A REVIEW: SMART CARD BASED PAKE PROTOCOL ON DISTRIBUTED SYSTEM

Pritaj Yadav
Research Scholar

Dr.Sitesh Kumar Sinha
Prof., Deptt. of CSE,RNTU,Bhopal

Dr.S.Veenadhari
Associate Prof.,Deptt. of CSE,RNTU,Bhopal

***Abstract* —** for the past few decades, an extensive variety of cryptographic protocols have been suggested in order to resolve the 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 smart card based password-based authenticated key exchange (PAKE). Especially, we show that smart card based PAKE protocols provably meeting the existing formal definitions do not accomplish the anticipated level of password privacy when organized in the real world. Authentication is necessary for any secure transaction. Smart card based authentication mechanism are most popular because of the strong security and simplicity. This paper also describes about various smartcard based authentication mechanisms.

***Index Terms* — Smart Card, Password-Based Authenticated Key exchanges (PAKE), Authentication, Symmetric Key, attacks.**

1. INTRODUCTION

Authentications based on smart card provide an improvement on basic password operations. It is similar to taking cash from an ATM, where we have a bank card and a PIN number. A user's private key certificate information is stored on the smart card that helps to uniquely identify the user. The card will be automatically blocked after a number of unsuccessful PIN entries. A number of cryptographic operations on the card protects from malicious attacks. Those cryptographic operations are carried out by the processor. In many insecure transmission environments, such as internet and wireless channel, when a user wants to access the valuable resource from the server, typically, a user's identity and password are needed for the server to authenticate the validity of the user. Smartcard based authentication is one of the best known and simplest mechanisms for dealing with the transmission of secret data over insecure networks. A smart card is a plastic card that contains user's data with a microchip. Cards must interface to a computer or terminal through a standard card reader. There are two types of smart cards. Contact smartcards and Contactless smart cards. Contact smart cards can be inserted into a smart card reader. They contain a small gold plate on the front. Electrical connectors in the smart card reader help to transfer data to and from the chip. Transactions in contact less smart cards are carried with the help of an antenna. They are also similar to plastic credit cards. It contains an electronic microchip and antenna for communication. These components allow the card to communicate with an antenna without a physical contact. Contactless cards provide transactions quickly. Smart card based authentication scheme mainly consists of the following phases. They are the registration phase, login phase, verification phase and password change phase. The registration phase is activated when new user wants to register within the server. For the purpose of registration, the user submits his or her details to the server. When the registration request from the user reached on the server side it calculates essential parameters by using the submitted information and finally issue smart card to the user by storing important parameters into the memory of smart card. The login phase and verification phase are used when a user wants to access resources from the server. In the login phase, user creates a login request and sends it to server for verification. Once the login request is received, server checks the validity of login request and the legitimacy of user. In password change phase user can change the password according to their needs.

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 MacKenzie 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-EPAKE protocol [5] which can resist the *e*-residue attack based on number-theoretic techniques.

