ISSN No. 0976-5697

Volume 3, No. 5, Sept-Oct 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Efficient Password-based Authenticated Key Exchange Protocol

Sharad Kumar Verma*
Research Scholar, Department of CSE
Mewar University, Chittorgarh, Rajasthan, India
sharadverm@gmail.com

Dr. D.B. Ojha
Professor, Department of Mathematics
Mewar University, Chittorgarh, Rajasthan, India
ojhabrat@gmail.com

Abstract: Password-based encrypted key exchange are protocols that are designed to provide pair of users communicating over an unreliable channel with a secure session key even when the secret key or password shared between two users is drawn from a small set of values. The proposed key exchange protocol provides implicit key authentication as well as the desired security attributes of an authenticated key exchange protocol. In this paper, we also conduct a detailed analysis on the flaws and also propose a verifier-based password-authenticated key exchange protocol via elliptic curves which is secure against various known attacks.

Keywords: Encryption, secret key, key exchange protocol, authentication, password-based authentication, elliptic curves.

I. INTRODUCTION

Keys exchange protocols are cryptographic primitives used to provide a pair of users communicating over a public unreliable channel with a secure session key. In practice, one can find several flavors of key exchange protocols, each with its own benefits and drawbacks. An example of a popular one is the SIGMA protocol [1] used as the basis for the signature-based modes of the Internet Key Exchange (IKE) protocol.

Two of the most important services offered by cryptography are those of providing private and authenticated communications. Much research has been done into creating encryption schemes to meet highly developed notions of privacy.

In 1997 Zheng proposed a primitive that he called Signcryption[5]. The idea of a Signcryption schemes is to combine the functionality of an encryption scheme with that of a signature scheme. It must provide privacy; Signcryption must be unforgeable; and there must be a method to settle repudiation disputes.

In [6], Zheng proposed two key exchange protocol using Signcryption scheme that he called DKEUN (Direct Key Exchange Using a Nonce) and DKEUTS(Direct Key Exchange Using Time-stamp).

PAK protocol used to establish a short-term session key between a client and a server is known as a key agreement protocol. The protocol refers to be authenticated if one party is authenticated to the other during the authentication protocol run. The authenticated key exchange protocol is to be authenticated, if simple password is used to authenticate each other [4].

We describe working environments for PAK protocol. Two entities, who only share the secret information, and who are communicating over an insecure network, want to authenticate each other and agree on a large session key to be used for protecting their subsequent communication. In this case, password is shared among the servers and a client can be authenticated by a group of servers using the shared secret password.

II. PASSWORD-BASED AUTHENTICATED KEY EXCHANGE SCHEME

Password-Authenticated Key Exchange (PAK) enables two communication entities to authenticate each other and establish a session key via easily memorable passwords. Right now PAK is widely used because of the advantages of simplicity, convenience, adaptability, mobility, and less hardware requirement. [2]

A high-level description of the protocol is given below. Our protocol is in a finite cyclic group G = (g) with a k-bit prime order q, where G is chosen by client C. Ƒ$_H$ is denoted as the family of universal one-way hash function: $\{0, 1\}^* \to \{0, 1\}^{k'}$. k and k' are security parameters.[3]

As given below, the protocol runs between a client C and a server S, who initially share a low-entropy secret string pwd, the password, uniformly drawn from the dictionary P, without knowing other public parameters, such as the generator g of the underlying finite cyclic group G, where k and k' are security parameters. Note that all computations are in G.

The protocol consists of the following four flows.[3]

a. The client first chooses a random finite cyclic group G = (g) of order a k-bit prime number q, and selects a random number rC ∈ Z_q^* , and computes the value Rc ← g^{rC} , then it sends (G, q, g, Rc, client) to the server as Flow$_1$.

b. After receiving Flow$_1$, the server first checks whether q is k-bit prime, g and R_C are two members of G with order q ($g^q \overset{?}{=} 1$ and $R_C^q \overset{?}{=} 1$). If not, reject Flow$_1$ and abort; otherwise, choose a random number $r_S \in Z_Q^*$, and compute $R_S \leftarrow g^{rs}$, $R_S^* \leftarrow (R_C)^{pwd} R_S$, and $R' \leftarrow (R_C)^{rS}$, then it sends (R_S^* ,server) to the client as Flow$_2$.

c. Upon receiving Flow$_2$, the client first checks whether R_S^* is a member of G with order q ($(R_S^*)^q \overset{?}{=} 1$), if not, reject Flow$_2$ and abort; otherwise, choose randomly three hash functions H_0, H_1, H_2 from Ƒ$_H$, and compute $R'S \leftarrow R_S^* (R_C)^{-pwd}$, $R \leftarrow (R'S)^{rC}$, and $\alpha \leftarrow \overset{?}{=}$ H1(client||server||R_C||R_S ||R') and send (H_0, H_1, H_2, α) to the client as Flow$_3$.

d. On receiving Flow_3, the server first checks whether $H_{0,}H_1,H_2$ are chosen from $Ƒ_H$, and $\alpha \overset{?}{=} H_1(\text{client}||\text{server}||R_C||R_S||R')$. If not, reject Flow_3 and abort; otherwise, compute
$sk_S \leftarrow H_0(\text{client}||\text{server}||R_C||R_S||R')$, $\beta \leftarrow H_3(\text{client}||\text{server}||R_C||R_S||R')$
which the server sends to the client as Flow_4.

e. If $\beta \overset{?}{=} H_3(\text{client}||\text{server}||R_C||R_S||R')$ holds on the client side, the client computes $sk_S \leftarrow H_0 (\text{client}||\text{server}||R_C||R_S||R')$, which means that they have successfully exchanged the session key.

