Generating Multi Server Environment for implementation of Ideal Password Authentication Scheme

Kuljeet Kaur
School of Computer Applications
Lovely Professional University
Phagwara, India

Dr.G.Geetha
School of Computer Applications
Lovely Professional University
Phagwara, India

***Abstract*—Ideal Password Authentication Scheme comprises of two identity authentication parameters Fingerprint and Password. When two identity authentication parameters are used then for fortification of transport layer, mutual authentication is done in the Multi Server Environment of an organization. Paper elucidates the process for generating Multi Server Environment in an Organization. Complete implementation of ideal password authentication scheme in the multi server environment of an organization is revealed in the paper. Proof is derived in the paper that mutual authentication if done in the multi server environment of an organization then Phishing, IP Spoofing and Server spoofing would almost diminish. Overall paper concludes that intruders or hackers would be unable to spoof or hack at any level at the transport layer in multi server environment and fortification of transport layer security protocol is proved.**

***Keywords*—Ideal Password Authentication Scheme, Multi Server Environment, Fortification, Transport Layer**

I. Introduction

When Public Network is used and resources are to be accessed from remote systems then proving identity becomes complex [1]. Some parameter like Password, Smart Card and Fingerprint etc are required for proving the identity. Generally in online transactions Password is mainly used as identity authentication parameter. Common Password Authentication Schemes like RSA Based and ElGamal Based could not withstand mutual authentication requirement but Hash Based can with stand the security requirement of mutual authentication. Password if used as an identity authentication parameter then intruders can try many attacks like denial of service attack, replay attack, session hijacking, man in the middle attack etc. So there is need to add one more tier of security. For this either smart card or fingerprint could be used as an identity authentication parameter.

The structure of the remainder of the paper is as follows. In Section II process of generation of an ideal password authentication scheme is defined. In Section III process for generating multi server environment is elucidated. In Section IV implementation of ideal password authentication scheme in the multi server environment of an organization is given. In Section V mutual authentication in the multi server environment of an organization is illustrated, it results in fortification of transport layer security protocol. In Section VI security from Phishing, IP Spoofing and Server Spoofing is shown. In Section VII conclusion is derived that ideal password authentication scheme when implemented in the multi server environment of an organization would result in fortification of transport layer security protocol.

II. Generating an Ideal Password Authentication Scheme

As majority of the organizations use Password for Online transactions, so security of the Password becomes prime concern for all the users [1]. Majority of the attacks could be tried by the intruders like Dictionary Attack, Denial of Service, Forgery Attack, Man in the Middle Attack etc to break the security of the password. So there is need for an ideal password authentication scheme [2]. Generation of an Ideal Password Authentication scheme needs that common password authentication schemes should be defined on the basis of some attacks and security requirements which intruders hack or spoof. Figure 1 elucidates the process followed for generating an ideal password authentication scheme. Process states that RSA Based and ElGamal Based Scheme could not withstand the security requirement. These schemes are vulnerable to Dictionary Attack, Denial of Service, Forgery Attack, Man in the Middle Attack, Session Hijacking, and Replay Attack etc. But Hash Based scheme is vulnerable to only smart card loss attack but can withstand the security requirement of mutual authentication.

So Hash Based Scheme is used to generate an Ideal Password Authentication Scheme because this scheme requires mutual authentication in the multi server environment [3]. New identity authentication parameter Fingerprint would be used for adding one more tier of security to the transport layer security protocol. Password and Fingerprint as identity authentication parameters would generate an Ideal Password Authentication Scheme. Smart Card would not be used as identity authentication parameter for ideal password authentication scheme because it is vulnerable to smart card loss attack (If the smart card of the legitimate user is lost or

Proc. of the Intl. Conf. on Advances in Electronics, Electrical and Computer Science Engineering — EEC 2012
Edited by Dr. R. K. Singh.

