RESEARCH ARTICLE OPEN

Zero Knowledge Protocol for Authentication and Key Exchange – A Survey

Sudha D [1], Anupama Usha [2]
Department of MCA
SCMS, Muttom Aluva
Kerala

ABSTRACT
Zero Knowledge Proof (Protocol) is a protocol which does not reveal the secrets during the process. In this paper we investigate Zero Knowledge Protocol Applications based on Two Factor Authentication, Zero Knowledge Protocol password authentication Protocol with Public Key Encryption and Modification of Diffie Hellman Key Exchange Algorithm.. Zero Knowledge Protocol provides one more level of security between the Client and Server. This era requires the application of Zero Knowledge Protocols to enforce Authentication.

Keywords :— Zero knowledge, Two factor Authentication ,Public Key, Encryption, Decryption, Diffie Hellman, Man in the middle attack

I. INTRODUCTION

Zero Knowledge Protocol is a method by which one party proves to the other party that a given statement is true without giving any secret information. Here the secret information is the password. The intention is to force a prover to prove to a verifier that its behaviour is correct according to the protocol. The protocol requires input from the verifier, in the form of a challenge such that responses from the prover will convince the verifier that the statement is true, which proves that the prover does have the claimed knowledge .The protocol has to satisfy 3 features: completeness, soundness, zero knowledge. This paper intends to perform a survey on 3 applications of zero knowledge proof: two factor authentications using zero knowledge protocol, zero knowledge password authentications with public key encryption and Diffie Hellman exchange using zero knowledge protocol.

II. ZERO KNOWLEDGE PROTOCOL

Zero Knowledge Protocol is used for transmitting the data more securely by which one party authenticates itself without disclosing private credentials.

A. Definition

The concept of zero-knowledge can be explained with the help of a classical example of two identical balls [9]. Suppose a person, say 'A' has two identical billiards balls of different colors, say red and blue. Now he wants to convince his friend, say 'B' that the two balls are of different colors. The basic approach will be to give the two balls to B so that he can see them and confirm the fact that the two balls are of different colors or not. However, in this scheme B gains knowle dge about the colors of the balls. Using the zero-knowledge approach, however A can convince his friend B that he has balls of different colors without having B see the balls actually. To do this, A blindfolds B and then places a ball on each of B's hand. Though B has no idea about which ball is of which color but A can see the color of the two balls. Now A asks B to take his hands at the back and either swap the arrangement of the two balls or keep the arrangement same as original and show him the balls again. A sees the new arrangement of the balls and lets B know whether the balls were swapped or not. Thus A can prove to B that he has given him balls of different colors without revealing anything about color of the balls.

Properties Expected: :1) completeness(if the statement is true, a honest verifier will be convinced of it by a honest prover).

2) Soundness (if statement is false, no cheating prover can deceive a honest verifier).

3) zero knowledge (if the statement is true, no cheating verifier knows anything other than the statement)

III. LITERATURE REVIEW

B. Two Factor Authentication

Here, the user is allowed to log into a remote service by providing his username and password as credentials for authentication. The same is extended nowadays by providing multiple factors like personal information etc thus forming multi factor authentication. But the problem with these techniques arises when the login attempts are made through unsecure devices like public systems, ATMs etc.

Principles Used in This Scheme

a) User: The user is the individual who wishes to securely maintain and access an account with one or more services

