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. 2, Issue 11, November 2014

An Efficient Two-Server Password Only Authenticated Key Exchange Secure Against Dictionary Attacks

Sonal C. Pansare, Prof.Vaishali Nandedkar

II[nd] Year ME, Department of Computer Engineering, PVPIT, Pune, Maharashtra, India

Assistant Professor, Department of Computer Engineering, PVPIT, Pune, Maharashtra, India

ABSTRACT: Password-authenticated key exchange(PAKE) is where a client and a server, who share a password, authenticate each other and meanwhile establish a crypto-graphic key by exchange of messages. In this, 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 this paper, consider a scenario where two servers cooperate to authenticate a client and if one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server. Current solutions for two-server PAKE are either symmetric in the sense that two peer servers equally contribute to the authentication or asymmetric in the sense that one server authenticates the client with the help of another server. This paper presents asymmetric solution for two-server PAKE, where the client can establish different cryptographic keys with the two servers. Our protocol runs in parallel and is more efficient than existing symmetric two-server PAKE protocol and even more efficient than existing asymmetric two-server PAKE protocols in terms of parallel computation.

KEYWORDS: Password-authenticated key exchange,Dictionary Attacks, Diffie-Hellman Key Exchange,ElGamal Encryption,SOAP

I. INTRODUCTION

Nowadays, passwords are commonly used by people during login process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines and so on. A computer user may require pass-words for many purposes: logging in to computer accounts, retrieving e-mail from servers, accessing programs, databases, networks, websites, and even reading the morning newspaper online. Earlier password-based authentication systems trans-mitted 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 passwords hash value.

Current solutions for two-server PAKE are either symmetric in the sense that two peer servers equally contribute to the authentication, such as or asymmetric in the sense that one server authenticates the client with the help of another server, such as. A symmetric two server PAKE protocol, for example, Katz etal.s protocol can run in parallel and establishes secret session keys between the client and two servers, respectively. In case one of the two servers shuts down due to the denial-of-service attack, another server can continue to provide services to authenticated clients. In terms of parallel computation and reliable service, a symmetric protocol is superior to an asymmetric protocol. So far, only Katz etal.s two-server PAKE protocol has been symmetric. But their protocol is not efficient for practical use. An asymmetric two-server PAKE protocol runs in series and only the front-end server and the client need to establish a secret session key. Current asymmetric protocols, for example, Yang et al.s protocol and Jin et al.s protocol, need two servers to exchange messages for several times in series. These asymmetric designsare less efficient than a symmetric design which allows two servers to compute in parallel.

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. 2, Issue 11, November 2014

In this paper, it propose a new symmetric solution for two-server PAKE. In all existing two-server PAKE protocols, two servers are provided random password shares pw1 and pw2 subject to pw1+ pw2=pw. In our protocol, it provide one server S1 with an encryption of the password (g_2^{pw}; pk_2); and another server S2 with an encryption of the password(g_2^{pw}; pk_1) where $pk_1$and pk_2 are the encryption keys of S1 and S2 respectively. In addition, two servers are provided random password shares b1 and b2 subject tob_1b_2 = H(pw) where H is a hash function.

Although it use the concept of public key cryptosystem, our protocol follows the password-only model. The encryption and decryption key pairs for the two servers are generated by the client and delivered to the servers through different secure channels during the client registration, as the client in any two-server PAKE protocol sends two halves of the password to the two servers in secret, respectively. In fact, a server should not know the encryption key of another server and is restricted to operate on the encryption of the password on the basis of the homo-morphic properties of El Gamal encryption scheme.

Security analysis has shown that our protocol is secure against both passive and active attacks in case that one server is compromised. Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols in terms of parallel computation.

Our protocol can be applied in distributed systems where multiple servers exist. For example, Microsoft active directory domain service (AD DS) is the foundation for distributed networks built on Windows server operating systems that use domain controllers. AD DS provides structured and hierarchical data storage for objects in a network such as users, computers, printers, and services.AD DS also provides support for locating and working with these objects. For a large enterprise running its own domain, there must be two AD DS domain controllers, for fault-tolerance purpose. To authenticate a user on a network, the user usually needs to provide his/her identification and password to one AD DS domain controller. Based on our two-server PAKE protocol, it can split the users password into two parts and store them, respectively, on the two AD DS domain controllers, which can then cooperate to authenticate the user. Even if one domain controller is com-promised, the system can still work. In this way, we can achieve more secure AD DS.

