Comparison of ZKP based Authentication Mechanisms for securing the web server

Kayathri Devi D [#1], Akilan S S [*2]

[#] Department of Information technology, Kamaraj College of Engineering and technology
Virudhunagar, Tamilnadu, India
[1] gayathridevprasad2007@gmail.com
[*] Department of Computer Applications, Mepco Schlenk Engineering College
Sivakasi, Tamilnadu, India
[2] akilan@mepcoeng.ac.in

***Abstract*— Traditional authentication mechanisms aim at validating the authorized users to access the Information Systems such as web servers or services considering the various factors such as text based passwords, image based passwords, multi factors including password, biometric proofs. All these mechanisms store the authenticating factors in some form in a database or in a file system. There comes the thought that what will happen to the stored factors when they are exposed to the adversaries. This particular aspect insists the necessity to safeguard the Information Systems as well as the storage places. ZKP mechanisms eliminate the stored credentials to be validated. Instead, it allows one who wishes to prove his identity to the web server that he knows the authentication secret. The eligible user may be the group of administrators those who are maintaining the web server. We compared the variants of algorithms such as Feige-Fiat-Shamir identification scheme and The Guillou-Quisquater protocol in terms of their time efficiency to support authentication to secure the Web Server.**

Keyword - Authentication, Zero Knowledge Proof, Web Servers, Feige-Fiat-Shamir Identification Scheme, Guillou Quisquater Protocol

I. INTRODUCTION

Authentication is a mechanism to check the credibility of the user of a system. Authentication decides whether the user can access the system or not. Traditional authentication mechanisms like user id and password based authentication suffers the most common dictionary attack or attacks through key logging mechanisms, Shoulder surfing etc., In this paper , we have discussed the various types of authentication systems along with their shortcomings. Zero Knowledge Proof is a proof of the user's credibility without revealing his/her secret to the verifier. The memory requirements will greatly be reduced because of the advent of Zero Knowledge Proof. This type of authentication mechanism is best suitable for applications which pay more attention towards password secrecy. Zero Knowledge Proof finds its applications in Key Exchanges, Network Authentications

II. EXISTING SYSTEM

In the existing authentication mechanisms, the passwords are the authenticating entities passed in clear text form or they might be stored in the server in unencrypted form. Hence the authentication mechanisms needed to be revised. In the following section, we will be discussing the various types of authentication mechanisms

A. Derived Passwords

Storing the password in plain text format is a serious risk. Storing encrypted passwords may also be decrypted. Storing message digests of passwords is another improvement that can be done to safeguard the passwords. Server asking the client for partial passwords may also be helpful to avoid shoulder surfing and keyboard logging.

B. Token based authentication

Token authentication is nothing but generating one time passwords to the registered email or device generated randomly by an authentication token with a pre programmed seed value. The tokens are of two types: Challenge/Response tokens or time based tokens

