International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-9, July 2020

Zero-Knowledge Proof Based Authentication Over Untrusted Networks

Cherukupalli Veda Vyasa Aditya, Rajesh Kannan Megalingam

Abstract*: Zero knowledge proof is a powerful cryptographic protocol that is utilized to establish data security whilst ensuring and maintaining user anonymity. ZKP has relatively less complex computational requirements as compared to the other protocols for authentication. Conventional authentication schemes are susceptible to attacks such as MiTM, IP spoofing, DoS, replay and other eavesdropping based attacks, when the data is shared across an untrusted network. This paper shows an approach to ensure authentication of a device over an untrusted network whilst maintaining and safeguarding user credentials, by using the concepts of ZKP protocol.

***Keywords*: Zero-Knowledge proof, cryptography, authentication, XOR, untrusted networks.**

I. INTRODUCTION

In today's world, agreeing to the terms and conditions of data handling procedures of a product is necessary to attain services as per user flexibility. Thus, an approach where a user can be authenticated based on the randomness of credentials, in particular to a user authentication is necessary. Our fundamental notion of Zero-Knowledge proof is to ensure that, no personal data is sent over an untrusted network and the services are obtained without paying the cost of personal data in exchange i.e. provide the organizations with the required and relevant data without revealing the requested data.

Although, the password is stored and sent over the untrusted network in hashed format along with its associated username, but the fact that these are still susceptible to attacks like packet sniffing, eavesdropping cannot be disregarded and may lead to the leakage of personal data as it provides a visibility to the public.

In this paper we presented an improvised protocol, in particular to Password-Authentication Protocol (PAP) [6,7,10,11] and Challenge-Handshake authentication protocol (CHAP), by introduction of a concept of ZKP that provides additional level of security for authentication of both the client and the server while data transmission.

Our approach is more of an improvisation and combination of CHAP and PAP oriented, with the usage of random number like nonce. This nonce is beneficial, if attacks mentioned above need to be avoided

Revised Manuscript Received on July 30, 2020.

***** Correspondence Author

Cherukupalli Veda Vyasa Aditya*, Department of Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham University, Amritapuri Campus, Kollam, India.

Dr. Rajesh Kannan Megalingam, Assistant Professor, Department OF ECE, Amrita School of Engineering, Amrita Vishwa Vidyapeetham University, Amritapuri Campus, Kollam, India.

II. PROPOSED METHODOLOGY

A. Definition – Zero-Knowledge Proof (ZKP)

Prior to implementation of our approach, it is necessary that ZKP must satisfy the following 3 key properties:

a) Completeness – This property is to ensure that the ZKP protocol is properly followed i.e. if the information or data is true, then the authentic or a legitimate verifier must prove that the information is true every time.

b) Soundness – This mainly deals with false-positives, i.e. if the information is not true, then it must be almost impossible to convince the verifier that the information is true.

c) Zero-Knowledge – This mainly deals with providing no information apart from the fact that the information is true or false.

We shall discuss it in the form of a classic example using the concept of two identical balls [9].

Assume, 2 people, 'Person 1' and 'Person 2'. Person 1 has 2 identical balls, 'Ball 1' and 'Ball 2' but they vary in colors. Assume 'Color 1' and 'Color 2'.

The key challenge faced, is to convince that Person 1 knows that both the balls are of un-identical colors without revealing the colors of the balls to Person 2.

Furthermore, assume that a prover needs to prove the color of the balls to the verifier without revealing the colors of the balls.

a) Now, in order to ease the approach, let us assume that 'Person 1' who have 2 identical shaped, but different colour balls, is the Prover and 'Person 2' is the Verifier.

b) To prove the Verifier about the knowledge that both the balls are of different colors, one simple approach would be to handover the balls to the Verifier and thus the verifier would be convinced about the knowledge the prover has i.e. the balls are of two different colors. But ZKP's goal is to prove without providing any knowledge about the colors of the balls as stated in one of its property.

c) Thus, another approach is, if the Verifier is blindfolded and then Prover gives both the balls to the Verifier i.e., the Prover still has visibility whereas the Verifier does not.
The Verifier is asked to perform a swap operation in such a way that the Prover has no visibility of that operation and then is asked to present it in front, if the prover answers correctly, the verifier can assure that both the balls are definitely of different colors. But this is only true if this process is done a certain number of times. ZKP mainly deals with probabilistic approach. Thus, more the number of transaction, more certainty of getting the trust that the Prover is actually telling the truth. This ensures completeness, soundness and zero-knowledge and finally satisfying the requirement about proving to the verifier about the knowledge of the balls. This ensures that the colors of the balls are not revealed and both parties agree to the fact that the balls are indeed of different colors

