International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 25-29
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

PREVENT DICTINORY ATTACK USING SECURE PASSWORD AUTHENTICATED KEY AGREEMENT

S. Arthi, S. Saranya, E. Monika Selas
UG Scholar,
Manakula Vinayagar Institute of Technology, Puducherry

D.Nagamany Abirami
Assistant Professor,
Manakula Vinayagar Institute of Technology, Puducherry

***Abstract*— Most password-based user authentication systems place total trust on the authentication server where clear text passwords or easily derived password verification data are stored in a central database. Such systems are not resilient against offline dictionary attacks initiated at the server side. To secure communications between two parties, an authenticated encryption key is required to agree on in advance. In this paper, we present secure password-authenticated key agreement protocol (SPAKA) with two server, the client and server share a password, which is used to achieve mutual assurance that a cryptographically strong session key is established privately by the two parties. To address the problem of weak passwords, SPAKA protocols are constructed so as to leak no password information, even in the presence of an active attacker. Many roaming-credentials proposals involve use of a SPAKA protocol as a leverage point for obtaining credentials, or as a freestanding authentication protocol.**

Keywords: Password-authenticated key exchange, identity-based encryption and signature, Diffie-Hellman key exchange, decisional Diffie-Hellman problem

I. INTRODUCTION

To secure communications between two parties, anthenticated encryption key is required to agree on in advance. So far, two models have existed for authenticated key exchange. One model assumes that two parties already share some cryptographically-strong information: either a secret key which can be used for encryption/authentication of messages, or a public key which can be used for encryption/signing of messages. These keys are random and hard to remember. In practice, a user often keeps his keys in
a personal device protected by a password/PIN. Another model assumes that users, without help of personal devices, are only capable of storing "human-memorable" passwords. Bellovin and Merritt [1] were the first to introduce password-based authenticated key exchange (PAKE), where two parties, based only on their knowledge of a password, establish a cryptographic key by exchange of messages. A PAKE protocol has to be immune to on-line and off-line dictionary attacks. In an off-line dictionary attack, an adversary exhaustively tries all possible passwords in a dictionary in order to determine the password of the client on the basis of the exchanged messages. In on-line dictionary attack, an adversary simply attempts to login repeatedly, trying each possible password. By cryptographic means only, none of PAKE protocols can prevent on-line dictionary attacks. But on-line attacks can be stopped simply by setting a threshold
to the number of login failures.

Password-only PAKE: Typical examples are the "encrypted key exchange" (EKE) protocols given by Bellovin and Merritt, where two parties [1], who share a password, exchange messages encrypted by the password, and establish a common secret key. The formal model of security for PAKE was firstly given in [2] [3]. Based on the security model, PAKE protocols have been proposed and proved to be secure.

PKI-based PAKE: PKI-based PAKE protocol was first given by Gong et al. [4] , where the client stores the server's public key in addition to share a password with the server.
Halevi and Krawczyk [5] were the first to provide formal definitions and rigorous proofs of security for PKI-based PAKE.

ID-based PAKE: ID-based PAKE protocols were proposed by Yi et al. [6] [7] where the client needs to remember a password in addition to the identity of the server, whereas
the server keeps the password in addition to a private key related to its identity. ID-based PAKE can be thought as a trade-off between password-only and PKI-based PAKE.

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 25-29
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

II. LITERATURE SURVEY

A literature review is an account of what has been published on a topic by accredited scholars and researchers. Occasionally we will be asked to write one as a separate assignment, but more often it is part of the introduction to an essay, research report, or thesis. In writing the literature review, our purpose is to convey to our reader what knowledge and ideas have been established on a topic, and what their strengths and weaknesses are. As a piece of writing, the literature review must be defined by a guiding concept (e.g., your research objective, the problem or issue we are discussing or our argumentative thesis). It is not just a descriptive list of the material available, or a set of summaries. Besides enlarging our knowledge about the topic, writing a literature review lets we gain and demonstrate skills in two areas:

1. INFORMATION SEEKING: the ability to scan the literature efficiently, using manual or computerized methods, to identify a set of useful articles and books
2. CRITICAL APPRAISAL: the ability to apply principles analysis to identify unbiased and valid studies.

PASSWORD-BASED PROTOCOLS SECURE AGAINST DICTIONARY ATTACKS [1]

Classic cryptographic protocols based on user-chosen keys allow an attacker to mount password-guessing attacks. A combination of asymmetric (public-key) and symmetric (secret-key) cryptography that allow two parties sharing a common password to exchange confidential and authenticated information over an insecure network is introduced. In particular, a protocol relying on the counter-intuitive motion of using a secret key to encrypt a public key is presented. Such protocols are secure against active attacks, and have the property that the password is protected against offline dictionary attacks.

