Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8170 - 8174
Received 16 February 2021; Accepted 08 March 2021.

Fixing the Generalized Integrated Diffie-Hellman-DSA Key Exchange Protocol

Y. Venkatramana Reddy[1]
[1]Anurag University, Hyderabad, India. E-mail: vaiviar@ieee.org

ABSTRACT
A few integrated key exchange schemes providing authenticate DSA signature have been proposed in the new literature to provide authentication to the diffie-hellman key exchange.Generalized scheme for Phan's work[9].devised in this article. Our generalized key exchangescheme is suitable for resource sharing applications, like cloud computing, distributed computing and internet banking for joint accounts.

KEYWORDS
Exchange Protocol, Reveal Attacks, Phan's Schemes.

Introduction

Secret communication key(s) is (are) established by a key agreement protocol among all parties involved based on exchanged public keys. Well known key distribution scheme was proposed by diffie and hellman (DH) [3] in 1976, on the basis of discrete logarithm to enable two parties to establish a common secret key. A series of security standards under Federal Information Processing Standard (FIPS) [12] has been published by NIST in the past years. Digital signature algorithm is introduced by FIPS 186-2 digital signature standard. FIPS standard for key agreement between two parties is not available so far. For achieving key authentication replacing the message in the DSA algorithm with DH key exchange was suggested by Arazi[1] in 1993. Weakness in Arazi's scheme was detected by Nyberg and Rueppel [8]. A kind of attack known as known key attack, because when one secret session key is compromised which results in the disclosure of other keys as well.Unknown key attack which is another kind of attack involves coercion of known parties by an opponent into establishing secret key when t least one of the honest parties is not aware of the secret key shared with the others. Third kind of attack namely key replay attack takes place where the information of the on going session is recorded by attacker and then it is replayed to impersonate party in future.

Arazi used DSA (Digital Signature Algorithm) [1] for providing authentication to the Diffie-Hellman key exchabge. Key independence is not provided by integrated key exchange scheme. Scheme of [1] hs modified by Harn *et al.*to provide key independence [5]. But the scheme in [5] does not provide *forward secrecy* [9]. Phan modified the scheme of [5] to provide forward secrecy[9]. A group key between only two entities is established in this scheme.

Review of DSA

The parameters of DSA are two primes p, q and an integer g,whereq is a divisorof p-1, and $g = h^{(p-1)/q} \bmod p > 1$. The private key of the user is arandom value x(0 < x < q). y is a corresponding public key, $y = g^x \bmod p$. H is a secure hash function on message m. {p, q, g, y} are public values and {xx} is a user's private key. kis a randomly chosen integer suchthat 0 < k < q. The signature of a message is the pair ofnumbers r and s computed as $r = ((g^k \bmod p) \bmod q)$ and $s = (k^{-1}(H(m) + xr)) \bmod q$. Here, $k^{-1}$is the multiplicativeinverse of (k mod q). i.e. $(k^{-1}k) \bmod q = 1$. On the receiverend, letm', r' and s'be the received versions of m, r, and s,respectively. To verify the signature, the verifier first checks tosee if 0 <$r' < q$ and 0 <$s' < q$; if either condition is violated,the signature is rejected. Otherwise, the verifier computes$a = (s')^{-1} \bmod q$, and$u_1 = (H(m')a) \bmod q, u_2 = (r'a) \bmod q$and $b = ((g^{u_1}y^{u_2} \bmod p) \bmod q$. If $b = r'$, the signature isverified.

Review of Raphael Phan's Key Exchange Scheme

Key independence[8]is not provided by the integrated key exchange scheme of [1]. For providing key independence,the scheme of [1] was modified by Harn et al [5].Modification of the scheme of [5] was done by Phan[9] for providing forward secrecy. Ephemer values of the session my be moe easily leaked than the secret keys of the public keys results in the origin of this security.

