Action-based user authentication

Roman V. Yampolskiy

Speed School of Engineering,
University of Louisville,
425 Paul C. Lutz Hall,
Louisville, KY 40292, USA
E-mail: roman.yampolskiy@louisville.edu

Abstract: Network security partially depends on reliable user authentication; unfortunately currently used passwords are not completely secure. One of the main problems with passwords is that very good passwords are hard to remember and the ones which are easy to remember are too short or simple to be secure. We have designed a number of authentication schemas, which are easy to remember and can be relatively quickly provided to the system, while at the same time remaining impossible to break with brute force alone. In this article, we have compared the size of password spaces and how easy they are to remember for many popular alphanumeric and graphical authentication schemas against the approaches developed by us, namely PassText, PassArt and PassMap.

Keywords: PassArt; PassMap; passtext; password; password space; unit of memory; user authentication.

Reference to this paper should be made as follows: Yampolskiy, R.V. (2008) 'Action-based user authentication', *Int. J. Electronic Security and Digital Forensics*, Vol. 1, No. 3, pp.281–300.

Biographical note: Roman V. Yampolskiy holds a PhD from the Department of Computer Science and Engineering at the University at Buffalo. There he was a recipient of a four-year NSF fellowship. Before beginning his doctoral studies, Yampolskiy received a BS MS (High Honors) combined degree in Computer Science from Rochester Institute of Technology. After completing his PhD dissertation Yampolskiy held a position of an Affiliate Academic at the Center for Advanced Spatial Analysis, University of London, College of London. In August of 2008, Yampolskiy accepted an Assistant Professor position at the Speed School of Engineering, University of Louisville. He had previously conducted research at the Laboratory for Applied Computing at the Rochester Institute of Technology and at the Center for Unified Biometrics and Sensors at the University at Buffalo. Yampolskiy's main areas of interest are computer forensics, behavioural biometrics, pattern recognition, genetic algorithms, neural networks, artificial intelligence and games. Yampolskiy is an Author of over 40 publications including multiple journal articles and books.

1 Introduction

As computer technology continues to grow in importance in our every day lives, it becomes increasingly important to provide safe and secure ways to authenticate users of different systems, and to allow people access to information, networks and decision making modules. The first and most important step in network and computer security is reliable user authentication. For decades, simple passwords were sufficient for insuring that only authorised individuals had access to privileged resources and information. As computers became more computationally powerful, brute force attacks on the previously unprecedented scale became possible. Because users tend to create simple and easy to remember passwords, classical passwords no longer provide a sufficient level of security for most systems.

This problem has not been ignored by researchers who are trying to create secure and easy to remember novel authentication systems or to improve existing approaches (Morris and Thompson, 1979; Provos and Mazieres, 1999; Renaud and Smith, 2001; Brostoff, 2004; Birget, Hong and Memon, 2005). Currently most research in user authentication is geared towards graphical passwords, but such methodologies present problems of their own. In this article, we describe and analyse a number of user authentication approaches, which are both easy to remember and provide a very high level of security. They are not threatened by a brute force attack with significant computational resources. After our methodologies are described, they are compared to other commonly used authentication mechanisms in terms of how easy they are to remember and with respect to the password space size (Yampolskiy, 2006). The results of the comparison are favourable for our approaches.

2 Existing authentication mechanisms

Many researchers have recognised inherent shortcomings of simple passwords and as a result, a wealth of different authentication approaches exists. This section provides a quick overview of the most well-known user authenticating techniques. We will follow a classification schema proposed by Renaud (2003) in her paper on quantifying the quality of authentication mechanisms while also considering user's location as one possible, but questionable way of authenticating users. All authentication approaches can be divided into four categories based on what a user has, knows, is or where the user is currently located. What the user has is typically a token or a private key and both cases, while very popular, are beyond the scope of this article.

2.1 Where the user is located

This is an approach used mostly by online casinos to verify that the user is located in a region where gambling operations are legal. However, it does provide some level of verification of who the user is and is therefore included in our overview for completeness of presentation.

2.1.1 Internet protocol filtering

This is a way to identify the location from which a user is connecting to the server, an assumption is made that if the service provider and or geographic location associated with the internet protocol (IP) address has not changed from the last login, neither did the user identity. This is a questionable assumption and so the technology is mostly used to tell if a user is located in a locality where a certain activity such as gambling is legal, not to identify or verify users. If a direct broadband connection is used, this mechanism is virtually foolproof. If a dialup is used, these filtering systems lack an ability to accurately identify location. These systems can be used to allow a connection through known Internet service provider's (ISP) where the final hop is hard wired. In general, where this cannot be ascertained admittance is denied. As a result, this is a coarse selection mechanism that will deny many users who are in fact geographically acceptable, but assures that anyone permitted within the filter is within the jurisdiction (Player Id, 2005).

2.1.2 GeoBio indicator

A device consisting of an integrated global positioning system (GPS)-based geographical indicator and a biometric-based smart card that is attached to a personal computer via the universal serial bus (USB) port. As with any device using a standard USB, it is self-installing. GeoBio indicators can be used for user identification and border control, but have significant implementation costs and distribution barriers associated with hardware purchasing and distribution as well as with the enrollment process (Player Id, 2005). Along with other problems in this approach are privacy issues inevitably raised by integration of biometric and geographic information in one data-system.

2.1.3 Phone call verification

Represents a method utilising a synchronised phone call with a web session to identify a user's geographic location. It even works for users with a single phone line.

> "During the synchronized call, [verifier] employs data matching and telephone provisioning information to determine who owns the phone and its location. A voice recording and voice biometric is captured to ensure acceptance of a transaction and limit use of an account. Country code, area code, and local exchange information can be matched to IP address providing strong location assurance. This approach offers a way to verify user's … location, in real-time, without installing hardware or software on the end users computer." (Player Id, 2005)

This approach works well for a geographical location-based restriction of access, but it only identifies the geographic location and not the user. It also requires the knowledge of English language from the user and is time consuming.

2.2 Who the user is

This is a biometrics-based approach and can be extremely reliable, unfortunately physical biometrics such as fingerprints, iris scans and faces require special hardware which could be expensive to install and maintain or simply not available to all users. Behavioural biometrics-based on keystroke dynamics (Monrose, Reiter and Wetzel, 2001), mouse usage patterns or signature dynamics do not require any special hardware and can be utilised for reliable user authentication (Yampolskiy, 2007b,c,d).

2.2.1 BioPassword

BioPassword is a patented software-only authentication system based on the keystroke dynamics biometric. While the user enters his password the system captures information about just how the user types, including any pauses between the pressings of different keys. Essentially the software observes the typing rhythm, pace and syncopation. This information is used to create a statistically reliable profile for an individual. In combination with the user's password, BioPassword creates a so-called hardened password (BioPassword, 2005). It is no longer enough to know the password itself, it is also important to enter it in precisely the same way as the true account owner would. This approach however requires an extended enrollment period.

2.2.2 Pass-Thoughts

Thorpe, Oorschot and Somayaji (2005) proposed using brain computer interface technology to have a user directly transmit his thoughts to a computer. The system extracts entropy from a user's brain signal upon reading a thought. The brain signals are processed in an accurate and repeatable way providing a changeable, authentication method resilient to shoulder-surfing. The potential size of the space of a Pass-Thought system is not clear at this point but likely to be very large, due to the lack of bounds on what composes a thought.