SECURE DATA EXCHANGE USING AUTHENTICATED CIPHERTEXT-POLICY ATTRIBUTED- BASED ENCRYPTION [8]

Easy sharing files in public network that is intended only for certain people often resulting in the leaking of sharing folders or files and able to be read also by others who are not authorized. Secure data is one of the most challenging issues in data sharing systems. Here, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a reliable asymmetric encryption mechanism which deals with secure data and used for data encryption. It is not necessary encrypted to one particular user, but recipient is only able to decrypt if and only if the attribute set of his private key match with the specified policy in the ciphertext. In this paper, we propose a secure data exchange using CP-ABE with authentication feature. The data is attribute-based encrypted to satisfy confidentiality feature and authenticated to satisfy data authentication simultaneously.

SOME REMARKS ON PROTECTING WEAK KEYS AND POORLY-CHOSEN SECRETS FROM GUESSING ATTACKS[9]

Authentication and key distribution protocols that utilize weak secrets (such as passwords and personal identification numbers) are traditionally susceptible to guessing attacks whereby an adversary iterates through a relatively small key space and verifies the correct guess. Such attacks can be defeated by the use of public key encryption and careful protocol construction. T. Lomas et al. (Proc. of ACM Symp. on Operating Syst. Principles, 1989) investigated this topic and developed a methodology for avoiding guessing attacks while incurring only moderate overhead. Several issues concerning the proposed solution are discussed here, and modifications that remove some of the constraints (such as synchronized time and state retention by the server) and result in simpler and more efficient protocols are suggested.

EFFICIENT TWO-SERVER PASSWORD-ONLY AUTHENTICATED KEY EXCHANGE [10]

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.

III. EXISTING SYSTEM

In the single-server setting [11], 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. This is also true to Kerberos, where a user authenticates against the authentication server with his username and password and obtains a token to authenticate against the service server. PAKE protocols in the single-server setting can be classified into three

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 25-29
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

categories as follows[12]: Password-only PAKE, PKI-based and PAKE ID-based PAKE

DRAW BACKS OF EXISTING SYSTEM

1. In PAKE, where two parties, based only on their knowledge of a password, establish a cryptographic key by exchange of messages.
2. A PAKE protocol has to be immune to on-line and off-line dictionary attacks.
3. In an off-line dictionary attack, an adversary exhaustively tries all possible passwords in a dictionary in order to determine the password of the client on the basis of the exchanged messages.
4. In on-line dictionary attack, an adversary simply attempts to login repeatedly, trying each possible password.
5. None of PAKE protocols can prevent on-line dictionary attacks.

IV. PROPOSED SYSTEM

We propose a new compiler for ID2S PAKE protocol based on any identity-based signature scheme (IBS), such as the Paterson et al.'s scheme [13]. 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.

ALGORITHM :

C1 The i-th client,i=1,2…..,n
S The trusted server
P1 The password shared between c1 and s
P,q Two large primes with p=2q+1
G,g The subgroup of order q in z*p and its generator, respectively
H(*) A secure hash function mapping{0,1}*to{0,1}len
K t,BKt1 The secrete key and blinded key for client

C1,i=1,2,…n
(l,v) The v-th node at the l-th level on the binary key tree (Fig.1)
K(l,v),BK(l,v) The secret key and blinded key fo5r node(l,v)
Ski The session key shared between C1 and Ci+1,i=1,2……,n-1.

SPAKA (secure password-authenticated key agreement) is a basic tool for mutual authentication via passwords. The client and server share a password, which is used to achieve mutual assurance that a cryptographically strong session key is established privately by the two parties. To address the problem of weak passwords, SPAKA protocols are constructed so as to leak no password information, even in the presence of an active attacker.

When used as a means of authentication to obtain credentials from a trusted server, a SPAKA protocol is typically supplemented with a throttling or lockout mechanism to prevent on-line guessing attacks. Many roaming-credentials proposals involve use of a SPAKA protocol as a leverage point for obtaining credentials, or as a freestanding authentication protocol.

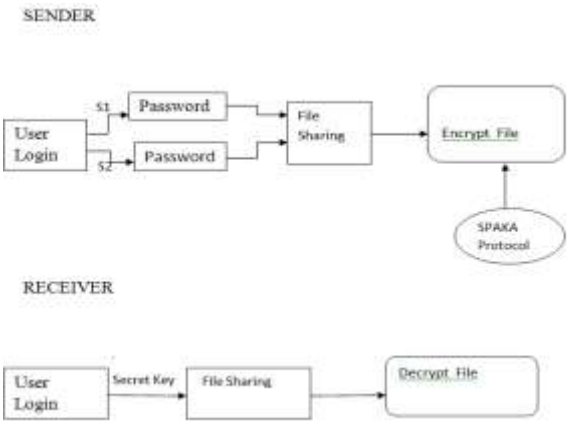


Figure 1: Encryption System

In Fig.1, System architecture is a conceptual model that defines the structure, behavior, 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 and behaviors of the system.

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.

