IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Protection against man-in-the-middle attack in Banking Transaction using Diffie Hellman key Exchange Algorithm

Mr. Ajeet Kumar Bhartee[1], Neha Pal[2], Abhishek Verma[3]

Asst. Prof, Department of CSE, Galgotia College of Engineering &Technology, Greater Noida[1]

Department of Information Technology, Galgotia College of Engineering &Technology, Greater Noida [2]

Department of Computer Science, United College of Engineering & Research, Greater Noida [3]

Abstract: With the development of e-commerce and cloud Computing, SSL protocol is more and more widely used in all kinds of network services. SSL protocol by providing end to end authentication, message encryption, message Integrity check and other security mechanisms protects the security of the communication process. In recent years, due to the development of cloud computing, the connection security between the client and the cloud is also an extremely important issue.SSL have three protocols under it: Handshake Protocol; Record Protocol; and Alert Protocol. Handshake protocol is used to establish the secure connection between the client and the server using the cipher suites and other parameters that both have agreed upon. Record Protocol is used to encrypt the data that is to be sent through the network using the key that have been established during the handshake protocol. Alert protocol is used to send the custom messages to other whenever they detect any intrusion in the system. The goal of our proposed system is to create secure channels over insecure networks using Diffie Hellman key exchange algorithm.

Keywords: MITM, SSL, Cryptography, Security, Diffie-Hellmen-Key-Exchange Algorithm, Authorization, Attack.

I. INTRODUCTION

SSL have three protocols under it: Handshake Protocol; Record Protocol; and Alert Protocol. Handshake protocol is used to establish the secure connection between the client and the server using the cipher suites and other parameters that both have agreed upon. Record Protocol is used to encrypt the data that is to be sent through the network using the key that have been established during the handshake protocol. Alert protocol is used to send the custom messages to other whenever they detect any intrusion in the system. As I need to show the defects in the SSL methods, handshake protocol (see Figure 1) need to be discussed first. It is as follows:
Step 1: Client Sends a **ClientHello** message to the server he wishes to contact. This message contains the Version No of the SSL which client can support with a 32-byte random no. this message also contains the Cipher Suites and the ompression Method that the client can support.

Step 2: Now the Server sends a **ServerHello** message to the client. This message is the complement to the Client Hello message. This message contains the version of SSL both the party will support, 32-byte random no., Session ID and the cipher suite and the compression method that it will support.

Step 3: Server then sends the **ServerKeyExchange** message to the client. This message contains the public key information itself, for e.g.: the Public Key in case of RSA. Then to authenticate the client, server requests for the client’s certificate information, if it has one.

Step 4: After all the information have been passed to the client, server sends a **ServerHelloDone** indicating the client that server’s phase of initial negotiation have been done and now its clients turn.

Step 5: Now the client will send its key information to the server with **ClientKeyExchange** message encrypted with the server public key so that the legitimate server only can access client’s information.

Step 6: Now as both the client and the server have sent their key information and other parameters, Client sends a **ChangeCipherSpec** message to the server to notify all the parameters of the secured connection and activate the same.

Step 7: Then the client sends the **Finished** message to the server to let it check the newly activated options.

DOI10.17148/IJARCCE.2017.6458

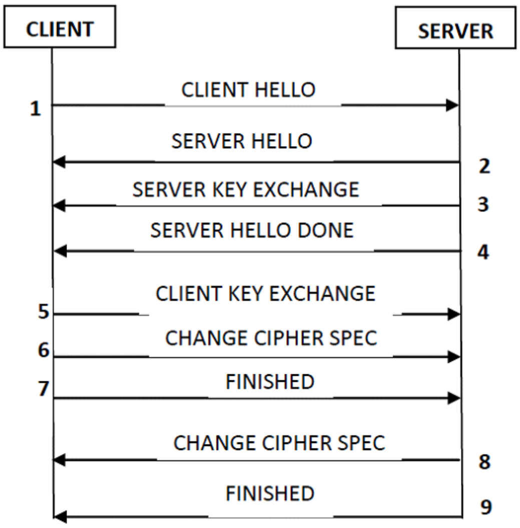


Fig. 1. SSL Handshake

Step 8: Server sends the same message "**ChangeCipherSpec** " to client side to notify all the options in the secured connections and then send " **Finished**" message to the client to verify all options.