II. LITERATURE SURVEY

- **Katz et.al system**

In 2005, Katz et al. proposed the first two-server password-only authenticated key exchange protocol with a proof of security in the standard model. Their protocol extended and built upon the Katz-Ostrovsky-Yung PAKE protocol called KOY protocol for brevity. In their protocol, a client C randomly chooses a password pw, and two servers A and B are provided random password shares pw1 and pw2 subject to pw1+pw2=pw. At high level, their protocol can be viewed as two executions of the KOY protocol, one between the client C and the server A, using the server B to assist with the authentication, and one between the client C and the server B, using the server A to assist with the authentication. The assistance of the other server is necessary since the password is split between two servers. In the end of their protocol, each server and the client agree on a secret session key. Katz etal.s protocol is symmetric where two servers equally contribute to the client authentication and key exchange. For their basic protocol secure against a passive adversary, each party performs roughly twice the amount of works as the KOY protocol. For the protocol secure against active adversaries, the work of the client remains the same but the work of the servers increase by a factor of roughly 2-4.

- **Yang et al. system**

Built on Brainard et al.s work in 2005, Yang et al. suggested an asymmetric setting, where a front-end server, called service server (SS), interacts with the client, while a back-end server, called control server (CS), helps SS with the authentication, and only SS and the client agree on a secret session key in the end. They proposed a PKI-based asymmetric two-server PAKE protocol in 2005 and several asymmetric password-only two-server PAKE protocols.

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. 2, Issue 11, November 2014

Next, SS and the client authenticate each other by checking if they can agree on the same secret session key, with the help of CS, where a, (a1,b1) and b2 are randomly chosen by the client, SS and CS, respectively. The security of Yang etal.s protocol in [30] is based on an assumption that the back-end server cannot be compromised by an active adversary. This assumption was later removed at the cost of more computation and communication rounds.

- **Jin Two-Server System**

Jin further improved Yang etal.s protocol and proposed a two-server PAKE protocol with less communication rounds. In their protocol, the client sends

$B = g_1^a g_2$
to SS; SS forwards
$B_1 = B = g_1^{(b1)} g_2^{(1)}$

to CS; CS returns

$A1 = g1^{(b2)}$; $B2 = ((B1 = g2^{(2)}))^{(b2)} = g1^{((a\ b1)b2)}$

to SS; SS computes
$B3 = ((B2 = A1^{(b2)}))^{(b3)} = g^{(ab2b3)}$

and responds
$A_2 = A_1^{(b3)}$; $S_1 = H(B_3)$

to the client, where H is a hash function. Next, SS and the client authenticate each other by checking if they can agree on the same secret session key

III. MODELS

- **Server Password Authentication Models**

In the single-server model, where a single server is involved and it keeps a database of user passwords. Most of the existing password systems follow this single-server model, but the single server results in a single point of vulnerability in terms of off line dictionary attacks against the user password database.

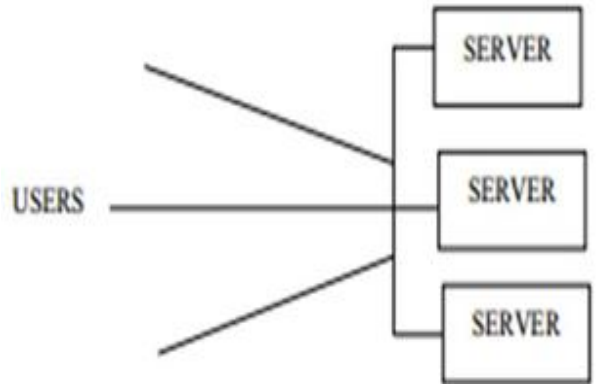

Fig1 Multi Server Password Model

In the multi-server model as shown above Figure, the server side comprises multiple servers for the purpose of removing the single point of vulnerability, the servers are equally exposed to users and a user has to communicate in

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. 2, Issue 11, November 2014

parallel with several or all servers for authentication. The main problem with the plain multi-server model is the demand on communication band-width and the need for synchronization at the user side since a user has to engage in simultaneous communications with multiple servers. This may cause problems to resource-constrained mobile devices such as hand phones and PDAs.

