International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Investigative Analysis of PAKE Protocol with OTSP and Image Based Password Authentication

Prof. Satish Soni[1], Pooja Shukla[2]

[1]Professor & Head of Computer Science & Engineering Department, JNCT Rewa M.P. 486001 India
[2]Scholar, Computer Science & Engineering Department, JNCT Rewa M.P. 486001 India

ABSTRACT:

Security plays a vital role in information protection from unauthorized or accidental discovery, although the information is in communication and while the information is storage. To reduce the damage of various attacks, banks, governments, and other security sensitive areas are deploying one time password systems, after used that password will automatically destroy. In previous some years invented many password authentication key exchange protocols like DH-PAKE, J-PAKE etc, but they all suffered from some critical security problems. We give a formal approach to overcome these various problems in password authentication key exchange protocols. We use one time private key (OTPK) in the context of password authentication key exchange (PAKE), which allows for mutual verification, session key agreement, and opposition to various critical attacks. And enhance more security in our protocol we have used strong session keys which is generated by imaged based key generation process.

1. INTRODUCTION:

Password-Authenticated Key Exchange (PAKE) empowers two correspondence substances to verify one another and set up a session key by means of effectively extraordinary passwords. The primary PAKE convention was presented by Bellovin and Merritt in 1992 known as Encrypted Key Exchange (EKE).Two-party password based authenticated key exchange (two-PAKE) protocol is somewhat helpful for client-server structures. Notwithstanding, in enormous scope client correspondence conditions where a client needs to speak with a ton of different clients, Two-PAKE protocol is truly challenging in key administration that the quantity of passwords that the client would have to memorize. Security in PCs is data safeguard from unapproved or unintentional divulgence while the data is in transmission and keeping in mind that data is away. Authentication protocols give two elements to ensure that the counterparty is the expected one whom he endeavors to speak with over an unconfident network. These protocols can be considered from three aspects: type, efficiency and security. By and large, there are two kinds of verification conventions, the secret phrase based and the public-key based. In a secret key based protocol, a client enlists his record and secret key to a distant server. Afterward, he can get to the distant server on the off chance that he can demonstrate his insight into the secret key. The server generally keeps a secret phrase or confirmation table yet this will make the framework effortlessly exposed to a taken verifier assault. To resolve this issue, late examinations recommend a methodology with no secret phrase or confirmation table in the server. Besides, to upgrade secret word security, ongoing examinations likewise present an alter safe shrewd card in the client end. In a public key-based framework, a client ought to enroll himself to a trust party, named KGC (Key Generation Center) to get his public key and relating private key. Then, at that point, they can be perceived by an organization substance through his public key. To work on the key administration, a character based public-key cryptosystem is generally embraced, in which KGC issues client ¡s ID as open key and figures relating private key for a client.

1.1 One time private key

Although there are various techniques implemented that are needed for the secure transmission of data from the sender to the receiver. During the transmission of data from the sender to the receiver security plays an important role because the chances of attacks in the network are more. Hence to overcome these limitations there are security techniques implemented for the secure transmission of data. Authentication is also one of the technique through which the data can be send securely. One such concept of providing a strong authentication is using key generation using one time private key. As we know that key is important part for the authentication of the data where the sender and receiver uses his own key for the authentication, but if these keys can't be made strong then such techniques is not a secure one. In the concept of key generation using OTPK during the generation of key by the sender or receiver or by any third party a key is generated for the authentication or for the encryption of the data or for the decryption a key is used and as soon as the sender and the receiver gets authenticated and data is send securely the key gets destroyed.

1.2 The objective

Authentication is the subject of this paper. We propose a simple idea that improves the authentication process, and helps in solving numerous problems in this crucial security field. Users are required to identify themselves so that they can be authenticated as the individuals they claim to be. In the

authentication process, you always use username is never secret. Attacker simply guesses at username and password combinations until they either get lucky or give up. This paper will extensively research password authentication and related problems, and provide some useful key points to reinforce the weakest link in the authentication process. However; our main contribution is the introduction of a new password authentication key exchange protocol using OTPK concept. That is used for authentication and to provide the communication parties with a session key that is used to encrypt the rest of the communication through an unsecured medium.