Next to the Handshake Protocol is the Record Layer Protocol. This layer encapsulates all the data into a frame format of size 5bytes preceding other protocol messages. This protocol provides a single frame format for Alert, ChangeCipherSpec, Handshake, and Application Data.

A. PHISHING

Your Phishing is the act of stealing user information by pretending to be a trustworthy entity. In the simplest avatar of Phishing attack, a Phisher sets up a bogus website, which closely resembles the targeted original website. It then sends out a bulk of spam e-mails, purporting to be from a legitimate organization, which convinces the user to visit the counterfeit website. Of the many users who get the e-mails, a few fall prey to the attack and give out their credentials. It is well known that Phishers rely on almost any kind of social engineering methods including email, telephone call, people to people communication, SMS, IM. They also leverage other technical subterfuge to lure the victims to the spoofed webpage.
Apart from this mechanism of Phishing attacks, other technical subterfuge schemes plant crimeware onto user's PC which intercepts any information which can be cashed upon by the Phisher such as usernames, passwords, SSN's etc. According the latest reports from Anti-Phishing Working Group (APWG) about 35 percent of the computers were infected with malware.
Yet in another dangerous scenario a Phisher can run its own network node e.g. WiFi access point which allows travellers and even other user to free Internet connectivity. Once user connects to such network node for access to Internet, it is obvious that user's information can be compromised easily.

B. MAN IN THE MIDDLE ATTACK

Man-In-The-Middle attack is the major attack on SSL. MITM attack makes the users difficult to understand that whether they are connected to original secured connection or not. Since the certificate that is being passed during the connection setup is insecure, attacker can easily modify the information in the certificate and leave the approval of the certificate to the user. Since many users are not well educated about the where abouts of the forged certificates and their corresponding attacks, they accept the certificates making way for the attackers to implement the attack.

II. PROPOSED SYSTEM

The ultimate goal of our proposed system is to create secure channels over insecure networks. The TLS (Transport Layer Security, or SSL (Secure Socket Layers) in its more modern implementation, is protocols designed to provide security for network communication by means of encryption we use Diffie Hellman key exchange algorithm. This protocol is most commonly associated with other protocols to provide a secure implementation of the service that protocol provides that is HTTPS with secure socket layer.

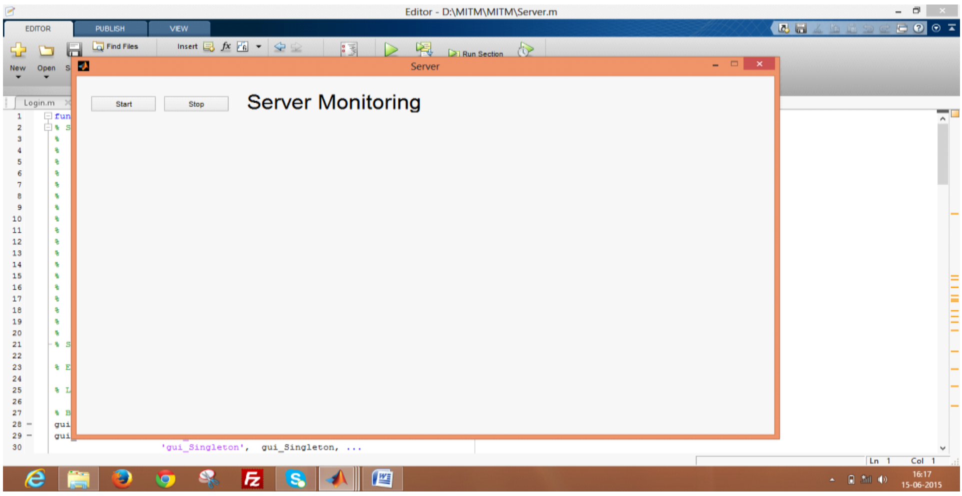
We will use the browser plugin for Man-in-the middle having the same url as the original website.

DOI10.17148/IJARCCE.2017.6458

III.SIMULATION

For design our system we used MATLAB for development. MATLAB is best suited for our proposed method.

