SECURITY ANALYSIS OF PASSWORD BASED MUTUAL AUTHENTICATION METHOD FOR REMOTE USER

Mrs. P.Venkateswari
Assistant Professor / CSE
Erode Sengunthar Engineering College,
Thudupathi

Dr.T.Purusothaman
Assistant Professor / CSE& IT ,
Government College of Technology,
Coimbatore

ABSTRACT

Nowadays Communication becomes wireless and devices are ubiquitous in nature, it mandatory to verify the identity of the parties before starts sending and receiving the messages. For such identity verification so many authentication schemes are available. Password based is the oldest and simplest way of Authentication. Since it is vulnerable to impersonation and replay attack, instead of depending on one factor it is better to have two factors. The second factor may be a possession of physical cards like smart card. In this paper the existing password based remote user authentication scheme is analyzed and the remedy to overcome the replay attack is proposed.

Keywords: Communication, authentication, remote.

1.INTRODUCTION

Authentication enables a legitimate user to login onto a remote server, which is more important in mobile business. Lamport proposed a password authentication scheme to provide authentication between the users and the remote server. Since then, many password-based remote user authentication schemes have been proposed .In a smart card based password authentication scheme, the smart card takes the password from the users as input, computes the login message and sends the login message to the server. The server checks the validity of the user's login message. In the mutual authentication situation, not only the server can verify the user but also a user can verify the server.

The adversary is modeled as follows :

(a)The adversary can tap the communication channel between the users and the server during the login and authentication phase.

(b) The adversary either can extract the information by obtaining the smart card or can get a user's password. The adversary cannot do both, or the adversary can login the server as a legitimate user.

1.2 MOTIVATION.

Every time a person uses a smartcard, the implicit assumption is that the computer has not been compromised. The possibility always exists that the computer or any other device implanted on the Net along the way has been infected by a hidden software routine that exploits the user's identity after authentication has been accomplished. Because users authenticate themselves to a potentially compromised computer, they can never be secure in their subsequent computer transactions.

Perhaps the greatest inhibition to the use of smartcards in electronic commerce is their variety. The chances of adoption of smartcards as the universal means for authentication of individuals in electronic commerce are nil. Access security requirements vary depending on the severity of risks and local circumstances. Therefore, a wide range of smartcard solutions is almost certain to persist. Technology obsolescence and proliferation will continue to inhibit the adoption of smartcards and reduce the applicability of this means for solving personal privacy issues.

In order to develop a secure authentication scheme for the smart card applications and to resist Replay Attack from the adversary. For this we use a strong cryptographic technique such as strong cryptographic symmetric key algorithm.

2.1 LITERATURE SURVEY

Fan-Chan-Zhang's scheme consists of Registration, Login, Authentication phases.

Registration

The server S chooses two distinct random large primes p and q and computes n=pq. The server keeps p , q secret and chooses a private key s for the symmetric encryption.

Login

A user U inserts his smart card to a device reader and inputs his identity ID and password pw. The smart card randomly chooses u and sends the authentication information to the server S.

Authentication

In the Authentication, User and Server authenticated with each other by using some authentication information.

2.2 EXISTING SYSTEM

Existing System uses Registration, Login, Authentication phases.

In the Registration phase, User should Register into the System by giving the User's id and the User's password. Server encrypts the hash

code of user's id (id) and the password(pwd) and card id(cid) and the random string v. These card id and the v chosen by the Server. Server stores the card id, id, c, n in the User's card. Here c is the cipher text of hash of password, hash of id, card id and v.

In the Login phase, Registered User can able to login to the system by giving the Random Number u. And the server decrypts the c and verify the card id and the User's id.In the r Authentication phase,Server select a string and computes $\alpha = r \oplus u$ and$\beta = h(r||u)$ and Server sends the α, β to the client. Next the Client computes the $r = \alpha \oplus u$ and verifies β. However, this System affects with Replay Attack.

2.3 PROPOSED SYSTEM

Proposed System uses Registration, Login, Authentication phases.

In the Registration phase, User should Register into the System by giving the User's id and the User's password. Server encrypts the hash code of user's id (id) and the hash code password (pwd) and card id(cid) and the random string v. These card id and the v chosen by the Server. Server stores the card id, id, c,(n,e) in the User's card. Here c is the cipher text of hash of password, id, card id and v and (n,e) is the key.

In the Login phase, Registered User can able to login to the system by giving the Random Number u and Current Time Stamp. And the server decrypts the c and verifies the card id ,User's id and the Time Stamp. By validating the these information Server allows the correct User for further Authentication.