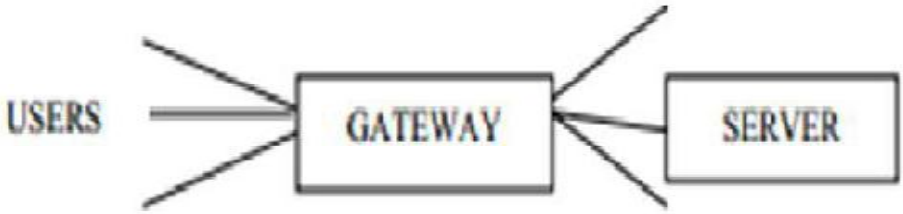

Fig 2 Gateway Augmented Multi Server Model

In the gateway augmented multi-server model as shown in Figure 2, gateway is positioned s a relaying point between users and servers and a user only needs to contact the gateway. Apparently, the introduction of the gateway removes the demand of simultaneous communications by a user with multiple servers as in the plain multi-server model. However, the gateway introduces an additional layer in the architecture, which appears redundant since the purpose of the gateway is simply to relay messages between users and servers, and it does not in any way involve in service provision, authentication, and other security enforcements. From security perspective, more components generally imply more points of vulnerabilities.

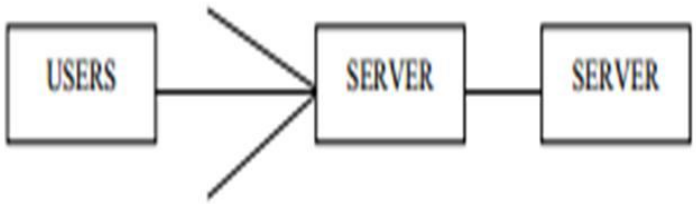

Fig 3 Two Server Model

The two-server model comprises two servers at the server side, one of which is a public server exposing itself to users and the other of which is a back-end server staying behind the scene; users contact only the public server, but the two servers work together to authenticate users. The differences between the two-server model and the earlier multi-server models are

1. In the two-server model, a user ends up establishing a session key only with the public server, and the role of the back-end server is merely to assist the public server in user authentication, while in the multi-server models, a user establishes a session key (either different or the same) with each of the servers.

2. From a security point of view, servers in the multi-server models are equally exposed to outside attackers (recall that the gateway in the gateway augmented multi-server model does not enforce security), while in the two-server model, only the public server faces such a problem. This improves the server side security and the overall system security in the two-server model. In two server model, different levels of trust upon the two servers with respect to outside attackers can be made. The back-end server is more trustworthy than the public server. This is logical since the back-end server is located in the back-end and is hidden from the public, and it is thus less likely to be attacked. Two-server model has successfully eliminated drawbacks in the plain multi-server model (i.e., simultaneous communications between a user and multiple servers) and the gateway augmented multi-

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. 2, Issue 11, November 2014

server model (i.e., redundancy) while allowing us to distribute user passwords and the authentication functionality to two servers in order to eliminate a single point of vulnerability in the single server model. As a result, the two-server model appears to be a sound model for practical applications. The existing systems upon the two server model are not sufficient, in turn motivated to present a password-only system over the two server model.

IV. PROTOCOLS

- **Diffie-Hellman Key Exchange Protocol**

Diffie Hellman establishes a shared secret that can be used for secret communications while exchanging data over a public network. To implement Diffie-Hellman[3], the two end users Alice and Bob, at the same time as communicating under a channel they mutually agree on two positive whole numbers q and g, such that q is a prime number and g is a generator of q. The generator g is a number to facilitate, when raised to constructive whole-number powers less than q, never produces the same result for any two such whole numbers. The value of q may be large but the value of g is usually small. Diffie Hellman key exchange (DH)[nb 1] is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
Although Diffie Hellman key agreement itself is an anonymous (non-authenticated) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite).The method was followed shortly afterwards by RSA, an implementation of public key cryptography using asymmetric algorithms.Once Alice and Bob have agreed on q and g in private, they choose random positive whole-number m and n, Next, Alice and Bob compute public keys A and B based on their personal keys according to the formulas
1. $A = g^m \text{mod} p$
2. $B = g^n \text{mod} q$
3. The two users can share their public keys A and B over a communications medium assumed to be not confident, such as the Internet or a commercial wide area network (WAN). From these public keys, a number x can be generated by either user on the basis of their own personal keys. Alice computes K1 using the formula
4. $K_1 = (B)^m \text{mod} q$
5.Bob computes K2 using the formula
6.$K_2 = (A)^n \text{mod} q$
Obviously K1=K2.So this will be shared secret key among Alice and Bob.