2.3 What the user knows

This is the most popular approach and the one we are most interested in for the purpose of comparison of our approach to existing solutions. The authentication schemas based on what a user knows can be grouped into two classes: text- and graphics-based.

2.3.1 Text-based approaches

Text-based approaches can be further subdivided into syntactic, semantic and one-time methods. The classical passwords and passphrases are examples of syntactic methods in which a user is expected to memorise a sequence of characters or words. The sequence can either be generated for the user or user selected (Renaud, 2003). The problem is that a user's ability to memorise complicated or multiple passwords is limited, and so authentication may present problems for the user. Alternatively, easy to remember passwords are also easy to guess and so provide a low level of security. Some researchers present methods which might be easier for users to remember, for example, the check-off password system (COPS; Bekkering, Warkentin and Davis, 2003) allows users to enter characters in any order and therefore the users can choose to remember their password in many different ways. Each user is assigned eight different characters selected from the sixteen most commonly used letters. The user may use any character more than once to form words which are easy to remember and so it is claimed COPS provides an advantage over regular passwords.

Semantic or cognitive passwords typically work by asking a user some questions and treating the user's answer as the key to the authentication mechanism. One approach described by Renaud (2003) relies on asking the user clarifying questions until the answer matches the one expected by the system. An alternative technique provided a set of questionnaires, which asking users to answer some fact- or opinion-based questions. These approaches are not very user friendly as it might take a long time for the user to arrive at the desired answer, and since users are very sensitive to the time component of authentication protocol, the cognitive-based methods are not expected to become widely popular.

One-time password approaches are designed to provide a higher level of security for crucial systems such as bank accounts. If a hacker somehow obtains a valid password he would not be able to reuse it after the initial break in. Two main approaches exist either using hardware or using codebooks. Both of these are expensive to implement and demanding of the user's time (McDonald, Atkinson and Metz, 1995; Rubin, 1995). In passbooks methodology a user is provided with a listing of codes, each code can be used for only a single log in. After a code is used it is crossed off and the next code becomes a valid password for the next session. After all of the codes in the passbook are used a new passbook needs to be ordered. This approach clearly only works in cases where access to the system is not needed on a daily basis.

2.3.2 Graphics-based approaches

Graphical passwords are designed to take advantage of human visual memory capabilities, which are far superior to our ability to remember textual information. Two main types of graphical passwords are currently in use: recognition- and position-based methods are the main approaches in current research. In recognition-based systems, users must identify images they have previously seen among new graphics.

Probably, the most well-known recognition-based graphical authentication system is called passfaces (Brostoff, 2004; The Science Behind Passfaces, Real User Corporation, 2004). It relies on the ease with which people recognise familiar faces. During enrollment, a user is presented with a set of faces he is asked to memorise. During authentication a screen with nine faces is presented to the user, with one of the faces being from his passface set. User has to select a face, which is familiar from the enrollment step. This process is repeated five times resulting in a relatively small space of 59,050 possible face combinations. Obviously this is not sufficient if the system is open to an exhaustive search.

Another authentication system, Déjà Vu, is based on random art images. User is asked to choose five images as his pass set and during authentication needs to select his pass set from a challenge set of 25 pictures. Since the pictures used are completely random and are generated by a computer program it is next to impossible to share a Déjà Vu password with others. Preliminary research shows that users prefer real photographs to random art images and that the enrollment phase is more time consuming than that of alphanumeric passwords (Dhamija and Perrig, 2000).

The two systems mentioned above are probably representative of many other similar recognition-based graphical authentication systems currently in existence. Visual identification protocol (Angeli et al., 2003; Renaud, 2003), picture password (Jansen, 2005), and picturepins (Pointsec, 2002) are all reliant on exploiting the users' good visual memory and power of recall to easily authenticate users by making them pick familiar images from a large set of graphics.

The remaining authentication approaches presented in this article are graphical position-based systems. A typical position-based approach is presented in PassPoints, a system-based on having the user select points of interest within a single image. The number of points is not limited and so a relatively large search space is protecting against any attempt to guess a PassPoints authentication sequence (Wiedenbeck et al., 2005a,c). This is similar to the methodology used in the original patent for graphical passwords obtained by Blonder in 1996 (Blonder, 1996).

An alternative to having a user select a portion of an image is to have a user input a simple drawing into a pre-defined grid space. This approach is attempted in Varenhorst (2004) with a system called Passdoodles and also in Jermyn (1999) and Thorpe and Oorschot (2004b) with a system called draw-a-secret (DAS). Finally, a V-go password requests a user to perform simulation of simple actions such as mixing a cocktail using a graphical interface (Renaud, 2003).

The aim of this overview of user authentication systems was not to produce a comprehensive listing, but rather to introduce the reader to the current state of the art in the field. Many variations on the presented approaches were not described in sufficient detail and some, such as textual passwords with graphical assistance (Jermyn, 1999), Authentigraph (Pierce, 2003), Pseudoword recognition (Weinshall and Kirkpatrick, 2005), Image with Sound (Liddell, Renaud and Angeli, 2003), Triangle and Movable Frame schema (Sobrado and Birget, 2005), Inkblot reminder (Ross, 2005), Handwriting reminders (Porter, 2005) and Artificial Grammar Learning (Weinshall and Kirkpatrick, 2005) are only mentioned here so that an interested reader can investigate them further.

3 Shortcomings of the existing approaches

The reason why so many different user authentication approaches exist is because all current methodologies have certain shortcomings making their use difficult or impossible for some groups of users or on some systems. Alphanumeric passwords suffer from users picking names, simple words or their phone numbers as passwords instead of random strings. Such tendencies make the actual password search space much smaller and therefore susceptible to a dictionary brute force attack. A lot of research went into restricting a user's choices during enrollment process in order to make passwords more secure (Feldmeier and Karn 1989; Klein, 1990; Bishop, 1992; Player Id, 2005; Spafford, 2005). For example, the following set of restrictions on alphanumeric password choices is given by Klein (1990):

- passwords based on the user's account name
- passwords based on the user's initials or given name
- passwords which exactly match a word in a dictionary (not just /usr/dict/words)
- passwords which match a word in the dictionary with some or all letters capitalised
- passwords which match a reversed word in the dictionary
- passwords which match a reversed word in the dictionary with some or all letters capitalised
- passwords which match a word in a dictionary with an arbitrary letter turned into a control character
- passwords which match a dictionary word with the numbers '0', '1', '2' and '5' substituted for the letters 'o', 'l'
- passwords which are simple conjugations of a dictionary word (i.e. plurals adding 'ing' or 'ed' to the end of the word, etc.)

- passwords which are patterns from the keyboard (i.e. 'aaaaaa' or 'qwerty')
- passwords which are shorter than a specific length (i.e. nothing shorter than six characters)
- passwords which consist solely of numeric characters (i.e. social security numbers, telephone numbers, house addresses or office numbers)
- passwords which do not contain mixed upper and lower case or mixed letter and numbers or mixed letters and punctuation
- passwords which look like a state issued license plate number.

Unfortunately those restrictions have mostly failed at creating secure, but memorable alphanumeric passwords as it is beyond natural capability of human memory to easily reproduce random bits of alphanumeric information. As a result of this situation, a solution was proposed which came to be known as graphical password. An approach, which is supposedly extremely easy to remember, yet at the same time is sufficiently secure. However to this day, graphical passwords do not have a significant share of the authentication market potentially because they have introduced a number of new problems to the task of user identification.

