Andrews University

Digital Commons @ Andrews University

Master's Theses

Graduate Research

2012

An Exploratory Investigation Into the Use of eAUP as an Alternative to Text-based Passwords

Joseph Ahor Abandoh-Sam
Andrews University

ABSTRACT

AN EXPLORATORY INVESTIGATION INTO THE USE OF eAUP AS AN ALTERNATIVE TO TEXT-BASED PASSWORDS

by

Joseph Ahor Abandoh-Sam

Chair: Roy Villafane

ABSTRACT OF GRADUATE STUDENT RESEARCH

Thesis

Andrews University

College of Arts and Sciences

Title: AN EXPLORATORY INVESTIGATION INTO THE USE OF eAUP AS AN ALTERNATIVE TO TEXT-BASED PASSWORDS

Name of researcher: Joseph Ahor Abandoh-Sam

Name and degree of faculty chair: Roy Villafane, Ph.D.

Date completed: July 2012

Security is one of the major concerns of every industry in the world today. One of the best ways of hacking into a computer system is brute forcing. And with the increase in computing, brute forcing has become faster and easy to do.

Text-based passwords are still the most popular and most commonly used form of authentication even though the requirements for a good password are still increasing. Research has shown that the best text-based passwords are the random ones that have no sequence or pattern to them. But this also makes it difficult to remember. Well-

documented research has shown that it is easier to remember an image than words, hence the adage “A picture is worth a thousand words.”

Even though there are good policies for text-based passwords, the unpredictability of users’ attitudes and behavior has most of the time rendered these policies inefficient. The common trade-off for the complexity of text-based passwords is recallability. Most users would prefer to use a password they can easily remember than a complex one that they can easily forget.

One of the proposed alternatives to text-based passwords is graphical passwords. There are several schemes that have been proposed but are still unpopular.

This thesis investigated one of these schemes that are used on mobile devices to determine whether it can be used as an alternative to text-based passwords. Also this research proposes ways to improve this scheme and options of bringing it at par with the current minimum requirements of a good text-based password.

Andrews University

College of Arts and Sciences

AN EXPLORATORY INVESTIGATION INTO THE USE OF eAUP AS AN ALTERNATIVE TO TEXT-BASED PASSWORDS

A Thesis

Presented in Partial Fulfillment

of the Requirements for the Degree

Master of Science

by

Joseph Ahor Abandoh-Sam

2012

AN EXPLORATORY INVESTIGATION INTO THE USE OF eAUP AS AN ALTERNATIVE TO TEXT-BASED PASSWORDS

A thesis
presented in partial fulfillment
of the requirements for the degree
Master of Science

by

Joseph Ahor Abandoh-Sam

APPROVAL BY THE COMMITTEE:

Roy Villafane, Ph.D., Chair

Stephen Thorman, Ph.D.

William Wolfer, M.S.

Date approved

TABLE OF CONTENTS

Appendix

LIST OF FIGURES

ACKNOWLEDGMENTS

I wish to thank God for His guidance and protection and to also express sincere appreciation to Dr. Roy Villafane and Mr. Bill Wolfer for their invaluable assistance in the preparation of this manuscript. In addition, special thanks to family and friends and other faculties whose prayers and support helped encourage me to complete this research.

CHAPTER 1

INTRODUCTION

The number one concern of every organization in the world is the security of its assets. Depending on the value of the asset, the security level can range from a password to encryption keys, biometric scanners, and so on. “The number of mobile workers is rapidly increasing and most mobile workers will be relying on their smart phones in the course of their work” (Landman, 2010, p. 145). This can be true for other mobile devices such as laptops, tablets, etc.

In a centralized system, intrusion and unauthorized access to the system is easily detectible since there is constant monitoring of the system by the information technology personnel. The same cannot hold true for most personal computer systems (desktops, laptops, tablets, smart phones, etc.).

According to the research of Shay et al. (2010) on the habit and attitudes of computer users, “nearly 80% of users based their password on a word or name, with special characters added to the beginning or end” (p. 12) despite the implementation of a new policy to check for dictionary words. Hence there has been a lot of research into the use of graphical-based passwords. One such password is the Android Unlocking Pattern (AUP), which instead of entering a numeric PIN to unlock the screen, a user must connect several dots to unlock their android mobile device.

Statement of the Problem

The fundamental problem of every security personnel is how to authenticate the users of the systems securely and conveniently (Shay et al., 2010). “A common problem with password-based methods is the low entropy available in user-chosen passwords, which may be used by an attacker to mount password-guessing attacks” (Halevi & Krawczyk, 1999, p. 231). Due to the unpredictability of user-chosen passwords, to determine the entropy of a user-chosen password is challenging, but the entropy of a text-based password can be calculated assuming the characters were randomly generated.

> In recent years, a number of devices and techniques have been proposed including smart cards, RFID cards, USB tokens, and graphical passwords to make authentication more usable, convenient, and secure. While each of these technologies has its advantages and may be well suited for use in a specific environment or for a specific application, text-based

> passwords remain the most commonly used authentication mechanism. This is in part because text-based passwords require no special hardware and are easy for end users to input and for system developers to implement. (Shay et al., 2010, p. 1)

Text-based passwords are still the most commonly used method of authentication. “To combat both the inherent and user-induced weaknesses of text-based passwords, administrators and organizations typically institute a series of rules—a password policy—to which users must adhere when choosing a password” (Shay et al., 2010, p. 1) Even with the implementation of policies to make text-based passwords more secure, they can still be unpredictable because the behavior of users is still unpredictable.

> Without feedback from security experts, users created their own rules on password design that were often anything but secure. Dictionary words and names are the most vulnerable forms of passwords, but many users do not understand how password cracking works. (Adams & Sasse, 1999, p. 42)

To counteract this issue, most security systems employ persuasive methods to guide the users in the choice of their passwords. One of these methods is the establishment of rules that predict the strength of the password.

Some users also result to writing down their passwords or choose very simple passwords that would be more easily broken due to frequent password expirations as reported by Adams and Sasse (1999).

According to several studies in learning in education, combining a visual aid with the human body’s motor sensors (doing an activity) promotes learning and better recall for students. Hence there has been a lot of research into the use of graphical passwords as an alternative to text-based passwords. Graphical passwords can provide the complexity needed for passwords and yet can also be easily recalled.

Hypothesis

Van Oorschot and Thorpe (2008), in their investigation of the Draw-A-Secret (DAS) graphical password scheme, defined the complexity of a DAS based on the password length, number of components, and symmetry. DAS is similar to AUP in that they both allow the user free reign to determine his or her authentication pattern. Hence the objects or pattern of a user’s AUP is not known until drawn.

Unlike DAS (which uses a canvas), an AUP uses a grid of dots that need to be connected. But by increasing the size of the grid, can an expanded AUP (eAUP) provide better security than a text-based password? Van Oorschot and Thorpe (2008) suggested a method to predict and model a number of classes for systems where passwords are created solely from a user’s memory. They hypothesize that these classes define weak password subspaces suitable for an attack dictionary. “For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall” (Van Oorschot & Thorpe, 2008, p. 1).

The research of Van Oorschot and Thorpe (2008) was based on the Draw-A-Secret (DAS) scheme proposed by Jermyn, Mayer, Monrose, Reiter, and Rubin (1999). “We introduce a set of user-drawn graphical password complexity properties, including: password length, number of components, and symmetry. We model what we conjecture to be classes of higher-probability user-drawn graphical passwords based on these complexity properties” (Van Oorschot & Thorpe, 2008, p. 3).

Hence, a hypothesis can be constructed as follows: By modifying the parameters of an AUP and a method to determine familiar or common patterns, an eAUP scheme can provide the same level of security as a text-based password.

Research Question

From the hypothesis, the research question can be constructed as: Can an eAUP provide the same level of security as a text-based password?

Purpose of the Study

In order for graphical passwords to replace text-based passwords, they need to offer the same level of, if not more, complexity and difficulty in hacking it. Increasing the complexity of the graphical password will make it difficult to crack. Also a predictive model will help prevent the use of familiar patterns that can easily be hacked. Furthermore, increasing the parameters of the AUP scheme can provide the same level of security as a text-based password scheme.