1.3 Authentication techniques

There exist three different techniques to identify the authenticity of a user:

1. **Relying on something users know (such as passwords):**

The authenticity of the user is established by asking the user to provide some piece of information that only the legitimate user knows. The classic username and password combination is by far the most common implementation of this authentication strategy. Variations of this method of authentication, is asking the user to answer a secret question (such as "What is your mother maiden name?").

2. **Something they have(such as physical keys):**

Instead of relying on user's memory, the system could require that users actually have in their possession some artifact or token that is not easily reproducible.

3. **Some physical attributes of themselves (such as fingerprints):**

This methodology is based on biometric devices that measure some unique property of the user that cannot be easily forged or altered, thus providing an extremely accurate method of identifying an individual user. Biometric authentication method includes face topology and geometry fingerprints, eye patterns, hand topology and geometry, and voice. Ideally, a combination of two or more of these methods should be used.

1.4 Authentication requirements

The authentication process demands some requirements for its success, which are based on the needs of the user and the system. These requirements determine the choice of one of the three authentication mechanism:

- **Accuracy:** The accuracy of an authentication mechanism can be measured in terms of the percentage of legitimate users who attempt to authenticate themselves but are rejected by the system, and by the percentage of unauthorized users, who are able to deceive the system.
- **Availability:** Where and when the services must be accessible and available to properly authorized users.
- **Cost:** Service provider's view cost as a key requirement and they strive for the least cost possible. Of course, the three techniques have different costs in terms of implementing, operating, and maintaining the authentication process. For example, we all know that biometric measurements introduce variable costs in terms of the specific choice used.
- **Convenience:** The system should be as friendly as possible and the authentication process should be as invisible as possible. This is one of the major aspects in authentication, as it plays a major role in the user's encouragement to use the system. The balance between security and convenience should be considered to the furthermost point without falling into the edge of vulnerability.
- **Practicality:** The practicality of the authentication mechanisms is crucial. For example, it is not always possible for the user to carry any form of authentication with him such as a key, card, or any other form of physical matter. At the same time, it is not easy to reproduce such an object if it is lost or damaged. Nonetheless, technological advancements have made it possible to face physical attributes, such as: geometry fingerprints, eye patterns, and some other forms of biometric measurements. One may raise the question: what happens if a biometric ID is compromised?
- **Robustness and reliability:** The system should perform as designed while being resilient to failures and attacks.

1.5 OTPK

The OTPK concept is alarmingly simple to understand. Whenever a digital signature is required, the private key is generated, certified, used to compute the digital signature and immediately deleted. All that remains is the digital signature and the public key certificate from the Certification Authority (CA) that is used to verify the digital signature. There is no possible compromise on the private key, no need for user smart cards/USB tokens, no need for CRLs, no need for LDAP directories, no need for OCSP. It is compliant to international digital signature laws. The OTPK technology should be evaluated as a new and cost effective solution for on-line digital signature providing full mobility for mass usage of the public in different industries. It should be evaluated for this perspective, not from a CA perspective.

The validity of PKI certificate in this case need only be an extremely short term (in the order of minutes or seconds) to remove any chances of compromise. Since OTPK would result in a one-to-one mapping between the certificate and the transaction to be signed, details of the transaction can even be embedded in the certificate request for time stamping purposes. In a typical PKI system, the user does a one-time generation and registration, and stores the certified key in a smartcard (or USB token) for a longer period of use. In contrast, the private key in the OTPK system is for one-time use only. A user always

generates a new private key and authenticates securely with the CA in order to get a digital certificate for every transaction. Once the private key is used, itis expired and erased. There is no need to permanently store the private key in anymedia. Such a process sounds cumbersome; however, the overheads are actually not much more than any mobile credential solution. The setup of OTPK requires the CAto have an online authentication and certification facility to fulfill all certification requests at a much higher throughput than existing setups of PKI. The entity could require a plug-in, implemented entirely in software to generate the private key, send the public key for certification, perform the digital signature operation, and delete the private key securely. The plug-in can be implemented as PKCS #11, CAPI DLL or even as a zero-install Java applet embedded within the web browser.