ISBN: 978-981-07-2950-9

stolen the attacker can easily change the password of the smart card by using password guessing attacks, dictionary attacks and could impersonate the legitimate user in order to login into the system). Mutual Authentication would be done for authenticating Client Side and Server Side both. When mutual authentication would be done with the help of ideal password authentication scheme then it would result in data integrity and security. Further two protocols of SSL (Secured Socket Layer) record and handshake protocol would be enhanced as of data integrity and security [4]. Enhancement of record and handshake protocol would strengthen SSL and would result in the fortification of transport layer security protocol.

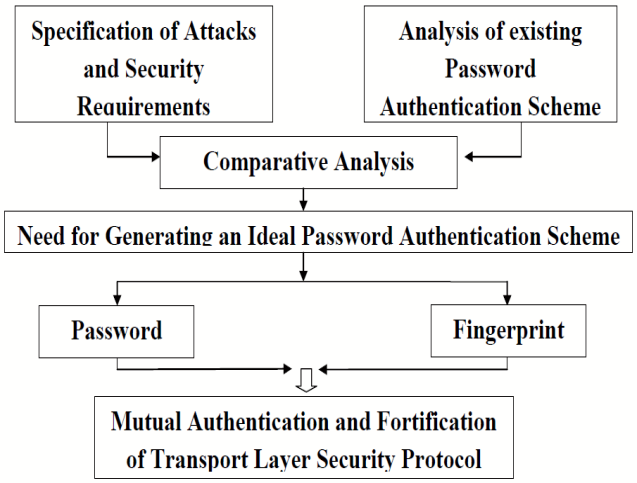


Figure 1: Generating Ideal Password Authentication Scheme

Overall an Ideal Password Authentication Scheme would result in Fortification of the Transport Layer Security Protocol.

III. Process for generating a Multi Server Environment

Multi server environment means having more than one server. Reason for using multi server environment is save the transaction or communication from Phishing, IP Spoofing (This is basically lying about an IP address. In this the source address given is normally incorrect [5]. So when the source address is not true then it lets an attacker assume a new identity because the source address is not the same as the attacker's address, so any replies generated by the destination would be sent to the attacker. And if the attackers adhere to the protocol requirements then the connection would be very well maintained.

IP Spoofing exploits trust relationships between routers) and Server Spoofing (In this attacker pretends to be server to manipulate sensitive data of the legitimate users. The attacker creates a situation to masquerade legitimate user by falsifying data and getting an access as legitimate user. It generally happens because TCP/IP does not provide any mechanism by which authentication of source or destination message could be proved. Because of this data becomes vulnerable to server spoofing attack) etc.

Process for generating multi server environment is:

1. Establish a connection with the Server after opening First SQL SERVER Instance.
2. Establish a connection with the Server after opening Second SQL SERVER Instance.
3. Connect First Instance of SQL Server with Second Instance of SQL Server with the following steps [5]:
   - Click Connect in Object Explorer
   - Server Name:- Second Instance Server Name(Example-AMIT-PC/MSSQLSERVER2)
   - Authentication:- SQL SERVER Authentication
   - Login:- Second Server Instance Login Name(Example:-sa)
   - Password:- Second Server Instance Password(Example:-gaurav)
   - Now click on Connect.

4. Create Linked Server in First Instance to Access the Databases of Second Instance
   - In object explorer of First Instance->Open Server Objects->Right Click On Linked Server->Select New Linked Server.
   - Following Window would appear when click on New Linked Server is done:
   - In the General properties following specifications to be written [6]:
   - Linked Server Name:-Any name(VAKUL)
   - Provider:- Select Microsoft OLEDB Provider for SQL SERVER
   - Product Name:- Any name (But Different From Linked Server Name) (Example:-vakul1)
   - Data Source:- Second Instance SERVER Name (Example-AMIT-PC\MSSQLSERVER2)
   - Provider String:- source=second instance SERVER name(Example-AMIT-PC\MSSQLSERVER2);database=any database of Second Instance(Example-amrit); userid=Login name of Second Instance(Example-sa);password=second instance Server Password(Example-gaurav)

i) Select the next property of Security.
ii) After selecting Security option from the left-> Now click on ADD button
iii) After clicked on ADD button you have to insert the
- Local login:- First instance login name(example-sa)
- Remote User:- Second Instance Login Name(Example-sa)
- Remote Password:- Second Instance Server Password (Example-gaurav)
- Impersonate:- Do not Check the Impersonate checkbox.

