Someone in Your Contact List Cued Recall-Based Textual Passwords

ABSTRACT

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. In fact, passwords are to blame for many recent data breaches. A recent report considered the ineffective use of passwords as a major factor that enabled top IT security attacks in 2016.

EXISTING SYSTEM

In Existing System, 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.

DIS ADVANTAGES

- Lack of knowledge regarding the direct financial and data losses resulting from password related security issues.
- Increases the amounts of cognitive effort, time, and resources required to memorize new passwords.

www.takeoffprojects.com

PROPOSED SYSTEM

In Proposed System, we presented SYNTHIMA, a mechanism that applies cued recall to textual passwords. We apply SYNTHIMA on minimizing the number of invalid login attempts, and improving memory recall for textual passwords. Our preliminary findings demonstrate that the application of SYSNTHIMA decreased the number of failed login attempts and improved the password recall rate. We also expect that the application of SYNTHIMA would have important implications on minimizing users need to resort to other verification methods to regain access to blocked accounts.

ADVANTAGES

- A better security level is achieved as the length of the salt value increases.
- Effective password hint system under various conflicting constraints.

SYSTEM REQUIREMENTS

H/W System Configuration:-

Processor	-	Pentium –III
RAM	-	256 MB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

S/W System Configuration:-

Operating System	:	Windows95/98/2000/XP
Application Server	:	Tomcat5.0/6.X

www.takeoffprojects.com

Front End	:	HTML, Jsp
Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.
Database	:	MySQL 5.0
Database Connectivity	:	JDBC

www.takeoffprojects.com