2. LITERATURE SURVEY:

1. P. Murali, R. Palraj [2011]: propose a new method for generating True random numbers based on image which generates 256 bits key or higher for key exchange algorithm. True random numbers are always secured and good, compared to pseudo random numbers. Diffie-Hellman key exchange algorithm has two weaknesses: Discrete logarithm attack and Man-in-the-Middle attack. Our proposed method can easily overcome the above problems. This method of implementation is very easy, cost effective and convenient for transmission of shared session keys. Our proposed method rapidly increases the security of the key exchange protocols over an unsecured channel and can also be used for Public key cryptosystem. In this paper, propose a method to generate True Random numbers based on image which is very cheap, cost effective, convenient and universal. The attacker could not derive the key from the image. And also it does not require any additional devices. Small change in the image should lead to a significant difference in the generated random number. Further we can also use lossless compression techniques to protect image during transmission.

2**. Abdalla, Dario Catalano, Celine Chevalier, and David Pointcheval [2009}:** In this paper, Michel Abdalla, Dario Catalano, Celine Chevalier, and David Pointcheval investigate whether some of the existing protocols that were proven secure in BPR and BMP models can also be proven secure in the new UC model and we answer this question in the affirmative. The proof of security relies in the random-oracle and ideal-cipher models and works even in the presence of adaptive adversaries, capable of corrupting players at any time and learning their internal states.

3. PROPOSED PROTOCOL:

The problem in public key cryptography is that if the file size is much longer then it takes more time to the encryption or decryption of the message [18]. So we used symmetric key cryptography for sending large file into the insecure networks. Again the problem with the symmetric cryptography is that how to share the common session key, because sharing the common session key is causing the various types of attacks. So for reduced these types of problem to share common session key we have produced a very efficient protocol. In this protocol, we have proposed that when two users or agencies wants to share their common session key and establish a session with 2-factor authentication, for that purpose they required to register himself to the trusted third party. First party login with a password to the TTP, TTP verify that password if the password is valid then 1-factor of authentication is done otherwise return the message with the wrong password. First party chooses the other party (from the list of members which is already registered to the server) for the communication and sent his/her identity (User domain name) along with the own identity to the trusted third party. TTP match these identities from the database and if valid then sent these identity to the second party via other media (email or mobile), and wait for a response from the second party. Second party identifies their identity and if he is interested then goes into the process of login with own password. TTP verify that password if the password is valid then 1-factor authentication is done for second party. After this authentication process, TTP generate a unique random value by the pseudo random generator and sent to the both parties via other registered media (email or mobile). Parties enters this random number and generate the master key and sent to the TTP for further verification, TTP verify this master key to the own master key if it is valid then 2-factor authentication is done for the both parties, Otherwise return with unauthorized person message. Now our second aim is generating a common session key for the both parties, so TTP again generate a random number but this time using the method of true random number generator and calculate the hash value of this number. This hash value sent to the both parties for the purpose of making session key. Parties receive that value and calculate the common session keys, after that first party encrypted the message using own common session key and sent to the second party directly. Second Party decrypt the message using own session key if he is able to decrypt the message successfully then understood that the opposite party is authenticated by the TTP and valid. After the completion of session, session key will be destroyed and again for the new session fresh session key will we generated. The contract signing protocol proposed here works in three Stages.

Stage 1: Registration

In the registration process TTP (trusted third party) generate a registration form for the user, user filled all the required information and send to the TTP. TTP verify all the beneficial information and store in his database. User generate password as per the instruction given by the trusted third party and send to the TTP, after that TTP store this password in his database for further verification of the user at the time of signing.

Here example of some important information which is needed to registration form to registered like:

1. user name
2. mobile number
3. email address
4. Address etc.

Stage 2: Signing

In this stage, already registered users enter the user name and password for signing to the trusted third party. Here in this stage each of the users needs to generate digital signatures for the authentication. Trusted third party verifies the password if password is valid then goes to the process of key generation, otherwise return the user invalid message.

Stage 3: Key generation

Third stage of our protocol is key generation, in this stage trusted third party generate two times random number (keys), first key is generated by the process of pseudo random generator for authentication purpose and after verifying that key second key is generated by the process of true random number generator for making session key .

