International Research Journal of Emerging Trends in Multidisciplinary
ISSN 2395-4434
Volume 1, Issue 6 August 2015
www.irjetm.com

PREVENTION OF MITM ATTACKS USING SSL

R. Sathiyasri[1] , V.Shalini[2] , Sindhujaa.N[3] and S.Kesavan[4]
[1,2,,3,4] Assistant Professor, Department of Master of Computer Applications, Mahendra College of Engineering, Anna University,Chennai,Tamilnadu,
sathiyasri90@gmail.com, shaliniv43@gmail.com,sindhujaan@mahendracollege.com and kesavansmca@gmail.com

***Abstract*— In our day to day life new technique has been implemented by the attackers to steal information. Most common technique used to steal information through network is man in the middle attack. A man-in-the-middle attack can be successful only when the attacker form mutual authentication between two parties. Most cryptographic protocols which always provides some form of end point authentication, which specify to block MITM attacks on users. We proposed a Secure Sockets Layer (SSL) protocol is always being used to authenticate one or both parties using a mutually trusted certification authority.**

Keywords—Attack, Protocol, Socket,

1. Introduction

Cyber security are standards security which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks. Cyber security has some standards which have been created recently because of the sensitive information which is now frequently stored on computers that are attached to the Internet. Information security is a practice that defends information from unauthorized access, use, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may taken from electronic, physical, etc... Information security has two major aspects :

IT security: Information Technology Security where information security applied to technology (most often some form of computer system). Information assurance: Ensuring of data is not lost when critical issues arise. These issues include to natural disasters, computer malfunction, physical theft or any other instance where data has the potential of being lost. Most of the information is stored on computers, information assurance is typically deal with by IT security specialists. The most common methods of providing information assurance is to have an off-site backup of the data.

Now a days data transmission is the most serious security threats occur within the Wide Area Network (WAN).

Hackers can easily intercept, alter or delete important data with little danger of detection. A general definition of a man-in-the-middle attack may be described as a "Computer security breach in which a malicious user intercepts and possibly alters data traveling along a network" [1].

Information stealing is performed in different activity like

- Form Grabbing,
- Man in the middle attacks,
- DLL injection.

2. Related Work

Mattias Eriksson [2] has proposed a tool to perform attacks against authenticated SSL-sessions can be made quite easy by using available programming libraries. The security protocol SSL (Secure Socket Layer) or TLS (Transport Layer Security) is used to create a secure connection to web services. The connections is mainly server authenticated, which means that the servers can trust any client. The man-in-the-middle attack is often discussed as practical inconceivable. Internet applications use SSL/TLS [3][4] to provide an encrypted connection. SSL/TLS can create a two-way trust relationship between the user and the application which require administration and distribution of certificates to all users and management of revocation lists which tend to be complex. The tool that can make the following capabilities in useful way:

· Handle SSL-connections.
· Log all traffic.

· Manipulation of data, and temporary store values in variables.
· Hijack sessions.

A tool with these capabilities could be used to launch attacks against e-commercesites, and other quite sophisticated web services.

Architectural Design

To make it possible to handle "safe" web services a modular design of the input is required, where it is possible to alter between ordinary sockets and SSL.
A configuration interface is also required to control the input/output layer and also to configure the data processing engine.

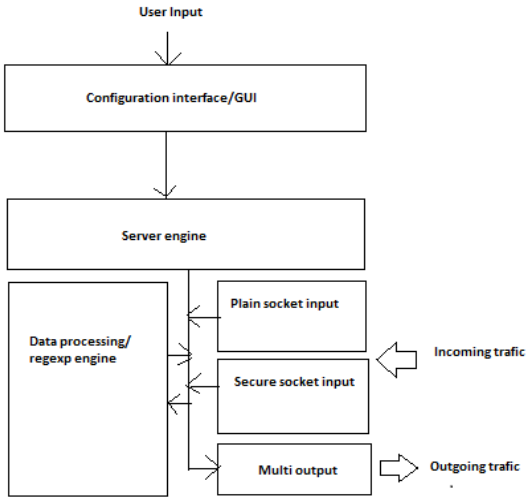

Figure 2.1: An architectural overview of the attack tool

All the parts of the architecture should perform a small but vital part in the design, bydesigning the architecture this way it is easy to add or replace a certain part of the toolto extend the functionality.

Ulrike Meyer and Susanne Wetzel[5] has proposed the Universal Mobile Telecommunication Standard (UMTS) in man-in-the-middle attack, one of the newly emerging 3G mobile technologies. The attackers allows an intruder to impersonate a valid GSM base station to a UMTS subscriber regardless of the fact that UMTS authentication and key agreement are used.where an intruder can eavesdrop on all mobile-station-initiated traffic. the UMTS standard requires mutual authentication between the mobile station and the network, the UMTS networks were considered to be secure against man-in-the-middle attacks. The network authentication which defines the UMTS standard depends on both the validity of the authentication token and the integrity protection of the subsequent security mode command.

JethroBeekman and Christopher Thompson[6] has proposed a man in the middle attrack on T-mobile on wi-fi calling, in which users make and receive calls even without cellular service. This service has been pre-installed on millions of TMobile Android smartphones. Analyzing the security aspects of this service from a network perspective, and to demonstrate a man-in-the-middle attack caused by a lack of TLS, allowing an attacker to eavesdrop and even modify calls and text messages placed using the Wi-Fi Calling feature. a TLS connection is established to the host and port returned by DNS.