In the Authentication phase, Server selects a string r and computes $\alpha = r \oplus u$ and $\beta = h(r||u)$ and Server sends the α, β to the client. Next the Client computes the $\alpha = r \oplus u$ and verifies β. Finally, Client and the Server authenticated with each other.

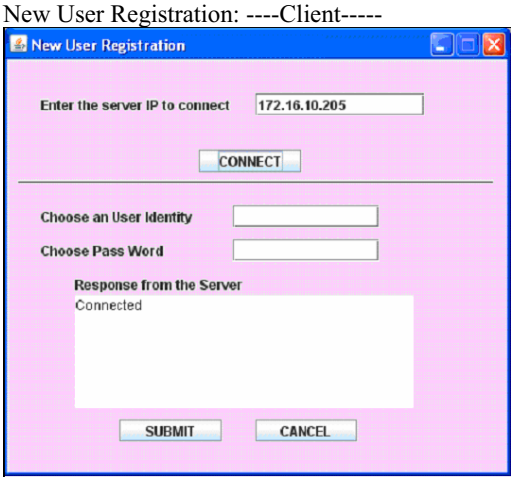
To overcome impersonations attack is simply attach the hashed string of user id & password send along with other components and it can be recalculated by the server and the validity was verified. It increases the computational time and makes the verification process be lengthier one.

3. IMPLEMENTATION

The modules used in the development of the prototype are

Screen shots

New User Registration: ----Client-----

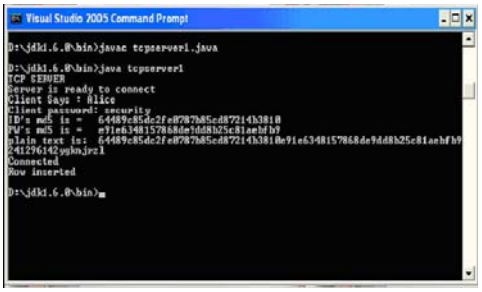


Screenshot 1

This is a design lay out of the User Registration screen, It provide necessary text boxes and control boxes which enables the client to feed the data in user comfortably The Screenshot 2 illustrates the response produced by the server after receiving the information from the client.

Screenshot 2

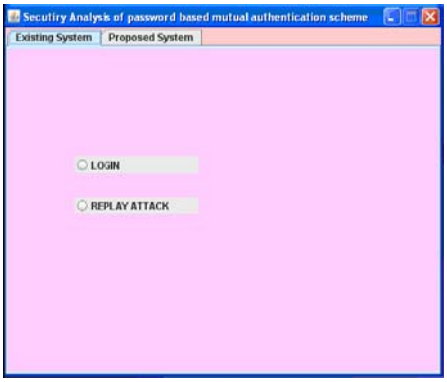
------Server------



Screenshot 3

The operations held by the server to register the user is visualized in screenshot 3.

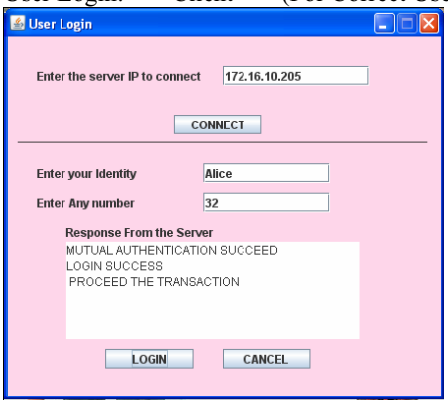
-----Client----



Screen Shot 4 Client side -GUI

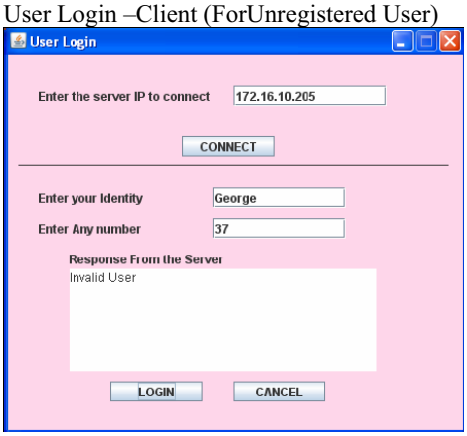
The Screenshot 5 and 6 shows the login process of the Registered and Unregistered User. The server response to the Login process is visualized in the Screenshot 7.