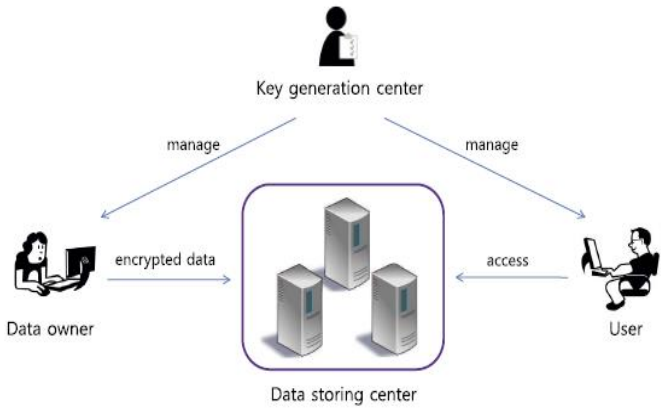

Fig 1. An Example of Data Sharing System

2. PASSWORD AUTHENTICATED KEY EXCHANGE PROTOCOLS

2.1 Password-Based Key Exchange: Authentication is not possible while not sharing some data earlier. Maybe the smallest such data that also provides a helpful level of authentication could be a short, easy-to-memorize word. Protocols for password-based authenticated key exchange (PAKE) permit 2 entities who have shared a low-entropy password to confirm that they're communication with one another (that is, to perform mutual authentication), moreover on establish a high-entropy (cryptographic) session key that may be wont to cipher and certify their resulting communication. By this, users will communicate over a public unreliable channel and might agree a secure session key. Because the password primarily based authenticated key exchange protocols [6, 7] need users solely to recollect an individual's unforgettable (low-entropy) password, it's rather easy and efficient. Although password-based systems have their drawbacks — their security is inherently restricted and this is often solely exacerbated by users' poor selection of passwords — their convenience (e.g., no special devices ought to be carried by users) and easy preparation (e.g., no public-key infrastructure to support use of public key primitives needed) appear to confirm their widespread use for the predictable future. Indeed, probabilities of large-scale preparation of PAKE protocols ar greatly increased by their recent IEEE standardization. Password-based attested key exchange permits 2 parties holding solely short, human-memorable passwords to determine a secure session key of high-entropy once they share constant password. Such a key exchange is authenticated in an exceedingly sense that it's secure against man-in-the-middle adversaries. Whereas on-line attackers will guess a password with non-negligible chance, interference of on-line attackers is easy with alternative mechanism (e.g., access block once consecutive log-in failures), it's challenging to stop on-line assaulter from enumerating all attainable passwords of little area into execution transcripts. Therefore, primarily, major security property of password-based authenticated key exchange is security against off-line dictionary attackers.

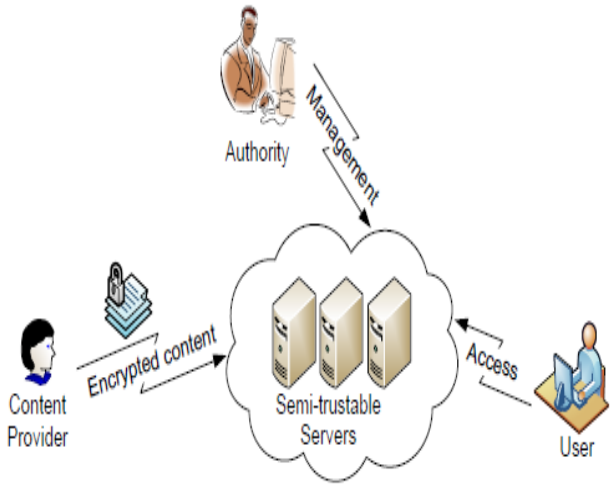

Fig 2. Scenario of secrete data sharing

2.2 General Description: Just like in key-agreement, password-based key exchange protocols (PAKEs) 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 PAKE 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 PAKE 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 PAKE 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 certain the protection of a protocol formally, the likelihood of an adversary's "breaking" the method as perform of the no. of on-line attacks that occur, whereas in apply one would like an absolute certain on the protection of the protocol freelance of the amount of on-line tries. Despite their intuitive utility there has been very little take up within the world of PAKE protocols. One reason, that is commonly mentioned for this, is that the subsistence of a wide-ranging copyright on the EKE protocol. It should be helpful to notice 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 very challenging scenario. as an example, if 2 parties, A and B, would really like to securely communicate over a lively open network, they'd completely need to create clear in your mind that the information they correspond between themselves ought to stay non-public and genuineness of the info ought to be maintained. However, for this, there should be a primitive cryptologic key agreement that contains each cryptography and digital signature. With the assistance of such protocols carrying a typical session key, 2 or a lot of parties will exchange very important data over associate adversely controlled and insecure network. These protected key agreement protocols act because the basic building block for accumulating secure, sophisticated, higher-level protocols. Key establishment is typically separated into key transport and key agreement section.

