ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

Various Multi-Server PAKE Protocols in Key Exchange

Shafnamol.N, Simi Krishna.K.R

M. Tech Scholar, Department of Information Technology, Government Engineering College, Barton Hill, India

Assistant Professor, Department of Information Technology, Government Engineering College, Barton Hill, India

ABSTRACT: 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 other words they use password to authenticate, that is Password-authenticated key exchange (PAKE). Typical protocols for password-based authentication assume a single server which stores all the information (e.g., the password) necessary to authenticate a user. Unfortunately, an inherent limitation of this approach (assuming low-entropy passwords are used) is that the user's password is exposed if this server is ever compromised. To address this issue, it has been suggested to share a user's password information among multiple servers, and to have these servers cooperate when the user wants to authenticate.

This paper presents a study on multi-server PAKE protocols, different types and comparison of them.

KEYWORDS*:* PAKE protocol,ID-Based Encryption,password

I. INTRODUCTION

To secure communication between two parties, an authenticated encryption key is required to agree on in advance. In a key exchange (KE) (or agreement) protocol, two parties (usually referred to as the client and the server), run a protocol which terminates with them agreeing on a common random value which is secret to any other party in the network. Such random value can then be used as a key to encrypt and authenticate the communication in the session. In the basic version of this protocol the adversary is supposed to be passive, i.e., limited to eavesdropping. In other words, the communication channels connecting parties are assumed to be authentic, i.e., guarantee that messages received have not been modified. A more realistic setting is the one of non-authentic channels, where the adversary may modify messages sent between honest parties. In this case an authenticated key exchange protocol (AKE) must also guarantee the identity of the two parties taking place. In a password-authenticated key exchange (PAKE) protocol, this guarantee is built upon the fact that the two parties share a secret (humanly-memorizable) password.

In general, there exist two kinds of PAKE settings, one assumes that the password of the client is stored in a single server and another assumes that the password of the client is distributed in multiple servers. In the single-server 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. To address this problem, the multi-server setting for PAKE was proposed, where the password of the client is distributed in n servers. PAKE protocols in the multi-server setting can be classified into two categories: Threshold PAKE, where n severs sharing the password of the client, cooperate to authenticate the client and establish independent session keys with the client and two-server PAKE where two servers cooperate to authenticate the client and the password remains secure if one server is compromised.

This paper presents a brief description of multi-server PAKE protocols. Section II discusses about different types of PAKE protocols. Section III does a comparison of different multi-server PAKE protocols.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

II. MULTI-SERVER PAKE PROTOCOLS

PAKE protocols in the multi-server setting can be classified into two categories as follows.

Two-server PAKE: A two-server password-only PAKE protocol was given by Katz [1],which is built upon the two-party PAKE protocol (i.e., the KOY protocol [2]), where two parties, who share a password, exchange messages to establish a common secret key. Their basic two-server protocol is secure against a passive (i.e., honest-but-curious) adversary who has access to one of the servers throughout the protocol execution, but cannot cause this server to deviate from its prescribed behavior. In [23], Katz et al. also showed how to modify their basic protocol so as to achieve security against an active adversary who may cause a corrupted server to deviate arbitrarily from the protocol. The core of their protocol is the KOY protocol. The client looks like running two KOY protocols with two servers in parallel.However, each server must perform a total of roughly 80 exponentiations (i.e., each servers work is increased by a factor of roughly 6 as compared to the basic protocol [2]).

Another protocol was given by Yi et al.[3]which propose a new compiler to construct a two-server PAKE protocol with any two-party PAKE protocol.This compiler employs the two-party PAKE protocol between two servers when they authenticate the client. To achieve the goal,this compiler adds an identity-based encryption (IBE)[4] scheme to protect the messages (containing the password information) from the client to the two servers. The basic idea is: first of all, 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. In key exchange, the client sends to each server one share of the password encrypted according to the identity of the server. From the client messages, 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.This compiler also needs a public key encryption scheme for the servers to protect the messages (containing the password information) from the servers to the client. 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 an IBE scheme, the decryption 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.Using standard techniques from threshold cryptography, the PKG can be distributed so that the master-key is never available in a single location. In order to prevent a malicious PKG from decrypting the password information encrypted with the identity of a server, a strategy is to employ multiple PKGs which cooperate to generate the decryption key for the server. As long as one of the PKGs is honest to follow the protocol, the decryption key for the server is known only to the server. Since it can assume that the two servers in two-server PAKE never collude, it can also assume that at least one of the PKGs do not collude with other PKGs.

Recently, Yi et al. constructed an ID2S PAKE protocol[5] with the Identity-based signature scheme.It propose a new compiler for ID2S PAKE protocol based on any identitybased signature scheme (IBS). 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. If the signature is genuine, the client submits to the server one share of the password encrypted with the public key of the server. 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, it generalize the compiler based on IBE in [3] by replacing the Cramer-Shoup public key encryption scheme with any public key encryption scheme. 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. 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. 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.

