Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Authentication Methodology for Electronic Mail Security Based on Zero Knowledge Protocol

[1]P Lalitha Surya Kumari, [2]Prof. Avula Damodaram

[1] Assistant Professor, Dept. of Computer Science and Engineering Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India

[2] Department of Computer Science and Engineering, JNT University, Hyderabad, Telanagana, India

***Abstract** - The authenticity of a genuine user needs to be determined in all corporate and commercial sectors like the banking, aviation, military etc,. usually authentication mechanisms are derived from three factors such as knowledge, biometrics and possession. These factors are inclined to (prone to) hardware failure, theft, expensive, etc. Hence, there is a need for a strong authentication solution. Zero-knowledge proofs of knowledge (ZK - PoK) play an important role in many cryptographic applications. In this paper, we present an adaptively secure identity based authentication system for electronic mail security using Zero Knowledge Protocol. This paper presents a novel methodology to provide the authentication and confidentiality using zero knowledge protocol. This simple protocol can prove to the authentication server that the user has the password without having to send the password to the server either clear text or in encrypted format. This is a protocol in which the statistics learned by one party (i.e., the inspector) allow him/her to verify that a statement is true but does not disclose any additional information. This simple protocol involves mutual identification of two users, exchange of a random common secret key or session key for the verification of public keys*

***Keywords**: zero knowledge proof; authentication; confidentiality; signature; secret key; public key; e- mail security; MD 5;hash function*

I. INTRODUCTION

The most commonly used system for exchanging information over the Internet (or any other computer network) is Electronic mail (email). At the most basic level, the email process can be divided into two primary components: (1) mail servers[6], which are applications that deliver, forward, and store mail; (2) clients[6] which interface with users and allow users to read, compose, send, and store email messages. This document addresses the security issues of both mail servers and mail clients. There is a need to secure mail servers and mail clients and the network infrastructure that supports them. The specific security threats to email generally fall into one of the following categories: Denial of service (DoS) attacks, Sensitive information on the mail server may be distributed to unauthorized individuals or changed for malicious purposes. The organizations interested in improving security on present and upcoming email systems can use this document in an effort to reduce the email related security incidents

II. BACKGROUND

Before one can comprehend (understand) the concepts of email security, it is essential (necessary) to fully understand how email messages are composed, delivered, and stored. RFC 822 set the standard for transmitting messages containing textual content. MIME uses the convention of content-type/subtype pairs to specify the native representation or encoding of associated data. MIME extensions allow for binary message content to incorporate into an RFC 822 message using a Base64 encoding, which provides a textual representation of binary data. Mail transport standards were established to ensure reliability and interoperability among various email applications. Simple Mail Transfer Protocol (SMTP)[3] is the most common MTA transfer protocol. Before Simple Mail Transport Protocol (SMTP) was assumed to be well behaved and trust worthy and designed for a small community of users. Simple Mail Transport Protocol [1] is the primary and the most widely adopted protocol for e-mail delivery. It lacks security features for privacy and authentication of sending party. To make e-mail system more secure, several technological and strategy changes were made to SMTP servers without creating incompatibility between older and newer systems. These include SMTP session refusal to unauthorized servers through IP address verification, refusal of e-mail relaying, restriction on use of certain SMTP commands like EXPN, verification of e-mail envelope and headers, limiting the size of e-mail message and filtering. These security features were updated, upgraded and some of them have been standardized. The security in e-mail systems are provided by add-on security protocols. These protocols either use cryptographic techniques or encryption or some domain validation standards. Security in E-mail messaging, can be defined as the ability of the system to provide i) privacy, ii) sender authentication, iii) message integrity, iv) non-repudiation, and v) consistency . The two encryption based methods that create encrypted secure channel between the sending and receiving MTA's at sockets and transport layers are Secure Socket Layer (SSL) [2] and Secure SMTP over TLS [2] respectively. Secure SMTP over TLS guards only the path between client and server and not the Domain Name System (DNS). The endpoints are authenticated by certifying authorities.

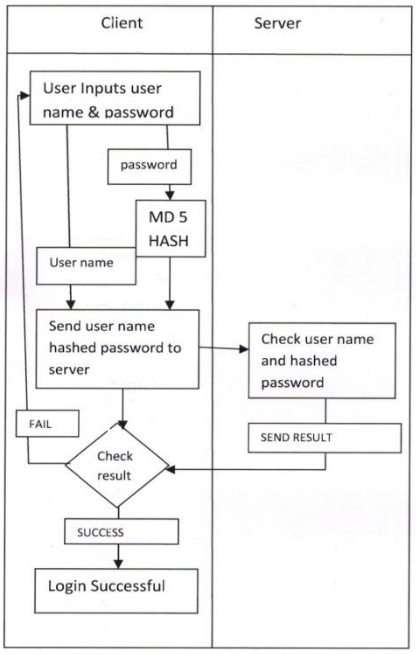
Client
Server
User Inputs user name & password
password
MD 5 HASH
User name
Send user name hashed password to server
Check user name and hashed password
FAIL
SEND RESULT
Check result
SUCCESS
Login Successful

