Multi-Server Password-Authenticated Key Exchange for Provable Security

Hussein Ali Ghadhban Alsalman, MSC(IS), Directorate of Education in Basra

hussain_alsalman@yahoo.com

Abstract

Password authentication has been around for long time. In the contemporary digital world, password plays very important role. However, there are many issues with password based authentication mechanisms. Different kinds of attacks like dictionary attack are to be considered in order to have high level of security. In this context, it is recommended to have strong passwords that cannot be subjected to such attacks. Moreover, it is important to implement limitation to number of attempts. Many researchers contributed towards password authentication and secure key exchange. However, it is an open problem that can be optimized. In this paper, we proposed a methodology to build a protocol that makes use of two or more servers in order to store shares of passwords. These servers provide cooperation for secure password-authenticated key exchange for provable security. We built a prototype application to demonstrate the proof of the concept. The results revealed that the proposed system is able to show the utility of the protocol.

Index Terms – Security, authentication, authorization, key exchange

الخلاصة

مصادقة كلمات المرور كانت مستخدمة منذ فترة طويلة ، وفي العالم الرقمي المعاصر فإن كلمات المرور تلعب دوراً مهماً ، مع ذلك فإن هنالك العديد من المشاكل التي تصاحب آليات المصادقة باستخدام كلمات المرور . وقد اعتمدت أنواع مختلفة من الهجمات مثل هجوم القاموس للحصول على مستوٍ عالٍ من الامان ، وفي هذا السياق فأنه يوصى بامتلاك كلمات مرور قوية للحيلولة دون التعرض للهجوم ، علاوة على ذلك فأنه من الضروري وضع حد لمرات المحاولة . الكثير من الابحاث ساهمت في مجال مصادقة كلمات المرور وكذلك تبادل المفاتيح الآمن مع ذلك فأنها تبقى مشكلة مفتوحة قابة للتطوير .في هذا البحث اقترحنا منهجية لبناء بروتوكول لاستخدام اثنين او اكثر من الخوادم من أجل خزن كلمات مرور مشتركة ، وهذا الخوادم توفر امكانية التعاون لمصادقة مفتاح كلمة المرور الآمن ، وقد قمنا ببناء نموذج مبدئي لأثبات هذا المفهوم حيث اظهرت النتائج ان النظام المقترح قادر على اظهار فائدة البروتوكول المستخدم .

الكلمات الدالة – الأمان ، المصادقة ، الترخيص ، تبادل المفاتيح

INTRODUCTION

Secure communications play important role in different networks. Traditionally security is provided for applications in the form of user id and password. Moreover the security can be provided using cryptographic primitives with respect to data. Even the credentials can be encrypted in order to avoid leakage. Private Key or symmetric key cryptography and public key or asymmetric cryptography are two important cryptographic primitives came into existence. There is another layer of security used of late. It is known as one time password which is generated by the server and user is challenged to prove credentials. With mobile devices being used by users, the OTP became very hand for authorization. The traditional authentication based on password is shown in Figure 1.

