An accuracy of attack detection using attack recognition technique in multi-factor authentication scheme

ABSTRACT

One popular scheme used for authentication security is the implementation of multi-factor authentication (MFA). There have been several researches that discusses on multi-factor authentication scheme but most of these research do not entirely protect data against all types of attacks. Furthermore, most current research only focuses on improving the security part of authentication while neglecting other important parts such as the systems accuracy. Accuracy is based on how perfect is the system able to identify a genuine user or an intruder. Current multifactor authentication schemes were simply not designed to have security and accuracy as their focus. Accuracy can be measured as the success rate on tasks that requires a certain degree. For instance, the number of users who is successfully logging into the system using any technique provides a measure of accuracy. Usually, accuracy demands of users are impacted by other demands such as recall of required information, environmental, or other factors. In authentication, the accuracy factor was identified through the device pairing studies. In many cases in the authentication system requires users to enter a password or biometric traits with 100 percent accuracy for comparing it. Nevertheless, this research analyzes the level of accuracy based on the biometric accuracy of authentication. In this paper will explain the evaluation process on the accuracy level of the proposed authentication to get a highly accurate performance, which is based on FAR (false acceptance rate) and FRR (false rejection rate). Result from the experiment shows that the accuracy of proposed scheme is better than the accuracy of other previous schemes. This is even after additional security features has been added to the scheme.

Keyword: Security; Multi-factor authentication; Accuracy