IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. II (Jan – Feb. 2015), PP 71-74
www.iosrjournals.org

Cryptanalysis of Efficient Unlinkable Secret Handshakes for Anonymous Communications

Preeti Kulshrestha[1], Arun Kumar Pal[1], Manmohan Singh Chauhan[2]
[1] *(Department Of Mathematics, Statistics & Computer Science,*
G.B. Pant University Of Agriculture And Technology Pantnagar, India)
[2]*(DST- Center For Interdisciplinary Mathematical Sciences,*
Banaras Hindu University, Varanasi, India)

Abstract: *Several unlinkable secret handshakes schemes have been proposed in recent years. As performing the successful secret handshakes is essentially equivalent to computing a common key between two interactive members of the same group. Therefore secret handshakes scheme is a key agreement protocol between two members of the same group. So it is necessary for a secret handshakes scheme to fulfill security requirement of secret handshakes protocol as well as key agreement protocol. In this Paper, we show that the Ryu et al. unlinkable secret handshakes scheme does not provide key compromise impersonation resilience which is an important requirement in ID-based two party authenticated key exchange scheme.*
Keywords: *Authentication, Key Agreement, Unlinkability, Secret Handshakes, Cryptanalysis*

I. Introduction

The secret handshake, which allows two parties of the same group to authenticate each other secretly and privately and shared a secret key for further communication over an open channel, was first introduced by Balfanz et al. [1] in 2003. They also introduced a 2-party secret handshake scheme by adapting the key agreement protocol of Sakai et al. [5], based on bilinear maps. The scheme is secure under the BDH assumption. It uses one time credentials to achieve the unlinkability, which means that each user must store a large number of credentials. An unlinkable secret handshakes scheme provides unlinkability which means that two different instances of the same party cannot be linked by the observer.

Xu -Yung [7] in 2004 present the first SH scheme that achieves unlinkability while allowing users to reuse their credentials. They introduce the concept of k-anonymous secret handshake where k is an adjustable parameter indicating the desired anonymity assurance.

Huang -Cao [3] in 2009 proposed an efficient unlinkable secret handshakes scheme and claimed that scheme achieve affiliation hiding and unlinkability later on which is proved by Su [6] and Youn -Park [9] that Huang -Cao Scheme have a design flaw and insecure.

Ryu, Yoo and Ha [4] in 2010 proposed an efficient unlinkable secret handshakes scheme for anonymous communications allowing arbitrary two communicating parties with same role in either one single group or multiple groups to privately authenticate each other.

Gu -Xue [2] in 2011 proposed an improved secret handshakes scheme with unlinkability based on the Huang -Cao scheme. Yoon [8] in 2011 points out that Gu -Xue scheme is insecure to key compromise impersonation attack and cannot provide master key forward secrecy.

In this paper we will show that Ryu et al. [4] unlinkable secret handshakes scheme is insecure under the key-compromise impersonation attack (K-CI), which was described in [8] while [4] provide better performance in terms of both computational and communication cost as compared to previous work. As successful secret handshakes is equivalent to a key agreement between two members of the same group. So it is necessary for a secret handshakes scheme to fulfill security requirement of secret handshakes protocol as well as key agreement protocol. K-CI resilience is one of the most important security requirements in key exchange protocol but unfortunately Ryu et al. [4] scheme is fail to achieve this security requirement.

The rest of this paper is organized as follows. In section II, we briefly review the bilinear group and secure property of the secret handshakes and key agreement protocol. In section III, we review the protocol of Ryu et al. scheme. In section IV we show that Ryu et al. scheme suffer from K-CI attack. We draw our conclusion in section V.

II. Preliminaries

2.1 Bilinear Pairing:

Let G and G' are two cyclic additives group and G_T be a cyclic multiplicative group of the same large prime order q. Let P be a generator of G and Q be the generator of G' then a Bilinear Pairing on (G, G') is a function $e: G \times G' \to G_T$ with the following properties:

(1) Bilinearity: for all $P \in G,\ Q \in G'$ and $a, b \in Z_q$, then, $e(aP, bQ) = e(P, Q)^{ab}$.