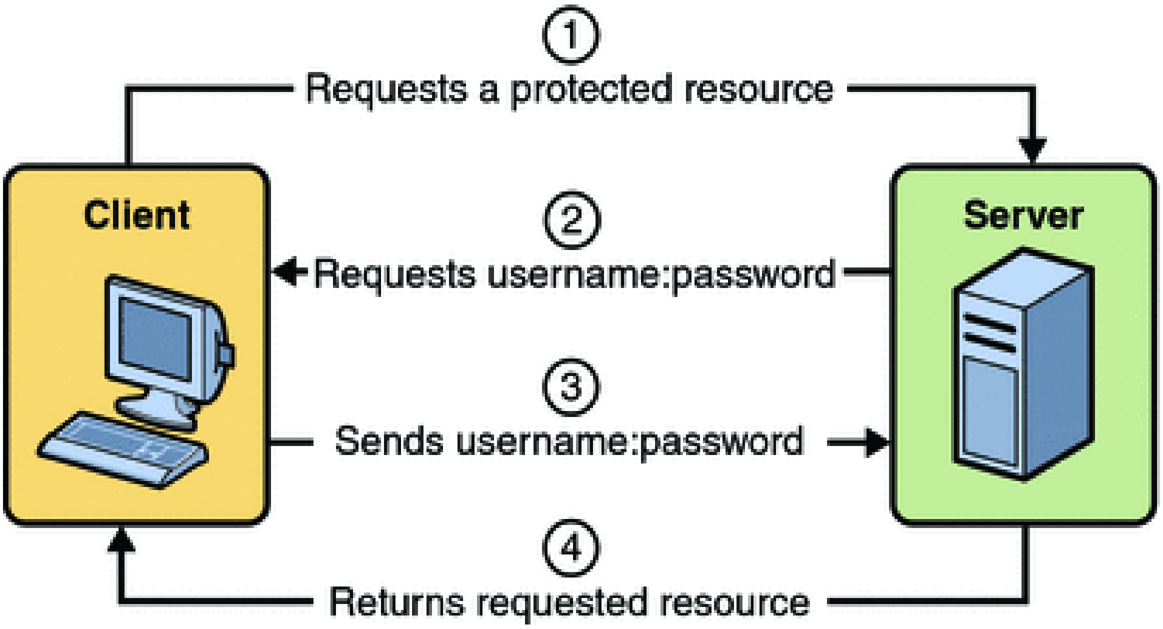

1
Requests a protected resource
Client
Server
2
Requests username:password
3
Sends username:password
4
Returns requested resource

Figure 1: Secure access to a protected resource

First of all, client makes a request to server in order to obtain a protected resource. The server will ask the user to enter user name and password. Accordingly client enters user id and password and sends to server. Then the server performs something known asauthentication. If the user is genuine the authentication is successful and the user is provided access to requested resource. This is the traditional mechanism being used.

Many researchers [2], [5], [8]-[10] contributed to have secure mechanisms in communication networks and applications. However, there is need for improving authentication mechanisms as it is an open problem to be addressed. In this paper we proposed a protocol which makes use of two servers and helps users split password into two partial shares and store in two servers. These two servers provide perfect cooperation while checking credentials. There is mechanism for key exchange and password authentication. This protocol is illustrated in Figure 2. The remainder of the paper is structured as follows. Section II provides review of literature. Section III explores the proposed protocol. Section IV presents implementation details and results. Section V concludes the paper and provides directions for future work.

RELATED WORKS

This section provides review of literature on password based security mechanisms. Password based authentication process of first introduced in [1] where two parties can have key exchange mechanism using cryptographic primitives. Such mechanisms need to have robust securityagainst dictionary attacks. Adversaries can try both online and offline dictionaries in order to gain access to resources with respect to password based authentication. That is the reason, it is important to provide strong passwords. Online dictionary attacks can be prevented with cryptographic means. It is also possible to set limit to number of attempts.

With respect to such mechanisms there are two possible settings such as single server authentication and multi-server authentication. Again single server approaches are of three types namely password only PAKE, PKI-based PAKE, and identity based PAKE. Formal model of PAKE security are explored in [2]-[11]. In [12] PKI based approaches are explored where client stores public key of server and share a password with the server. PKI based PAKE and security proofs are explored in [13]. ID based PAKE and its utility in the world are studied in [14] and [15]. Here client needs to remember password and also remember id of server. Server has its own private key and stores client's identities. The trade-offs between PKI based PAKE and password only PAKE can be reflected in ID-based PAKE.

In case of single setting servers, all security keys are stored in a single server. When such server is compromised, it is possible that security is lost. For instance in Kerberos [16] all keys are stored in one server only which is not highly secure. Multi-server PAKE is therefore given importance in [17] and [18]. In this case password is distributed across multiple networked servers in a distributed environment.

Again this kind of PAKE can be divided into two kinds. They are PKI-based threshold PAKE and Two server PAKE. The former is presented in [17] where n number of servers is used for password authentication. The advantage of this kind of protocol is that as long as n-1 or fewer servers are compromised, the protocol is still secure. Password-only kind of setting is studied in [18] and [19]. The two server PAKE is first introduced in [20] where two server machines cooperate each other for client authentication. Even if one server is compromised, the password remains secure. Later on a variant of this protocol was studied in [21]. It was a password-only PAKE with two servers. Katz et al. [22] proposed a two server approach in which two servers symmetrically cooperate in authentication mechanism. Similar protocols were introduced in [23], [24], [25] and [26]. In all these settings, front end server will interact with backend in order to authenticate users.

Many such protocols are asymmetric in nature. Many are asymmetric in nature and need different keys in order to perform their operations. However, in [27] more efficient protocol was presented when compared with its predecessors. In [28] ID2S PAKE was introduced and the IBE is done in [28]. In this paper we make use of IBE and IBS in order to achieve high level of security.

