ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

ID-Based Multi-Server Password-Authenticated Key Exchange

Sayli Kokate[1], Prof. Prashant Jawalkar [2]

M.E Student, Dept. of Computer, JSPM's BSIOTR Wagholi, Pune, India[1]

Asst. Professor, Dept. of Computer, JSPM's BSIOTR Wagholi, Pune, India[2]

ABSTRACT: Password Authenticated Key Exchange (PAKE) protocols enable two entities to agree on a common session key based on a pre-shared human memorable password. The main security goal of these protocols is providing security against password guessing attacks. In this setting, all the passwords necessary to authenticate clients are stored in a single server. If the server is compromised, due to, for example, hacking or even insider attacks, passwords stored in the server are all disclosed. In Existing the researchers consider a two-server password-authenticated key exchange (PAKE) protocol. In two-server PAKE protocol, a client splits its password and stores two shares of its password in the two servers, respectively, and the two servers then cooperate to authenticate the client without knowing the password of the client. In case one server is compromised by an adversary, the password of the client is required to remain secure. But both two servers are compromised by an adversary, the password is not secure. To tackle this problem, we proposed ID-Based Multi-Server Password-Authenticated Key Exchange Protocol. In this thesis, we present two compilers that transform any two-party PAKE protocol to a multi-server PAKE protocol on the basis of the identity-based cryptography, called ID Based Multi-server PAKE protocol. By the compilers, we can construct ID Based Multi-server PAKE protocols which achieve implicit authentication. As long as the underlying two-party PAKE protocol and identity-based encryption or signature scheme have provable security without random oracles, the ID Based Multi-server PAKE protocols constructed by the compilers can be proven to be secure without random oracles.

KEYWORDS: Password-authenticated key exchange, identity-based encryption and signature, Diffie-Hellman key exchange, decisional Diffie-Hellman problem.

I. INTRODUCTION

Nowadays, passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines and so on[5]. A computer user may require passwords for many purposes: logging in to computer accounts, retrieving e-mail from servers, accessing programs, databases, networks, web sites, and even reading the morning newspaper online[8].
Earlier password-based authentication systems transmitted a cryptographic hash of the password over a public channel which makes the hash value accessible to an attacker. When this is done, and it is very common, the attacker can work offline, rapidly testing possible passwords against the true password's hash value. Studies have consistently shown that a large fraction of user-chosen passwords are readily guessed automatically. For example, according to Bruce Schneier, examining data from a 2006 phishing attack, 55 percent of MySpace passwords would be crackable in 8 hours using a commercially available Password Recovery Toolkit capable of testing 200,000 passwords per second in 2006[4].

Recent research advances in password-based authentication have allowed a client and a server mutually to authenticate with a password and meanwhile to establish a cryptographic key for secure communications after authentication [2]. In general, current solutions for password based authentication follow two models [6]. The first model, called PKI-based model, assumes that the client keeps the server's public key in addition to share a password with the server. In this setting, the client can send the password to the server by public key encryption [7].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

II. RELATED WORK

Propose a new compiler for ID2S PAKE protocol based on any identity-based signature scheme (IBS), such as the Paterson et al.'s scheme[8]. The basic idea is: The client splits its password into two shares and each server keeps one share of the password in addition to a private key related to its identity for signing. In key exchange, each server sends the client its public key for encryption with its identity-based signature on it. The signature can be verified by the client on the basis of the identity of the server [5].

If the signature is genuine, the client submits to the server one share of the password encrypted with the public key of the server [1]. With the decryption keys, both servers can derive the same one-time password, by which the two servers can run a two-party PAKE protocol to authenticate the client. In addition, we generalize the compiler based on IBE by replacing the Cramer-Shoup public key encryption scheme with any public key encryption scheme [4]. Unlike the compiler based on IBS, the compiler based on IBE assumes that each server has a private key related to its identity for decryption. In key exchange, the client sends to each server one share of the password encrypted according to the identity of the server [7].

In addition, a one-time public key encryption scheme is used to protect the messages (containing the password information) from the servers to the client [1]. The one-time public key is generated by the client and sent to the servers along with the password information in the first phase. In the identity-based cryptography, the decryption key or the signing key of a server is usually generated by a Private Key Generator (PKG). Therefore the PKG can decrypt any messages encrypted with the identity of the server or sign any document on behalf of the server.