Insecurity of HMH [5] and P [9] Schemes

Three key exchange protocols are suggested by Harn *et al[5]*. Third protocol is referred as HMH. A modified version of HMH as P is suggested by Phan[9] as a key exchange protocol is depicted in Fig 3.1.

In the protocols the two session keys, $k_{AB}$and k_{BA}, are made in a session. k_{AB}may be used as a cryptographic key for a communication from user *A* to user *B*, and k_{BA}may be used as a cryptographic key for a communication from user *B* to user *A*.

If an adversary *A* gets the random numbers used by user *A* and user *B*, *A* can calculate the session keys, $k_{AB}$and k_{BA}. In P, $k_{AB}$and $k_{BA}$are calculated as $k_{AB} = g^{x_b vw}\ mod\ p$.and $k_{BA} = g^{x_a vw}\ mod\ p$. where v and w are random numbers selected by user *A* and *B*. If *A* gets v and w, *A* can easily calculate $k_{AB} = g^{x_b vw}\ mod\ p = {y_b}^{vw}\ mod\ p$and $k_{BA} = g^{x_a vw}\ mod\ p = {y_a}^{vw}\ mod\ p$. Thus, P is insecure against session state reveal attacks.

In HMH, $k_{AB}$and $k_{BA}$are calculated as $k_{AB} = g^{x_b v}\ mod\ p$and $k_{BA} = g^{x_a w}\ mod\ p$, where v and w are random numbers selected by user *A* and *B*. If *A* gets v and w, *A* can easily calculate $k_{AB} = {y_b}^{v}\ mod\ p$and $k_{BA} = {y_a}^{w}\ mod\ p$. Thus, HMH is insecure against session state reveal attacks.

Step	User *A*User *B*
1	Select random integer, v. $m_a = g^v\ mod\ p$. $n_a = {y_a}^v\ mod\ p$. m_a, n_a $\longrightarrow$
2	Select random integer, w. $k_{BA} = {n_a}^w\ mod\ p = g^{x_a vw}\ mod\ p$. $k_{AB} = {m_a}^{x_b w}\ mod\ p = g^{x_b vw}\ mod\ p$. $m_b = g^w\ mod\ p$. $n_b = {y_b}^w\ mod\ p$. $r_b = m_b\ mod\ q$. $s_b = ((w)^{-1}(H(m_b \|\| k_{BA}\|\|k_{AB}) + x_b r_b))\ mod\ q$ $\longleftarrow$ m_b, n_b, s_b
3	$k_{AB} = {n_b}^v\ mod\ p = g^{x_b vw}\ mod\ p$ $k_{BA} = {m_b}^{x_a v}\ mod\ p = g^{x_a vw}\ mod\ p$ $r_b = m_b\ mod\ q$ Verify DSA signature (r_b, s_b) of message“ m_b” $r_a = m_a\ mod\ q$ $s_a = ((v)^{-1}(H(m_a \|\|k_{AB}\|\| k_{BA}) + x_a r_a))\ mod\ q$ s_1 $\longrightarrow$
4	$r_a = m_a\ mod\ q$ Verify DSA signature (r_a, s_a) of message“ m_a"

Fig. 3.1. Phan’s Key Exchange Scheme

Our Contribution

This section is divided into two subsections. In section 1, we generaliseRaphael Phan’s Key Exchange Scheme. In section 4.2 we devisekey generation and communication protocol for Raphael Phan’s Key Exchange Scheme.

1.Generalized Key Exchange Schemes

We generalized Raphael Phan’s Key Exchange Schemeby generalizing diffie-hellman key exchange scheme.q is a prime number and **g** is a primitive root of q are common to all entities and known to every one. Each entity selectsa random number x_i<q; 1<= i <= n is the private key of entity i, stored in local non sharable memory of entity i and computes $y_i = (g)^{x_i}$; 1<= i<= n, is the public key of entity i. We described the group construction protocol by generalization of Raphael Phan’s Key Exchange Schemein section 2.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8170 - 8174
Received 16 February 2021; Accepted 08 March 2021.

pk	ps	ts

Figure 4.1. Partial signatures table

The group has a list of group members. Each member is associated with partial signature(ps). The structure of a partial signatures table of a group is given in Fig: 4.1. The partial signatures table are stored in central directory. The central directory is not trusted.