A. Starting of the Server



```
'gui_Singleton',  gui_Singleton, ...
```

Fig. 2. Start the Server

B. Server Monitoring after Start

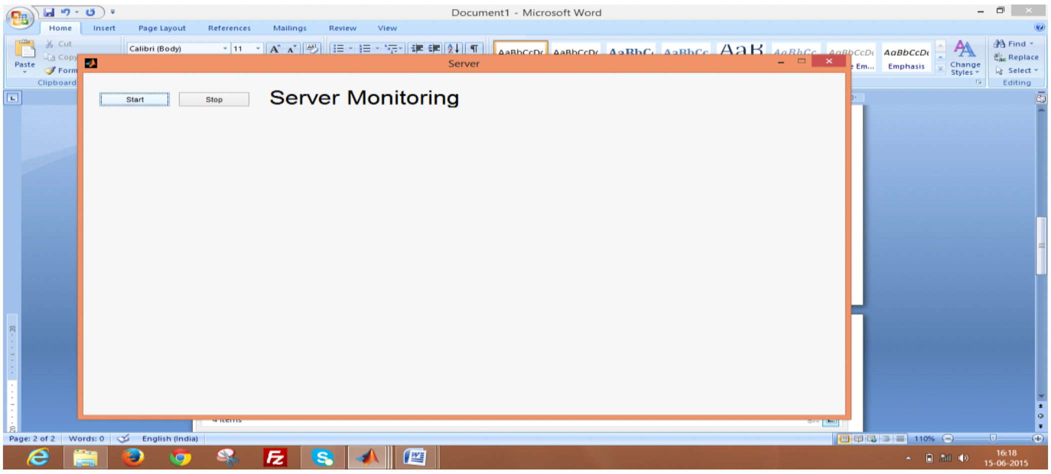


Fig. 3. Server Monitoring after Start

C. Authorization by the Users

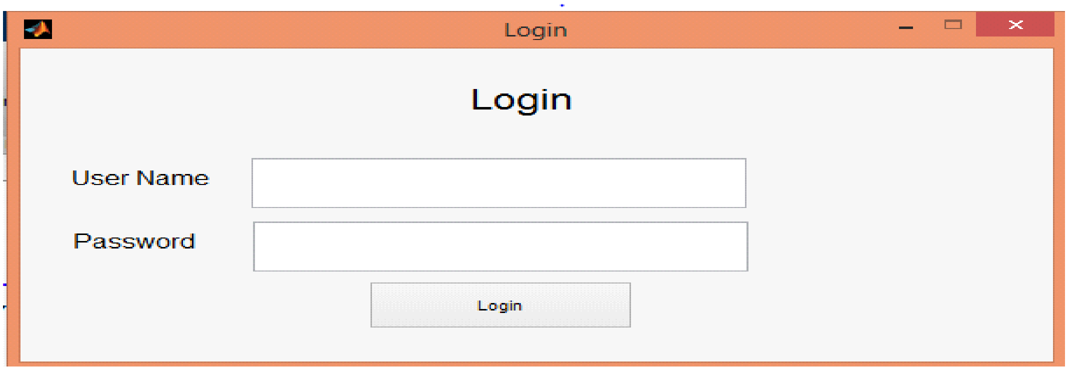


Fig. 4. Authorization by the user

DOI10.17148/IJARCCE.2017.6458

D. Valid User Account Assessment

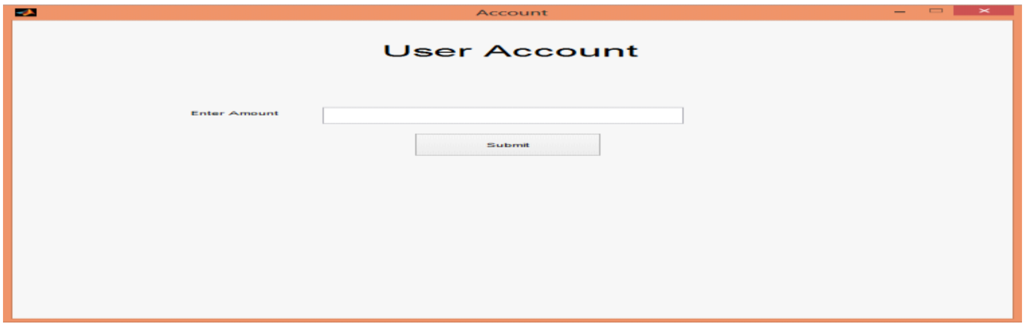
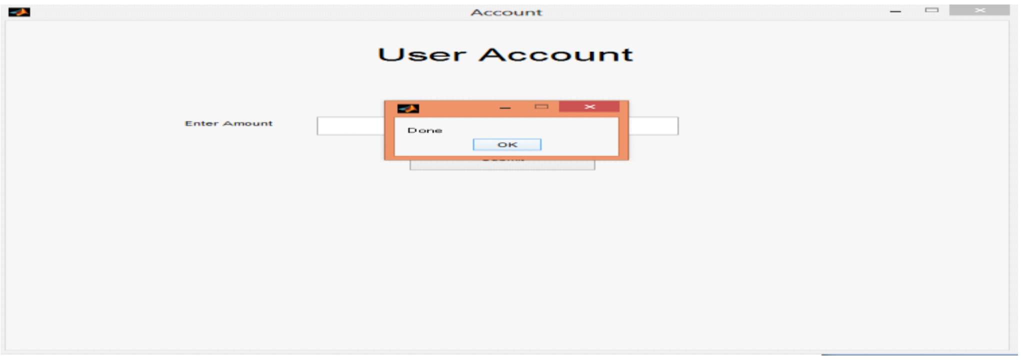


