Improving VPN Security Performance Based on One-Time Password Technique Using Quantum Keys

Montida Pattaranantakul*, Paramin Sangwongngam* and Keattisak Sripimanwat*

Abstract

Network encryption technology has become an essential factor for organizational security. Virtual Private Network (VPN) or VPN encryption technology is the most popular technique used to prevent unauthorized users access to private network. This technique normally relies on mathematical function in order to generate periodic key. As a result, it may decrease security performance and vulnerable system, if high performance computing make rapid progress to reverse mathematical calculation to find out the next secret key pattern.The main contribution of this paper emphasizes on improving VPN performance by adopting quantum keys as a seed value into one-time password technique to encompasses the whole process of authentication, data confidentiality and security key management methodology in order to protect against eavesdroppers during data transmission over insecure network.

Keyword: Quantum Keys, One-Time-Password , Virtual Private Network.

1. Introduction

The evolution of information technologies has been growing rapidly in order to meet human communication need today. In which the security of data transmission has always been concerned to transfer information from sender to receiver over internet channel in a secure manner. Addressing on the network security issues are the main priority concern to protect against unauthorized users since the security technique should also cover data integrity, confidentiality, authorization and further non-repudiation services.

The lack of adequate knowledge with well known understanding of software architecture and security engineering leads to security vulnerabilities due to the eavesdroppers might be able to gain information by monitoring the transmission for pattern of communication, the capability to detect data packets during transmission over internet, or enable to access information within private data storage that may lead to the occurance of data loss and data corruption. This is the critical factor cause to new threads arise and may effect business objectives change. In terms of worst case scenario this will definitely affect to organizational stability, business opportunities and then may become a national security threat. For this reason, many organizations have to pay attention in order to find out the way to protect their information from eavesdroppers based on security technology solutions that agile enough to adapt itself and combat with an existing threats due to security breach.

Therefore, data reliability and security protection are primary concern for information exchange through unprotected network connections in order to verify user, since only an authorized user can entrance and ability to govern the resource access, while encryption technology is also required for further data protection.

Presently, there are several types of cryptography [1] that have been used to achieve comprehensive data protection based on proven standard technology due to it is the most important aspect of network and communication security which provide as a basic building block for computer security. According end to end security encryption typically rely on application layer closest to the end user thus only data is encrypted. While, network security encryption where IPsec comes into play to encompasses confidentiality area by encapsulating security payload in both transport mode operation and tunnel mode operation through this type of encryption the entire IP packet including headers and payload are encrypted. IPsec encryption based on Virtual Private Network technology [2] presents an alternative approach for network encryption since it fully provide trusted collaboration framwork to be able to communicate each other over private network. Nevertheless, user authentication mechanism, cryptographic algorithms, key exchange procedure and traffic selector information need to be configured and maintained among two endpoints in order to establish VPN trusted tunnel before data transmission begins.

Although, the widespread usage of classical VPN can improve data transfer rate with maximum throughput, minimum delay and well guranteed on non bottleneck occurrence due to every communication routes is built the shortest part communication with independent IPsec to improve elastic traffic performance. In contrast, key exchange procedure during VPN setup is still a major hurdle process of vulnerability, if either secret key get trapped or key pattern broken up. In addition, most of the random numbers have been used as the secret keys into cryptographic algorithms derived based on mathematical functions. This key generation manner is the one of the potential security vulnerabilities for data communications when computer technology become a high performance computing such make rapid progress to reverse mathematical calculation to find out secret key value.

** Optical and Quantum Communications Laboratory, National Electronics and Computer Technology Center, Pathumthani, Thailand.*

One-time password mechanism [3] using quantum keys as a seed value into hash function can be solved a traditional VPN security problem in which it can eliminate the spoofing attack caused by an eavesdropper has successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. The main contribution of this paper emphasizes on improving VPN security performance that adopted one-time password technique to generate corresponding once symmetric key upon a time for further VPN tunnel establishment as using quantum keys as a seed value. Thus, the two endpoints are typically authenticated themselves in a secure manner process which rely on confidential protection. While, quantum keys have been proposed to avoid repeating the same password several times due to traditional password creation was derived from mathematical calculation may lead to system vulnerabilities. Addressing on quantum keys bring perfectly security enhancement of password generation due to the beauty of quantum key distribution (QKD) [4] promises to revolutionize secure communication by providing security based on the fundamental laws of physics [5], instead of the current state of mathematical algorithms or computing technology [6].

