Journal of Computer Science 6 (12): 1396-1405, 2010
ISSN 1549-3636

Integrated Quantum and Classical Key Scheme for Two Servers Password Authentication

[1]T.S.Thangavel and [2]A. Krishnan
[1]Department of MCA,
[2]Department of Electronics and Communication Engineering,
KS Rangasamy College of Technology, Tamilnadu, India

Abstract: Problem statement: Traditional user authentication system uses passwords for their secured accessibility in a central server, which is prone to attack by adversaries. The adversaries gain access to the contents of the user in attack prone servers. To overcome this problem, the multi-server systems were being proposed in which the user communicate in parallel with several or all of the servers for the purpose of authentication. Such system requires a large communication bandwidth and needs for synchronization at the user. **Approach:** Present an efficient two server user password authentication and reduce the usage of communication traffic and bandwidth consumption between the servers. Integration of quantum and classical key exchange model is deployed to safeguard user access security in large networks. The proposed work presented, a two server system, front end service server interacts directly to the user and the back end control server visible to the service server. The performance measure of the user password made for the transformed two long secrets held by both service and control server. Further the proposal applied quantum key distribution model along with classical key exchange in the two server authentication. Three-party Quantum key distribution used in this model, one with implicit user authentication and other with explicit mutual authentication, deployed for ecommerce buyer authentication in internet peer servers. **Results:** Effect of online and offline dictionary attacks prevailing in the single and multi-server systems are analyzed. The performance efficiency test carried out in terms success rate of authenticity for two server shows 35% better than single server. The performance of integrated Quantum Key Distribution (QKD) systems and classical public key model have shown experimentally better performance in terms of computational efficiency and security rounds (11% improvement) than traditional cryptic security model. **Conclusion:** With the results obtained it is concluded that intricate security principle of quantum theory and traditional public key model integration provides an improved security model for password authentication between the password exchanges of two servers.

Key words: Password authentication, two server, quantum key distribution, classical key exchange

INTRODUCTION

Most password-based user authentication systems place total trust on the authentication server where passwords or easily derived password verification data are stored in a central database. These systems could be easily compromised by offline dictionary attacks initiated at the server side. Compromise of the authentication server by either outsiders or insiders subjects all user passwords to exposure and may have serious problems. To overcome these problems in the single server system many of the systems has been proposed such as multi-server systems, public key cryptography and password systems, threshold password authentication systems, two server password authentication systems.

The proposed work continues the line of research on the two-server paradigm in (Wen *et al*., 2005; Nam *et al*., 2004), extend the model by imposing different levels of trust upon the two servers and adopt a very different method at the technical level in the protocol design. As a result, we propose a practical two-server password authentication and key exchange system that is secure against offline dictionary attacks by servers when they are controlled by adversaries. Moreover, the proposed system is particularly suitable for resource constrained users due to its efficiency in terms of both computation and communication. Computing exponential increase in power requires setting the bar always higher to secure password data transmissions in two server

Corresponding Author: T.S. Thangavel, Department of MCA, KS Rangasamy College of Technology, Tamilnadu, India

authentication. The ideal solution would transmit data in quantum bits, but truly quantum information processing may lie decades away. Therefore, several companies have focused on bringing one aspect of quantum communications to market Quantum Key Distribution (QKD), used to exchange secret keys that protect data during transmission.

The key distributed using quantum cryptography would be almost impossible to steal because QKD systems continually and randomly generate new private keys that both parties share automatically. A compromised key in a QKD system can only decrypt a small amount of encoded information because the private key may be changed every second or even continuously. To build up a secret key from a stream of single photons, each photon is encoded with a bit value of 0 or 1, typically by a photon in some superposition state, such as polarization. These photons are emitted by a conventional laser as pulses of light so dim that most pulses do not emit a photon. This approach ensures that few pulses contain more than one photon. Additional losses occur as photons travel through the fiber-optic line. In the end, only a small fraction of the received pulses actually contain a photon. However, this low yield is not problematic for QKD because only photons that reach the receiver are used. The key is generally encoded in either the polarization or the relative phase of the photon.

Key distribution protocols are used to facilitate sharing secret session keys between users on communication networks. By using these shared session keys, secure communication is possible on insecure public networks. However, various security problems exist in poorly designed key distribution protocol, for example, a malicious attacker may derive the session key from the key distribution process. A legitimate participant cannot ensure that the received session key is correct or fresh and a legitimate participant cannot confirm the identity of the other participant. Designing secure key distribution protocols in communication security is a top priority.