Hence, the main purpose of this research was to change the parameters of an AUP (to create eAUP) to increase its complexity. This was done to determine whether it was equal or better than a text-based password. Additionally, the study proposes a theoretical model for determining common patterns such as spirals, zigzags, polygon, squares, and rectangles in a constructed pattern using the geometric properties of these shapes.

Significance and Justification of the Study

The complexity of text-based password requirements has grown, making it increasingly more difficult for users to remember. Several studies have shown that although users are aware of the security concerns, their habits can still make a systems security vulnerable.

According to the studies of McDowell, Rafail, and Herman (2009) and Shay et al. (2010), the major trade-offs of password complexity are easy recall, so users tend to modify old passwords to create new ones, write them down, or share their passwords over time.

Bragdon et al. (2010) found that users of the game “Gesture Play” had an improved short-term recall. User-drawn graphical passwords combine two important qualities for recall: motor sensory and visual sensory. This research is a contribution to the ongoing research of graphical passwords, which can be a suitable alternative to graphical-based passwords.

Limitation and Delimitations

Due to time constraints, this research is limited to proposing a theoretical model for detecting familiar patterns such as squares, rectangles, spirals, and zigzags. This is to prove that a model can be constructed for user-pattern choices using the geometric properties of familiar patterns. Correspondingly, in calculating the Space, Entropy, and minimum Length of a pattern for an eAUP scheme, known functions with slight modifications will be used to accommodate the structure of an eAUP scheme.

This research can be expanded to include a brute-force test of the eAUP as well as the construction of a working model of the eAUP to tests its usability in real time. Also, the modified equations are prone to errors, and further studies may be required to prove their accuracy.

Furthermore, this research can also be expanded to cover the detection of other common and familiar patterns such as regular polygons, arcs, etc.

Assumptions

The following assumptions were made in the calculation of the entropy of an eAUP grid:

1. A dot cannot be used more than once.

2. A stroke follows an order in the direction of the stroke. Hence dots D_1 follows D_2 in an ordered system.

3. Let N represent the space (the number of all possible passwords of length not greater than a specified character length in a symbols set).

4. For an eAUP, grid size represents the total number of dots (that is, the horizontal length of the grid X the vertical length of the grid) divided by the length of a stroke (Van Oorschot & Thorpe, 2008).

5. Let H be the entropy of a character of a random password.

Definition of Terms

The following terminologies are used in this context in the research:

1*. Space* refers to the maximum possible dots that are available in an eAUB.

2. *Entropy* is the measure of uncertainty of a random dot selected in the grid.

3. *Dot* is a spot in the grid.

4. *Stroke* is a straight line connecting two or more dots in the grid.

Validity

“The main motivation for graphical passwords is the hypothesis that people are better at remembering images than artificial words” (Dirik, Memon, & Birget, 2007, p. 20). The formula and functions that were used in collecting data are a modification of similar ones that were used in the calculations of similar values in previous research into other graphical passwords.

The formula and functions used in this research are similar to the ones used by Barker and Kelsey (2012), Chiasson, Stobert, Forget, Biddle, and Van Oorschot (2012), Passfaces Corporation (2012), Esteban, Morales, Pardo, and Menendez (1994), Halevi and Krawczyk (1999), and Komanduri and Hutchings (2008) in their research. Even though DAS allows the construction of discontinued shapes, the same functions and formula can be applied to eAUPs.

Organization

This thesis is organized into four chapters. Chapter 1 is the general introduction to the research. Chapter 2 is the literature review. Chapter 3 describes the variables and methodology used to collect the data, and Chapter 4 presents the analysis and discussion of the data.

CHAPTER 2

LITERATURE REVIEW

Introduction

Technology has turned the world into a global village. Increasingly, research is being made into discovering ways to improve the global communication. After a few clicks of a mouse, one can access information that decades ago would have required an individual days of rummaging through library books to find. However, advancement in technology has created several issues in security for experts. One of the major concerns is the weak link of the user to a system. According to most researchers, human beings in a system have been recognized as the weakest link in computer systems security (Adams & Sasse, 1999; Sasse, Brostoff, & Weirich, 2001).

According to Vidyaraman, Chandrasekaran, and Upadhyaya (2008), there are two categories of legitimate users dubbed “the enemy within.” For the first category, although they do not have any malicious intent, their actions cause security breaches, whereas for the second category, dubbed the “saboteur,” they are legitimate users with malicious intent. Even though they possess legal credentials, their goal is to disrupt the system such as sabotaging, stealing information, etc.

According to Shay et al. (2010), in their research into “user attitude and behavior towards stronger password requirements,” users’ attitude and behavior compromise the relevance of the security policies. For this reason, lots of research has been done into how to reduce the effects of the “weakest link” in security systems, the user.

Several research areas that studied solving this issue include but are not limited to implementing stricter security policies, increasing the complexity of the existing security protocols, and discovering alternative methods for security.

One of the proposed alternative methods is the use of graphics-based passwords as substitutes for the traditional username and text-based password combination. “Visual objects seem to offer a much larger set of usable passwords” (Dirik et al., 2007, p. 20). According to Zhang, Monrose, and Reiter (2010), users tend to vary their passwords by changing a few characters from the old password or use the name of a familiar object such as highschool name, hometown name, or the name of someone close to them such as spouse, children, parents, and so on.

Purpose

The purpose of this literature review is to explore other research into graphics-based passwords and how they compare with a traditional username and alphanumeric password combinations in computer security. There is a lot of research in the recall ability of graphic-based passwords versus alphanumeric passwords, as well as the usability of graphical-based passwords.

This research compares pattern-drawn graphic passwords similarly found on the android mobile devices with alphanumeric passwords. The main focus of this will be to propose ways of increasing the strength of a user-drawn pattern password based on the space, entropy, and minimum length of pattern-drawn passwords. Also, this research proposes ways of eliminating easily guessable passwords.

Source and Search Criteria

The sources for previous work and research related to this research were selected from a comprehensive search in several journals and article databases. The online journals that were used include ACM Digital Library, IEEE

Publications and Journals, EBESCOhost, ProQuest, and Wiley Online Library. The “Google” search engine was also used to expansively acquire tributary sources for amplification of the lexicons used in the reviewed literature.

The following terms were used fundamentally to search for articles and other publications on the subject of this research.

Password strength: According to McDowell et al. (2009), a password strength is a password’s degree of resistivity to guessing and brute-force attacks. In this research, password strength is a function of its space, density, and randomness.

Graphical passwords: A graphical password is a password that requires the user to remember an image, picture, or pattern-based information instead of text-based information (Van Oorschot & Thorpe, 2008). For the purpose of this research, graphical-based passwords is used to refer to user-drawn passwords (UD) (Van Oorschot & Thorpe, 2008), picture passwords (Komanduri & Hutchings, 2008), click-based graphical passwords (CBG) (Forget, Chiasson, & Biddle, 2007, 2010), persuasive cued click-points (PCCP) (Spitzer, Singh, & Schweitzer, 2010), cued gaze-points (CGP) (Forget et al., 2010), and pass-point password schemes (Dirik et al., 2007).

Authentication: According to the RSA information security glossary, authentication is a procedure where a person or a computer program verifies their identity in order to access information (Czekalski, 2012).

Text, text-based, and alphanumeric passwords: Represent passwords that use ASCII and other forms of characters, which include but are not limited to alphabets, numbers, and other symbols.

Users' Behavior and Attitude Toward Passwords

One of the major problems in computer security is "how to authenticate a user securely and conveniently" (Shay et al., 2010, p. 1). "Authentication is typically the first step toward confirming that a user is authorized to perform a requested action, be it retrieving email, withdrawing money from an ATM, or issuing commands to a power-distribution grid" (Shay et al., 2010, p. 1). Even though text-based passwords still remain the most commonly used method of authentication, user behavior and attitude make it unpredictable.

Shay et al. (2010) conducted research on the attitude of users towards new password policies at Carnegie Mellon University (CMU). They analyzed the difference between the old and new policies and also the attitude of the users to these new policies. Their study provided new insights into the behavior and attitudes of users towards strict password policies. These insights are outlined as follows:

1. Users find new requirements annoying but believe they provide security.

2. Some users struggle to comply with new password requirements.

3. Users are more likely to share and reuse their passwords than to write them down.

4. Users tend to modify old passwords to create new ones.

5. Users are more likely to share their passwords over time (about 25% had shared their passwords with at least one person).

