2012

ColorDots: An Intersection Analysis Resistant Graphical Password Scheme for the Prevention of Shoulder-surfing Attack

Jim Littleton
University of North Florida

ColorDots: An Intersection Analysis Resistant Graphical Password Scheme for the Prevention of Shoulder-surfing Attack

by

Jim Littleton

A thesis submitted to the
School of Computing
in partial fulfillment of the requirements for the degree of

Master of Science in Computer and Information Sciences

UNIVERSITY OF NORTH FLORIDA
SCHOOL OF COMPUTING

April 2012

The thesis "ColorDots: An Intersection Analysis Resistant Graphical Password Scheme for the Prevention of Shoulder-surfing Attack" submitted by Jim Littleton in partial fulfillment of the requirements for the degree of Master of Science in Computer and Information Sciences has been

Approved by the thesis committee: Date

Signature Deleted

4/6/2012

Dr. F. Layne Wallace
Thesis Adviser and Committee Chairman

Signature Deleted

4/6/2012

Dr. Robert F. Roggio

Signature Deleted

4/6/2012

Dr. Karthikeyan Umapathy

Accepted for the School of Computing:

Signature Deleted

7-11-2012

Dr. Asai Asaithambi
Director of the School

Accepted for the College of Computing, Engineering, and Construction:

Signature Deleted

7/13/12

Dr. Mark A. Tumeo
Dean of the College

Accepted for the University:

Signature Deleted

8/6/12

Dr. Len Roberson
Dean of the Graduate School

ACKNOWLEDGEMENT

This thesis would have been impossible without the loving support and understanding of my beautiful wife, Jeannie – to her I owe the greatest debt of gratitude. I would also like to thank my adviser, Dr. Layne Wallace, whose guidance and support, not only helped me complete this thesis, but also taught me that research can be fun. Furthermore, I would like to show my gratitude to a great friend, Bart Wheeler, who has always been willing to offer writing advice or simply listen as I vent my frustrations. Finally, I would like to thank everyone who made this thesis possible, especially the students and faculty members at the School of Computing who participated.

CONTENTS

TABLES

FIGURES

ABSTRACT

In an increasingly mobile world, the combination of mobile computing devices, publicly accessible Wi-Fi hotspots, and camera phones pose a significant threat to alphanumeric passwords in public environments. Graphical passwords, introduced as an alternative to alphanumerical passwords, help prevent successful shoulder-surfing attacks – covertly observing or recording a password login session, however, most cannot prevent intersection analysis on the data collected through shoulder-surfing. ColorDots is a new graphical password scheme designed to be easy to use and learn, to prevent successful shoulder-surfing attacks, and to hinder intersection analysis. A software implementation of ColorDots is tested, and the results analyzed. This study showed the ColorDots graphical password scheme does prevent shoulder-surfing, and hinders intersection analysis on digital recordings of multiple shoulder-surfing attacks. Furthermore, ColorDots may be just as convenient to use as alphanumeric passwords, while improving password security in public environments.

Chapter 1

INTRODUCTION

Computer passwords control access to computer systems and digital information. As computing systems have become more accessible, stronger and more complex password schemes have been required to prevent unauthorized access and to protect information. The preponderance of mobile computing devices, publicly accessible Wi-Fi hotspots, and camera phones (mobile phones with built-in, high-quality cameras) pose a significant threat to the continued use of alphanumeric passwords for the purpose of user authentication in public environments.

Graphical password schemes are an alternative to traditional alphanumeric passwords. Graphical passwords offer several advantages over alphanumeric passwords; however, many of the proposed schemes are susceptible to shoulder-surfing. A form of social engineering, shoulder-surfing occurs when an attacker observes or records a user entering their password to gain access to a computer system. A number of shoulder-surfing-resistant graphical password schemes have been proposed, but they offer little defense against intersection analysis. Intersection analysis is a method used to analyze the changes observed between multiple login attempts to help determine a user's password (Dumphy10). A successful graphical password scheme must prevent successful shoulder-surfing attacks and resist intersection analysis; however, it must also be easy to learn and use. A review of the literature failed to produce a single

graphical password scheme that significantly met these requirements. ColorDots is a new graphical password scheme based on the effective elements of three successful graphical password schemes. The purpose of this study is to determine whether ColorDots satisfies each of the requirements for a successful graphical password scheme. A software implementation of ColorDots allows subjects to interact with the graphical password scheme during multiple phases of testing, and the results analyzed.

Chapter 2

GRAPHICAL PASSWORDS

Greg Blonder was the first to propose graphical passwords as an alternative to alphanumeric passwords (Blonder96). Graphical password schemes are a solution to many of the human-induced vulnerabilities of alphanumeric passwords such as selecting simple or common words for passwords, writing passwords down, and using personal information within passwords. The concept that human beings are capable of recalling graphical information more easily than alphanumeric information is the basis for graphical passwords. Moncur *et al.* describes three general graphical password systems (Moncur07). Drawmetric schemes, Figure 1-A, require users to redraw a predefined picture. Cognometric schemes, Figure 1-B, require users to select a set of predefined target images from a larger set of distraction images. Locimetric schemes, Figure 1-C, require users to click predefined points on a given image.

A major drawback of the Drawmetric and Locimetric schemes is that user input is time-invariant – does not change from login to login (Man03). Although early Cognometric schemes also suffered from time-invariant input, later proposals took steps to overcome this vulnerability. The primary disadvantage of time-invariant password schemes, alphanumeric or graphical, is their susceptibility to shoulder-surfing attacks – an

attacker need only view a successful authentication attempt once to compromise a user's account (Tari06).

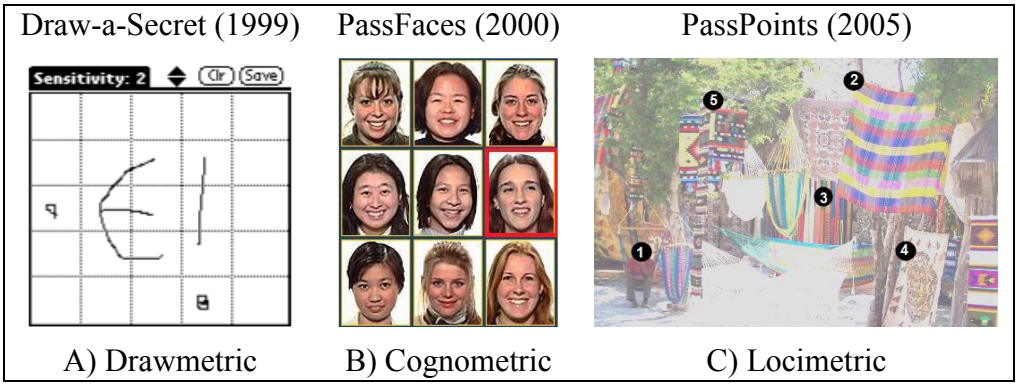

Figure 1: Graphical Password Schemes

2.1 Shoulder-surfing

Shoulder-surfing is most likely to occur in public environments such as a coffee shop, café or library where users are less likely to be suspicious of others sitting or standing nearby (Gao09). Attackers often use devices such as a camera phone to record the password entry process to reduce their risk of discovery. This has the potential of allowing attackers to collect passwords over an extended period. Such techniques have been successful against Automatic Teller Machines (ATMs) to allow attackers to make fraudulent withdrawals (De Luca10). As camera phones become more prevalent in society, shoulder-surfing attacks are likely to become more common and successful (Tari06). For this reason, researchers have proposed several graphical password schemes that resist shoulder-surfing attacks.

2.2 Shoulder-surfing Resistant Graphical Password Schemes

Graphical password schemes resistant to shoulder-surfing attacks appear in two general categories: multi-factor schemes and indirect input schemes (Lashkari09). Multi-factor schemes involve the use of multiple inputs or technologies such as a smart card, key generator dongle, voice recognition or optical scanner. Even if an attacker acquires the user's graphical password, they are unable to log into the system without the additional authentication factor(s). Indirect input schemes involve surreptitious input methods to avoid direct identification of the password such as using a keyboard, clicking within an on-screen region containing the graphical password images or tracking the user's eye movements. Due to the scope of this paper, the review of graphical password schemes is limited to indirect input schemes involving the use of a keyboard and/or mouse.

Sorbrado *et al.* proposed several graphical password schemes resistant to shoulder-surfing attacks (Sobrado02). The Intersection scheme, Figure 2, requires the user to locate their password images and click within the region containing the intersection point of the imaginary lines connecting each pair of images (the lines and circles in Figure 2 are for illustration purposes only and are not visible to the user). To prevent guessing, users are required to complete this process multiple times using different image layouts to log into the system.

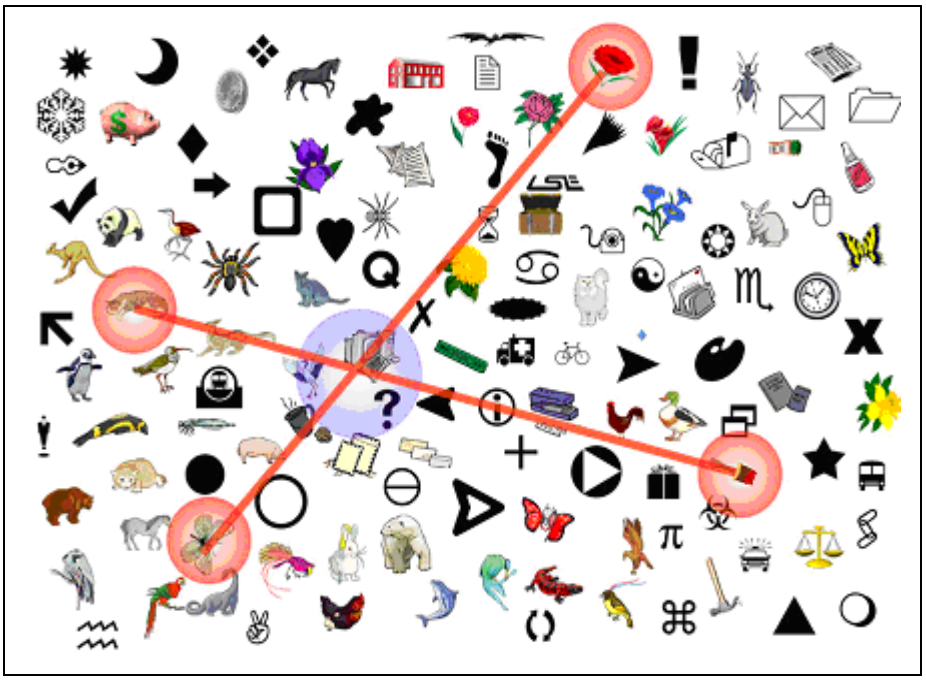

Figure 2: Intersection Scheme

The Triangle scheme, proposed by Sobrado and Birget (Sobrado02), influenced the Convex Hull Click (CHC) scheme proposed by Wiedenbeck *et al*., Figure 3 (Wiedenbeck06). The CHC scheme requires users to locate their password images and then click within the convex hull region created by the images. Like the Intersection scheme, users must complete this process multiple times in order to log into the system.

