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. 3, Issue 5, May 2015

Efficient Two-Server Password-Only Authenticated Key Exchange

Rachana R. Gundewar

Department of CSE, Khurana Sawant Institute of Engineering &Technology, Hingoli, SRTM University Nanded, MS, 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 cryptographic key by exchange of messages. 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 attack, passwords stored in the server are all disclosed. In this paper, we 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 a symmetric solution for two-server PAKE, where the client can establish different cryptographic keys with the two servers, respectively. 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 attack, Diffie-Hellman key exchange, ElGamal

I. INTRODUCTION

In recent days, 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. 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. 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.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. In general, current solutions for password based authentication follow two models. 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. Gong et al. were the first to present this kind of authentication protocols with heuristic resistant to offline dictionary attacks, and Halevi and Krawczyk were the first to provide formal definitions and rigorous proofs of security for PKI-based model. The second model is called password-only model. Bellovin and Merritt were the first to consider authentication based on password only, and introduced a set of so-called "encrypted key exchange" protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose. Formal models of security for the password-only authentication were first given independently by Bellare et al. and Boyko et al.Katz et al. were the first to give a password-only authentication protocol which is both practical and provably secure under standard cryptographic assumption. Based on the identity-based encryption technique suggested an identity-based model where the client needs to remember the password only while the server keeps the password in addition to private keys related to its identity. In this setting, the client can encrypt the password based on the identity of the server. This model is between the PKI-based and the password only

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. 3, Issue 5, May 2015

models. Typical protocols for password-based authentication assume a single server stores all the passwords necessary to authenticate clients. If the server is compromised, due to, for example, hacking, or installing a "Trojan horse," or even insider attack, user passwords store in the server are disclosed. To address this issue, two-server password-based authentication protocols were introduced in , where two servers cooperate to authenticate a client on the basis of password and if one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server.

II. RESEARCH ELABORATIONS

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 et al.'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 et al.'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 [18], need two servers to exchange messages for several times in series. These asymmetric designs are less efficient than a symmetric design which allows two servers to compute in parallel.Basically our work will be divide in three different phases when Our protocol runs in three phases—initialization, registration, and authentication we have to implement all strategies in given.

Algorithms:
Diffie-Hellman Key Exchange Protocol
Elgamal Encryption Key exchange

Enhancement: In the given research work on the basis paper results we have to improve the current results with the drastic security. Basically we have some procedures to improve the results. Basically the Our protocol runs in three phases—initialization, registration, and authentication we have to implement all strategies in given research work.

Additional algorithm

Secrete sharing algorithm
Key threshold algorithm
Web services

We will use here web services, for authentication purpose, we will use secrete sharing algorithm for authentication purpose. above algorithms will provide the drastic security to all kind of applications.

Approach:

Registration phase
In the registration phase, the user has to enter the password and another one random number which should be at least two less than the length of the password. (i.e.) 1<R<L-2, R - Random Integer L - Length of the Password
For example the user registered with the password," 1234567". In our system, the user should also enter a random number. Here let it be "3". It could not be an integer greater than 5 in this case. Upto this, the registration phase is over. Users are not allowed to set null password as well as zero as the random number.

Authentication phase
In this phase the entered password is divided into two shares according to that random number which was entered during the registration phase. In our example, the password 'P' is divided into 'P1' and 'P2'. Here the share of P1 is"

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. 3, Issue 5, May 2015

123" and P2 is" 4567" as in Fig.4. So, the share of P1 is authenticated by the Front end server and the P2 is authenticated by the back end server. In case of a legitimate user, if he enters the correct password, he is uthenticated by the two servers. Next, we will check for an intruder.

Advantages:

- Using proposed it will maintain drastic security.
- Data will be encrypted when it serialize.
- Improve security Quality

III. RESULTS OR FINDINGS

Public key techniques are absolutely necessary to make password systems secure against offline dictionary attacks, whereas the involvement of public key cryptosys-tems under a PKI (e.g., public key encryption and digital signature schemes) is not essential. There are two separate approaches to the development of secure pass-word systems one is a combined use of a password and public key cryptosystem under a PKI and the other is a password only approach. In these systems, the use of public keys entails the deployment and maintenance of a PKI for public key certification and adds to users the burden of checking key validity. To eliminate this drawback, password-only protocols (password authenticated key exchange or PAKE) have been extensively studied. The PAKE protocols do not involve any public key cryptosystem under a PKI and, therefore, are much more attractive for real world applications. Any use of public key cryptosystem under a PKI in a password authentication system should be avoided since; otherwise, the benefits brought by the use of password would be counteracted to a great extent. Most of the existing password systems were designed over a single server, where each user shares a password or some password verification data (PVD) with a single authentication server. These systems are essentially intended to defeat offline dic-tionary attacks by outside attackers and assume that the sever is completely trusted in protecting the user password database. Unfortunately, attackers in practice take on a variety of forms, such as hackers, viruses, worms, accidents, misconfigurations, and disgruntled system administrators. As a result, no security measures and precautions can guarantee that a system will never be penetrated. Once an authentication server is compromised, all the user passwords or PVD fall in the hands of the attackers, who are definitely effective in offline dictionary attacks against the user passwords. To eliminate this single point of vulnerability inherent in the single-server systems, password systems based on multiple servers were proposed. The principle is distributing the password database as well as the authentication function to multiple servers so that an attacker is forced to compromise several servers to be successful in offline dictionary attacks. The system in D. Boneh and M. Franklin protocol, believed to be the first multi-server password system, splits a password among multiple servers. However, the servers in D. Boneh and M. Franklin protocol need to use public keys. An improved version of D. Boneh and M. Franklin protocol was proposed in D. Boneh, The Decisional Diffie-Hellman Problem, protocol, which eliminates the use of public keys by the servers.

