# Password Authentication for Multicast Host Using Zero Knowledge Proof

**Seetha Ranganathan, R. Saravanan**
School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India

**Article Info**

***Article history:***

Received Feb 13, 2015
Revised Jul 17, 2015
Accepted Aug 1, 2015

***Keyword:***

Authentiction
One time password
Prover
Verifier
Zero knowledge proof

**ABSTRACT**

The password which is a more secure and valuable data should be highly protected from eavesdropper. This paper presents how password required for authentication of members of group communication is securely delivered by the source or initiator of the group. The password delivery uses zero knowledge proof and sent to the group member in an encrypted format using cipher block mode encryption. The password delivered is a One Time Password which can be used for certain amount of time in order to ensure a highly secure communication environment among the group.

***Corresponding Author:***

Seetha. R,
School of Information Technology and Engineering,
VIT University,
Katpadi, Vellore, 632007, Tamilnadu, India.
Email: rseetha@vit.ac.in

## 1. INTRODUCTION

A zero-knowledge password proof (ZKPP) [1], [2] is a collaborative method for the prover to prove to the verifier that it knows the password, without revealing any other information to the verifier. A ZKPP prevents any one from verifying guesses for the password. A common use of a zero-knowledge password proof in authentication systems include the prover wants to prove its identity to the verifier (Source or host, the group member) using a password without allowing anyone to learn anything about the password generated and delivered to them.

Passwords in various formats [3], [4] are important data for one to get authenticated by themselves to access valuable services and resources. The One Time Password (OTP) which is used nowadays is valid for only certain amount of time or for one session. OTP provide a highly secure environment comparing to the traditional static passwords which can be easily traced by eavesdroppers. Such OTP is highly useful in smart card authentication, online fund transactions and so on. OTP generation is carried out using pseudo random number generator and hash functions that are difficult to reverse. OTP can be generated based on time synchronization between the source and the participating host or based on previous password or based on some challenges to generate OTP randomly.

In this paper the password delivered by the prover (source/initiator of the group) is an OTP. The OTP generated is sent to the group member requiring authentication in an encrypted form using cipher block chaining mode (CBC) along with other details like nonce of joining host, nonce of source/initiator and host id.

The paper is organised as follows: Section II details the algorithms used in the proposed model, Section III focuses on related work carried out, and Section IV proposes the authentication algorithm that uses zero knowledge proof.

## 2. EXISTING ALGORITHMS AND PROTOCOLS FOR AUTHENTICATION

### 2.1. Time-based One-time Password Algorithm (TOTP)

TOTP [5] algorithm computes a one-time password (OTP) using a shared secret key and the current time. TOTP is an example of a hash-based message authentication code (HMAC). In this algorithm a secret key is combined with the current timestamp using a cryptographic hash function to generate a one-time password. The main advantage is TOTP passwords are short-lived passwords.

Parameters used in TOTP:

TC = (unixtime(now) - unixtime(T0)) / TS

TOTP = HOTP(SecretKey, TC) (HOTP is defined below)

TOTP-Value = TOTP mod 10d, where d is the desired number of digits of the one-time password.

Where TC – integer time counter, T0-Start time, TS – time step count

Let K be a secret key and C be a counter

HMAC (K,C) = SHA1(K ⊕ 0x5c5c... ∥ SHA1(K ⊕ 0x3636... ∥ C)) be an HMAC calculated with the SHA-1 cryptographic hash algorithm. A Truncate function selects 4 bytes from the result of the HMAC in a defined manner such that HMAC – based One Time Password (HOTP) is given as

HOTP (K,C) = Truncate(HMAC(K,C)) & 0x7FFFFFFF. The mask is used to set the most significant bit to 0, to prevent the number from being interpreted as negative.

### 2.2. Cipher Block Chaining (CBC)

CBC [1] is the most widely used block cipher mode. In this mode of encryption plain text is randomized using previous cipher text block. The advantage of CBC is equal plain text blocks get encrypt to different cipher text blocks, hence reducing the chance of attacking. CBC is defined as:

$C_i = E(K, P_i \oplus C_{i-1})$ for i=1,…….,n

### 2.3. Zero Knowledge Proof (ZKP)

A zero-knowledge proof protocol [6], [7] allows one party, called prover, to convince another party, called verifier, that prover knows some facts without revealing to the verifier any information about his knowledge.

