ISSN:0975-9646

# An Efficient password based Two-Server Authentication and Pre-shared Key Exchange System using Smart Cards

Anamika Chouksey, Yogadhar Pandey

*Sagar Institute of Research and Technology*
*Bhopal, India*

**Abstract: Password Authenticated Key Exchange (PAKE) protocols enable two entities to agree on a common session key based on a pre-shared human memorable password. The main security goal of these protocols is providing security against password guessing attacks.**

**Recently, In 2010 R. Song [1] proposed advanced smart card based password authentication protocol with such non-tamper resistant smart card based on symmetric key cryptosystem as well as modular exponentiation. R. Song et al Scheme is vulnerable to the offline password attack, insider attack; forward secrecy and denial of service attack are cryptanalysis by W B Horng. Here in this paper we will survey on different protocols implemented based on two password authentication and a brief review is given based on different techniques.**

## 1. Introduction

Providing secure communication over insecure open networks has been a great concern for researchers. During recent years, cryptographic approaches have been applied to remove these problems. Among these approaches, Password Authenticated Key Exchange (PAKE) protocols have been played an essential role in providing secure communications. PAKE protocols permit a client and a server to authenticate each other and generate a strong common session key through a pre-shared human memorable password over an insecure channel.

Two-party password-based authenticated key exchange (two-PAKE) protocol is quite useful for client-server architectures. However, in large-scale client-client communication environments where a user wants to communicate with many other users, Two-PAKE protocol is very inconvenient in key management that the number of passwords that the user would need to remember.

Security in computers is information protection from unauthorized or accidental disclosure while the information is in transmission and while information is in storage.

Authentication protocols provide two entities to ensure that the counterparty is the intended one whom he attempts to communicate with over an insecure network. These protocols can be considered from three dimensions: type, efficiency and security.

In general, there are two types of authentication protocols, the password-based and the public-key based. In a password based protocol, a user registers his account and password to a remote server. Later, he can access the remote server if he can prove his knowledge of the password. The server usually maintains a password or verification table but this will make the system easily subjected to a stolen-verifier attack. To address this problem, recent studies suggest an approach without any password or verification table in the server. Moreover, to enhance password protection, recent studies also introduce a tamper-resistant smart card in the user end. In a public key-based system, a user should register himself to a trust party, named KGC (Key Generation Center) to obtain his public key and corresponding private key. Then, they can be recognized by a network entity through his public key. To simplify the key management, an identity-based public-key cryptosystem is usually adopted, in which KGC issues user ¡s ID as public key and computes corresponding private key for a user.

Considering computational efficiency in an authentication protocol, researchers employs low computational techniques encryptions rather than much expensive computation like asymmetric key encryptions (i.e., RSA, ECC, ElGamal, and bilinear pairings). As considering communication efficiency, it usually to reduce the number of passes (rounds) of a protocol since the round efficiency is more significant than the computation efficiency. The most important dimension of an authentication protocol is its security, and it should ensure secure communications for any two legal entities over an insecure network. Attackers easily eavesdrop, modify or intercept the communication messages on the open network. Hence, an authentication protocol should withstand various attacks, such as password guessing attack, replay attack, impersonation attack, insider attack, and man-in-the-middle attack.

## 2. Background

Password-based authenticated key exchange (PAKE) protocols enable two users to generate a common, cryptographically-strong key based on an initial, low-entropy, shared secret (i.e., a password). The difficulty in this setting is to prevent off-line dictionary attacks where an adversary exhaustively enumerates potential passwords on its own, attempting to match the correct password to observed protocol executions. Roughly, a PAKE protocol is secure if off-line attacks are of no use and the best attack is an on-line dictionary attack where an adversary must actively try to impersonate an honest party using each possible password. On-line attacks of this sort are inherent in the model of password-based authentication; more importantly, they can be detected by the server as failed login attempts and defended against.

## 3. RELATED WORK

In 2011, Maryam Saeed has suggested a new two party authentication protocol without the server's public key in which the limitations of PAKE1 and PAKE2 protocols has been overcome and new authentication protocols has been implemented which can provide several security attributes while it has a remarkable computational efficiency and lower number of rounds [2].

In [2], it is proved that the Hitchcock et al.'s protocol is vulnerable to ephemeral key compromise impersonation, off-line dictionary and Key Compromise Impersonation (KCI) attacks while it does not provide the mutual authentication and forward secrecy attributes. It is also shown that SPAKEI and SPAKE2 protocols are vulnerable to password compromise impersonation and Denial-of-Service (DoS) attacks while they do not provide the mutual authentication property. To remove the above disadvantages, an efficient secure two-party P AKE protocol is designed to provide several securities attributes while the efficiency is also improved.

