The Effects of Increased Security on Graphical User Authentication Usability

William M. Martin
Aaron Cass, Advisor

UNION COLLEGE

Introduction and Motivation

The idea of Graphical Passwords is to have the user select a few chosen regions from an image as their password input. This image will then be presented again in a Graphical User Authentication (GUA) interface, where the user will recall these regions in specif c order. This approach has been shown to be user friendly and secure against certain types of attacks, such as brute force and phishing [1].

Figure 2. PassMatrix, a GUA proposed by Sun et. al.

However, GUA still has vulnerabilities to security attacks such as Shoulder Surf ng (SS). Many attempts have been made to solve this specif c problem, but they either do not test for usability, or observe a decrease in usability when it is tested for [2].

This has resulted in countless proposed systems with poor usability, and unfortunately halted the trend towards implementing GUA systems.

	Brute Force	Phishing Attack	Shoulder Surfing	User Friendly
Alphanumeric	✗	✗	✓	O.K.
1-Time Pass	✗	✓	✓	✗
PassMatrix	✓	✓	✗	?
PassDecoy	✓	✓	✓	?

Figure 1. Password Type Comparison

Question

Can a Graphical User Authentication System achieve resilience to Shoulder Surf ng with out lowering Usability?

Solution

I propose implementing two GUA systems and testing usability measures across each. One of these systems will be PassMatrix, a previously studied model which is susceptible to SS attacks. The second model will be PassDecoy, which contains an additional level of security, but an unknown degree of usability due to the fact it has not been tested in a user study.

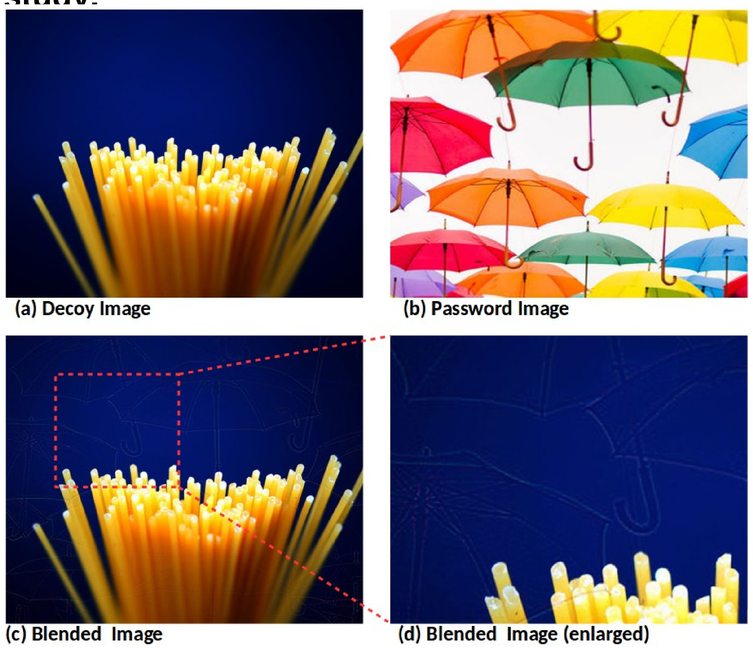

Figure 3. PassDecoy example image.

PassDecoy

In the proposed solution, the additional level of security is a decoy image. This decoy is blended with a password image using High–Pass Filters in Photoshop.

Experiment Design

To determine whether an increase in security explicitly results in decreased usability a user study will be conducted in CROCHET Laboratory.

- 30 participants across two 15 minute sessions
- Participant interacts with both models

Usability measures will be recorded to determine each models degree of usability. User Effectiveness, Eff ciency and Satisfaction will be studied using the following measures:

Effectiveness
- Success Ratio (%)
- Number of Retries (Mead, Median, SD)

Efficiency
- Authentication Time (Seconds)
- Number of Errors (Mean, Median, SD)

Satisfaction
- Questionnaire (5-8 Questions)

Measures for usability are consistent with measures used in previous studies, so that results may be generalized

Figure 4. Usability Measures

Future Work

- Implementation of PassDecoy
- User Study Comparing Usability
- Proposal of a User-Friendly and Shoulder-Surf ng resilient GUA model.

References

[1] Zhi Li, Qibin Sun, Youg Lian, and D.D. Giusto ”An Association-Based Graphical Password Design Resistant to Shoulder-Surf ng Attack,” in IEEE Amsterdam, Netherlands. 2005.

[2] Hung-Min Sun and Shiuan-Tung Chen “A Shoulder Surf ng Resistant Graphical Authentication System” in IEEE Transactions on Dependable and Secure Computing. 2015.