In some key distribution protocols, two users obtain a shared session key via a Trusted Center (TC). Since three parties (two users and one TC) are involved in session key negotiations, these protocols are called three-party key distribution protocols, as in contrast with two-party protocols where only the sender and receiver are involved in session key negotiations. In quantum cryptography, Quantum Key Distribution Protocols (QKDPs) employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. However, public discussions require additional communication rounds between a sender and receiver and cost precious qubits. By contrast, classical cryptography provides convenient techniques that enable efficient key verification and user authentication. These QKDP and classical cryptographic model motivates us to propose an integrated password communication between two server authentication systems. The proposal work in this study provides a pattern of integrating the classical key verification with the quantum mechanism employed in distributing the session key and provide efficient password sharing between the two servers to make the password authentication more robust.

Literature review: Public key techniques are absolutely necessary to make password systems secure against offline dictionary attacks, whereas the involvement of public key cryptosystems under a PKI (e.g., public key encryption and digital signature schemes) is not essential. There are two separate approaches to the development of secure password systems one is a combined use of a password and public key cryptosystem under a PKI and the other is a password only approach. In these systems, the use of public keys entails the deployment and maintenance of a PKI for public key certification and adds to users the burden of checking key validity. To eliminate this drawback, password-only protocols Password Authenticated Key Exchange (PAKE) have been extensively studied, e.g., (Bellovin and Merritt, 1992; 1993; Bellare *et al*., 2000). The PAKE protocols do not involve any public key cryptosystem under a PKI and therefore, are much more attractive for real-world applications. Any use of public key cryptosystem under a PKI in a password authentication system should be avoided since; otherwise, the benefits brought by the use of password would be counteracted to a great extent.

Most of the existing password systems were designed over a single server, where each user shares a password or some Password Verification Data (PVD) with a single authentication server (Bellovin and Merritt, 1992; 1993; Bellare *et al*., 2000). These systems are essentially intended to defeat offline dictionary attacks by outside attackers and assume that the sever is completely trusted in protecting the user password database. Unfortunately, attackers in practice take on a variety of forms, such as hackers, viruses, worms, accidents, mis-configurations and disgruntled system administrators. As a result, no security measures and precautions can guarantee that a system will never be penetrated. Once an authentication server is compromised, all the user passwords or PVD fall in the hands of the attackers, who are definitely effective in offline dictionary attacks against the user passwords. To

eliminate this single point of vulnerability inherent in the single-server systems, password systems based on multiple servers were proposed. The principle is distributing the password database as well as the authentication function to multiple servers so that an attacker is forced to compromise several servers to be successful in offline dictionary attacks.

The system in (Ford and Kaliski, 2000), believed to be the first multiserver password system, splits a password among multiple servers. However, the servers in (Ford and Kaliski, 2000) need to use public keys. An improved version of (Ford and Kaliski, 2000) was proposed in (Jablon, 2001), which eliminates the use of public keys by the servers. Further and more rigorous extensions were due to (Mackenzie *et al*., 2002), where the former built a t-out-of-n threshold PAKE protocol and provided a formal security proof under the random oracle model (Bellare *et al*., 2000) and the latter presented two provably secure threshold PAKE protocols under the standard model. While the protocols are theoretically significant, they have low efficiency and high operational overhead. In these multi-server password systems, either the servers are equally exposed to the users and a user has to communicate in parallel with several or all servers for authentication, or a gateway is introduced between the users and the servers.

Recently, (Brainard *et al*., 2003; Gottesman and Lo, 2003) proposed a two-server password system in which one server exposes itself to users and the other is hidden from the public. While this two-server setting is interesting, it is not a password-only system: Both servers need to have public keys to protect the communication channels from users to servers. As we have stressed earlier, this makes it difficult to fully enjoy the benefits of a password system. In addition, the system in (Gottesman and Lo, 2003) only performs unilateral authentication and relies on the Secure Socket Layer (SSL) to establish a session key between a user and the front-end server. Subsequently, (Yang *et al*., 2006; Bennett, 1992) extended and tailored this two-server system to the context of federated enterprises, where the back-end server is managed by an enterprise head quarter and each affiliating organization operates a front-end server.

The most common standard protocol for QKD is called BB84, after its inventors, IBM's Bennett and Brassard (1984). Invented in 1984, it uses a stream of single photons to transfer a cryptographic key between two parties, who can use it to encode and decode data transmitted using standard high-speed techniques. Right now, single photons allow real-time data transmissions only at low speed, typically 100 bits/s-a hundred millionths the speeds of today's fastest fiber-optic transmission systems. That explains why most companies have focused on commercializing QKD and not on data encryption. Slimen *et al*. (2007) study some conditions to stop BB84 protocol in the context of depolarizing channel and implement two types of eavesdropping strategy i.e., Intercept and Resend and Cloning Attack.