ColorPIN, Figure 4, the indirect input scheme proposed by De Luca *et al.*, uses a keyboard for password entry rather than a mouse because the scheme is intended for use with ATMs. With this scheme, users locate each number in their Personal Identification Number (PIN) and select the appropriate letter corresponding to the number's position in the PIN – black, red, white or black for positions 1, 2, 3 and 4 respectively.

Figure 3: Convex Hull Click (CHC) Scheme

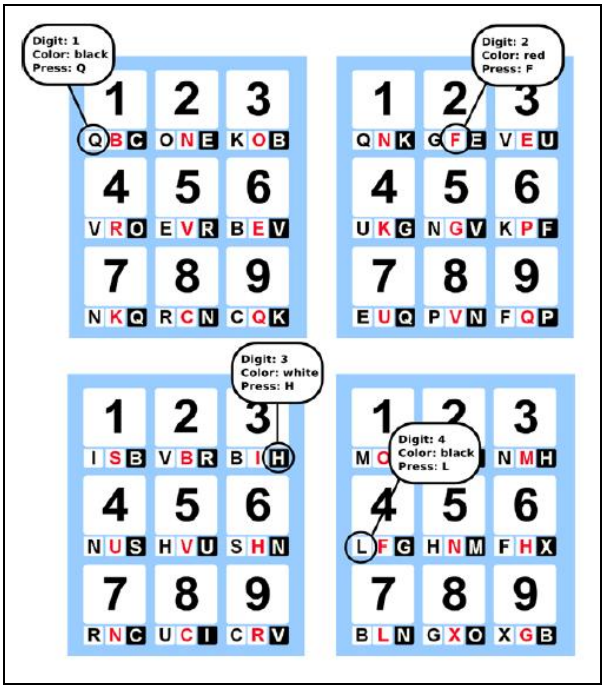

Figure 4: ColorPIN Scheme

Due to the shoulder-surfing resistant design of the reviewed graphical password schemes, even if an attacker records the user entering their password, the attacker is unable to identify the user's password images – preventing the attacker from logging into the system. However, if an attacker is able to record the user entering their password multiple times, the attacker is more likely to discover the user's password by performing intersection analysis on the recordings.

2.3 Intersection Analysis

Intersection analysis is useful for identifying users' passwords in time-variant graphical password schemes such as Intersection, CHC, and ColorPIN, where the input required to log into the system changes with each login session. Intersection analysis is more effective when performed on data contained in shoulder-surfing recordings allowing for repeated analysis of the recorded data. Studies have shown that intersection analysis performed on as few as two recordings can successfully identify a user's password (De Luca10).

One characteristic of graphical password schemes, which make them more susceptible to intersection analysis, is the ratio of the number of displayed distraction images and the total number of distraction images. A particular distraction image may appear in the interface at a lower frequency than the target images, if this ratio is low (Dumphy10). By comparing the frequency at which the images appear in the interface, an attacker

may identify the user's password images. To prevent this form of intersection analysis, researchers suggest using the same set of images for each login session.

A review of the available literature produced a number of graphical password schemes resistant to shoulder-surfing attacks, but all were susceptible to intersection analysis. Although two of these schemes claimed to be resistant to intersection analysis involving video recordings of a user's password entries, the authors failed to support their claims by considering only two such recordings or by ignoring analysis of video recordings altogether (Gao09 and Shi09).

Chapter 3

COLORDOTS

ColorDots, a new graphical password scheme, implements effective elements of the Intersection, Convex Hull Click (CHC), and ColorPIN graphical password schemes in an attempt to produce a graphical password scheme that not only resists shoulder-surfing attack, but also hinders intersection analysis.

Users must complete a registration process prior to using the ColorDots graphical password scheme. During the registration process, users will enter their personal data such as their name and email address. Additionally, users will create a username and graphical password, which involves choosing three images from the set of available images. Users can authenticate using the graphical password scheme once they complete the registration process.

The proposed graphical password interface, Figure 5, consists of the image grid, registration dots for each row and column, and a set of user controls. The image grid contains 5x5 cells where each cell consists of a border color, a password image, and five uniquely colored alphanumeric characters – each selected randomly from its respective set. The user controls include the *Enter Password* field and buttons to refresh the grid or request help.

To defend against shoulder-surfing attack, the interface prevents the mouse pointer from entering the image grid section during the authentication process. To defend against intersection analysis, after each keystroke, the interface refreshes the ColorDots grid – the system randomly shuffles all of the colors, as well as creates a new set of alphanumeric characters for each cell, however, the images are unaffected.

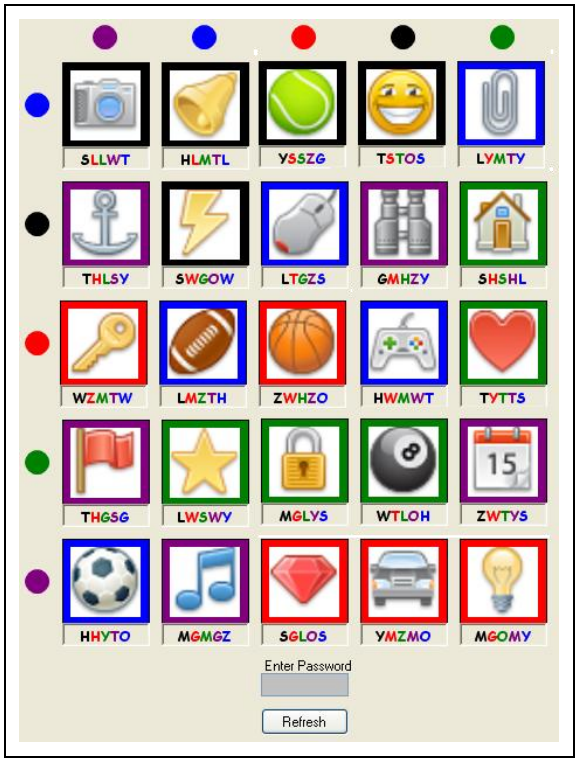

Figure 5: ColorDots Interface (FatCow11)

To log in using the ColorDots graphical password scheme, the following procedure is performed (refer to Figure 6).

1. Locate the three password images in the ColorDots grid (Figure 6-A).
2. Visualize a triangle over the ColorDots grid that connects the three password images (Figure 6-B).

3. Visually draw horizontal, vertical and diagonal lines from the center of each of the three password images towards the interior of the triangle (Figure 6-B).
4. Continue to extend the lines until one line from each password image intersects over one of the image cells within the triangle – the Initial Intersection Cell (C_0) (Figure 6-C).
5. Identify the Row Registration Dot (RRD) that has the same color as the border of C_n[1] (Figure 6-D).
6. Identify the Column Registration Dot (CRD) that has the same color as the RRD of C_n (Figure 6-D).
7. Locate the cell that exists at the intersection of the RRD and CRD identified in steps 5 and 6, respectively – the First Password Cell (C_{n+1}[2]) (Figure 6-D).
8. Identify the letter from C_{n+1} that has the same color as the CRD of C_n, and enter the letter in the password field (Figure 6-E).
9. Repeat steps 5 through 8 to locate the four remaining password cells (C_2 through C_5) starting from the last password cell identified (C_{n+1}).

After entering all five letters in the password field, the interface automatically submits the password for authentication. Clicking the Refresh button during the authentication process refreshes the image grid, and the authentication process restarts from the beginning. Clicking the Help button during the authentication process hides the image grid and displays the help screen – the image grid becomes visible again only after the help screen is closed.

[1] Possible values C_n are C_0 through C_4
[2] Possible values of C_{n+1} are C_1 through C_5