- **ElGamal Encryption Scheme**

In cryptography, the ElGamal encryption system [5] is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie Hellman key exchange. It was described by TaherElgamal in 1984. It consists of key creation, encryption, and decryption all the steps (Algorithms) as followsKey generation:-
The key generator works as follows:

1. Alice generates an efficient description of a multiplicative cyclic group G of order q with generator g. See below for a discussion on the required properties of this group.
2. Alice chooses a random x from 1, , q-1.
3. Alice computes $h = g^x$:
4. Alice publishes h, along with the description of G,q,g as her public key. Alice retains x as her private key which must be kept secret.

V. WEB SERVICES

A Web service, in the context of .NET, is a component that resides on a Web server and provides information and

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. 2, Issue 11, November 2014

services to other network applications using standard Web protocols such as HTTP and Simple Object Access Protocol (SOAP).A Web service is a method of communication between two electronic devices over World Wide Web (WWW). A web service is a software task provide at a network address over the web or the cloud; it is a service that is ”always on” as in the concept of utility computing.

- What is SOAP?

SOAP is nothing but Simple Object Access Protocol. SOAP is a communication protocol. SOAP is for communication between applications SOAP is a format for sending messages. SOAP communicates via Internet. SOAP is platform independent. SOAP is based on XML. SOAP is language independent. SOAP is simple and extensible. SOAP allow you to get approximately firewalls.SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built. This XML-based protocol consists of three parts: an envelope, which defines what is in the message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing procedure calls and responses. SOAP has three major characteristics: extensibility (security and WS-routing are among the extensions under development), neutrality (SOAP can be used over any transport protocol such as HTTP, SMTP, TCP, UDP, or JMS), and independence (SOAP allows for any programming model). As an example of how SOAP procedures can be used, a SOAP message could be sent to a web site that has web services enabled, such as a real-estate price database, with the parameters needed for a search. The site would then re-turn an XML-formatted document with the resulting data, e.g., prices, location, features. With the data being returned in a standardized machine-parsable format, it can then be integrated directly into a third-party web site or application.

- **2-Step Verification**

In this paper it using a technique called ”2-Step Verification” which is explained be-low:

The following common actions could put you at risk of having your password stolen:

- Using the same password on more than one site.
- Downloading software from the Internet.
- Clicking on links in email messages.

2-Step Verification can help keep bad guys out, even if they have your password.

1. Signing in to your account will work a little differently:
   - Enter your password:
   - Whenever you sign in to account, you’ll enter your password as usual.
   - Enter a verification code:
   - Then, you’ll be asked for a code that will be sent to your phone via text, voice call, or email.
2. An extra layer of security:

Most people only have one layer their password to protect their account. With 2-Step Verification, if a bad guy hacks through your password layer, he’ll still need your phone to get into your account.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Figure 42-step verification

VI. PROPOSED SYSTEM

Our system consist a group of clients and two servers S1 and S2. The S1 and S2 cooperate and communicate for client authentication and allows the client to use services. A password pwC is chosen by each client C and password authentication information Authc(1) and Au-thc(2) is generated for S1 and S2, such that no one can identify the password pwC from Au-thc(1) or Authc(2) unless and until S1 and S2 collaborate. During the client registration, client sends Authc(1) and Authc(2) to S1 and S2, respectively, through various secure channels. After that, password authentication information i.eAuthc(1) and Authc(2) is kept by two servers and the client only remembers the password.

Like all present solutions for two-server PAKE, we guess the two servers never get together to expose the password of the client. When the two servers collaborate to validate a client C, we think that the client C can transmit a message to both of S1 and S2 concurrently, In our system, the two servers and the client communicate through a public medium which may be snooped, belated, replayed, and even tampered by an attacker. If two servers equally contribute to the verification in form of communication and calculation then we can say that our protocol is symmetric. The challenges in our system may be passive or active. We are concern with both online dictionary attack and offline dictionary attack, online dictionary attack hacker try to login frequently, attempts each possible password, and in offline dictionary attack, where an attacker builds the information about the password from observed transcripts of log sessions.