iv) Now select option Server Option from the left of the Current Window
v) After selecting Server Option two things to do:-
- RPC:- True
- RPC OUT:- True

5. Press ok to save all the details.
6. Linked Server has been created in First Instance of SQL SERVER. Do check in Server Objects of First SQL SERVER Instance->Open Linked Server there you find your Linked Server name(Example:- VAKUL)

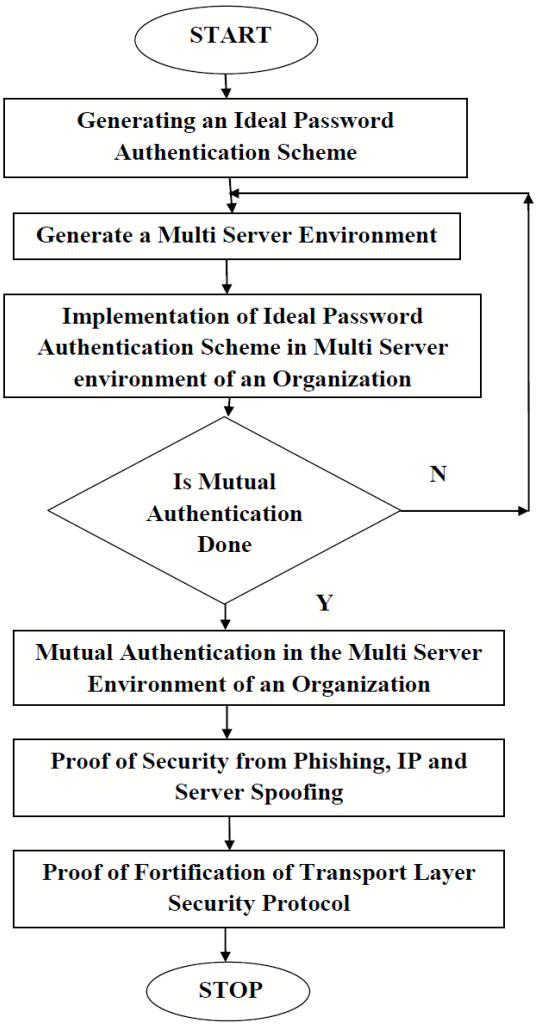
On the basis of above defined steps multi server environment in an organization is generated.

IV. Implementation of IPAS in the MSE of an Organization

Ideal Password Authentication Scheme comprises of Password and Fingerprint as two identity authentication parameters. Two identity authentication parameters would add one more tier of security to the transport layer security protocol. Multi Server Environment in an organization is generated by installing two instances of SQL Server in the same operating system [6]. Two instances will be connected to each other with the steps mentioned in Section III. After connection is successfully done then both instances could communicate with each other through Linked Servers [7]. Ideal Password Authentication Scheme would be implemented in the multi server environment of an organization with the following steps [8]:

- Login form is there which would ask user for initial input values which are username, image of the choice of user, password, fingerprint of index and middle finger. Below mentioned is the Login Form:
- Database would be created in SQL Server which would store initial input of the Username, Image (Selected by the User), Password and hashed finger print values of Index and Middle finger of the legitimate user.

i. When initial input would be sent to the database new generated hash algorithm would save the hashed finger print values to the created database. So the database would have username stored in the text format, image only jpeg format, password in hashed code and index and middle finger fingerprints in the hashed code format.
ii. Mutual Authentication form tab checks for the implementation part. When the process of mutual authentication has to be done then steps of Flow Diagram 2 would be followed.



Flow Diagram 1: Flow for generating Multi Server Environment

Following steps would be followed in mutual authentication form for validating results:

- STEP 1 Client would send User Name, Server would send selected image to the client.
- STEP 2 Client would check the image and put fingerprint of middle finger for Server side authentication. If the middle fingerprint matches with the stored value then server side authentication is proved.
- STEP 3 Server would ask for Password, if it is correct then server would ask for fingerprint of Index finger for Client side Authentication.
- STEP 4 when all these tiers of security are fulfilled and Client and Server prove their authenticity then Mutual Authentication is done.