Polarization-based encoding works best for free-space communication systems rather than fiber-optic lines. Data are transmitted faster in free-space systems, but they cannot traverse the longer distances of fiber-optic links. Majeed *et al*. (2010) study presented a new protocol concept that allows the session and key generation on-site by independently applying a cascade of two hash functions on a random string of bits at the sender and receiver sides. This protocol however, required a reliable method of authentication. It employed an out-of-band authentication methodology based on quantum theory, which uses entangled pairs of photons. Dehmani *et al*. (2010) study was known if the number of the eavesdroppers and their angle of cloning act on the safety of information. The quantum error and the mutual information were calculated analytically and computed for arbitrary number of cloning attacks.

In classical cryptography, three-party key distribution protocols (Wen *et al*., 2005; Nam *et al*., 2004) utilize challenge response mechanisms (Stallings, 1998) or timestamps (Shirey, 2000) to prevent replay attacks (Bennett and Brassard, 1984), However, challenge response mechanisms require at least two communication rounds (Gottesman and Lo, 2003) between the TC and participants and the timestamp approach needs the assumption of clock synchronization which is not practical in distributed systems (due to the unpredictable nature of network delays and potential hostile attacks) (Bennett, 1992). Furthermore, classical cryptography cannot detect the existence of passive attacks (Hwang *et al*., 2007) such as eavesdropping. On the contrary, a quantum channel eliminates eavesdropping and, therefore, replay attacks. This fact can then be used to reduce the number of rounds of other protocols based on challenge-response mechanisms to a trusted center (and not only three-party authenticated key distribution protocols).

The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions and cannot provide any indication of eavesdropping or guarantee of key security. Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to

encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key. The proposal in this study integrates QKDP and classical model, in which TC and a participant synchronize their polarization bases according to a pre-shared secret key in the two server password authentication system. During the session key distribution, the pre-shared secret key together with a random string are used to produce another key encryption key to encipher the session key. A recipient will not receive the same polarization q-bits even if an identical session key is retransmitted.

MATERIALS AND METHODS

Two server password authentication systems: Three types of entities are involved in our system, i.e., users, a Service Server (SS) that is the public server in the two server model and a Control Server (CS) that is the back-end server. In this setting, users only communicate with SS and do not necessarily know CS. For the purpose of user authentication, a user U has a password which is transformed into two long secrets, which are held by SS and CS, respectively. Based on their respective shares, SS and CS together validate users during user login. CS is controlled by a passive adversary and SS is controlled by an active adversary in terms of offline dictionary attacks to user passwords, but they do not collude (otherwise, it equates the single-server model).

A passive adversary follows honest-but-curious behavior, that is, it honestly executes the protocol according to the protocol specification and does not modify data, but it eavesdrops on communication channels, collects protocol transcripts and tries to derive user passwords from the transcripts, moreover, when an passive adversary controls a server, it knows all internal states of knowledge known to the server, including its private key (if any) and the shares of user passwords. In contrast, an active adversary can act arbitrarily in order to uncover user passwords. Besides, we assume a secret communication channel between SS and CS for this basic protocol. This security model exploits the different levels of trust upon the two servers. This holds with respect to outside attackers. As far as inside attackers are concerned, justifications come from our application and generalization of the system to the architecture of a single control server supporting multiple service servers, where the control server affords and deserves enforcing more stringent security measurements against inside attackers. The back-end server is strictly passive and is not allowed to eavesdrop on communication channels, while CS in our setting is allowed for eavesdropping (Fig. 1).

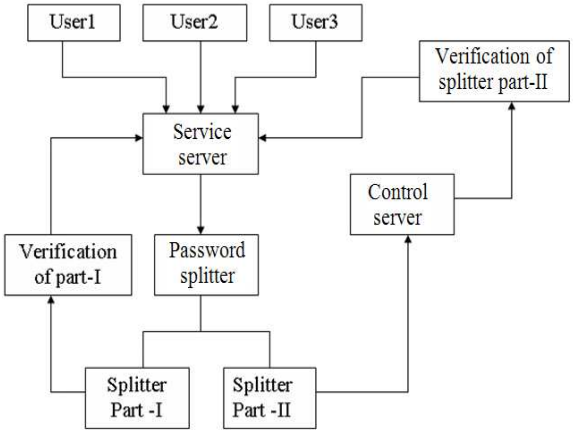

Fig. 1: Generalized two server architecture of a single control server with service server

Integrated quantum key distribution and classical key: With QKDP implicit user authentication that confidentiality is only possible for legitimate users and mutual authentication is achieved only after secure communication using the session key start. The proposed three-party QKDPs are executed purely in the quantum channel and this work does not consider errors caused by environmental noise. The proposed integrated QKDP and its classical security assumes that every participant shares a secret key with the TC in advance either by direct contact or by other ways. The integrated QKD and classical key model deployed in the two server password system are explained in the following phases.