Next, we consider the drawbacks of graphical passwords. First, people with impaired vision will have a problem with most graphical passwords, particularly those employing images with many small details. These users typically depend on text-reading software to interact with a computer and so would have no way of knowing what is on the picture. Second, people who have motor control problems will have a hard time precisely manipulating a mouse or any other similar pointing device and so may experience some difficulty in using graphical passwords, particularly those based on the selection of small subparts of an image, such as PassPoints. People with certain other types of visual problems such as colourblindness may also experience problems with graphical passwords dependent on colourful images (Wiedenbeck et al., 2005c).

In general, almost any possible user authentication approach will have a group of individuals to which such an approach presents a problem. For example, Dyslexic users will have problems reading and therefore remembering text. Dyspraxics have problems with memorisation of sequences, which is necessary in almost all authentication approaches reliant on sequential selection or entry of data. Prosopagnosic people have difficulty with face recognition and so cannot deal well with systems like PassFaces (Renaud, 2003). The only solution is to have user authentication schemas, which incorporate multiple approaches within a single user validation methodology.

Particular problems have been identified with most of the more popular graphical password methodologies.

- In a DAS schema, it has been shown that users tend to select drawings, which are easy to remember and as a result decrease the size of DAS password space. In particular, users tend to create drawings, which are symmetric, contain only 1–3 strokes and are centered (Pointsec, 2002; Nali and Thorpe, 2004). Having this information makes a brute force attack against DAS possible.
- In an investigation of the PassPoints system, it has been demonstrated that accurate recollection of the password is strongly reduced if a small tolerance region is used around the user's password points. But, if a large region is used the password space

of PassPoints is being reduced. In addition, it was established that not all images are suitable as PassPoints graphics. In particular, images with few memorable points such as images with large expanses of green grass or overly complicated images should be avoided (Wiedenbeck et al., 2005b).

- A system such as PassFaces is also subject to a reduced password space, which in the case of passfaces is already barely sufficient. It has been shown that users of a face recognition-based authentication system tend to select certain faces more often than others if they are permitted to select their own passwords. In particular, both males and females select attractive female faces predominantly over all other types of faces. People also tend to choose faces of people from their own race (Davis, Monrose and Reiter, 2004).

Another significant drawback of graphical passwords is the so-called shoulder-surfing problem. While in alphanumeric authentication schemas it is easily solved with a replacement of the password with a familiar star pattern [******], the situation is much harder for graphical password (GP). A person who observes a few login sessions could eventually realise what the password is or obtain information making the guessing of the password much easier. Sobrado and Birget (2005) propose a shoulder-surfing secure graphical password schema, however it requires over a 1,000 small pictures to be displayed on a single screen, making it impossible to use on most portable devices and a nightmare for people with impaired vision. In addition, a lengthy, ten step, sequence is required for secure authentication. A similar but somewhat modified approach is presented in Hoanca and Mock (2005) and a broad overview of solutions to the shoulder-surfing problem is given by Li and Shum (2005).

4 PassText

We describe a novel approach to user authentication, which addresses some of the limitations of current password schemes both graphical and textual. We call our approach PassText and as the name implies it is a close relative of both passwords and passphrases. In fact, it takes the difference between passwords and passphrases to the next level. Some work in this direction for text-based passwords has been started by Jermyn (1999) who proposed a scheme for combining textual passwords with pre-defined simple graphical input displays allowing a user to input the same password in multiple locations. Similarly, in Thorpe and Oorschot (2004b) researchers present an approach for selecting between different grid spaces for input of graphical passwords (Yampolskiy, 2007e).

Ideally, we want our passphrases to be as long as is humanly possible to remember, making them impossible to guess by brute force or other means. At the same time, the users should not easily forget their passphrases or parts thereof as time from the initial enrollment step passes. It is not reasonable to expect a user to remember, or to have to type in any passphrase longer than a dozen words. So what we propose is, instead of having the burden of providing the passphrase rest on the user’s shoulders, it should be instead stored and readily available in the user authentication system itself. At the PassText creation stage, also known as the enrollment stage, the user is presented with a large body of text to which he is asked to make any modifications he pleases. A possible list of atomic modifications includes: deleting any character from the text or typing any character in any location (Yampolskiy, 2007e).

Obviously, a combination of the above modifications with possible repetitions can be used to produce a unique PassText. A user can delete whole paragraphs, move around sections of the text, replace words with different ones, and replace capitalisation of individual characters and so on. Basically, any standard word processing operation can be utilised. A resulting PassText is just a very long string of characters, which for simplicity is restricted to being plain text. The PassText acts just like any simple text string, deleting a character causes all following characters to shift one character to the left and the size of the PassText decreases by one. The opposite is also true, adding a character shifts all of the following characters to the right and increases the size of PassText by one. To insure that the user has correctly entered his desired PassText we might ask him to repeat it during the enrollment stage and set it only if the verification is successfully performed (Yampolskiy, 2007e).

In the PassText system of authentication, the user is not required to memorise any difficult character combinations such as 'D@$0o#bk2', in fact the user is not required to memorise any text at all, he is however free to do so. User only needs to memorise the sequence of changes he makes to the base document. We argue that this is relatively easy since working with documents is something many computer users frequently do anyways. In addition, the choice of the base document can be made to reflect a user's previous knowledge without sacrificing the security aspect of the system. In fact, a system can be designed with customisable options for each user:

1 The default option is for all users to be presented with a common text. For example, the declaration of independence can serve as a widely known base text document.

2 A user can select an option of having his user name associated with a particular text from a list of possible base text (a more secure but less convenient option is for user to select a text from a larger list of texts).

3 Another option is for a user to provide his own base text file, but this might be a problem for login from remote systems. Due to the limited resources particularly in the case of small mobile devices, there may not be immediate access to the user's chosen base text file.