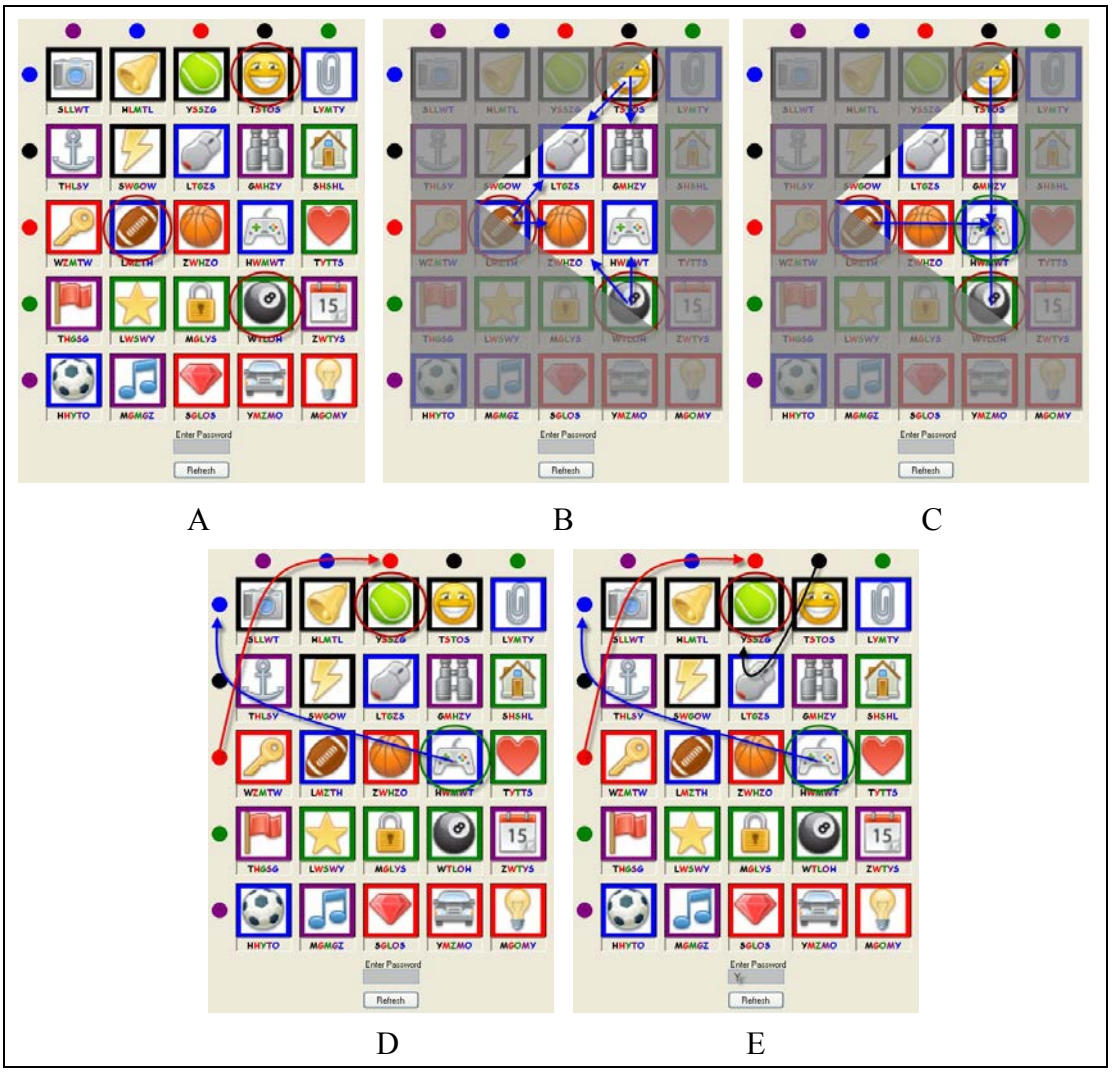

Figure 6: The ColorDots Process (FatCow11)

To prevent brute force attacks, users have a maximum of three attempts to log into the system. After each failed attempt, the interface automatically refreshes the image grid to prevent an attacker from isolating a series of image combinations. If a user fails to authenticate within three attempts, the system locks their account and sends an email message detailing the excessive attempts to their configured email address. The message directs the user to unlock their account using an enclosed link. After

unlocking their account, the system cautions the user to create a new graphical password images.

The proposed graphical password scheme eliminates shoulder-surfing attacks involving a casual observer through several key features. The user cannot move the mouse pointer over the image grid section preventing them from accidentally identifying their graphical password. The randomly selected alphanumeric characters making up the password occur throughout the interface and can appear multiple times, even in the same cell. The user enters the alphanumeric characters of the password in the password field using the keyboard, preventing simultaneous observation of the keyboard and interface. Finally, refreshing the ColorDots grid after every keystroke produces too much information for the casual observer to process.

The proposed graphical password scheme eliminates shoulder-surfing attacks involving a single recorded session using a recording device such as a camera phone. Due to the time-variant nature of the proposed scheme, the recording of a single login session is insufficient to reduce the set of password image candidates to a manageable number, which has been determined to be seven images (a 3-in-35 or 8.57% chance of selecting the correct password images).

The proposed graphical password scheme resists shoulder-surfing attacks involving multiple recorded sessions using a recording device such as a camera phone. The random nature of the ColorDots grid, including refreshing the grid after every

keystroke, hinders the use of intersection analysis to reduce the set of password image candidates to a manageable number. Although the potential exists that the analysis of each recorded session will reveal a unique set of distraction images, an estimated minimum of five such recorded sessions must exist to produce a set of seven password image candidates.

Chapter 4

EXPERIMENTAL DESIGN

The objective of the current study is to determine whether the ColorDots graphical password scheme is easy to learn, easy to use, prevents single-session shoulder-surfing attacks, and resists the intersection analysis of multiple recordings of shoulder-surfing attacks.

The evaluation of the ColorDots graphical password scheme uses a factorial design based on repeated measurements of participant performance. The independent variables are the password type (random or user-generated) and password method (alphanumeric or graphical). The alphanumeric password entries serve as the control condition. Participants perform four authentications – one authentication for each combination of the independent variables.

The current study occurs in three independent phases. The first phase tests the ability of participants to authenticate using ColorDots. The second phase tests the ability of participants to recall their graphical password one week after their initial exposure to the graphical password scheme. The third phase tests the ability of participants to identify a ColorDots graphical password using intersection analysis techniques on multiple recordings of simulated shoulder-surfing attack on a victim authenticating with ColorDots. Afterwards, participants complete a survey regarding the characteristics of

the ColorDots graphical password scheme, including its ease of use and its perceived vulnerability to shoulder-surfing attack.

4.1 Phase 1: ColorDots Familiarization and Initial Tests

After an introduction to the ColorDots graphical password scheme, participants complete the registration process, practice using the ColorDots password scheme, and perform four tests involving alphanumeric and graphical passwords. During the registration process, participants enter their demographic data and create an alphanumeric and graphical password (the user-generated passwords), which are used throughout the study. Next, participants review instructions on authenticating with the ColorDots password scheme and practice authenticating until they successfully log in three times, assuring they are sufficiently prepared to complete the initial tests. Throughout the practice period, participants have access to the ColorDots instructions.

During initial testing, participants demonstrate their ability to authenticate using random and user-generated alphanumeric and graphical passwords. For each test, participants have three attempts to authenticate successfully with the given password type and method. If successful, the system records the password type and method, the number of attempts, the elapsed time of the successful attempt, and the total elapsed time, however, the system records only the password type and method if the participant is unable to authenticate within the allotted attempts.

4.2 Phase 2: Recall Tests

One week after completing the phase one tests, participants perform two recall tests involving the user-generated alphanumeric and graphical passwords. Participants perform the recall tests in the same manner as the initial tests, including the recording of the data. Participants whom fail to authenticate using their graphical password have an opportunity to review and practice the ColorDots authentication process using a random graphical password until they successfully log in one time. With their remediation completed, participants have another opportunity to authenticate using their graphical password. This second opportunity helps distinguish the participants who are unable to recall the ColorDots authentication process from those who are unable to recall their graphical password.

4.3 Phase 3: Shoulder-surfing Attack Test

Upon completion of the phase one tests, participants receive a collection of 10 screenshots of a simulated shoulder-surfing attack against a user authenticating with the ColorDots password scheme. Participants perform intersection analysis techniques on the collection of screenshots during the one-week period between Phases 1 and 2 in an attempt to identify the victim's graphical password. Participants receive an example of an intersection analysis algorithm to use; however, they are free to use any process they choose. Participants are free to analyze as many screenshots as necessary to reduce the number of candidate graphical password images to seven or less.

To prepare for the simulated shoulder-surfing attacks, modifications to the ColorDots graphical password scheme compensated for the inability of the screenshots to capture the level of detail possible with a recording device such as a camera phone. Although the ColorDots password scheme leverages indirect input to prevent shoulder-surfing attacks, the screenshots display only the ColorDots interface. Furthermore, the screenshots clearly display the alphanumeric password characters entered in the *Enter Password* field, which normally masks the characters. Finally, by disabling the feature responsible for randomly updating the ColorDots interface after entering each alphanumeric password character, each screenshot represents a complete graphical password login session. Ultimately, these modifications limit the overall complexity of the ColorDots graphical password scheme, allowing participants to focus on identifying the victim's graphical password rather than analyzing the ColorDots graphical password scheme.

To complete the test, participants select three graphical password images that, based on their analysis, represent the victim's graphical password. The system records the password images selected and whether the participant identified the victim's graphical password. To eliminate instances of guessing, participants who correctly identified the victim's graphical password must demonstrate the intersection analysis technique used.

Chapter 5

DATA COLLECTION

5.1 Subjects

The participants for the study are volunteers from a population consisting of University of North Florida (UNF) students, 18 years of age or older, enrolled in at least one course offered through the School of Computing. All volunteers are eligible regardless of gender, race or other demographic variables. The selecting of participants is in accordance with the Institutional Review Board (IRB), which is responsible for reviewing and approving all human subject studies performed at the University of North Florida. The IRB reviewed and approved the ColorDots study application as Exempt-Category 2 (IRB# 10-111).

5.2 Demographics

The collected demographic data includes each participant's age, gender, visual acuity, colorblindness, handedness, computer experience, and education level. A participant's age, gender or handedness may reduce his or her ability to learn and/or use the ColorDots graphical password scheme. Furthermore, due to its visual components, participants with less than optimal eyesight or colorblindness may be unable to

distinguish between the alphanumeric characters or perceive one or more of the colors present in the ColorDots interface. Finally, a participant's computer experience or education level may improve his or her ability to learn and/or use the ColorDots graphical password scheme.

5.3 Procedure

The study takes place over a two-week period. Participants complete Phase 1 during the first week and Phases 2 and 3 one week later. All volunteers may participate during the first week; however, only those participants who completed Phase 1 may complete Phases 2 and 3. The student identification scheme used at UNF (the "N" number) uniquely tracks each participant throughout the study. Upon completion of each phase, data collected on the participant's performance is stored in two locations – the ColorDots database and a participant-specific XML data file – to prevent data loss in the event of a system failure.

5.4 Apparatus

For the purpose of the study, the ColorDots graphical password scheme is implemented as a Windows application, using the Microsoft® Visual Studio® 2010 development software with the Visual C#® programming language and the .Net 3.5 Framework®, and Microsoft® SQL Server® 2008. The hardware for the study consists of 15 desktop computers running the Microsoft® Windows 7 ® operating system with the .Net 3.5

Framework®, and the database server running the Microsoft® Windows Server® 2008 operating system. The University of North Florida's School of Computing provided all of the computer hardware for this study.

The source code for the ColorDots application, the database design schema, the collected data, and all other documentation for this study is available on the accompanying compact disc.

Chapter 6

RESULTS OF DATA ANALYSIS

The Statistical Package for the Social Sciences (SPSS) software package, provided by the University of North Florida, was used to analyze the data collected during this study.