Setup phase: Let A and B be two users who would like to establish a session key. KTU is the secret key shared between TC and user U. Bit sequence in KTU is treated as the measuring bases between user U and the TC. If $(K_{TV})_i = 0$, the basis D is chosen; otherwise, the basis R. Notice that $(K_{TV})_i$ denotes the ith bit of the secret key KTU.

Key distribution phase: The following describes the details of key distribution phase. Assume that the TC has been notified to start the 3AQKDP with A and B. TC and the users have to perform the 3AQKDP as follows:

Trusted center:

- The TC generates a random number rTA and a session key SK. TC then computes h (K_{TA}, r_{TA})ˆ $(SK||U_A||\ U_B)$ for A and, similarly, rTB and R_{TB}=h (K_{TB}, r_{TB}) $(SK||U_B||\ U_A)$ for B.

- The TC creates the qubits, QTA, based on (r_{TA} || $R_{TA)i}$ and ($K_{TA)i}$ for Alice where i = 2,....n and (r_{TA} || $R_{TA)i}$ denotes the i^{th} bit of the concatenation r_{TA} || R_{TA}
  - If (r_{TA} || $R_{TA)\ i\ =}$ 0, (K_{TA})i=0, then $(Q_{TA})_i$ is 1\√2 (|0›+|1›)
  - IF (r_{TA}|| R_{TA})i=1,(K_{TA})i=0, then $(Q_{TA})_i$ is 1\√2 (|0›-|1›)
  - If(r_{TA} ||R_{TA})i=0,(K_{TA})I =0, (K_{TA})i = 1, then (Q_{TA})i is (|0›)
  - If(r_{TA} ||R_{TA})i=1,(K_{TA})I =1, then (Q_{TA})i is | 1)

TC then sends QTA to A. TC creates qubits QTB in the same way for B.

Users:

- A measure the received qubits QTA depending on KTA. If $(KTA)_i$ = 0, then the qubit is measured based on the basis D; otherwise, the basis R. Similarly, B measures the receiving qubits QTB depending on KTB.
- Once A obtains the measuring results $r'_{TA}||R'_{TA}$, she then computes $SK'||U_A||U_B$ = h (K_{TA}, r'_{TA}) $R'_{TA'}$
- The session key SK^1 can be obtained and the values UA and UB can be verified. Similarly, B gains $r'_{TB}||R'_{TB}$ and computes$SK''||U_B||U_A$ = h (K_{TB}, r'_{TB}) $R'_{TB'}$

Then, B obtains the session key SK00 and checks the correctness of UB and UA. In item a of TC, the hash value is used to encipher the sequence. Therefore, a recipient will not receive the same polarization qubits even if an identical session key is retransmitted. This also makes an eavesdropper not be able to perform offline guessing attacks to guess the bases over the quantum channel and, thus, the secret key, KTA (or KTB), can be repeatedly used.

In item b of Users, only A (or B), with the secret key KTA (or KTB), is able to obtain $SK'||U_A||U_B$ (or $SK''||U_B||U_A$) by measuring the qubits QTA (or QTB) and computing:

h (K_{TA}, r'_{TA}) ^ R'_{TA} (or h (K_{TB}, ^ r'_{TB}) R'_{TB})

Hence, A (or B) alone can verify the correctness of the ID concatenation $U_A||U_B$ (or $U_B||U_A$) (Fig. 2).

Security proof of QKDP: A new primitive, Unbiased-Chosen Basis (UCB) assumption, based on the no cloning theorem is also proposed to facilitate the proof.

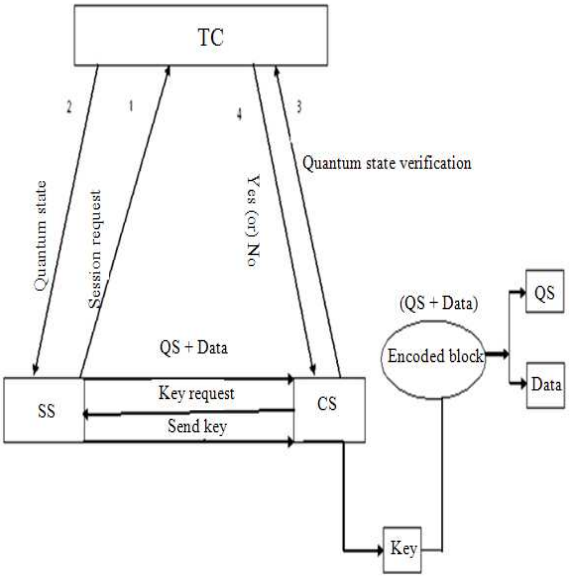

Fig. 2: Process Flow diagram for Quantum based two server password authentications

The UCB assumption describes that one can distinguish the polarization basis of an unknown quantum state with only a negligible probability.