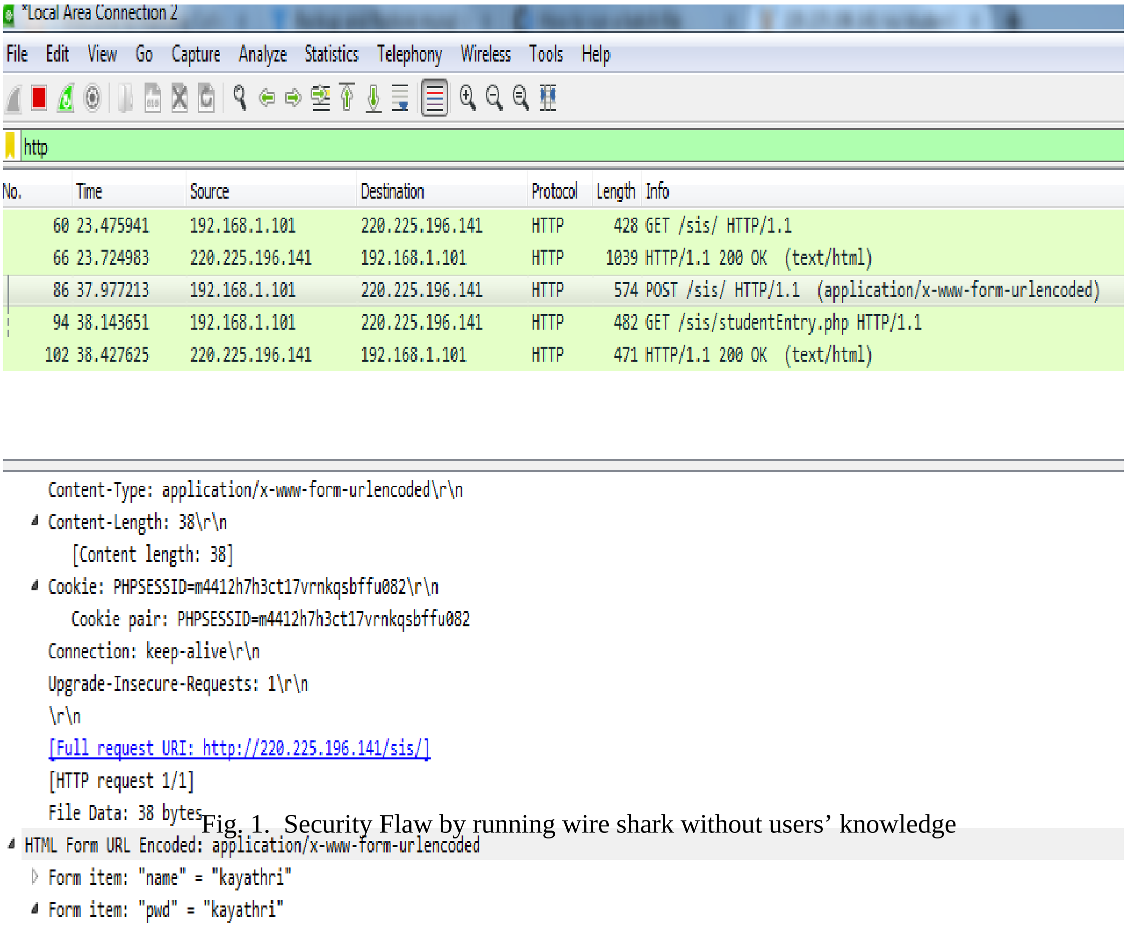
C. Certificate based authentication

Digital certificate based authentication is stronger compared to password based authentication. Because of the fact that, digital certificate is possessed by the prover.

D. Biometric based authentication

Biometric authentication is based on something the user has in his body which is unique. The features considered are iris lines of an eye ball of a person, fingerprint, voice etc., It requires biometric authenticating device also to authenticate the users.

The following screenshot shows the security flaw in the traditional password based authentication systems. Wire shark tool which captured the username and password.


*Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source           Destination      Protocol  Length  Info
   60 23.475941   192.168.1.101    220.225.196.141  HTTP       428 GET /sis/ HTTP/1.1
   66 23.724983   220.225.196.141  192.168.1.101    HTTP      1039 HTTP/1.1 200 OK  (text/html)
   86 37.977213   192.168.1.101    220.225.196.141  HTTP       574 POST /sis/ HTTP/1.1  (application/x-www-form-urlencoded)
   94 38.143651   192.168.1.101    220.225.196.141  HTTP       482 GET /sis/studentEntry.php HTTP/1.1
  102 38.427625   220.225.196.141  192.168.1.101    HTTP       471 HTTP/1.1 200 OK  (text/html)
```

