Abstract

Man-In-The-Middle attack is the major attack on SSL. Some of the major attacks on SSL are ARP poisoning and the phishing attack. Phishing is the social engineering attack to steal the credential information from the user using either fake certificates or fake web-pages. Same in the case of ARP Poisoning, where in the attacker act as middle-man in the client-server communication channel. 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 whereabouts of the forged certificates and their corresponding attacks, they accept the certificates making way for the attackers to implement the attack. To deal with such attacks, two approaches have been proposed: one for the ARP poisoning; and other for phishing attack.

References

- Introduction to Secured Socket Layer. White Paper Cisco System.
Analysis on Man in the Middle Attack on SSL


Index Terms

Computer Science

Network Security

Keywords

Ssl  Tls  Man In The Middle Attack  Security  Arp  Phishing