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 25-29
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

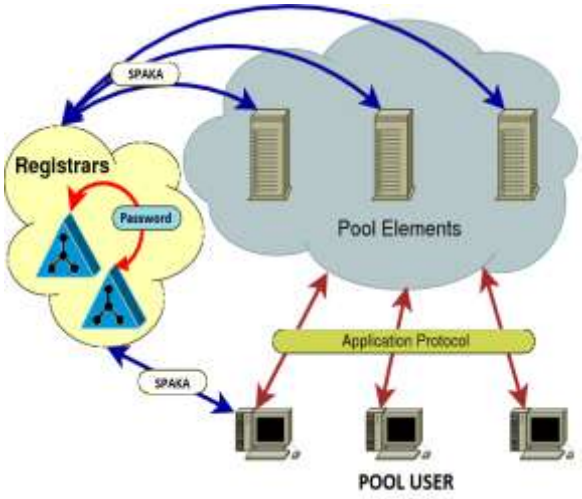


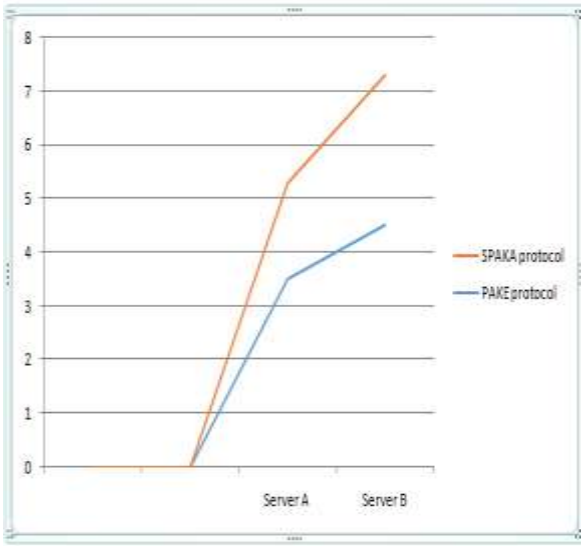
Figure 2: SPAKA Protocol

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 SPAKA protocol to authenticate the client.

In this paper, we propose a new compiler for ID2S PAKE protocol based on any identity-based 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, we generalize the compiler based on IBE in 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. As mentioned in
, using standard techniques from threshold cryptography, the PKG can be distributed so that the master-key is never available in a single location. Like , our strategy is to employ multiple PKGs which cooperate to generate the decryption key or the signing key for the server. As long as one of the PKGs is honest to follow the protocol, the decryption key or the signing key for the server is known only to the server. Since we can assume that the two servers in two-server PAKE never collude, we can also assume that at least one of the PKGs do not collude with other PKGs.

V. Experimental Analysis

The efficiency of the compiled protocols using our compilers depends on performance of the underlying protocols. In our IBS-based protocol, if we use the KOY twoparty PAKE protocol , the Paterson et al.'s IBS scheme and the Cramer-Shoup public key encryption scheme as cryptographic building blocks, the performance of our IBS-based protocol . In our IBE-based protocol, if we use the KOY two-party PAKE protocol , the Waters IBE scheme and the CramerShoup public key encryption scheme as cryptographic building blocks, the performance of our IBE-based protocol. In addition, we compare our protocols with the Katz et al. two-server PAKE protocol (secure against active adversary) .



In 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.

VI. CONCLUSION

In this paper, we presented two efficient compilers to transform any two-party PAKE protocol to an SPAKA protocols. Our system is a highly practical approach to the problem of secure authentication via weak secrets. By employing two servers the systems able to offer considerably more protection of sensitive user data than any single-server approach could permit. At the same time, the system architecture avoids many of the conceptual and design complexities of multi-server cryptographic protocols.

VII. FUTURE ENHANCEMENT

In this paper, we proposed SPAKA with two server s, a client splits its password and stores two shares of its password in the two servers, respectively, and the two servers then cooperate to authenticate the client without knowing the password of the client. In case one server is compromised by an adversary, the password of the client is required to remain secure. It also leaks no password information, even in the presence of an active attacker. When used as a means of authentication to obtain credentials from a trusted server, a SPAKA protocol is typically supplemented with a throttling or lockout mechanism to prevent on-line guessing attack.

VIII. REFERENCES

[1] S. M. Bellovin and M. Merritt. Encrypted key exchange: Passwordbased protocol secure against dictionary attack. In Proc. 1992 IEEE Symposium on Research in 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] 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.

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

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

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

[8] R. Cramer and V. Shoup. Secure Data Exchange Using Authenticated Ciphertext-Policy Attributed-Based Encryption In Proc. Crypto'98, pages 13-25, 1998.

[9] X. Yi, R. Tso and E. Okamoto Some Remarks On Protecting Weak Keys And Poorly-Chosen Secrets From Guessing Attacks. In SECRYPT'12, pages 45-54, 2012.

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

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

[12] 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.

[13] K. G. Paterson and J. C.N. Schuldt. Efficient identity-based signatures secure in the standard model. In ACISP'06, pages 207-222, 2006.