Protocol participant: A fixed nonempty set of legitimate participants and a TC are supposed to take part in 3QKDP. A participant and TC may have many instances correlated in distinct and concurrent executions of 3QKDP.

Long-term secret key: Every participant and TC share one secret key KTU, which is a sufficient long random binary string. TC maintains a table to store for every participant. Besides, U saves KTU as his long-term secret key.

Instance states: A client instance U accepts when it gains sufficient information to compute a session key SK. It should be noted that the state of acceptance only appears in client instances. Moreover, a client instance U can accept at any time and only accept once.

Session Identifier (SID) and Partner Identifier (PID): The SID is used for a participant U to uniquely name his proceeding session. We define the SID for instance U in an execution of 3AQKDP. The PID names the participant with which a client instance affirms that it has just shared a session key SK. UA affirms that it has just shared SK with an instance of participant UB. It should be noted that the SID and PID are public and available to the adversary A.

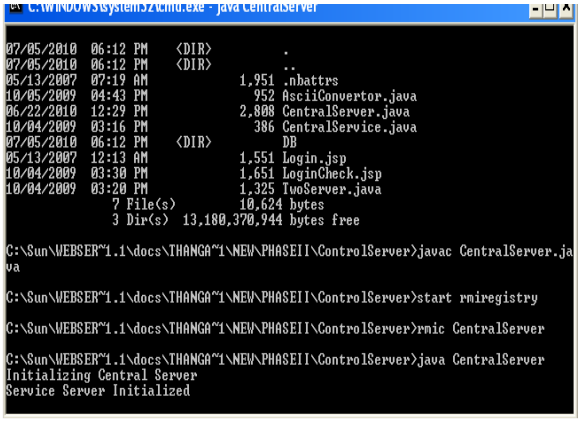

Fig. 3: Initialization of control server and service server

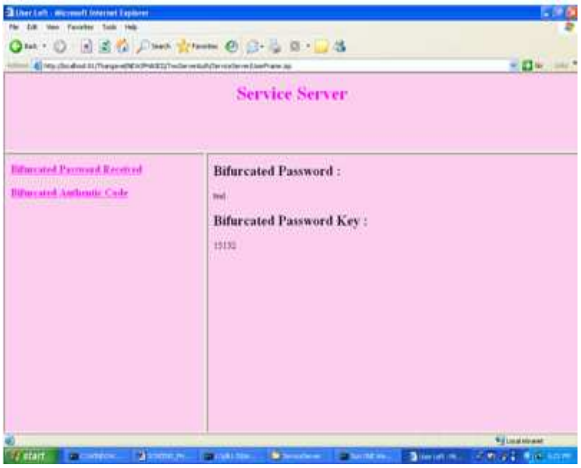

Fig. 4: Service server password authenticity

Adversary's queries: The queries, Initiate query, Send query, Reveal query, Hash query and Test query, represent the capabilities of adversary A.

Experimental evaluation: In our experimental implementation, a password is split into two random numbers. Therefore, a user can use the same password to register to different service servers; they connect either to distinct control servers or to the same control server. This is a highly desirable feature since it makes the system user friendly. The big inconvenience in the traditional password systems is that a user has to memorize different passwords for different applications. The system has no compatibility problem with the single-server model. The user contacts only the service server but both the control and service servers are responsible for the authentication of the user. The user has a password which is transformed into two long secrets which are held by service server and control server. Both the system using their respective shares Validate user during the login. The servers compute function to verify the user and finally a session key is being established between the user and service server for the confirmation of the user and the server. The service server which is an active adversary acts arbitrarily to uncover the passwords and could control the corruption of the password, the control server which is a passive adversary acts according to the protocol specification (Fig. 3).

In the offline dictionary attacks, where the successful logins between the user and the server is recorded by the intruder and it tries the passwords in the dictionary against login transcripts and this is overcome in the system by control server as passive adversary and service server as active adversary (Fig. 4). In the system, the communication and the computations are more efficient. The user can use the same password to register to different service server, the service server connect either to distinct control servers or to the same control server. This is a highly desirable feature since it makes the system user friendly. The system could be Adapted to any existing FTP and web applications that are available today by adding a control server to it where these are managed by the administrative domain.