PROPOSED SYSTEM

In this paper, we proposed a protocol which involves three roles for authentication process to be completed. The roles include user, server A and server B. User has a resource which needs to be protected with password. The password is generated with two partial shares and they are stored in two different servers. These servers cooperate and help in generating credentials correctly to support authentication. The protocol is known a password-authentication key exchange protocol. The protocol works as per the illustration provided in Figure 2.

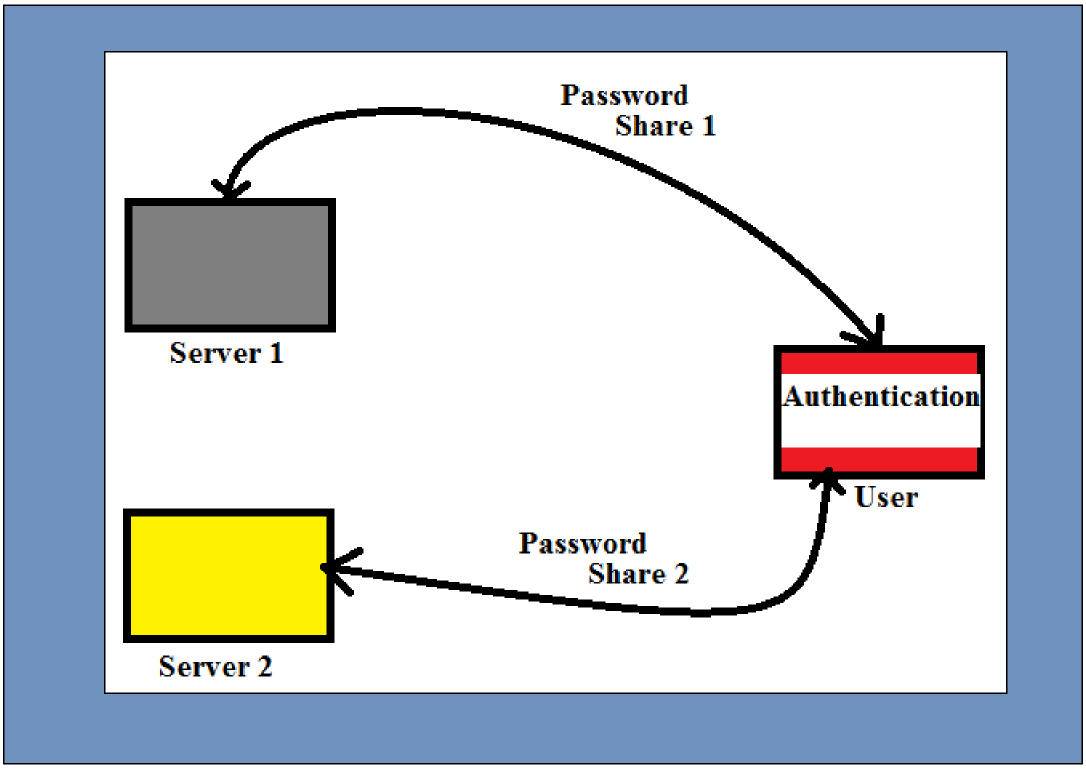
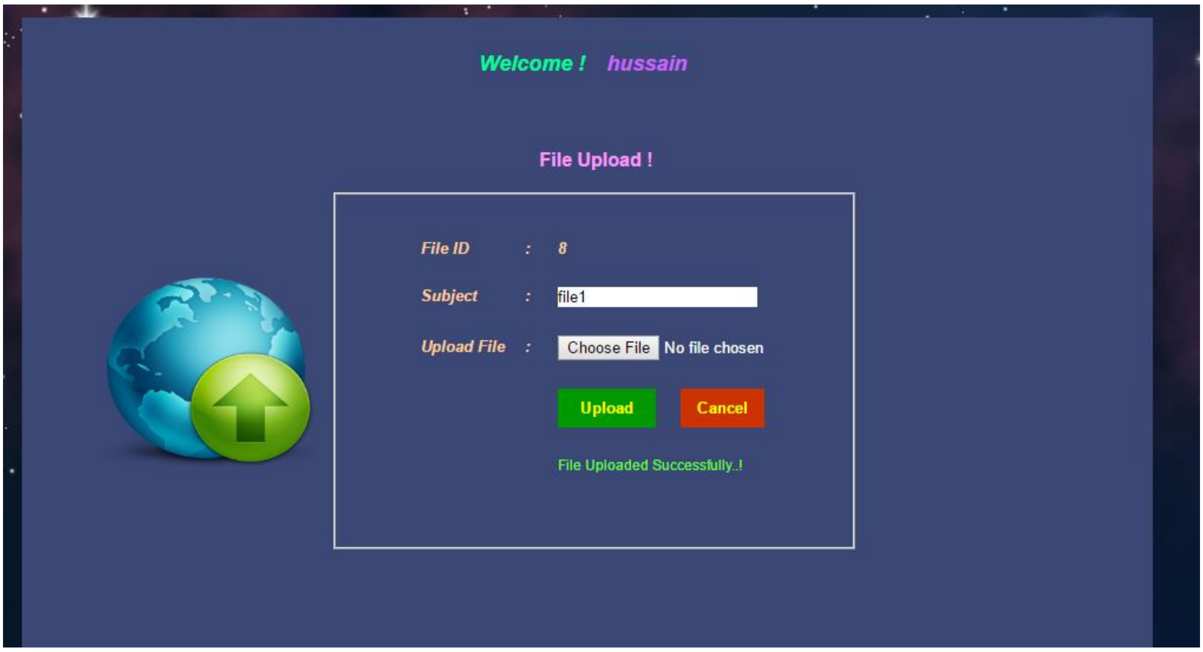