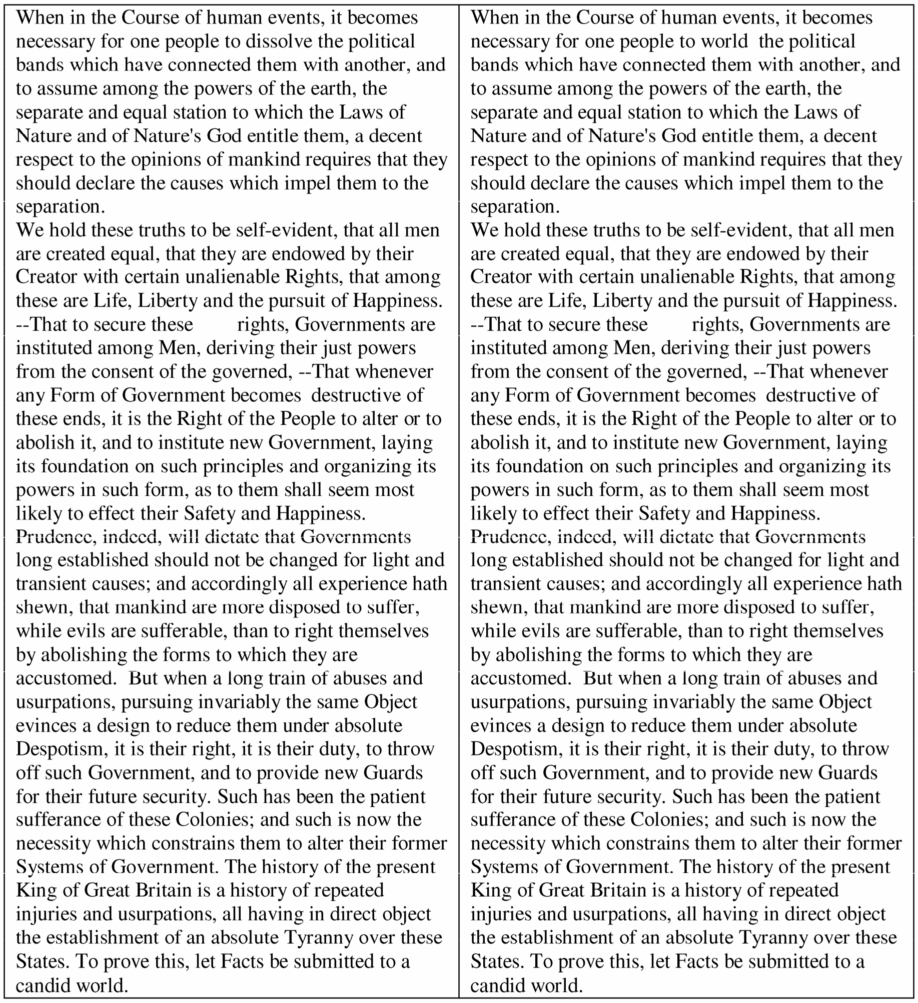
An observant reader has probably noticed that it is possible to use multiple-base-text-selection-menu to create PassTexts made up of the parts of multiple documents with a simple copy and paste command sequence. However, this is not necessary as PassText security is inherently very strong. In a relatively short text of just one page, we have up to 80 characters per line and about 40 lines per page. For example, this page of text you are currently reading contains around 2,500 characters. Assuming a very small alphabet of only 64 characters, we have a total possible PassText space of 64^{2500}, which is enough to disillusion any potential hacker (Yampolskiy, 2007e).

Perhaps an example is in order to demonstrate how the system works and what kind of PassTexts users can generate. Continuing with our example using the declaration of independence as the base text and shortening it for illustration purposes, we have the text on the left side of Figure 1. On the right hand side is the PassText created by removing the word 'dissolve' from the first sentence of the base text and replacing it with the last word, 'world'. Both sides of Figure 1 look fairly similar to the user since they are presented as a formatted text. The system, however, sees them as strings that are drastically different both in size and in makeup (Yampolskiy, 2007e).

While the number of possible base text manipulations is truly enormous, we would like to reiterate that memorising the actual sequence leading to the creation of a secure PassText is very easy and can be used for authentication on multiple systems with multiple base texts without any additional memorisation being required. For example, your PassText might be to replace the first occurrence of the letter ‘a’ in a base text with a word ‘USA’ that is very easy to remember.

In addition, the PassText technology is not very susceptible to ‘shoulder-surfing’ as can be clearly seen from Figure 1. Noticing a single new word in a large body of text or even an absence of some word in a text is not a trivial task particularly if the PassText is created by modifying multiple pages in the base text not all visible on the screen at the same time. While it is common to use asterisks [******] to prevent others from viewing your password it is not a very good idea in the case of PassText as the formation easily draws attention and can help a hacker identify a region which needs to be explored using brute force for a potential guess of your PassText.

Figure 1 Left: declaration of independence; right: PassText example



When in the Course of human events, it becomes necessary for one people to dissolve the political bands which have connected them with another, and to assume among the powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation. We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. --That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, --That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn, that mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security. Such has been the patient sufferance of these Colonies; and such is now the necessity which constrains them to alter their former Systems of Government. The history of the present King of Great Britain is a history of repeated injuries and usurpations, all having in direct object the establishment of an absolute Tyranny over these States. To prove this, let Facts be submitted to a candid world.	When in the Course of human events, it becomes necessary for one people to world the political bands which have connected them with another, and to assume among the powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation. We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. --That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, --That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn, that mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security. Such has been the patient sufferance of these Colonies; and such is now the necessity which constrains them to alter their former Systems of Government. The history of the present King of Great Britain is a history of repeated injuries and usurpations, all having in direct object the establishment of an absolute Tyranny over these States. To prove this, let Facts be submitted to a candid world.

PassText is also better than graphical passwords since storing and manipulating text requires fewer resources than working with images. In fact, it takes only a few kilobytes of space to store a PassText base text of two pages, while a complicated high-resolution graphical password may require multiple megabytes of storage. This is particularly important in the case of small screen devices, such as cell phones, on which resolution is not sufficient to display high content graphics. Unlike graphics, text is also readable by the special software used by blind people to interact with a computer, making it usable for people with impaired vision. PassText requires no colour comprehension and so is friendly towards the colour blind. Finally, it is much easier to manipulate text as compared to graphics making it better for people with poor motor coordination. Overall PassText is a much more handicapped friendly technology relative to typical graphical password approaches.

It is possible to develop a much more complicated and as a result more secure PassText model based on full capabilities of an advanced word processor such as setting different styles of the document, using different fonts, various sizes of characters and even different colours of individual letters. Most readers of this article should be fairly familiar with modern word processors and understand how many text-formatting possibilities they present. However, those additional features are purely optional as the PassText system is designed to work perfectly well within the limitations of simple plain-text manipulating software.

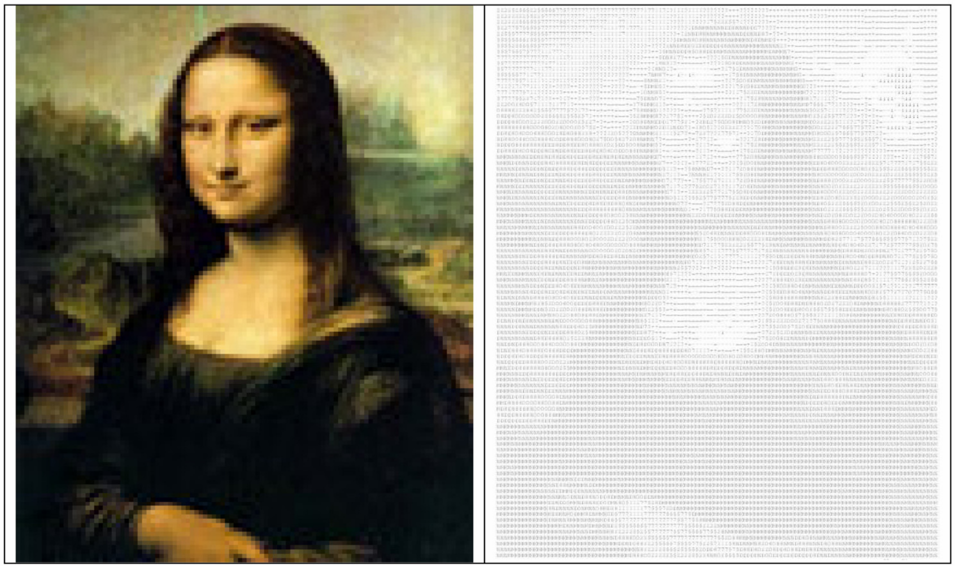
5 PassArt

Another novel user authentication approach can be based on what is commonly known as 'ASCII art' (Wikipedia, 2005). ASCII art is a graphic made out of individual characters placed together and selected from the standard 95 character printable alphabet defined by American Standard Code for Information Interchange. Two approaches to creation of ASCII images are known: either an artist manually places characters in a desired location or a computer program converts a given image file by sampling it and replacing individual pixels or pixel-regions with ASCII characters. Figure 2 shows an ASCII representation of an image file created by one of many ASCII art generating programs (Wikipedia, 2005; Wilson, 2005).