6.1 Demographics

Although 59 subjects participated in the study, analysis of the collected data did not occur for 20 participants. Of the participants not included in the analysis, 13 did not attend the second week of the study, four completed only one of the three training tests due to a software configuration error, and three had to evacuate the testing area due to a fire alarm in Building 15. This study used only the collected data of 39 participants.

Table 1 lists the collected participant demographics. All but two of the 18 participants, whose corrected visual acuity was 20/20, wore their corrective lenses throughout the study. All the participants used their mouse hand – the hand normally used to control the mouse.

Demographic	Female			Male
Gender (G)	7			32
	Minimum		Average	Maximum
Age (A)	18		25	64
Computer Experience (CE)	3		11	44
Education Level (EL)	14		16	19
	<= 20/20	Corr. to 20/20	> 20/20	Not Sure
Visual Acuity (VA)	14	18	3	4
Corrective Lenses (CL)	0	18	0	0
	Left			Right
Writing Handedness (WH)	5			34
Mouse Handedness (MH)	1			38

Table 1: Demographic Data

6.2 Correlations

Analysis performed on select demographic data and survey questions sought whether correlations existed between, or within, the analyzed data. Table 2 lists the results of this analysis. Each of the eight survey questions was in one of two categories. Questions 0, 3, 4, 5 and 7 referred to whether ColorDots was easy to learn and use. Questions 1, 2 and 6 referred to the perceived vulnerability of alphanumeric and graphical passwords to shoulder-surfing attacks. The survey questions are included in Appendix B of this paper.

Several significant correlations existed between the analyzed data.

- Gender and Question 6 (Q6) (sig. 0.045)
- Age and Education Level (sig. 0.006)
- Age and Computer Experience (sig. 0.000)
- Question 0 (Q0) and Question 3 (Q3) (sig. 0.011)
- Question 0 and Question 5 (Q5) (sig. 0.026)
- Question 2 (Q2) and Question 3 (sig. 0.009)
- Question 2 and Question 4 (Q4) (sig. 0.022)
- Question 2 and Question 6 (sig. 0.033)
- Question 3 and Question 4 (sig. 0.000)
- Question 3 and Question 5 (sig. 0.019)
- Question 4 and Question 5 (sig. 0.004)
- Question 4 and Question 7 (Q7) (sig. 0.035)

	A	EL	CE	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
G	.735	.261	.826	.704	.056	.797	.447	.470	.289	.045	.737
A		.006	.000	.416	.494	.545	.663	.964	.739	.444	.188
EL			.070	.368	.747	.086	.827	.472	.709	.128	.738
CE				.172	.223	.817	.799	.753	.361	.498	.218
Q0					.742	.377	.011	.085	.026	.856	.050
Q1						.728	.315	.510	.720	.456	.897
Q2							.009	.022	.582	.033	.937
Q3								.000	.019	.585	.075
Q4									.004	.755	.035
Q5										.260	.112
Q6											.395

Table 2: Demographic and Survey Question Correlations

6.3 Initial Tests

The initial tests measured the ability of participants to log into alphanumeric and graphical interfaces with random and user-generated passwords. The subsections below present the results of the initial tests. Throughout this section, the data analyzed represent successful attempts only.

The two-way repeated measures analysis of variation (ANOVA) performed on the collected data sought to discover significant differences between the alphanumeric and graphical interfaces, the random and user-generated passwords, and the interaction between the interfaces and passwords. The analyzed data defined two sections of results. The first section reported password input accuracy, which represented the pass rate – the number of participants who successfully logged in, and the attempt and interface refresh counts required to enter the password successfully. Higher pass rates, and lower attempt and refresh counts, equated to greater accuracy. The second section reported password completion time, which represented the time required to log in during the successful attempt and the total time required to log in, which includes the successful attempt and each, if any, of the failed attempts. Throughout the analysis, the differential main effect - the difference of effects of each of the independent variables on the dependent variables - was calculated, and a probability of less than 0.05 was used to determine whether the difference was statistically significant, and not simply due to chance.

6.3.1 Accuracy

Table 3 lists the pass rate, the average attempt count and the average refresh count when logging into the graphical interface. The alphanumeric interface with the user-generated password had the highest pass rate (100%), and the graphical interface with the random password had the lowest pass rate (82.05%). The alphanumeric interface with the user-generated password had the lowest attempt count (1.05), but the alphanumeric interface with the random password and the graphical interface with the user-generated password had 1.08 average attempts. The graphical interface with the random password had the lowest refresh count (0.03); however, the alphanumeric interface did not support the refresh functionality.

Interface	Pass Rate (%)	Average Attempt Count	Average Refresh Count
Alphanumeric Random	94.87	1.08	N/A
Alphanumeric User Gen.	100.00	1.05	N/A
Graphical Random	82.05	1.13	0.03
Graphical User Gen.	84.62	1.08	0.23

Table 3: Accuracy Components by Interface (Initial Tests)

6.3.1.1 Pass Rate

One of the most important considerations of a password scheme was whether users were likely to log in successfully and consistently. Since the analyzed data only represented successful attempts for both interfaces, no significant difference existed between the interface or password aspects with respect to pass rate.

6.3.1.2 Attempt Count

Another important consideration for a password scheme was the number of attempts users needed to log in successfully. Table 4 lists the ANOVA results for the analyzed attempt count data.

Source	Value	F	Sig.
Interface	.157	3.459	.076
Password	.030	.657	.426
Inf/Pwd	.006	.137	.714

Table 4: Analysis of Variance: Attempt Count (Initial Tests)

No significance existed for the interface or password aspects of the attempt count data.

6.3.1.3 Refresh Count

If a password scheme was too complex or confusing, users might need to refresh the interface multiple times to log in successfully. Table 5 lists the ANOVA results for the analyzed refresh count data. The alphanumeric interface did not support the refresh functionality.

Source	Value	F	Sig.
Interface	N/A	N/A	N/A
Password	.131	2.885	.103
Inf/Pwd	.131	2.885	.103

Table 5: Analysis of Variance: Refresh Count (Initial Tests)

No significance existed for the interface or password aspects of the refresh count data.

6.3.2 Completion Time

Table 6 lists the average attempt and login times recorded for the initial tests. The alphanumeric interface with the user-generated password had the lowest average attempt and login times (3.65 and 3.80 seconds, respectively), and the graphical interface with the user-generated password had the lowest average attempt and login times for the graphical interface (57.95 and 82.67 seconds, respectively).

Interface	Average Attempt Time (sec)	Average Login Time (sec)
Alphanumeric Random	5.99	7.01
Alphanumeric User Gen.	3.65	3.80
Graphical Random	69.83	92.35
Graphical User Gen.	57.95	82.67

Table 6: Completion Time Components by Interface (Initial Tests)

Although analyzed data considers the interface and password combinations separately, it is important to analyze the interaction between the two variables. The performed ANOVA evaluated the interactions between interfaces and password types with respect to the attempt and login time.

6.3.2.1 Attempt Time

How long it took users to complete a single attempt is important in determining whether users will choose to use a given password scheme. Table 7 lists the ANOVA results for the analyzed attempt time data.

Source	Value	F	Sig.
Interface	3.013	66.287	.000
Password	.117	2.572	.123
Inf/Pwd	.089	1.953	.176

Table 7: Analysis of Variance: Attempt Time (Initial Tests)

A significant differential main effect existed for the interface aspect (sig. 0.000), but no significance existed for the password or interaction aspects of the attempt time data.

6.3.2.2 Login Time

The total time required to log in determines whether users will likely choose to use a given password scheme. Table 8 lists the ANOVA results for the analyzed.

Source	Value	F	Sig.
Interface	.942	20.718	.000
Password	.053	1.168	.292
Inf/Pwd	.036	.800	.381

Table 8: Analysis of Variance: Login Time (Initial Tests)

A significant differential main effect existed for the interface aspect (sig. 0.000), but no significance existed for the password or interaction aspects of the login time data.

6.4 Recall Tests

The recall tests measured participants' ability to log into the alphanumeric and graphical interfaces, using the passwords created during initial testing, after one week of disuse. The subsections below present the results of the recall tests. Throughout this section, the data analyzed represent successful logins only.

The one-way repeated measures ANOVA performed on the collected data sought to discover significant differences between the alphanumeric and graphical interfaces. The analyzed data defined two sections of results. The first section reported password input accuracy, which represented the pass rate, and the attempt and interface refresh counts required to enter the password successfully. The second section reported password completion time. Throughout the analysis, the differential main effect - the difference of effects of each of the independent variables on the dependent variables - was calculated, and a probability of less than 0.05 was used to determine whether the difference was statistically significant, and not simply due to chance.

6.4.1 Accuracy

Table 9 lists the pass rate, the average attempt count and the average refresh count when logging into the graphical interface. Both interfaces achieved a pass rate of 94.87%. The alphanumeric interface had the lowest attempt count (1.05). The graphical interface with the user-generated password had the lowest refresh count (0.18); however, the alphanumeric interface did not support the refresh functionality.

Interface	Pass Rate (%)	Average Attempt Count	Average Refresh Count
Alphanumeric User Gen.	94.87	1.05	N/A
Graphical User Gen.	94.87	1.41	0.18

Table 9: Accuracy Components by Interface (Recall Tests)

The analyzed data did not consider the password type or the interaction between the two variables since the interfaces used the user-generated passwords only. The performed ANOVA evaluated the differences between the two interfaces using the user-generated password with respect to the pass rate, and attempt and refresh counts.

6.4.1.1 Pass Rate

One of the most important considerations of a password scheme was whether users were likely to log in successfully and consistently, after a period of disuse. Since the analyzed data only represented successful logins for both interfaces, no significant difference existed between the interface or password aspects with respect to pass rate.

6.4.1.2 Attempt Count

Another important consideration for a password scheme was the number of attempts users needed to log in successfully. Table 10 lists the ANOVA results for the analyzed attempt count data.

Source	Value	F	Sig.
Interface	.448	9.859	.005

Table 10: Analysis of Variance: Attempt Count (Recall Tests)

A significant differential main effect existed for the interface aspect (sig. 0.005) of the attempt count data.

6.4.1.3 Refresh Count

If a password scheme was too complex, or confusing, users might need to refresh the interface multiple times to log in successfully. The analyzed data did not consider the refresh count results since the alphanumeric interface did not support the refresh functionality.

