MIS Review Vol. 16, No. 2, March (2011), pp. 93-110

Secure Password Based Authentication Protocol to Thwart Online Dictionary Attacks

Sandeep K. Sood
Department of Computer Science and Engineering, Guru Nanak Dev University Regional Campus, Gurdaspur, India

ABSTRACT: *Password is the most universally used authentication technique to authenticate the users on the web. Password based authentication protocols are vulnerable to dictionary attacks by means of automated programs because most of the user chosen passwords are limited to the user's personal domain. In this paper, we propose a secure password based authentication protocol in which the computation efforts required from the attacker during login on to the web server increases with each login failure. The web server stores the cookie on the client's computer if the legitimate client authenticates itself to the web server. There after, the legitimate client can easily authenticate itself to the web server from a computer that contains cookie. However, the legitimate client or the attacker has to put up some additional computational efforts during login from a computer that does not contain cookie. The client generated dynamic authentication information is different for the same user in different sessions of Secure Socket Layer (SSL) protocol. The concept used in this paper is to combine traditional password authentication with a challenge that is easy to answer by the legitimate client and the computational cost of authentication increases for an attacker with each login failure. Therefore, even the automated programs can not launch online dictionary attacks on the proposed protocol. This protocol provides better protection against different types of attacks launched by the attacker. The proposed protocol is easy to implement and it removes the some of the deficiencies of previously suggested password based authentication protocols.*

KEYWORDS: *Hyper Text Transfer Protocol, Cookies, Password, Secure Socket Layer, Online Dictionary Attacks.*

1. Introduction

Hyper Text Transfer Protocol (HTTP) is used to provide interaction between the web browser and the web server. It is stateless because the HTTP server treats each request independent of any previous request from the same client. The HTTP server does not maintain the correlation of the user visits from the same browser between successive sessions. The users are always strange to the web server if the web server does not maintain the state and continuity of the user (Park and Sandhu, 2000). Statelessness on the web makes it difficult to carry out online financial transactions in e-commerce.