6. Use of dictionary words and names are still the most common strategies to create passwords (about 80% of the participants had passwords based on names and dictionary words).

In concluding, they realized that the results were inconsistent with some of the assumptions of the National Institute of Standards and Technology (NIST). “NIST bases its per-password entropy estimates on several assumptions that are inconsistent with our findings” (Shay et al., 2010, p. 12).

However, if their population sample was from an academic demography, it raises the question of whether it is the same demography that NIST based their assumptions on.

According to Sasse et al. (2001), even though text passwords are required to be memorable and secured, “most passwords are either memorable but easy-to-guess or secure but difficult-to-remember” (Stobert, 2010, p. 4304). Usually users tend to choose between memorability and security. For example, it will be easier for a user to modify an existing password to make a new one than to create a new password from scratch, since it will be easy for the user to remember a slightly modified password than a newly created one.

“Two common techniques for helping people to remember complex passwords are to use pass phrases and substitutions” (Holt, 2011, p. 37). For example, a pass phrase such as “My birthday is first January 2001” can be represented as a password as “Mbdi1j01,” and in using substitutions, a user can replace the letters of a word with the letters that appear above it on the keyboard. For example, “Friday” can be represented as “t49rw7.” However, users tend to use the same password for several sites (Sasse et al., 2001), hence once the password is determined for one site, it may be applicable to several other sites.

Background of Graphical Passwords

Several graphical password schemes have been produced on the premise that an image is easier to remember than text-based passwords (Dunphy & Yan, 2007). Dirik et al. (2007) classify password systems as: (a) Recognition-based systems (RBS); (b) Cued recall-based systems (CRBS); and (c) Pure recall-based systems (PRBS).

Recognition-Based Systems

In this type of password system, a user must recognize a set of previously selected set of images, symbol, or icons from a large collection for authentication (Dirik et al., 2007). An example of an RBS scheme is Passfaces (a commercial scheme).

Passfaces is a scheme where user authentication is done by selecting a set of pre-selected facial images out of a stock of images (Dunphy, Heiner, & Asokan, 2010). Research into a mobile implementation of this scheme used varying entropies to determine the user’s attitudes towards this type of scheme on mobile devices.

Though their survey was short-termed (they recommended a longitudinal study), it provided helpful insight into real-world performance levels expected of recognition-based schemes. Although their method of calculating the entropy was not stated, it is assumed that they used Shannon’s method (Shannon, 2001). Also, their observations showed that the choice of facial images was influenced by the ethnicity of the user.

Cued Recall-Based Systems

Human recall of long-term memory is usually tied to an activity or event. Hence, capturing these events in the form of pictures or other visual form can be used as a roadmap to recalling otherwise “lost memory” (Gyorbiro, Larkin, & Cohen, 2010a, 2010b) CRBS passwords employ the use of images to aid recall of passwords. To authenticate, a user selects several points on an image or a series of images as a password (Chiasson, Forget, Stobert, Van Oorschot, & Biddle, 2009; Chiasson et al., 2012; Stobert, 2010a; Stobert, Forget, Chiasson, Van Oorschot, & Biddle, 2010b). A sample password scheme that uses CRBS is a passpoint password.

“A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen” (Dirik et al., 2007, p. 20). Another example is the “persuasive cued click-points” (PCCP) (Chiasson, Forget, Biddle, & Van Oorschot, 2008; Chiasson et al., 2012) which is similar to the passpoints.

> Persuasive Cued Click-Points (PCCP) is a click-based graphical password system in which a user is presented with a number of images in sequence, and is asked to choose one click-point on each image. The first image is assigned by the system, but each subsequent image in the sequence is determined by the user’s previous click. This means that clicking in different places on an earlier image leads the user to different next images. (Stobert, 2010, p. 4304)

Calculating the theoretical space of a PCCP, according to Stobert (2010, p. 4304), was based on the following formula: w is the width of the image, h is the height of the image, t is the size of the tolerance square, and c is the number of click points.

Pure Recall-Based Systems

A PRB can be defined as a password system where “a user is asked to reproduce something (e.g. a drawing or a sequence of actions) that he or she created or selected earlier during the registration stage” (Suo, Zhu, & Owen, 2006, p. 742). The main reason behind PRB systems, according to Jermyn et al. (1999), is that they “have shown that there is a substantial improvement of performance in recall and recognition with pictorial representations of to-be-remembered material than for verbal representations" (p. 3).

The most popular PRB system password scheme is the Draw-A-Secret (DAS) scheme. The DAS uses a canvas that has a grid of cells. Each cell has a coordinate (h,w) where h is the horizontal value and w is the vertical value. A password of the DAS consists of the cells that an image or a drawing passes through (Jermyn et al., 1999).

According to Jermyn et al. (1999), two factors that make DAS strong are: (a) Users do not pick passwords uniformly, and (b) An attack does not have a significant knowledge of the user's password distribution.

AUP is similar to DAS but, unlike DAS, cell or dot (in AUP) repetition is not possible. Oorschot and Thorpe (2008) contributed to this password scheme by introducing a model for predicting weak passwords. In computing the space of a DAS, Jermyn et al. (1999) assumed that passwords of a length greater than a certain length had a probability of zero.

Definition of Variables

Password Space

A password space may be described as the set of all possible character combinations as a function of the number of characters and the maximum length of the password (Jermyn et al., 1999; Narayanan & Shmatikov, 2005; Van Oorschot & Thorpe, 2008). The size of the password space has an upper bound and a lower bound. The upper bound size is the number of all possible characters. The calculation of the lower bound size varies depending on the type of password scheme.

For RBS passwords, Suo et al. (2006) computed the password space as:

$$\sum_{l=1}^{m} \frac{(n+l-1)!}{l!\,(n-1)!} \quad - \quad (1)$$

where n is the total number of pictures, l is the password length, and m is the maximum password length, assuming that a picture can be selected more than once.

For PRBS passwords, Suo et al. (2006) proposed that if the drawing is allowed to pass through multiple units or pixels, then the maximum password space can be computed as:

$$\sum_{l=1}^{m} n^{l} \quad - \quad (2)$$

However if the scheme does not allow the drawing to pass through the same pixel or unit multiple times, then the minimum space is computed as:

$$\sum_{l=1}^{n} \frac{n!}{(n-l)!} \quad - \quad (3)$$

Minimum Length

The minimum length of a password for a password scheme is the minimum number of character sequence needed to achieve a given password strength (entropy) in bits (Chiasson et al., 2008; Dunphy & Yan, 2007; Forget et al., 2010; Jermyn et al., 1999; Komanduri & Hutchings, 2008; Yokota, Ootsu, & Baba, 2007).

Using the information-theory entropy based on Shannon's entropy (Shannon, 2001), the minimum length can be computed as follows:

$$L = \frac{H}{\log_2 N} \quad - \quad (4)$$

where H is the desired entropy and N the number of possible passwords ("Password Strength," 2012).

The minimum length of a password is needed to determine the least number of characters in a password needed to achieve certain strength.

Entropy

> The entropy is a statistical parameter which measures in a certain sense, how much information is produced on the average for each letter of a text in the language. If the language is translated into binary

> digits (0 or 1) in the most efficient way, the entropy H is the average number of binary digits required per letter of the original language. (Burr, Dodson, & Polk, 2006, p. 46)

The National Institute of Standards and Technology also defines entropy as a degree of the disorder, uncertainty, or unpredictability in a closed system (Barker & Kelsey, 2012; Burr et al., 2006; Komanduri & Hutchings, 2008; Milton & Kennedy, 2010; Wong & Chen, 2006; Zhang et al., 2010)

Information entropy, usually used as a measure (in bits) for the strength of a password, is a concept from information theory which implies that for a password of strength 64 bits will require 2^{64} attempts during a brute force search to exhaust all possibilities ("Password Strength," n.d.).