6.4.2 Completion Time

Table 11 lists the average attempt and login times recorded for the recall tests. The alphanumeric interface had the lowest average attempt and login times (5.97 and 6.59

seconds, respectively), and the graphical interface had an average attempt and login times of 98.71 and 154.12 seconds, respectively.

Interface	Attempt Time (sec)	Login Time (sec)
Alphanumeric User Gen.	5.97	6.59
Graphical User Gen.	98.71	154.12

Table 11: Completion Time Components by Interface (Recall Tests)

The analyzed data did not consider the password type or the interaction between the two variables since the interfaces used the user-generated passwords only. The performed ANOVA evaluated the differences between the two interfaces using the user-generated password with respect to the attempt and login times.

6.4.2.1 Attempt Time

How long it took users to complete a single login attempt is important in determining whether users will choose to use a given password scheme. Table 12 lists the ANOVA results for the analyzed attempt time data.

Source	Value	F	Sig.
Interface	3.340	73.484	.000

Table 12: Analysis of Variance: Attempt Time (Recall Tests)

A significant differential main effect existed for the interface aspect (sig. 0.000) of the attempt time data.

6.4.2.2 Login Time

The total time required to log in determines whether users will likely choose to use a given password scheme. Table 13 lists the ANOVA results for the analyzed login time data.

Source	Value	F	Sig.
Interface	1.269	27.919	.000

Table 13: Analysis of Variance: Login Time (Recall Tests)

A significant differential main effect existed for the interface aspect (sig. 0.000) of the login time data.

6.5 ColorDots Training and Test Results Comparison

The data collected and analyzed, representing the three training sessions, and the initial and recall tests, determined whether the ColorDots graphical password scheme was easy to learn. Table 14 lists the average values of this data. A common pattern existed within the presented results. The initial test value was lower than the three training values, and the recall test value, while lower than the three training values, was higher than the initial test value. The only exception to this pattern occurred within the refresh count results where the recall test value was lower than the initial test value.

Source	Average Attempt Count	Average Attempt Time (sec)	Average Login Time (sec)	Average Refresh Count
Training 1	2.57	284.79	632.09	4.00
Training 2	1.83	119.62	858.47	4.44
Training 3	1.87	86.58	1019.05	4.44
Initial	1.26	66.82	100.867	0.39
Recall	1.57	104.63	179.08	0.30

Table 14: Graphical User-generated Password Results

Tables 15 and 16 list the ANOVA results for the initial and recall data, respectively.

Source	Average Attempt Count	Average Attempt Time (sec)	Average Login Time (sec)	Average Refresh Count
Training 1	.011	.000	.000	.059
Training 2	.039	.034	.000	.038
Training 3	.023	.053	.000	.034

Table 15: Graphical User-generated Password Analysis (Initial Tests)

Source	Average Attempt Count	Average Attempt Time (sec)	Average Login Time (sec)	Average Refresh Count
Training 1	.063	.001	.000	.067
Training 2	.208	.442	.000	.044
Training 3	.245	.129	.000	.041

Table 16: Graphical User-generated Password Analysis (Recall Tests)

A significant differential main effect existed for each of the comparisons between the trainings and the initial tests, except for the refresh count and attempt time for Training Sessions 1 and 3, respectively. A significant differential main effect existed for none of the comparisons between the trainings and the recall tests except for Training Session

1's attempt time, the login times for each of the training sessions, and the refresh counts for Training Sessions 2 and 3.

6.6 Shoulder-surfing Test

An easily compromised password scheme is useless regardless of whether it is easy to learn and use. The shoulder-surfing test sought to determine whether the ColorDots graphical password could be compromised using intersection analysis. Table 17 lists the results of the shoulder-surfing test. Of the 39 participants, only 3 (7.70%) successfully identified the graphical password images used.

Passed	Failed	Success Rate (%)
3	36	7.70

Table 17: Shoulder-surfing Test Outcome

The performed one-way repeated measure ANOVA compared the collected shoulder-surfing test to a set of all-pass values. Table 18 lists the ANOVA results for the analyzed shoulder-surfing data.

Source	Value	F	Sig.
STP	12.000	456.000	.000

Table 18: Analysis of Variance: Shoulder-surfing Test

A significant differential main effect existed for the shoulder-surfing data (sig. 0.000).

Chapter 7

DISCUSSION

Graphical password research began in the mid 1990's as an alternative to traditional alphanumeric passwords, not only to provide a mechanism for improved password recall, but also to prevent shoulder-surfing attacks. Researchers continued to study new ways to improve graphical password security; however, while many graphical password schemes were resistant to shoulder-surfing attacks involving direct observation or single-session recordings, most remained vulnerable to intersection analysis performed on multiple recordings. The current study presented a newly proposed graphical password scheme capable of preventing shoulder-surfing attacks, as well as resisting attempts to compromise a graphical password using intersection analysis. The findings suggested that the proposed graphical password scheme would be easy to learn and to use while preventing shoulder-surfing attacks and resisting intersection analysis.

7.1 Implications of Data Analysis

In reference to graphical passwords, a balance must exist between security and ease-of-use – attaining a greater level of security through a modest increase in password complexity. One of the primary questions answered in this study was whether users, accustomed to using alphanumeric passwords, would be willing to accept the additional

complexity inherent in a graphical password, in exchange for improved password security.

7.1.1 Accuracy

The first aspect of accuracy considered in the evaluation of the ColorDots graphical password scheme was whether users were as likely to log in successfully using a graphical password compared to an alphanumeric password, referred to as the pass rate. The analyzed pass rate data indicated a significant difference existed between the graphical and alphanumeric interfaces with respect to successful login attempts. The mean percentage of successful login attempts was 90.39% for all subjects, and the mean percentage of successful login attempts for the alphanumeric and graphical interfaces using user-generated passwords was 100% and 84.62%, respectively. These results are indicative of the relative experience subjects had with each interface. For the recall tests, the mean percentage of successful login attempts for both interfaces using user-generated passwords was 94.87% for all subjects. This outcome – a decreased pass rate for the alphanumeric interface and an increased pass rate for the graphical interface – supports previous research suggesting graphical passwords are easier to remember than alphanumeric passwords (Sobrado02). The results suggested users were as likely to recall their graphical password as their alphanumeric password; therefore, they are equally likely to log in successfully using either password type.

The second aspect of accuracy considered in the evaluation of the ColorDots graphical password scheme was whether users required a greater number of attempts to log in successfully using the graphical password compared to the alphanumeric password. The results indicated no significant difference existed in the number of attempts required to log into either interface. The mean percentage of correctness – the number of subjects who logged in with a single attempt compared to all the subjects – was 92.17%, and the mean percentage of correctness for the alphanumeric and graphical interfaces using user-generated passwords was 95.24% and 92.59%, respectively. These values are higher than, but consistent with, previous research (Wiedenbeck06). The recall tests indicated a significant difference existed between the alphanumeric and graphical interfaces with respect to attempt count. The mean percentage of correctness for all subjects, as well as the graphical interface using user-generated passwords, fell to 81.30% and 70.92%, respectively, while the alphanumeric interface using user-generated passwords remained unaffected. This disparity is likely due to subjects having more experience with alphanumeric passwords than graphical passwords.

The third aspect of accuracy considered in the evaluation of the ColorDots graphical password scheme was whether users required a greater number of refreshes to successfully log into the graphical interface. The results indicated no significant difference existed in the number of refreshes required to log into the graphical interface regardless of password familiarity. The mean percentage of refreshes – the total number of interface refreshes made compared to the total number of login attempts – for all subjects was 13.82%, and the mean percentage of refreshes for the random and user-

generated graphical passwords was 2.56% and 23.08%, respectively. The number of subjects that performed a refresh on the random and user-generated graphical interface was one and four, respectfully. The refresh count results for the recall tests, which involved only the user-generated graphical password, showed an improvement with a mean percentage of refreshes of 17.95%, and only two subjects performed a refresh. The results agreed with those published in previous research (De Luca10). The results indicated that the complexity of the graphical interface, and not the graphical password, was the primary factor affecting successful logins.

7.1.2 Completion Time

The first aspect of completion time considered in the evaluation of the ColorDots graphical password scheme was whether the attempt time – the time required to complete a successful login attempt – was likely to increase using a graphical password compared to a alphanumeric password. An analysis of the attempt times indicated a significant difference existed between the graphical and alphanumeric interfaces regarding attempt time. The mean attempt time for the alphanumeric and graphical interfaces using user-generated passwords was 3.65 seconds and 57.95 seconds, respectively. Due to the simplicity of alphanumeric passwords, these results were not surprising. For the recall tests, the mean attempt time was 5.97 seconds for the alphanumeric interface and 98.71 seconds for the graphical interface using user-generated passwords, which was an increase over initial test results of 63.56% and 70.34%, respectively. Again, these results were not surprising considering users had to

recall not only their graphical password, but how to log into the graphical interface, as well. Furthermore, the relative increase in attempt time during the recall tests for the interfaces was consistent – the graphical interface attempt time increased 10.67% more than the alphanumeric interface. This increase in the graphical interface attempt time compared to the alphanumeric interface is supported by previous research; furthermore, the results presented by Wiedenbeck, *et al,* were consistent with the results presented here (Wiedenbeck06).

The second aspect of completion time considered in the evaluation of the ColorDots graphical password scheme was whether the login time – the total time required to complete the login process, including the successful attempt and each, if any, of the failed log in attempts – was likely to increase using graphical passwords compared to alphanumeric passwords. An analysis of the login times indicated a significant difference existed between the graphical and alphanumeric interfaces with respect to login time. The mean login time for the alphanumeric and graphical interfaces using user-generated passwords was 3.80 seconds and 82.67 seconds, respectively. For the recall tests, the mean login time was 6.59 seconds for the alphanumeric interface and 154.12 seconds for the graphical interface using user-generated passwords, which was an increase of 73.42% and 86.43%, respectively, over initial test results. The relative increase in login time during the recall tests for the alphanumeric and graphical interfaces was less consistent than the attempt time results – the graphical interface's login time increased 17.72% more than the alphanumeric interface. Login time is composed of two factors – the number of attempts required to successfully login and

attempt time. Although a reduction in either of these factors should result in a decrease in login time, a decrease in attempt count would have the greatest affect.

