Middle-East Journal of Scientific Research
24 (Recent Innovations in Engineering, Technology, Management & Applications): 194-196, 2016
ISSN 1990-9233; © IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.RIETMA131

Implementation of Password Authentication Scheme Using Smartcard for Client-Server

R. Sridevi, S. Rosi and G. Sathish

Department of MCA, Priyadarshini Engineering College, Vaniyambadi, India

Abstract: User authentication is accessing resources, particularly with Personal Digital Assistants (PDAs), Vending machines using Smartcard. User authentication is difficult for systems to provide safe access over private information or personalized services. User authentication is the primary line of security for any handheld devices that comes into the hands of any unauthorized individual. Password (PWD) or Personal Identification Number (PIN) based authentication is the leading mechanism for verifying the identity of an authentic device user. It is mainly focused on security requirements using smartcard authentication scheme. Implementation of more secure schemes and easy to understand the schemes compared to previous schemes.

Key words: Authentication · Password · Smartcard · Security

INTRODUCTION

Implementation of password authentication scheme using smart cards is a better solution for an internet, e-commerce technologies and services, such things as online shopping, online gaming, e-learning, e-health, internet banking sectors, online trading and so on., are offered the internet to given a good solution for many applications. The fundamentals of networking and telecommunication are being changed and the integrated networks becoming a reality owing to the wireless communication revolution. Personal communications networks, wireless LAN's, mobile radio networks and cellular systems are harboring the premise of fully distributed mobile computing and communications anytime, anywhere by freeing the user from the smart card [1]. The communication channel employed in wireless environment is air. It given opportunity an password or other sector information to access the un-authorized user. So the security is very important sector in password authentication scheme, e.g., authenticity. Authentication is a method to validate user who attempt to validate access a computer system or resources, to ensure they are authorized. The security fundamental overall mostly based on three information that who you are, what you have and what you know. For proving who they are, users can provide their name, email address, or a user ID. Than the users can produce service cards (i.e., ATM cards), physical keys, digital certificates, smart cards, or one-time login cards such as the Secure ID card. So the users are given they password or pass phrase, or a Personal Identification Number (PIN). Password authentication scheme is the most techniques for verifying the identity of computer users. In the existing traditional setup the ID and password are maintained by the remote system in a verification table [2]. If a user wants to log in a remote server, then the user must to submit his ID and password to the server. The computer server receives the login message and checks the eligibility of the user by referencing the password or verification table. If the submitted ID and password matches with the corresponding pair stored in the server's verification table, then user will be granted access to the server. The password authentication secure the information on the user is saved. In the scheme the authentication server and user, the scheme users can identity of the individual login. Implementation of the password the user can create a valid login message to the authentication server. Authentication Server checks the validity of the login message and provides the access right [1].

Problems in the Traditional Method: There are many problems are existing in the real world of wireless environment. In that there are two important problems are found in this existing traditional mechanism and taken to this proposal is,

- The administrator of the server will come to know the password, because the Server maintains the password table.
- An intruder can impersonate a legal user by stealing the user's ID and password from the password table [3].

Corresponding Author: Ms. R. Sridevi, Department of MCA, Priyadarshini Engineering College, Vaniyambadi, India.

The internet is involved in many attacks such as denial of service attack, forgery attack, forward secrecy attack, server spoofing attack, parallel session attack, guessing attack, replay attack and stolen verifier attack. The work of proposes an efficient password mutual authentication scheme with smart card using RSA. Security has analysis of this scheme without password table, which circumvents most of these attacks. Based on our proposed method, the particular scheme does not maintain the password table, but instead maintains the one time registration date and time of the users in the encrypted format by using its secret key. It is difficult for the attacker to find the password without knowing the registration time of the user and the secret key of the particular scheme [2].

Preliminaries: In this section, provide the information about one-way hash function and RSA in these mathematical concepts from the basic of the security.

One-Way Hash Function: A one-way hash function is that generates a fixed string of numbers from a text message h: x -> y function is following,

- The function h takes message of variable length as the input and converts it into the output of a fixed-length message digest.
- The function h is one-way in the sense that, given x, it is trivial to compute h(x) =y. However, given y, it is difficult to compute h1 (y) ¼ x [1].