Shannon (2001) describes entropy as a measure of uncertainty and hence proposed that:

$$H(N) = -\sum_{i=1}^{N} p_i \log p_i \quad - \qquad (5)$$

where p_i is the probability of a sequence occurring in a space. Milton and Kennedy (2010) suggested that the frequency f_a of a symbol *a* in an arbitrary list of N symbols will vary and hence *pa* = ${}^{f_a}\!/_{N}$.

CHAPTER 3

METHODOLOGY AND INSTRUMENTATION

Introduction

This research and its instruments are designed to measure the strength of an eAUP password based on the space, minimum length, and entropy. This method helped me answer the question: Does an eAUP have the comparable strength and complexity of a text-based password?

Type of Research

The methodology for this study is a comparative experimental quantitative research design. This method was selected because in order to determine what parameters of an eAUP meet the minimum strength of the current text-based password standard, the minimum length, the space, entropy, and strength of the eAUP need to be computed. The purpose of this research design was to enable me to compute the entropy, space, and minimum length of all possible eAUPs.

This design was also selected because of its usefulness and versatility in aiding me to manipulate variables to achieve the desired results.

Hypothesis

There are three dependent variables and one independent variable, which is the screen resolution. Hence the null hypothesis is identified as follows:

H_0: The *space N, entropy H, and minimum Length* L_{min} of a text-based password are equal to the *space N, entropy H, and minimum Length* L_{min} of any eAUP.

Mathematically,

$N_{text} = \forall N_{eAUP}$ and $H_{text} = \forall H_{eAUP}$ and $L_{text} = \forall L_{eAUP}$

The null hypothesis will be rejected if the level of significance is below 0.05.

Definitions of Functions in eAUP Password

Figure 1 shows a 10-by-10 eAUP grid.

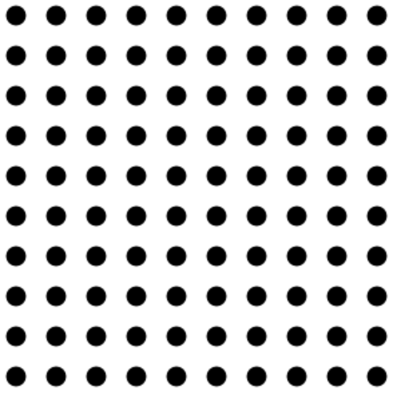

Figure 1. A sample grid.

An eAUP consists of a grid of h * v dots (D) (since the dimension of the grid may be a square or rectangle) that can be connected to each other; h is the number of horizontal dots and v is the number of vertical dots. Hence, the size of the grid can be computed. Theoretically, an eAUP password can be defined as a set of interconnected strokes (s). Therefore, the Length (L_{eAUP}) of an eAUP password can be determined as the number of strokes in the password.

Mathematically:

$$L_{eAUP} = \forall s \quad - \quad (6),$$

where $\forall s$ = number of strokes in the pattern.

Since a stroke (s) is a line connecting two or more dots (D), the minimum size (min_s) of a stroke is two Ds and the maximum possible size (max_s) is maximum $(m,n)_D$, where it is possible to connect a straight line across the longest side of the grid. Since the min_s can be a subset of max_s of a stroke and the size of min_s = 2, then the number of min_s in max_s can be computed as:

$$(N(min_{s)} = {}^{max_s}/_2) \quad \cong \aleph \quad - \quad (7)$$

where, ℵ means rounded down to the nearest whole number, since min_s cannot be a single dot. Hence the shortest stroke s_{min} can be a line between two neighboring Ds. If a dot is defined by the horizontal position h and vertical position v in the grid as (h,v), then its neighbors can be any possible combination of {$D_{(h-1,v)}$, $D_{(h-1,v+1)}$, $D_{(h,v+1)}$, $D_{(h+1,v+1)}$, $D_{(h+1,v)}$, $D_{(h+1,v-1)}$, $D_{(h,v-1)}$, $D_{(h-1,v-1)}$}. Hence the length of an eAUP password can be defined in terms of min_D as:

$$L_{eAUP} = n\,(min_D) \quad - \quad (8)$$

From the fourth assumption, the number of strokes n in a grid is mathematically represented as,

$$n = \frac{(m \times n)}{t} \quad - \quad (9)$$

where $t = (size_D + \overline{D_1 D_2})^2$. The entropy (Yokota et al., 2007) of a random character in a text-based password is defined as:

$$H = L \times \frac{\log n}{\log 2} \quad - \quad (10)$$

Using extended ASCII characters and the current password policy of a minimum password length of eight characters,

N = 218 for printable extended characters

L = 8 characters

then, H = 62.1454745982154, approximately 64 bits. Therefore 64 bits can be used as a baseline to calculate the minimum length of strokes needed by any grid to satisfy the required strength of a character in a space N in any grid.

Instruments for Computing Variables

Minimum Length for H

Given the entropy, the minimum length of characters in a space can be computed as:

$$L_{min} = {}^{H}\Big/_{(\frac{\log n}{\log 2})} \quad - \quad (11)$$

The length of a stroke in an eAUP password cannot be pre-determined since users can be unpredictable, therefore it will range between $\min_s = 2$ and $\max_s$ which depends on the longest side.

Space

Since the longest stroke can be expressed in terms of the smallest stroke (2 dots), the $\min_s$ is used to compute the total space. Also, eAUP does not allow the same dot to be used multiple times, thus using the minimum password space for PRBS, the space of eAUP is computed as:

$$N = \sum_{l=2}^{n} \frac{n!}{(n-l)!} \quad - \quad (12)$$

N is computed to the nearest lower bound whole number.

Entropy

Due to the nature of an eAUP, it is assumed that the probability of selecting a dot is dependent on the immediately preceding dot. We therefore get the Shannon formula for calculating the entropy of a character (Shannon, 2001), which is

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_b p(x_i) \qquad - \qquad (13)$$

Even though Shannon's entropy is not fitting to compute the entropy of an eAUP (due to the continuous nature of eAUP patterns), it is used in this research for simplicity. A more appropriate method is Markov's ***m*** order data process (Hornbeck, 1975; MacRae, 1977). Markov's first-order data process (where $p(x_i) \log_b p(x_i)$ is the probability mass function of outcome $\mathbf{x}_{\boldsymbol{i}}$ and ***n*** the space) is:

$$H = -\sum_{D_{n-1}} P(D_{n-1}) \sum_{D_n} P(D_n) \log_2 P(D_n) \qquad - \qquad (14)$$

where,

P ($\mathbf{D_{n-1}}$) = probability of previous dot and P **($\mathbf{D_n}$)** is the probability of **D** occurring (Schmidt, Wählisch, & Gröning, 2011).

CHAPTER 4

RESULTS, DISCUSSION, AND CONCLUSION

Design

Using the screen resolution of popular screen sizes, a theoretical grid was created that covered the entire screen. It was assumed that a dot had a diameter of 5 pixels and each dot is 10 pixels apart. This gave off a square tolerance of 15px * 15px equivalent to a square tolerance area of 225 pixels. See Appendix A for the code of the grid. The size of the smallest screen was 640 by 480 pixels (VGA), and the size of the largest screen was 2560 by 1600 pixels (WQXGA). The entire screen was used, assuming that the entire screen can be a canvas for the eAUP grid.

A stand-alone java application was used to compute the values for analyzing the eAUP grid. See Appendix A. The application was executed on an Intel i5 core computer with 8GB RAM. The difficulty in constructing a real eAUP grid was overcome by employing this alternative method.

Setup

The resolutions of 22 different screen types were used as parameters for application. Table 1 shows the types of the screen and their resolutions.

Table 1

Types of Screens and Their Resolutions

Screen	**Resolution**
VGA	640 X 480
SVGA	800 X 600
WSVGA	1024 X 600
XGA	1024 X 768
XGA+	1152 X 864
WXGA	1280 X 720
WXGA	1280 X 768
WXGA	1280 X 800
SXGA	1280 X 960
SXGA	1280 X 1024
HD	1360 X 768
HD	1366 X 768
SXGA+	1400 X 1050
WXGA+	1440 X 900
HD+	1600 X 900
UXGA	1600 X 1200
WSXGA+	1680 X 1050
FHD	1920 X 1080
WUXGA	1920 X 1200
QWXGA	2048 X 1152
WQHD	2560 X 1440
WQXGA	2560 X 1600

Results

Due to my limited computing capabilities, the password space for the eAUP grids could not be computed. See Appendix B.

