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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

A Survey on Identity based Two Server Password-Authenticated Key Exchange Protocol

Amol Bhagat[1], Manik Payal[1], Ganesh Admane[1], Rushikesh Fuke[1]

Student, Department of Computer Engineering, Savitribai Phule Pune University, JSPM's JSCOE, Hadapsar, Pune, India[1]

ABSTRACT: The Password Authenticated Key Exchange(PAKE) are protocols, which are designed to be secure even when the secret key used for authentication is a human memorable password. In identity based two-server PAKE protocols, a client devides its password in the two- servers respectively. Then these two-servers cooperate with each other to authenticate the client without knowing the password of the client. In case of one server is compromised by an opponent, the password of the client is required to remain secure. For this, we present two compilers that can transform any two-party PAKE protocols to a two-server PAKE protocols on the basis of identitybased cryptography called ID2S PAKE protocol. Here, we are using two algorithms encryption and decryption algorithms. By the compilers, we can construct ID2S 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 ID2S PAKE protocols constructed by the compilers can be proven to be secure without random oracles our ID2S PAKE protocol can same from 22 % to 66 % of computation in each server.

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

I. INTRODUCTION

To secure communications between two parties, an authenticated encryption key is required to agree on in advance. we consider PAKE protocols in the three-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. In this system, we are providing efficient compilers to transform many three-party PAKE protocol to an ID2S PAKE protocol with identity-based cryptography. By the compilers, we can construct ID2S PAKE protocol which achieve implicit authentication. With the advancement of wireless technology and the increasing demand for resource-constrained mobile devices, secure and efficient password authenticated key exchange (PAKE) protocols are needed for various kinds of secure communications among low-power wireless devices. We present a new protocol called PAK which is the first Diffie-Hellman-based password-authenticated key exchange protocol to provide a formal proof of security against both passive and active adversaries.

II. RELATED WORK

In this project, we present a password-based tripartite key agreement protocol using pairings, it seem that in the standard model. It allows three parties to negotiate a common session key via a shared password over an adversary controlled channel. The paper is organized as follows. In section 2, we introduce some complexity assumptions. In section3, we give the security model. Our protocol is presented in section 4. In section 5, we discuss the security under the standard model. Finally we draw conclusions in section 6.We consider the security of N-EKE-D and N-EKE-M protocol variants of [2],[3],[4]. Although current protocols require a trusted Servers, the advantage of this setting is that it partitions the trust of the group secret among thegroup members, thus in the event of compromise e.g. the shared

DOI: 10.15680/IJIRCCE.2016. 0410182

password is leaked by the compromised member, the remaining non-compromised member scan safely establish future group session keys without needing any change to the members' individual passwords.

In this project, we present a new construction of 3-party PAKE protocol, based on the identity-based encryption (IBE) scheme with security against adaptive chosen cipher text attacks without random oracles, such as (Gentry, 2006; Waters, 2005), and the El Gamal encryption scheme (ElGamal, 1985), which has been proved to be secure against chosen-plaintext attacks without random oracles providing that the Decisional Diffie-Hellman (DDH) assumption holds (Waters, 2009). Our protocol needs only 2 rounds of communications and enjoys provably security without random oracles. It is rather efficient, when compared to the generic construction (Abdalla et al., 2005; Abdalla et al., 2006) and the ID-based group PAKE compiler.In this project, we propose a new symmetric two-server PAKE protocol which supports two servers to compute in parallel and meanwhile keeps efficiency for practical use. Our protocol needs only four communication rounds for the client and two servers mutually to authenticate and simultaneously to establish secret session keys. Our protocol is more efficient than existing symmetric two-server PAKE protocol, such as Katz et al.'s protocol [5].

III. EXISTING SYSTEM

In existing system ID-based PAKE protocol propose by Yi et al., where the client needs to remember a password in addition to the identity of the server, where as the server keeps the password in addition to a private key related to its identity. However, each server must have to perform a total of roughly 80 exponentiations (i.e. is each server's work is increase by a factor of roughly 6 as compare to the basic protocol). To address this problem, the multi-server setting for PAKE was first suggested, where the password of the client is distributed in n server.

Disadvantages of Existing System:

1. **Password Strength:** -Is a measure of the effectiveness of a password in resisting guessing and brute-force attacks.

2. **Lack of Identity Check** is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss.

3. **Shoulder Surfing:** In computer security, shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data.

