Implementing RNA-FINNT in Ideal Password Authentication Scheme results in Fortification of Transport Layer Security Protocol

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

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

***Abstract*—** Mutual Authentication in the multi server environment of an organization, done at the transport layer, becomes complex when communication is done over the public link. Secure Shell protocol is the de facto standard and is deployed over the public network, for determining identity of client and server through Password-based key exchange schemes like AuthA and DH-EKE etc. This password based key exchange schemes and their multiple modes of operation are secure under the computational Diffie-Hellman intractability assumption but could not withstand security requirements and are vulnerable to attacks. So the paper focuses on additional tier of security for transport layer security protocol by using Fingerprint for mutual authentication in the multi server environment of an organization along with the Password. With the help of two identity parameters password and fingerprint, an ideal password authentication scheme would be generated. In this paper RNA-FINNT a new fingerprint hash algorithm would be implemented in the ideal password authentication scheme for generating a proof of fortification of transport layer security protocol. This could withstand security requirements and is not vulnerable to attacks. Paper generates a proof that if mutual authentication in the multi server environment of an organization is done with ideal password authentication scheme than intruders could not practice Phishing, IP or Server Spoofing etc and it would result in fortification of transport layer security protocol.

Keywords—Mutual Authentication, Password Authentication, Diffie-Hellman Key Exchange, Secured Shell Protocol, Secured Socket Lock.

I. INTRODUCTION

Computer Network allows people and machines to communicate with each other using various services like distributed and networked. Distributed applications of network provide services to users on other machines or to other machines. These are the programs which run on interconnected computers. Examples are Web Server, Remote Login Server and Email Exchanger etc. Networked infrastructure supports transport of data between computers where distributed applications reside. It is the collection of systems which are required for the interconnection of computers which run the distributed applications. Examples are Distance (interconnection of remote systems which are too far apart for a direct cable connection), Meshing (interconnection of systems when they are close to each other) etc [1].

Whenever distributed applications run and the network connection used is wireless, it is called Public Network. This link has unguided media of connection. So communication with this public link needs strong security at the transport layer where actual communication process takes place. Majority organizations deploy Secured Shell Protocol (in this the client is asked to log into another computer at some remote location but with some password authentication, then only the files could move from one location to another [2]. In this case association between client name and password is maintained by remote machine) for security.

Whenever there is communication, proving identity over the public link becomes complex. When resources are to be accessed from remote systems (networked infrastructure) then generally password is being used for identity authentication at the Public Network. But this paper assimilates one more tier of security to transport layer security protocol over the public link, with the use of fingerprint as identity authentication along with password. It would be an Ideal Password Authentication Scheme (IPAS) which would be used at the public network to establish a session.

Login process of the session would do mutual authentication (Client would authenticate Server and Server would authenticate Client as legitimate). Mutual Authentication of Client and Server would be done in the Multi Server Environment (comprises of two or more Servers) of an organization. And a new fingerprint hash algorithm RNA-FINNT is implemented in the IPAS for mutual authentication in the multi server environment of an organization in this paper. Thus it would result in fortification of transport layer security protocol.

Proc. of the International Conference on Advances in Information Technology – AIT 2012
Edited by Dr. R. K. Singh.

ISBN: 978-981-07-2683-6

The structure of the remainder of the paper is as follows. In Section II proposed methodology is mentioned, in Section III elucidation of public network for security requirement is done, in Section IV deployment of secured shell protocol is done with password as identity authentication parameter, in Section V assimilation of fingerprint with password in the login process of session is done, and it adds to one more tier of security, in Section VI mutual authentication is done in the multi server environment of an organization, in Section VII an ideal password authentication scheme is generated, in Section VIII implementation of new fingerprint hash algorithm RNA-FINNT is done, Section IX generates a proof of fortification of Transport Layer Security Protocol and Section X specifies the references.

II. PROPOSED METHODOLOGY

This paper focuses on adding one more tier of security in the login process of the session. This additional tier would comprise of two identity authentication parameters Password and Fingerprint. The following steps are proposed in the paper for generating a proof of fortification of transport layer security protocol with implementation of RNA-FINNT in the Ideal Password Authentication Scheme:

1. Elucidation of public network for security requirement.
2. Deployment of secured shell protocol with password as identity authentication parameter.
3. Assimilation of fingerprint with password in the login process of session and it adds to one more tier of security.
4. Mutual Authentication is done in the multi server environment of an organization.
5. Generation of an ideal password authentication scheme.
6. Implementation of new fingerprint hash algorithm RNA-FINNT.
7. Generating a proof of fortification of Transport Layer Security Protocol.