Secret keys provide message integrity and confidentiality wherever solely sure parties usually have copies of the key key. However, during an all over world of technological advancement, key distribution may be a major drawback from the protection facet. Basically, key establishment protocols want a set-up part through that authentic and secret initial keying material is distributed. Most protocols are created with the target of distinct keys on every protocol execution. In bound cases, the initial keying material pre-defines a hard and fast key which can result anytime the protocol is enforced by a given combine or perhaps a bunch of users. To enhance secure key establishment, the best method during a key establishment protocol is to work out truth identity of the sender and receiver which might be attainable by gaining access to the ensuing key and prohibit any further unauthorized parties from extracting identical key. For a secure key institution, secrecy of the key and identification of accessing parties are needed. In addition to the above mentioned come back reachable of that are tailored to the password-based setting there continue living over some additional 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 kinds.

- 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-memorable 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]

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 additionally liable to offline guesswork attacks. An offender tries to use a guessed secret in a web transaction. Host verifies the correctness of his guess mistreatment responses from server. If his guess fails, he should begin a replacement transaction with server using another guessed secret. An unsuccessful guess can't be detected and logged by server, as server isn't able to depart an honest request from a malicious request. In offline guesswork attacks an offender guesses a secret and verifies his guess offline. No participation of server is needed; therefore, server doesn't notice the attack. If his guess fails, the offender tries once more with another secret, till he finds the correct one. Among these categories of attacks, the offline secret guesswork attack is that the comfiest and promising one for an offender. It not noticeable and has no communication price. Storing a clear text version of the shared secret at the server may be a constraint that can't (or ought not) forever be met. Particularly, think about the matter of a user logging in to a laptop that doesn't accept a secure key server for authentication. It's inadvisable for many hosts to store passwords in either plain type or in a very reversibly encrypted type.

Chun-Li carver et al. (LSH) [16] planned a 3 party EKE. This protocol is secure against each the offline guess attack and undetectable on-line guess attacks however additionally satisfies the protection properties of good forward secrecy. The foremost vital demand to stop undetectable on-line guess attacks is to produce authentication of host to server. In STW, there's no verifiable data for server to certify host. On the contrary, if there's any verifiable data for server combined with secret can lead to offline guess attacks. LSH uses server public keys for this purpose. However, this can be not a satisfactory resolution all the days and is impractical for a few environments. Communication parties need to acquire and verify the general public key of the server, a task that puts a high burden on the user.

In this paper [18] author discusses the security measures for a simple and adept three-way secret primarily based genuine key exchange protocol projected by Huang most in recent times. Password-Authenticated Key Exchange (PAKE) protocol permits 2 parties sharing a same excellent secret to possess a similar opinion on a widespread secret worth i.e. a session key over an insecure communication through open network. Here author [18] study provide you with a concept concerning her protocol is silent liable to 3 types of attacks: 1). imperceptible on-line lexicon attacks, 2). key-cooperation masquerade attack. Later on they propose an improved protocol that may defeat the attacks represented and but are much practiced. On the opposite hand, each off-line and undetectable on-line lexicon attacks are serious attacks alongside password-based settings therefore that a secure password-based protocol ought to ideally resist the 2 sorts of attacks.

In this paper [19] author has attempt to shown that it's weak to secret compromise masquerade attack whereas it's not adept owing to its enlarged variety of rounds, process complexness and process load. Therefore, the secret genuine Key Exchange (PAKE) protocols allow 2 entities to get an oversized common session key and certify one another supported a pre-shared human unforgettable secret. In 2006, Strangio planned the DH-BPAKE protocol and declared that time out protocol is demonstrably protected against quite a few attacks. To reduce these weaknesses, an improved PAKE protocol is projected that provides many security properties. To overcome exceptional weakness, a well-organized and guarded PAKE protocol is planned that's competent to create offered many securities attributes whereas the ability is additionally retrieve. to beat higher than disadvantages, an improved PAKE Protocol with mutual authentication is additionally projected that gives many security attributes as well as mutual authentication, Unknown Key Share (UKS), off-line lexicon, undetectable on-line lexicon, forward secrecy, acknowledged session key security, and resilience to Denning-Sacco, secret cooperation masquerade, temporary key cooperation masquerade and replay attacks.