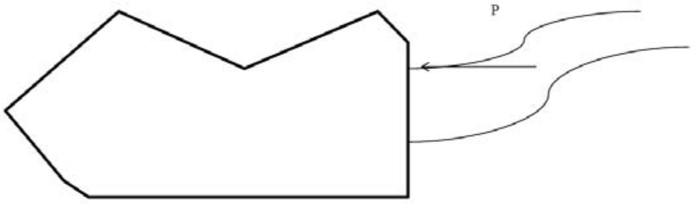

Figure 1. Magical Cave

ZKP can be explained through opening the secret door of a cave using the magic words example. The story says, someone who knows the magic words can open the secret door to enter into cave. To everyone else, it seems to be a rock. Assume, Alice knows the secret of the cave. She wants to prove her knowledge to Bob, but she doesn't want to reveal the magic words. Here's how she convinces him:

1) Bob stands at point P.
2) Alice walks all the way up to the cave door at point Q
3) Alice confirms, using the magic words to open the secret door if she has to

## 3. RELATED WORK

Some related works are Password Authentication Protocol (PAP), Challenge handshake Authentication Protocol (CHAP), Zero Knowledge-Password Authentication Protocol (ZK-PAP). PAP is most widely used authentication protocol to validate users accessing to server resources. It is a simple protocol which transmits ASCII values of password entered over the network and hence considered insecure. The PAP involves two steps process

1) User who wants to access the server resources logins using username and password.
2) The server or system in turn validates the username and password entered and either accepts or denies the service accordingly.

PAP [8], [9] uses three types of packets namely authenticate-request, used by the user to send user name and password, authenticate-ack, used by system to allow access and authenticate-nak, used by system to deny access.

CHAP [9]-[11] is a three way hand shaking authentication protocol based on challenge-response model. It is more secure than PAP as the password is not transmitted over the network and is kept secret but requires that both the user and system to know the plaintext of the secret. CHAP provides protection against replay attacks by using an incrementally changing variable and of a variable challenge-value. The protocol works as follow:

1) The system sends a few bytes of challenge message to the user.
2) The user sends a response message which has a value calculated using one -way hash function on the challenge and secret combined.
3) The system in turn applies the same hash function to retrieve the value. If the value obtained matches, access is granted otherwise it is denied.

CHAP uses four types of packets namely, Challenge which is used by the system to send challenge message, Response is used by the user to send the computed value, Success used by the system to grant access and Deny used by the system to deny access to the user.

In ZK-PAP [12], the authentication process is initiated by the user who sends the user name and nonce N1. The system sends a response message on concatenating the random session key k, N1 (user nonce), N2 (system nonce) and encrypts using hash of password value corresponding to username received. The user in turn applies the same hash function and retrieves back the nonce N1. If matches, retrieves the key k otherwise denies. If match occurs, the user sends the nonce N2 to the system encrypted using the session key k. The system decrypts and checks its nonce N2. If match occurs, the user is allowed to access the resources else denied access.

## 4. PASSWORD AUTHENTICATION ALGORITHM FOR MULTICAST HOST – PROPOSED METHOD

The proposed algorithm for authenticating multicast host to participate in group communication uses challenge-response messages.

1) The host who wants to join a group sends a nonce N to the Source or initiator of the group.
2) The Source uses the nonce N as an initial value to CBC mode of encryption. The encryption is performed on OTP||N||M||host_id, where M is source nonce,host_id is the id for joining host.
3) The user decrypts and verifies the N. If matches, sends a response message containing M||host_id using M as an initial value for CBC encryption otherwise denies.
4) The Source checks its nonce M on decrypting it and sends acknowledge (ACK) message allowing the host to join the group else denies (DENY).
5) The host now joins the group using host_id as login or user name and OTP as password for the multicast session.

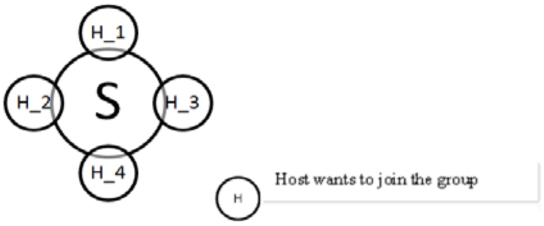

Figure 2. Multicast Communications

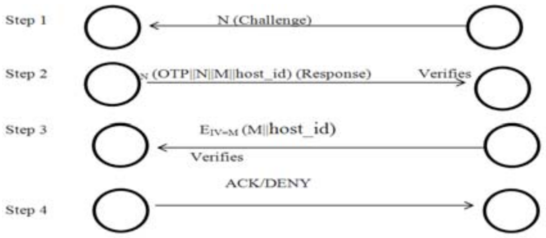

Figure 3. Handshaking messages between Source S and Host H

## 5. RESULTS AND DISCUSSION

The use of nonce N and M prevents replay attacks. Though password is transmitted over the network, encryption of password makes it secure. Moreover password generated is a one-time password which provides high security as password is stored elsewhere.Use of CBC mode of encryption is uses nonce as its initial value which is also a randomly generated number which could be used only once. The chance of attacking the encrypted message is also considerably less as CBC modes of encryption produces different blocks of cipher as output.The Source or the initiator of the group communication also does not reveal any information to the hosts.