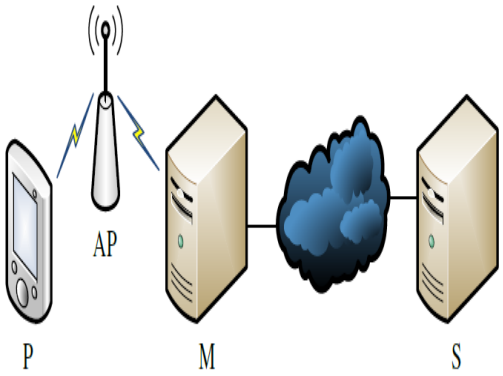

Figure 2.3 Wireless man-in-the-middle setup where P-Phone, AP-Access point, M-Man in the middle, S- Server.

Mike Burkitt [6] describes a Virtual Private Network (VPN) which refers to use of public networks to carry secure private information between intra-company locations (intranets) or inter-company locations (extranets). A VPN can built on the Internet or on a network service provider's IP, which relays frame or ATM infrastructure. VPNsis based on IP extend intranets over wide area links to remote offices, to mobile users or to telecomputers. Extended extranets, linking to the business partner's, customers and suppliers which providesa better customer satisfaction and reduced manufacturing costs.

Authentication servers and usernames or passwords

Authentication of identity is often used to carry out within a RADIUS server and TACACS server. The basic material for the authentication is to identity within RADIUS or TACACS is the username attribute and optional password attribute.

Tokens

There are two distinct types of tokens.

PC Card compatible portable hardware device .
Credit card-size portable hardware device.

Digital signatures

Digital signatures are derived through public key cryptography,while using the same key to encrypt and decrypt data, the public key cryptography system is used a match the pair of encryption and decryption keys. Each key can perform a one way transformation upon the data. The public key encrypts data while the private key decrypts data. When a "message" is encrypted with a private key, it provides a "digital signature", a message that are scrambled where only one person could produce, and everyone could verify with the person's public key.

Roi Saltzman and AdiSharabani [7] described 'Man-in-the-Middle' attacks is revist and examine a frightening category of MITM attacks that targets WebApplications. An attacker can steal user's private data form any site the attacker chooses when the victim uses a public network. "Passive attack" is the term which is used to describe methods in which an attacker intercepts sensitive data sent to or received by a user from the router in an untrusted network. The new category of attack that will be presented here is to enables an attacker to harm even a cautious user who avoids the risk of Passive attacks by surfing only "vanilla" sites such as news sites, this category is called Active attacks. Microsoft suggests various rules for using public wireless networks, for example, the user is advised to use firewall, not to connect to unencrypted networks and not to submit a sensitive information. These are the precautions for using a public network securely. This protect against Passive attacks, and are not enough to protect against Active attacks.

Active attack cautious against *Passive* attacks, an attacker could achieve the following goals while the user browses an "innocent" site.

1. Steal the victim's session cookies for any other site
2. Override Same Origin Policy for any other site (this has the same impact as XSS)
3. Steal the browser's saved passwords for any other site
4. Poison the browser cache for any other site (this will make the attack persistent)
5. Maybe even more…

Dealing with the issue of Active attacks is of fixing specific bugs and the result is of a fundamental design flaw. Browsing the Internet using a publicnetwork cannot be considered safe no matter which sites you visit or what information yousubmit.

3. Proposed methodology

A Secure Sockets Layer (SSL) protocol is always being used to authenticate one or both parties using a mutually trusted certification authority. The Secure Sockets Layer is a commonly used protocol for managing the security of a message transmission on the Internet. SSL has been recently succeeded by TLS, which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. TLS and SSL are an integral part of most Web browsers (clients) and Web servers. A website is on a server that supports SSL, and that can be enabled to specify a web pages that can be identified as requiring SSL access. Web server can be enabled by using Netscape's SSLwhich refers the program library that can be downloaded for noncommercial use or licensed for commercial use. TLS and SSL are not interoperable. A message can be sent with TLS and are handled by a client that handles SSL but not TLS.

4. Conclusion

In this paper a Secure Sockets Layer (SSL) protocol is proposed which is always being used to authenticate one or both parties using a mutually trusted certification authority. A man-in-the-middle attack can be successful only when the attacker form mutual authentication between two parties. Most cryptographic protocols which always provides some form of end point authentication, which specify to block MITM attacks on users. Possible future efforts include the SSL in all process of message transfer protocol .

4.1.1.1.1 References

[1] Definition of man-in-the-middle - http://www.wordspy.com/words/maninthemiddleattack.asp

[2] Eriksson, Mattias, Simovits Consulting, and Wenner-Gren Center. "An example of a man-in-the-middle attack against server authenticated SSL-sessions", International Conference on applied cryptography and network security, 2003.

[3] http://wp.netscape.com/eng/ssl3/-
SSL specification.

[4]http://www.ietf.org/rfc/rfc2246.txt- TLSspecification

[5] Ulrike Meyer and Susanne Wetzel, "A Man-in- the-Middle Attack on UMTS",processings of the 3rd ACM workshop on wireless security,pages 90-97,2004.

[6] JethroBeekman and Christopher Thompson, "Man-in-the-Middle Attack on T-Mobile Wi-Fi Calling",http://www.eecs.berkeley.edu/Pubs/TechRpts/2013/EECS-2013-18.html,March19,2013.

[7] Roi Saltzman and AdiSharabani" Active Man in the Middle Attacks"A whitepaper from IBM Rational Application Security Group, February 27, 2009.