Above mentioned steps would show implementation of RNA-FINNT in IPAS for fortification if transport layer security protocol (*Shown in the Flow Diagram 1*).

III. ELUCIDATION OF PUBLIC NETWORK FOR SECURITY REQUIREMENT

Unguided media used for communication is Public Network. A network is made up of components; it's divided into functions which are called Layers. Interface is there for interaction and one component interacts with adjacent two components only. When public network is used, proving identity becomes complex for logging into the session. One of the important layers which deal with security of the communication is the Transport Layer [3]. This layer makes network services available to programs. It adds functions to the network services like reliability, congestion control and multiplexing etc. User datagram protocol (unreliable) and transmission control protocol (reliable) are the two main transport protocols which offer the stream services. Any communication which has to start may use UDP or TCP depending upon the requirement of the legitimate user [3]. Complete security is required at the transport layer because it has to guarantee and make sure that communication is safely done.

Generally organizations use password as identity authentication parameter, in the login process of the session, to prove identity over the public network. But only password does not make the communication process secure. So there is need of one more tier of security in the login process of session. This paper has suggested assimilating fingerprint with password in the login process of session. This would add one more tier of security at the transport layer where actual communication takes place.

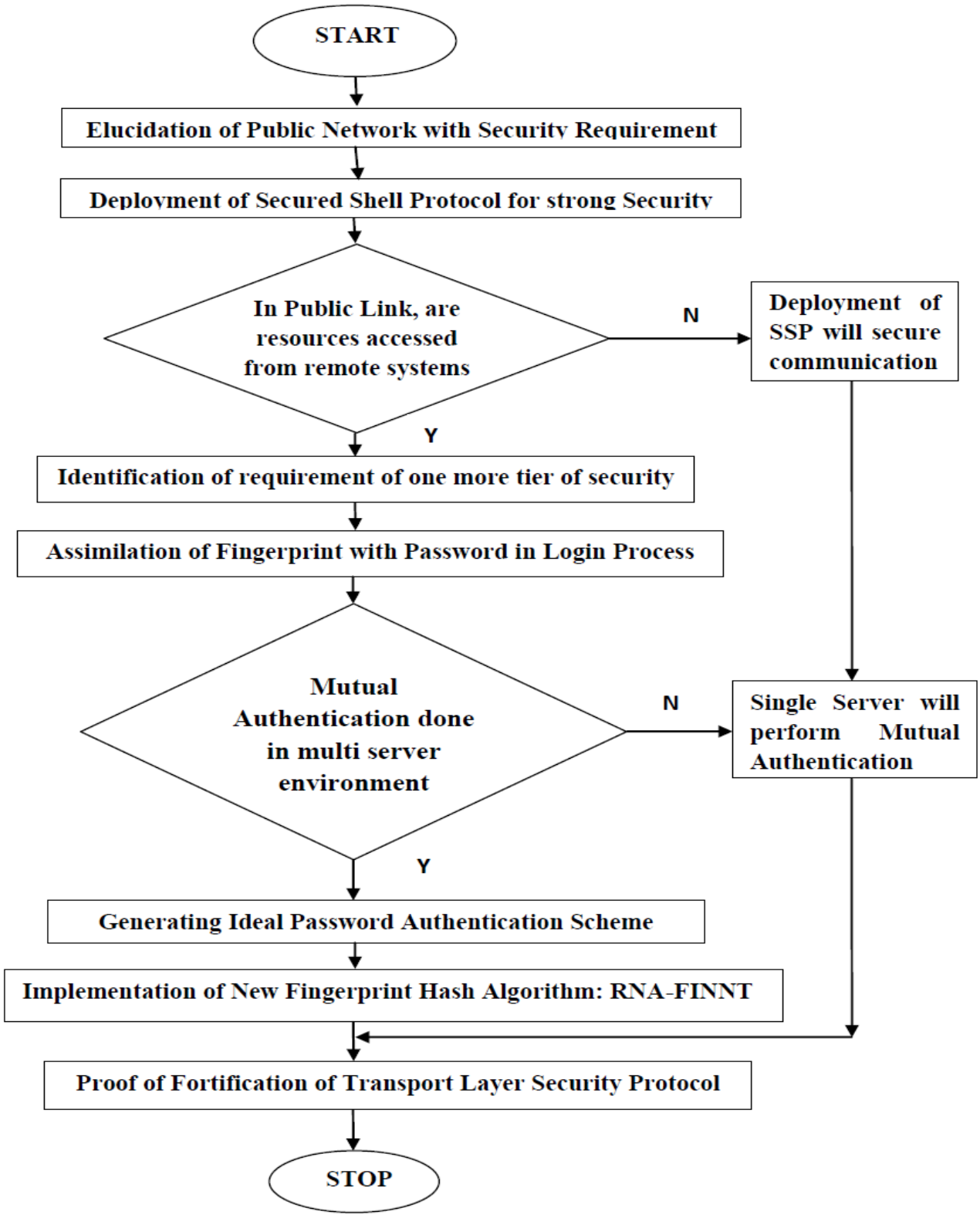
IV. DEPLOYMENT OF SECURED SHELL PROTOCOL WITH PASSWORD AS IDENTITY AUTHENTICATION PARAMETER