The actual algorithm for generating ASCII art is beyond the scope of this article, but it is sufficient to say what many algorithms exist and public domain converters are widely available (Wikipedia, 2005). Any image can be used as the base image regardless of colour, complexity or size for creation of ASCII art for esthetic purposes, however for our purpose of user authentication we would like to have a base image, which is not very high in resolution or picture size. This is needed to have the resulting ASCII text easily fit into a single screen with individual characters easily visible.

From that point on PassArt works, a lot like PassText also proposed by us for simplification of user authentication process (Yampolskiy, 2007e). At the PassArt creation stage also known as the enrolment stage the user is presented with a sample of ASCII art to which he is asked to make any modifications he pleases.

Figure 2 Left: original image; right: ASCII representation (see online version for colours)

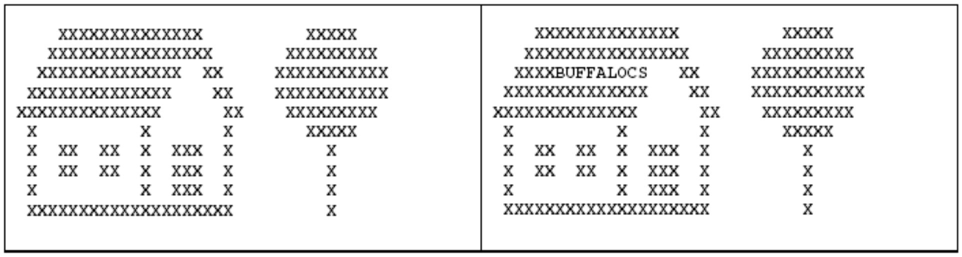


In the PassArt system of authentication, the user is not required to memorise any difficult character combinations, in fact the user is not required to memorise any text at all. User only needs to memorise the locations within the base art piece he makes the changes to. We argue that this is relatively easy since it relies on user's visual memory, which is known to be very long lasting and partially subconscious.

PassArt system does not explicitly limit the size of the base art, which can be used, depending on the desired level of security any image can be utilised as a base art from a small drawing to a Michelangelo's ceiling in the Sistine Chapel. Overall PassArt provides a password space, which cannot be searched with current computational resources. We can take an alphabet of all 95 printable characters and use a large painting made up of perhaps a million different characters giving as a PassArt space, which would not be fully searchable.

Figure 3 gives an example of how the system works and what kind of PassArt users can utilise. Due to the limited size of PassArt we can incorporate into this publication, the example is trivial and manually produced (The History of ASCII (Text) Art, 2005). For real life use much larger and automatically generated ASCII art pieces should be used, consisting of multiple characters. Given a picture of a house and a tree as a base art piece a user can for example create a simple PassArt by changing part of the roof to a text 'BUFFALOCS', which should be relatively easy to remember for someone attending Buffalo University. Any other simple word would do, or nothing at all as it is sufficient to simply delete different aspects of the base art. One may find it easier to simply remove the front window from the house all together as his unique and easy to remember PassArt.

Figure 3 Left: base ASCII image; right: PassArt example



```
    XXXXXXXXXXXXXX          XXXXX
   XXXXXXXXXXXXXXXX       XXXXXXXXX
  XXXXXXXXXXXXXX  XX     XXXXXXXXXXX
 XXXXXXXXXXXXXX    XX    XXXXXXXXXXX
XXXXXXXXXXXXXX      XX    XXXXXXXXX
 X          X       X       XXXXX
 X  XX  XX  X  XXX  X         X
 X  XX  XX  X  XXX  X         X
 X          X  XXX  X         X
 XXXXXXXXXXXXXXXXXXXX         X
```

```
    XXXXXXXXXXXXXX          XXXXX
   XXXXXXXXXXXXXXXX       XXXXXXXXX
  XXXXBUFFALOCS    XX     XXXXXXXXXXX
 XXXXXXXXXXXXXX    XX    XXXXXXXXXXX
XXXXXXXXXXXXXX      XX    XXXXXXXXX
 X          X       X       XXXXX
 X  XX  XX  X  XXX  X         X
 X  XX  XX  X  XXX  X         X
 X          X  XXX  X         X
 XXXXXXXXXXXXXXXXXXXX         X
```

PassArt is better than graphical passwords since storing and manipulating text requires fewer resources than working with images. In fact, it takes only a few kilobytes of space to store a PassArt base art of two screens in size, but a complicated high-resolution graphical password may require multiple megabytes of storage. This is particularly important in the case of small screen devices, such as cell phones, on which resolution is not sufficient to display high content graphics. Unlike graphics, text is also readable by the special software used by the blind people to interact with a computer, making it usable for people with impaired vision. PassArt requires no colour comprehension and so is friendly towards the colour blind. Finally, it is much easier to manipulate text as compared to graphics making it better for people with poor motor coordination. Overall PassArt is a much more handicapped friendly technology as compared to typical graphical password approaches.

6 PassMap

One of the main problems with passwords is that very good passwords are hard to remember and the once which are easy to remember are too short of simple to be secure. From the studies of human memory, we know that it is relatively easy to remember landmarks on a well-known journey (Mindtools, 2005). Perhaps, we can design an authentication schema based around this idea, a password which would be easy to remember and relatively quick to provide to the system, while at the same time is impossible to break with brute force alone.

The travelling salesman problem or TSP as it is known, is a classical NP-Hard problem in which a salesperson is trying to find the shortest path for visiting N cities. The formal definition of the problem states: “Find a path through a weighted graph which starts and ends at the same vertex, includes every other vertex exactly once, and minimizes the total cost of edges”(Black, 2005). Numerous approaches for solving the TSP exist, but only the brute force approach provides optimal solutions, but as a result of the magnitude of the search space it is not an option to use the brute force approach for any reasonably large network of cities.

For user authentication, we are not really concerned with solving TSP or even with the efficiency of any particular route. We are only interested in utilisation of the large search space inherent in the TSP problem and the ease of memorisation of routes enjoyed by the human long-term memory system. Initially for our user authentication system, we considered having a user provide a path among N cities as his unique access code we call a PassMap. This approach is not very user friendly, as it requires the user to remember and input a long sequence of routes between cities. An alternative would be to have some path between N cities already provided to the user and have the user make changes to the route to personalise it. This also creates a problem, as a large number of changes are needed to make the resulting path not easily discovered by brute force approach given that the original provided tour is known.

The solution we found is to relax the requirement for PassMap to visit all N cities (Yampolskiy, 2007f). A user is shown a map of some N cities with some routes selected and all other routes between all cities available, but not activated. If we treat N given cities as edges in a complete graph it has $N(N-1) / 2$ undirected edges. In a relatively standard map of just 50 cities, we have about $2^{50(50-1)/2} = 2^{1225}$ possible edge combinations. The user's PassMap consists of some modifications to the given map of routes, or in more precise terms of the set of selected and not selected edges in a sub-graph of the whole map. Since the search space is really enormous, it is safe for the user to make relatively few modifications to the base map and as a result have no problems with their memorisation. In addition, PassMap system does not explicitly limit the size of the base map, which can be used; depending on the desired level of security any map can be utilised as a base map from a small town to a map of a whole continent with hundreds of cities. Then, again it is unlikely for any application to require such extremely high level of security (Yampolskiy, 2007f).