## 6. CONCLUSION

The algorithm proposed uses a randomly generated One-time password for the host to join the group communication session. The encryption algorithm used to encrypt the response message also makes the handshaking mechanism more secure. The chance of eavesdroppers to access the communication session is also reduced as information about the source of the group is kept secret using zero knowledge proof.

Thus use of nonce as initial value for CBC mode of encryption and CBC mode of encryption producing different blocks of cipher as output provides two level of security for transmitting the generated OTP over insecure network in a secure manner.

## REFERENCES

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC Press, pp. 228–233, 1996.

[2] S. M. Bellovin and M. Merritt. “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks”, *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, 1992.

[3] Kameswara Rao, Sushma Yalamanchili, “Novel Shoulder Surfing Resistant Authentication Schemes using Text Graphical Passwords”, *International Journal of Information and Network Security (IJINS),* Vol. 1, No. 3, pp163-170, 2012.

[4] Hang Tu, “A Security Enhanced Password Authentication and Update Scheme Based on Elliptic Curve Cryptography”, *TELKOMNIKA Indonesian Journal of Electrical Engineering*, Vol. 12, No. 10, pp. 7353-7360, 2014.

[5] M’Raihi D., Bellare M., Hoornaert F., Naccache D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, 2005.

[6] “Zeroknowledgeproof.”Wikipedia, TheFreeEncyclopedia (http://en.wikipedia.org/wiki/Zeroknowledge_proof).

[7] Oded Goldreich, “Zero Knowledge twenty years after its invention”, *Unpublished manuscript*, 2002.

[8] Leslie Lamport, “Password Authentication with Insecure Communication”, *ACM*, pp. 770-772, 1981.

[9] Forouzan, “Data Communication & Networking”, Fourth Edition, McGraw-Hill Education (India) Pvt Limited, pp. 352–353, 2007.

[10] W. Simpson, “Request for Comments 1994, PPP Challenge Handshake Authentication Protocol (CHAP)”, *Network Working Group,* California, 1996.

[11] M. W. Youssef and Hazem El-Gendy, “Securing Authentication of TCP/IP Layer Two by Modifying Challenge-Handshake Authentication Protocol”, *Advanced Computing: An International Journal (ACIJ),* Vol. 3, No. 2, 2012.

[12] Nivedita Datta, “Zero Knowledge Password Authentication Protocol”, *International Journal of Communication Network Security,* Vol. 1, No. 4, pp. 30-34, 2012.

## BIOGRAPHIES OF AUTHORS

Seetha Ranganathan received her B.E Degree from Madras University in the year 2003 in the field of Computer Science and Engineering. She received her M.Tech Degree in Computer Science and Engineering from SRM University in the year 2007. She is currently working as Assistant Professor (Senior) in the School of Information Technology and Engineering, VIT University Vellore. She is pursuing her PhD thesis in VIT University.Her areas of research includes Graph theory, Algorithm analysis, cryptography, Mobile networking and security.

R Saravanan completed his doctoral thesis in the area of Approximation Algorithms in 1997 at Ramanujan Institute for Advanced Study in Mathematics and obtained the Ph.D degree from University of Madras. He received M.E. degree in Computer Science & Engineering from College of Engineering, Guindy, Anna University, Chennai. He has rich research experience in areas of algorithms and published more than seventy five research papers in the peer reviewed international journals and numerous research papers in national journals, international and national conferences. He served as an academic council member and board of study member in many universities and autonomous colleges. He has about two decades of teaching and research experience. He is a life member of Computer Society of India (CSI), Cryptology Research Society of India (CRSI) and Ramanujan Mathematical Society and also he is a member of IEEE. Three research scholars completed their Ph.D under his guidance and supervision and ten more his research scholars are carrying out their research towards their Ph.D. His areas of research include approximation algorithms, mobile computing, cryptography, and network security.