7.1.3 Shoulder-surfing Prevention and Intersection Analysis Hindrance

The primary goal of the ColorDots graphical password scheme was to prevent shoulder-surfing attacks. The graphical interface design incorporated components – from the works of De Luca, Sobrado, and Wiedenbeck – that successfully deterred or prevented shoulder-surfing attacks (De Luca10, Sobrado02, Wiedenbeck06). One of the key features of the ColorDots graphical interface was the use of indirect input – entering password characters using the keyboard rather than the mouse, which was shown to prevent shoulder-surfing at ATMs (De Luca10). According to shoulder-surfing test surveys of the subjects that successfully determined the graphical password, a single screenshot of the graphical login process was insufficient to compromise the graphical password. Furthermore, the surveys showed subjects had to utilize intersection analysis on a number of screenshots before they could successfully compromise the graphical password. The surveys, as well as the previous works, showed that the ColorDots graphical interface was successful in preventing a shoulder-surfing attack involving the digital recording of a single login session. By extension, the ColorDots graphical interface was successful in preventing a shoulder-surfing attack involving the direct observation of a single login session. Finally, the shoulder-surfing test surveys showed that subjects needed to utilize intersection analysis on an average of seven screenshots before they could successfully compromise the graphical password, which required an

average of 1.67 hours. A minimum of five screenshots were needed to compromise the graphical password during the shoulder-surfing test, which was over twice the number needed to compromise the graphical PIN used in the study by De Luca, *et al.* (De Luca10). As configured for the shoulder-surfing test, the ColorDots graphical interface successfully resisted intersection analysis involving the digital recordings of multiple login sessions.

7.2 Conclusion

This study has shown the ColorDots graphical password scheme was easy to learn, easy to use, prevented shoulder-surfing, and resisted intersection analysis on digital recordings of multiple login sessions. Although the subjects participating in this study had limited exposure to the graphical interface, they were able to learn the graphical password scheme, and produced test results that rivaled those of the alphanumeric interface. Furthermore, while attempt and login times for the graphical interface (57.95 seconds and 82.67 seconds, respectively) were significantly longer than the alphanumeric interface (3.65 seconds and 3.80 seconds, respectively), the average attempt and login times for the 20 best results were 42.60 seconds and 44.49 seconds, respectively. With experience, ColorDots could be just as convenient to use as alphanumeric passwords, and could improve password security in public environments.

7.3 Suggestions for Further Research

The ColorDots graphical password scheme relies on a combination of colors and alphanumeric characters, which could make it difficult, if not impossible, for users with colorblindness or poor eyesight to use successfully. Would improvements to the ColorDots graphical password scheme make it accessible to a larger group of users? One improvement example would involve introducing shapes to represent each of the unique colors in the ColorDots interface to make it more accessible to users with color blindness. Another improvement example would involve temporarily increasing the font size of the alphanumeric characters used in the ColorDots interface to assist users with poor eyesight or those without access to their corrective lenses.

Allowing only UNF student volunteers, who were over the age of 18 and enrolled in at least one course offered by the School of Computing, limited the variety of computer users who participated in this study. It is important to test the ColorDots graphical password scheme using a larger variety of computer users. Does research involving a larger variety of computer users produce results consistent with those presented in this study? One research example would accept any UNF student volunteer over the age of 18 and enrolled in at least one course offered by the university. Another research example would accept any UNF student, faculty or staff volunteer over the age of 18. A final research example would accept any UNF student, faculty or staff volunteer over the age of 18, as well as members of his or her immediate family, within a larger age range.

To reduce the time and effort required for participants to complete the shoulder-surfing test conducted in this study, a number of modifications were made to the ColorDots graphical password scheme. Some of the modifications made include displaying the actual alphanumeric characters entered in the *Enter Password* field rather than masking the characters and disabling the feature responsible for randomly updating the ColorDots interface after each alphanumeric password character was entered. These modifications were necessary to capture the entire login process in a single screenshot, but they limited the complexity of the ColorDots graphical password scheme during this study; therefore, additional research should test the ColorDots graphical password scheme without these modifications. Does the complexity of the ColorDots graphical password scheme increase when these modifications are removed? Is a ColorDots graphical password less likely to be compromised by shoulder-surfing and intersection analysis when these modifications are removed?

7.4 Example Use of the ColorDots Graphical Interface

Although the ColorDots graphical password scheme was more complex and time consuming than traditional alphanumeric passwords, it was capable of providing increased password security in public environments, where shoulder-surfing attacks were more likely to occur. Positioning ColorDots as a secure alternative to alphanumeric passwords for users authenticating in public environments has great potential. For example, a link, which launches the ColorDots interface, could be

positioned on an alphanumeric password interface such as login screen of an operating system or website, like those used for social networking, online banking and online shopping websites. If a user needs to log in while visiting a public location such as a coffee shop or café, they could choose to use their ColorDots graphical password rather than their alphanumeric password.

REFERENCES

Print Publications:

[Blonder96]
Blonder, G., “Graphical Passwords,” United States Patent 5559961, (September, 1996).

[De Luca10]
De Luca, A., K. Hertzschuch, and H. Hussmann, "ColorPIN: Securing PIN Entry Through Indirect Input," 28th International Conference on Human Factors in Computing Systems, ACM, Atlanta, Georgia, 2010, pp. 1103-1106.

[Dumphy10]
Dumphy, P., A.P. Heiner, and N. Asokan, "A Closer Look at Recognition-based Graphical Passwords on Mobile Devices," Sixth Symposium on Usable Privacy and Security, ACM, Redmond, Washingston, 2010, pp. 1-12.

[Gao09]
Gao, H., X. Liu, R. Dai, S. Wang, and X. Chang, "2009." Fifth International Conference on Image and Graphics, IEEE Computer Society, Washington, DC, 2009, pp. 722-727.

[Lashkari09]
Lashkari, A. H., S. Farmand, O. B. Zakaria, and R. Saleh, "Shoulder Surfing Attack in Graphical Password Authentication," Journal of Computer Science and Information Security, IJCSIS 6, 2 (November, 2009), pp. 145-144.

[Man03]
Man, S., D. Hong, and M. Mathews, "A Shoulder-surfing Resistant Graphical Password Scheme – WIW," International Conference on Security and Management, CSREA Press, Las Vegas, Nevada, 2003, pp. 101-111.

[Moncur07]
Moncur, W. and G. Leplatre, "Pictures at the ATM: Exploring the Usability of Multiple Graphical Passwords," SIGCHI Conference on Human Factors in Computing Systems, ACM, San Jose, California, 2007, pp. 887-894.

[Shi09]
Shi, P., B. Zhu, and A. Youssef, "A PIN Entry Scheme Resistant to Recording-based Shoulder-surfing," Third International Conference on Emerging Security Information, Systems and Technologies, IEEE Computer Society, Washington, DC, 2009, pp. 237-241.

[Tari06]
Tari, F., A. A. Ozok, and S. H. Holden, "A Comparison of Perceived and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords," Second Symposium on Usable Privacy and Security (SOUPS), ACM, Pittsburgh, Pennsylvania, 2006, pp. 56-66.

[Wiedenbeck06]
Wiedenbeck, S., J. Waters, L. Sobrado, and J. Birget, "Design and Evaluation of a Shoulder-surfing Resistant Graphical Password Scheme," Working Conference on Advanced Visual Interfaces, ACM, Venezia, Italy, 2006, pp. 177-184.

Electronic Sources:

[FatCow11]
FatCow Web Hosting, “2400 Free Farm-Fresh Web Icons,” download from http://www.fatcow.com/free-icons, last revision 2011, last accessed March 11, 2012.

[Sobrado02]
Sobrado, L. and J. C. Birget, “Graphical Passwords,” The Rutgers Scholar 4 (September, 2002), http://RutgersScholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm, last accessed March 11, 2012.

APPENDIX A

ColorDots Testing Literature and Instructions

The following pages represent the literature and instructions presented to the subjects who completed the ColorDots research study. The literature provides general information about each stage of the research study, and the instructions describe the steps necessary to complete each stage of the research study.

Overview

Welcome to ColorDots - a graphical password authentication mechanism to prevent shoulder-surfing attacks and resist intersection analysis.

Advances in technology have resulted in an increase in the number of college students who use laptop computers, the number of public Wi-Fi hotspots available to college students - on and off campus, and the number of cell phones and other mobile devices that have built-in, high-resolution cameras. In this environment, a college student logging into a secure account in a public location such as the Thomas G. Carpenter library, Starbucks or Panera Bread is more likely to have their alphanumeric password stolen using shoulder-surfing.

Shoulder-surfing is a technique for acquiring a student's alphanumeric password in which the attacker observes, and memorizes, or records the victim's finger movements as they log into a secure computer account such as their UNF myWings, Facebook or bank accounts. The attacker simply needs to analyze the observed or recorded finger movements to determine the password entered by the victim, allowing the attacker to access the victim's account, compromising their security. Consequentially, since computer users commonly use the same password for multiple accounts, the attacker may also gain access to these accounts.

ColorDots is an alternative to traditional, alphanumeric passwords, designed to prevent shoulder-surfing attacks, protecting computer users while accessing their secure computer accounts while in public.

The purpose of this study is to determine whether ColorDots is a superior alternative to alphanumeric passwords compared to other popular graphical password mechanisms.

The ColorDots study is comprised of two sessions - today's session and a session one week from today. During these sessions, you will complete the following tasks:

1. Enter your demographic data.
2. Create your alphanumeric and graphical passwords.
3. Complete the ColorDots training.
4. Complete the initial tests using alphanumeric and graphical passwords.
5. Receive material to help prepare you for the shoulder-surfing test.
6. Complete the recall tests using alphanumeric and graphical passwords.
7. Select the victim's graphical password images you derived from the shoulder-surfing material provided in step 5.

During today's session, you will complete tasks 1 through 5.

Creating Test Passwords

You have reached the password creation stage of the study. You will create an alphanumeric password and a graphical password. Please take your time when creating your passwords because they will be used throughout the study; therefore, you will want to choose passwords that are easy for you to remember.