```
    Content-Type: application/x-www-form-urlencoded\r\n
  ◢ Content-Length: 38\r\n
      [Content length: 38]
  ◢ Cookie: PHPSESSID=m4412h7h3ct17vrnkqsbffu082\r\n
      Cookie pair: PHPSESSID=m4412h7h3ct17vrnkqsbffu082
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://220.225.196.141/sis/]
    [HTTP request 1/1]
    File Data: 38 bytes
◢ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▷ Form item: "name" = "kayathri"
  ◢ Form item: "pwd" = "kayathri"
```

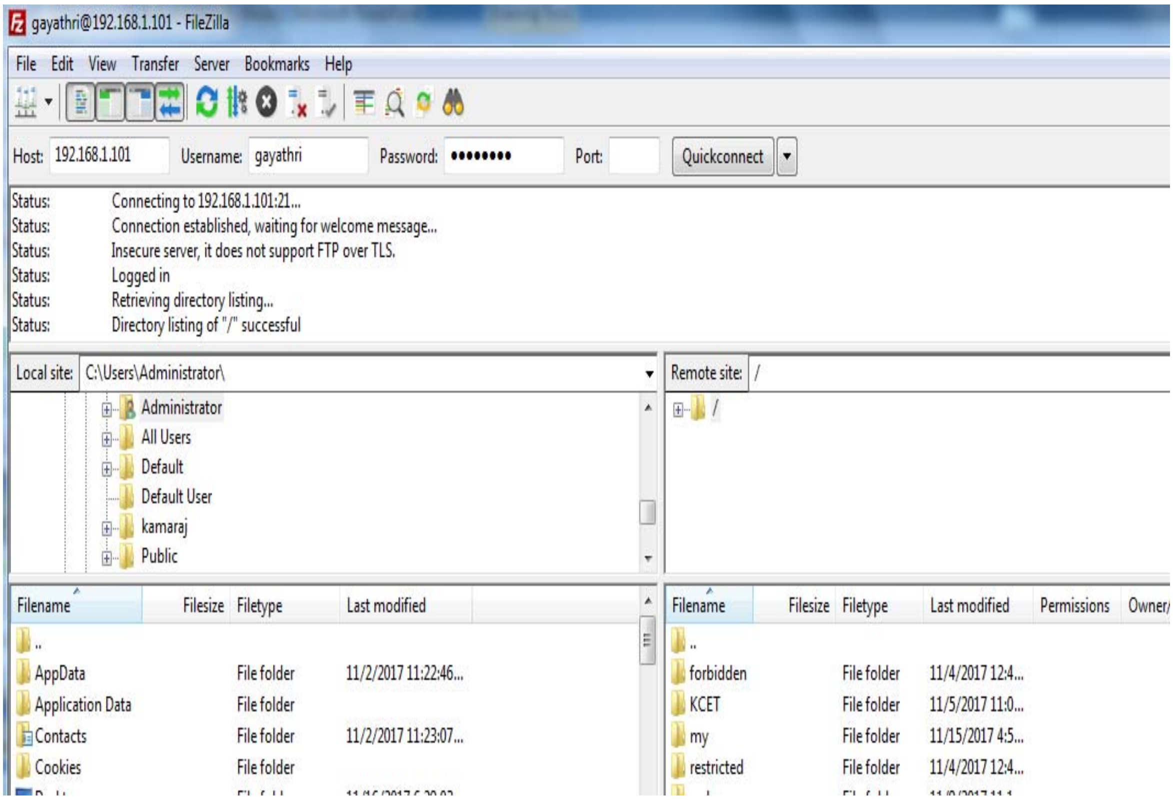
Fig. 1. Security Flaw by running wire shark without users' knowledge

III. PROPOSED SYSTEM

The Proposed System focuses more on eliminating the necessity to store passwords in the database. Zero Knowledge Proof can definitely bring an evolution towards this traditional password based authentication mechanism. Let us revisit some of the algorithms to identify the prover.

The comparison of Fiat – Shamir algorithm and Guillou Quisquater shows the time efficiency of those algorithm s to verify the proof of statement provided by the prover.

The proposed system will be suitable for Entity Identification especially to safeguard the web server. The web server is one which is a hardware/software with trusted users issued with appropriate credentials. Web server is responsible for showcasing the Information about the particular organization/Industry. Web server is assigned with a public IP Address. Using the credentials, the user can access the web server to update or create or delete a new or existing web page. In traditional web server environment, the content update will be performed by the credible user for appropriate tasks through File Transfer Protocol server and client software.[FileZilla Client and FileZilla server software]



Host: 192.168.1.101 Username: gayathri Password: •••••••• Port:

```
Status:     Connecting to 192.168.1.101:21...
Status:     Connection established, waiting for welcome message...
Status:     Insecure server, it does not support FTP over TLS.
Status:     Logged in
Status:     Retrieving directory listing...
Status:     Directory listing of "/" successful
```

Local site: C:\Users\Administrator\

- Administrator
- All Users
- Default
- Default User
- kamaraj
- Public

Remote site: /

- /

Filename	Filesize	Filetype	Last modified
..			
AppData		File folder	11/2/2017 11:22:46...
Application Data		File folder	
Contacts		File folder	11/2/2017 11:23:07...
Cookies		File folder	

Filename	Filesize	Filetype	Last modified	Permissions	Owner/
..					
forbidden		File folder	11/4/2017 12:4...		
KCET		File folder	11/5/2017 11:0...		
my		File folder	11/15/2017 4:5...		
restricted		File folder	11/4/2017 12:4...		

Fig. 2. Traditional FileZilla FTP Client Software

In Fig 2, the server side of the web server can be updated with the help of FTP Client software. There is a provision to investigate the login history when there is an attack.

A. Fiat Shamir ZKP Algorithm

- It is the algorithm used by the potential prover to reveal his/her identity to the verifier.
- Some trusted third party will provide the multiplicative value of n which is the product of two large primes p and q. It is a one time setup.

$$n=p*q \qquad (1)$$

- Each prover will select his/her own secret value S which must be relatively prime to n.

$$\text{ie., } \gcd(S,n)=1 \qquad (2)$$

- Each prover will compute their own public key value by the following formula:

$$v=s^2 \bmod n \qquad (3)$$

- The prover publishes the result of equation(3) which is nothing but v to the verifier without revealing the secret S.
- Also, the prover chooses a random number r and computes

$$r^2 \bmod n \qquad (4)$$

where r may be any random positive integer.

- Verifier randomly selects a single bit value of 0 or 1 called e which is called the challenge and send e to the prover
- The prover computes the response by using the following formula:

$$y = r*S^e \bmod n \qquad (5)$$

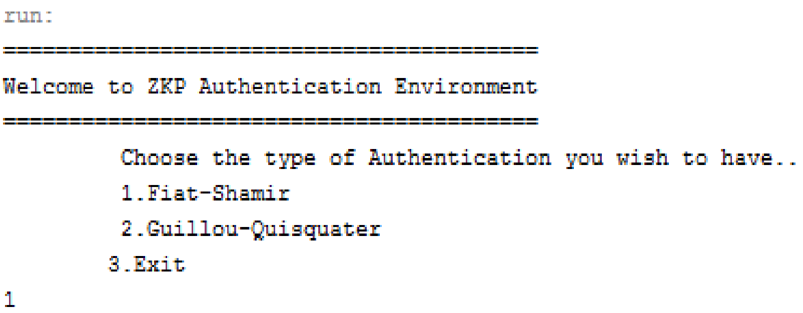
- The computed value by the equation(5) will be sent to the verifier.
- The verifier will check the value of y. If the value is 0, the verifier will reject its proof.
- Else, the verifier will compute another value

$$y^2 \text{ congruent to } r^2 * v^e \bmod n \qquad (6)$$

B. Test Bed Environment :

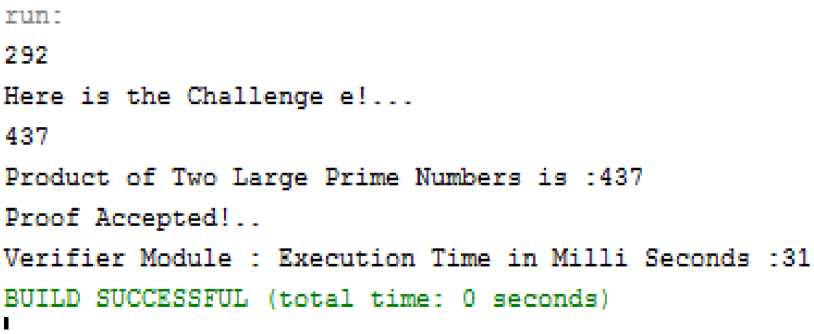
- Fiat – Shamir Cryptographic Identification scheme is implemented in Java with NetBeans IDE
- The Client Server model was applied

- Time Efficiency for both prover and verifier model was calculated in terms of milliseconds
- The results are shown in the following figures.