Fig 1: Traditional Authentication System

Cryptography based encryption techniques for e-mail security includes Privacy-Enhanced Mail (PEM) , Pretty Good Privacy (PGP) , GNU Privacy Guard (GPG) and Secure Multi-purpose Internet Mail Extensions (S/MIME). PEM requires to trusting a single Certificate Authority (CA) infrastructure which is the reason for its almost negligible acceptance. PGP and GPG are PKI based scheme with sporadic adoption and are restricted to a minor user community. S/MIME provides cryptographic security services to e-mails. These services include sender authentication, non-repudiation of sender, message integrity and message security using encryption and digital signatures. But it has several deficiencies such as the recipient forward an e-mail along with digital signature to third party without the consent of sender thus posing a security threat to the sender's privacy and both sender and receiver need to purchase digital signatures from authorized certification authorities. S/MIME imposes mobility restrictions as users need to install certificates on clients from where they want to access e-mail and it cannot be used effectively through Webmail programs as these do not have S/MIME capabilities. The intensity of security provided by S/MIME depends upon the strength of its basic cryptographic algorithms and PKI profile which may differ in implementations. Other issues related to PKI based encryption protocols are concerns of key distribution, key renewal and key management and issues pertaining to correspondence with unfamiliar correspondents. Further, these protocols require a compatible mail systems and highly skilled users.

To overcome all these problems and deficiencies we must use a new protocol called Zero Knowledge protocol, which provides authentication and confidentiality (privacy) and indirectly provides services like message integrity and non repudiation**.** Wireless technologies have become increasingly popular in burgeoning military affairs and so is security, where the identity of an individual on the other side of the network has become challenging to determine. Thus, authenticity of an individual to access the private resources is the foremost concern and strong authentication between two parties (end-to-end) needs to be implemented. The authentication protocol which is to be discussed in this paper is Zero Knowledge Protocol.

III. ZERO KNOWLEDGE PROTOCOL

A. Main idea

Using Zero Knowledge protocols, a Prover tries to prove knowledge of a secret to a Verifier without revealing the secret itself. The Verifier can ask questions to find out if the Prover really knows the secret. Verifier does not learn any information about the secret even if he doesn't follow the policies of the protocol. Eavesdropper is a third party does not able to find out anything about the secret, or convince somebody else that he knows the secret if the protocol is secure. There is also a malicious user able to send, modify or destroy messages. A good protocol should be resistant against this user. A protocol has to consider cases that both Peggy and Victor may have malicious intentions as well. Peggy might try to cheat Victor into accepting a false statement, and Victor might try to get information to use in the future for personal advantage.

A good proposal must be developed by taking the following factors into account:

1. If Peggy does not know the secret information, she is unable to pretend to have such knowledge. Many rounds of the protocol should assure that (with probability close to 1) she couldn't cheat Victor.

2. Victor is able to convince himself that Peggy knows the secret, but he is unable to get any additional information, which could allow him to convince somebody else that he knows the secret. In specific he cannot find out anything from the protocol that he could not learn without asking Peggy direct questions. From this concept comes the name of this approach

B. Example analysis

Consider an example of counting leaves of big maple tree[4]. Victor asks the prover to count the leaves of tree without reveling any method and the number of leaves. Prover says some number to convince victor. If it is correct then cycle repeats by asking the question after doing something like pull off a leaf or do nothing. If prover gives the wrong answer, victor immediately says that prover is wrong. If answer is right, victor can think that prover was just lucky. Repeat the steps as many times as to convince the victor. If prover gives victor right answer for more than 1,000 times then victor will be convinced. This operation of the protocol can be repeated 10,000 or 30,000 times. After 100,000 rounds, victor should be quite sure of prover's knowledge.