Figure 2 shows the distribution of the number of dots in the height and width of the screens.

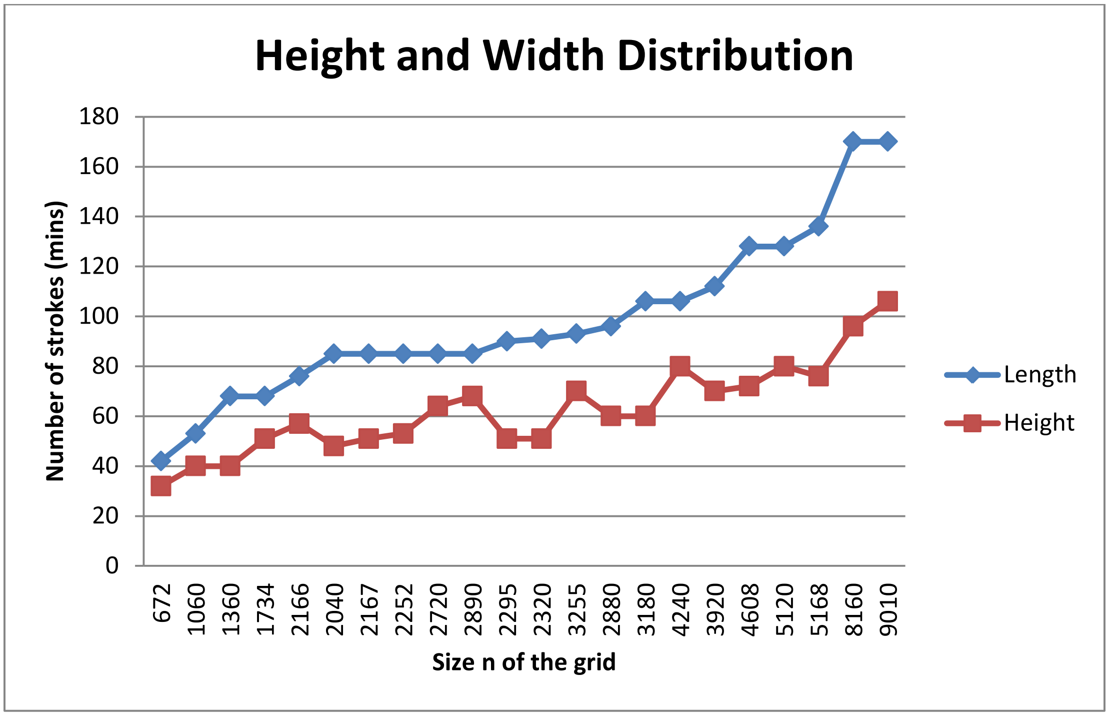

Figure 2. The height and width distribution of the screens.

While the number of strokes in the length of the grid increased steadily, the number of strokes dropped along the graph due to the decrease in the resolution for those screens.

The initial assumption of this research was that the size of the grid will follow a linear trend. However, from Figure 3, the data show that the size of the grid follows a polynomial of the order of 5, which may be due to the fluctuating of the screen resolutions.

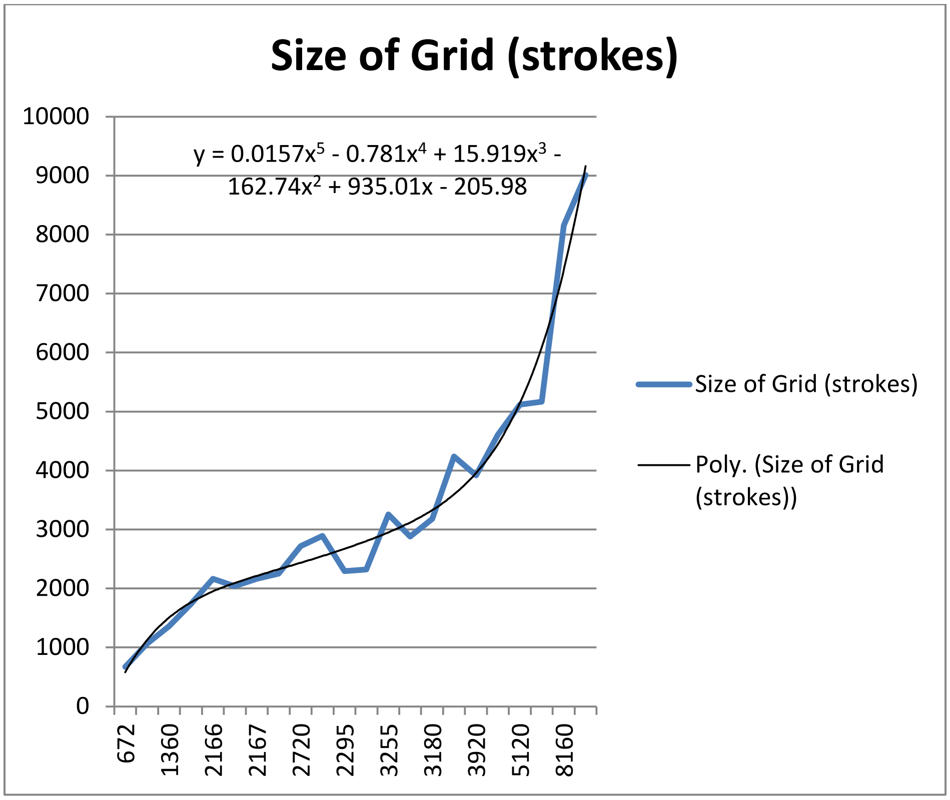

Figure 3. The size of the grid in terms of strokes.

However the entropy for a pattern of length 8 $\min_s$ for the screens follows a linear trend on the line y = 1.0237x + 79.364. See Figure 4.

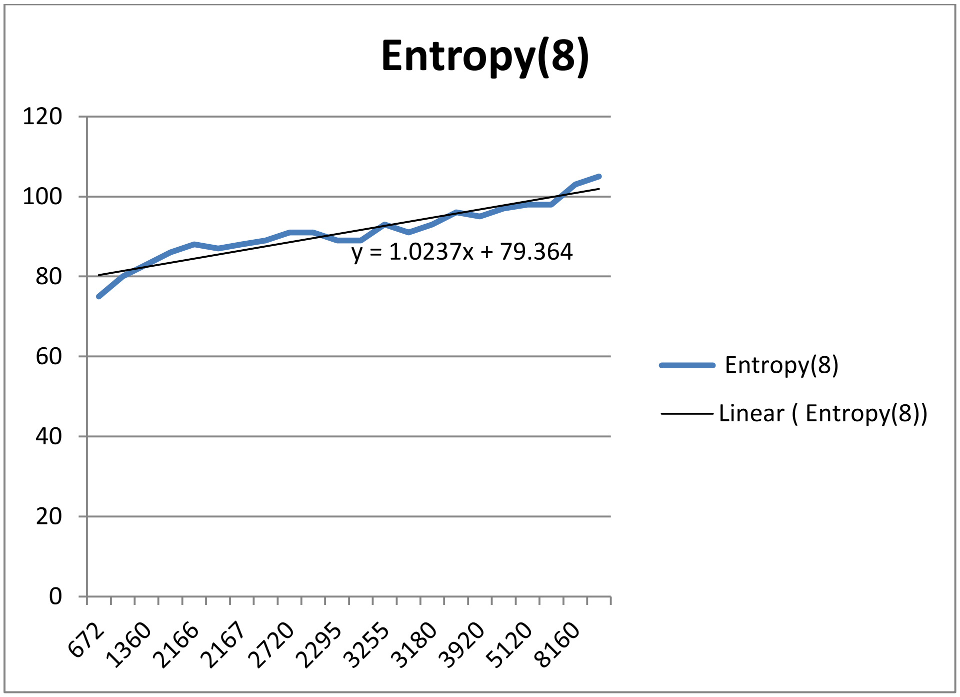

Figure 4. The trend of the Entropy of patterns of length 8 minimum strokes.

