Security Analysis on Remote Authentication against Man-in-the-Middle Attack on Secure Socket Layer

1O.Rama Devi, 2S Parvathi Vallabhaneni, 3Dr. Mohammed Ali Hussain and 4Tulisetti Kranthi Kumar

1Professor, Department of CSE, Lakireddy Bali Reddy College of Engineering, Mylavaram.
2Asst. Professor, Dept of CSE, Prasad V Potluri Siddhartha Institute of Technology
3Professor, Dept. of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., Andhra Pradesh, India.
4Director, Standard Solutions, Vijayawada, India

Email: odugu.rama@gmail.com

Abstract. One of the biggest SSL assaults is Man-In-The-Middle. ARP poisoning and phishing are some of the principal attacks against SSL. Phishing offends the user by using false certificates or fake websites to steal certificate information. As for ARP poisoning, the attacker may act as a representative on the client/server communication channel. The MITM attack makes it difficult for users to know if they have linked to an original secured link or not. Since the certificate issued during the connection setup is not secure, an intruder can alter the details in the certificate and grant user authorization. Because a number of clients have not been well trained above the whereabouts and their attacks, they can recognize the certificates that allow attackers to perform the attack. They can also acknowledge the attack. Two techniques have been suggested in order to cope with such assaults: first for ARP poisoning and secondly for phishing.

Keywords: SSL, ARP, Security, Phishing, TLS, Man-in-the-Middle attack.

1. Introduction

As the network grows immensely and the information passed on to the organization is becoming critical, we have to provide customers, as the company offers some confidentiality and authentication, which allow all internet users to guarantee that the right person is contacted. In the year 1994, Netscape created the solution, Secured Socket Layer (SSL) which offered this security level to the client and organization. Due to certain constraints within the system, the first version of SSL is not available [2]. SSLv2 became released in 1994, and then IETF standardized its SSL and its free SSLv3.0 protocol improved with a wide range of secured algorithms and written management of document data. They have renamed a future upgraded SSLv3.1 version to TLSv1.0[3].

SSL was created to provide privacy and safety in information, but there are still some restrictions on this protocol. The SSL implements initially the soft model of PKI: web-model [6-8]. The web-model is best suited for large-scale SSL application, but the most important part of this is a few different kinds of Trust Roots: CA, and User. In this case, users can also decide if they have to allow other certifications which do not appear to be in CA or not. Secondly, the attacks that the SSL primarily faces as a result of the attack by the MITM, mainly ARP Poisoning, which enables the attacker to hide the protected session and get the...
credentials needed.

Here article, addressing the system to improve SSL through the protocol for RADIUS (Remote Authentication Dial-In User Service) which offers customers that link and use the network services with centralized authentication, authorization and account management.

This article is split into three sections. In section 1, data about the SSL will be discussed. In section 2, we addressed the potential attacks on SSL and how much they are harmful. And we addressed the solution suggested in the third section.

2. Secure Socket Layer
The 3 underlying protocols that SSL having are handshake protocol, record protocol and alert protocol. The handshake protocol uses to create a safe connection among the user and the server by utilizing a cipher suite and alternative parameters, which have been configured for each. With the key setup via handshake protocol, record protocol encodes the data sent over the network. Whenever an disturbances within the system seen, the alarming message shall be used to pass custom mails to alternative systems. In order to identify the flaws of the SSL strategy, the acknowledgement protocol must be referenced first [1]. Figure 1 illustrates the implementation process for SSL handshaking.