Figure 2: Password-authentication key exchange protocol

As shown in Figure 2, it is evident that user has resources that need to be protected. The user can protect resources by setting password. The important observation in the proposed system is that the password is divided into two partial shared and stored in two different servers for security reasons. The two servers and the client program work in coordination in order to have a successful password-authenticated key exchange protocol.

IMPLEMENTATION AND RESULTS

The proposed system is implemented using Microsoft.NET platform. Visual Studio is the development environment used. C# programming is used to provide functionality while ASP.NET is used for designing web based application. ADO.NET is used to perform database operations programmatically. The proposed protocol involves different activities such as file upload, sharing data, and viewing shared data subjected to password authentication. There are two roles involved. They are client and server. The clients can upload a file, share it and view shared files. The server can view client requests, and perform key verification process.



Welcome ! hussain

File Upload !

File ID : 8

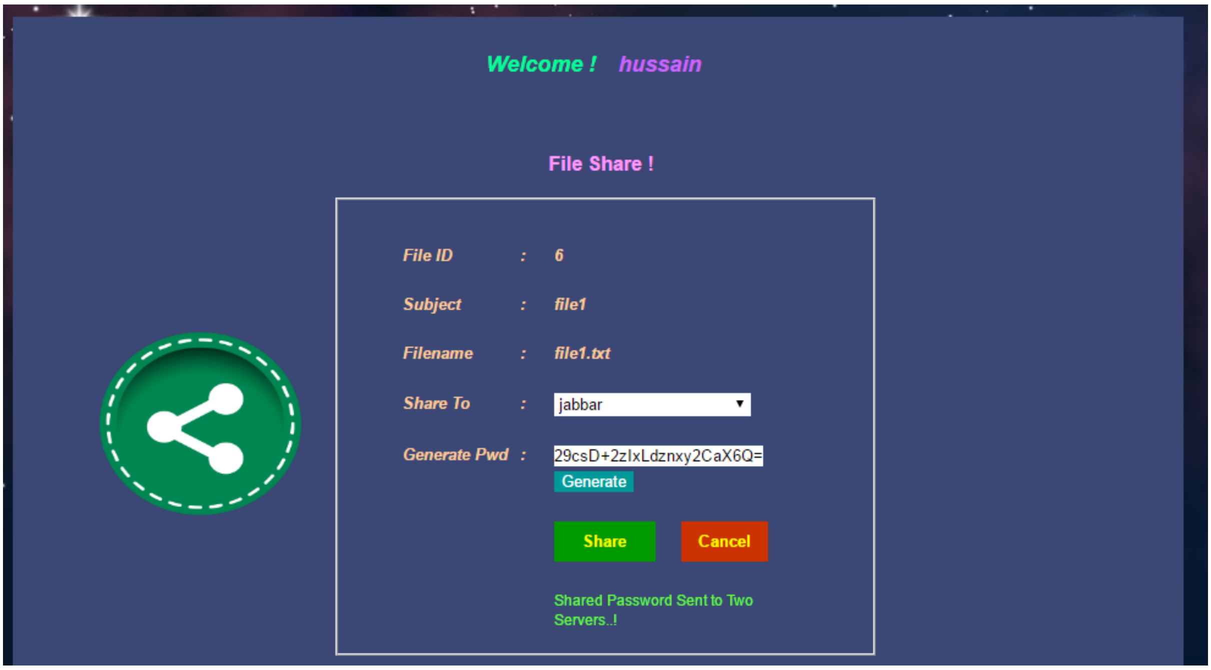
Subject : file1

Upload File : No file chosen

File Uploaded Successfully..!

