IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-6 E-ISSN: 2347-2693

A Review of Authenticated Key Exchange Protocol Using Random Key Selection with Minimum Space Complexity

Stuti Nathaniel[1*], Dr. Syed Imran Ali [2], Sujeet Singh[3]

[1,2,3] Department of computer Science, Sagar Institute Of Science & Technology Research , Bhopal

Available online at: www.ijcseonline.org

Received: May/21/2016 Revised: May/30/2016 Accepted: Jun/17/2016 Published: Jun/30/ 2016

***Abstract* — for the past decades, an extensive variety of cryptographic protocols have been suggested to resolve secure communication problems even in the occurrence of challenger. The assortment of this work varies from developing fundamental security primitives providing confidentiality and authenticity to solving more difficult, application-specific problems. With rapid developments in perimeters and potential of communications and information broadcasts, there is a rising require of authentication protocol. However, when these protocols are deployed in practice, a significant challenge is to ensure not just security but also privacy throughout these protocols's lifetime. As computer-based devices are more extensively used and the Internet is more globally accessible, new types of applications and new types of privacy threats are being introduced to password privacy in the context of authenticated key exchange (AKE). Especially, we show that AKE protocols provably meeting the existing formal definitions do not accomplish the anticipated level of password privacy when organized in the real world.**

***Index Terms* — Authenticated Key exchanges (AKE), Authentication, AMEA, minimum space complexity, Symmetric Key, attacks.**

1. INTRODUCTION

The introduction of formal definitions of security marked a turning point in cryptographic-protocol analysis, and has proved to be extremely beneficial in practice. Formal definitions are useful in their own right: they force precise specification of desired goals; enable comparisons between protocols meeting different notions of security; and offer guidance as to what protocols are appropriate to achieve a desired level of security when used as a building block of a larger system. Formal definitions have also made possible rigorous mathematical proofs of protocol security, and provide distributed system and network designers with increased confidence in real-world protocols that can be proven secure in this manner. A cryptographic protocol is a procedure carried out between two parties which are used to perform some safety measures undertaking. Characteristically cryptographic protocols make use of one, or more, cryptographic primitives and/or schemes. Secure communication problems pose challenges when two (or more) parties participate to complete predefined tasks in a certain desired secure way, even in the presence of adversaries. For the past two decades, to solve secure communication problems, cryptography has provided work by (1) establishing a concrete framework to formally define the adversarial model and security model, (2) designing and developing protocol constructions for the real world, and (3) guaranteeing these constructions satisfy the security model via rigorously driven proofs. Password-based authenticated key exchange protocols, however, are vulnerable to password guessing attacks [1] since users usually choose easy-to-remember passwords. While the approach of designing PAKE protocols with RSA is far from maturity and perfection. In 1997, Lucks presented a scheme called OKE (open key exchange) [2] which are based on RSA. It was later found to be insecure against a variant of *e*-residue attacks because of Mac Kenzie et al. [3]. Furthermore, the authors modified OKE and proposed the first secure RSA-based PAKE protocol SNAPI. Since SNAPI protocol required that the RSA public exponent should be a larger prime than RSA modular, it is not practical. Later, Zhang proposed PEKEP and CEKEP protocols [4], which allow using both large and small prime numbers as RSA public exponents. To resist the *e*-residue attack, PEKEP protocol needs multiple RSA encryptions, and it is not very efficient. In 2007, Park et al. presented another efficient RSA-EAKE protocol [5] which can resist the *e*-residue attack based on number-theoretic techniques.

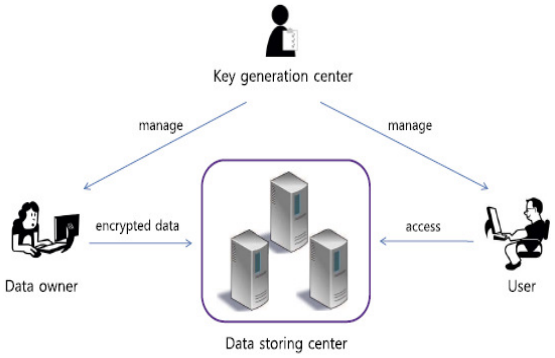

Fig 1. An Example of Data Sharing System

2. AUTHENTICATED KEY EXCHANGE PROTOCOLS

2.1 Key Exchange protocol: Authentication is impossible without sharing some information in advance. Perhaps the minimal such information that still provides a useful level of authentication is a short, easy-to-memorize password. Protocols for password-based authenticated key exchange (AKE) allow two entities who have shared a low-entropy password to ensure that they are communicating with each