IV. PROPOSED SYSTEM

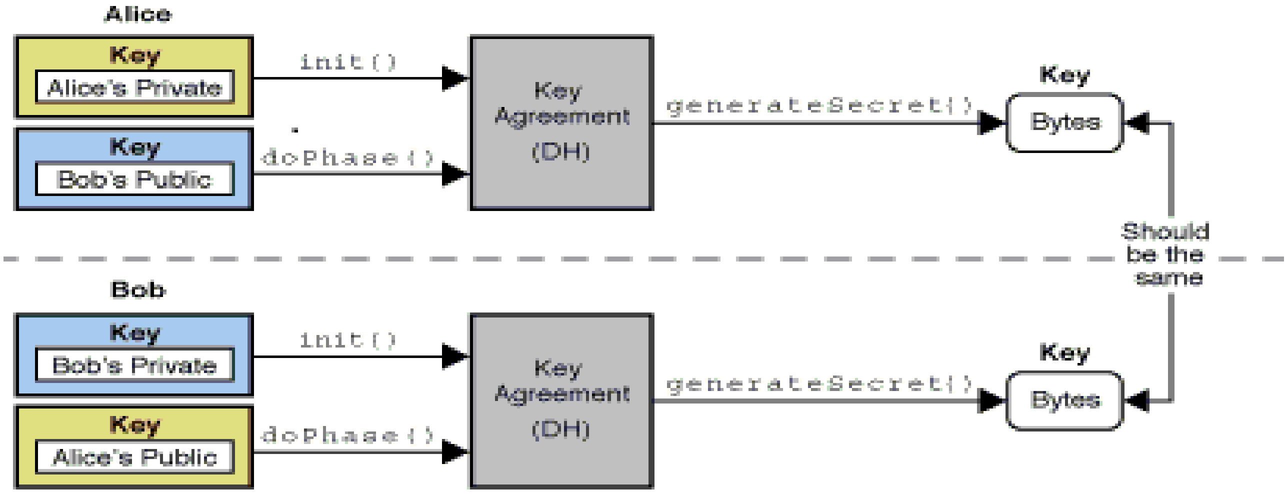

Fig. Proposed system Architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

The architecture consists of the following system entities.

1. User: A user is a person who uses a computer or network service. Users generally use a system or a software product without the technical expertise required to fully understand it. Power users use advanced features of programs, though they are not necessarily capable of computer programming and system administration.
2. Server: A server operating system, also called a server OS, is an operating system specifically designed turn-on servers, which are specialized computers that operate within a client/server architecture to serve the requests of client computers on the network.
3. Admin: A system administrator, or system admin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multiuser computers, such as servers. The system administrator seeks to ensure that the uptime, performance, resources, and security of the computers he or she manages meet the needs of the users, without exceeding the budget.

V. ADVANTAGES

1. It provides a secure, authenticated key-exchange protocol.
2. It is secure against offline dictionary attacks when passwords are used.
3. It ensures Forward Secrecy.
4. It has been proven to be as secure as the Diffie-Hellman solution.

.

VI. CONCLUSION

We proposed a password-based authentication and key exchange system that is built upon a novel two-server model, where only one server communicates to users while the other server stays transparent to the public. Compared with previous solutions, our system possesses many advantages, such as the elimination of a single point of vulnerability, avoidance of PKI, and high efficiency.

REFERENCES

1. X. Yi, S. Ling, and H. Wang. Efficient two-server password-only authenticated key exchange. sIEEE Trans. Parallel Distrib. Syst. 24(9): 1773-1782, 2013.
2. X. Yi, R. Tso and E. Okamoto.ID-based group password authenticated key exchange. In Proc. IWSEC'09, pages 192-211, 2009.
3. Y. Yang, R. H. Deng, and F. Bao. A practical password-based two-server authentication and key exchange system. IEEE Trans. Dependable and Secure Computing, 105-114, 2006.
4. P. MacKenzie, T. Shrimpton, and M. Jakobsson. Threshold password authenticated key exchange. J. Cryptology, 19(1): 27-66, 2006.
5. B. Waters. Efficient identity-based encryption without random oracles. In Proc. Eurocrypt'05, pages 114-
6. 127, 2005.
7. M. Abdalla, P. A. Fouque, D. Pointcheval, "Password-based authenticated key exchange in the three-party setting", *Proc. Public Key Cryptography*, pp. 65-84, 2005.
8. M. Bellare, D. Pointcheval, P. Rogaway, "Authenticated key exchange secure against dictionary attacks", *Proc. 19th Int. Conf. Theory Appl. Cryptographic Techn.*, pp. 139-155, 2000
9. S. M. Bellovin, M. Merritt, "Encrypted key exchange: Password-based protocol secure against dictionary attack", *Proc. IEEE Symp. Res. Security Privacy*, pp. 72-84, 1992.
10. J. Bender, M. Fischlin, D. Kugler, "Security analysis of the PACE key-agreement protocol", *Proc. 12th Int. Conf. Inform. Security*, pp. 33-48, 2009.
11. D. Boneh, M. Franklin, "Identity based encryption from the Weil pairing", *Proc. 21st Annu. Int. Crypto. Conf.*, pp. 213-229, 2001.
12. V. Boyko, P. Mackenzie, S. Patel, "Provably secure password-authenticated key exchange using Diffie-Hellman", *Proc. 19th Int. Conf. Theory Appl. Cryptographic Techn.*, pp. 156-171, 2000.
13. E. Bresson, O. Chevassut, D. Pointcheval, "New security results on encrypted key exchange", *Proc. 7th Int. Workshop Theory Practice Public Key Cryptography*, pp. 145-158, 2004.
14. W. Diffie, M. Hellman, "New directions in cryptography", *IEEE Trans. Inf. Theory*, vol. 32, no. 2, pp. 644-654, Nov. 1976.
15. S. Jiang, G. Gong, "Password based key exchange with mutual authentication", *Proc. 11th Int. Workshop SAC*, pp. 267-279, 2004.
16. J. Katz, P. MacKenzie, G. Taban, V. Gligor, "Two-server password-only authenticated key exchange", *Proc. 3rd Int. Conf. ACNS*, pp. 1-16, 2005.

DOI: 10.15680/IJIRCCE.2016. 0410182