In this way Ideal Password Authentication Scheme would be implemented in the Multi Server Environment of an Organization.

V. Mutual Authentication in MSE results in Fortification of Transport Layer Security Protocol

Mutual Authentication in the ideal password authentication scheme means client authenticates server and server authenticates client [9]. Steps mentioned in Section IV illustrate that authentication on Client and Server side both are required for enhancing security. It is a security requirement, which an ideal password authentication scheme can withstand. In this the user and the server can authenticate each other. This means not only the server verifies the legitimate user but the user also verifies the legitimate server [10]. This security requirement helps to withstand server spoofing (In this attacker pretends to be server to manipulate sensitive data of the legitimate users. The attacker creates a situation to masquerade legitimate user by falsifying data and getting an access as legitimate user. It generally happens because TCP/IP does not provide any mechanism by which authentication of source or destination message could be proved. Because of this data becomes vulnerable to server spoofing attack).

In Ideal Password Authentication Scheme two steps would be followed for mutual authentication:

- Client would put fingerprint of middle finger for Server side authentication. If the middle fingerprint matches with the stored value then server side authentication is proved.
- Server would ask for fingerprint of Index finger for Client side Authentication.

When intruder would be unable to hack or spoof then the result would be data integrity and security which enhances the record and handshake protocol of SSL. Enhancement of the protocols of SSL would result in fortification of transport layer security protocol.

VI. Security from Phishing, IP Spoofing and Server Spoofing

Security at the transport layer is completely possible if SSL (Secured Socket Layer) is enhanced with security. Certain big organizations like CISCO have identified that security of the data at Transport Layer with SSL could only be possible if following statements are implemented [11]:

1. Security policies and secure access through strong user authentication
2. Host identity verification
3. Host security posture validation
4. Secure desktop
5. Cache cleaning
6. Keystroke logger detection
7. Configuration consideration
8. User education and security awareness

But the complete security starts with proof of authentication, which is done by passwords in majority of the organizations. For identity authentication there are two more parameters smart cards and finger prints which could be used. As mentioned in Section II ideal password authentication scheme should be vulnerable to all attacks and could withstand the security requirements. So if authentication process could be in tiers then it would make the data transfer or communication process more secure.

So for this passwords would be combined with the finger prints for enhancing security on the public network. Intruders could not practice:

- Phishing (It is a fraudulent attempt, usually made through email, to steal your personal information. Often times phishing attempts appear to come from sites, services and companies with which you do not even have an account)- Best way to secure from phishing is to learn how to recognize a phish [12].

- IP Spoofing (This is basically lying about an IP address [13]. In this the source address given is normally incorrect. So when the source address is not true then it lets an attacker assume a new identity because the source address is not the same as the attacker's address, so any replies generated by the destination would be sent to the attacker. And if the attackers adhere to the protocol requirements then the connection would be very well maintained. IP Spoofing exploits trust relationships between routers) – Best way to save from IP Spoofing is make use of Multi Server Environment, as intruder could apply only one attack at a time for one server with a specific IP address so multi server would save the communication process to be hacked [14].

- Server Spoofing (In this attacker pretends to be server to manipulate sensitive data of the legitimate users. The attacker creates a situation to masquerade legitimate user by falsifying data and getting an access as legitimate user. It generally happens because TCP/IP does not provide any mechanism by which authentication of source or destination message could be proved. Because of this data becomes vulnerable to server spoofing attack) – Best way to save from Server Spoofing is make use of Multi Server Environment, as intruder could apply only one attack at a time for one server so multi server would save the communication process or transaction to be hacked [15].

Overall enhancement of SSL and knowledge how to recognize Phishing, IP Spoofing and Server Spoofing would increase the awareness of the user. Multi Server Environment implemented with the ideal password authentication scheme would result in fortification of transport layer security protocol.