© 2016, IJCSE All Rights Reserved

other (that is, to perform mutual authentication), as well as to establish a high-entropy (cryptographic) session key that can be used to encrypt and authenticate their subsequent communication. By this, users can communicate over a public unreliable channel and can agree a secure session key. As the password based authenticated key exchange protocols [6, 7] require users only to remember a human memorable (low-entropy) password, it is rather simple and efficient. Though password-based systems have their drawbacks — their security is inherently limited and this is only exacerbated by users' poor choice of passwords — their convenience (e.g., no special devices need to be carried by users) and ease of deployment (e.g., no public-key infrastructure to support use of public key primitives needed) seem to ensure their widespread use for the foreseeable future. Indeed, chances of large-scale deployment of AKE protocols are greatly enhanced by their recent IEEE standardization. Password-based authenticated key exchange allows two parties holding only short, human-memorable passwords to establish a secure session key of high-entropy when they share the same password. Such a key exchange is authenticated in a sense that it is secure against man-in-the-middle adversaries. While on-line attackers can guess a password with non-negligible probability, prevention of on-line attackers is straightforward with other mechanism (e.g., access block after consecutive log-in failures), it is not easy to prevent o?-line attacker from enumerating all possible passwords of small space into execution transcripts. Therefore, essentially, major security property of password-based authenticated key exchange is security against off-line dictionary attackers.

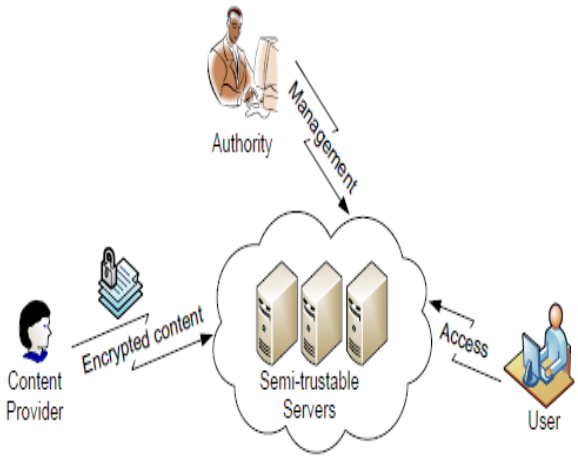

Fig 2. Scenario of secrete data sharing

2.2 General Description: Just like in key-agreement, password-based key exchange protocols (AKEs) allow two parties to allocate a key. The discrepancy is that the authentication of the entities involved in the exchange relies on passwords shared between clients and servers (thus reducing the dependence on a PKI). The challenge is to design protocols [6] that are secure against off-line dictionary attacks – attacks where adversaries infer information about the password only from the transcripts of protocol executions. The guarantee one wants is that an adversary cannot impersonate a user except if he successfully guesses a password.

2.3 Standardization Efforts: Definitions for AKE protocols are somewhat atypical in that they must explicitly take into account the fact that an adversary can "break" any protocol with "high" probability by either making a lucky guess of the correct password or by performing an on-line dictionary attack in which it repeatedly attempts to impersonate the client. There has been some standardization of AKE protocols. But these are usually relatively limited in terms of relevance regions, being attached to a definite submission, or have limited if any take up.

2.4 Limitations: security for AKE protocols are inadequate in that they do not match, nor do they provide any way to achieve, the level of security desired in practice. Specifically, these definitions bound the security of a protocol formally, the probability of an adversary's "breaking" the scheme as a function of the number of on-line attacks that occur, whereas in practice one would prefer an absolute bound on the security of the protocol independent of the number of on-line attempts. Despite their intuitive usefulness there has been little take up in the real world of AKE protocols. One reason, which is often mentioned for this, is the subsistence of a wide-ranging copyright on the EKE protocol. It may be useful to note that the patent on the EKE protocol expired in 2011.