(2) Non-Degeneracy: $e(P, Q) \neq 1$

(3) Computability: e can be efficiently computed in polynomial time.

2.2 Security Property:

A secret handshakes scheme must have the following security properties:

Completeness/ Correctness: If two honest members *A, B* belonging to the same group and *A, B* run handshake protocol with valid credentials of their identities and group public keys, then both members always output *accept.*

Impersonator Resistance: An adversary not satisfying the rules of the handshake protocol is unable to successfully authenticate to an honest member.

Detector Resistance: An adversary not satisfying the rules of the handshake protocol cannot decide whether some honest party satisfies the rule or not.

Unlinkability: It is not feasible to tell whether two execution of the handshake protocol were performed by the same party or not, even if both of them were successful.

2.3 Fundamental Security Property For Key Agreement:

A key agreement protocol must have the following security properties:

Known-Key Security: In each round of a key agreement between *A* and *B*, both the user should produce a unique secret key; such a key is called a session key and should not be exposed if other secret keys are compromised.

Forward Secrecy: If long-term private keys of one or both entities are compromised, the secrecy of previous session keys established by honest entities should not be affected.

Key-Compromise Impersonation Resilience: If entity *A's* long-term private key is disclosed then an adversary who knows this value can impersonate *A*, but this should not enable an adversary to impersonate other entities as well and obtain the session key.

Unknown Key-Share Resilience: An entity *A* should not be able to be coerced into sharing a key with any entity *C* when entity *A* believes that he is sharing the key with another entity *B*.

III. Review Of Ryu, Yoo And Ha Scheme

This section is briefly reviews the Ryu et al. scheme [4]. given a security parameter k, the algorithm generates the system parameters params $(G, G', G_T, q, e, P, P')$, where $G,\ and\ G'$ are two cyclic additive group of same prime order q, P is the generator of G, P' is the generator of G', and G_T is the cyclic multiplicative group of prime order q, and $e: G \times G' \to G_T$ is a bilinear pairing. Let $H_o: \{0,1\}^* \to G'$, and H_1, H_2 be collision resistant hash functions taking arbitrary string as input, such as SHA-1. A group authority GA for each group is associated with a unique pair (pk, sk) of keys, such that $pk = sP$ and $sk = s$, where s is the group master secret. Also, each group member in the group is assumed to be associated with a group secret key $S = s.H_0(gid \| role) \in G'$, corresponding to the group identity gid and the role $role$ to the party.

The protocol is a 3-round interactive communication algorithm executed by arbitrary two communication parties. Concatenation of two strings is denoted by $\|$ and by A, B two communication parties. ini and res are predefined values, representing initiator and responder, respectively.
The protocol works as follows:

Round 1. $A \rightarrow B$: R_A

1.1) Choose a random k - bit value r_A

1.2) Compute $R_A = r_A P$

1.3) Send R_A to B.

Round 2. $B \rightarrow A$: R_B, $resp_B$

2.1) Choose a random k - bit value r_B

2.2) Compute $R_B = r_B P$, $K_B = e(R_A, S_B)^{r_B}$ and $resp_B = H_1(K_B \| R_A \| R_B \| res)$

2.3) Send R_B, $resp_B$ to A.

Round 3. $A \rightarrow B$: $resp_A$

3.1) Compute $K_A = e(R_B, S_A)^{r_A}$ and verify if $resp_A = H_1(K_A \| R_A \| R_B \| res)$

3.2) If its holds, compute $resp_A = H_1(K_A \| R_A \| R_B \| ini)$

3.3) Send $resp_A$ to B.

3.4) Upon receiving $resp_A$, B verifies it using its own key K_B, in the exactly same way as A.

If A and B are in the same group with the same role i.e. $S_A = s_A.H_0(gid_A \| role_A) = s_B.H_0(gid_B \| role_B) = S_B$ they will successfully authenticate their respective memberships, due to fact that
$K_A = e(R_B, S_A)^{r_A} = e(P, S_A)^{r_A \cdot r_B} = e(P, S_B)^{r_A \cdot r_B} = e(R_A, S_B)^{r_B} = K_B$. After the verification succeeds, A and *B* can compute the shared key for further communication as
$SK_A = H_2(K_A \| R_A \| R_B \| resp_A \| resp_B)$, and $SK_B = H_2(K_B \| R_A \| R_B \| resp_A \| resp_B)$ respectively.