Secured Shell Protocol is the de facto standard and is deployed by majority of the organizations over the public network. It is used to determine identity of client and server through password only. Password based key exchange schemes like AuthA and DH-EKE etc is used for identity authentication. These schemes are secure under the computational Diffie-Hellman intractability assumption [4]. But this scheme could not withstand all the security requirements like forward secrecy and mutual authentication etc. This scheme is also vulnerable to attacks like dictionary attack, denial of service attack, man in the middle attack, IP spoofing, phishing and server spoofing etc.

So the paper focuses on:

1. Additional tier of security for transport layer security protocol by using Fingerprint for mutual authentication.
2. Mutual Authentication would be done in the multi server environment of an organization.
3. It would be implemented in the login process of the session along with the Password.
4. Two identity parameters password and fingerprint, would be used for mutual authentication, in the multi server environment of an organization.

With the help of secured shell protocol only password was being used. So this paper suggests fingerprint to be used as identity parameter along with password. Both identity parameters would be implemented in the login process of the session and would provide more security.



Flow Diagram 1: Proposed Methodology for generating a proof of fortification of transport layer security protocol with implementation of RNA-FINNT in the Ideal Password Authentication Scheme

V. ASSIMILATION OF FINGERPRINT WITH PASSWORD FOR ADDING ONE MORE TIER OF SECURITY IN THE LOGIN PROCESS OF SESSION

Fingerprint is of three types: arches (it may have plain ridge or tented ridge which has angle in the arch), loops (it contains one core and one delta) and whorls (in it one ridge contains two deltas) [5].

Fingerprint is used for authentication and following are the technologies used for fingerprint authentication [5]:

1. Correlation (image of fingerprint is used as template)
2. Texture Descriptors (texture is used as template)
3. Minutiae Descriptors (set of unique points over the fingerprint)

Everyone falls into one of the above said categories which are arches, loops and whorls. Within these three categories there are thirty different minutiae points over the fingerprint. This makes fingerprint unique because no one has the same number of minutiae points on the same place. So with assimilation of fingerprint and password an ideal password authentication scheme would be generated and security would be enhanced at the transport layer.

So in this paper Minutiae Descriptors technology is used to extract fingerprint value. New fingerprint hash algorithm RNA-FINNT would be implemented in IPAS which would result in fortification of transport layer security protocol.

VI. MUTUAL AUTHENTICATION IS DONE IN THE MULTI SERVER ENVIRONMENT OF AN ORGANIZATION

In mutual authentication the user and the server authenticates each other. This means not only the server verifies the legitimate user but the user also verifies the legitimate server.
Mutual Authentication is the security requirement which helps to withstand:

- Phishing (an attack that tricks users out of confidential information. For phishing create authentic looking fraudulent web page, spam a large number of users towards that fraudulent web page, provide requested authentication and make use of provided information) [6].
- IP spoofing (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, 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.) [7].
- Server spoofing (In this attacker pretends to be server to manipulate sensitive data of the legitimate users. It generally happens because TCP/IP does not provide any mechanism by which authentication of source or destination message could be proved.) [8].

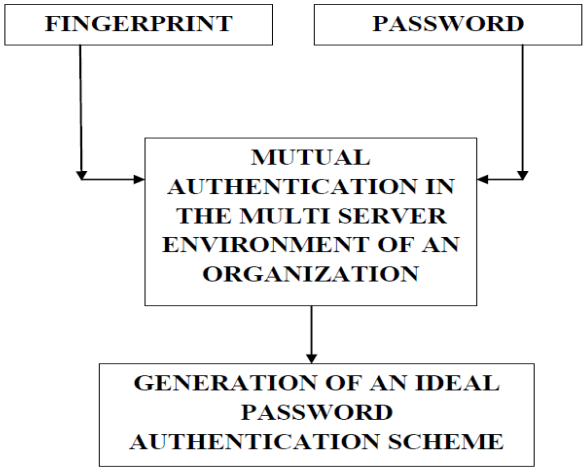
Overall mutual authentication enhances the security of the transport layer security protocol.
Mutual authentication would be done in the login phase to create a session. Following steps would be followed for mutual authentication:

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 proves their authenticity then mutual Authentication is done.