The generalization as well as the applications of the two-server password system well support the underlying security model, in the sense that the enterprise headquarter naturally assume adequate funds and strong security expertise and, therefore, affords and is capable of maintaining a highly trustworthy control server against both inside attackers and outside attackers. Without the concern of a single point of vulnerability, affiliating organizations that operate service servers are offloaded to some extent from strict security management, so they can dedicate their limited expertise and resources to their core competencies and to enhancing service provision to the users. From the perspective of users, they are able to assume the higher creditability of the enterprise while engaging in business with individual affiliating organizations (Fig. 5).

In the implementation process of two servers for password exchange between the servers combines classical key with quantum key model. It achieves key verification and user authentication. It preserves a long term secret key between the TC and each user. It measures EPR pairs and reconstructs TC and a participant after one QKDP execution. It detects the existence of passive attacks like eavesdropping. It resists replay and passive attacks. The three-party QKDPs, with implicit user authentication is designed. It executes three-party QKDPs purely in the quantum channel.

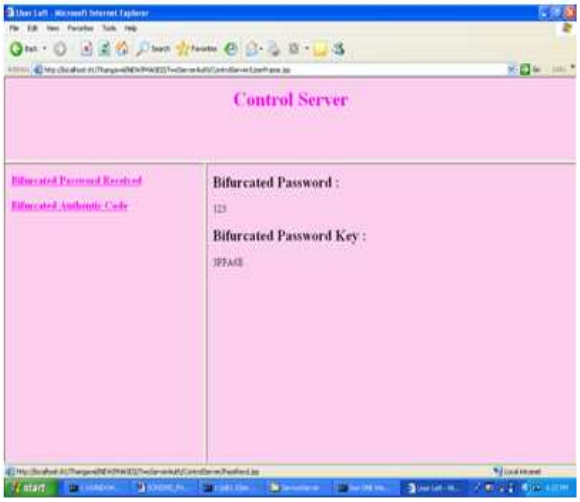

Fig. 5: Control server authentication

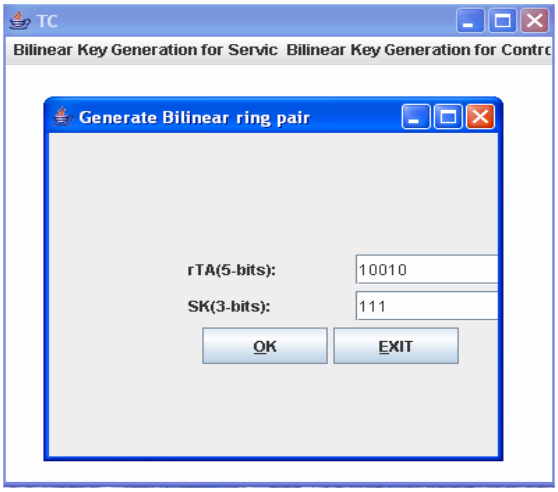

Fig. 6: Quantum generator for session keys

Every participant shares a secret key with the TC in either by direct contact or by other ways. The three parties QKDP allows explicit mutual authentication. The secret key pre-shared between the TC and a participant is long-term. The number of communication rounds is reduced to three. It integrates The advantages of both the classical and quantum cryptographies. Key distribution protocols facilitate sharing secret session keys between users on communication networks (Fig. 6). It provides secure communication on insecure public networks. A malicious attacker may derive the session key from the key distribution process. Designing secure key distribution protocols in security is a top priority. The three-party QKDP requires that the TC and each participant pre-share.

Fig. 7: Quantum ring signature

It provides secure communication on insecure public networks (Fig. 7). A malicious attacker may derive the session key from the key distribution process. Designing secure key distribution protocols in security is a top priority. The three-party QKDP requires that the TC and each participant pre-share.

RESULTS

Performance measure on two server authentication: The exponentiations dominate each party's computation overhead, the two server password authentication system only count the number of exponentiations as the computation performance. The digits before "/" denote the total number of exponentiations performed by each party and the digits following "/" denote the number of exponentiations that can be computed offline. One round is a one-way transmission of messages. The proposed two protocols demonstrate performance quite efficient in terms of both computation and communication to all parties. The Table 1 listed below indicates the computation performance in terms of time and success rate (number of rounds) of the two servers and single server password authentication. The better success rate for authentication in two server system (11% more) shown in Table 1 assures its efficiency.

Performance Issue on classical and quantum key on two servers: In the security proofs, the capability of an adversary is modeled by queries, which also represent the possible attacks performed by an adversary.

