Someone in Your Contact List: Cued Recall-Based Textual Passwords

Aim:

The aim of this project is to achieve a novel and sound cued recallbased textual password method that reveals no information regarding the password, requires no modifications to authentication servers, and requires no additional setup or registration steps.

Objective:

- To formulate the notion of a password hint, and discuss the optimal features of an effective password hint system under various conflicting constraints.

Abstract:

Textual passwords remain the most commonly employed user authentication mechanism, and potentially will continue to be so for years to come. Despite the well-known security and usability issues concerning textual passwords, none of the numerous proposed authentication alternatives appear to have achieved a sufficient level of adoption to dominate in the foreseeable future. Password hints, consisting of a user generated text saved at the account setup stage, are employed in several authentication systems to help users to recall forgotten passwords. However, users are often unable to create hints that jog the memory without revealing too much information regarding the passwords themselves.

We propose a rethink of password hints by introducing S`YNTHIMA, a novel cued recall-based textual password method that reveals no information regarding the password, requires no modifications to authentication servers, and requires no additional setup or registration steps.

Introduction:

IN the vast majority of authentication systems, textual password schemes are the dominant choice for authenticating end users, despite the well-known security issues concerning passwords, and the inconvenience incurred by end users in remembering multiple passwords for different accounts. Typically, users tend to choose easy-to-remember passwords that are also easy for adversaries to guess . In addition, security vulnerabilities, phishing of credentials, and poor security practices in storing password-related files have led to large-scale security breaches and an ongoing online trade of hundreds of millions of stolen usernames and passwords belonging to various accounts End users are often compelled to choose "strong" passwords

(e.g., through password meters). However, security and usability trade-offs (e.g., password strength vs. memorability and password strength vs. reuse) limit not only the ability of users to create unique and strong passwords for their accounts , but also increase the likelihood that users find such processes burdensome and irritating