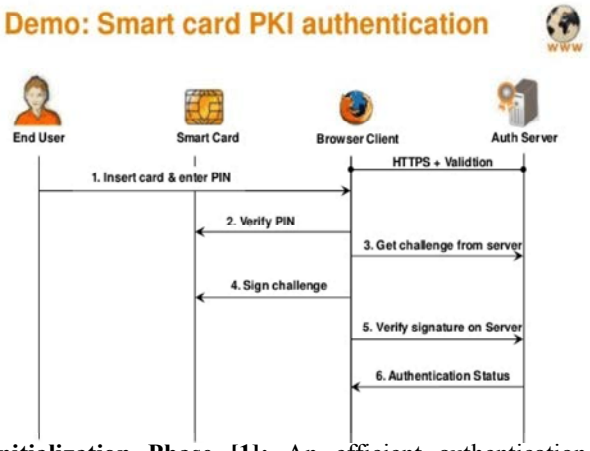
RSA Algorithm for Security: The RSA algorithm has been very attractable for smart card security problem. Normally we know the meaning for RSA that is mathematically related keys for encryption and decryption.

RSA is widely used asymmetric encryption algorithm. E and D with former the public file and the latter kept securer. That is properly implements far cannot be cracked in acceptable time. This problem was related to the keys, which in RSA specifically, or sets of two special members. We of course start out with the message itself, symbolized by m, which is to the "encrypted". There are four procedures that are specie and essentials to a public key cryptosystem [3].

- Deciphering and the enciphered message gives you to original message, specifically
  D (E (M)) =M
- Reversing the procedures still return to be M.
  E (D (M)) =M
- E and D are easy to compute for this procedure.
- The publicity of E does not compromised the secrecy of D, meaning you cannot easy figure out for D form E.

With the given E we are still not given an efficient way of computing D. If C=E (M) is cipher text, then trying to figure out D by trying to satisfy M in E of M=C is a readably difficult, the number of message to test would be impractically large [4].

Four Phase Smart Card Authentication: In this paper we proposes an implementation of secure password authentication scheme for client and server environment based on smartcard and also using four phases in implementation purpose. Those are, the initialization phase, the registration phase, the login phase and the authentication phase. That particular scheme does not maintain the password table [5].



Initialization Phase [1]: An efficient authentication scheme can perform smart card issue operation whenever and wherever a new user registers through the registration phase. Here using the D is deciphering and E enciphering and M is finite the message and also it's a set of two special numbers R and S, then the server perform those based on operations. The server performs this formulation m= ((r-1)*(s-1)). The smart card is identification password ID and user calculation for symmetric key.

Registration Phase [2, 4]: Let R and S as a secret key maintain by client and server environment be a secure on way hash function. To access the server S and user U submit their identity ID, password PWD and special numbers R and S, which is used to protect the password PWD and submit the server S. Upon receiving the registrations request, the server S verifies credential of

identity ID. If it points ID and its database that mean unauthorized person is register with some other user means suddenly the server ask for identity to the user.

Login Phase: The user enters his or her password PWD and then the smartcard reader determine for user password invalid or not to check it.

- Smartcard check the legality of ID and password ensured.
- Smartcard select the special numbers R and S for use construct the massage to send server S.
- The user to allow choose a password and this password is stored in the smartcard by secure techniques.

Authentication Phase [2, 4]: When the identical server receives the secret message M from the user U at the time T, where the time T is corrected means that particular time and date of information is to me stored in table. After the message is received server authenticates give the login for user.

- The expected legal time is the travel for transmission delay means the server will reject the log in request
- When the server computes the message and its verification true means the server will accept the login request otherwise the server reject the login request.
- After the correct verification of secure authentication user U and servers S identity the secret key.

CONCLUSION

Finally this paper concludes that table based authentication scheme does not provide reasonable way of authenticity by securing your passwords. Why because the table of passwords may be stored somewhere and it is accessible or harmed by intruders. To overcome this, we have demonstrate a secure password authentication security analysis and performance comparison based on card based password mechanism and also, we provide more security and to be away from the intruders, the four phase authenticity mechanism were included in this concept in future it may be extended or incorporated with other security features.

REFERENCES

1. Journal of information security and applications 19, 2014. A secure remote user mutual authentication scheme using smart cards, Marimuthu karuppiah, R.Saravanan, School of computer and engineering, vellore 632014, Tamil nadu, India, pp: 282-294.
2. International Journal of Network Security, May 2012, An efficient Password Authentication Scheme for Smart Card, Rajaram Ramasamy, Department of Computer Science and Engineering, Thiagarajar College of Enginneering, Madurai, Tamil Nadu, India, 14(3): 180-186.
3. Journal of information, Jan-2013, secure password based remote user authentication scheme against smart card security breach, Ding Wang, College of computer science and Technology, Harbin Engineering University, China, 8(1): 148-155.
4. International Journal of Engineering Technology and Advanced Engineering, vol 4, issue 6, June 2014, An Efficient Password Based Authentication Scheme Using Time Hash Function And Smart Card, Dr.P.Kumar, Assistant Professor, Department of Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India, 4(6): 764-770.
5. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC40.