1. The client sends a signal to the contact server ‘CLIENT HELLO’. This message includes SSL version no that is supported by consumers with a random 32-byte no. Together with the cipher suites and the consumer compression method, this message includes.
2. The server now sends a ‘SERVER HELLO’ to the client. This message includes the version no. of SSL, 32-byte random no, session ID and therefore the cipher suite and consequently the compression process it supports.
3. Again the server sends a message ‘SERVER KEY EXCHANGE’ to client. For example, the general public key for RSA only is included in this message. Then server requests the customer for the certificate information to demonstrate the customer whether they are one.
4. Once the client has received the information, the server then sends a ‘SERVER HELLO DONE’ to the client stating that the original negotiations on the server are complete.
5. The client can presently forward his/her main information to the server using a public-key server encrypted signal ‘CLIENT KEY EXCHANGE’ to enable the legitimate server solely will access client’s data.
6. The client sends the ‘CHANGE CIPHER SPEC’ to the server to receive all the encrypted link parameters and to trigger the same, as client and server both send their key information and alternative settings.
7. The client then sends the completed ‘FINISHED’ message to the server to track the recently approved choices.
8. The server sends ‘CHANGE CIPHER SPEC’ message to the client to recognize all the functionality within the encrypted connections so that the final message ‘FINISHED’ is sent to the client in order to check all the options.

Next to the handshaking protocol is record layer protocol. It covers the information in a 5 byte frame format and includes the Alert, ChangeCipherSpec, Handshake, and user data frame format [1].
3. A) ARP Poisoning

Stands for ‘Address Resolution Protocol’ are the protocol technique for determining MAC address of the particular node. A transmitted packet demanding the MAC address will be sent from the destination so it will be placed on the network. This mapping is stored in the ARP cache once you have received IP/MAC mapping of a network.

The attacker tries to capture the packets first and foremost, to find out the connected device gateway [4]. After he has identified the IP address of the victim and gateway, the victim receives an ARP response indicating that the MAC address of the gateway is now the MAC address of the attacker.

The attacker can hijack a session with this attack even though the aforementioned is secured by SSL/TLS as illustrated in figure 2. In this scenario, the victim associates the server via the attacker’s gateway. Attacker acquires all the packets via the network to show all the data.

B) Phishing Attack

The attack in which users are attempted to enter user credentials in fake internet websites is phishing [9,10]. These web sites look like the real websites and make users fool themselves to enter information. The attacker may, however trick the client/server session in more sophisticated manner.

![SSL Handshake Diagram](image-url)
Figure 2: ARP Poisoning

In order to provide the client with public key information, it is evident from the hand shaking SSL protocol that initial negotiations are not secure. It helps the hacker to intercept the message and change the certificate information. The attacker can change the public key information and the victim will receive it [11].

Figure 3: MITM attack

The connection is safe with the victims because the victim is safely linked to the server’s device. Such an attack warns a user of the forged certificate and grants the user the right to accept or non-accept the connection. Some associates ignore the alerts and proceed the link.
4. Solution Proposed

a) For ARP Poisoning

Here suggests a Linux shell script as the solution. Previously in [6] the author introduced an ARP poisoning solution in which the shell script was not capable of checking the ARP table without the manual entry of gateway address’s. The important things are here is that the gateway in a network is never changed and thus the allocated IP is not ever modified until the gateway shutdowns. Therefore the gateway IP/MAC combination would be the common. The following works for this script.

1. The script monitors the gateway IP address associated MAC address via the –n and arp-a path.
2. Redirect IP-MAC mapping from arp –a outputs on regular basis.
3. Test the same value of the MAC and IP address with awk for each two successive redirects.
4. The user is informed that the ARP cache is compromised if the same MAC scan is detected for several IPs.
5. The script must modify the original value of a ARP cache, as the user specifies the modification of the ARP table.

This script helps to overcome attacks of ARP poisoning by testing the system’s ARP cache periodically. The ARP cache has the optimum time to ensure that the ARP cache is not managed at small intervals and that critical packets are not leaked at long intervals.

4.1 RADIUS Protocol

We proposed a solution for avoiding MITM attacks using the Remote Authentication Dial-In User Service protocol which provides centrally authentication, authorization, and accounting management for network users. RADIUS was developed as an associate access database authentication and accounting protocol in 1991 by Robert R. Livingston Enterprises, Inc. and integrated into IETF (Web Technology Task Force) standards. It is widely used by ISPs and businesses in order to control access to network and internal networks, wireless networks, and email services by means of broad support of the RADIUS protocol. Such networks could include DSL, modems, VPNs, access points, network ports and internet servers.