III. RELATED WORK

Some of the related work have been done in a Password authentication protocol (PAP) [12,11] which ensure an end point encryption whilst providing the access to the resources, or indeed prior to the resource allocation. In a PAP based approach there is requirement of credentials such as username and a password and is susceptible to attacks such as network, packet sniffing and Man-In-the middle scenario. Another security enhancement in such scenarios is the usage of hashed passwords which are generally collision resistant. For example – 'A' sends username and password to the server and the server matches against the stored username along with the associated hashed password. If the match is true, allow login. The key constraint is the sending of the unencrypted password over an unsecure channel although it is resilient to most of the risks at the server as the password is stored in hashed format at the server's end. Further studies and relevant work include the usage of CHAP i.e. Challenge-handshake authentication protocol [1,2,3,5,12].
This is mainly based on a challenge-response based approach where one-time use keys, in some cases OTP's, are used as a security enhancement. For example – Upon request of resource from client's end, the server generates a one-time use key with the associated username and sends it to the client along with an expiration time in some cases. The client then needs to send the password in encrypted format using that one-time use key which is then matched against the server stored credentials and then mapped with the encrypted result of received encrypted credentials. If match, then login is allowed. The CHAP based approach ensures the verification of unattended systems and that only authorized login is allowed. But however certain disadvantages do exist such as
a) Unencrypted storage of password at the server end.
b) Packet sniffing of the sent one-time used keys and thus the attacker can perform key-cipher text-based attacks which similar to dictionary or birthday attacks.

Another scenario of ensuring security is by the usage of collision resistance hashes [13]. The key properties of a hash function include –

a) Variable length input, fixed length output.
b) Must be resistant to collision.
c) One-way function
d) Deterministic.

Below figures depicts few key exchange mechanisms and traditional ZKP approach.

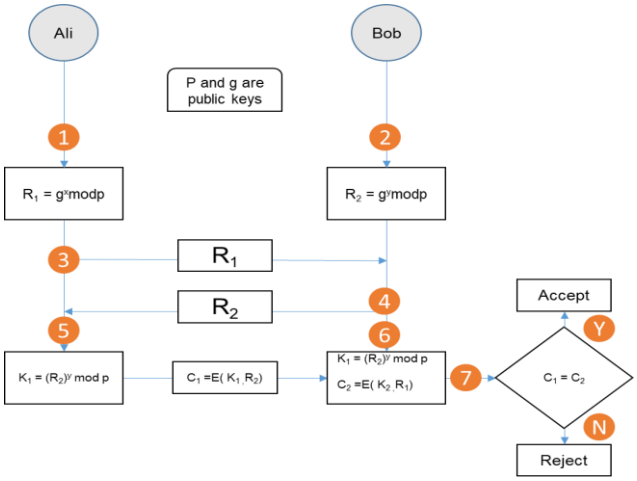


Fig 1: Diffie-Hellman based Authentication

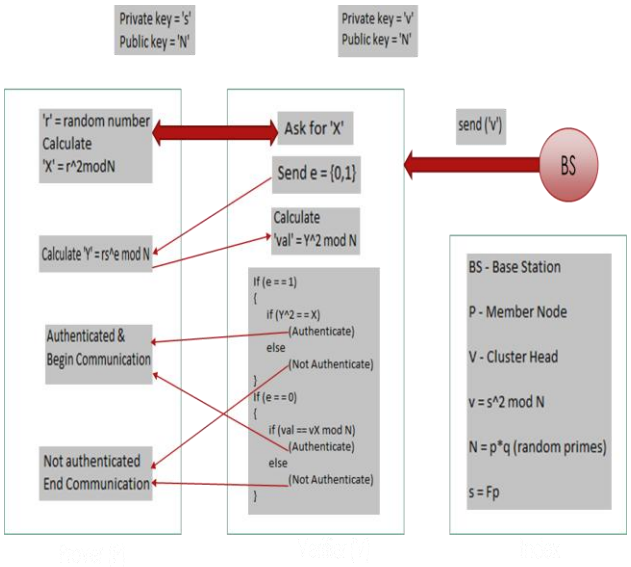


Fig 2: General Zero-Knowledge Proof based Approach

Some of the applications [8] of Zero-Knowledge proof include
a) Authentication Systems – Prove an information without revealing any information to the verifier
b) Ethical Behavior – The idea is to ensure that the behavior is correct according to the ZKP protocol
c) Nuclear Disarmament – Allowing inspectors to confirm the objective of a nuclear weapon without actually recording, sharing or revealing the internal secret workings.
d) Blockchains – provide a proof of concept that the transactions are valid or not despite the fact that the information is hidden.