Creating Your Alphanumeric Password

Your alphanumeric password MUST BE EXACTLY 5 characters long; otherwise, you will receive an error. Enter your alphanumeric password in the "Your Text Password" field and click the "Set Password" button (Figure 1). Once you "set" your alphanumeric password, you will not be able to change it.

Figure 1

Creating Your Graphical Password

Your graphical password MUST consist of EXACTLY 3 images, and it cannot contain any duplicate images; otherwise, you will receive an error. To create your graphical password (Figure 2), select three images from the 25 available images. Each image you select (i.e., Football, Smiley Face, 8-Ball) will appear in the cells located in the "Your Password Images" section. Once you have selected three images for your graphical password, click the "Set Password" button (Figure 2). If you make a mistake or want to change the images you have selected, clicking the "Clear Password" button will remove all of the selected images from the "Your Password Images" section. You can change

your graphical password images at any time; however, you will be unable to change your graphical password after you click the "Click Here to Continue" button.

Figure 2

Training

The ColorDots environment (Figure 1) consists of the following items:

- 25 cells, in a 5x5 grid, each containing
  - A border color
  - An image
  - 5 letters, each with a unique color
- 5 Column Registration Dots (CRD)
- 5 Row Registration Dots (RRD)
- A password field and refresh button

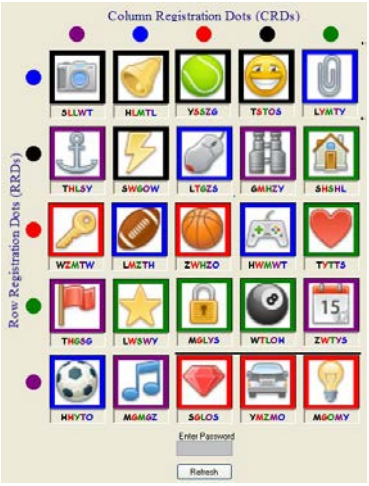

Figure 1

Entering Your Password in the ColorDots Interface

Step 1: Locate your password images in the ColorDots interface (Figure 3). For this example, assume you selected the password images displayed in Figure 2 for your graphical password (image order is not important).


Figure 2

Figure 3

Step 2: Visualize a triangle over the ColorDots grid that connects the three password images (Figure 4). In the next step, ignore the images NOT covered by the triangle (Figure 5).

Figure 4

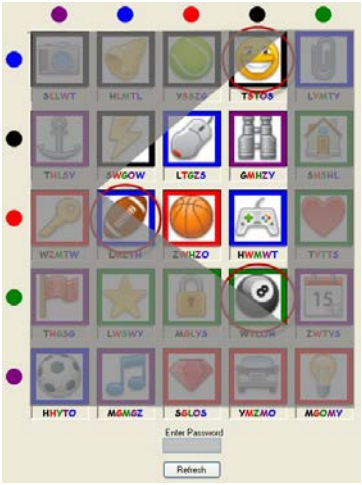

Figure 5

Step 3: Visually draw horizontal, vertical and diagonal lines from each password image into the triangle (Figure 6). Continue until one line from each password image intersects over a single image, which cannot be one of the original password images (Figure 7). The cell containing this image is the Initial Intersection Cell (C_0) (Figure 8).

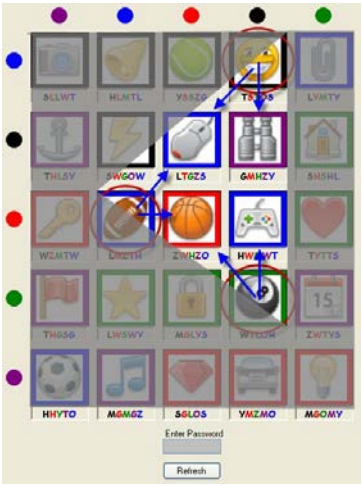

Figure 6

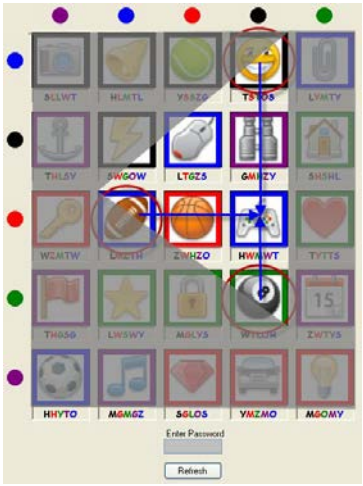

Figure 7

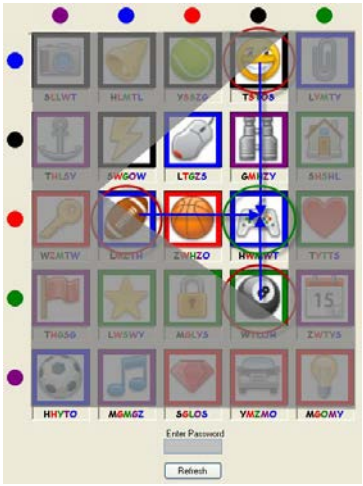

Figure 8

Step 4: Select the Row Registration Dot (RRD) that has the same color as the border of C_0 (Figure 9). Then, select the Column Registration Dot (CRD) that has the same color as the RRD of C_0 (Figure 10). Locate the cell that exists at the intersection of the selected RRD and CRD – this is the First Password Cell (C_1) (Figure 11). Finally, select the letter from C_1 that has the same color as the CRD of C_0, and enter this letter in the password field (Figure 12).

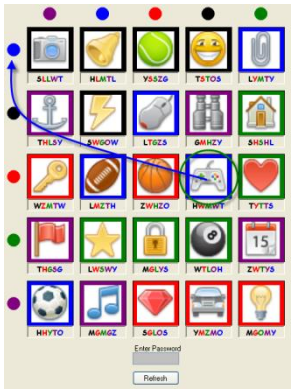

Figure 9

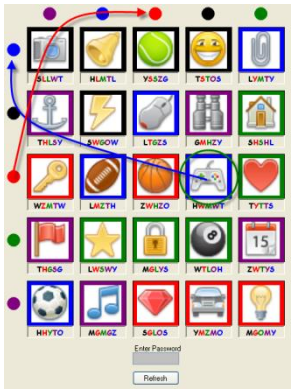

Figure 10

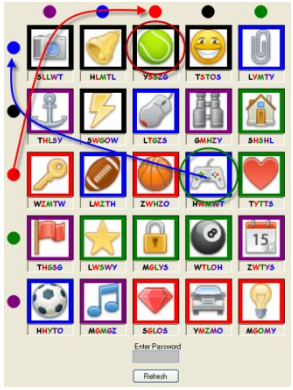

Figure 11

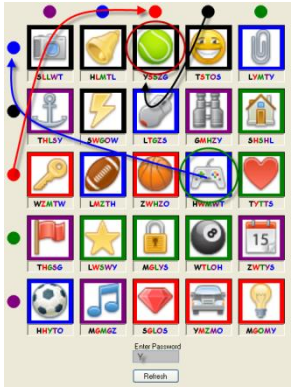

Figure 12

Step 5: Repeat step 4 to locate the Second Password Cell (C_2), select the appropriate letter from C_2, and enter the letter in the password field (Figure 13).

Figure 13

Figure 14

Step 6: Repeat step 4 to locate the Third Password Cell (C_3), select the appropriate letter from C_3, and enter the letter in the password field (Figure 14).

Step 7: Repeat step 4 to locate the Fourth Password Cell (C_4), select the appropriate letter from C_4, and enter the letter in the password field (Figure 15).

Step 8: Repeat step 4 to locate the Fifth Password Cell (C_5), select the appropriate letter from C_5, and enter the letter in the password field (Figure 16).

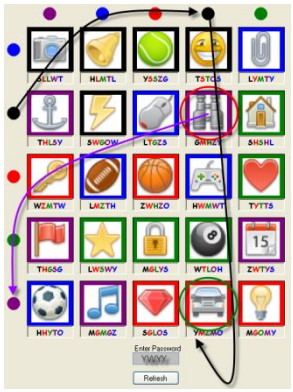

Figure 15

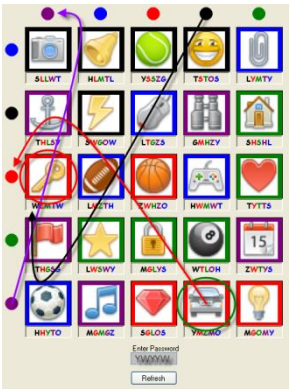

Figure 16

After you enter the fifth letter in the password field, validation of the entered password occurs automatically.

You will have access to these instructions throughout the training stage of this study to review. You should become comfortable with the ColorDots login process before continuing on to the training stage. If you have any questions, please contact the primary investigator.

Initial Test Phase

You are now prepared to take the four login tests, which will determine your performance when using alphanumeric and graphical passwords.

Alphanumeric Password Tests

The first two tests involve alphanumeric passwords. The first test requires you to log in using a randomly generated alphanumeric password. The system will prompt you with the random alphanumeric password to use prior to commencing the test (Figure 1).

Figure 1

When prompted for the random alphanumeric password (Figure 2), enter the password, and click the Submit button. Once the test is completed, you will continue on to the next test.

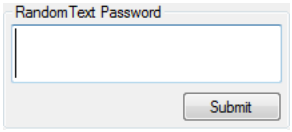

Figure 2

The second test requires you to log in using the alphanumeric password you created earlier. The system will prompt you with the alphanumeric password you created prior to commencing the test (Figure 3).

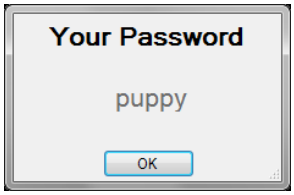

Figure 3

When prompted for your alphanumeric password (Figure 4), enter the password, and click the Submit button. Once the test is completed, you will continue on to the graphical password tests.

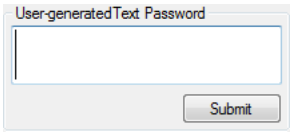

Figure 4

Graphical Password Tests

The last two tests involve graphical passwords. The third test requires you to log in using a randomly generated graphical password. The system will prompt you with the random graphical password to use prior to commencing the test (Figure 5).

Figure 5

When prompted with the ColorDots interface, enter the password using the ColorDots process. Once the test is completed, you will continue on to the last test.