```
run:
=========================================
Welcome to ZKP Authentication Environment
=========================================
         Choose the type of Authentication you wish to have..
         1.Fiat-Shamir
         2.Guillou-Quisquater
        3.Exit
1
```

Fig 3 : Prover Module



```
run:
292
Here is the Challenge e!...
437
Product of Two Large Prime Numbers is :437
Proof Accepted!..
Verifier Module : Execution Time in Milli Seconds :31
BUILD SUCCESSFUL (total time: 0 seconds)
```

Fig 4: Verifier Module

C. Advantages of Fiat-Shamir Scheme:

- Simple algorithm to ZKP
- No need to share the secret
- Time Efficiency .The algorithm works in a faster rate

TABLE I. Performance Analysis of FS_ZKP

Module Name	**Time Taken**	**Actions**
Prover	6 s	Sending v,r,n,y to Verifier
Verifier	0.3 s	Generating random challenge e and sending e to prover

D. Guillou Quisquater Authentication Scheme:

- Very similar to Fiat – Shamir Identification algorithmic scheme
- Fiat –Shamir algorithm suffers from impersonation attack, chosen text attack.
- The challenge e in Fiat-Shamir algorithm takes only two random values 0,1
- Here comes the slight change in terms of e value. It can be called as C
- C ranges from 1 to e
- Proceed with the algorithm
- Compared to Fiat-Shamir, Guillou Quisquater algorithm is better in providing security
- Also, Compared to Fiat-Shamir, Guillou Quisquater will consume more time for computation purposes

TABLE III. Performance Analysis of GQ_ZKP

Module Name	**Time Taken**	**Actions**
Prover	20 s	Sending v,r,n,y to Verifier
Verifier	0.4 s	Generating random challenge e and sending e to prover

IV. EXPERIMENTAL ANALYSIS

Experiments show that the Guillou Quisquater's Identification scheme is better that the Fiat-Shamir Simple Identification Scheme.

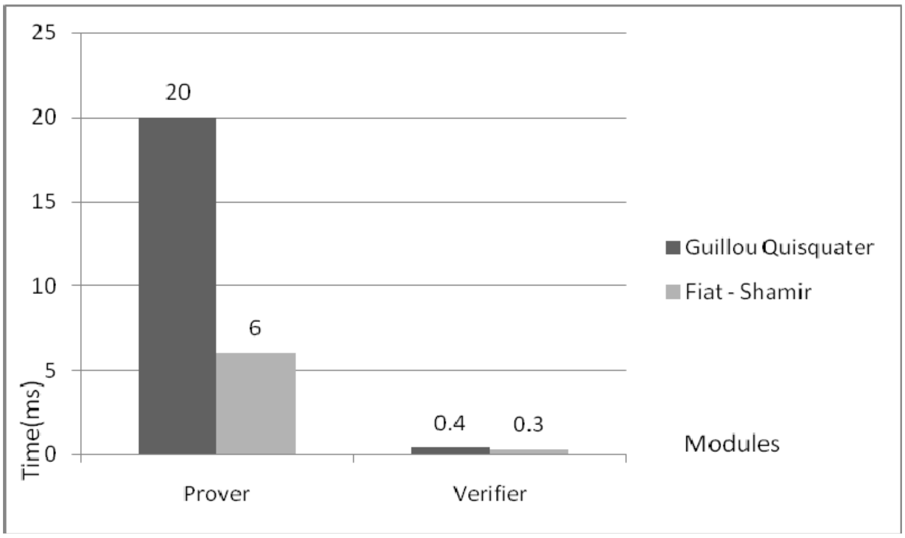


Fig 4 : Experimental Analysis

V. CONCLUSION

This work suggests replacing the traditional Password based authentication with Zero Knowledge Proof authentication schemes in applications which require at most security from attacks such as shoulder surfing, Password sniffing, Hacking/Stealing passwords etc.,

REFERENCES

[1] Lum Jia Jun, Brandon, " Implementing Zero Knowledge Authentication with n Zero Knowledge (ZKA_wzk)", proceedings of Pycon Asia-Pacific 2010

[2] Ahamed Patel, Kenan Kalajdzic, Laleh Golafshan, Mona Taghavi, "Design and Implementation of a Zero- Knowledge Aythentication Framework for Java Card", International Journal of Information Security and Privacy, 2011

AUTHOR PROFILE

D.Kayathri Devi received her Master Degree in Computer Science and Engineering from Anna University, Chennai in the year 2009. Currently, She is pursuing her Doctoral Degree under Anna University, Chennai. Her research area includes detecting and preventing attacks over Information Systems.

S.S AKILAN received his Master Degree in Computer Science and Engineering from Anna University, Chennai in the year 2009. Currently, He is pursuing his Doctoral Degree under Anna University, Chennai. Her research area includes Internet of things.