The online dictionary attack cannot be prohibited by cryptography however it can be easily detected and suspended once the authentication fails several times. We have assumption that an attacker can compromise only one server and can get all information stored in the server. A passive attack is able to check the communications among the two server and client. An active attack is able to imagine that, the client and one server to communicate with the truthful server or imagine to be both servers to communicate with the valid client, diverge in random way from the actions set by the protocol. In our protocol, the attacker tries to learn the private session key which is established between the client and the honest server. In an active attack, if the attacker able to determine the password of the client then an attacker can learn the private session key between the honest server and the client. Normally, we say that our protocol is secure if attacker cannot successful in any active and passive attacks in case that one server is compromised.

VII. SYSTEM ARCHITECTURE

A system architecture or system's architecture is the conceptual model that de-fines the structure, behaviour, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures of the system.

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. 2, Issue 11, November 2014

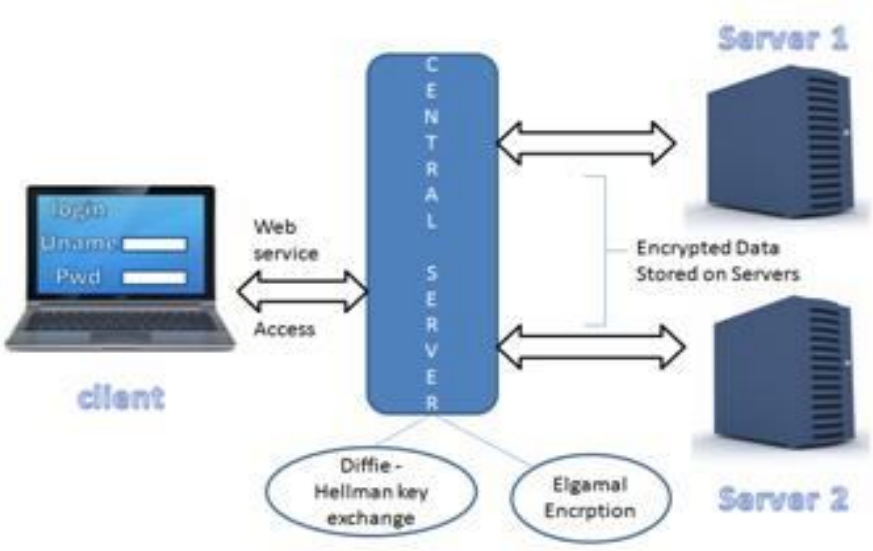

Figure 5 System Architecture

Our protocol works in four stages

1. Initialization
In almost all existing two-server PAKE protocols such as [15], [16], [8], it is implied that the discrete logarithm of g2 to the base g1 is unidentified to anyone hence their protocols are secure. Our initialization can ensure that no one is capable to know the discrete logarithm of g2 to the base g1 unless and until the two servers get together. Our model assumes that the two servers never collude because discrete logarithm problem is hard.

2. Registration
For authentication, each client C is need to register both server S1 and S2 through unlike secure channels. Firstly, the client C generates encryption and decryption key pairs (xi, yi) using the public parameters published by the two servers where yi=g1xi for the server Si (i=1, 2).
After that, client C elects a password pwC and encrypts that password by using the encryption key yi, i.e., (g2pwc,yi)=(Ai, Bi)=(g1ai, g2pwc yiai) (i=1,2) where ai is chosen randomly from Z*q , according to ElGamal encryption.
After that, the client C chooses b1 randomly from Z*q and lets b2=H(pwC) b1, where stands for two l-bit blocks exclusive ORFinally, client C sends the password authentication information to S1 through a secure channel, i.e. Authc(1)=x1,a1,b1,(g2pwc,y2) and the password authentication information to S2 through another secure channel i.e. Authc(2) =x2,a2,b2,(g2pwc,y1).
Next, client C remembers the only password pwC
For all two servers PAKE protocols the two secure channels are required. During registration a password is split into two distinct parts and those parts are securely distributed to the two servers S1 and S2, respectively. The encryption key of one server is unknown to another server and after registration client remembers a only password.