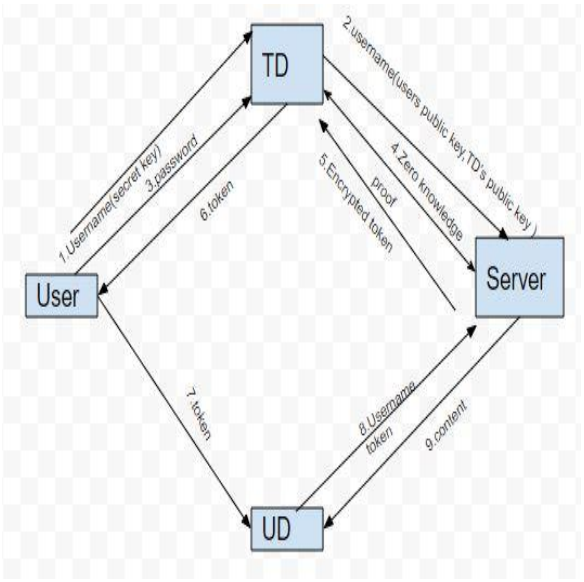
b) Trusted Device (TD): The trusted device is a device that belongs to the user. It must be a mobile device such as a phone, tablet, or laptop because it will be required every time the user attempts to log in. We assume that the trusted device is not compromised.

c) Untrusted Device (UD): An untrusted device is a device that the user wishes to use in order to log into an account that the user has. The untrusted device is, as the name implies, not trusted; it is assumed to be key logged and shoulder surfed.

d) Server: A server in this scheme is the device in charge of a particular service. All interaction with the service is achieved through communication with the server.

e) Adversary: Here we consolidate all possible malicious actions under a single hypothetical individual who we refer to as the adversary

In [1] it makes clear that to login both the password and ownership of the device is necessary. Proposed protocol is an improvement over hashing based password scheme.



This proposed implementation was written in Python with flask and Zero Knowledge Computation was done in Java Script and python on the back end. An app or a particular website is used to interface with server. After registration if the user wishes to login the proposed protocol allow them to start Zero Knowledge Proof Process through trusted device. First login is halfway successful and second token is generated on the trusted device .and entering this token results in successful login in untrusted device [1].

In [2] it gives an overview of 2 factor authentication, Properties of ZKP, Woking, Stages and Architecture. It ensures more security, also providing extra layer of security network. Also the data transmitted through network is of no use to the adversary.

In [3], it presents a simple protocol based on ZKP by which the prover can prove to the verifier that he is honest without revealing the secret key either as cipher or plain text .So again, one more level of security is proposed.

C. Zero Knowledge Password Authentication Protocol with Public Key Encryption

The core idea of this protocol is that the password is not travelling, instead the protocol uses a challenge-response mechanism between the server and the client based on a nonce which is a randomly generated number that is used throughout the session in order to avoid replay attacks .Now, instead of just the server authenticating the client, a second round of authentication where the client can authenticate the server is accomplished, by the use of public key encryption[4] .

Working

In [4] ,it is assumed that server has its public key and the it can receive the public keys of other users. The protocol works as follows:

- The user, say A sends his username and a nonce to the server after encrypting it with server's public key.
- The server decrypts the message with his private key and extracts the value of the nonce N1.
- The server then generates a nonce N2 and a random session key k, concatenates N1, k & N2 , encrypts them with hash of the password of user A, then with public key of the user A and sends the encrypted data to A.
- User A then decrypts the received encrypted data with his private key, then with the hash of his password and extracts the values of N1, N2 & k. He then matches the value of received nonce N1 & the generated value of N1.
- If match occurs, then A extracts the value of k & nonce N2, applies the transformation function F on N2 and encrypts the transformed value first with the session key k, then with public key of the server and sends the encrypted message to the server.
- The server decrypts the received value with its private key & then with the shared session key.
- The user A is allowed to login if the server receives the expected value else access is denied.

.

D. Modification of Diffie Hellman Key Exchange Algorithm for Zero Knowledge Protocol

In [5] DH key Exchange algorithm is vulnerable to Man in the Middle Attack. By using the Modification DH Key Exchange Algorithm for ZKP prover can prove the verifier that he/she knows the secret without revealing it.

Before sending the actual secret both should prove that they are honest. For that they create an initial key and both verify. First prover verifies that whether Verifier is honest by checking the values of R1 and R2'. Then Prover proves the verifier that he/she is honest by sending the correct R2'[5].