The most typical example of zero-knowledge proof is the Cave model [4]. As shown in Figure given below:

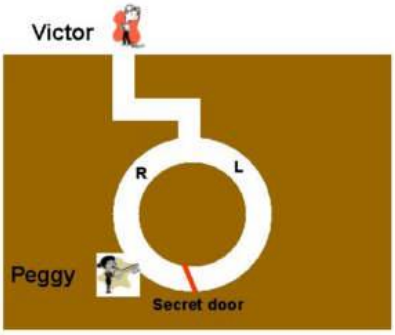

Fig 2: Conventional Example of Zeri knowledge protocol

Victor stands outside while Peggy goes into a branch of the cave (Victor doesn't know which one). Then Victor goes inside the cave and asks Peggy to come out from a particular branch that he chooses at arbitrary. It is obvious that if Peggy knows the secret key to open the door, she is able to come out from the branch that Victor called out, but if she doesn't know the password, she has 50% probability of coming out from the wrong branch. Victor can easily tell that she does not have the knowledge she claims to have. Victor could be very difficult to convince, so he could require many repetitions of these steps but, if, after 100 times, Peggy comes out the right way and doesn't fail once, he could be "sure" that she knows the password to open the door. In fact, she has a probability of 0.5^100 to cheat Victor, and this number is close to zero. Victor can repeat the round as many times as he desires until he is certain that Peggy knows the secret word. A main point here is that Victor is not able to convince anybody else even if he is completely convinced that Peggy knows the secret word. Let's say that he records everything. An Eavesdropper could think that Victor agreed with Peggy about which branch to choose each time. This attests that Victor cannot use any information he got for his own purposes.

C. Characteristics of zero-knowledge proof protocol

Zero-knowledge proof protocol has the following three important properties [4] .In other words, using zero knowledge proof protocol to prove a problem, the proving system must meet the following requirements [1]

1) Completeness

If the Prover P and the verifier V comply with the general process of zero- knowledge proof protocol strictly, the proof is considered to be successful and P is credible

2) Rationality

If it fails once in N times of verification, the proof is regarded as failed and P is a fake prover who is unreliable

3) Zero-knowledge

During the verification, V can't obtain any privacy or important information, let alone anything about the knowledge, except to believe that P does have it. Even though V verifies repeatedly, he cannot prove the existing fact to others anymore

IV. PROPOSED AUTHENTICATION METHODOLOGY FOR ELECTRONIC MAIL SECURITY

The method involves mutual identification of two users, exchange of a random common secret key or session key for the verification of public keys over an open channel. It enhances security by preventing the Man in the middle attack when the Diffie Hellman protocol is used. Previous protocols like PGP use digital signature and hashing for mutual identification of users. Both senders and recipients may have to buy digital certificates at a cost from trusted certification authorities to use digital signatures effectively. For using the digital signature the user has to obtain private and public key, the receiver has to obtain the digital signature certificate also. This requires them to pay additional amount of money. The process of generation and verification of digital signature requires considerable amount of time. So, for frequent exchange of messages the speed of communication will reduce. The new protocol overcomes all these problems. This protocol sends shared secret or session key through Zero Knowledge Protocol. Hence, An Eavesdropper is a third party that listens to the conversation but, he is not able to learn anything about the secret (public keys send between two parties to generate secret or shared key) or convince somebody else that he knows the secret. It also enhances security by providing the session key or secret key used by the both the parties along with the information (information send using ZKP) used for identification of both users. That means it provides authentication among both users without creating any signature for the verification of the public keys.

A. Proposed Algorithm

- An integer N = p*q where p and q are prime numbers
- g is a generator of an order q subgroup of Z*p g Є Zp^* $(2 \le g \le p - 2)$ are selected and published.
- The prover P Knows **s** such that **$t=g^s$ mod p** and wants to prove this fact to verifier V
- P selects a random no **r** in [1.. q] and calculates **$X_1= g^r$ mod p** sends to V
- V chooses a random number c in$[1..2^n]$ and sends to P
- P calculates **z=r + sc** and send to V
- V verifies the response **$X_2=g^z\ t^{-c}$ mod p** [i.e. **$g^{r+sc}\ (g^s)^{-c}$ mod p = g^r mod p**]
- X_1 is congruent to X_2
- Repeat steps from 3 to 7 for n number of times
- Algorithm is shown in Fig 3.

V. SECURITY ANALYSIS OF PROPOSED MODEL

A. Cryptanalysis

1) Man -In-The-Middle Attack

In our model, the Prover's secret key never gets transmitted and the intruder never gets a chance to know them. Although the attacker tries to produce a secret key in some brute force method, it will not be able to break out the check as every time a new public key N and a new random challenge question will be used.

2) Replay Attack

In this attack, an attacker tries to replay the previous message and authenticate itself to the verifier. But, as the verifier will be sending different challenge values for each communication, replaying previous communication will not authenticate the sender.

