A Better Improvement on the Integrated Diffie-Hellman-DSA Key Agreement Protocol

Jie Liu and Jianhua Li
(Corresponding author: Jie Liu)
Department of Electronic Engineering, Shanghai Jiao Tong University
no. 1954, Hua Shan Road, Xu Hui District, Shanghai, 200030, China
(Email: ljiesh@gmail.com)
(Received Dec. 20, 2006; revised and accepted June 13, 2007)

Abstract

Harn et al. proposed a series of Diffie-Hellman key exchange protocols which are integrated into Digital Signature Algorithm in 2004. Recently, Phan pointed out that Harn et al.'s protocols cannot provide forward secrecy and key freshness, which are two standard security attributes that key exchange protocols should have. Phan also gave his improvement. In this paper we present a better improvement, which is more secure than Phan's scheme.

Keywords: Diffie-Hellman, digital signature algorithm (DSA), key exchange protocols, network security

1 Introduction

In 1993, Arazi integrated the Diffie-Hellman key exchange protocol with the digital signature algorithm (DSA) to achieve mutual authentication of the established keys [1]. In 1994, Nyberg and Rueppel showed that Arazi's scheme did not provide known-key security [2]. In 2004, Harn et al. improved Arazi's concept and proposed three similar key exchange protocols, which can prevent known key attack, key relay attack and unknown-key attack [3]. Recently, Phan showed that Harn et al.'s protocols failed to provide another two security attributes, forward secrecy and key freshness, that key exchange protocols should have [4]. Phan also gave a fixing on these protocols such that they provide those security attributes.

In this paper, we will give a further cryptanalysis on Phan's improvement and present a little modification on it. Our improvement is more secure than Phan's scheme while preserving all advantages of Phan's protocol.

2 Harn et al.'s Key Exchange Protocols

Harn et al. proposed three protocols that integrated Diffie-Hellman key exchange into DSA for authenticated key distribution. Since the third is the most advanced version, we only review and analyze the third protocol here. We omit the description of Digital Signature Algorithm (DSA) for the sake of simplicity.

The third protocol of Harn et al's key exchange is illustrated in Figure 1. K_{AB} and K_{BA} are the two session keys negotiated by user A and B. Phan pointed out that Harn et al.'s protocols can not provide forward secrecy and key freshness in [4].

1) No Forward Secrecy
The session key for direction from A to B is computed by A as:

$$K_{AB} = (y_B)^v \bmod p, \tag{1}$$

while it is computed by B as:

$$K_{AB} = (m_A)^{x_B} \bmod p. \tag{2}$$

Therefore, when the long-term private key x_B of B is leaked, an attacker can easily compute any previously established session key, K_{AB} by Equation (2). The same thing will happen to K_{BA} when x_A is compromised.

2) No Key Freshness
Key freshness means that neither party can predetermine the shared secret key being established.

In Harn et al.'s protocols, A computes K_{AB} via Equation (1), which depends on B's public key y_B, known by A all the time, and a random secret value v chosen by A. Therefore, A could decide that K_{AB} must be equal to a predetermined value. B also could do the similar thing to K_{BA} as A.

3 Phan's Fixing

Phan gave a fixing on Harn et al.'s protocol such that they can provide forward secrecy and key freshness. Figure 2 shows Phan's fixing [4].

Step	User A	User B
1	Select random integer v $m_A = g^v \bmod p$ $\xrightarrow{m_A}$	
2		Select random integer w $K_{BA} = (y_A)^w \bmod p$ $K_{AB} = (m_A)^{x_B} \bmod p$ $m_B = g^w \bmod q$ $r_B = m_B \bmod q$ $s_B = ((w)^{-1}(H(m_B \| K_{BA} \| K_{AB}) + x_B r_B)) \bmod q$ $\xleftarrow{(m_B, s_B)}$
3	$K_{AB} = (y_B)^v \bmod p$ $K_{BA} = (m_B)^{x_A} \bmod p$ $r_B = m_B \bmod q$ Verify DSA signature (r_B, s_B) $r_A = m_A \bmod q$ $s_A = ((v)^{-1}(H(m_A \| K_{AB} \| K_{BA}) + x_A r_A)) \bmod q$ $\xrightarrow{S_A}$	
4		$r_A = m_A \bmod q$ Verify DSA signature (r_A, s_A)

