

Abstract

Phishing attack is a kind of identity theft which tries to steal confidential data like on-line banking account information. Different approaches have been proposed to defeat phishing attacks, but none of them prevents real-time phishing attacks. This research proposes two approaches to prevent phishing attacks. In a typical phishing attack scenario, a fraudulent email which is called scam is sent to users in order to mislead them. In this research we propose a hierarchical mechanism based on heuristic and learning methods to detect scams.

This research also proposes another new approach that specifically prevents from Man In the Middle Phishing attacks. It uses two-way authentication. Since passwords are not exchanged, there is no way a password can be Phished. The proposed technique assumes the preexistence of a shared secret key between any two communicating partners, and ignores the existence of any Malware at client sides. A tool is developed based on this approach that consists of an extension to the browser and a set of routines at server side to check the authenticity of users who log in.