Figure 5 shows that the graphs for the L_{min} follow a power trend where the base is approximately $\frac{H}{8}$ and power is approximately -0.093. Hence given H,

$$L_{\min} \quad \cong (\frac{H}{8})^{-0.093}$$

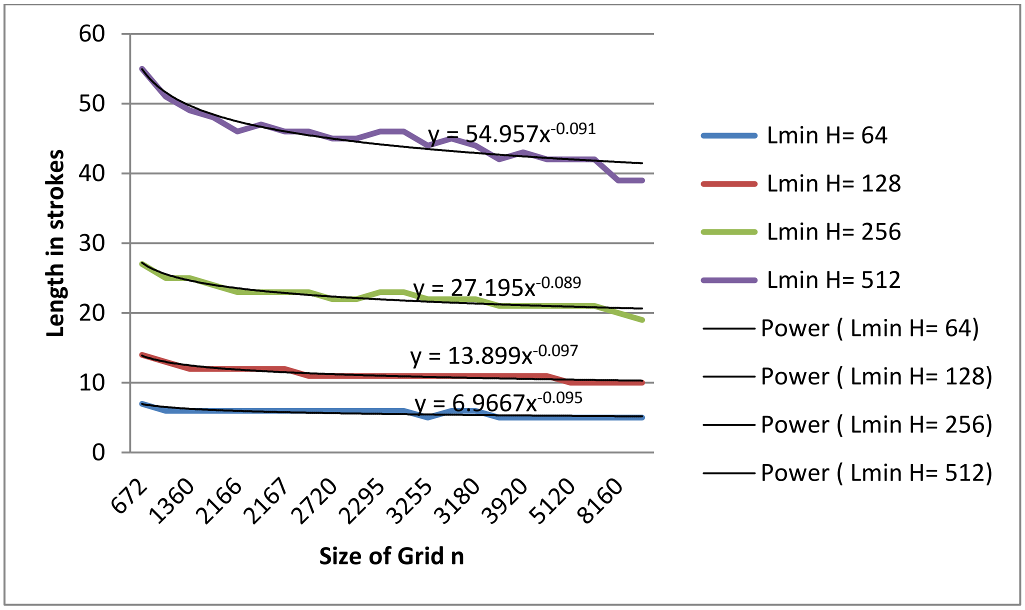

Figure 5. The minimum length in strokes.

Detecting Familiar Shapes

Matte and Warren (2006) describe a line segment in geometry as a line that is confined by two distinct end points, and contains every point on the line between its end points. From the definition, a stroke can be a line segment between dots where $\mathbf{D_S}$ is the beginning dot with position $\mathbf{D_S(h_S,v_S)}$ and $\mathbf{D_E}$ is the ending dot with position $\mathbf{D_E(h_E,v_E)}$.

It is assumed that all strokes in the grid are straights lines that are horizontal, vertical, or diagonal at an angle of 45^o. This will cause all strokes to connect all dots within points $\mathbf{D_S}$ and $\mathbf{D_E}$. Another assumption is that once a dot is used by a stroke in a grid, it cannot be reused as a starting dot of a stroke or an ending dot to a stroke. Also, the end dot is determined when the direction of the stroke changes. The change in direction can be any one of the following: vertical up (↑), vertical down (↓), horizontal left (←), horizontal right (→), diagonal up right (↗), diagonal up left (↖), diagonal down left (↙), and diagonal down right (↘).

Additionally, a middle stroke ***s*** can have only two neighboring strokes since the pattern is drawn continuously except the starting stroke (the first stroke in the pattern) and ending stroke (the last stroke in the pattern), which can have only one neighbor. The neighbor ***sn*** of a stroke ***s*** is such that the beginning or ending dot of ***sn*** is equal to the starting or ending dot of ***s***. Mathematically,

$$s \cap sn \neq \emptyset \quad - \quad (15)$$

However, for the starting stroke ***s***, a neighbor ***sn*** is such that,

$${}^{s}_{E}D\,(h_E, v_E) \;=\; {}^{sn}_{S}D(h_S, v_S) \quad - \quad (16)$$

And the reverse is true for the ending stroke ***e*** such that,

$${}^{e}_{E}D\,(h_E, v_E) \;=\; {}^{e}_{S}D(h_S, v_S) \quad - \quad (17)$$

Even though the pattern is open-ended meaning,

$${}_{E}^{e}D\,(h_E, v_E) \neq \quad {}_{s}^{s}D(h_S, v_S) \quad - \quad (18)$$

the pattern can have vertices for closed shapes like squares, rectangles, triangles, and more. Hence a vertex dot **D$_V$** can be:

1. **D$_V$** such that it is the starting dot **D$_S$** and ending dot **D$_E$** of two neighboring strokes such that:

$$D_v = \quad D_S \quad = \quad D_E \qquad - \quad (19)$$

2. Also **D$_V$** is the intersection of two non-neighboring strokes such that:

$$S_m \cap \quad S_n \quad = \quad D_v \qquad - \quad (20)$$

In order to detect common or familiar shapes and patterns, I used the existing properties of these shapes to detect their existence in an eAUP password.

Square

A square is a four-sided regular polygon with all edges equal, all internal angles are 90°, and whose position on the coordinate plane is determined by the coordinates of the four vertices (corners) (Page, 2012). Figure 6 shows a sample square with vertices ABCD.

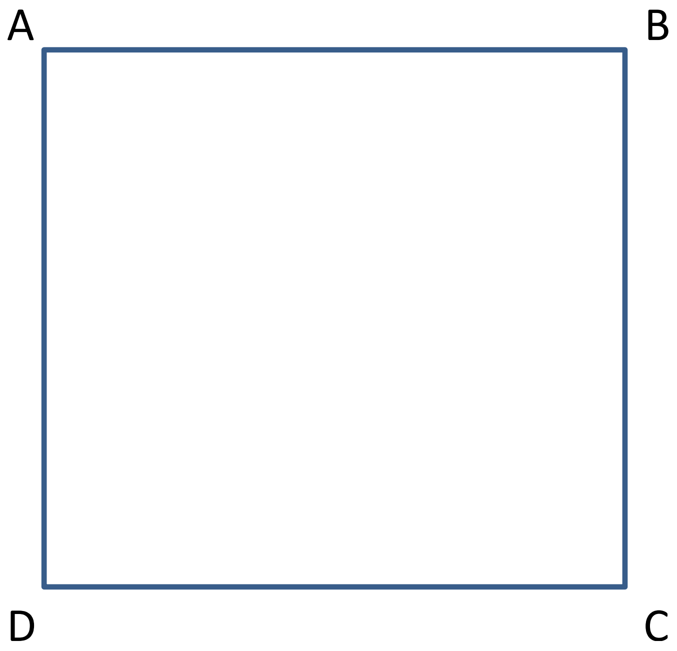

Figure 6. A square ABCD.

Using the properties of a square, a square pattern **ABCD** can be found in a pattern if,

1. All dots between vertices {D_A, D_B, D_C, D_D} are active.

2. $|AB| = |BC| = |CD| = |DA|$

3. $<ABC = <BAC = <BCD = <CDA = 90°$

4. $|AB| \parallel |CD|$ and $|BC| \parallel |AD|$

Rectangle

A rectangle is similar to a square except that only the two parallel line segments are equal. Figure 7 shows a sample rectangle with vertices **ABCD**.

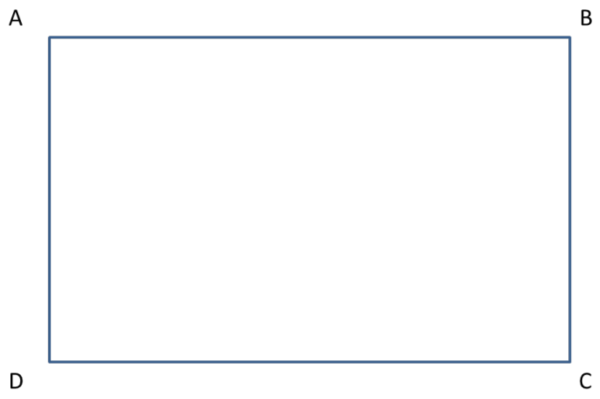

Figure 7. A rectangle ABCD.