3. THEORETICAL BACKGROUND

The primary objective of cryptography is to facilitate secure communication in a challenger situation. For example, if two parties, A and B, would like to safely communicate over an active open network, they would absolutely want to make clear in your mind that the data they correspond between themselves should remain private and authenticity of the data should be maintained. However, for this, there has to be a primitive cryptographic key agreement which contains both encryption and digital signature. With the help of such protocols carrying a common session key, two or more parties can exchange vital information over an adversely controlled and insecure network. These protected key agreement protocols act as the basic building block for accumulating secure, complicated, higher-level protocols. Key establishment is usually separated into key transport and key agreement section.

Secret keys offer message integrity and confidentiality where only trusted parties generally have copies of the secret key. However, in a global world of technological advancement, key distribution is a major problem from the security aspect. Basically, key establishment protocols need a set-up phase through which authentic and secret initial keying material is distributed. Most protocols are created with the objective of distinct keys on each protocol execution. In certain cases, the initial keying material pre-defines a fixed key which will result each time the protocol

© 2016, IJCSE All Rights Reserved

is implemented by a given pair or even a group of users. To improve secure key establishment, the ideal way in a key establishment protocol is to determine the true identity of the sender and receiver which can be possible by gaining access to the resulting key and restrict any additional unauthorized parties from extracting the same key. For a secure key establishment, secrecy of the key and identification of accessing parties are required. Additionally to the abovementioned come within reach of that are adapted to the password-based setting there continue living more than a few more wide-ranging authentication and key exchange frameworks [8, 9].

4. AUTHENTICATED KEY EXCHANGE

Authentication allows the authentication initiator to be convinced of the identity of the communicating object. The object can be human being (user authentication), a device (entity authentication) or a received message (message authentication).

User Authentication: According to the forms of authentication information, user authentication technologies can be divided into three main kind.

- Something the user is (voice identification, retinal scanners).
- Something the user has (ID cards, smart cards)
- Something the user knows (PINs, passwords.)

Entities Authentication: Different from user authentication, in entity authentication, we are interested in knowing whether the device itself but not the user is legitimate. For example, the SSL 3.0 [10] and the TSL 1.0 [11] is used to perform only the server authentication to the users in a secure web-based application.

Message Authentication: Message authentication allows a message receiver to be convinced of the identity of the message sender. There are various kinds of message authentication technologies. For example, Message Authentication Code (MAC), digital signature and so on.

Authentication is always provided in conjunction with key establishment protocol since the involved two parties should make sure the session key is shared by the intended party.

Adversary: In general, the adversary with respect to AKE can be categorized into two types: passive and active.

– *Passive Adversaries:* A passive adversary only has the ability of eavesdropping the message exchanged. There is no interaction between the passive adversary and the communicating parties. Therefore, the goal of the adversary is to get the secret information shared between the parties through eavesdropping. For example, if the adversary is able to get the several established session keys from the messages exchanged in other distinct sessions, we consider that such AKE protocol is broken.

– *Active Adversaries:* An active adversary can control all the communication links of the system and schedules all protocol events including the initiation of protocol executions and message delivery. The adversary can perform any actions such as injecting, modifying, deleting, redirecting and delaying messages. Besides gaining some secret information, the active adversary may also want to impersonate the legitimate communicating parties. No matter which attacks he is successful to launch, we consider that such AKE protocol is broken.

Symmetric Key Based AKE: When compared with public key based schemes, symmetric key based schemes usually provide higher performance both on computation and communication. In a symmetric key based AKE, the two communicating parties share a long-lived symmetric key or rely on a third party, Trusted Authority (TA), to distribute the session key. However, for the former case, if there are N parties in the system, in total N (N - 1)/2 keys are needed. And each party need to stored N - 1 keys in his secure database. For the latter case, the total number of distinct keys is only N, but the TA usually becomes to be the bottleneck and the single point of failure in some large applications. There have been many such schemes proposed [12].