Figure 3: File uploads operation

As can be seen in Figure 3, it is evident that files can be uploaded by client. The uploaded files can be shared and shared files can be viewed by clients. File sharing is done to provide access to files to other registered users. File sharing needs to generate password that can be used later in order to access file.



Welcome ! hussain

File Share !

File ID : 6

Subject : file1

Filename : file1.txt

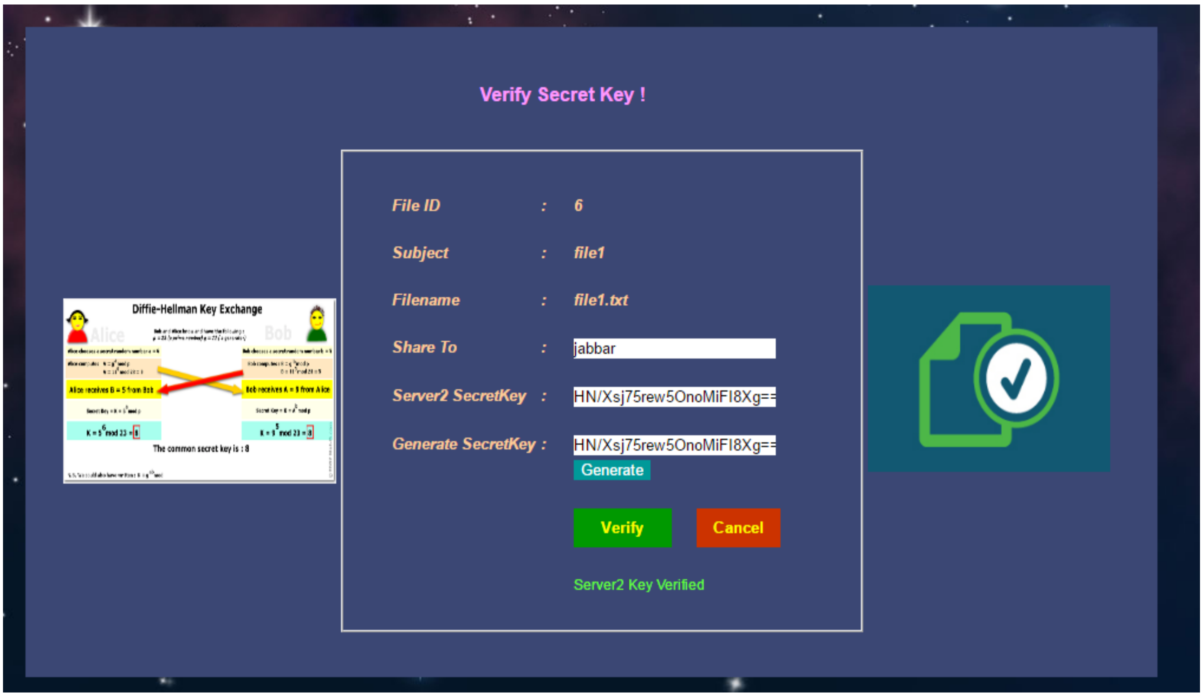
Share To : jabbar

Generate Pwd : 29csD+2zIxLdznxy2CaX6Q=

Shared Password Sent to Two Servers..!

Figure 4: Generates password and allows sharing of file

As shown in Figure 4, it is evident that the file is shared to a user and password is associated with the user and file. Once the file is shared to another user, the generated password needs to be used in order to access the file according to the password-authenticated protocol implemented in this paper. The generated secret key and exchanges it to corresponding user thus the user can access the file anytime. The secret key generation and storage process may be done by multiple servers involved.



Verify Secret Key !