User Login: -----Client----- (For Correct User)



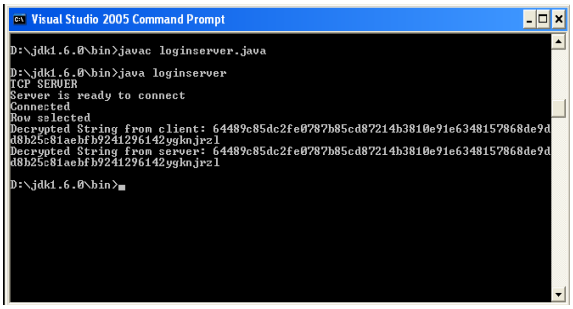
Screenshot 5

User Login –Client (ForUnregistered User)



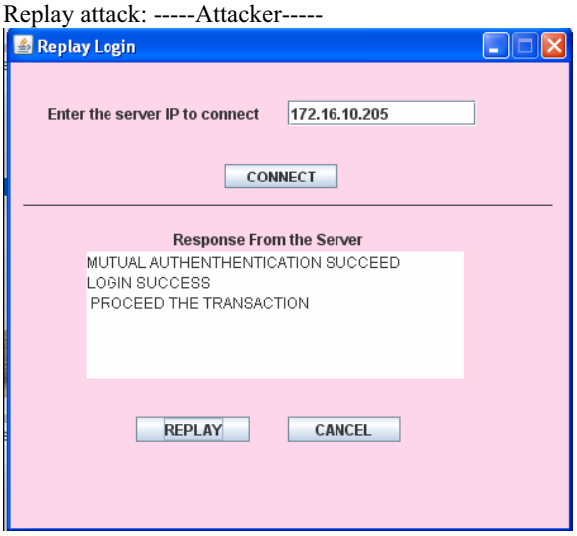
Screenshot 6

----Server----



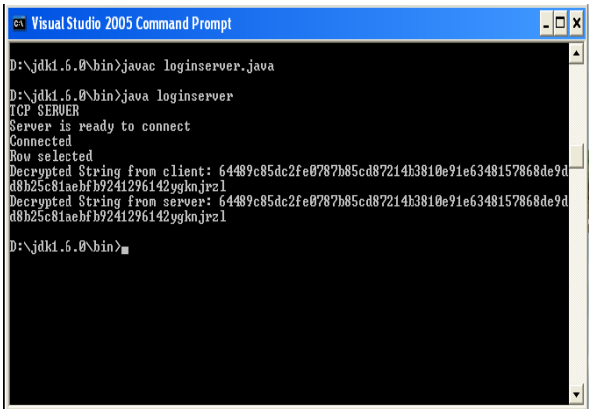
Screenshot 7

Replay attack: -----Attacker-----



Screenshot 8

-------Server-------

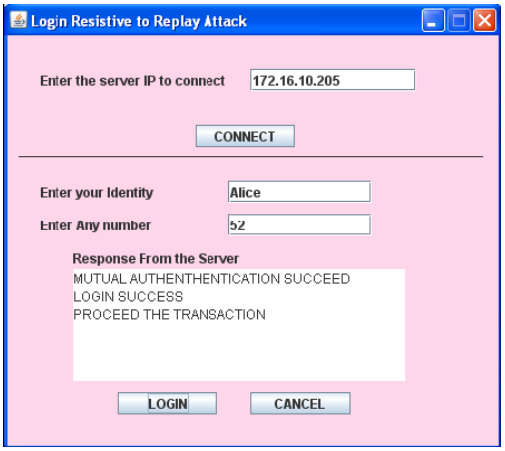


Screenshot 9

Replay Attack is visualized through Screenshot 8 and 9.

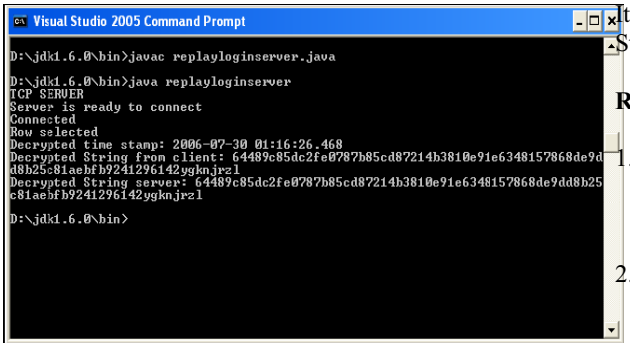
Proposed Login System:

-------Client-------



Screenshot 10

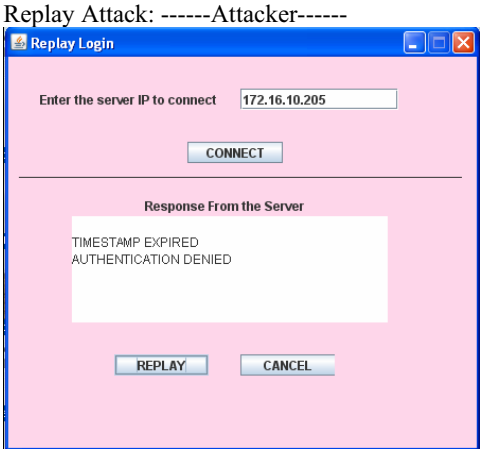
------Server------



Screenshot 11

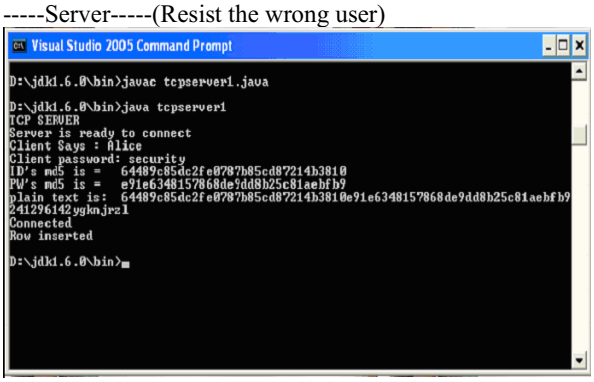
The Login process as per the proposed system and the response of the server which is resistive to replay attack are visualized in the Screen shot 10 &11.

Replay Attack: ------Attacker------



Screenshot 12

-----Server-----(Resist the wrong user)



Screenshot 13

The Resistive ness of the proposed system against Replay Attack is proven in the Screenshot 12 and 13.

4. CONCLUSION

Thus the system resistive to the Replay Attack. But still suffers from impersonation attacks. The remedy of the impersonation is also proposed but yet to be implemented. Thus it becomes an strong Mutual Authentication Scheme. It is applied anywhere when the System needs Strong Mutual Authentication.

REFERENCES

1. Zuowen Tan Security Analysis of Two Password Authentication Schemes, 2009 Eighth International Conference on Mobile Business.
2. L. Lamport. Password authentication with insecur communication. Communication of ACM 24(1981).
3. H. Guo, Z. Li, Y. Mu, X. Zhang, Cryptanalysis of simple three-party key exchange protocol, Computers & Security,Vol. 27, No. 1-2, pp. 16-21, March 2008.
4. J. Xu, W.-T. Zhu, D.-G. Feng, An improved smart card based password authentication scheme with provable security, Computer Standards & Interfaces, doi:10.1016/j.csi.2008.09.006.
5. T. Xiang, K. Wong, X. Liao, “Cryptanalysis of a password authentication scheme over insecure networks”, Computer and System Sciences, Vol. 74, No. 5, pp. 657- 661 August 2008.
6. C.L. Hsu, Security of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards & Interfaces 26 (3) (2004) 167–169.

BIOGRAPHY

Dr.T.Purusothaman currently working as a Assistant Professor (RD) in the department of Computer Science and Engineering and Information technology, Government College of Technology, Coimbatore. He has twenty one years of teaching experience. He has completed Ph.D in the area of Network Security and Grid Computing. In his thesis, a novel key management scheme was proposed to provide service only for the paid customers in Internet. He has successfully completed a project funded by DIT (Government of India) in the area of cryptanalysis in the year 2006. He has presented a number of papers in various National and International conferences. Many of his papers were published in IEEE Explore. He has to his credit several International Journal Publications in reputed journals including Journal of Grid Computing, Springer. His research interests include Network Security, Grid Computing and Data Mining.

P.Venkateswari, working as an Assistant Professor in CSE Department at, Erode. She had completed her M.E in Computer Science from Government college of Technology and is pursuing Ph.D. in the area of network Security. Currently she is working as a HOD & Assistant Professor in CSE Dept, Erode Sengunthar Engineering College Erode, TamilNadu, India and she is having 18 years of Experience in Teaching. She had published 12 Papers in Various National Conferences and she had presented 4 Papers in Various International Conferences held at many Engineering Colleges. She has 2 numbers of International publication. Her interests include Network Security, Distributed Systems and Social Network