ID_A, ID_B)$ and $\sigma' = (0, \alpha_A, \alpha_B, ID_A,\ ID_B)$. Finally, Alice computes $MAC_{SK}(\sigma')$ for verification and sends it to the adversary.

At this moment in time, the adversary is succeeded to impersonate him-or herself as $\mathcal{B}$ and shares a valid session key with the participant $\mathcal{A}$.

IV. Conclusion and Countermeasure

In this paper, the provably secure SAKE-C protocol is analyzed. Notwithstanding the fact that the security of the analyzed protocol is evinced and proved in the formal model, we demonstrated that how easy the adversary can apply E-KCI attack which is introduced for the first time by Tang et al. on this protocol by installing some Trojans on the victim's system or the adversary can employ the imperfectness of the pseudo-random number generator and breaks the protocol. Unfortunately, it goes without saying that most of the PAKE and AKE protocols are vulnerable to E-KCI attack which is a new-introduced flaw in this field, because even one of the most famous PAKE protocols such as the 3-pass HMQV protocol suffers from this vulnerability.

As a countermeasure, it is suggested that a deterministic EU-CMA secure signature can be employed in the protocols. Through a deterministic signature, we mean that a signature is a function of the private signing key and a signed message, and does not require any ephemeral secret, since we presume that our resolution works in the environment where the ephemeral secret might be in jeopardy. For instance, we select the BLS signature for a reasonably good functioning [14], in spite of the fact that other secure deterministic signature schemes should also be adequate.

References

[1] C. Boyd, A. Mathuria, "Protocols for Authentication and Key Establishment," Springer, 2004.

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

[3] W. Diffie, M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory IT-22 (6) (1976) 644–654.

[4] R. Needham, M. Schroeder, "Using encryption for authentication in large networks of computers," Communications of the ACM 21 (12), 993-999, 1978.

[5] Institute of Electrical and Electronics Engineers, Inc. IEEE P1363-2000: Standard Specifications for Public-Key Cryptography and IEEE 1363a-2004: Standard Specifications for Public-Key Cryptography – Amendment 1: Additional Techniques.

[6] Institute of Electrical and Electronics Engineers, Inc. IEEE P1363.2 draft D26, Standard Specifications for Password-Based Public-Key Cryptographic Techniques, September 2006.

[7] International Organization for Standardization, ISO/IEC 11770 (all parts), Information technology-Security techniques-Key management.

[8] K.-K. Choo, C. Boyd, and Y. Hitchcock, "Errors in computational complexity proofs for protocols," in: Advances in Cryptology Asiacrypt05, LNCS, 3788:624–643, 2005.

[9] K.-K. Choo, C. Boyd, and Y. Hitchcock, "Examining indistinguishability- based proof models for key establishment protocols," in: Advances in Cryptology Asiacrypt05, LNCS, 3788:585-604, 2005.

[10] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in: Proceedings of the 19th international conference on Theory and application of cryptographic techniques, LNCS, 1807:139–155, 2000.

[11] R. Canetti, O. Goldreich, S. Halevi, " The random oracle methodology," in: Proceeding of the 30th ACM Symp, on Theory of computing(STOC), Pages 209-218, 1998.

[12] J. Zhaoa, D. Gu, "Provably secure authenticated key exchange protocol under the CDH assumption," Systems and Software, 83(11): 2297-2304, 2010.

[13] Q. Tang, L. Chen, "Extended KCI attack against two-party key establishment protocols," Information Processing Letters, 111(15): 744-747, 2011.

[14] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," Journal of Cryptology 17 (4) (2004) 297–319.

[15] M. Gouda, A. Liu, L. Leung, and M. Alam, "Spp: An anti-phishing single password protocol," Computer Networks, 51(13):3715–3726, 2007.

[16] S. Halevi and H. Krawczyk, "Public-key cryptography and password protocols," ACM Transactions on Information and System Security (TISSEC), 2(3):230 – 268, 1999.

[17] M. Saeed and H. Shahhoseini, "Security Analysis and Improvement of Smart Card-based Authenticated Key Exchange Protocol with CAPTCHAs for Wireless Mobile Network," In: Proceedings of the 2011 IEEE 16th Symposium on Computers and Communications (ISCC2011), pp. 652 - 657 July, 2011.

[18] M. Saeed, H. Shahhoseini, and A. Mackvandi, "An Improved two-party Password Authenticated Key Exchange Protocol without Server's Public Key," In: Proceedings of the 2011 IEEE 3th International Conference on Communication Software and Networks (ICCSN 2011), pages: 90–95, January, 2011.