

ABSTRACT

Simple Network Management Protocol (SNMP) is a protocol designed to enable administrators to monitor the state of a network. SNMP server would store a lot of information related to the monitored devices, Therefore SNMP requires an authentication system that is able to identify each client. To reduce the level of aggression and minimize the possibility of attacks against password, administrator made Two Factor Authentication System using One Time Password (OTP) method.

Mobile One Time Password (MOTP) is a one of OTP authentication method where the administrator is required to use a dynamic passwords and using a mobile phone as a token generator. This final project will be implementing a authentication systems using MOTP method on the SNMP server, then do testing and analyze of issues at MOTP Collison, MOTP time required to identify a client, experiment to sniff the token during the sending process, memory consumption and CPU usage of MOTP authentication system, enhanced features to limiting the duration of the login and access authority.

From the research, can be seen that MOTP can verifying every client that want to access SNMP server, but the tokens that generated by MOTP still can be sniff by an unauthorized person. MOTP proved that MOTP not affected by Collison issue on MOTP tokens. MOTP also has average verification time and CPU usage that is less favorable than auth_basic authentication methods, but MOTP has the features to limiting the duration of login and access authority.

Keywords: SNMP, Two Factor Authentication, MOTP