Abstract

The concept of having to identify an entity before being allowed to perform any action is quite acceptable, and expected, and required in today’s wired world. Password managers, graphical systems, pattern recognition, biometrics have always been found to be incapable of providing robust security in some or the other aspect, in critical authentication systems [24]. In our approach, the user at the time of profile creation is required to enter the password, minimum of 6 characters and a secret numeric PIN of minimum 4 digits. Now during subsequent login attempts, the user will be asked to enter the password as an answer to a random mathematical question displayed in front of him in the form of an image (readable only by human and not by a software entity) [15]. Example; Consider the password: KOREAN and secret pin: 1234, the question would be; your 2nd character of password varies by 1+3rd character of your secret pin.
Now instead of the original password, the user will enter the new password as KSREAN. The password can contain any combination of the available 96 characters on the keyboard. Every time only the same character of the password will be changed. The secret pin must contain only digits (to increase security, length can be increased to 10 or more digits). If the user enters the correct password he is authenticated otherwise denied access. This concept has some assumptions that the site locks the account if number of attempts for a particular user name exceeds a predetermined threshold.

References

- W. Belgers, "Unix password security". http://www. het. brown. edu/guide/UNIX-password-security. txt
org/conference/15th-usenix-security-symposium/usability-study-and-critique-two-password-managers&quot;.

Index Terms

Computer Science

Security
User Authentication System using Cryptography Involving Arithmetic Operations

Keywords
Information security  user authentication  cryptography  phishing  click recorders
screen recorders
arithmetic operations