B. Performance Analysis

ZKP also has lighter computational requirement than public key protocols (much faster than RSA). This new protocol provides confidentiality without using any encryption techniques (such as RSA). Hence, it is more efficient because it reduces complexity of algorithm used for encryption techniques. It also increases the performance due to less mathematical calculations used when compared to public key cryptographic systems. This protocol works with low memory when compared with PK encryption algorithms. Moreover a third party may not be able to impersonate sender (Alice) to convince receiver (Bob). More over it is more suitable and efficient for electronic mail security because digital signatures are used for authentication in protocol like PGP. Digital are more complicated and takes more time to create when compared to Zero knowledge Protocol

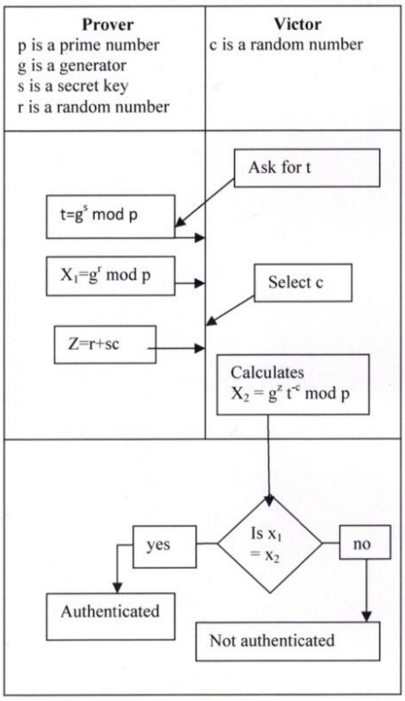

Fig 3: Proposed Algorithm

C. Cryptographic Strength:

The cryptographic strength of ZKP is based on hard to solve problem. It uses problem of factoring large numbers which are product of two or more large prime numbers. It is not easy for attacker to identify the value of secret due to change the value of public key with every communication. The prover also generates a random number and the fingerprints also changes randomly. Thus as public key changes from verifier and a new random number from the prover, becomes extremely difficult for the attacker to break the security.

D. Applications of proposed methodology

This methodology can be used where secret knowledge that is too sensitive to reveal or needs to be verified such as RFID tags, passports, PIN numbers. This methodology can also be applied where key exchange is required like in Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Shell (SSH), Internet Protocol Security (IPSec), Public Key Infrastructure (PKI).

The applications of zero-knowledge proofs[2] in which honesty needs to be enforced without sacrificing privacy are electronic voting, anonymous authentication, anonymous electronic ticketing for public transportation , verifiable outsourced computation. .Much recent attention has been paid to protocols based on anonymous credentials which allow users to anonymously prove possession of a valid credential (e.g., a driver's license), or prove relationships based on data associated with that credential (e.g., that a user's age lies within a certain range) without revealing their identity or other data. These protocols also prevent the person verifying a credential and the credential's issuer from colluding to link activity to specific users. As corporations and governments move to put an increasing amount of personal information online, the need for efficient privacy-preserving systems has become increasingly important and a major focus of recent research. .Another application of zero-knowledge proofs is electronic cash Though no single application can be pinpointed as a compelling application for use of this protocol, it can be a better choice for several applications considering the absence of the third party and the involvement of less mathematical calculations. A few real world applications of the proposed protocol would be Network Authentications, E-mail security, Smart Cards and Key Exchanges.

VI. CONCLUSION

In this paper, we proposed a new security model to address three important active attacks namely cloning attack, MITM attack and Replay attack. We used the concept of zero knowledge protocol which ensures non-transmission of crucial information between the prover and verifier. We analyzed various attack scenarios, cryptographic strength and performance of the proposed model. We have seen a zero knowledge proof is a way to prove that user knows a secret without revealing the secret. Identification Proof based on Zero Knowledge theory. The idea behind this kind of authentication is to associate with each person something unique, so that if the person can prove to have such information, he can identify himself. A practical scenario is proving that a public key is good without revealing the private key. We have seen some examples of classical identification scheme and some new techniques using zero knowledge theory This protocol is more efficient and less costlier when compared to PGP because of digital signature. It is very costlier, time taking and uses complicated mathematics. The new protocol involves mutual identification between two users. This protocol involves authentication and confidentially using ZKP This new protocol provides confidentiality without using any encryption techniques (such as RSA). Hence, it is more efficient because it reduces complexity of algorithm used for encryption techniques. It also increases the performance due to less mathematical calculations used when compared to public key cryptographic systems. This protocol works with low memory when compared with PK encryption algorithms. Moreover a third party may not be able to impersonate sender (Alice) to convince receiver (Bob).

REFERENCES

[1] Hannu A. Aronsson, Zero Knowledge Protocols and Small Systems

[2] C. Chris Erway, Alptekin Küpçü, ZKPDL: A Language-Based System for Efficient Zero-Knowledge Proofs and Electronic Cash

[3] M. Tariq Banday, Effectiveness and limitations of e-mail security protocols

[4] SANS Institute InfoSec Reading Room, Identification with Zero Knowledge Protocols

[5] Mady, Drawbacks of using digital signature

[6] Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield Guidelines on Electronic Mail Security