At the PassMap creation stage also known as the enrolment stage the user is presented with a relatively large map of routes to which he is asked to make any modifications he pleases A possible list of atomic modifications includes:

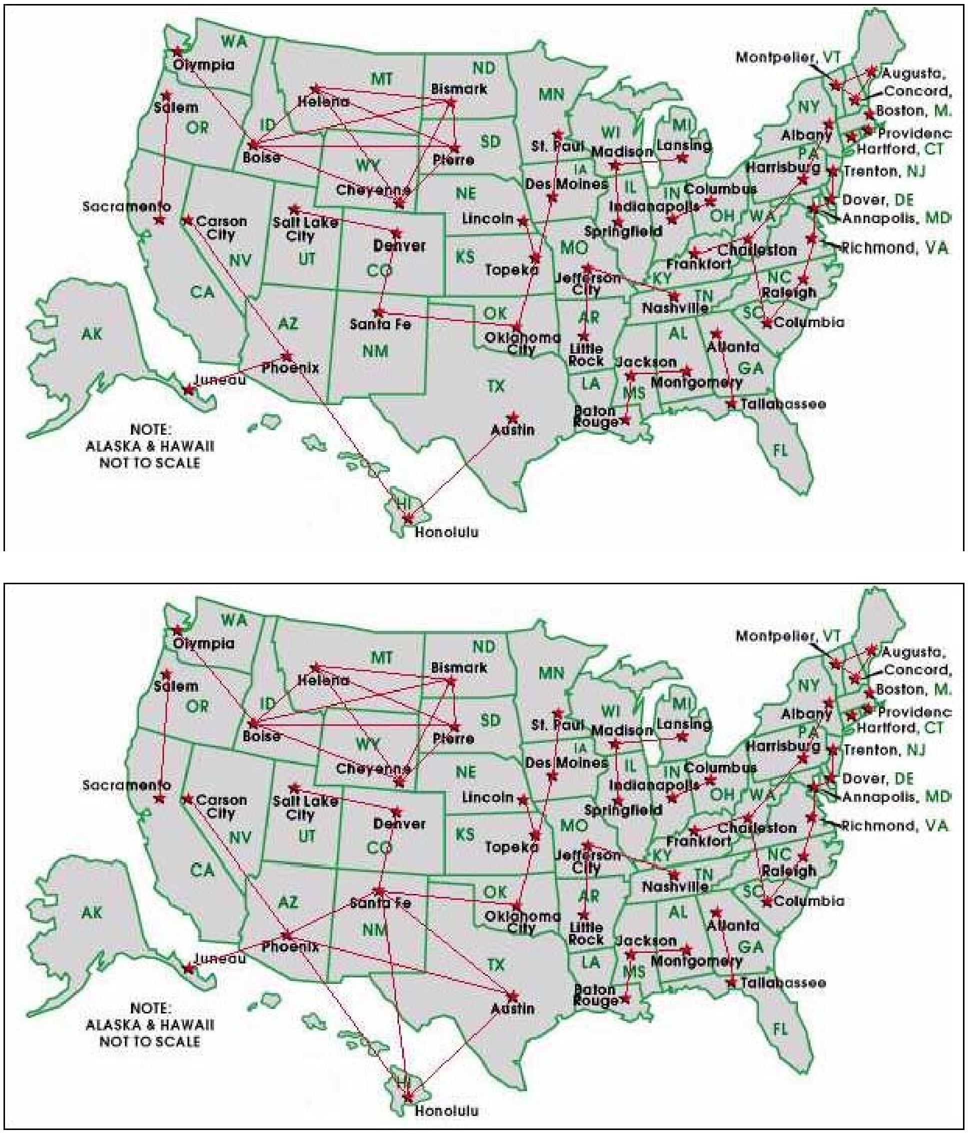
- selecting a direct route between any two cities
- un-selecting a direct route between any two cities.

Obviously, a combination of the above modifications with possible repetitions can be used to produce a unique PassMap. A user can delete whole routes, make certain cities inaccessible, provide multiple paths between any two cities and so on. A resulting PassMap is just a set of edges of a graph. To insure that the user has correctly entered his desired PassMap we might ask him to repeat it again during the enrollment stage and set it up only if the verification is successfully performed. The map itself is trivial to generate by using a simple random number generator, which assigns each possible edge to either activated or deactivated mode. Once generated, such map can be reused for multiple users and in multiple systems without any additional processing being required (Yampolskiy, 2007f).

Figure 4 demonstrate how the system works and what kind of PassMaps users can generate. Due to the limited size of maps we can incorporate into this publication, the example is simple and manually produced (Encyberpedia, 2005). Suppose, the user is presented with a map of all 50 US states with their capitals and some routes indicated as shown in Figure 4 (top). The user has great memories of Santa Fe, Austin, Honolulu and Phoenix, perhaps he met his wife in Sante Fe, his parents are from Austin, he went to school in Phoenix and always dreamed of going to Hawaii. He decided to create his PassMap by making a complete graph of those four cities or in plain terms connecting them in every way possible. Since Phoenix and Honolulu and Honolulu and Phoenix are already connected he only needs to add the four remaining edges to create his own unique PassMap. Ideally of course users should not utilise their personal information in generation of their password since someone who knows them well might be able to guess it (Yampolskiy, 2007a,f).

As an alternative example, we can use a map of Europe and a user who has never been to Europe before should have no problem memorising that he wants to one day see the Eiffel Tour in Paris, the Big Ben in London and the Kremlin in Moscow and his PassMap might be to visit all of them one at a time flying in from his hometown.

Figure 4 Top: given base map; bottom: PassMap example (see online version for colours)



Source: Encyberpedia (2005).

While the number of possible base map manipulations is truly enormous, we would like to reiterate that memorising the actual sequence leading to the creation of a secure

PassMap is very easy and can even be done for authentication on multiple systems with multiple base maps without any additional memorisation being required. For example, your PassMap might be to connect the most upper-left city with the lowest city and with most upper-right city regardless of the actual map presented to you. In addition, the PassMap technology is not very susceptible to 'shoulder-surfing' as can be clearly seen from Figure 4. Noticing a single new edge in a large graph or even an absence of some edge in the map is not a trivial task (Yampolskiy, 2007f).

7 Results and conclusions

It seems unfair to say that any set of alphanumeric characters are equally easy to commit to memory. For example, 'Ffi0o' and word 'black' are not both equal to five units of memory. We propose a new measure of password length based on a unit of memorable information (UMI). A single word is just a single UMI since we do not memorise the characters in the word one at a time, but rather as a whole. In a similar fashion, a single picture or a single point in a picture is also one UMI, just like recognition of a single face is. With respect to our PassText algorithms, a single change to the base code is also a single unit of memorable information and should be treated as such for comparison purposes with other authentication techniques.

By comparing password space for different password schemas, we can identify the most secure approaches with respect to brute force attacks while at the same time considering how good those mechanisms are in terms of how memorable they are. Table 1 demonstrates comparison of password space and password length for popular user authentication schemas.