This paper is organized as follows. Section 2 an overview of VPN architecture and mechanism where the theory has been applied upon design processes, technical solution and implementation approach. Section 3 gives a details view to design a VPN security architecture for further VPN tunnel establishment. Since, the entire information are transferred through this corresponded tunnel regarding to the authorization control. Section 4 gives a comparison and analysis of an existing VPN security method and proposed challenge idea will be disscussed. Finally, some concluding remarks and future works are mentioned in section 5.

2. VPN Architecture and Mechanism

Fortunately, there are several network encryption technologies that have been used to protect private information from eavesdroppers over insecure network. At the current VPN encryption technology has become an attractive choice and widely used for protection against network security attacks.

VPN encryption mechanism normally process as Client/Server operation in order to establish a direct tunnel between source address and destination address while the virtual private network is built up. All data packets are consecutively passed over VPN tunnel. Due to the merit of VPN technology can reduce network cost consumption cause from physical leased lines, so that the users can exchange such private information with high data protection and trust. In addition, VPN architecture is encompassed based on authentication [7], confidentiality and key management functional areas. According to authentication service is typically used to control the users when entrance into the system, only authorized user able to do forward to encrypt a tunnel during process of VPN connection start up. As the result, the authentication header is inserted between the original IP header and the new IP header shown in Figure 1. Next, confidentiality service provide message encryption to prevent eavesdropping by third parties. Finally, Key management service has been concerned in order to handle a model of secure keys exchange protocol.

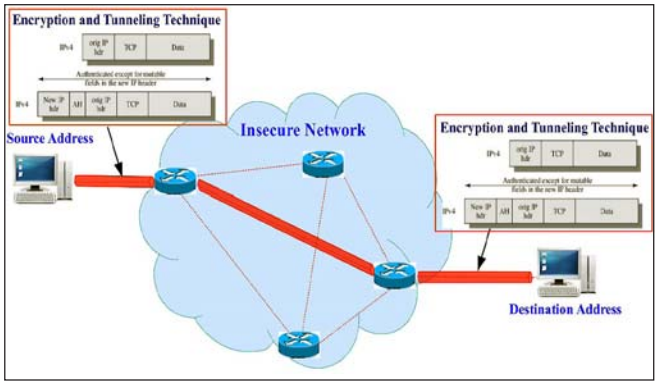

***Figure 1**. The scenario of VPN encryption techniques*

3. Designing a new VPN security architecture

Basically, VPN tunnel encryption can be classified into two main methods. There are public key encryption method and symmetric key encryption method. The paper has been addressed only on symmetric key encryption that adopted one-time password mechanism such one time key encryption is used over time when VPN connection start up and finally destroy the keys when disconnection. Since, the one-time keys is originated from quantum keys as a seed value into hash function [8][9]. The mechanism is covered both user authentication process and tunnel establishment in order to prevent against data integrity problem. Therefore, the overview of VPN security architecture are mainly divided into three major modules.

3.1 User Registration Module

In order to improve VPN security performance such a connection, user registration module must required for either first time entry or password is expired. This module will be activated when new users enroll to the system to request legitimate password. Figure 2 shows user registration procedure that each individual process are explained as follows. The result of this step will indicate the corresponding password to those users. Such the password will be essentail used in the step of user authentication and negotiation.

1) New user login/ Password expired: This case can be occurred with two reasons. When new users who need to register into the server want to ask for the legitimate password, or their password are expired due to it exceeded the password life time. So, the registration phase will be activated to regenerated a new password.

2) Request for the password: The users transfer his/her identity information including an official name, identification number/passport number, date of birth, address and so on to the server in order to request a legitimate password. The correspondence user information will be stored in the user right database for further reference.

3) Random a unique 10 digit code: Generate a legitimate password based on random selection from Quantum Key Distribution (QKD) device.