2. Generalization of Phan's Scheme

In this section we design group signature for a group of m entities by generalizing Phan's scheme. The protocol is specified Fig 4.2. We select m entities from n entities we need to communicate. Here n is the number of entities available in the world. The initiator of the groupselect m-1 members(m<n) from n members, then public keys of allm members (including himself) are stored in pk[i] = y_i.For 1<= i <= m. Assume member "1" is the initiator. ps[1] = g.

Step	Initiator(assume member"1" is the initiator)Remaining members 2<= i <= n
1	The initiator would select random number v_1 $m_1 = g^{v_1} \bmod p;\ n_1 = (y_1)^{v_1} \bmod p$;ps[1] = g; I = 2. broadcast the message $m_1$to all n members. m_1, n_1 $\longrightarrow$

2	while (i <= m) do the following operationsmember "i"
	Select random integer " v_i"
	$k_{u_i1} = (n_1)^{v_i} \, mod \, p = g^{x_1 v_1 v_i} \, mod \, p$
	$k_{1u_i} = (m_1)^{x_i v_i} \, mod \, p = g^{x_i v_1 v_i} \, mod \, p$
	$m_i = g^{v_i} \, mod \, p$
	$n_i = (y_i)^{v_i} \, mod \, p$
	$r_i = m_i \, mod \, q$
	$s_i = ((v_i)^{-1}(H(m_i \| k_{u_i1} \| k_{1u_i}) + x_i r_i)) \, mod \, q$
	$\longleftarrow$ m_i, n_i, s_i
	$k_{1u_i} = (n_i)^{v_1} \, mod \, p = g^{x_i v_1 v_i} \, mod \, p$
	$k_{u_i1} = (m_i)^{x_1 v} \, mod \, p = g^{x_1 v_1 v_i} \, mod \, p$
	$r_i = m_i \, mod \, q$
	Verify DSA signature (r_i, s_i) of message" m_i"
	If he is not a expected member
	Select next person
	Else
	$ps[i] = (ps[1]^{x_1} \, mod \, p$
	$r_1 = m_1 \, mod \, q$
	$s_1 = ((v_1)^{-1}(H(m_1 \| k_{1u_i} \| k_{u_i1}) + x_1 r_1)) \, mod \, q$
	s_1 $\longrightarrow$
	$r_1 = m_1 \, mod \, q$
	Verify DSA signature (r_1, s_1) of message" m_1"
	For k = 1 to i-1
	$ps[k] = (ps[k])^{x_i} \, mod \, p$
	I++

Fig. 4.2. Generalized Lein Harn, Phan's key exchange scheme

3) Key Generation andCommunication Protocol for the Phan'sSchemes

Public keys and partial signatures are available in public directory. The group member who needs to transfer the message to the remaining members, generate key by using his partial key, decript the message by using the generated key. The cipher text can be transferred to all entities in the communication but, only group members can encrypt the original message. The protocol is shown in Fig 4.3.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8170 - 8174
Received 16 February 2021; Accepted 08 March 2021.

