World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:04, 2020

Evaluation of Gesture-Based Password: User Behavioral Features Using Machine Learning Algorithms

Authors : Lakshmidevi Sreeramareddy, Komalpreet Kaur, Nane Pothier

Abstract : Graphical-based passwords have existed for decades. Their major advantage is that they are easier to remember than an alphanumeric password. However, their disadvantage (especially recognition-based passwords) is the smaller password space, making them more vulnerable to brute force attacks. Graphical passwords are also highly susceptible to the shoulder-surfing effect. The gesture-based password method that we developed is a grid-free, template-free method. In this study, we evaluated the gesture-based passwords for usability and vulnerability. The results of the study are significant. We developed a gesture-based password application for data collection. Two modes of data collection were used: Creation mode and Replication mode. In creation mode (Session 1), users were asked to create six different passwords and reenter each password five times. In replication mode, users saw a password image created by some other user for a fixed duration of time. Three different duration timers, such as 5 seconds (Session 2), 10 seconds (Session 3), and 15 seconds (Session 4), were used to mimic the shoulder-surfing attack. After the timer expired, the password image was removed, and users were asked to replicate the password. There were 74, 57, 50, and 44 users participated in Session 1, Session 2, Session 3, and Session 4 respectfully. In this study, the machine learning algorithms have been applied to determine whether the person is a genuine user or an imposter based on the password entered. Five different machine learning algorithms were deployed to compare the performance in user authentication: namely, Decision Trees, Linear Discriminant Analysis, Naive Bayes Classifier, Support Vector Machines (SVMs) with Gaussian Radial Basis Kernel function, and K-Nearest Neighbor. Gesture-based password features vary from one entry to the next. It is difficult to distinguish between a creator and an intruder for authentication. For each password entered by the user, four features were extracted: password score, password length, password speed, and password size. All four features were normalized before being fed to a classifier. Three different classifiers were trained using data from all four sessions. Classifiers A, B, and C were trained and tested using data from the password creation session and the password replication with a timer of 5 seconds, 10 seconds, and 15 seconds, respectively. The classification accuracies for Classifier A using five ML algorithms are 72.5%, 71.3%, 71.9%, 74.4%, and 72.9%, respectively. The classification accuracies for Classifier B using five ML algorithms are 69.7%, 67.9%, 70.2%, 73.8%, and 71.2%, respectively. The classification accuracies for Classifier C using five ML algorithms are 68.1%, 64.9%, 68.4%, 71.5%, and 69.8%, respectively. SVMs with Gaussian Radial Basis Kernel outperform other ML algorithms for gesture-based password authentication. Results confirm that the shorter the duration of the shoulder-surfing attack, the higher the authentication accuracy. In conclusion, behavioral features extracted from the gesture-based passwords lead to less vulnerable user authentication.

Keywords : authentication, gesture-based passwords, machine learning algorithms, shoulder-surfing attacks, usability
Conference Title : ICMLDM 2020 : International Conference on Machine Learning and Data Mining
Conference Location : Boston, United States
Conference Dates : April 23-24, 2020