4) Store username and password: The username and the legitimate password created from QKD device called quantum keys are fabricated into the basic form of hash function. Therefore, only the corresponding username and the

password hash value will be stored in the user right database wherewith the server does not also know the exact password value.

5) Transfer the legitimate password: The legitimate password will transfer back to the corresponding user across trusted channel to avoid password attack.

6) Treated as confidential information: Thus, the legitimate pasword will be used to verify user him/herself in authentication phase whether the user is authorized to perform VPN establishment.

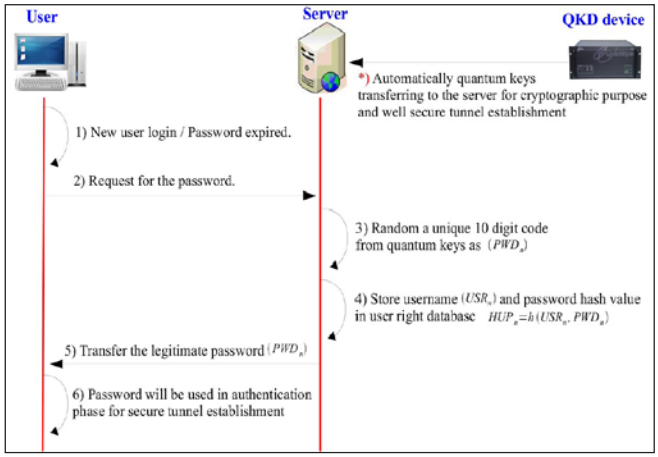

***Figure 2**. User rigistration phase*

3.2 User Authentication Mechanism Module

User authentication procedure maintains high level of security through one-site checking. Before creating VPN tunnel, the users must verify themselves with the server by logging into the system with corresponding username and password when the users had been registered at the beginning of the registration phase. The stages of the process are similar to S/key authentication mechanism [10] shown in the Figure. 3. Hence, only the authorized user can go forward to create a secure VPN tunnel. The user authentication procedures can be explained as follows.

1) Logging into the system: After user registration phase finished, if the user wish to create secure VPN tunnel then authentication phase will proceed respectively. Since, the username and the password must register to the server for the authentication whether a user is authorized to perform a task.

2) Received username and password: At the start service mode begins, the server is waiting for user call. When the server gets the signal of user authentication, the username and the password will be temporal stored as the input of hash function.

3) Password expiration checking: This function will examine the password life cycle due to the password life time is exceeded than the permitted allowance which may decrease security performance. Therefore, password expiration checking procedure was introduced to avoid against password attack.

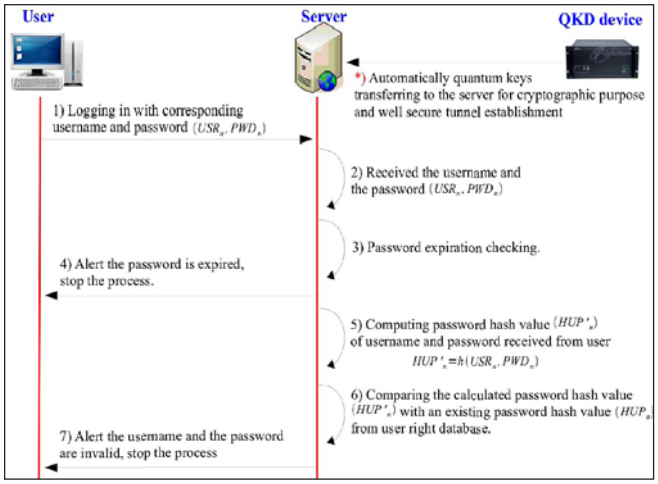

***Figure 3**. User authentication phase*

4) Alert the password is expired: The password expiration result will be sent back to the corresponding user to notify whether password is valid or invalid. Invalid password result will return back to user registration phase in order to re-enrollment again, otherwise continue to the next procedure.

5) Computing password hash value: Computing the password hash value with the corresponding username and the password obtained from the previous process.

6) Comparing with an existing password hash value: Comparing the calcuated password hash valule with an existing password hash value in the user right database.