Table 1: Performance measure on two server and single server password authentication scheme

Scheme	Time of authenticity (m sec)	Success rate (%)
Two server password authentication	10	96
Single server	8	87

Table 2: Comparison of proposed quantum and classical to individualized classical and quantum key models

Performance metrics	Proposed quantum key and classical	Quantum model	Classical key model
Pre-shared secret key	Longer duration	Sampling pair instances	Longer duration
Communication round	2	5	3
Quantum channel	Yes	Yes	No
Clock synchronization	No	No	No
Vulnerable to passive attack	No	No	No
Security proof	Yes	No	No

However, since the online guessing attack in which an adversary guesses the possible secret and judges the correctness of the guess by the execution result of the protocols cannot be avoided in existing key distribution protocols, as no proper queries have been adopted to model this attack in existing security proofs. An online guessing attack is not modeled in the security proofs of older systems. The online guessing attack can occur when an adversary performs an intercept-resend attack on one qubit at a time (by say starting from the first qubit) over the qubit sequence sent from TC. The adversary intercepts the qubit sequence and measures the first qubit using an arbitrary basis. Then, the adversary produces a qubit according to the measurement result to replace the first qubit of the intercepted sequence and then resends the new qubit sequence to the participant.

The adversary then observes the participant reaction. In the case of a negative reaction (25% probability), the adversary immediately knows the correct basis; otherwise, the adversary has to repeat the process on the same bit in the next executions of protocols. Table 2 shows the performance improvement of proposed Quantum and classical key password authentication model with other tradition cryptographic techniques in terms of low communication round (35%) and longer duration of pre-shared key (25%). The security proof is instantiated in the proposed Quantum and classical key authentication system.

DISCUSSION

With two-server password system, single point of vulnerability, is totally eliminated. Without compromising both servers, no attacker can find user passwords through offline dictionary attacks. The control server being isolated from the public, the chance for it being attacked is substantially minimized, thereby increasing the security of the overall system. The system is also resilient to offline dictionary attacks by outside attackers. This allows users to use easy to remember passwords and still have strong authentication and key exchange. The system has no compatibility problem with the single-server model. The generalization of the two-server password system well supports the underlying security model. In reality, adversaries take on a variety of forms and no security measures and precautions can guarantee that a system will never be penetrated. By avoiding a single point of vulnerability, it gives a system more time to react to attacks. The password-based authentication and key exchange system that is built upon a novel two-server model, where only one server communicates to users while the other server stays transparent to the public. Compared with previous solutions, our system possesses many advantages, such as the elimination of a single point of vulnerability, avoidance of PKI and high efficiency.

Among classical three-party key distribution protocols focuses on the low bounds of communication rounds of three-party key distribution protocols, such as the low bound of timestamp-based protocols and the low bound of nonce-based protocols. Therefore, this project evaluates the communication rounds with the proposed protocol. The three parties QKDP allows explicit mutual authentication is chosen for comparison. The three-party QKDP avoids passive and replay attacks due to the quantum phenomena. Pre-shared key pair is used between the TC and participants to prevent man-in-the-middle attacks. However, not only must participants perform public discussions to verify the correctness of the session key, but the pre-shared pairs must be reconstructed for each session. The classical three-party key distribution protocols utilize challenge-response mechanisms or timestamps to prevent replay attacks. However, challenge-response mechanisms require at least two communication rounds between the TC and participants and clock synchronization is impractical. Furthermore, classical cryptography cannot detect passive attacks such as eavesdropping. By integrating the advantages of both classical and quantum cryptographies, the proposed model avoid man-in-the-middle, passive and replay attacks. Furthermore, since the challenge-response mechanism is no longer necessary, the number of communication rounds is reduced to three, the same as the low bound in the timestamp-based protocol and one fewer than the low bound of the challenge-response protocol.

CONCLUSION

The two-server password authentication architecture presented has control server and service server. The control server is controlled by a passive adversary while the service server is controlled by an active adversary. A single point of vulnerability, as in the existing password systems, is totally eliminated. Work with today's peer to peer internet servers for ecommerce applications (nearly 96% success rate).

The two server authentication utilizes the advantages of combining classical key with quantum key model to improve the performance of password sharing between the control server and service server. Compared with classical three-party key distribution protocols, the proposed one easily resists replay and passive attacks. Compared with other QKDPs, the proposed schemes efficiently achieve key verification and user authentication and preserve a long term secret key between the TC and each user. The keys are stored and managed within key stores, placed in nodes and not within QKD devices or within the machines running endpoint secure applications. This design choice allows to manage keys over a dedicated global network (the network of secrets) composed of key stores linked together with classical channels. The proposed integrated key model had 35% fewer communication rounds than other protocols. By combining the advantages of classical cryptography with quantum cryptography, this work presents a new direction in designing QKDPs. The future work may analyze other machine learning authentication model for the two server password authentication system.