PAK Protocol allows two parties to authenticate each other, while maintaining a perfect forward secrecy by performing the Diffie-Hellman key exchange procedure. The authentication relies on a preshared secret, which is concealed (i.e., remains unrevealed) from an eavesdropper preventing an offline dictionary attack.

III. VERIFIER-BASED PASSWORD-AUTHENTICATION KEY EXCHANGE PROTOCOL

Let G be a point on the elliptic curve, $H(\cdot)$ is a function which makes a point map to another point on elliptic curve. H_0, H_1 are strong one-way hash function. The server only stores the verifier: $V = vG$ for each client in the database, $v = H_0(A, S, pw)$, pw is the client's password. The protocol can be described as follows. [2]

Step A1. $A \rightarrow S$: $A \,||\, X_A$

The client chooses a random number $a \in Z_q^*$, computes $X_A = a\,G + H(V)$. Next, the client sends $A \,||X_A$ to the server.

Step A2. $S \rightarrow A$: $\mu \,||d\, ||k$

Upon receiving $A \,||\, X_A$, the server takes out the client's verifier V, and then chooses a random number $b \in Z_q^*$ to compute $\mu = b\,G$, $\sigma = b\,(X_A - H(V))$, $d = H_0(A, S, \mu, \sigma)\,G$, $e{=}H_0(A, S, \mu, \sigma)\,V$ and $k = H_1(A, S, X_A, \mu, \sigma, d, e)$. Next, the server sends $\mu \,||\, d \,||\, k$ to the client.

Step A3. $A \rightarrow S$: k'

Upon receiving $\mu \,||\, d \,||\, k$, the client computes $\sigma = a\,\mu$, $e = v\,d$ and checks whether k is equal to $H_1(A, S, X_A, \mu, \sigma, d, e)$. If $k = H_1(A, S, X_A, \mu, \sigma, d, e)$, the client continues to compute $k' = H_1(A, S, X_A, \mu, \sigma, d, k)$ and sends k' to the server. Next, the client computes the shared session key $K_A = H_1(A, S, X_A, \mu, \sigma, V)$.

Step A4.

Upon receiving k', the server checks whether k' is equal to $H_1(A, S, X_A, \mu, \sigma, d, k)$. If $k' = H_1(A, S, X_A, \mu, \sigma, d, k)$, the server computes the shared session key $K_S = H_1(A, S, X_A, \mu, \sigma, V)$. Our protocol also contains a password change mechanism as in the following. Assume that the client requests to change his old password pw to a new password pw_{new}.

Step B1.

The client executes Steps A1–A4 to establish a shared session key $K_A = K_S$ with the server.

Step B2. $A \rightarrow S$: $H_0(K_A, \mu) \oplus pw_{new} \,||H_0(K_A \,||\, pw_{new})$

The client enters his new password pw_{new}, and then computes $H_0(K_A, \mu) \oplus pw_{new}$ and $H_0(K_A \,||\, pw_{new})$. Next, the client sends $H_0(K_A, \mu) \oplus pw_{new} \,||\, H_0(K_A \,||\, pw_{new})$ to the server.

Step B3. $S \rightarrow A$: *Accepted/Denied*

The server uses K_S, which equals K_A, to compute $H_0(K_A, \mu)$ and extract pw_{new} from the received $H_0(K_A, \mu) \oplus pw_{new}$. Then the server uses K_S and the extracted pw_{new} to compute $H_0(K_S \,||\, pw_{new})$. If the computed $H_0(K_S \,||\, pw_{new})$ equals the received $H_0(K_A \,||\, pw_{new})$, the server changes his old password pw to the new password pw_{new} and sends "Accepted" to the client. Otherwise, the server rejects the client's password change request and sends "Denied" to the client.

IV. CONCLUSION

In this paper, to remove the disadvantages raised by getting valid public information, we have explored an efficient password-based authenticated exchange protocol. We have also defined a verifier-based password-authenticated key exchange protocol via elliptic curves, which is secure against the off-line dictionary attack and the server compromise attack. Moreover, the proposed protocol can also provide mutual authentication, the forward secrecy and the backward secrecy.

V. REFERENCES

[1]. Hugo Krawczyk. SIGMA: The SIGn-and-MAc" approach to authenticated Diffie-Hellman and its use in the IKE protocols. In Dan Boneh, editor, Advances in Cryptology - CRYPTO 2003, volume 2729 of Lecture Notes in Computer Science, pages 400-425, Santa Barbara, CA, USA, August 17-21, 2003. Springer-Verlag, Berlin, Germany.

[2]. Junhan YANG, Tianjie CAO "A Verifier-based Password-Authenticated Key Exchange Protocol via Elliptic Curves", Journal of Computational Information Systems 7:2 (2011) 548-553.

[3]. Jun Shao Zhenfu Cao , Licheng Wang, Rongxing Lu, "Efficient Password-based Authenticated Key Exchange without Public Information", volume 4734 of LNCS, pp. 299-310, Sringer-Verlag, 2007.

[4]. Rack-Hyun Kim, Heung-Youl Youm, "Secure Authenticated Key Exchange protocol based on EC using Signcryption Scheme", 2006 International Conference on Hybrid Information Technology (ICHIT'06) 0-7695-2674-8/06 © 2006 IEEE.

[5]. Y. Zhen g , "Digital signcryption or how to achieve cost (signature and encryption) cost (signature) + cost (encryption)", Advances in Cryptology , Proceeding s of CRYPTO'97, LNCS Vol. 1294, Springer - Verlag , pp . 165- 179, 1997.

[6]. Y. Zheng, "Shortened Digital Signature, Signcryption and Compact and Unforgeable Key Agreement Schemes" IEEE P1363a: Standard Specifications for Public-key Cryptography : Additional Techiques, 1998.