VII. Conclusion with Fortification of Transport Layer Security Protocol

Implementation of ideal password authentication scheme in the multi server environment of an organization would help to with stand the security requirement of mutual authentication. When all the requirements of security are fulfilled then data becomes secure and results in integrity. It would enhance two protocols of SSL record and handshake which would help in strengthening SSL at the transport layer. When SSL is strengthened at the transport layer with the implementation of ideal password authentication scheme in the multi server environment of an organization then it results in the fortification of transport layer security protocol. The major security requirements which this ideal password authentication scheme would fulfill are [16]:

i. Confidentiality
ii. Integrity
iii. Authentication
iv. Non-Repudiation
v. Availability
vi. Anonymity
vii. Traffic Analysis

This ideal password authentication scheme with two parameters executed in the multi server environment of an organization would overall result in the fortification of the transport layer security protocol. So generating multi server environment of an organization for implementation of an ideal password authentication scheme would result in fortification of transport layer security protocol.

References

[1] Public Network "Secured Shell Protocol and Public Key Infrastructure",http://www.ietf.org/rfc/rfc4716.txt

[2] Kuljeet Kaur. Article: Fortification of Transport Layer Security Protocol. IJCA Special Issue on Network Security and Cryptography NSC(2):11-14, December 2011. Published by Foundation of Computer Science, NY, USA. (http://www.ijcaonline.org/specialissues/nsc/number2/4328- spe020t)

[3] Kuljeet Kaur and G Geetha. Article: Fortification of Transport Layer Security Protocol by using Password and Fingerprint as Identity Authentication Parameters. International Journal of Computer Applications 42(6):36-42, March 2012. Published by FCS,NY,USA. (http://www.ijcaonline.org/archives/volume42/number6/5700-7751)

[4] "SSL Essentials: Technology, Applications, Advantages, Disadvantages", http://apps1.eere.energy.gov/buildings /publications/pdfs/ssl/dowling_ssl_essentials_07-16-07. pdf

[5] Kuljeet Kaur and G Geetha. Article: Fortification of Transport Layer Security Protocol with Hashed Fingerprint Identity Parameter. International Journal of Computer Science Issues,Vol.9, Issue.2, No.2, PP.188-193,March 2012. (http://www.ijcsi.org/papers/IJCSI-9-2-2-188-193.pdf)

[6] "Single to Multi Server Environement", www.msexchange.org/...server.../designing-multi-server-environmen...

[7] "Creating Multi Server Environement", msdn.microsoft.com/en-us/library/ms191305.aspx

[8] Kuljeet Kaur and G Geetha. Article: Fortification of Transport Layer Security Protocol by using Password and Fingerprint as Identity Authentication Parameters. International Journal of Computer Applications 42(6):36-42, March 2012. Published by FCS,NY,USA. (http://www.ijcaonline.org/archives/volume42/number6/5700-7751)

[9] "Mutual Authentication", technet.microsoft.com/en-us/library/cc961730.aspx

[10] "Mutual Authentication," en.wikipedia.org/wiki/Mutual_authentication

[11] "SSL VPN Security," http://www.cisco.com/web/about/security/intelligence/ 05_08_SSL-VPN-Security.html

[12] "Phishing", *searchsecurity.techtarget.com/definition/**phishing***

[13] "IP Spoofing,"www.sans.org/reading.../introduction-ip-spoofing_959, United States, SANS

[14] Christoph Hofer, Rafael Wampfler,"IP Spoofing," rvs.unibe.ch/teaching /cn%20applets/IP_Spoofing/IP%20Spoofing.pdf

[15] Larry Seltzer ,"Spoofing Server-Server Communication: How You Can Prevent It," www.verisign.com/ssl/ssl.../ssl.../whitepaper-ev-prevent-spoofing.pdf ,2009

[16] Kuljeet Kaur and G Geetha. Article: Fortification of Transport Layer Security Protocol by using Password and Fingerprint as Identity Authentication Parameters. International Journal of Computer Applications 42(6):36-42, March 2012. Published by FCS,NY,USA. (http://www.ijcaonline.org/archives/volume42/number6/5700-7751)