Public Key Based AKE: In a public key based AKE, each party only needs to store their secret key and the public key of the TA and it only responses for the certificates management, namely, the joining or deleting the parties by issuing or revoking their public key certificates. The AKE protocol running itself does not require the TA be online. And there is no need for TA to store the secret keys of all the parties in his secure storage. Thus this scheme is scalable and provides a good key management solution. However, the computational complexity of these schemes is usually too high to be carried out by the low-power devices such as mobile phone. There have been lots of such schemes proposed [13, 15].

Password Based AKE: As a special case of symmetric key based AKE, password based AKE is widely analyzed and applied due to its high usability and easiness of the system implementation. For the authentication of themselves, the communication parties (users) only need to use a short human-memorizable password instead of the long cryptographic symmetric key as mentioned such system is susceptible to dictionary attacks. Dictionary attacks are feasible by efficiently enumerating all the possible passwords from a dictionary or a small extension of it, if enough information is given to an attacker. Dictionary attacks can be launched online or offline. In an online attack, an attacker attempts to log into a server by trying all possible passwords until a correct one is found. This can easily be defended against at the system level by limiting the number of unsuccessful login attempts. In an offline attack, the attacker records several successful login sessions and then tries all the possible passwords against the login transcripts. This type of attacks is notoriously difficult to defend against and it is the main challenge on designing a secure password-based authenticated key exchange scheme. Since the first set of password-based AKE called EKE was proposed by Bellovin and Merritt [14]

© 2016, IJCSE All Rights Reserved

Forward Secrecy: The corruption of the communication's long-term secret key (e.g. password, PINs, smart card and etc.) will not lead to retrieve of the session key established within the previous sessions. A classical technology to achieving forward secrecy in designing AKE protocol is employing the famous Diffie-Hellman key exchange scheme [15].

5. LITERATURE SURVEY

According to Chun-Li Lin et al. [17], this protocol is also vulnerable to offline guessing attacks. An attacker attempts to use a guessed password in an online transaction. Host verifies the correctness of his guess using responses from server. If his guess fails he must start a new transaction with server using another guessed password. A failed guess cannot be detected and logged by server, as server is not able to depart an honest request from a malicious request. In offline guessing attacks an attacker guesses a password and verifies his guess offline. No participation of server is required, so server does not notice the attack. If his guess fails, the attacker tries again with another password, until he finds the proper one. Among these classes of attacks, the offline password guessing attack is the most comfortable and promising one for an attacker. It is not noticeable and has no communication cost. Storing a plain text version of the shared password at the server is a constraint that cannot (or ought not) always be met. In particular, consider the problem of a user logging in to a computer that does not rely on a secure key server for authentication. It is inadvisable for most hosts to store passwords in either plain form or in a reversibly encrypted form.

Chun-Li Lin et al. (LSH) [16] proposed a three party EKE. This protocol is secure against both the offline guessing attack and undetectable online guessing attacks but also stasis the security properties of perfect forward secrecy. The most important requirement to prevent undetectable online guessing attacks is to provide authentication of host to server. In STW, there is no verifiable information for server to authenticate host. On the contrary, if there is any verifiable information for server combined with password will result in offline guessing attacks. LSH uses server public keys for this purpose. But this is not a satisfactory solution all the times and is impractical for some environments. Communication parties have to obtain and verify the public key of the server, a task which puts a high burden on the user.

In this paper [18] author discusses the safety measures for an easy and proficient three-party password based authenticated key exchange protocol proposed by Huang most in recent times. Password-Authenticated Key Exchange (AKE) protocol allows two parties sharing a same excellent password to have the same opinion on a widespread secret value i.e. a session key over an insecure communication through open network. Here author [18] study give you an idea about her protocol is silent susceptible to three kinds of attacks: 1). imperceptible online dictionary attacks, 2).key-cooperation masquerade attack. Subsequently they propose an enhanced protocol that can defeat the attacks described and however are practically proficient. On the other hand, both off-line and undetectable on-line dictionary attacks are serious attacks alongside password-based settings so that a secure password-based protocol should ideally resist the two types of attacks.