In 2010 Songs proposed very recently a password-based authentication and key establishment protocol using smart cards which attempts to solve some weaknesses [1] found in a previous scheme suggested by Xu, Zhu, and Feng [3].

In 2009, Lee et al. showed that Juang et al.'s scheme is not secure against stolen-verifier attack. Moreover, Juang's scheme does not satisfy the user anonymity. To solve this problem, Kyung-kug Kim proposed an improved anonymous authentication and key exchange scheme. Then, we show that the proposed scheme is secure against various well-known attacks [4].

In 2011 a password based authentication using Elliptic Curve Cryptography (ECC) for smart card. Since the secret key of the AS is a long-term key, it requires further security. When the secret key of the AS is compromised, the entire operation of the AS will be disrupted. Is it necessary to replace or alter the long term secret key [5].

Password-authenticated secret sharing (PASS) schemes, first introduced by Bagherzandi et al. at CCS 2011, allow users to distribute data among several servers so that the data can be recovered using a single human-memorizable password, but no single server (or even no collusion of servers up to a certain size) can mount an off-line dictionary attack on the password or learn anything about the data. Further in 2012 present a concrete 2PASS protocol and prove that it meets our definition. Given the strong security guarantees, our protocol is surprisingly efficient: in its most efficient instantiation under the DDH assumption in the random oracle model [6].

In 2011 the TW-KEAP is an efficient protocol for sharing a session key to protect communication in an insecure network. It is based on the concept of the Diffie-Hellman key exchange protocol which allows the key exchange without session key appearing in the message. The TW KEAP could support lawful interception because the corresponding server is involved in the key exchange procedure to derive the session key [7].

In 2012 a simple and intuitive model for expressing the semantics of privacy-friendly authentication and accountability technologies such as anonymous credentials systems and verifiable encryption. It allows for expressing the precise relations as well as the authentication and accountability properties between parties. The concepts cover in the model comprises pseudonyms, attribute-based authentication, as well as conditional release of information. As a result, the model can express the relevant primitives for privacy-preserving authentication and accountability at the same time [8].

Many standards exist for authentication, ranging from simple static passwords stored on a single machine to complicated distributed systems. Organizations concerned about protecting their digital assets from sophisticated cyber attacks have begun relying on two-factor authentication as a defense against unauthorized access [9]. These protocols were proven secure in the random oracle model. Katz, Ostrovsky, and Yung (KOY) [10] demonstrated the first efficient PAKE protocol with a proof of security in the standard model.

It also achieves mutual authentication in three rounds. In their work [11], Groce and Katz mentioned their framework will significantly improve efficiency when basing the protocol on lattice assumptions. Katz and Vaikuntanathan [12] first instantiated the KOY/GL PAKE protocol under lattice assumptions. The most technically difficult aspect of their work is the construction of a lattice-based CCA-secure encryption scheme with an associated approximate smooth projective hash system. In order to plug into the JG/GK's framework, we use an approximate lattice-based SPH and an error correcting code (ECC) to do the job of an exact lattice-based SPH.

## 4. PROPOSED SCHEME

We present a secure and an efficient ID-based remote user authentication protocol with smart card. We use one-way hash function and Bitwise XOR operation in this proposed scheme. Which execution time is extremely very low to compare to using Modular exponentiation. Our proposed scheme doesn‟t use any common key for encryption and decryption algorithm. Using one-way Hash function, it‟s computationally infeasible to invert operation. This scheme has four phases.

1-Registration phase
2-Login phase
3- authentication/verification phase and
4-password change phase.

The notations use in proposed scheme and phases are describe below-

The Notations
U – Remote User
ID – Identity of User
PW– password chosen by User
S– Remote authentication Server
X– Permanent secret key of S
H (·) – One-way hash Function
xor – Bitwise XOR operation
|| – concatenation

**Registration Phase-** In the registration phase, User Ui wants to register himself/herself in remote server S. Firstly User chooses his/her ID and PW. Before register on Server, registration authority computes h (ID) and h (ID||PW) and sends to remote server S over a secure channel. Upon receiving the registration request from User Ui. Server S computes same parameters related to the User Ui. S computes

$Ai = h\ (ID)\ \text{xor}\ h\ (X \| h\ (ID))$

$Bi = Ai\ \text{xor}\ h\ (ID \| PW)$

$Ci = h\ (Ai)$

$Di = h\ (ID \| PW)\ \text{xor}\ h(X)$

And stored some of them in the smart card memory and issues this smart card to User Ui. This smart card is delivered to User Ui through a secure channel.