7) Alert username and password are invalid: The comparision result will acknowledgement back to the corresponding user such only authorized user able to continue performing VPN tunnel establishment .

3.3 VPN Tunnel Establishment Based On One-Time

In Password Mechanism Module, the proposed technique has adopted two unique features of one-time password mechanism and the promise of quantum key exchange. One-time password mechanism which each password is used only once upon a time and frequenly updated when a new connection has been established to eliminate the possibility of attack that may come from replay attack, spoofing attack or birthday attack. In addition, using one-time password mechanism based on hash chain are more elegant design and attractive properties such to be able to reach the high security performace.

While, applying the quantum keys as a seed value into a hash function will improve more efficiency and security against the system. The fascination of quantum technology that uses polarization property to ensure the transmistted keys. In which the keys cannot be trapped by eavesdroppers due to it may affect the key error rate more than a certain threshold vulue.

Moreover, the VPN tunnel establishment based on one-time password mechanism using quantum keys as a seed input to the hash function can be illustrated in the Figure 4. Such, creating a hash chain value is called the response value which it is computed from both the password phase, the

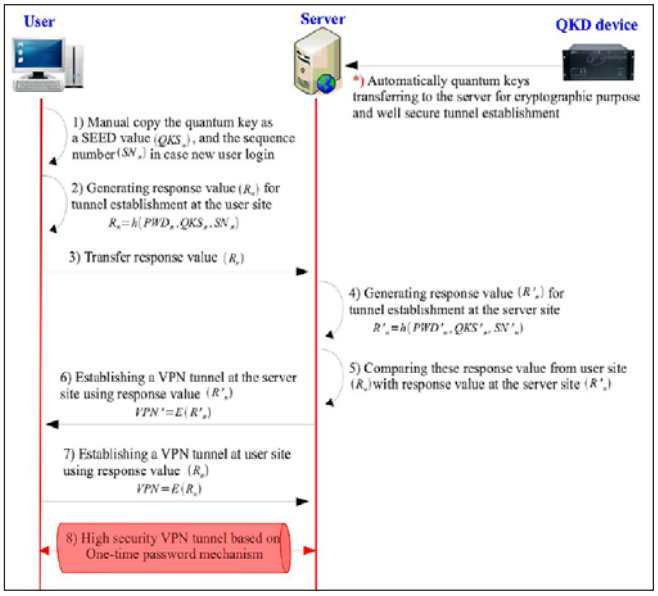

***Figure 4**. VPN tunnel establishment phase*

quantum seed and the sequence number in order to establish high secure VPN tunnel. The process get started by reversing from the N^{th} element of the hash chain which referred from the sequence number in order to identify the current position of response value to be used and finally destroy after the VPN tunnel get disconnected. The procedure of creating high secure VPN tunnel are explained as follows.

1) Manual copy quantum key and sequence number: At the first time of VPN tunnel setting up, the quantum keys as consider as a seed value (QKS) which it was generated from Quantum Random Number Generator (QRNG) [11]. While, the sequence number (SN) is used to indicate the hashing order. Both of the two values are manually distributed to the user in such a way that to prevent being attacked. These key values will be the input of the hash function. For any further reestablished a VPN tunnel, this procedure will not be proceeded until the sequence number become zero.

2) Generate response value at user site: The user needs to complete the legitimate password acquired from the registration phase, the quantum key seed and the sequence number which is allocated from the server to each particular user such the inputs of hash function. Thus, an intermediate response value will be generated after finish its processing.

3) Transfer response value: The response value from the proper user site has been typically transmitted to the server in order to compare identities.

4) Generating response value at the server site: The server will also generate its response value based on the relevant user information that had been stored in a user right database.

5) Comparing two response values: These the two response values are compared with each other. Matching result will be considered as a symmetric key encryption for VPN tunnel establishment. According to this procedure is very attractive approach due to it offer high security protection without performing a key exchange over insecure network.

6) Establishing a VPN tunnel at the server site: If the two response values match, then go forward to establish a tunnel. Creating a one site tunnel for secure connections the server will assigns virtual IP address to the user from local virtual subnet.