The fourth test requires you to log in using the graphical password you created earlier. The system will prompt you with the graphical password you created prior to commencing the test (Figure 6).

Figure 6

When prompted with the ColorDots interface, enter the password using the ColorDots process. Once the test is completed, you will continue on to the next stage of the study.

Important Notes

- Each test will commence the moment you click the OK button on the password prompts (Figures 1, 3, 5, and 6); therefore, take as much time as necessary to commit each password to memory, but do not write the password down or make any notes to assist you as this may skew the test results.
- You have three attempts to enter a password correctly. After the third attempt, you will automatically continue on to the next test.

If you have any questions, contact the primary investigator - the individual responsible for this research study - now or prior to starting a test.

Recall Test Phase

You are about to take 2 final login tests, which will determine your ability to recall your alphanumeric and graphical passwords, as well as your ability to recall how to log in using the ColorDots process.

Alphanumeric Password Recall Test

During this test, you will log in using the alphanumeric password you created during the first session of the ColorDots study. The system will prompt you prior to commencing the test (Figure 1).

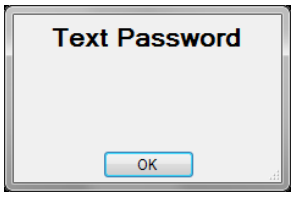

Figure 1

When prompted for your alphanumeric password (Figure 2), enter the password, and click the Submit button. Once the test is completed, you will continue on to the next test.

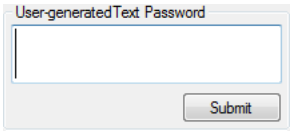

Figure 2

Graphical Password Recall Test

During the final test, you will log in using the graphical password you created during the first session of the ColorDots study. The system will prompt you prior to commencing the test (Figure 3).

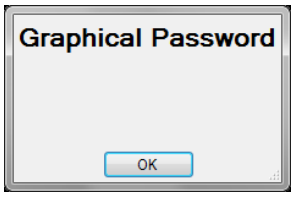

Figure 3

When prompted with the ColorDots interface, enter the password using the ColorDots process. Once the test is completed, you will continue on to the next stage of the study.

Important Notes

- Each test will commence the moment you click the OK button on the recall test prompts (Figures 1 and 3); therefore, do not click the OK button until you are prepared to take the test.
- You have three attempts to enter your alphanumeric password correctly. After the third attempt, you will automatically continue on to the graphical password recall test.
- You have three attempts to enter your graphical password correctly. After the third attempt, you will have an opportunity to practice using the ColorDots process. Once you complete the ColorDots refresher, you will have three additional attempts to enter your graphical password correctly. After the third attempt, you will automatically continue on to the next stage of the study.

If you have any questions, contact the primary investigator - the individual responsible for this research study - now or prior to starting a test.

Shoulder-surfing Test Phase

You have reached the final stage of this study. You will select the three graphical password images you identified from the 10 screenshots provided after completing session 1, last week. If necessary, you may review the shoulder-surfing material now by clicking on the following link: (link to shoulder-surfing review material).

Please take as much time as necessary to examine the provided material adequately and attempt to discover the three graphical password images used. To maintain the legitimacy of the shoulder-surfing test, you are asked to keep to yourself any notes used while reviewing the shoulder-surfing material and not to discuss your image choices with other participants.

Graphical Password Images Selection

You MUST select EXACTLY 3 images, and you cannot choose duplicate images. To enter your selected images (Figure 1), select three images from the 25 available images. Each image you select (i.e., Football, Smiley Face, 8-Ball) will appear in the cells located in the "Your Password Images" section. Once you select your three graphical password images, click the "Set Password" button (Figure 1). If you make a mistake or want to change the images you selected, clicking the "Clear Password" button will remove all of the selected images from the "Your Password Images" section. You can only enter your selected password images once; therefore, please verify the password images you selected before clicking the "Set Password" button.

Figure 1

Clicking the "Set Password" button records your selected password images. To maintain the legitimacy of the shoulder-surfing test, neither the primary investigator nor his adviser can confirm or deny the validity of your selected password images. After the study is completed, the primary investigator will reveal the correct graphical password images, as well as the participants who guessed correctly, in an email message to each participant.

If you have any questions about selecting your password images, contact the primary investigator.

How to Perform Intersection Analysis

This material will help you prepare for the shoulder-surfing test during session 2.

Please refer to the 10 screenshots below. Each screen shot shows the letters used to log into a computer system using the ColorDots system. Use your knowledge of the ColorDots login process to analyze the information available in each screenshot, and attempt to deduce the three password images used for the password. The ColorDots instructions are available for you to review.

The following steps provide one possible method to identify the user's password images using intersection analysis:

1. Using the letters in the *Enter Password* field, work the process backwards to discover the original intersection (C_0).
2. Create a list of all the images that can have a line drawn to C_0.
3. Create a list of all the possible 3-image combinations from these images.
4. Repeat steps 1 - 3 using two or more screenshots.
5. Compare each list of image combinations created in step 3 for each screenshot, and remove any combinations that do not appear for each screenshot.
6. Continue to reduce the number of image combinations (repeat steps 1 - 5 for each additional screenshot, if necessary) until you are left with 3 to 5 image combinations. One of these combinations is the graphical password.

Please note that it may be possible to perform this process until only one image combination exists.

Bring your final list of image combinations to session 2.

APPENDIX B

ColorDots Surveys

The following pages represent the surveys provided to the subjects whom completed the ColorDots research study. The surveys allow the subjects to provide information about their experience with ColorDots during the study, as well as their opinions about the ColorDots graphical password scheme.

ColorDots Research Study Survey

Thank you for participating in the ColorDots research study over the past two weeks. We would appreciate it if you would provide us with some feedback related to your experiences with the ColorDots graphical password tool. For the first eight statements, use the following scale:

1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree

0. ColorDots is easy to use.

1 2 3 4 5

1. Alphanumeric passwords are vulnerable to shoulder-surfing attack.

1 2 3 4 5

2. ColorDots graphical passwords are more secure than alphanumeric passwords.

1 2 3 4 5

3. I would use ColorDots as my primary login interface.

1 2 3 4 5

4. I would use ColorDots rather than an alphanumeric password to login in public.

1 2 3 4 5

5. The time required to log in using a ColorDots graphical password is acceptable.

1 2 3 4 5

6. ColorDots graphical passwords are vulnerable to shoulder-surfing attack.

1 2 3 4 5

7. The time required to log in using a ColorDots graphical password will improve as I become more comfortable and experienced with ColorDots.

1 2 3 4 5

8. Please provide any additional comments or feedback you may have regarding the ColorDots graphical password scheme and your experiences during this research study (use the back of this sheet, if necessary).

ColorDots Shoulder-surfing Survey

Congratulations! You correctly selected my password images during the shoulder-surfing stage of the ColorDots research study. I would appreciate it if you would answer the following questions concerning your experiences while deducing the correct password images.

0. How many screenshots were required to identify the password images?

1. How much time (in hours) was required to identify the password images?

2. Did you use a "brute force" methodology or did you follow a logical system such as the one provided with the shoulder-surfing material?

3. Did you identify any patterns that assisted in deducing the password images?

4. In your opinion, are there any aspects of the ColorDots graphical password scheme that make it vulnerable to shoulder-surfing attack?

5. In your opinion, are there any aspects of the ColorDots graphical password scheme that, if changed, could make ColorDots more secure?

6. Please provide any additional comments or feedback you may have regarding the ColorDots graphical password scheme that could make ColorDots more secure and/or less vulnerable to shoulder-surfing attack (use the back of this sheet, if necessary).

APPENDIX C

ColotDots Challenge-Response Authentication Example

The following represents an example challenge-response authentication process for the ColorDots graphical password scheme. The example lists the messages passed between the client and server, the order of communication and the values contained in each message. Although the ColorDots implementation used for testing did not fully implement this example, the implementation included most of the concepts.

Stage	Stage Name	Source	Destination	Values Passed
0	Announcement	Client	Server	Session, EventID, Client
1	Acknowledgement	Server	Client	Session, EventID, Port
2	Request	Client	Server	Session, EventID, Client, Username
3	Response	Server	Client	Session, EventID, Seed
4	Submission	Client	Server	Session, EventID, Password
5	Validation	Server	Client	Session, EventID, Result

Term	Definition
Session	Random, unique value representing the current login session
EventID	An integer value starting at 0, and incremented with each stage
Client	Unique value representing the client to prevent unauthorized access
Port	Server selected value used for each stage after Acknowledgement
Username	Uniquely identifies the user during the login attempt (encrypted value)
Seed	Random value that "seeds" the client and server (encrypted value)
Password	String of characters entered during the login attempt (encrypted value)
Result	Represents the pass/fail condition of the login attempt (encrypted value)

Stage	Procedure
	Note: For each stage, the Session and EventID values are validated
0	Client transmits the Announcement message with required values
1	Server validates Client, selects a port, transmits Acknowledgement message
2	Client reconnects to the server on new port, transmits Request message with encrypted Username value
3	Server validates Client and Username, selects Seed value, calculates encrypted password, transmits Response message with encrypted Seed value
4	Client displays interface using Seed value, accepts submitted password, transmits Submission message with encrypted Password value
5	Server compares encrypted password value, transmits Validation message

VITA

Jim Littleton has a Bachelor of Science in Computer and Information Sciences from the University of North Florida, May 2009, and expects to receive a Master of Science in Computer and Information Sciences from the University of North Florida, August 2012. Dr. Layne Wallace of the University of North Florida is serving as Jim's thesis adviser. During his undergraduate and graduate work, Jim worked as a software engineer for several notable Jacksonville-based companies such as Blue Cross and Blue Shield of Florida, Allstate, and Lender Processing Services.

During his graduate work, Jim received the Upsilon Pi Epsilon Award for Academic Excellence in 2011, and he has been a member of the Association for Computing Machinery (ACM) since 2010. He has served as an adjunct instructor for the School of Computing since January 2011. Jim's graduate work has specialized in software and interface design. He has programming experience in C, C++, C#, Java, and Visual Basic.

Jim leads an active lifestyle with hobbies ranging from flying airplanes as a General Aviation pilot to reading books from a variety of genres. He has been married for 19 years to his wonderful wife, Jeannie, and has a two-year-old Rottweiler, named Rayne.