The above mentioned steps would be used for mutual authentication in the multi server environment of an organization.

VII. GENERATION OF AN IDEAL PASSWORD AUTHENTICATION SCHEME

Fingerprint and password are used in Section VI for mutual authentication in the multi server environment of an organization. Because according to one of the Survey of Ideal Password Authentication Scheme which results in Fortification of transport layer, Fingerprint is the choice of the user after Passwords as it is more secure and usable, and even the user is ready to bear extra cost for any prototype which would result in assimilation of Fingerprint and Password [9]. Following diagram states the generation of an ideal password authentication scheme:



Flow Diagram 3: Generating an Ideal Password Authentication Scheme

The mentioned diagram has shown how an IPAS would be generated. With two identity parameters mutual authentication would be done in the multi server environment of an organization. This IPAS will enhance security and would result in the fortification of transport layer security protocol.

VIII. IMPLEMENTATION OF NEW FINGERPRINT HASH ALGORITHM: RNA-FINNT

RNA-FINNT is the reduced number of angles fingerprint hash algorithm [11]. Implementation of this algorithm would be done by creating a website using ASP.Net and SQL Server.

Following steps would be followed:

1. A form would be created in ASP.Net for taking initial input values which are username, image of the choice of user, password, fingerprint of index and middle finger.
2. Database would be created in SQL Server which would store initial input taken through form of ASP.Net.
3. Fingerprint value which is hashed code would be stored through RNA-FINNT.
4. Now when the process of mutual authentication has to be done then steps of Section VI would be followed.
5. It will result in the fortification of the Transport Layer Security Protocol.

This is how RNA-FINNT would be implemented in IPAS for fortifying transport layer security protocol.

IX. GENERATING PROOF OF FORTIFICATION OF TRANSPORT LAYER SECURITY PROTOCOL

IPAS would not be vulnerable to attacks and would be able to withstand the security requirements. When the security requirements are fulfilled then transmission or communication results in data integrity and security. With this, protocols at the transport layer gets strengthened which would further result in the fortification of transport layer.
IPAS has the following benefits with implementation of RNA-FINNT:

1. Two parameters password and fingerprint are used to enhance security.
2. IP or Server spoofing is not possible with the implementation of this scheme.
3. In hash algorithm global points core or delta are not considered so it results in the reduced number of angles and there is no dependency.
4. All the squares of grid run in parallel so execution of the algorithm is much faster than the existing hash algorithms.

With the implementation of ideal password-authentication scheme in multi-server environment of any Organization, the proof is generated that transport layer is fortified. The major security requirements which this ideal password authentication scheme fulfills are [10]:

1. Confidentiality (Protection from disclosure to unauthorized persons)
2. Integrity (Assurance that information has not been modified unauthorizedly)
3. Authentication (Assurance of identity of originator of information)
4. Non-Repudiation (Originator cannot deny sending message)
5. Availability (Not able to use system or communicate when desired)
6. Traffic Analysis (Sender and Receiver should not know their identity)

So this IPAS in which RNA-FINNT is implemented results in the fortification of transport layer security protocol.

X. REFERENCES

[1] Jean-Yves Le Boudec, Andrzej Duda,Laurent Toutain and Patrick Thiran," Introduction to Computer Networking", ICA, EPFL.

[2] "SSL VPN Security," http://www.cisco.com/web/about/ security/intelligence/ 05_08_ SSL-VPN-Security.html

[3] "Transport Layer," www.cs.st-andrews.ac.uk/~tristan/teaching/cs78.../transport-layer.pdf

[4] 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)

[5] Sahil Goyal and Mayank Goyal," Generation of hash functions from fingerprint scans," Department of Electronics and Communications Engineering, Indian Institute of Technology Guwahati, October 2011

[6] "Technical Trends in Phishing Attacks," www.us-cert.gov/reading_room/phishing_ trends0511.pdf

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

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

[9] Kuljeet Kaur and Dr. G.Geetha," Survey for Generating an Ideal Password Authentication Scheme Which Results In Fortification of Transport Layer Security Protocol," International Journal of Computer Science and Information Technologies, Vol.3, Issue.2, PP.3608–3614, March-April 2012 (http://www.ijcsit.com/ijcsit-v3issue2.php)

[10] 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)

[11] 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)