7) Establishing a VPN tunnel at user site: The procedure for setting up VPN tunnel at user site are similar to the one at server site via extenal network interface.

8) Site-to-Site VPN tunnel: The user and the server use virtual network interface to maintain a encrypted virtual tunnel. The entire information such as the actual user data, the ultimate source and the destination address are carried as a payload with authentication header. Lastly, the virtual IP address is inserted to the packet before transmission.

4. Comparison and Analysis

This paper performs a comparison and analysis for the qualities of VPN connection using the different types of encryption techniques including the term of symmetric key encryption, public key encryption. Finally, the proposed system has been distinguished since the technique adopted from classical encryption technique with added more features of one-time password mechanism and quantum keys to improve security performance.

4.1 Key Pattern Generator And Its Properites

Most of high secure communications are belonged with two important key factors. One is the quality of random number using as a cryptographic key and the two is the complexity of encryption algorithms. The algorithm will produce a different output that depend on the specific key being used at the time. Addressing to the sources of key generator can be produced into two different ways. Pseudo random number generators is the algorithms uses regarding to the mathematical functions, or simply precalculated tables in order to produce the sequence numbers to appear as the random value based on periodic pattern since this technique may decrease the securiy key performance due to it is feasible to find the next value of key generation from the existed pattern. As a result, it can taking to the risks associated with the use of pseudo random numbers to produce a key into cryptography systems. The proposed technique has applied the challenge of quantum keys to be used in both password generation and VPN tunneling encryption. Concerning with the performance of quantum keys which is actually true random number generator based on quantum physics use. The fact that subatomic particles appear to behave randomly in circumstances which difficult to find out the key value. The probability of key generation based on aperiodic pattern along with the random distribution scheme can increase the quality of key performance as great as the data security enhancement.

4.2 Security Key Protection and Performance

One of the best characteristics of QKD technology offers a promising unbreakable way to secure communications. In the way that eavesdroppers are trying to attempt to intercept the quantum keys during the key exchange state is detectable by introducing an abnormal Quantum Bit Error Rate (QBER). The result may occur error rate more than a certain threshold value due to unavoidable disturbance including an imperfect system configuration, noise or eavesdropper across to the quantum

***Table 1**. Performance comparison of differential evolution techniques.*

Features	*Properties of VPN Connections*		
	Symmetric Key Encryption	***Public Key Encryption***	***Proposed Mechanism***
Key Pattern Generator	Periodic pettern based on mathematical functions	Periodic pettern based on mathematical functions	Random pettern based on quantum phenomenon
Key Properties	Pseudo random number based on mathematical functions	Pseudo random number based on mathematical functions	True random number based on quantum physics laws
Security Key Protection and Performance	Not provided any key protection mechanism	Not provided any key protection mechanism	Quantum Bit Error Rate (QBER) ratio
Key Exchange Protocol	Secret key exchange with one classical link communication	Public key exchange protocol with one classical link communication	Secret key exchange with two data link communition (Quantum channel and classical channel)
Mechanism Used	Secret key encryption	Public and private key encryption	Secret key encryption based on one-time password mechanism using quantum keys

channel and secret key generation with respect to time. Hence, the exploitation of quantum mechanics offer the perfectly secure communications.

4.3 Key Exchange Protocol

In general QKD technology describes the process of using quantum communication to establish a shared secret key between two parties which is similar to the secret key exchange architecture. The proposed technique has applied the quantum keys acquired from the QKD system and then take forward to distribute to each responding user in secure mode. When the server received the signaling such password request, a partial key is dedicated to each user for further identifying as well as some of the quantum keys has assigned as a seed value into hash function in order to generate a particular secret key use to establish a VPN tunnel for secure data communications.

4.4 Mechanism Used

The promising of VPN encryption technology leads to client/server confidentiality. Thus, the proposed technique is focused to establish the high secure VPN tunnel such the technique has applied the challenges of one-time password mechanism as using the beauty of quantum keys, the sequential number and the user secret password in order to produce the response value as a specific symmetric key. This symmetric key will be used once at a particular time and later destroyed after the VPN tunnel disconnected. In addition, new symmetric key will be periodically change along the one-way hash function properites which able to enhance data confidentiality and network security protection.

