Authentication Using Graphical Password: Effects of Increased Security on Usability

William M. Martin

Aaron G. Cass
March 3, 2018
Introduction

01 Human Computer Interface Security (HClsec)
02 Password Problem
03 Graphical User Authentication
Enter your password.
Introduction

Graphical User Authentication

Extremely suitable for mobile devices.

Quick registration and login times.

Greater ability to memorize images in long term memory.

Error rates and failed login attempts are reduced.
Background and Related Work

Previous Research states that in many areas, GUA is more secure when compared to alphanumeric authentication.

Brute-Force  Dictionary  Phishing  Spy-Ware

Previous Research states that in many areas, GUA is more secure when compared to alphanumeric authentication.
Background and Related Work
Can a Graphical User Authentication System achieve resilience towards shoulder surfing without lowering usability?
Methods and Design

PassPoints

Discrete Wavelet Transform

(a) Decoy image (256 × 256 pixels, 24bpp)
(b) Pass-image (256 × 256 pixels, 24bpp)
(c) Blended image
(d) A part of blended image (Enlarged)
Methods and Design

Enter your password.

PassMatrix

Enter your password.

PassDecoy
Methods and Design

Hybrid Imagery

High Frequency - Password Image

Low Frequency - Decoy Image
Experiments Performed

User Study

- 20 Participants
- Interact with both systems
- Test order was randomly administered

Effectiveness
- Number of Failures
- Number of Errors

Efficiency
- Registration Time
- Login Time

Satisfaction
- 5 question survey
- Likert-Scale Responses
Results

Number of User Errors

There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.

Number of Failed Login Attempts

There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.

p-value: .716

p-value: 1
Results

Login Time

There is sufficient evidence to demonstrate that there is a difference between the two systems, if the test was given to a larger group.

With a confidence of 95%, it can be said that PassDecoy will take users an additional .25 - 1.13 seconds per login attempt.
Results

It did not take me long to input my password 3 times.

There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.

Once I created my password, I was able to input it correctly.

There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.

p-value: .330

p-value: .666
There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.

**Registering my password was fast.**

p-value: .494

**Inputting my password was easy.**

p-value: .330
My password images are easy to memorize.

There is sufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.

p-value: .007
Research Question

Can a Graphical User Authentication System achieve resilience towards shoulder surfing without lowering usability?
Future Work

01. Remove color from the password image during registration.

02. Test how differences in visual capability effected the results.

03. Conduct additional user tests to see if login time can be reduced through practice.