IV. OUR APPROACH

In our approach, we would be following a similar username, password authentication mechanism but at 3 stage phase level, namely.

a) Registration – This is an initial phase where the device is registered with the trusted server.

b) Verification – Depending upon the approach the device is verified whether it is legitimate or not and then sent to next phase.

c) Authentication – Once the device has gone through the verification and is verified then it will be authenticated for the usage of resource.

Our approach is mainly a mixture of CHAP, PAP and ZKP with the addition of XOR functionality along with public key encryption.

Assumptions

Category	Description
Security	It is assumed that the server is secured from any external threats and the registration is performed over a secured channel.
Platform	Python v3.0
Operating System	Ubuntu 16.04
Network Latency	2.10 Mbps Uplink 1.81 Mbps Downlink

a) Registration –

i) The user generates Public key (Pub U) and Private Key (Pvt U) pair and sends the Pub U to the sever.

ii) The user register based on traditional registration approach i.e. Username, hashed password encrypted with server Public key (Pub S).

iii) The server generates a secret number (s), stores alongside the associated username. The server then stores the username, hashed password so received, public key of user and a randomly generated secret number in its database and that secret number is stored at user's end as well.

b) Verification –

i) The server generates a random sequence of '0' and '1' such that the XOR of all bits equals 1.

ii) In our case, a total of 10(ten) bits of '0' and '1' are produced, making it to a probabilistic security level of 210, as ZKP is more of a probabilistic approach i.e. more the number of transactions, higher the level of security. This random sequence is stored alongside the user credentials.

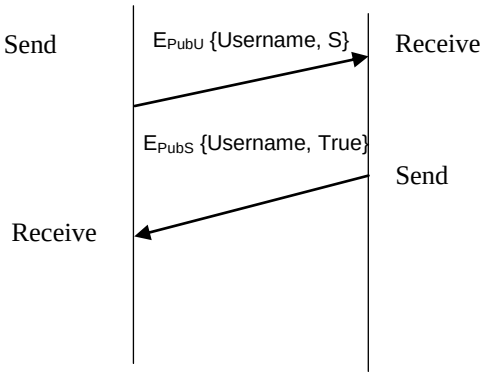
Next, at the server end, the start pointer pointing at start bit from the 10 bits' random sequence of '0' and '1' such that their XOR =1 is selected. If the bit =1, then the server sends, the secret number along with the username encrypted in the public key of user.

- Once the user decrypts using his private key, he checks if the secret number and username matches with his stored data.
- If matched, then the user sends, username with true as response encrypted in the public key of server. The server then decrypts using its private to verify the response of the user's ends.
- If the response matches, then a counter is increased, else it moves to the next bit in the 10(ten) -bit sequence without increasing the counter.
- If the bit value from the 10 (ten) bits sequence is 0, then the server sends a random number along with the associated username, encrypted with user's public key in which the server is expecting 0 as a response.
- Follow this procedure for all the 10(ten) bits.

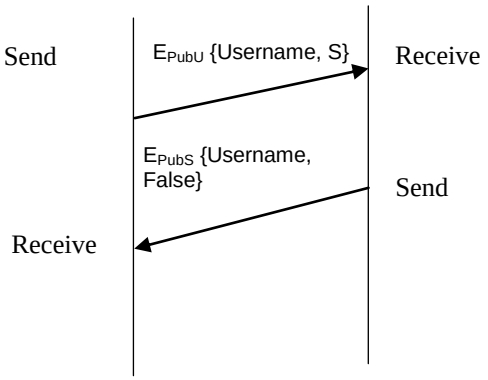
c) Authentication –

To authenticate the user, 100% valid transactions is required and the counter that started from 0 must be equal to 10 (ten).

i) When leading bit = 1



ii) When leading bit = 0



- EPubU – Public key encryption using user's public key'
- S – Secret number
- EPubS – Public key encryption using server's public key.
- Rnd – random number generated using random number generator.

Fig 3: Authentication using XOR approach in ZKP

All submitted paper should be cutting edge, result oriented, original paper and under the scope of the journal that should belong to the engineering and technology area.

In the paper title, there should not be word 'Overview/brief/ Introduction, Review, Case study/ Study, Survey, Approach, Comparative, Analysis, Comparative Investigation, Investigation'.