4. Result analysis

The table 1 shows the comparison of basic features, security, and efficiency between these referenced and our protocols. In the category of basic features, the properties such as transparent trusted third party or not, off-line or on-line trusted third party are considered. Here two main security requirements are compared: fairness and timeliness. The protocol which guarantees the two parties obtain or not obtain the other's signature simultaneously is fair. This property implies that even a fraud party who tries to cheat cannot get an advantage over the other party. At any possible state in the protocol execution, each honest party can complete the protocol uniquely, i.e., without any cooperation of the other (potentially malicious) party then it provides timeliness. In the efficiency evaluation; the costs of over all communication is compared. Our protocol cost is very cheap as compare to other protocols. Some protocol provides timeliness, a protocol provides timeliness if and only if all honest parties always have the ability to completed, in a finite amount of duration, a point in the protocol where they can stop the protocol while preserving fairness. Various types of TTP can be considered according to their involvement in the protocol. Online TTP - A trusted third party involved during each session of the protocol but not during each message's transmission, is said to be online. Off-line TTP - A trusted third party involved in a protocol only in case of an incorrect behaviour of a dishonest entity or in case of a network error, is said to be off-line.

TABLE-1:

Parameters	**Protocols**				
	Escrows Based Protocol [19]	**Park et. al,'s RSA based protocol [21]**	**Bao et. al.'s Protocol [22]**	**Contract Signing Protocol based on RSA[20]**	**Proposed Protocol**
Fairness	YES	YES	YES	YES	YES
Timeliness	YES	YE	YES(weak)	YES	YES
Multiple TTP	YES	YES	YES	YES	YES
Replay attack	YES	YES	YES	YES	NO
Confidentiability	NO	NO	NO	YES	YES
Additional Authentication	NO	NO	NO	NO	YES
Storage Cost	MORE	MORE	MORE	MORE	LESS

5. Conclusion:

The importance of network security is continuously increasing with the rapid growth of computer technology, and becomes nowadays the most essential aspect in the computing world.

Fifty year ago, computer crimes neither were nor heard of. New technologies bring new problems, as the computer technology progresses dramatically; the phenomena of computer crimes threaten computer security. Nowadays, more and more computer crimes are committed; to cope with the current crime rate, computer security is becoming a fundamental need. Effective computer security is now more crucial than ever, and the need to increase awareness is compelling.

Their appreciated finding in this domain has led to incredible levels of security that contributed to magnificent advancements in the computing world. In order to advance more, we have to accept the fact that security is not static, and the risk are always there and therefore do our utmost to minimize those risks as for as is humanly and technologically possible.

In this paper, we have addressed authentication which is one of the most important factor in the computer security world. Then we focused on one time private key in the context of password authentication key exchange protocol. By using of our protocol we have exchanged common session key with strong two factor authentication. The proposed technique implemented here doesn't require much of the storage it doesn't store any key or data for a while hence the chances of various attacks in the network has been reduced such as replay attack or identity disclosure attack. To make session key more strong we have used TRNG (true random number generator) for the key generation. Session key produced by the concatenation of the image generated master key and OTP(one time password), that make more strong session key, so they can also reduce all possibilities of attacks. After the session key established there are no involvement of the TTP, so parties don't share their information to the TTP. After the verification is done OTP will destroy from the TTP side. The OTPK doesn't allow any party to use its signatures again and again for the contract signing since as soon as the TTP verifies the parties the keys generated will be lost and the parties needs to generate different signatures for different contract exchange. The concept of two factor

authentication using an image is an efficient technique as per the authentication is concerned and the types of attacks which are difficult to achieve can be easily prevented by the technique. Various types of attacks such as replay attack, DOS attack, insider attack, outsider attack, password impersonation attacks are easily prevented. The concept of two factor authentication can be applied for multiple parties so that the parties when communicate with each other can be easily shared their data in a secure manner.

References:

[1]. G. Wang, "An abuse-free fair contract signing protocol based on the RSA signature," IEEE Transactions on Information Forensics andSecurity, vol. 5, no. 1, pp. 158–168, Mar 2010

[2]. N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," IEEE J. Sel. Areas Commun., vol. 18, no. 4,pp. 591–606, Apr. 2000.