In this paper [19] author has try to shown that it is weak to password compromise masquerade attack while it is not proficient due to its enlarged number of rounds, computational complexity and computational load. So the Password Authenticated Key Exchange (AKE) protocols permit two entities to generate a large common session key and authenticate each other based on a pre-shared human memorable password. In 2006, Strangio proposed the DH-BAKE protocol and declared that point out protocol is provably protected against quite a few attacks. To overcome these weaknesses, an enhanced AKE protocol is proposed which provides several security properties. To conquer exceeding weakness, a well-organized and protected AKE protocol is proposed that is competent to make available several securities attributes while the competence is also get better. To overcome above disadvantages, an enhanced AKE Protocol with mutual authentication is also proposed that provides several security attributes including mutual authentication, Unknown Key Share (UKS), off-line dictionary, undetectable online dictionary, forward secrecy, known session key security, and resilience to Denning-Sacco, password cooperation masquerade, short-lived key cooperation masquerade and replay attacks.

Additionally, [19] it also removes some additional prerequisites such as needing to modular multiplication, modular addition and modular inverse that are imposed by DH-BAKE protocol. So the proposed scheme provides several security properties while it has a significant computational effectiveness and lower number of rounds. So the proposed scheme is more efficient with DH-BAKE protocol.

In this paper [20] author try to reduce the harm of phishing and spyware attacks, banks, governments, other security-sensitive industries and corporate virtual private networks (VPNs) are arranging one-time password systems, where users have many passwords and use each password only formerly to reduce the effects of password compromise. Bank customers nowadays are using sheets of paper with lists of one-time passwords. Online shoppers and gamers nowadays are using hardware one-time password generators. The money being spent on deploying one-time passwords is wasted if these passwords are not being used safely and securely. If a single password is cooperation, it can be only be used to pretend to be the user once maximum value the damage reason by using one-time passwords in one-time-AKE protocols.

In this paper [20], author can be promised that one-time passwords are being used in a more secure way. Here they have presented a model for the protected use of one-time

© 2016, IJCSE All Rights Reserved

passwords in AKE protocols, taking into explanation the initiative that such protocols should be protected even if previous or future one-time passwords have been compromised. On the other hand, existing convenient approaches to one-time passwords have been vulnerable to complicated phishing attacks. Here they give a recognized security management of this significant realistic trouble. So author has consider the use of one-time passwords in the circumstance of password-authenticated key exchange (AKE), which allows for mutual authentication, session key agreement, and conflict to phishing attacks. Here author explain a security model for the use of one-time passwords, unambiguously thinking the cooperation of past and future one-time passwords, and show a universal method for building a secure one-time-AKE protocol from any secure AKE protocol. Their methods also allow for the secure use of pseudo randomly generated and time-dependent passwords and providing superior competence in one-time password circulation.

Implemented a new and efficient technique for the detection of JavaScript vulnerability at the client side [20]. Here in this paper a secure detection of java script attack such as click-hijacking, password capturing and phishing and cookies stealing are implemented and successfully detection from the script.

An automated process for the client-server side attack ad alerts using DES [21] also proposed an efficient Data Encryption Standard technique is implemented for the secure detection and secure communication of data from the client and server such that it prevents from various attacks.

6. CONCLUSION

With regards to key management lots of work has been done, but globally accessible, new types of applications and new types of privacy threats are being introduced to password privacy in the context of authenticated key exchange (AKE) behaves as authentication. In case of offline signature verification method, widespread work have been done to become aware of random and uncomplicated counterfeit, but very few research has been done to verify the proficiencies counterfeit. Outstanding to this, this problem are unmoving open and requires significant research problem. After performing this algorithm with different file having different size we found that proposed algorithm does not require extra space for encrypted file in comparison to existing algorithm. We have already compared AMEA with some symmetric key encryption technique and found that AMEA is better than compared algorithm. This algorithm is not best in only space complexity, it also provides better security feature by using random key selection and transposition features. AMEA is good for minimum bandwidth channel whose transmission capacity is limited, so we can easily transmit our data from one point to another within less time because this algorithm does not increase the size of encrypted file. There are different Application areas for this algorithm. Such as: cloud computing (provides congestion control and data security between users and sever because multiple user access same server at the same time). Banking, Online Payment gateway, E-Commerce. One of the most important feature that makes this algorithm better is that in proposed technique it is impossible to crack by hacker or unauthorized user without knowledge of original key used for encryption, because Random key generation and random key selection and transposition is calculated by performing some calculation On that original key.