V. RESULT ANALYSIS

The below table depicts a comparative analysis for the taken for registration,
verification and authentication of various devices using the traditional and our ZKP approach for authentication of various devices

Device ID	Random ten Bits	Registration and verification time (in seconds)	Traditional ZKP authentication time (in seconds)	Our ZKP authentication time (in seconds)
Device 1	1010010101	8.1888	4.3232	5.1885
Device 2	0110010101	7.2642	3.5343	4.13123
Device 3	1011010001	8.2424	3.2312	4.5454
Device 4	0000000001	9.2131	3.9783	5.2223
Device 5	1000000000	8.2323	3.6412	5.2242

VI. SECURITY

i) Valid transactions column must have 10 (ten) as a count to ensure authentication.
ii) Prevents Spoofing based attacks, as the attacker must ensure the sequence of the random bits to be followed which is a probability of 1/ 210.

iii) Prevents replay attacks due to the randomized generation of bits in authentication.

iv) Resilient to password-based attacks (Brute force, dictionary) as the password is not sent over the untrusted channel and once the valid transactions counter column is 10 (ten), the transaction will stop.

Additional benefits:

- No additional hardware requirements such as biometrics or a token generator
- Prevents similar values such as same hash of same password due to the use of random bits' generator
- Lesser computational load on other devices as random bits are generated only at the server end.
- The authentication is done without the need of the password to travel across the wire.
- The password in the password file on server is stored in encrypted format thus making it less vulnerable to attacks.
- The security of the protocol mainly depends on the strength of the encryption algorithm being used.
- Thus, using the standard algorithms like AES, DES etc. will provide high degree of security to the protocol.
- Solves problem of unattended servers.
- Additional hardware requirements such RSA token generator, OTP is not required.
- Random bit generator is at server end, lesser computation to client.

Our approach comparatively requires more time due to the complexity of the algorithm, but at the same time ensures that security for most of the password-based attacks over the unencrypted channels can be achieved.

VII. CONCLUSION AND FUTURE WORK

This paper illustrates the usage of Zero-knowledge proof in Challenge-handshake authentication protocols and Password authentication protocol which makes it lesser vulnerable to the attacks as only a random number is sent over the untrusted channel.

The XOR based approach provides anonymity and with the inclusion of PKE (Public-Key encryption) into the system the security levels are hardened and the strengthening is complete.
Although the XOR based approach of ours takes relatively more time as compared to the traditional authentication approach, but there's always a tradeoff between efficiency and security.
The approach is protocol is simple and efficient thus enabling their practical use.
The future work includes making the protocol more efficient and provide efficiency in a multi-threading environment

REFERENCES

1. W. Simpson, Request for Comments 1994, PPP Challenge Handshake Authentication Protocol (CHAP), Network Working Group, California, 1996..
2. Securing Authentication of TCP/IP Layer Two by Modifying Challenge-Handshake Authentication Protocol, M. W. Youssef and Hazem El-Gendy, Advanced Computing: An International Journal (ACIJ), Vol.3, No.2, March 2012B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.
3. G. Zorn, Request for Comments: 2759: Microsoft PPP CHAP Extensions- Version 2, Network Working Group, Microsoft Corporation, 2000.
4. Dolev, and A. Yao. On the Security of Public Key Protocols. IEEE Transactions on Information Theory, 29(2):198-208, March 1983.
5. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
6. Oded Goldreich. Zero-knowledge twenty years after its invention. Un-published manuscript. 2002.].
7. "Zero-knowledge proof." Wikipedia, The Free Encyclopedia (http://en.wikipedia.org/wiki/Zeroknowledge_proof).
8. (Padraig, F. (2014). Securing the Internet of things: A ZKP-based approach. [online] Osna-solutions.com. Available at: http://www.osna-solutions.com/wp-content/uploads/Securing-the-Internet-of-Things-A-ZKP-Approach-Thesis-Extract.pdf
9. 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) 490–501
10. A Survey of Zero-Knowledge Proofs with Applications to Cryptography, Austin Mohr, Southern Illinois University at Carbondale.
11. Microsoft Technet "Password Authentication Protocol" (http://technet.microsoft.com/enus/library/cc737807%28v =ws.10%29
12. Microsoft Tech Net,"Authentication Methods" (http://technet.microsoft.com/en-us/library/cc958013.aspx).
13. "Cryptographic Hash Function" Wikipedia, the free encyclopedia (http://en.wikipedia.org/wiki/ Cryptographic_hash_function

AUTHORS PROFILE

Cherukupalli Veda Vyasa Aditya is an M.Tech (Cyber Security systems and Networks) graduate and have worked on various fields related to IoT security, ZKP, Blockchain and have performed relevant research on other networking protocols in re-defining the efficiency and security parameters.

Dr. Rajesh Kannan Megalingam is an electronics engineer leading research on humanitarian technologies with special emphasis on Robotics at HuT (Humanitarian Technology) Labs and Assistant Professor at ECE Department. His research areas include Embedded Systems, Robotics, Semiconductors, and Healthcare. His research focuses on autonomous robots, vertical climbing robots, robots for rehabilitation, and robots and VLSI, etc.