REFERENCES

Majeed, M.M.A., K.A.S A1-Khateeb, M.R. Wahiddin and M.M. Saeb, 2010. Protocol of secure key distribution using hash functions and quantum authenticated channels key distribution process six-state quantum protocol. J. Comput. Sci., 6: 1094-1100. http://www.scipub.org/fulltext/jcs/jcs6101094-1100.pdf

Bellare, M., D. Point cheval and P. Rogaway, 2000. Authenticated key exchange secure against dictionary attacks. Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques, May 14-18, Springer-Verlag, Bruges, Belgium, pp: 139-155. http://portal.acm.org/citation.cfm?id=1756185

Bellovin, S.M. and M. Merritt, 1992. Encrypted key exchange: Password based protocols secure against dictionary attacks. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, May 4-6, IEEE Xplore Press, Oakland, CA., USA., pp: 72-84. DOI: 10.1109/RISP.1992.213269

Bellovin, S.M. and M. Merritt, 1993. Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise. Proceeding of the ACM Conference Computer and Communications Security, Nov. 3-5, ACM Press, Fairfax, Virginia, United States, pp: 244-250. DOI: 10.1145/168588.168618

Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing. Proc. IEEE International Conference on Computers, Systems and Signal Processing, (CSSp'84), IEEE Computer Society, Bangalore, India, pp: 175-179. http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf

Bennett, C.H., 1992. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 68: 3121- 3124. PMID: 10045619

Brainard, J., A. Juels, B. Kaliski and M. Szydlo, 2003. A new two server approach for authentication with short secrets. Proceedings of the 12th conference on USENIX Security Symposium, Aug. 4-8, USENIX Association, Washington, DC., pp: 14-14. http://portal.acm.org/citation.cfm?id=1251367

Dehmani, M., H. Ez-Zahraouy and A. Benyoussef, 2010. Quantum cryptography with several cloning attacks. J. Comput. Sci., 6: 684-688. http://www.scipub.org/fulltext/jcs/jcs67684-688.pdf

Ford, W. and B.S. Kaliski Jr., 2000. Server-assisted generation of a strong secret from a password. Proceedings of the IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, June 14-16, IEEE Xplore Press, Gaithersburg, MD., USA., pp: 176-180. DOI: 10.1109/ENABL.2000.883724

Gottesman, D. and H.K. Lo, 2003. Proof of security of quantum key distribution with two-way classical communications. IEEE Trans. Inform. Theory, 49: 457-475. DOI: 10.1109/TIT.2002.807289

Hwang, T., K.C. Lee and C.M. Li, 2007. Provably secure three party authenticated quantum key distribution protocols. IEEE Trans. Depend. Secure Comput., 4: 71-80. DOI: 10.1109/TDSC.2007.13

Jablon, D.P., 2001. Password authentication using multiple servers. Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA, Apr. 8-12, Springer-Verlag, London, UK., pp. 344-360. http://portal.acm.org/citation.cfm?id=680777

MacKenzie, P., T. Shrimpton and M. Jakobsson, 2002. Threshold password-authenticated key exchange. Lecture Notes Comput. Sci., 2442: 385-400. DOI: 10.1007/3-540-45708-9_25

Nam, J., S. Cho, S. Kim and D. Won, 2004. Simple and efficient group key agreement based on factoring. Lecture Notes Comput. Sci., 3043: 645-654. DOI: 10.1007/978-3-540-24707-4_76

Slimen, I.B., O. Trabelsi, H. Rezig, R. Bouallègue and A. Bouallègue, 2007. Stop conditions of BB84 protocol via a depolarizing channel (quantum cryptography). J. Comput. Sci., 3: 424-429. http://www.scipub.org/fulltext/jcs/jcs36424-429.pdf

Shirey, R., 2000. Internet security glossary. Network Working Group. http://www.ietf.org/rfc/rfc2828.txt

Stallings, W., 1998. Cryptography and network security: Principles and Practice. 2nd Edn., Prentice Hall, New York, ISBN: 10: 0138690170, pp: 569.

Wen, H.A., T.F. Lee and T. Hwang, 2005. A provably secure three- party password-based authenticated key exchange protocol using Weil pairing. IEE Proc. Commun., 152: 138-143. DOI: 10.1049/ip-com:20045087

Yang, Y., R.H. Deng and F. Bao, 2006. A practical Password-based two server authentication and key Exchange system. IEEE Trans. Secure Depend. Comput., 3: 105-114. DOI: 10.1109/TDSC.2006.16