Chapter 12

A Quantum Secure Entity Authentication Protocol Design for Network Security

Surjit Paul
https://orcid.org/0000-0002-2213-1752
IIT Kharagpur, Kharagpur, India

Sanjay Kumar
NIT Jamshedpur, Jamshedpur, India

Rajiv Ranjan Suman
NIT Jamshedpur, Jamshedpur, India

ABSTRACT

Authentication is one of the significant issues for all kinds of network communications. Most of the authentication protocols designed and implemented so far for entity authentication are based on classical cryptographic techniques to prevent themselves from different types of attacks. These protocols use either password or challenge for authentication. In this article, the design of the proposed quantum secure entity authentication protocol is shown. The proposed protocol is based on the challenge response method. Due to quantum computer capability to break mathematical complexity-based cryptographic techniques, the proposed protocol uses the one-time pad (OTP) to secure itself from attacks, i.e., eavesdropping, reply attack, password guessing attack, man-in-the-middle attack, brute-force attack, quantum computer attack, etc. Security of the proposed protocol was analyzed, and it shows that the proposed protocol may prevent itself from different types of attacks. Further, analysis for quantum Secure was carried out. From the analysis, it is found that if the OTP key is truly random and cannot be reused, then a computer with infinite capacity or quantum computer cannot break the encrypted challenge and response. The proposed protocol may be used for entity authentication for the client, server, process, and user.

DOI: 10.4018/978-1-7998-8593-1.ch012

1. INTRODUCTION

Due to the extensive use of information and communication technology, protecting resources from unauthorized users are essential nowadays. Authentication plays a vital role in protecting resources from malicious attempts by attackers to breach the security. Most organizations depend on the security measures at the perimeter of network using firewalls, in order to secure their information technology (IT) infrastructure. Several authentication protocols have been designed and implemented to secure systems from unauthorized access. Entity authentication is used to safeguard digital devices from attacks like eavesdropping, man-in the middle attack, reply attack etc. Initially, password-based authentication protocol was developed. In this protocol, the password was used for authentication and password was sent as plaintext through the communication channel. This protocol suffered from replay attack, password guessing attack, and dictionary attacks, etc. Later on, Challenge-handshake authentication protocol was developed based on the challenge response paradigm. In this technique, a challenge contained a hash of a random string concatenated with the key using MD5 or SHA algorithms. When claimant got the challenge, then it sent the response to the verifier. Later, on the Extensible Authentication Protocol (EAP) (Aboba et al., 2004), KERBEROS (Kohl & Neuman, 1993), RADIUS (Rigney et al., 2000), DIAMETER (Calhoun at al., 2003) protocol, zero knowledge-based entity authentication protocols were developed. The classical authentication schemes are based on hardness of the mathematical equation.

Due to the advent of high-performance computers and quantum computers, any security mechanism based on mathematical complexity could be broken easily. Hence, the quantum secure authentication protocol is the utmost requirement for the next decade to protect resources from attacks.

One time pad (OTP) is the classical cryptographic algorithm that is almost unbreakable if it is appropriately implemented. In OTP, the ciphertext is generated by using XORing of plaintext and shared OTP between entities. In this paper, the design of a proposed entity authentication protocol to secure authenticated data from quantum computer attacks is discussed.

The rest of the paper is organized as follows: Section 2 deals with related work; Section 3 describes the proposed quantum secure authentication protocol; Section 4 deals with security analysis of the proposed protocol, and finally, section 5 deals with the conclusion and future work.

2. RELATED WORK

To maintain user convenience and high level of security, a highly unpredictable data must be available to the attacker so that they cannot get any information and prevent off-line verification or guess. A common form of guessing attack was examined and developed cryptographic protocols immune to attacks, and suggested a systematic way to examine protocols to detect vulnerabilities to such attacks (Gong et al., 1993). Several password authentication protocols were analyzed and found that public key cryptography provided resistance to offline password guessing attacks. They also incorporated public passwords as handy certificates that the user could carry without any requirement of computing devices (Halevi & Krawczyk, 1999). Further, the password-based authentication protocol model was proposed, and the model for this problem prevented threats like password guessing, forward secrecy, server compromise, and loss of session keys. Authentication Key Exchange (AKE) was used to secure the entity authentication protocol (Bellare et al., 2000). Encrypted Key Exchange (EKE) became the basis for many of the