Using these properties, a rectangle in an eAUP can be detected based on the following conditions:

1. All dots between vertices {D_A, D_B, D_C, D_D} are active.
2. |AB|= |CD| and |BC| = |DA|
3. <ABC= <BAC= <BCD= <CDA=90°
4. |AB| ∥ |CD| and |BC| ∥ |AD|

Zigzag

A zigzag is a shape made up of small corners at variable angles, though perpetual within the zigzag, outlining a route between two parallel lines; it can be defined as both jagged and fairly regular (“Zigzag,” 2012). Zigzags can be irregular, but due to time constraints, this research was limited to only regular zigzags, which can be traced through two parallel lines and the alternating line segments are parallel to each other.

To find the angle between strokes in a pattern, the Euclidean calculations can be used (Weisstein, 2012). For a zigzag pattern to be detected, the dot products of all neighboring lines need to be computed. Assuming two neighboring strokes are denoted by $\mathbf{s_1}$ and $\mathbf{s_2}$ where $\mathbf{s_1}$ is bounded by $\mathbf{|D_{s1}D_{e1}|}$ where $\mathbf{D_{s1} = (h_{s1}, v_{s1})}$ and $\mathbf{D_{e1} = (h_{e1}, v_{e1})}$. Then,

$\Delta h_{s1} = h_{s1} - h_{e1}$ - (21) and

$\Delta v_{s1} = v_{s1} - v_{e11}$ - (22)

Hence,

$s_1 = (h_{s1}, v_{s1})$ - (23)and

$s_2 = (h_{s2}, v_{s2})$ - (24)

Applying Euclidean calculations, an angle θ between $\mathbf{s_1}$ and $\mathbf{s_2}$ is

$\cos\theta = \frac{(\Delta h_{s1} - \Delta v_{s1}) \times (\Delta h_{s2} - \Delta v_{s2})}{|\Delta h_{s1} - \Delta v_{s1}|\,|\Delta h_{s2} - \Delta v_{s2}|}$ - (25) hence,

$$\theta = \cos^{-1}\left(\frac{(\Delta h_{s1} - \Delta v_{s1}) \times (\Delta h_{s2} - \Delta v_{s2})}{|\Delta h_{s1} - \Delta v_{s1}|\,|\Delta h_{s2} - \Delta v_{s2}|}\right) \qquad - (26)$$

Assuming that $\mathbf{D_{v1}}$ is the dot that connects $\mathbf{s_1}$ and $\mathbf{s_2}$, $\mathbf{D_{v2}}$ is the dot that connects $\mathbf{s_2}$ and $\mathbf{s_3}$, and $\mathbf{D_{v3}}$ connects $\mathbf{s_3}$ and $\mathbf{s_4}$. Then to detect a zigzag, there must be a change of direction at each of the dots (in opposite direction) of each of the strokes at an angle of about $\boldsymbol{\theta}$.

Discussion and Conclusion

The formulae used in this research may be error-prone, but they give significant results that can help guide future research into an eAUP scheme. From the two-way *t* test = 6.36033E-09 on space and entropy, there is no significant difference between the grid size n and the entropy H of a password of length 8. Hence the null hypothesis cannot be rejected.

Even though each stroke is made of a straight line, by increasing the grid, the length of the minimum stroke can be reduced so that they can be used to construct curves within the grid.

Future work that can be done includes considering the continuous nature of the pattern in the calculations of space and entropy. Another potential research area is using the grid to draw Asian characters as passwords within the grid.

APPENDIX A

CODE USED FOR COMPUING RESULTS

Grid.java

```
/**
 * source of integration function is:
 *
http://introcs.cs.princeton.edu/java/93integration/Trapezoi
dalRule.java.html
 * @author Joseph Abandoh-Sam
 */
public class Grid {

    private int m = 0;
    private int v = 0;
    private int size;
    private String name = null;

    public Grid ( String name,int mtemp, int ntemp){
        this.name = name;
        m = mtemp/15;
        v = ntemp/15;

        size = (m * v)/2;
        //System.out.println(size);
    }

    public int getM(){
        return m;
    }

    public int getV(){
        return v;
    }
    public String getName(){
        return this.name;
    }
    public double f(double x){
        //return (Math.log(x)/Math.log(2));
        return (1/x )* (Math.log(1/x)/Math.log(2));
    }


    //from
    private double integrate(double a, double b, int N) {
      double h = (b - a) / N;              // step size
      double sum = 0.5 * (f(a) + f(b));    // area
      for (int i = 1; i < N; i++) {
         double x = a + h * i;
         sum = sum + f(x);
      }

      return sum * h;
    }

    public int getSize(){
        return size;
    }

    //returns the space for the grid.
    public long getN(){
        double sum = 0;
        for(int l = 2; l <= Math.max(m, v); l++){
            sum = sum + (factorial(size)/factorial(size -
l));
        }
        return Math.round(sum);
    }

    //returns the min number of strokes for
    public long Lmin (int H){
        return Math.round(H/(Math.log(size)/Math.log(2)));
    }

    //calculate the factorial of a number.
    private double factorial (int n){
        double fact = 1;
        if (n <= 1) {
     return 1;
 }

 else {
     for (int i=1 ; i<=n; i++){
```

```
                fact = fact*i;
                System.out.println(fact);
            }
            return fact;
        }
    }

    public int entropy(int l){
        int H = 0;

        for(int i = 0; i <= l; i++){
            //H = H + ((1/(size-i)) * l * ();
        }

        H = (int) (l * (Math.log(size) /
Math.log(2)));//(int)integrate(2,size, size-2);

        //double sum1 = 0.0; // the two summations in the
equation.

        return H;
    }

}
```

Running.java

```
/**
 * Calculate the values for each grid
 * @author Joseph Abandoh-Sam
 */
import java.io.*;
import java.util.Scanner;
import java.util.logging.Level;
import java.util.logging.Logger;

public class Running {


    private static Grid grid;

    public static void initialize()throws Exception{
        //fstream = new FileWriter("input.txt");
        //out = new BufferedWriter(fstream);
    }
    public static void main (String args[]){
        //grid = new Grid(100,100);
        Scanner sc = null;
        int m = 1024, n = 768;
        try {
            sc = new Scanner(new
FileReader("D:\\test\\grid_input.txt"));
            sc.useDelimiter(" ");
        } catch (FileNotFoundException ex) {

Logger.getLogger(Running.class.getName()).log(Level.SEVERE,
null, ex);
        }


        grid = new Grid(args[0], Integer.parseInt(args[1]),
Integer.parseInt(args[2]));

        System.out.println(grid.getName()+", "+ grid.getM()
+ ", " + grid.getV() + ", " + grid.getSize()+", " +
grid.entropy(8)+ ", " + grid.Lmin(64)
            + ", " + grid.Lmin(128)+ ", " + grid.Lmin(256)+
", " + grid.Lmin(512));
```

```
        }

    }
```

APPENDIX B

TABLE OF RESULTS

SCREEN	Length	Height	size	Entropy(8)	Lmin H= 64	Lmin H= 128	Lmin H= 256	Lmin H= 512
VGA	42	32	672	75	7	14	27	55
SVGA	53	40	1060	80	6	13	25	51
WSVGA	68	40	1360	83	6	12	25	49
XGA	68	51	1734	86	6	12	24	48
XGA+	76	57	2166	88	6	12	23	46
WXGA	85	48	2040	87	6	12	23	47
WXGA	85	51	2167	88	6	12	23	46
WXGA	85	53	2252	89	6	11	23	46
SXGA	85	64	2720	91	6	11	22	45
SXGA	85	68	2890	91	6	11	22	45
HD	90	51	2295	89	6	11	23	46
HD	91	51	2320	89	6	11	23	46
SXGA+	93	70	3255	93	5	11	22	44
WXGA+	96	60	2880	91	6	11	22	45
HD+	106	60	3180	93	6	11	22	44
UXGA	106	80	4240	96	5	11	21	42
WSXGA+	112	70	3920	95	5	11	21	43
FHD	128	72	4608	97	5	11	21	42
WUXGA	128	80	5120	98	5	10	21	42
QWXGA	136	76	5168	98	5	10	21	42
WQHD	170	96	8160	103	5	10	20	39
WQXGA	170	106	9010	105	5	10	19	39

REFERENCE LIST

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communication Association of Computer Machinery, 42*(12), 40-46. Doi: 10.1145/322796.322806

Barker, E., & Kelsey, J. (2012). *Recommendation for random number generation using deterministic random bit generators* (Sp800-90a). Gaithersburg, MD: National Institute of Standards and Technology.