Figure 1: Harn et al.'s three-round key exchange protocol

Step	User A	User B
1	Select random integer v $m_A = g^v \bmod p$ $n_A = (y_A)^v \bmod p$ $\xrightarrow{m_A, n_A}$	
2		Select random integer w $K_{AB} = (m_A)^{x_B w} \bmod p = g^{x_B vw} \bmod p$ $K_{BA} = (n_A)^w \bmod p = g^{x_A vw} \bmod p$ $m_B = g^w \bmod p$ $n_B = (y_B)^w \bmod p$ $r_B = m_B \bmod q$ $s_B = ((w)^{-1}(H(m_B \| K_{BA} \| K_{AB}) + x_B r_B)) \bmod q$ $\xleftarrow{(m_B, n_B, s_B)}$
3	$K_{AB} = (n_B)^v \bmod p = g^{x_B vw} \bmod p$ $K_{BA} = (m_B)^{x_A v} \bmod p = g^{x_A vw} \bmod p$ $r_B = m_B \bmod q$ Verify DSA signature (r_B, s_B) $r_A = m_A \bmod q$ $s_A = ((v)^{-1}(H(m_A \| K_{AB} \| K_{BA}) + x_A r_A)) \bmod q$ $\xrightarrow{S_A}$	
4		$r_A = m_A \bmod q$ Verify DSA signature (r_A, s_A)