Further and more rigorous extension were due to V. Boyko, P. Mackenzie, and S. Patel protocol, where the former built a t-out of-n threshold PAKE protocol and provided a formal security proof under the random oracle model D. Boneh and M. Franklin, Identity Based Encryption from the Weil Pairing, and the latter presented two provably secure threshold PAKE protocols under the standard model. While the protocols are theoretically significant, they have low efficiency and high operational overhead. In these multi-server password systems, either the servers are equally exposed to the users or a user has to communicate in parallel with several or all servers for authentication, or a gateway is introduced between the users and the servers. Recently, Brainard et al. proposed a two-server password system in which one server exposes itself to users and the other is hidden from the pub-lic. While this two-server setting is interesting, it is not a password-only system: Both servers need to have public keys to protect the communication channels from users to servers. As we have stressed earlier, this makes it difficult to fully en-joy the benefits of a password system. In addition, the system in M. Abdalla and D. Pointcheval protocol only performs unilateral authentication and relies on the Secure Socket Layer (SSL) to establish a session key between a user and the front-end server. Subsequently, Yang et al. extended and tailored this two-server system to the context of federated enterprises, where the back-end server is managed by an enterprise headquarters and each affiliating organization operates a front-end server. An improvement made in Yang is that only the back-end server holds a public key Nevertheless, the system in Yang is still not a password-only 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. 3, Issue 5, May 2015

In a single-server PAKE protocol, if the server is compromised, user passwords stored in the server are all disclosed. To address this issue, in 2000, Ford and Kaliskiproposed the first threshold PAKE protocol in the PKI- based model, in which n servers cooperate to authenticate a client. Their protocol remains secure as long as n 1 or few servers are compromised. Subsequently, in 2001, Joblonremoved the requirement for PKI and suggested a protocol with the similar property in the password-only model. Both the threshold PAKE protocols were not shown to be secure formally. In 2002, MacKenziegave a protocol in the PKI-based setting, which requires only t out of n servers to cooperate to authenticate a client and is secure as long as t1 or fewer servers are compromised. They were the first to provide a formal security proof for their threshold PAKE protocol in the random oracle model. In 2003, Di Raimondo and Gennaroproposed a protocol in the password-only setting, which requires less than 1/3 of the servers to be compromised, with a formal security proof in the standard model. In 2003, Brainard developed the first two-server protocol in the PKI-based setting. Their protocol and its variant assume a secure channel between the client and the server(s), which would be in practice implemented using public key techniques such as SSL.

1) In 2005, Katz 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 pw_1 and pw_2 subject to $pw_1+pw_2=pw$. 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 et al.'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.

Advantage:-The advantage of Katz et al.'s protocols is the protocol structure which supports two servers to compute in parallel.
Disadvantage:-Inefficiency for practical use.

2) 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 in 2006. In their password-only protocol the client initiates a request, and *SS* responds with *B*=, where = and = are generated by *SS* and *CS* on the basis of their random password shares π_1 and π_2, respectively and then the client can obtainby eliminating the password $\pi(=\pi_1+\pi_2)$ from *B*, i.e. computing *B/*. Next, *SS* and the client authenticate each other by checking if they can agree on the same secret session key, eitheror ,with the help of *CS*, where *a*, *(,)* and are randomly chosen by the client, *SS* and *CS*, respectively. The security of Yang et al.'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.
Advantage:-efficiency for practical use. Yang et al.'s protocols are more efficient than Katz et al.'s protocols in terms of communication and computation complexities,
Disadvantage:-it's protocol structure which requires two servers to compute in series and needs more communication rounds.

3)In 2007, Jin further improved Yang et al.'s protocol and proposed a two-server PAKE protocol with less communication rounds. In their protocol, the client sends *B*=to *SS; SS* forwards = *B/*to *CS*; *CS* returns =, ==to *SS; SS* computes ==and responds =, =*H* ()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 ,where *a*,(,), are randomly chosen by the client, *SS* and *CS*, respectively.
Advantage: -It needs less communication rounds than Yang et al.'s protocol without introducing additional computation complexity.

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. 3, Issue 5, May 2015

Disadvantage:-Its protocol structure which requires two servers to compute in series.