Bragdon, A., Uguray, A., Wigdor, D., Anagnostopoulos, S., Zeleznik, R., & Feman, R. (2010). *Gesture play: Motivating online gesture learning with fun, positive reinforcement and physical metaphors*. Paper presented at the ACM International Conference on Interactive Tabletops and Surfaces, Saarbrucken, Germany.

Burr, W. E., Dodson, D. F., & Polk, W. T. (2006). *Electronic authentication guideline* (Sp800-63). Gaithersburg, MD: National Institute of Standards and Technology.

Chiasson, S., Forget, A., Biddle, R., & Van Oorschot, P. C. V. (2008). *Influencing users towards better passwords: Persuasive cued click-points*. Paper presented at the Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, Volume 1, Liverpool, United Kingdom.

Chiasson, S., Forget, A., Stobert, E., Van Oorschot, P. C., & Biddle, R. (2009). *Multiple password interference in text passwords and click-based graphical passwords*. Paper presented at the Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL.

Chiasson, S., Stobert, E., Forget, A., Biddle, R., & Van Oorschot, P. C. (2012). Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *Dependable and Secure Computing, IEEE Transactions on, 9*(2), 222-235. Doi: 10.1109/Tdsc.2011.55

Czekalski, E. (2012). *RSA information security glossary.* Retrieved July 2012 from RSA website.

Dirik, A. E., Memon, N., & Birget, J.-C. (2007). *Modeling user choice in the passpoints graphical password scheme*. Paper presented at the Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA.

Dunphy, P., Heiner, A. P., & Asokan, N. (2010). *A closer look at recognition-based graphical passwords on mobile devices*. Paper presented at the Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA.

Dunphy, P., & Yan, J. (2007a). *Do background images improve "draw a secret" graphical passwords?* Paper presented at the Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, VA.

Esteban, M. D., Morales, D., Pardo, L., & Menendez, M. L. (1994). Order statistics and (r,s)-entropy measures (English). *Applications of Mathematics, 39*(5), 321-337.

Forget, A., Chiasson, S., & Biddle, R. (2007). *Helping users create better passwords: Is this the right approach?* Paper presented at the Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA.

Forget, A., Chiasson, S., & Biddle, R. (2010). *Input precision for gaze-based graphical passwords*. Paper presented at the Proceedings of the 28th International Conference Extended Abstracts on Human Factors in Computing Systems, Atlanta, GA.

Gyorbiro, N., Larkin, H., & Cohen, M. (2010a). *Spaced repetition tool for improving long-term memory retention and recall of collected personal experiences*. Paper presented at the Proceedings of the 7th International Conference on Advances in Computer Entertainment Technology, Taipei, Taiwan.

Gyorbiro, N., Larkin, H., & Cohen, M. (2010b). *Long-term memory retention and recall of collected personal memories*. Paper presented at the ACM SIGGRAPH 2010 Posters, Los Angeles, CA.

Halevi, S., & Krawczyk, H. (1999). Public-key cryptography and password protocols. *ACM Transaction on Information System Security, 2*(3), 230-268. Doi: 10.1145/322510.322514

Holt, L. (2011). *Increasing real-world security of user IDs and passwords*. Paper presented at the Proceedings of the 2011 Information Security Curriculum Development Conference, Kennesaw, GA.

Hornbeck, R. W. (1975). *Numerical methods*. New York, NY: Quantum Publishers.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). *The design and analysis of graphical passwords.* Paper presented at the USENIX Security Symposium, Washington, DC.

Komanduri, S., & Hutchings, D. R. (2008). *Order and entropy in picture passwords*. Paper presented at the Proceedings of Graphics Interface 2008, Windsor, Ontario, Canada.

Landman, M. (2010). *Managing smart phone security risks*. Paper presented at the 2010 Information Security Curriculum Development Conference, Kennesaw, GA.

MacRae, E. C. (1977). Estimation of time-varying Markov processes with aggregate data. *Econometrica, 45*(1), 183-198.

Matte, T. F., & Warren, B. (2006). Line segment, 9. *PlanetMath*. Retrieved from http://planetmath.org/LineSegment.html

McDowell, M., Rafail, J., & Herman, S. (2009). *Choosing and protecting passwords* (Security Tip [St04-002]). Retrieved from http://Www.Us-Cert.Gov/Cas/Tips/St04-002.Html

Milton, J., & Kennedy, P. J. (2010). *Entropy profiles of ranked and random populations*. Paper presented at the Proceedings of the 12th Annual Conference Companion on Genetic and Evolutionary Computation, Portland, OR.

Narayanan, A., & Shmatikov, V. (2005). *Fast dictionary attacks on passwords using time-space tradeoff*. Paper presented at the Proceedings of the 12th ACM Conference on Computer and Communications Security, Alexandria, VA.

Page, J. D. (2012). *Math open reference.* Retrieved from http://www.mathopenref.com

Passfaces Corporation. (2012). *Passfaces: Two factor authentication for the enterprise.* Retrieved from http://www.passfaces.com/index.htm

Password strength. (2012, July). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Password_strength

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131. Doi: 10.1023/A:1011902718709

Schmidt, T. C., Wählisch, M., & Gröning, M. (2011). Context-adaptive entropy analysis as a lightweight detector of zero-day shellcode intrusion for mobiles. *SIGMOBILE Mobile Computing Communication Review, 15*(3), 47-48. Doi: 10.1145/2073290.2073303

Shannon, C. E. (2001). A mathematical theory of communication. *SIGMOBILE Mobile Computing Communication Review, 5*(1), 3-55. Doi: 10.1145/584091.584093

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., & Cranor, L. F. (2010). *Encountering stronger password requirements: User attitudes and behaviors*. Paper presented at the Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA.

Spitzer, J., Singh, C., & Schweitzer, D. (2010). A security class project in graphical passwords. *Journal of Computing in Small Colleges, 26*(2), 7-13.

Stobert, E. (2010). *Usability and strength in click-based graphical passwords*. Paper presented at the Proceedings of the 28th of the International Conference Extended Abstracts on Human Factors in Computing Systems, Atlanta, GA.

Stobert, E., Forget, A., Chiasson, S., Van Oorschot, P. C., & Biddle, R. (2010b). *Exploring usability effects of increasing security in click-based graphical passwords*. Paper presented at the Proceedings of the 26th Annual Computer Security Applications Conference, Austin, TX.

Suo, X., Zhu, Y., & Owen, G. S. (2006). *Analysis and design of graphical password techniques*. Paper presented at the Proceedings of the Second International Conference on Advances in Visual Computing, Volume 2, Lake Tahoe, NV.

Van Oorschot, P. C., & Thorpe, J. (2008). On predictive models and user-drawn graphical passwords. *ACM Transactions Information Systems Security, 10*(4), 1-33. Doi: 10.1145/1284680.1284685

Vidyaraman, S., Chandrasekaran, M., & Upadhyaya, S. (2008). *Position: The user is the enemy*. Paper presented at the Proceedings of the 2007 Workshop on New Security Paradigms, North Conway, NH.

Weisstein, E. W. (2012). Line-line angle. *MathWorld*. Retrieved from http://mathworld.wolfram.com/ Line-LineAngle.html

Wong, K. M., & Chen, S. (2006). The entropy of ordered sequences and order statistics. *IEEE Transaction on Information Theory, 36*(2), 276-284. Doi: 10.1109/18.52473

Yokota, T., Ootsu, K., & Baba, T. (2007). *Introducing entropies for representing program behavior and branch predictor performance*. Paper presented at the Proceedings of the 2007 Workshop on Experimental Computer Science, San Diego, CA.

Zigzag. (2012, July). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Zigzag

Zhang, Y., Monrose, F., & Reiter, M. K. (2010). *The Security of Modern Password Expiration: An algorithmic framework and empirical analysis*. Paper presented at the Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, IL.