Threshold PAKE:Here n severs, sharing the password of the client, cooperate to authenticate the client and establish independent session keys with the client. As long as n - 1 or fewer servers are compromised, their protocol remains secure.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

Di Raimondo and Gennaro [6] suggested the first threshold protocols for password authentication which are provably secure in the standard model.This line of research can be thought as applying the tools of threshold cryptography to the problem of password authentication. Threshold cryptography aims at the protection of cryptographic secrets, such as keys, by distributing them across several servers in order to tolerate break-ins.Here the password is shared among a set of n servers so that t of them co-ordinate to authenticate the client.So the adversary can learn the password only by breaking into t+1 of them.It proposes two protocols:Transparent and Non-transparent protocols.In transparent protocol,the client is not aware that at the server's side the protocol has been implemented in a distributed fashion, nor should he know how many servers are involved. The client interacts with a gateway server which to the client's eyes will be the authentication server. At the end the secret key will be shared between the client and the gateway.To the eyes of the client the protocol should look exactly like a centralized KOY protocol. All the messages exchanged by the client and the gateway will follow the pattern of a regular KOY protocol.

In Non-transparent protocol,the client is aware of the distributed implementation of the servers and in particular of the number n of servers.At the end of this protocol the client will establish n separate keys, one with each server. The adversary will only learn the keys established by the corrupted servers.Here the client will basically run n copies of the KOY protocol, one with each server. The servers will cooperate to compute together the answers of the ith server in the ith execution of the KOY protocol.

III. PAKE PROTOCOLS:A COMPARISON

In terms of the setting and the client performance, the Katz et al.s protocol[1] is superior to ID2S protocols[5].In the Katz et al.s protocol, each server performs approximately six times the amount of the work as the KOY protocol, whereas in ID2S 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).A comparison between Katz' and ID2S scheme is shown in table TABLE1.

In IBS-based protocol, if we use the KOY two-party PAKE protocol [2], the Paterson et al.s IBS scheme and the CramerShoup public key encryption scheme as cryptographic building blocks, the performance of IBS-based protocol can be shown in TABLE 1. In IBE-based protocol, if we use the KOY two-party PAKE protocol [2], the Waters IBE scheme [4] and the Cramer- Shoup public key encryption scheme as cryptographic building blocks, the performance of

TABLE I
COMPARISON OF MULTI-SERVER PAKE PROTOCOLS

factors	Katz et al. Protocol [1]	IBS-based Protocol[5]	IBE-based Protocol[3]
Public Keys	Client: None Sever A: Public Key pkA Sever B: Public Key pkB	Client: None Server A: A Server B:B	Client: None Server A: A Server B:B
Private Keys	Client: pw_C Sever A: $pw_{C,A}$, Private Key sk_A Sever B: $g^{pw_{C,B}}$, Private Key sk_B	Client:pw_C Server A:$g^{pw_{C,A}}$, d_A Server B: $g^{pw_{C,B}}$,d_B	Client: pw_C Server A: $G^{pw_{C,A}}$, $g^{pw^*_{C,A}}$,d_B Server B: $G^{pw_{C,B}}$; $g^{pw^*_{C,B}}$,d_B
Computation Complexity	Client: 21(exp.)+1(Sign) Server: about 6(KOY)	Client: 23(Exp.)+6(Pair) Server: about 1(KOY)+9(Exp)	Client: 23(Exp.) Server:about 1(KOY)+2(Pair)+9(Exp.)
Communication Complexity	Client/Server: 27(exp.)+1(Sign) Server/Server: about 2(KOY)	Client/Server: 22(Exp.) Server/Server: about 1(KOY)	Client/Server: 24(Exp.) Server/Server: about 1(KOY)

IBE-based protocol can also be shown in TABLE 1. In addition,the comparison of protocols with the Katz et al. two-server PAKE protocol[2] in TABLE 1. In TABLE 1, Exp., exp. Sign. and Pair for computation represent the computation complexities of a modular exponentiation over an elliptic curve, a modular exponentiation over Zp, a signature generation and a pairing, respectively, and Exp., exp. and Sign. in communication denote the size of the modulus and the size of the signature, and KOY stands for the computation or communication complexity of the KOY protocol.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

Threshold PAKE protocols[6] provide higher layer of security. Since the adversary need to compromise t+1 of the servers to learn the password. In the case of the client, transparent protocol is exactly the same as the KOY protocol, so there is no efficiency loss for the transparent protocol. The non-transparent protocol will cost to the client n times as much as the execution of a single KOY protocol. For the servers the cost is higher, but still reasonable. In the case of the first protocol the cost for each server is 2n times the cost of a single KOY protocol. Again in the case of second protocol there is an extra factor of n bringing the total cost 2n2 times higher than the KOY protocol

IV. CONCLUSION

This is the review of different types of PAKE protocols that are in existence. The comparison based on their performance helps to suit for the respective applications. Adding IBE scheme to the threshold PAKE protocol can be considered as a future work.

REFERENCES

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

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

[3] X.Yi,F.Hao and E.Bertino."ID-based two-server password authenticated key exchange". In *ESORICS'14*, pages 257-276, 2014

[4] B.Waters."Efficient identity-based encryption without random oracles".In *Proc. Eurocrypt'05*,pages 114-127, 2005.

[5] X.Yi,F.Rao,Z.Tari,F.Hao,E.Bertino,I.Khalil, and A.Y.Zomaya."ID2S Password-Authenticated Key Exchange Protocols" in *IEEE Transactions on Computers* , vol. 65, no. 12, pp. 3687-3701,2016.

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