Figure 2: Phan's fixing

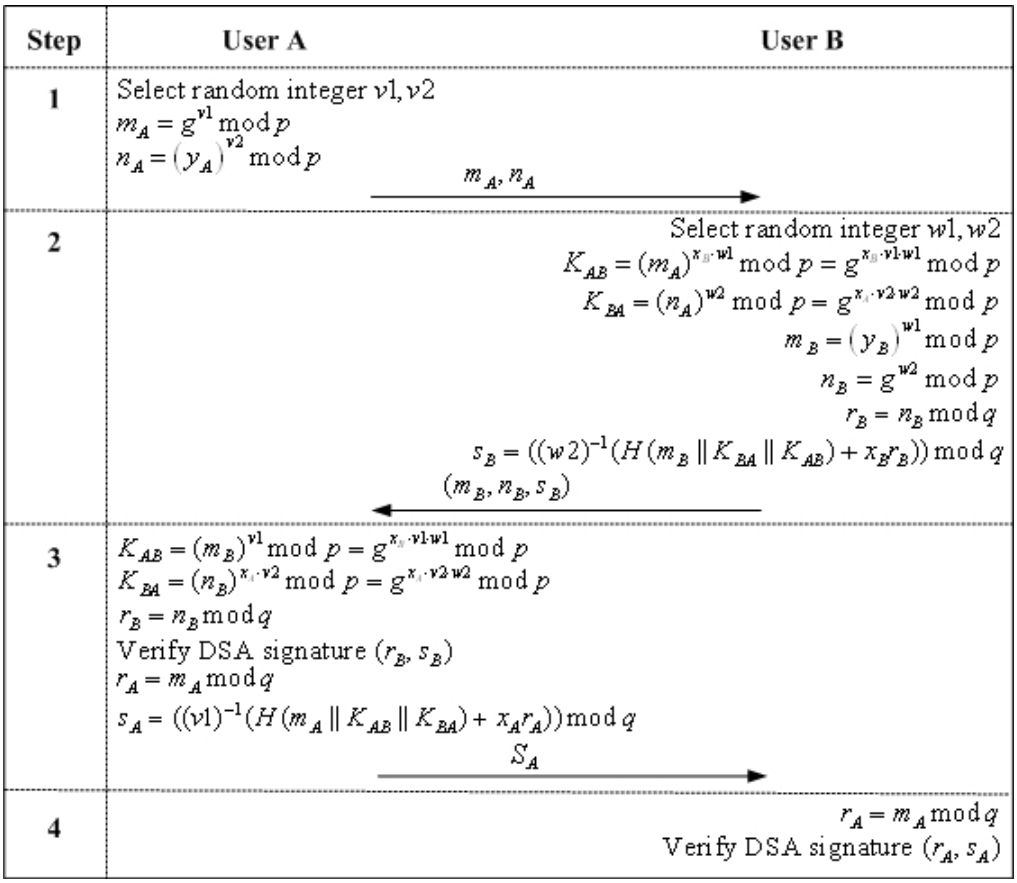

Figure 3: Our protocol

Phan's fixing does provide both forward secrecy and key freshness, while keeping the advantages of the original protocols. However, we think that there is still a flaw in it.

In Phan's protocol:

$$K_{AB} = g^{x_B \cdot v \cdot w} \bmod p.$$
$$K_{BA} = g^{x_A \cdot v \cdot w} \bmod p.$$

So we have:

$$K_{AB}^{x_B} = K_{BA}^{x_A} \bmod p.$$

Obviously there is an explicit relation between the two negotiated session keys, K_{AB} and K_{BA}. This relation maybe cause some vulnerability in future. For example, when the long-term private keys x_A and x_B are compromised simultaneously, one can compute K_{AB} from K_{BA} and vice versa. Although there are no existing attacks on it right now, we do believe that the protocol would be more secure if there is no explicit relation between the two negotiated session keys.

4 Our Improvement

We change Phan's protocol a little and present our improvement in Figure 3. Our improvement is the same as Phan's protocol except that there are two extra temporary random integers. Our protocol preserves the basic essence of Phan's protocol. Namely, it can provide both forward secrecy and key freshness too.

Moreover, the session keys in our improvement are combined by different random integers, as Equations (3) and (4) show. There is not any relation between K_{AB} and K_{BA}. Thus, our improvement must be more secure than Phan's protocol.

$$K_{AB} = g^{x_B \cdot v1 \cdot w1} \bmod p. \quad (3)$$

$$K_{BA} = g^{x_A \cdot v2 \cdot w2} \bmod p. \quad (4)$$

Also, our protocol has the identical computing complexity as Phan's protocol. Although the two extra temporary random integers make our improvement loss a tiny little space complexity, they do make the protocol more secure.

5 Conclusions

In this paper, we give a further cryptanalysis on Harn et al.'s key exchange protocols and Phan's fixing. We present a better improvement on Phan's protocol. Our improvement keeps the advantages of Phan's protocol and

has the same computing complexity as it. Two extra temporary random integers increase a tiny little space complexity but make the protocol more secure.

References

[1] A. Arazi, "Integrating a key cryptosystem into the digital signature standard," *Electronic Letters*, vol. 29, pp. 966-967, Nov. 1993.

[2] K. Nyberg, and R. A. Rueppel, "Weaknesses in some recent key agreement protocols," *Electronic Letters*, vol. 30, pp. 26-27, Jan. 1994.

[3] L. Harn, Ma. Mehta, and W. J. Hsin, "Integrating diffie-hellman key exchange into the digital signature algorithm (DSA)," *IEEE Communication Letters*, vol. 8, no. 3, Mar. 2004.

[4] R. C. W. Phan, "Fixing the integrated diffie-hellman-DSA key exchange protocol," *IEEE Communication Letters*, vol. 9, no. 6, Jun. 2005.

Jie Liu is now a Ph. D. candidate in the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China. His current research interests include information security, network security and public key cryptography.

Jianhua Li received his M. S. and Ph. D. in Communication and Information System from Shanghai Jiao Tong University. He is now a professor in the Department of Electronic Engineering, Shanghai Jiao Tong University. His research interests include mobile communications, network management and information security.