5. Conclusion and Future Work

Improving VPN security performance based on onetime password technique using quantum keys presents a new trend mechanism to protect against data snooping from eavesdroppers when data is transmitted over insecure network. The proposed technique has offered three main procedures of concern, user registration stage, user authentication stage and VPN tunnel establishment stage in order to figure out various vulnerabilities and attacks. User registration stage performs key generation process to create the secret password to the responding user for further authentication. Since, the secret password is truly random numbers based on QKD technology which typically rely on the beauty of key exchange method to protect against eavesdroppers rather than the pseudo random numbers derived from mathematical functions due to the probability of brute force attacks may occur, if the password can be guessed. User authentication stage provides the legitimate users with transparent authentication in such a way that managing and monitoring access to private resources. Morover, the password life cycle management and hash functions have also been applied to solve security vulnerabilities. Finally, VPN tunnel establishment stage based on one-time password mechanism bring to an attractive approach to build up the highest security of virtual private network thus the particular key will be used only once and destroy. In addition, the challenges of the proposed mechanism is a part of project of high efficiency key management methodology for advanced communication services (a pilot study for video conferencing system) under the user authentication and VPN establishment phase in order to prevent against unauthorized access into the restricted network and the illegal resources before distributing the quantum keys for further along secure video conferencing and any data communications services as considering the data protection and network security are the main priority for IT organization need to be concerned.

6. Acknowledgment

The authors would like to thank Dr. Weetit Wanalertlak for the invaluable feedback and the technical support to achieve such the supreme excellence and the perfection of research paper. While, the authors would like to thank NECTEC steering committee for research support funding with a great valuable opportunity for team to introduces the new challenges of data protection as well as to improve data reliability over insecure network. Finally, the authors would like to thank Mr. Sakdinan Jantarachote and all staffs of Optical and Quantum Communications Laboratory (OQC) for all kind support and encouragement.

7. References

[1] William Stallings, *Cryptography and Network Security Principles and Practices*, Fourth Edition, November 2005.

[2] Kazunori Ishimura, Toshihiko Tamura, Shiro Mizuno, Haruki Sato and Tomoharu Motono, "Dynamic IP-VPN architectuire with secure IP tunnels," *Information and Telecommunication Techonologies*, pp. 1-5, June 2010.

[3] Young Sil Lee, Hyo Taek Lim and Hoon Jae Lee, "A Study on Efficient OTP Generation using Stream with Random Digit,"*Internatinal Conference on Advanced Communication Technology 2010*, Vol. 2, pp. 1670-1675.

[4] W. Heisenberg, "Uber den anschaulichen Inhalt der quantenheoretischen Kinematik und Mechanik" In: Zeitschrift fur Physik, Vol.43, pp. 172-198, 1927.

[5] W.K. Wootters and W.H. Zurek, "A Single Quantum Cannot be Cloned," *Nature*, Vol.299, pp. 802-803, 1982.

[6] Erica Klarreich, "Quantum Cryptography: Can You Keep a Secret", *Nature*, Vol.418, pp.270-272, July 18, 2002.

[7] Hyun Chul Kim, Hong Woo Lee, Kyung Seok Lee, Moon Seong Jun, "A Design of One-Time Password Mechanism using Public Key Infrastructure," *Fourth Internatinal Conference on Network Computing and Advanced Information Management*, pp. 18-24, 2008.

[8] Harshvardhan Tiwari, "Cryptographic Hash Function: An Elevated View", *European Journal of Scientific Researchm*,Vol.43, No.4, pp. 452-465, 2010.

[9] Peiyue Li, Yongxin Sui, Huaijiang Yang and Peiyue Li "The Parallel Computation in One-Way Hash Function Designing," *International Conference on Computer, Mechatronics, Control and Electronic Engineering*, pp.189-192, Aug 2010.

[10] C.J.Mitchell and L. Chen, "Comments on the S/KEY user authentication scheme,"*ACM Operating Systems Review*,| Vol.30, No. 4 , pp. 12-16, 1996.

[11] ID Quantique White Paper, "Random Number Generation Using Quantum Physics", Version 3.0, April 2010.