Additionally, [19] it additionally removes some further conditions like wanting to standard multiplication, standard addition and standard inverse that are obligatory by DH-BPAKE protocol. That the projected method provides many security properties whereas it's a major process effectiveness and lower variety of rounds. That the projected method is additional economical with DH-BPAKE protocol.

In this paper [20] author attempt to cut back the damage of phishing and spyware attacks, banks, governments, different security-sensitive industries and company virtual personal networks (VPNs) are transcription one-time secret systems, wherever users have several secrets and use every secret solely once to cut back the results of password compromise. Bank customers these days are victimization sheets of paper with lists of one-time passwords. Internet buyers and gamers these days are victimization hardware one-time secret generators. The money being spent on deploying one-time passwords is wasted if these passwords aren't

getting used safely and firmly. If one secret is cooperation, it is solely being wont to faux to be the user once most price the injury reason by victimization one-time passwords in one-time-PAKE 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 passwords in PAKE 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 considered the use of one-time passwords in the circumstance of password-authenticated key exchange (PAKE), 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-PAKE protocol from any secure PAKE 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.

Saurabh Jain, Deepak Singh Tomar, Divya Rishi Sahu 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 phising and cookies stealing are implemented and successfully detection from the script.

Saket Gupta, Saurabh Jain, Rachana Mishra also proposed an automated process for the client-server side attack ad alerts using DES [21]. In this paper 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.

Manik Lal, Saxena and Gulati proposed a remote user authentication mechanism [22] for smart cards. This technique allows the users to change and choose the passwords according to their needs without a verifier table. One-way hash function provides better security to this approach. This method can resist all the attacks except the impersonate attack.

Wang et' al proposed [23] an efficient and secure dynamic ID-based remote user mutual authentication mechanism with improved security. This scheme provides security for the changing of passwords independently by the users.

Li Yang, Jian-Feng Ma, and Qi Jiang proposed smart cards and passwords mutual authentication under trusted computing [24] consists of client and server side. This scheme contains a TPM chip and its function is to manage the server through wired network. Smart card user firstly registers with the server that containing TPM chip. TPM chip is an independent coprocessor performs encryption function, security function, storage function and also provides software and hardware support. Chang–Cheng's authentication mechanism uses one-way hash function and exclusive OR operation for improving the performance of the system during multi server authentication process. Here the user performs the registration with registration center by giving the values of id, password and personal information as plain text so the insider of registration center can get id and password of the users. A password and smart card based user authentication mechanism for multi-server environments involve hash function encryption process. In registration phase user computes hash value of id and password and also the user chooses a random number that improves the security. Service provider gives permission to users for accessing the resources.

Kwong chan [25] proposed a cryptanalysis for smart card authentication in multiserver environment. Tsai et'al proposed a scheme for smart cards with mutual authentication. In this scheme server's secret key is stored in the protected memory of server and its corresponding public key Y=g x mod p is stored in each user's smartcard. Here verification of the user's is done after the login request so it takes more time for password detection.

Jiang et'al proposed [26] a user authentication with key agreement scheme can provide privacy to users. This remote authentication mechanism uses a public key based mechanism with low computational and communication cost.

Chien, Jan and Tseng, developed [27] an efficient and practical solution to remote authentication on smart card. It can provide mutual authentication between user and server without a verification table. Another advantage of this approach is that users can freely change password. Communication and computational cost is also very low.