A client/server interface can be used by RADIUS, using UDP as transportation. The gateways to which network access is handled typically contain a device component of the network access server which communicates with the RADIUS server. For 802.1X authentication, RADIUS is typically the backend for choice. Sometimes the RADIUS server is a background tool on UNIX and Microsoft Windows. Following are the steps to execute RADIUS protocol.
Figure 4: Radius Protocol

**Step1:** In this the client sends a connection request to the radius client which is connected by a network called PSTN. The exchange authentication information is sent to the client. Next the Access Request is forwarded to the radius server with the use of user Name, User password, IP address, Challenge-Handshake Authentication Protocol (CHAP) Password, NAS IP address etc.

**Step2:** This provides a feedback on the approval of requests, such as access-accept, access-reject and access-challenge.

In access-accept, the RADIUS server must confirm, once the user has authenticated that the client is allowed to use the requested network service.

In access-reject, connection to the requested network resources is refused by the user unconditionally. The explanations may be the absence of evidence or inactive user accounts.

Additional user information such as secondary user name, pin, token or ticket is provided in access-challenge. In more complicated authentication dialogs, the access-challenge is used to create a secure tunnel between the user device and the RADIUS server, which removes access credentials from the NAS.

**Step3:** The authentication information is exchanged to the customer in this phase. The above method is again carried out and the information can eventually be sent to the customer by sending access-accept or reject the client whether it is a failure or success.
5. Conclusion

The solution for ARP poisoning was provided. Here we introduced a design model as the radius protocol to avoid MITM attacks due to weak authentication problems. A brief overview has been given concerning the RADIUS protocol and its functioning to mitigate MITM attacks.

References

[1] Mohammad Arshad, Md. AliHussain, Volume 9, Issue 47, December 2016, Secure Framework to Mitigate Man-in-the-Middle Attack over SSL Protocol. Indian Journal of Science & Technology.

[2] Abdul, A.M. and Umar, S., 2017. Attacks of Denial of Service on networks layer of OSI model and maintaining of security. Indonesian Journal of Electrical Engineering and Computer Science, 5(1), pp.181-186

[3] Balakrishna A.S.V., Srinivasu N. (2018), 'Effective security in social data security in OSNs’, Advances in Intelligent Systems and Computing, 542, P.P. 445-452

[4] Kocharla L., Rao K.R., Kumar D.S. (2018), 'Secure data packet transmission over wireless sensor network using security architecture’, Journal of Advanced Research in Dynamical and Control Systems, 10 (0), P.P. 491-496.

[5] Jyothika Rani P., Navaneeth Kumar R., Ramesh Kumar M., Tenali R.K. (2019), ‘Security system solution for women’, International Journal of Innovative Technology and Exploring Engineering, 8(6), P.P. 348-350.

[6] Sai J.A., Kumar K.K. (2019), ‘Enabling public auditing for data integrity checking using ring signatures developed with aes in cyber security’, International Journal of Innovative Technology and Exploring Engineering, 8(6), P.P. 1536-1543.

[7] Maanas G., Raghava Rao K., Anjali L., Satyannarayana P. (2019), ‘An interactive GPS and RFID based receptacle security system’, International Journal of Engineering and Advanced Technology, 8(4), P.P. 922-928.

[8] Reddy L.R.S., Koushik T., Varaprasad B.B.V.S., Tenali R.K. (2019), ‘Intelligent home security system using one time password authentification’, International Journal of Innovative Technology and Exploring Engineering, 8(6), P.P. 205-207.

[9] Arshiya S., Aruna B., Guru Prasad P., Tenali R.K. (2019), ‘Steganography security on bank system’, International Journal of Recent Technology and Engineering, 8(1), P.P. 247-250.

[10] Dasari, Rakesh Nag, Y. Prasanth, and O. NagaRaju. "A Novel Framework for Cloud Storage Security Using two way Verification." International Journal of Applied Engineering Research 12, no. 22 (2017): 11787-11795.

[11] Suma P., Nagaraju O., Hussain M.A. (2017), 'Node disjoint random and optimal path selection (NDROPS) algorithm for security in MANETS', International Journal of Electrical and Computer Engineering, 7(3), P.P. 1197-1203.