Fig. 5. Valid User Account Assessment

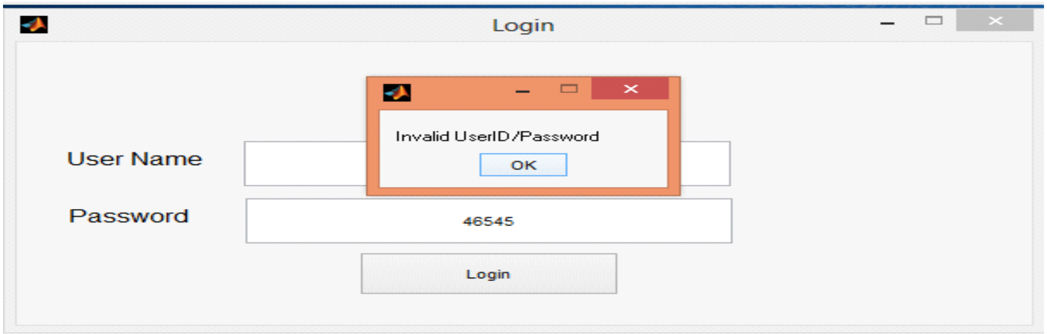
E. Transaction Done Message



Done

Fig. 6. Transaction done Message

F. Authorization By Server



Invalid UserID/Password

User Name

Password 46545

Fig. 7. Authorization By Server

G. Proxy Server of Hacker

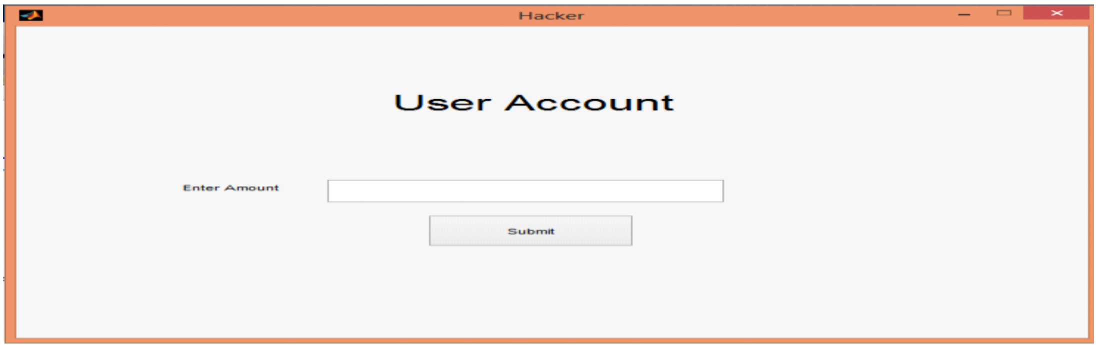
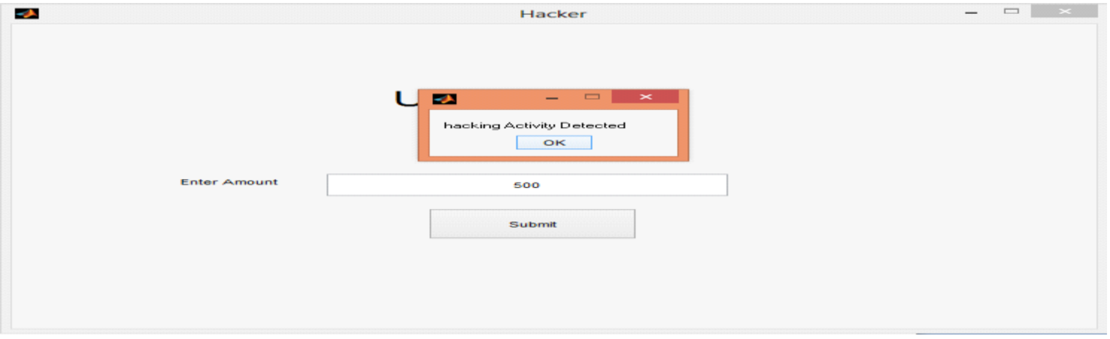


