ABSTRACT

The design of a user authentication protocol named oPass which

leverages a user’s cell phone and short message service to thwart password

stealing and password reuse attacks. OPass only requires each participating

website possesses a unique phone Number, and involves a

telecommunication service provider in registration and recovery phases

Textual passwords are the most common method used for authentication. But

textual Passwords are vulnerable to eves dropping, dictionary attacks, social

engineering and shoulder surfing. Graphical passwords are introduced as

alternative techniques to textual passwords. Most of the graphical schemes

are vulnerable to shoulder surfing. To address this problem, text can be

combined with images or colors to generate session passwords for

authentication. Session passwords can be used only once and every time a

new password is generated. The paper, two techniques are proposed to

generate session passwords using text and colors which are resistant to

shoulder surfing. These methods are suitable for Personal Digital Assistants.

It is designed using active server pages with Microsoft visual studio.