Table 1 Comparison of password space and password length for popular user authentication schemas and for the approaches proposed in this article

Authentication system	*Alphabet*	*Password length in UMI*	*Password space size*
Password[0]	64	8 (chars)	2.8×10^{14}
Password	72	8 (chars)	7.2×10^{14}
Password	96	8 (chars)	7.2×10^{15}
Passphrase[1]	50,000	5 (words)	3.1×10^{23}
PassPoints[2]	373	5 (clicks)	7.2×10^{12}
PassPoints[3]	1,925	5 (clicks)	2.6×10^{16}
PassPoints[4]	3,928	5 (clicks)	9.3×10^{17}
Pin Number[5]	10	4 (numbers)	1×10^{4}
Text with Graphical Assistance[6]	10 (spaces)	8 (chars)	2×10^{6}
DAS[6]	5 × 5 grid	5 (elements)	5×10^{5}
DAS	5 × 5 grid	6 (elements)	1.7×10^{7}
DAS	5 × 5 grid	7 (elements)	6×10^{8}
Picture password[7]	30	8 (selections)	6.5×10^{11}

Table 1 Comparison of password space and password length for popular user authentication schemas and for the approaches proposed in this article (continued)

Authentication system	*Alphabet*	*Password length in UMI*	*Password space size*
Daja Vu	20	5 (images)	1.5×10^4
PassFace	9	5 (faces)	5.9×10^4
Check-off password	16	4 (check-offs)	1.2×10^4
Check-off password[8]	16	4 (check-offs)	7.2×10^{16}
Pass-Thought[9]	95	8 (chars)	6.6×10^{15}
PassText[10]	95	2 (changes)	2.6×10^{494}
PassText[11]	95	3 (changes)	95^{1250}
PassText[12]	95	4 (changes)	95^{2500}
PassArt[13]	95	2 (changes)	2.6×10^{494}
PassArt[14]	95	3 (changes)	95^{1250}
PassArt[15]	95	4 (changes)	95^{2500}
PassMap[16]	10	2 (changes)	3.5×10^{13}
PassMap	25	3 (changes)	2×10^{90}
PassMap	50	3 (changes)	2^{1225}

Note: [0]see Wiedenbeck et al. (2005c) for details; [1]50,000 dictionary words are taken as a working vocabulary of an adult; [2]image size 451 × 331 with grid size of 20 × 20 pixels (Wiedenbeck et al., 2005c).; [3]image size 1,024 × 752 with grid size of 20 × 20 pixels (Wiedenbeck et al., 2005c).; [4]image size 1,024 × 752 with grid size of 14 × 14 pixels (Wiedenbeck et al., 2005c). ; [5]see Angeli (2003) for details; [6]see Jermyn (1999) for details; [7]see Jansen (2005) for details; [8]if OCR not possible see Bekkering, Warkentin and Davis (2003) for details; [9]proposed system currently not feasible (Thorpe, Oorschot and Somayaji, 2005).; [10]250 chars; [11]half page of text (1,250 chars); [12]1 page of text (2,500 chars); [13]250 char ASCII art piece; [14]half page ASCII art (1,250 chars); [15]1 page ASCII art (2,500 chars); [16]for N cities we have $2^{N(N-1)/2}$ password space.

Table 1 shows that approaches presented by us are both the most secure and easiest to remember, while at the same time are relatively fast to produce during authentication procedure. PassText and PassArt do not require unreasonable graphical or computational resources and PassMap is inherently easy to remember. Each one of the proposed methods may be easier for people with certain disabilities to utilise as compared to some other authentication approaches.

PassArt is a particularly handicapped-friendly methodology since it combines positive properties of both graphical and alphanumeric passwords. By doing so, it provides a choice to the user of either relying on image or textual manipulation for entry of the password sequence depending on the nature of their disability. In terms of the password space all three approaches exhibit a password space, which is sufficient to make a brute force attack impossible. With respect to memorisation, all our methods require fewer UMI then currently utilised approaches making it easier for the user to keep track of his authentication code. Field trials are required to determine which of the three-presented approaches are preferable for use with small mobile devices.

With the goal of total computer and network security, user authentication is only the first step. A good intruder detection mechanism is also required to protect the system against those who were able to defeat its identification mechanisms. Our research outlined in Yampolskiy and Govindaraju (2006, 2007) presents a system for continuous user verification based on user's behaviour and promises to provide improved system security then coupled with one of the proposed user authentication approaches. Integration of those methodologies into a single security system is the next step in our continuing research into making computers and computer networks more secure.

References

The History of ASCII (Text) Art. Available at: http://www.acid.org/info/mirror/jgs/history.html#typography. Retrieved 21 October, 2005.

Player Id, Age Verification and Border Control Technology Forum, Nevada Interactive Gaming Task Force. Available at: http://www.nevadaigtf.org/TechnologyForum.html.. Retrieved 23 October, 2005.

The Science Behind Passfaces, *Real User Corporation*. Available at: http://www.realuser.com/, June 2004.

Angeli, A.D., Coventry, L., Johnson, G.I. and Coutts, M. (2003) 'Usability and user authentication: pictorial passwords vs. PIN', *Contemporary Ergonomics*. London,UK: Taylor and Francis, pp.253–258.

Bekkering, E., Warkentin, M. and Davis, K. (2003) 'A longitudinal comparison of four password procedures', Paper presented in the Proceedings of the *2003 Hawaii International Conference on Business*, Honolulu, HI, June.

BioPassword (2005), *Biopassword*. Available at: http://www.biopassword.com/bp2/welcome.asp. Retrieved 24 October.

Birget, J-C., Hong, D. and Memon, N. (2005) *Robust Discretization, with an Application to Graphical Passwords*. Available at: citeseer.ist.psu.edu/birget03robust.html. Retrieved 4 November.

Bishop, M. (1992) 'Proactive password checking', *4th Workshop on Computer Security Incident Handling*. Available at: citeseer.ist.psu.edu/bishop92proactive.html, August.

Black, P.E. (2005) *Traveling Salesman from Dictionary of Algorithms and Data Structures*. Available at: http://www.nist.gov/dads/HTML/travelingSalesman.html. Retrieved 22 October.

Blonder, G.E. (1996) *Graphical Passwords*, United States Pattent 5559961.

Brostoff, A. (2004) 'Improving password system effectiveness', *PhD Dissertation*, Department of Computer Science University College London, 30 September.

Davis, D., Monrose, F. and Reiter, M.K. (2004) 'On user choice in graphical password schemes', Paper presented in the Proceedings of the *13th USENIX Security Symposium*, San Diego, August.

Dhamija, R. and Perrig, A. (2000) 'Deja Vu: a user study. using Images for authentication', Paper presented in the Proceedings of the *9th USENIX Security Symposium*, Denver, Colorado August.

Encyberpedia (2005), *Encyberpedia US Map with Capitals*. Available at: http://www.encyberpedia.com/cities.htm. Retrieved 23 October.

Feldmeier, D.C. and Karn, P.R. (1989) *UNIX Password Security – Ten Years Later*, *CRYPTO*. Available at: citeseer.ist.psu.edu/188968.html, pp.44–63.

Hoanca, B. and Mock, K. (2005) 'Screen oriented technique for reducing the incidence of shoulder surfing', *The 2005 International Conference on Security and Management*, Las Vegas, 20–23 June.

Jansen, W., Gavrila, S., Korolev, V., Ayers, R. and Swanstrom, R. (2005) *Picture Password: A Visual Login Technique for Mobile Devices*. Available at: http://csrc.nist.gov/publications/nistir/nistir-7030.pdf. Retrieved 24 October.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K. and Rubin, A.D. (1999) 'The design and analysis of graphical passwords', Paper presented in the Proceedings of the *8th USENIX Security Symposium*, Washington, D.C., 23–26 August.