[3]. M. Abadi, N. Glew, B. Horne, and B. Pinkas, "Certified e-mail with a light on-line trusted third party: Design and implementation," inProc. 2002 Int.World Wide Web Conf. (WWW'02), 2002, pp. 387–395, ACM Press.

[4]. G. Ateniese, "Efficient verifiable encryption (and fair exchange) of digital signature," in Proc. ACMConf. Computer and Communications Security (CCS'99), 1999, pp. 138–146, ACM Press.

[5]. G. Ateniese and C. Nita-Rotaru, "Stateless-receipient certified e-mail system based on verifiable encryption," in Proc. CT-RSA'02,2002, vol. 2271, LNCS, pp. 182–199, Springer-Verlag.

[6]. F. Bao, R. H. Deng, and W. Mao, "Efficient and practical fair exchange protocols with off-line TTP," in Proc. IEEE Symp. Securityand Privacy, 1998, pp. 77–85.

[7]. S. Gürgens, C. Rudolph, and H. Vogt, "On the security of fair nonrepudiation protocols," in Proc. ISC'03, 2003, vol. 2851, LNCS, pp.193–207, Springer-Verlag.

[8]. G. Wang, "Generic non-repudiation protocols supporting transparent off-line TTP," J. Comput. Security, vol. 14, no. 5, pp. 441–467,Nov. 2006.

[9]. S. Micali, "Simple and fast optimistic protocols for fair electronic exchange," in Proc. PODC'03, 2003, pp. 12–19, ACM Press.

[10]. J. Zhou, R. Deng, and F. Bao. Some remarks on a fair exchange protocol. In: Public Key Cryptography (PKC'00), LNCS 1751, pp. 46-57. Springer-Verlag, 2000.

[11]. C. Boyd and E. Foo, "Off-line fair payment protocols using convertible signatures," in Proc. ASIACRYPT'98, 1998, vol. 1514, LNCS,pp. 271–285, Springer-Verlag.

[12]. S. Kremer, O. Markowitch, and J. Zhou, "An intensive survey of fair non-repudiation protocols," Comput.Commun., vol. 25, no. 17,pp. 1606–1621, Nov. 2002, Elsevier.

[13]. F. Bao, G. Wang, J. Zhou, and H. Zhu, "Analysis and improvement of Micali's fair contract signing protocol," in Proc. ACISP'04,2004, vol. 3108, LNCS, pp. 176–187, Springer-Verlag.

[14]. M. Bellare and R. Sandhu, The Security of Practical Two-Party RSA Signature Schemes 2001 [Online]. Available: http://wwwcse.ucsd. edu/users/mihir/papers/

[15]. J. M. Park, E. Chong, H. J. Siegel, and I. Ray, "Constructing fair exchange protocols for e-commerce via distributed computation ofRSA signatures," in Proc. PODC'03, 2003, pp. 172–181, ACM Press.

[16]. M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proc. 1st ACM Conf.Computer and Communications Security (CCS'93), 1993, pp. 62–73, ACM press.

[17]. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM,vol. 21, no. 2, pp. 120–126, Feb. 1978.

[18]. O. Markowitch and S. Kremer.An optimistic non-repudiation protocol with transparent trusted third party. In: Information SecurityConference (ISC'01), LNCS 2200, pp. 363-378. Springer-Verlag, 2001.

[19]. Y. Dodis and L. Reyzin, "Breaking and repairing optimistic fair exchange from PODC 2003," in Proc. ACM Workshop on Digital Rights Management (DRM'03), 2003, pp. 47–54, ACM Press.

[20]. A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in Proc. CRYPTO'86, 1987, vol. 263, LNCS, pp. 186–194, Springer-Verlag.

[21]. S. M. Bellovin and M. Merrit, Encrypted key exchange: password-based protocols secure against dictionary attacks, Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992.

[22]. L. Gong, M. Lomas, R. Needham and J. Saltzer, Protecting poorly chosen secrets from guessing attacks, IEEE Journal on Selected Areas in Communications, Vol. 11, No. 5, pp. 648-656, 1993.