Step	Initiator(assume member"1" is the sender)Remaining members 2<= i <= m
1	Select message "m" $k = (ps[1])^{x_1} \bmod p$ $c = E_k(m)$ $\longrightarrow c$
2	$k = (ps[i])^{x_i} \bmod p$ $m = D_k(c)$

Fig. 4.3. Key generation and communication protocol for the Harn-Mehta's and Phan's schemes

Security Analysis

Session state reveal attacks: When an opponent is capable of obtaining random numbers used to make the session keys, the key exchange scheme providing security against session state reveal attacks must maintain the secret of session keys. The main advantage of our scheme is that the opponent A can not calculate $g^{x_1 x_2 \dots x_m}$ even if he knows $v_1, v_{2,}, \dots, v_{m-1}$ *and* v_m. Which means that a can not calculate session key K even if he gets $v_1, v_{2,}, \dots, v_{m-1}, v_m$. Hence security against session state reveal attack is provided in our scheme.

Forward secrecy: The key exchange scheme providing forward secrecy must maintain the secrecy of session keys even when *A* is able to obtain long-term secret keys of principals who have generated session keys. In our scheme, even if *A* knows $x_1, x_2, \dots, x_{m-1}$ *and* x_m, *A* cannot calculate $g^{v_1 v_2 \dots v_m}$. Therefore, the proposed scheme provides forward secrecy.

Key independence: Provision of key independence by key exchange scheme means that session keys are computationally independent from each other to protect "Denning-Sacco" attacks [4]. For providing key freshness each session makes use of new ephemeral random numbers in this scheme. An opponent can not known. There fore, key independence is provided in the proposed scheme.

Conclusion

Our session key generation scheme is useful for the application which provides security on resource sharing, cloud computing applications and internet banking for joint accounts.

References

[1] Arazi, B. (1993). Integrating a key distribution procedure into the digital signature standard. *Electronics Letters*, *29*(11), 966-967.

[2] Canetti, R., & Krawczyk, H. (2001). Analysis of key-exchange protocols and their use for building secure channels. *In International conference on the theory and applications of cryptographic techniques*, *Springer*, *Berlin*, *Heidelberg*, 453-474.

[3] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), 644-654.

[4] Denning, D.E., & Sacco, G.M. (1981). Timestamps in key distribution protocols. *Communications of the ACM*, *24*(8), 533-536.

[5] Harn, L., Mehta, M., & Hsin, W.J. (2004). Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA). *IEEE communications letters*, *8*(3), 198-200.

[6] Krawczyk, H. (2005). HMQV: A high-performance secure Diffie-Hellman protocol. In *Annual International Cryptology Conference*, Springer, Berlin, Heidelberg, 546-566.

[7] National Institute of Standards and Technology, Digital Signature Standard (DSS), *Federal information Processing Standards Publication*, FIPS PUB 186-2, Reaffirmed, 2000.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8170 - 8174
Received 16 February 2021; Accepted 08 March 2021.

[8] Nyberg, K., & Rueppel, R.A. (1994). Weaknesses in some recent key agreement protocols. *Electronics Letters*, *30*(1), 26-27.

[9] Phan, R.W. (2005). Fixing the integrated Diffie-Hellman-DSA key exchange protocol. *IEEE communications letters*, *9*(6), 570-572.

[10] Jeong, I.R., Kwon, J.O., & Lee, D.H. (2007). Strong diffie-hellman-DSA key exchange. *IEEE communications letters*, *11*(5), 432-433.

[11] Yoon, E.J., & Yoo, K.Y. (2009). An Efficient Diffie-Hellman-MAC Key Exchange Scheme. *Fourth International Conference on Innovative Computing, Information and Control (ICICIC)*, 398-400.

[12] Federal Information Processing Standards Publication, National Institute of Standards and Technology. http://www.itl.nist.gov/fipspubs/

[13] Kaliski Jr, B.S. (2001). An unknown key-share attack on the MQV key agreement protocol. *ACM Transactions on Information and System Security (TISSEC)*, *4*(3), 275-288.

[14] Menezes, A.J., Van Oorschot, P.C., & Vanstone, S.A. (1997). *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press.

[15] Hwang, M.S., Lin, I.C., & Li, L.H. (2001). A simple micro-payment scheme. *Journal of Systems and Software*, *55*(3), 221-229.