IV. CONCLUSION

In this paper, we have presented a symmetric protocol for two-server password-only authentication and key exchange. Security analysis has shown that our protocol is secure against passive and active attacks in case that one of the two servers is compromised. Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586-615, 2003.
[7] D. Boneh, "The Decisional Diffie-Hellman Problem," Proc. Third Int'l Algorithmic Number Theory Symp., pp. 241-250, 1998.
[8] V. Boyko, P. Mackenzie, and S. Patel, "Provably Secure Password- Authenticated Key Exchange Using Diffie-Hellman," Proc. 19thInt'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 156-171, 2000.
[9] 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.
[10] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, IT-22, no. 6, pp. 644-654, Nov. 1976.
[11] M. Di Raimondo and R. Gennaro, "Provably Secure Threshold Password Authenticated Key Exchange," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt '03), pp. 507-523, 2003.
[12] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.
[13] W. Ford and B.S. Kaliski Jr., "Server-Assisted Generation of a Strong Secret from a Password," Proc. IEEE Ninth Int'l Workshop Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 176-180, 2000.
[14] O. Goldreich and Y. Lindell, "Session-Key Generation using Human Passwords Only," Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (Crypto '01), pp. 408-432, 2001.
[15] L. Gong, T.M.A. Lomas, R.M. Needham, and J.H. Saltzer, "Protecting Poorly-Chosen Secret from Guessing Attacks," IEEE J. Selected Areas in Comm., vol. 11, no. 5, pp. 648-656, June 1993.
[16] S. Halevi and H. Krawczyk, "Public-Key Cryptography and Password Protocols," ACM Trans. Information and System Security, vol. 2, no. 3, pp. 230-268, 1999.
[17] 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.
[18] H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password-Only Two-Server Authenticated Key Exchange System," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS '07), pp. 44-56, 2007.
[19] J. Katz, R. Ostrovsky, and M. Yung, "Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords,"Proc. Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (Eurocrypt '01), pp. 457-494, 2001.
YI ET AL.: EFFICIENT TWO-SERVER PASSWORD-ONLY AUTHENTICATED KEY EXCHANGE 1781 TABLE 2 Performance Comparison of Our Protocol with YDB and JWX Protocols
[20] J. Katz, P. MacKenzie, G. Taban, and V. Gligor, "Two-Server Password-Only Authenticated Key Exchange," Proc. Applied Cryptography and Network Security (ACNS '05), pp. 1-16, 2005.
[21] J. Katz and M. Yung, "Scalable Protocols for Authenticated Group Key Exchange," Proc. Advances in Cryptology Conf. (Crypto '03), pp. 110-125, 2003.
[22] T.M.A. Lomas, L. Gong, J.H. Saltzer, and R.M. Needham, "Reducing Risks from Poorly-Chosen Keys," ACM Operating Systems Rev., vol. 23, no. 5, pp. 14-18, 1989.
[23] P. MacKenzie, S. Patel, and R. Swaminathan, "Password-Authenticated Key Exchange Based on RSA," Proc. Sixth Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt '00), pp. 599-613, 2000.
[24] P. Mackenize, T. Shrimpton, and M. Jakobsson, "Threshold Password-Authenticated key Exchange," Proc. 22nd Ann. Int'l Cryptology Conf. (Crypto '02), pp. 385-400, 2002.
[25] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.
[26] http://www.schneier.com/blog/archives/2006/12/realworld_ passw.html, 2013.
[27] M. Szydlo and B. Kaliski, "Proofs for Two-Server Password Authentication," Proc. Int'l Conf. Topics in Cryptology (RSA-CT '05),pp. 227-244, 2005.

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. 3, Issue 5, May 2015

[28] Y. Tsiounis and M. Yung, "On the Security of ElGamal based Encryption," Proc. First Int'l Workshop Practice and Theory in Public Key Cryptography: Public Key Cryptography (PKC '98), pp. 117-134,1998.
[29] Y. Yang, F. Bao, and R.H. Deng, "A New Architecture for Authentication and Key Exchange Using Password for Federated Enterprise," Proc. 20th IFIP Int'l Information Security Conf. (SEC'05), pp. 95-111, 2005.
[30] 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, vol. 3, no. 2, pp. 105-114,Apr.-June 2006.
[31] Y. Yang, R.H. Deng, and F. Bao, "Fortifying Password Authenticationin Integrated Healthcare Delivery Systems," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '06), pp. 255-265, 2006.
[32] X. Yi, R. Tso, and E. Okamoto, "ID-Based Group Password-Authenticated Key Exchange," Proc. Fourth Int'l Workshop Security:Advances in Information and Computer Security (IWSEC '09), pp. 192-211, 2009.
[33] X. Yi, R. Tso, and E. Okamoto, "Three-Party Password-Authenticated Key Exchange without Random Oracles," Proc. Int'l Conf. Security and Cryptography (SECRYPT '11), pp. 15-24, 2011.
[34] X. Yi, R. Tso, and E. Okamoto, "Identity-Based Password-Authenticated Key Exchange for Client/Server Model," Proc. Int'l Conf. Security and Cryptography (SECRYPT '12), pp. 45-54, 2012.