Klein, D.V. (1990) 'Foiling the cracker : a survey of and improvements to password security', Paper presented in the *USENIX Conference Proceedings*.

Li, S. and Shum, H-Y. (2005) *Secure Human–Computer Identification against Peeping Attacks*. Available at: citeseer.ist.psu.edu/li03secure.html. Retrieved 4 November.

Liddell, J., Renaud, K. and Angeli, A.D. (2003) 'Using a combination of sound and images to authenticate web users', *17th Annual Human Computer Interaction Conference. Designing for Society*, Bath, England, 8–12 September.

McDonald, D.L., Atkinson, R.J. and Metz, C. (1995) 'One time passwords in everything (OPIE): experiences with building and using stronger authentication', Paper presented in the Proceedings of the *Fifth USENIX UNIX Security Symposium*, Sal Lake City, Utah, June.

Mindtools (2005), *The Journey System*. Available at: http://www.mindtools.com/pages/article/newTIM_05.htm. Retrieved 22 October.

Monrose, F., Reiter, M.K. and Wetzel, S. (2001) 'Password hardening based on keystroke dynamics', *Int. J. Information Security*, Vol. 1*:*pp.69–83.

Morris, R. and Thompson, K. (1979) 'Password security: a case history', *CACM*, pp.594–597.

Nali, D. and Thorpe, J. (2004) 'Analyzing user choice in graphical passwords', *Technical Report TR-04-01*, School of Computer Science Carleton University, Canada.

Pierce, J., Wells, J., Warren, M. and Mackay, D. (2003) 'Conceptual model for graphical authentication', *1st Australian Information Security Management Conference*, Edith Cowan University, Australia.

Pointsec (2002), *PicturePINs*. Available at: http://www.pointsec.com/news/download/Pointsec_PPC_2.0_POP_PA1.pdf, November.

Porter, S. (2005) *Stronger Passwords Through Visual Authentication: Handwing*, University of Glasgow. Available at: http://www.dcs.gla.ac.uk/~porters/thesis.pdf. Retrieved 4 November.

Provos, N. and Mazieres, D. (1999) 'A future-adaptable password scheme', *USENIX Annual Technical Conference*, Monterey, California, USA, 6–11 June.

Renaud, K. (2003) 'Quantifying the quality of web authentication mechanisms. A usability perspective', *Journal of Web Engineering,* Vol. 0, Rinton Press. Available at: http://www.dcs.gla.ac.uk/~karen/Papers/j.pdf.

Renaud, K. and Smith, E. (2001) 'Jiminy: helping users to remember their passwords', *Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, Pretoria, South Africa, 25–28 September.

Ross, S. (2005) *Is It Just My Imagination?*. Available at: http://research.microsoft.com/display Article.aspx?id=417. Retrieved 4 November.

Rubin, A.D. (1995) 'Independent one-time passwords', Paper presented in the Proceedings of the *5th Security Symposium USENIX Association*, Berkeley, CA, June.

Spafford, E. (2005) *Observing Reusable Password Choices*. Available at: citeseer.ist.psu.edu/spafford92observing.html. Retrieved 3 November.

Sobrado, L. and Birget, J-C. (2005) *Graphical Passwords.* Available at: http://rutgersscholar .rutgers.edu/volume04/sobrbirg/sobrbirg.htm. Retrieved 3 November.

Thorpe, J. and Oorschot, P.v. (2004a) 'Graphical Dictionaries and the Memorable Space of Graphical Passwords', *13th USENIX Security Symposium*, pp.135–150.

Thorpe, J. and Oorschot, P.v. (2004b) 'Towards secure design choices for implementing graphical passwords', *20th Annual Computer Security Applications Conference*, Tucson, Arizona 6–10 December.

Thorpe, J., Oorschot, P.C.v. and Somayaji, A. (2005) *Pass-Thoughts: Authenticating with Our Minds*. Available at: citeseer.ist.psu.edu/thorpe05passthoughts.html. Retrieved 23 October.

Varenhorst, C. (2004) *Passdoodles: A Lightweight Authentication Method*. Available at: http://people.csail.mit.edu/emax/papers/varenhorst.pdf, 27 July.

Weinshall, D. and Kirkpatrick, S. (2005) *Passwords You'll Never Forget, But Can't Recall*. Available at: http://www.cs.huji.ac.il/~kirk/Imprint_CHI04_final.pdf. Retrieved 24 October.

Wiedenbeck, S., Waters, J., Birget, J-C., Brodskiy, A. and Memon, N. (2005a) *Authentication Using Graphical Passwords: Basic Results*. Available at: http://clam.rutgers.edu/~birget/grPssw/susan3.pdf. Retrieved 23 October.

Wiedenbeck, S., Waters, J., Birget, J-C., Brodskiy, A. and Memon, N. (2005b) 'Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice', *ACM International Conference Proceeding Series Vol*. 93, Paper presented in the Proceedings of the *2005 symposium on Usable privacy and security* Pittsburgh, Pennsylvania.

Wiedenbeck, S., Waters, J., Birget, J-C., Brodskiy, A. and Memon, N. (2005c) 'Passpoints: design and longitudinal evaluation of a graphical password system', *Int. J. Human–Computer Studies*, Vol. 63, Elsevier Science, July.

Wikipedia (2005) *ASCII Art*. Available at: http://en.wikipedia.org/wiki/Ascii_Art. Retrieved 21 October.

Wilson, S. (2005) *ASCII Artist*, http://www.glassgiant.com/. Retrieved 21 October.

Yampolskiy, R.V. (2006) 'Analyzing user password selection behavior for reduction of password space', *The IEEE International Carnahan Conference on Security Technology (ICCST06)*, Lexington, Kentucky, 17–19 October.

Yampolskiy, R.V. (2007a) 'Enhanced passwords for improved network security', *IEEE Upstate NY Workshop on Communications and Networks '07*, Syracuse, New York, 9 November.

Yampolskiy, R.V. (2007b) 'Human computer interaction based intrusion detection', *4th International Conference on Information Technology: New Generations (ITNG 2007)*, Las Vegas, Nevada, USA, 2–4 April.

Yampolskiy, R.V. (2007c) 'Indirect human computer interaction-based biometrics for intrusion detection system*s*', *The 41st Annual IEEE International Carnahan Conference on Security Technology (ICCST2007)*, Ottawa, Canada, 9–11 October.

Yampolskiy, R.V. (2007d) 'Motor-skill based biometrics in assuring business processes', Paper presented in the Proceedings of the *6th Annual Security Conference*, Ed. G. Dhillon. Global Publishing, Las Vegas, NV, USA, 11–12 April.

Yampolskiy, R.V. (2007e) 'Secure network authentication with passtext', *4th International Conference on Information Technology: New Generations (ITNG 2007)*, Las Vegas, Nevada, USA, 2–4 April.

Yampolskiy, R.V. (2007f) 'User authentication via behavior based passwords', *The Third Annual IEEE Long Island Systems Applications and Technology Conference (LISAT2007)*, Farmingdale, New York, 4 May.

Yampolskiy, R.V. and Govindaraju, V. (2006) 'Use of behavioral biometrics in intrusion detection and online gaming, biometric technology for human identification', *III. SPIE Defense and Security Symposium*, Orlando, Florida, 17–22 April.

Yampolskiy, R.V. and Govindaraju, V. (2007) 'Dissimilarity functions for behavior-based biometrics, biometric technology for human identification IV', *SPIE Defense and Security Symposium*, Orlando, Florida, 9–13 April.