Using standard techniques from threshold cryptography, the PKG can be distributed so that the master-key is never available in a single location [4]. Our strategy is to employ multiple PKGs which cooperate to generate the decryption key or the signing key for the server. As long as one of the PKGs is honest to follow the protocol, the decryption key or the signing key for the server is known only to the server.

Since assume that the two servers in two-server PAKE never collude, we can also assume that at least one of the PKGs do not collude with other PKGs. Based on this assumption, we provide a rigorous proof of security for our compilers[4]. The two compilers do not rely on the random oracle model as long as the underlying primitives themselves do not rely on it. For example, by using the KOY protocol and the Paterson et al.'s IBS scheme and the Cramer-Shoup public key encryption scheme, the compiler based on IBS can construct an ID2S PAKE protocol with provable security in the standard model [5].

By using the KOY protocol and the Waters IBE scheme and the Cramer-Shoup public key encryption scheme, the compiler based on IBE can construct an ID2S PAKE protocol with provable security in the standard model[10]. We also compare our ID2S PAKE protocols with the Katz et al.'s two-server PAKE protocol with provable security in the standard model. The Katz et al.'s protocol is password-only, where the client needs to remember the password only and refer to common public parameters, and each server, having a public and private key pair, and keeps a share of the password. Our protocols are identitybased, where the client needs to remember the password in addition to the meaningful identities of the two servers, and refer to common public parameters, including the master public key, and each server, having a private key related to his identity, keeps a share of the password. In terms of the setting and the client performance, the Katz et al.'s protocol is superior to our protocols [4]. However, in the Katz et al.'s protocol, each server performs approximately six times the amount of the work as the KOY protocol, whereas in our protocols, each server performs the same amount of work as the KOY protocol in addition to one identity-based decryption (or signature) and one public key encryption (or decryption).

III. PROPOSED ALGORITHAM

A. ALGORITHM :

1. Client Register and Login
2. Generate Password & Split into Multiple Parts
3. Share Splitted Passwords to Each Server
4. Access Password From Servers

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

B. CLIENT REGISTER & LOGIN:

In this module client register with server using client id, name, password, address and so on.
If he want to share his password to another client, first he login his form.
After the login he generates the passwords.

C. GENERATE PASSWORDS AND SPLIT IT INTO MULTIPLE PARTS:

In this module, he generates a password.
Then he split a password into multiple parts.
Followed by, he shares the splitted passwords to each server.

D. SHARE SPLITTED PASSWORDS TO EACH SERVER:

In this module he shares each password blocks to each server.
A client splits its password and stores multiple shares of its password in the two servers, respectively, and the two servers then cooperate to authenticate the client without knowing the password of the client.
In case one server is compromised by an adversary, the password of the client is required to remain secure.

E. ACCESS PASSWORDS FROM SERVERS:

In this module, the destination client wants to get the source password from server.
So he collects the each password parts and merge all.
Finally he access the whole password.

IV. PSEUDO CODE

Step 1: Client C
Step 2: public key encryption scheme E
Step 3: identity-based signature IBS
Step 4: identity-based encryption IBE
Step 5: Server S

V. SERVEY ON

1. Password-Based Authenticated Key Exchange in the Three-Party Setting [1]

Password-based authenticated key exchange (PAKE) consists of protocols which are designed to be secure even when the secret key used for authentication is a human-memorable password. In the article, the authors consider PAKE protocols in the 3-party scenario, in which the users trying to establish a common secret do not share a password between themselves but only with a trusted server. Towards their goal, the authors recall some of the existing security notions for PAKE protocols and introduce new ones that are more suitable to the case of generic constructions of 3-party protocols. The authors then present a natural generic construction of a 3-party PAKE protocol from any 2-party PAKE protocol and prove its security.