Chen, Kuo, and Wuu used [28] a strong and efficient smart card based remote user password authentication scheme. They proposed an improved and efficient password authentication mechanism. This approach can handle the secret information with a key agreement phase by mutual authentication. It can provide security to stolen smart card attack.

Hwang and Li proposed [29] another remote user authentication scheme using password based on El Gamal's public key encryption process. This scheme can check the legitimacy of user without any verification table. Another advantage is that it can overcome message replay attack.

Yoon, & Yoo develop [30] a robust biometrics based multi-server authentication mechanism on smart card based on elliptic curve cryptosystem. This scheme minimizes the complexity of hash operations. Biometric technique allows strong user authentication operation. It provides better security, reliability and efficiency and suitable to use in distributed multi server network environment.

Sood, Sarje, Kuldip projected [31] secure and ideal dynamic identity primarily based authentication protocol for multi-server setting. It contains 2 servers one is that the service supplier server and alternative is that the management server. Service supplier server is open for purchasers for obtaining the services throughout their registration, login and secret modification part. This theme uses unidirectional hash functions and XOR operations. This theme will modification the user's secret firmly while not the assistance from server.

Xiong Li et al projected [32] an increased open-end credit primarily based remote user secret authentication approach that will guarantee forward secrecy and additionally it can discover the incorrect secret given by the user throughout their login part. This theme is user friendly and therefore the user will modification or update the secret while not creating any communication to server system.

6. CONCLUSION

Authentications based on smart card provide an improvement on basic password operations. Smart card based authentication mechanism are most popular because of the strong security and simplicity. The survey shows various smart card based authentication mechanism. In this survey have looked on various papers of authentication mechanism based on smart cards and each of the paper has its own advantages and limitations. Therefore, it is necessary to design a secure and efficient smart card based

authentication mechanism. 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 smart card based password authenticated key exchange protocol (PAKE) behaves as authentication. In case of offline signature verification method, widespread work has 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 is unmoving open and requires significant research problem.

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.

[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.

[22] Das, M. L.,Saxana, A., & Gulati, V. P. (2004). A dynamic] ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629-631.

[23] Wang, Y.Y., Liu J.Y., Xiao,F.X., & Dan J., (2009). A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications, vol. 32, no. 4, pp. 583-585.

[24] Li Yang, Jian-Feng Ma, and Qi Jiang, Mutual Authentication Scheme with SmartCards and Password under Trusted Computing, International Journal of Network Security, Vol.14, No.3, PP. 156-163.

[25] C. K. Chan, and L. M. Chang, Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Trans. on Consumer Electron., vol. 46, no. 4, pp. 992-993, Nov. 2000

[26] Jiang, P., Wen, Q., Li,W., Jin Z., and Zhang, H. (2013). Ananonymous user authentication with key agreement scheme without pairings for multiserver architecture using SCPKs. The Scientific World Journal, vol. 2013, Article ID 419592, 8 pages

[27] H. Chien, J. Jan, and Y. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," Computers and Security,Vol. 21, No. 4, pp. 372-375, 2002

[28] Chen BL, Kuo WC, Wuu LC (2012). Robust smart-card-based remote user password authentication scheme, International Journal of Communication Systems

[29] M. Hwang and L. Li, A New Remote User Authentication Scheme Using Smart Cards, IEEE Transactions on Consumer Electronics,Vol. 46, No. 1, pp. 28-30, February, 2000

[30] Yoon, E.-J., & Yoo, K.-Y. (2010). Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. Journal of Supercomputing, 1–21.

[31] Sandeep K. Sood, Anil K. Sarje, Kuldip Singh (2011).”A secure dynamic identity based authentication protocol for multi-server architecture,” Journal of Network and Computer Applications, pp. 609-618.

[32] Xiong Li, Jianwei Niu, Muhammad Khurram Khan, Junguo Liao (2013). An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications, pp. 1365-1371