**Login Phase-** This phase provides the facility of a secure login to the user .User wants to access same services on remote server S. first it gain the access right on the remote server S. User Ui inserts the smart card to card reader and keys in ID* and PW*. The card reader computes –

$Ai^* = Bi\ \text{xor}\ h\ (ID^* \| PW^*)$

And Ci* = h (Ai*) and checks whether Ci (stored in the smart card memory) and Ci* are equal or not. If not, terminate to again login process. Otherwise yes, User Ui is legitimate bearer of the smart card. Then the card reader generates a random nonce Ri and computes –

$Ei = Ai^*\ \text{xor}\ Ri$

$Cid = h\ (ID \| PW)\ \text{xor}\ Ri$

$Fi = h\ (Ai \| Di \| Ri \| Tu)$

Where Tu is current time when login request proceed. And send the login request massage {Fi, Ei, Cid, Tu, h (ID)} to remote server S.

**Verification Phase-** Upon receiving the login request massage {Fi, Ei, Cid, Tu, h (ID)}. Server verifies the validity of time delay between Tu‟ and Tu. Where Tu’ is the travel time of the massage. $Tu' - Tu \le \Delta T$ where $\Delta T$ denotes expects valid time interval for transmission delay. Then server accepts the login request and go to next process, otherwise the server reject login request.

Server computes –

$Ai^* = h\ (ID)\ \text{xor}\ h\ (X \| h\ (ID))$

$Ri^* = Ai^*\ \text{xor}\ Ci$

$G = h\ (ID \| PW)^* = Cid\ \text{xor}\ Ri$

$Di^* = h\ (ID \| PW)^*\ \text{xor}\ h(X)$

And computes $F^* = h\ (Ai^* \| Di^* \| Ri^* \| Tu)$

And checks whether F and F* are equal or not. If they are not then reject the login request. If equal, then server S Computes–

$Fs = h\ (h\ (ID) \| Di \| Ri \| Ts)$ Where, Ts is remote server current time. And send acknowledge massage {Fs, G, Ts} to user Ui. Upon receiving acknowledge massage smart card compute

$G^* = h\ (ID \| PW)$

$Fs^* = h\ (h\ (ID) \| Di \| Ri \| Ts)$

And checks where G =G*and Fs = Fs* are same or not. It is mutual authentication process. In which both Server and User verify to each other. If they are same then card reader makes session key (Sk) and both Server and User share it.

$Sk = h\ (h\ (ID) \| Ts \| Tu \| Ai)$

Otherwise terminate to again login process.

**Password change Phase-** This phase is involved whenever User U want to change the password PW with a new Password PWnew .User U inserts the smart card to the card reader/client machine and keys in ID* and PW* and request to change password. The card reader checks whether C = C* are equal or not. If it is satisfy User U is a legitimate bearer of the smart card. Then the card reader asks the User Ui to input new password PWnew. After entering the new password the card reader calculate-

$Bnew = Ai\ \text{xor}\ h\ (ID \| PWnew)$ and

$Dnew = h\ (ID \| PWnew)\ \text{xor}\ h\ (ID \| PW)\ \text{xor}\ Di$

And change B with Bnew and D with Dnew in smart card memory.

## 5. SECURITY ANALYSIS

The security analysis is discussed with respect to the security features which the proposed protocol should satisfy. It is desirable for a two-party P AKE protocol to possess the following security attributes [13]:

- **Forward secrecy:** If the user's password or the server's private key is divulged, the secrecy of previously established session keys should not be revealed.
- **Known session key security:** Disclosure of one session key should not reveal other session keys.
- **Resilience to Denning-Sacco attack:** Disclosure of session key should not enable an attacker to calculate or guess the password.
- **Resilience to password compromise impersonation attack:** Password compromise of any user A should not enable an attacker to share any session key with A by impersonating himself/herself as any other entity.
- **Resilience to Unknown Key Share (UKS) attack:** User A should not be coerced into sharing a key with an attacker while he thinks that his key is shared with another user B.
- **Resilience to off-line dictionary attack:** If an attacker could guess a password, he should not be able to check his guess off-line.
- **Resilience to undetectable on-line dictionary attack:** If the attacker could guess a password in an on-line transaction, he should not be able to check the correctness of his guess by using responses from the server and the server is also able to detect an honest request from a malicious request.
- **Resilience to replay attack:** An attacker or originator, who captured the exchanged data, should not be able to reuse it maliciously.
- **Resilience to ephemeral key compromise impersonation attack:** Disclosure of the ephemeral key of any user A should not enable adversary to share session key with A by impersonating any other participant.
- **Resilience to Key Compromise Impersonation (KCI) attack:** Disclosure of the user A's private key should not enable the attacker to masquerade as other participants to A.
- **Resilience to malicious server attack:** If an attacker runs on a malicious server and tempts people to register with that server, he/she should not be able to obtain the passwords of users and impersonate himself/herself as users in login to another server.
- **Resilience to man-in-the-middle attack:** The attacker captures and changes the transferred messages between the user and server while two participants are unaware of being attacked by the attacker.

## 6. CONCLUSION

Here in this paper we will provide the literature survey on the basis of different PAKE techniques and the different ways of providing authentication to the user. We will only provide the survey of the work that had been done so far. In the next step we provide the simulation of the proposed work in the PAKE technique and analyse on the basis of different parameters.

## REFERENCES

[1] Juan E. Tapiador, Julio C. Hernandez-Castro, “Cryptanalysis of Song's advanced smart card based password authentication protocol”, 2010. Online available: http://arxiv.org/pdf/1111.2744.pdf

[2] Maryam Saeed, Hadi Shahriar Shahhoseini, “An Improved two-party Password Authenticated Key Exchange Protocol without Server's Public Key”, IEEE 3rd International Conference on Communication Software and Networks (ICCSN-2011), pp. 90-95, 2011.

[3] J. Xu, W.-T Zhu, and D.-G Feng. “An improved smart card based password authentication scheme with provable security.” Computer Stan- dards & Interfaces 31, pp. 723–728, 2009.

[4] Kyung-kug Kim, “An Improved Anonymous Authentication and Key Exchange Scheme”, Proceedings of the CUBE International Information Technology Conference, pp. 740-743, 2012.

[5] Amutha Prabakar Muniyandi, Rajaram Ramasamy, “Password Based Remote Authentication Scheme using ECC for Smart Card”, Proceedings of the 2011 International Conference on Communication, Computing & Security, pp. 549-554, 2011.

[6] Jan Camenisch, Anna Lysyanskaya, “Practical Yet Universally Composable Two-Server Password Authenticated Secret Sharing”, Proceedings of the 2012 ACM conference on Computer and communications security, pp. 525-536, 2012.

[7] Wei-Kuo Chiang and Jian-Hao Chen, “TW-KEAP: An Efficient Four-Party Key Exchange Protocol for End-to-End Communications”, Proceedings of the 4th international conference on Security of information and networks, pp. 167-174, 2011.

[8]Patrik Bichsel, Jan Camenisch, “A Calculus for Privacy friendly Authentication”, Proceedings of the 17th ACM symposium on Access Control Models and Technologies, pp. 157-166, 2012.

[9] Matthew A. Ezell, Gary L. Rogers, “A Framework for Federated Two-Factor Authentication Enabling Cost Effective Secure Access to Distributed Cyberinfrastructure”, Proceedings of the 1st Conference of the Extreme Science and Engineering Discovery Environment: Bridging from the eXtreme to the campus and beyond, article no 7, 2012.

[10] J. Katz, R. Ostrovsky, and M. Yung “Efficient and Secure Authenticated Key Exchange Using Weak Passwords”. Journal of the ACM, Vol. 57, issue 1, pp. 78–116, 2009.

[11] A. Groce, J. Katz “A New Framework For Efficient Password-based Authenticated Key Exchange”, In proceedings of 17th ACM Conference on Computer and Communications Security, pp. 516–525. ACM Press, New York, 2010.

[12] J. Katz and V. Vaikuntanathan “Password-based Authenticated Key Exchange Based on Lattices”, In Advances in Cryptology, volume 5912 of LNCS, pp. 636–652. Springer, 2009.

[13] M. Saeed, H.S. Shahhoseini, "APPMA - An Anti-Phishing Protocol with Mutual Authentication", Proceedings of the 15th IEEE Symposium on Computers and Communications (ISCC20 10), pp. 308-313, June. 2010.