2. Simple Password-Based Encrypted Key Exchange Protocols [2]

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. In this paper, we present two simple password-based encrypted key exchange protocols based on that of Bellovin and Merritt. While one protocol is more suitable to scenarios in which the password is shared across several servers, the other enjoys better security properties. Both protocols are as efficient, if not better, as any of the existing encrypted key exchange protocols in the literature, and yet they only require a single random oracle instance. The proof of security for both protocols is in the random oracle model and based on hardness of the computational Diffie-Hellman problem. However, some of the techniques that we use are

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

quite different from the usual ones and make use of new variants of the Diffie-Hellman problem, which are of independent interest.

3. **Authenticated Key Exchange Protocol Secure against Offline Dictionary Attack and Server Compromise [3]**

This paper introduces a new scheme, called Augmented Password AKE (APAKE), for authenticated key exchange protocols. In APAKE, a password is represented by a pair of values that is randomly selected in a huge space. We present an APAKE protocol. The protocol is secure against the attacks including offline dictionary attack and server compromise allowing for subsequent off-line dictionary attack. The protocol has a pass number of two, and it requires minor computational amounts. We also present a EKE protocol de-signed by simple modification of the APAKE protocol while preserving the security of the APAKE protocol.

VI. CONCLUSION AND FUTURE WORK

present two efficient compilers to transform any two-party PAKE protocol to an ID based Multi Server PAKE protocol with identity-based cryptography. In addition, we have provided a rigorous proof of security for our compilers without random oracle. Our compilers are in particular suitable for the applications of password-based authentication where an identity-based system has already established. proposed work has multiple servers. So Storage Space is high. To tackle this problem, need a novel PAKE protocol for reduce storage size.

REFERENCES

1. M. Abdalla, P. A. Fouque, and D. Pointcheval ,'Password-based authenticated key exchange in the three-party setting'. In Proc. PKC'05, pages 65-84, 2005.
2. M. Abdalla and D. Pointcheval., 'Simple password-based encrypted key exchange protocols'. In Proc. CT-RSA 2005, pages 191-208, 2005.
3. M. Bellare, D. Pointcheval, and P. Rogaway, 'Authenticated key exchange secure against dictionary attacks'. In Proc. Eurocrypt'00, pages 139-155, 2000.
4. S. M. Bellovin and M. Merritt, 'Encrypted key exchange: Passwordbased protocol secure against dictionary attack'. In Proc. 1992 IEEE Symposium on Research in Security and Privacy, pages 72-84, 1992.
5. J. Bender, M. Fischlin, and D. Kugler, 'Security analysis of the PACE key-agreement protocol', In Proc. ISC'09, pages 33-48, 2009.
6. D. Boneh and M. Franklin, 'Identity based encryption from the Weil pairing'. In Proc. Crypto'01, pages 213-229, 2001.
7. V. Boyko, P. Mackenzie, and S. Patel, 'Provably secure passwordauthenticated key exchange using Diffie-Hellman' In Proc. Eurocrypt'00, pages 156-171, 2000.
8. J. Brainard, A. Juels, B. Kaliski, and M. Szydlo, 'Nightingale: A new two-server approach for authentication with short secrets' InProc. 12th USENIX Security Symp., pages 201-213, 2003.
9. E. Bresson, O. Chevassut, and D. Pointcheval, 'Security proofs for an efficient password-based key exchange' In Proc. CCS'03, pages 241-250, 2003.
10. E. Bresson, O. Chevassut, and D. Pointcheval ,' New security results on encrypted key exchange', In Proc. PKC'04, pages 145-158, 2004.
11. X. Yi, S. Ling, and H. Wang, 'Efficient two-server password-only authenticated key exchange',IEEE Trans. Parallel Distrib. Syst.24(9): 1773- 1782, 2013.
12. X. Yi, F. Hao and E. Bertino,' ID-based two-server password authenticated key exchange', In ESORICS'14, pages 257-276, 2014.

BIOGRAPHY

Sayli Kokate is a M.E Student in the Computer Engineering Department, JSPM's BSIOTR wagholi College, Savitribai Phule Pune University. She received Bachelor of Engineering degree in 2015 from SPPU, Pune, MS, India. Her research interests are Network Security.

Prashant Jawalkar is Assistant Professor in Computer Engineering Department, JSPM's BSIOTR wagholi College, SPPU, Pune, MS, India.