REFERENCES

[1] Ding Y, Horster P. Undetectable on-line password guessing attacks. ACM Operat Syst Rev V29 (4), pp.77-86, 1995.

[2] S Lucks, Open key exchange: how to defeat dictionary attacks without encrypting public keys. *Proc of Security Protocol Workshop* (Springer, Heidelberg, 1997) 1361, pp. 79–90 LNCS

[3] P MacKenzie, S Patel, R Swaminathan, Password-authenticated key exchange based on RSA (Springer, Heidelberg, 2000) 1976, pp. 599–613 SIACRYPT 2000, LNCS

[4] MX Zhang, New approaches to password authenticated key exchange based on RSA (Springer, Heidelberg, 2004) 3329, pp. 230–244 ASIACRYPT 2004, LNCS

[5] S Park, J Nam, S Kim, D Won, Efficient password-authenticated key exchange based on RSA (Springer, Heidelberg, 2007) 4377, pp. 309–323 CT-RSA 2007, LNCS

[6] Chen TH, Lee WB. A new method for using hash functions to solve remote user authentication, Comput Electr Eng, v34 (1), pp.53-62, 2008.

[7] Yeh HT, Sun HM. Password authenticated key exchange protocols among diverse network domains, Comput Electr Eng, v31(3) pp.175-189, 2005.

[8] O. Blazy, D. Pointcheval, and D. Vergnaud. Round-Optimal privacy-preserving protocols with smooth projective hash functions. In TCC'12, pages 94-111. Springer-Verlag, 2012.

[9] J. Camenisch, N. Casati, T. Gross, and V. Shoup. Credential authenticated identification and key exchange. In CRYPTO'10, pages 255{276. Springer-Verlag, 2010.

[10] A. O. Freier, P. Karlton, and P. C. Kocher, The SSL Protocol Version 3.0. INTERNET-DRAFT, Nov. 1996. Available at http://www.netscape.com/eng/ssl3/draft302.txt.

[11] T. Dierks and C. Allen, "The TLS Protocol Version 1.0. IETF RFC 2246, Jan. 1999.

[12] M. Bellare and P. Rogaway, "Provably secure session key distribution the three party cases," in Proc. 27th ACM Symp. On Theory of Computing, (Las Vegas), pp. 57{66, ACM, 1995.

[13] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," IEEE Personal Communications, vol. 1, no. 1, pp. 25-31, 1994.

[14] S. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," IEEE Computer Society Symposium on Research in Security and Privacy, pp. 72-84, May 1992.

[15] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol. IT-22, pp. 644-654, Nov 1976.

[16] Chun-Li Lin, Hung-Min Sun, and Tzonelih Hwang. Three-party encrypted key exchange: attacks and a solution. SIGOPS Oper. Syst. Rev., 34(4):12–20, 2000.

© 2016, IJCSE All Rights Reserved

[17] Chun-Li Lin, Hung-Min Sun, M. Steiner, and T. Hwang. Three-party encrypted key exchange without server public-keys. IEEE Communications Letters, 5(12):497–499, Dec 2001.

[18] Shuhua Wu, Kefei Chen, and Yuefei Zhu, "Enhancements of a Three-Party Password-Based Authenticated Key Exchange Protocol" The International Arab Journal of Information Technology, Vol. 10, No. 3, May 2013.

[19] Maryam Saeed, Ali Mackvandi, Mansour Naddafiun, Hamid reza Karimnejad, "An Enhanced password authenticated key exchange protocol without server public keys" 978-1-4673-4828-7/122012.

[20] Detection of Javascript Vulnerability At Client Agent", International Journal of Scientific & Technology Research Volume 1, Issue 7, August 2012.

[21] Saket Gupta,Saurabh Jain,Rachana Mishra," Automated Process of Server and Client Environment with attack alert based on DES", 2014 Fourth International Conference on Communication Systems and NetworkTechnologies,2014.

© 2016, IJCSE All Rights Reserved