Graphical Passwords: A Qualitative Study of Password Patterns

Jo Vorster and Renier van Heerden

Abstract:
Graphical passwords schemas are becoming more main-stream. There are many different approaches to graphical passwords, each with its own drawbacks and advantages. There has been many studies to suggest that graphical passwords should be stronger in terms of security because people are better at remembering them. It is well known that the key-space for graphical passwords are at least equivalent to alpha-numeric passwords and can even be much stronger, depending on the schema. Similar to conventional passwords, graphical passwords may have patterns. A pattern that has been widely reported in the literature and studied in some detail are that of hotspots. That is, a high percentage of people will select the same spots on an image. This paper focus on a quantitative analysis of graphical passwords. During this study users from commercial companies were asked to enter graphical passwords. These passwords were then analysed and patterns identified. Users were also asked what there password selection strategies are. The combination of this information enable a qualitative analysis of graphical passwords. The results show that graphical passwords are less secure than expected, that there are a number of patterns that limit the key-space significantly and thus reduce the strength of such password schemas. Users were also asked about their perception of the security of graphical passwords. The survey suggest that users are divided in their opinion on how secure such technologies are. Lastly we also report on reasons that users gave for why they think such technology are not yet ready for use as a security mechanism in an organizational context.

Keywords: graphical passwords, access management