3. Authentication and Key Exchange:
Now it consider that the two servers S1 and S2 having the authentication information of a client C, to authenticate the client C there are following five steps for the S1 and S2 and establish private session keys with the client C in terms of parallel computation.

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. 2, Issue 11, November 2014

4.Two step Mobile Verification
Mobile users generating the verification code on gmail account then the user will generate random code and send it to the verification user system, and after that server 1 and server 2's data has match then commit otherwise, rollback the system.

VIII. CONCLUSION

This paper, proposed work continues the line of research on the two-server paradigm in, extend the model by imposing different levels of trust upon the two servers, and adopt a very different method at the technical level in the protocol design. As a result, propose a practical two-server password authentication and key exchange system that is secure against offline dictionary attacks by servers when they are controlled by adversaries. The proposed scheme is a password-only system in the sense that it requires no public key cryptosystem and, no PKI. The paper work, generalize the basic two-server model to architecture of a single back-end server supporting multiple frontend servers and envision interesting applications in federated enterprises. In the given authentication schema we also use SMS integration API for two step verification like Gmail, it will provide the additional security to end user.

REFERENCES

1. XunYi, San Ling, and Huaxiong WangEfficient Two-Server Password-Only Authenticated Key Exchange IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013
2. M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols," Proc. Int'l Conf. Topics in Cryptology (CT-RSA), pp. 191-208, 2005.
3. M. Abdalla, O. Chevassut, and D. Pointcheval, "One-Time Verifier-Based Encrypted Key Exchange," Proc. Eighth Int'l Conf. Theory and Practice in Public Key Cryptography (PKC '05), pp. 47-64, 2005.
4. M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure against Dictionary Attacks," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 139-155, 2000.
5. S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password- Based Protocol Secure against Dictionary Attack," Proc. IEEE Symp. Research in Security and Privacy, pp. 72-84, 1992.
6. D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. (Crypto '01), pp. 213-229, 2001.
7. D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586-615, 2003.
8. D. Boneh, "The Decisional Diffie-Hellman Problem," Proc. Third Int'l Algorithmic Number Theory Symp., pp. 241-250, 1998.
9. V. Boyko, P. Mackenzie, and S. Patel, "Provably Secure Password- Authenticated Key Exchange Using Diffie-Hellman," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 156-171, 2000.
10. J. Brainard, A. Jueles, B.S. Kaliski, and M. Szydlo, "A New Two- Server Approach for Authentication with Short Secret," Proc. 12th Conf. USENIX Security Symp., pp. 201-214, 2003.
11. W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, IT-22, no. 6, pp. 644-654,Nov. 1976.
12. L. Gong, T.M.A. Lomas, R.M. Needham, and J.H. Saltzer, "Protecting Poorly-Chosen Secret from Guessing Attacks," IEEE
13. J. Selected Areas in Comm., vol. 11, no. 5, pp. 648-656, June 1993.
14. S. Halevi and H. Krawczyk, "Public-Key Cryptography and Password Protocols," ACM Trans. Information and System Security,
15. vol. 2, no. 3, pp. 230-268, 1999.
16. D. Jablon, "Password Authentication Using Multiple Servers," Proc. Conf. Topics in Cryptology: The Cryptographer's Track at RSA (RSA-CT '01), pp. 344-360, 2001.
17. H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password-Only Two- Server Authenticated Key Exchange System," Proc. Ninth Int'lConf. Information and Comm. Security (ICICS '07), pp. 44-56, 2007.
18. J. Katz, R. Ostrovsky, and M. Yung, "Efficient Password- Authenticated Key Exchange Using Human-Memorable Passwords,"
19. Proc. Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (Eurocrypt '01), pp. 457-494,
20. 2001.YI ET AL.: EFFICIENT TWO-SERVER PASSWORD-ONLY AUTHENTICATED KEY EXCHANGE 1781

BIOGRAPHY

Miss. SonalChandrakantPansare is a student of Masters in Engineering,Computer Department, PVPIT ,PuneUniversity. She received Bachelors of Engineering in 2010 from Mumbai University. Her research interests are Computer Networks (wireless Networks), web 2.0, Network Security etc.

Prof.VaishaliNandedkar is working as Assistant Professor and Head of Department of Information Technology in PVPIT, Pune University. She Completed her master in engineering (CSE) with specialisation Signal Processing And now she is perusing her Ph.D.