ABSTRACT

Majority of enterprise machines which handle confidential data are Linux systems. These Linux systems are made to be publicly accessible by SSH or putty to customers, clients, and developers. Current Linux authentication only includes just username and password which is considered vulnerable today for many attacks like phishing, shoulder surfing etc. Enforcement of multifactor authentication by directly hooking the Linux authentication can help enhance security multi fold as added authorization layer helps identify personalities. Special logging techniques and custom IP level security can also be enforced by the proposed hooking method. This methodology of hooking Linux authentication can not only be used for Linux logins but also services that use Linux authentication which includes SSH, sudo, Identity providers like Active Directory. Every Linux machine irrespective of its distro has the authentication module which acts as the entry point in perspective of an user whether be the owner or a remote user.