IV. Cryptanalysis Of Ryu, Yoo And Ha Scheme

Key Compromise Impersonation Resilience: If legitimate entity *A's* long-term private key is compromised, then an adversary E is able to impersonate *A.* But this should not enable E to impersonate other legitimate entities to *A.* we show that Ryu et al. scheme [4] is insecure to K-CI attack.
Let private key of user A is $S_A = s_A.H_0(gid_A \| role_A)$, which disclosed to the adversary E. Then adversary E can impersonate to A as B (as any registered user of group) as follows:

1. E chooses r_B and compute $R'_B = r_B P$, send R'_B to A.
2. User A chooses r_A and compute $R_A = r_A P$, $K_A = e(R'_B, S_A)^{r_A}$ and message authentication value $resp_A = H_1(K_A \| R_A \| R'_B \| res)$, send R_A, $resp_A$ to *B* (which is adversary E).
3. Upon receiving $R_A, resp_A$ from A, adversary E compute $K'_B = e(R_A, S_A)^{r_B}$ and $resp'_B = H_1(K'_B \| R_A \| R'_B \| ini)$, send $resp'_B$ to A.

Upon receiving $resp'_B$ from E , A verify if $resp'_B \stackrel{?}{=} H_1(K_A \| R_A \| R'_B \| ini)$ which is always hold as $K_A = K'_B = e(P, S_A)^{r_A \cdot r_B}$, therefore A computes the shared key as

$SK_A = H_2\left(K_A \| R_A \| R'_B \| resp_A \| resp'_B\right)$ since adversary E is corrupt party, it does not need to verify the message authentication value $resp_A$ as the honest party therefore it accepts the computed value SK'_B as the session key. So E computes common session key as follows:

$$SK'_B = H_2\left(K'_B \| R_A \| R'_B \| resp_A \| resp'_B\right).$$

Hence using the private key of user A, adversary E can impersonate as the other parties in the same group, therefore Ryu et al. scheme cannot secure in K-CI attack.

V. Conclusion

In this paper we have shown that the Ryu et al. unlinkable secret handshakes scheme is insecure against the key-compromise impersonation attack though scheme provides strong anonymity.

Acknowledgements

The authors express sincere thanks to professor sunder lal for his help and encouragement.

References

[1]. D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, And H.-C. Wong, Secret Handshakes From Pairing Based Key Agreement, IEEE Symposium On Security And Privacy, 2003, 180-196.
[2]. J. Gu And Z. Xue, An Improved Efficient Secret Handshakes Scheme With Unlinkability, IEEE Communications Letters, 15(2), 2011, 259-261.
[3]. H. Huang And Z. Cao, A Novel And Efficient Unlinkable Secret Handshakes Scheme, IEEE Communications Letters, 13(5), 2009, 363-365.
[4]. E. K. Ryu, K. Y. Yoo And K. S. Ha, Efficient Unlinkable Secret Handshakes For Anonymous Communications, Journal Of Security Engineering, 17(6), 2010, 619-626.
[5]. R. Sakai, K. Ohgishi And M. Kasahara, Cryptosystems Based On Pairing, Symposium On Cryptography And Information Security, 2000, 26-28.
[6]. R. Su, On The Security Of A Novel And Efficient Unlinkable Secret Handshakes Scheme, IEEE Communications Letters, 13(9), 2009, 712-713.
[7]. S. Xu And M. Yung, K- Anonymous Secret Handshakes With Reusable Credentials, In Proc. CCS'04: 11th ACM Conference On Computer And Communications Security, 2004, 158-167.
[8]. E. J. Yoon, Cryptanalysis Of An Efficient Secret Handshakes Scheme With Unlinkability, International Conference On Advances In Engineering, 24, 2011, 128-132.
[9]. T. Y. Youn And Y. H. Park, Security Analysis Of An Unlinkable Secret Handshakes Scheme, IEEE Communications Letters, 14(1), 2010, 4-5.