File ID : 6

Subject : file1

Filename : file1.txt

Share To : jabbar

Server2 SecretKey : HN/Xsj75rew5OnoMiFI8Xg==

Generate SecretKey : HN/Xsj75rew5OnoMiFI8Xg==

Server2 Key Verified

Figure 5: Key verification done by server

As can be seen in Figure 5, the generated secret key and server 1 secret key for the given file shared to given user is verified successfully. Once the verification process is carried out, it does mean that the file can be accessed by the intended user with permissions provided in the process of password authentication protocol.

Role	Execution Time (s)		
	Katz et al.	lbs-based	lbe-based
Client	1.26	5.26	7.08
Server A	5.31	4.14	2.08
Server B	5.31	3.82	1.76

Table 1: Execution time taken for client, server A and server B

As shown in Table 1, it is evident that the execution time of the client, server A and server B is observed and presented. The results revealed that the lbe-based protocol consumes less time for server A and server B while Katz et al.'s protocol takes least time for client.

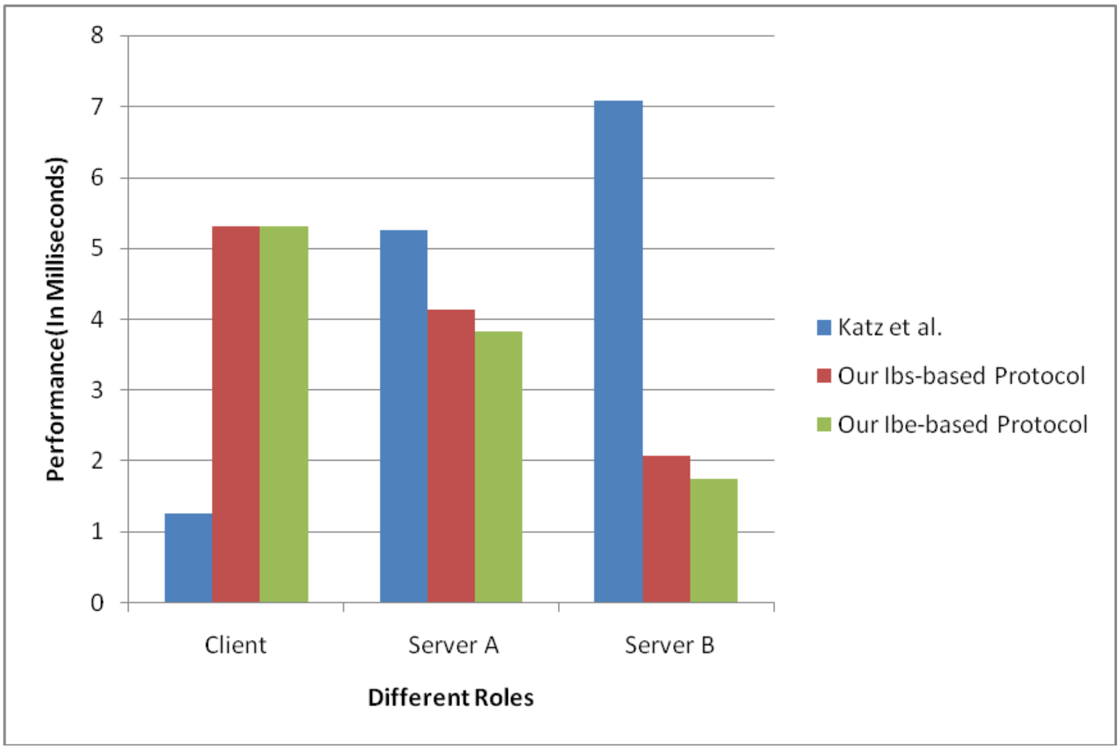


Figure 6: Performance comparison

As shown in Figure 6, it is evident that the execution time of the client, server A and server B is observed and presented. The results revealed that the lbe-based protocol consumes less time for server A and server B while Katz et al.'s protocol takes least time for client. More time is consumed by Katz et al.'s protocol with respect to server B. The least execution time is exhibited by lbe-based protocol with respect to server B.

CONCLUSIONS AND FUTURE WORK

In this paper we studied the concept of password based authentication systems. From the literature, it is found that there are many schemes that existed to have secure communications. However, the general way of authentication is that server demands for credentials and client provides them. In this paper, we proposed a protocol that does differently. The protocol takes password and divides it into two partial shares. The shares are stored in two different servers. Even one server is compromised;

the security is not lost as both servers need to work with cooperation to authenticate users. This kind of approach provides more security to systems and communications in networks. We built a prototype application to demonstrate the proof of the concept. The results revealed that the proposed system is able to show the utility of the protocol. This research can be extended further to have more sophisticated mechanism with multiple servers participating in the password-authenticated key exchange.

