PHISHING PREVENTION FROM MAN-IN-THE-MIDDLE ATTACK.

(1) Shrikant Patel, (2) Preeti Gulia

1. Assistant Professor, BPIBS, Govt. Of Delhi. E-Mail: patelshrikant@rediffmail.com
2. Assistant Professor, MDU, Rohtak. E-Mail: preetigulia81@gmail.com

Abstract

This research paper describes phishing attack and the measures available in order to prevent and rectify it using trusted computing technology. It gives an in depth study of the various malicious strategies used by attackers to deceive users and harvesting personal information. This paper focuses on the man-in-the-middle attacks as a sophisticated form of phishing attack. It then examines the various available solutions to phishing and the failures associated with each of these solutions. It then examines phishing prevention using trusted computing technology. Most secure web sites use the Secure Socket layer/Transport layer Security protocol for server authentication. Secure Socket layer/Transport layer Security supports mutual authentication, i.e. both server and client authentication. In any case, this discretionary element of Secure Socket layer/Transport layer Security is not utilized by most sites on the grounds that not every customer has an ensured open key. Rather client confirmation is regularly accomplished by sending a secret key to the server after the foundation of a SSL-ensured channel. Certain assaults depend on this, for example, web mocking and phishing assaults. In this paper the issue of online client validation is talked about, and a strategy for online client confirmation utilizing trusted figuring stages is proposed. The proposed methodology makes a class of phishing assaults insufficient; additionally, the proposed system can likewise be utilized to secure against other online assaults.