Here R1 is generated by prover with prover's generated secrete key and R2' is generated by verifier with verifiers secrete key and send back to prover. By encrypting R1 (C1) using the verifiers generated secrete key.C1 is send along with R1.Prover checks with R1=R2'. R2' is the decryption of C1 using the secrete key generated by prover. If R1=D(K2,C1)=R2' then verifier is honest [5].

If verifier is honest prover can send the secrete key. So prover should prove that she is honest. For that prover encrypt the data which is send by the verifier using provers generated secrete key and send back to verifier. Verifier Decrypt message using verifiers' key. If R1=R2' then prover proves that she is honest. Otherwise not[5].

IV. CONCLUSION

This Paper presents an Overview of Zero Knowledge Protocol used for Authentication. Zero Knowledge Protocol can verify whether the prover is honest or not by without revealing secret key. Two Factor Authentication using zero knowledge provides an extra layer of security. Public Key Encryption add a second level of security and enables mutual authentication. Just like Diffie Hellman key exchange can be modified with zero knowledge, counters the man in the middle attack, incorporation of zero knowledge proof in the existing security protocols will add additional security measures relevant in today's digital world .Simple and efficient protocols are prescribed here which gives more security so that we can send the message safely.

ACKNOWLEDGMENT

We thank our institution for providing the necessary support to study this emerging area of research .The insight into this topic provided by the fellow researchers were useful in framing this article.

REFERENCES

[1] Quan Nguyen ,Mikhail Rudoy ,Arjun Srinivasan,Two factor Zero Knowledge Proof Authentication System,6.857 Spring 2014 project..

[2] Niranjana Murthy M, Shashank K S , Sumantha P Gowda,Suhas Bhatta S, Research Study on two factor zero knowledge Proof Authentication System , IJARSE, Vol No.5 Special Issue No (01), February 2016

[3] Datta -"ZERO KNOWLEDGE PASSWORD AUTHENTICATION PROTOCOL" International Journal of Communication Network Security , Volume-1, Issue-4, 2012.

[4] M Nivedita Datta,Zero Knowledge Password Authentication Protocol ,SuperComputer Education And Research center,NISc,Bangalore, IJCNS vol 1 Issue 4, 2012

[5] Jithendra Kurmi Ankur Sodhi- A survey of Zero Knowledge Proof for authentication IJARCSSE, Vol 5 Issue 1 , January 2015.

[6] Challenging epistemology: Interactive proofs and zero knowledge Justin Bledin Group in Logic and the Methodology of Science, University of California, 910 Evans Hall #3840, Berkeley, CA 94720-3840, USA, Journal of Applied Logic 6 (2008) 490–50

[7] Mohammad Sadeq Dousti and Rasool Jalili "Effcient Statistical Zero-Knowledge Authentication Protocols for Smart Cards Secure Against Active & Concurrent Attacks" An abridged version of this paper is published in International Journal of Computer Mathematics, January 2015

[8] Vishal Parbat, Tushar Manikrao,Nitesh Tayade, Sushila Aghav "Zero Knowledge Protocol to design Security Model for threats in WSN" (IJERA) ISSN: 2248-9622 Vol. 2, Issue 2, pp.1533-1537, Mar-Apr 2012

[9] "Cryptographic Hash Function" Wikipedia, the free encyclopedia (http://en.wikipedia.org/wiki/ Cryptographic_hash_function)

[10] "Zero-knowledge password proof" Wikepedia, The Free Encyclopedia. (http://en.wikipedia.org/ wiki/Zeroknowledge_password_proof.

[11] A Survey of Zero-Knowledge Proofs with Applications to Cryptography, Austin Mohr, Southern Illinois University at Carbondale.

[12] B. Lloyd & W. Simpson, Request for Comments 1334, PPP AUTHENTICATION PROTOCOLS Network Working Group , October 1992.