REFERENCES

[1] S. M. Bellovin and M. Merritt. Encrypted key exchange: Passwordbased protocol secure against dictionary attack. In Proc. 1992 IEEE Symposium on Researchin Security and Privacy, pages 72-84, 1992.

[2] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Proc. Eurocrypt'00, pages 139-155, 2000.

[3] V. Boyko, P. Mackenzie, and S. Patel. Provably secure passwordauthenticated key exchange using Diffie-Hellman. In Proc. Eurocrypt'00, pages 156-171, 2000.

[4] 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.

[5] M. Abdalla and D. Pointcheval. Simple password-based encrypted key exchange protocols. In Proc. CT-RSA 2005, pages 191-208, 2005.

[6] J. Bender, M. Fischlin, and D. Kugler. Security analysis of the PACE key-agreement protocol. In Proc. ISC'09, pages 33-48, 2009.

[7] E. Bresson, O. Chevassut, and D. Pointcheval. Security proofs for an efficient password-based key exchange. In Proc. CCS'03, pages 241-250, 2003.

[8] E. Bresson, O. Chevassut, and D. Pointcheval. New security results on encrypted key exchange. In Proc. PKC'04, pages 145-158, 2004.

[9] O. Goldreich and Y. Lindell. Session-key generation using human passwords only. In Proc. Crypto'01, pages 408-432, 2001.

[10] S. Jiang and G. Gong. Password based key exchange with mutual authentication. In Proc. SAC'04, pages 267-279, 2004.

[11] J. Katz, R. Ostrovsky, and M. Yung. Efficient passwordauthenticated key exchange using human-memorable passwords. In Proc. Eurocrypt'01, pages 457-494, 2001.

[12] L. Gong, T. M. A. Lomas, R. M. Needham, and J. H. Saltzer. Protecting poorly-chosen secret from guessing attacks. IEEE J. on Selected Areas in Communications, 11(5):648-656, 1993.

[13] S. Halevi and H. Krawczyk. Public-key cryptography and password protocols. ACM Transactions on Information and System Security, 2(3):230-268, 1999.

[14] X. Yi, R. Tso and E. Okamoto. ID-based group passwordauthenticated key exchange. In Proc. IWSEC'09, pages 192-211, 2009.

[15] X. Yi, R. Tso and E. Okamoto. Identity-based passwordauthenticated key exchange for client/server model. In SECRYPT'12, pages 45-54, 2012.

[16] B. Clifford Neuman and Theodore Ts'o. Kerberos: An authentication service for computer networks. IEEE Communications, 32 (9): 33-38, 1994.

[17] W. Ford and B. S. Kaliski. Server-assisted generation of a strong secret from a password. In Proc. 5th IEEE Intl. Workshop on Enterprise Security, 2000.

[18] D. Jablon. Password authentication using multiple servers. In Proc. CT-RSA'01, pages 344-360, 2001.

[19] M. Di Raimondo and R. Gennaro. Provably Secure Threshold Password-Authenticated Key Exchange. J. Computer and System Sciences, 72(6): 978-1001 (2006).

[20] 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.

[21] M. Szydlo and B. Kaliski. Proofs for two-server password authentication. In Proc. CT-RSA'05, pages 227-244, 2005.

[22] J. Katz, P. MacKenzie, G. Taban, and V. Gligor. Two-server password-only authenticated key exchange. In Proc. ACNS'05, pages 1-16, 2005.

[23] H. Jin, D. S. Wong, and Y. Xu. An efficient password-only twoserver authenticated key exchange system. In Proc. ICICS'07, pages 44-56,2007

[24] Y. Yang, F. Bao, R. H. Deng. A new architecture for authentication and key exchange using password for federated enterprise. In Proc. SEC'05, pages 95-111, 2005.

[25] 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, 3(2), 105-114, 2006.

[26] Y. Yang, R. H. Deng, and F. Bao. Fortifying password authentication in integrated healthcare delivery systems. In Proc. ASIACCS'06, pages 255-265,2006.

[27] 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.

[28] X. Yi, F. Hao and E. Bertino. ID-based two-server passwordauthenticated key exchange. In ESORICS'14, pages 257-276, 2014