Fig. 8. Proxy Server of Hacker

DOI10.17148/IJARCCE.2017.6458

H. Hacking Detected



hacking Activity Detected

500

Fig. 9. Hacking Detected

IV. CONCLUSION

Experiments show that three protocol SSL,HTTP and hybridization of ssl and https with key exchange algorithm of attack on the session are feasible. In normal, connection speed of HTTPS services is 2-100 times slower than normal HTTP connection, users will not be aware of attacks even if the delay caused by the change of link. Because users usually do not care about the alert in browser, when attacking in the first and third method, the majority of users will tend to accept a warning certificate even if the alert dialog; when attacking in second method, the user will not be aware because the little difference between the normal and attacking pages. In our experiment, using SSLHTTPS effectively to avoid the attack. Configuring a static ARP table can avoid attack in first and second method howprevents man-in-the-middle attacks on HTTPS session more effective is the next focus of our study. Designing a Key exchange algorithm with 100% Accuracy is not at all possible. While proposing the Algorithm, We considered Man-in-the-middle Attack & Replay Attacks. However we can‘t say that Man-in-the-middle Attack cannot possible completely .because the base selected by the middle man can be same as ‘e‘unfortunately. The Algorithm uses simple method (mathematical concepts) making implementation easier as well as avoidance from the common Attacks.

REFERENCES

[1] Yogesh Joshi, Debabrata Das and Subir Saha "**Mitigating Man in the Middle Attack over Secure Sockets Layer**" 978-1-4244-4793-0 09© 2009 IEEE.

[2] ItaloDacosta, MustaqueAhamad, and Patrick Traynor,” Trust No One Else: Detecting MITM Attacks Against SSL/TLSWithout Third-Parties”, US National Science Foundation (CAREER CNS-0952959)

[3] Martin Georgiev,SubodhIyengar,Suman Jana, The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software, CCS’12, October 16–18, 2012, Raleigh, North Carolina, USA

[4] Pushpendra Kumar Pateriya, Srijith S. Kumar, Analysis on Man in the Middle Attack on SSL, International Journal of Computer Applications (0975 – 8887) Volume 45No.23, May 2012

[5] Kefei Cheng, TingqiangJia, MengGao, Research and Implementation of Three HTTPS Attacks, JOURNAL OF NETWORKS, VOL. 6, NO. 5, MAY 2011

[6] Maryam Ahmed, BaharanSanjabi, DifoAldiaz, Diffie-Hellman and Its Application in Security Protocols, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012

[7] SakthiNathiarasan A , Yuvaraj K, Secure Key Exchange Algorithm - Mathematical Approach, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013

[8] Certificate Patrol (2010), http://patrol.psyced.org/

[9] Soghoian , C ., Stamm, S.: Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL. In: Proceedings of Financial Cryptography and Data Security (2011)

[10] Evans, C., Palmer, C.: Certificate Pinning Extension for HSTS (2011), http://www.ietf.org/mailarchive/web/websec/current/pdfnSTRd9kYcY.pdf

[11] Parno, B., Kuo, C., Perrig, A.: Phoolproof Phishing Prevention. In: Proceedings of Financial Cryptography and Data Security (2006)

[12] Alicherry , M., Keromytis, A.D.: DoubleCheck: Multi-path Verification Against Man-in-the- Middle Attacks . In : Proceedings of the IEEE Symposium on Computers and Communications (2009)

DOI10.17148/IJARCCE.2017.6458