User Authentication via Behavior Based Passwords

Roman V. Yampolskiy

Abstract— **Computer security to a degree depends on trustworthy user authentication; unfortunately currently used passwords are not completely secure or user friendly. One of the main problems with passwords is that good passwords are hard to remember and the ones which are easy to remember are too short to be secure. We have designed a graphical authentication schema with a password, which is 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. We have also proposed a way to measure password length and compared password space sizes of many popular authentication schemas against the one proposed in this paper.**

Index Terms— **Authentication, Graphical Password, Password Space, Security.**

I. 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 authorized 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 [45].

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 [8, 32, 30, 4, 25] . Currently most research in user authentication is geared towards graphical passwords, but such methodologies present problems of their own. In this paper we present a user authentication approach, that is both easy to remember and provides a very high level of security not threatened by a brute force attack with significant computational resources. After our methodology is presented it is compared to other commonly used authentication mechanisms in terms of how easy it is to remember and with respect to the password space size [45]. The results of the comparison are favorable for our approach.

II. Existing Authentication Mechanisms

Many researchers have recognized 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 used by Yampolskiy [47] and originally proposed by Renaud [31] 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 [49]. 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 paper.

A. 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. The three approaches presented below all require additional hardware, and two out of three also rely on some form of biometric for improved accuracy of user authentication. It is obvious that the geographic location alone is not sufficient information for secure user authentication, as multiple scenarios exist where an intruder may end up in an approved location without being properly authorized [49].

1) IP filtering

This is a way to identify the location from which the user is connecting to the server, an assumption is made that if the service provider and or geographic location associated with the 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. ”Where direct broadband connections such as cable modem, DSL, or T1 services are used, this mechanism is virtually foolproof. Where dialup to the ISP is used, these filtering systems lack an ability to accurately identify location. These systems can be used to allow connections through known ISP's 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

1-4244-1302-8/07/$25.00 ©2007 IEEE

mechanism that will deny many users who are in fact geographically acceptable, but assures that anyone permitted within the filter is within the jurisdiction" [15].

2) GeoBio Indicator

A device consisting of an integrated GPS based geographical indicator and a biometric-based smart card that is attached to a personal computer via the Universal Serial Bus 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 [15]. Along with other problems in this approach are privacy issues inevitably raised by integration of biometric and geographic information in one data-system.

3) Phone Call Verification

Represents a method utilizing a synchronized 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" [15]. 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.

B. 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 [47]. Behavioral biometrics based on keystroke dynamics [24], mouse usage patterns or signature dynamics do not require any special hardware and can be utilized for reliable user authentication. In this section we present two interesting user authentication schemas based on biometrics. First we introduce BioPassword a system based on keyboard dynamics followed by Pass-Thought system a proposed futuristic approach requiring special hardware to make scanning of a user's thought patterns possible.

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 [3]. 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) Pass-Thoughts

Thorpe et al. 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 recorded and 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 [37].

C. 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 [47]. The authentication schemas based on what a user knows can be grouped into two classes: Text based and Graphics based.

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 memorize a sequence of characters or words. The sequence can either be generated for the user or user selected [31]. The problem is that a user's ability to memorize 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) [2] 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 8 different characters selected from the sixteen most commonly used letters. The user may use any character more then 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 [31] 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-based 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 [22, 34]. 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) 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 based 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 [9, 10]. It relies on the ease with which people recognize familiar faces. During enrollment, a user is presented with a set of faces he is asked to memorize. 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 59050 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 5 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 [12].

The two systems mentioned above are probably representative of many other similar recognition based graphical authentication systems currently in existence. Visual Identification Protocol [31, 1], Picture Password [17], and PicturePins [28] 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 paper 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 [42, 44]. This is similar to the methodology used in the original patent for graphical passwords obtained by Blonder in 1996 [7].

An alternative to having a user select a portion of an image is to have a user input a simple drawing into a predefined grid space. This approach is attempted in [40] with a system called Passdoodles and also in [18, 39] with a system called Draw-a-Secret. Finally, a V-go Password requests a user to perform simulation of simple actions such as mixing a cocktail using a graphical interface [31].

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 [18], Authentigraph [27], Pseudoword recognition [41], Image with Sound [21], Triangle and Movable Frame schema [35], Inkblot reminder [33], Handwriting reminders [29], and Artificial Grammar Learning [41] are only mentioned here so that an interested reader can investigate them further.

III. 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 [45].

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[5, 19, 14, 36]. For example the following set of restrictions on alphanumeric password choices is given by Klein [19]:

- 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 capitalized
- Passwords which match a reversed word in the dictionary

- Passwords which match a reversed word in the dictionary with some or all letters capitalized
- 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 [47].

Drawbacks of graphical passwords are numerous; we will start with the problems graphical passwords present to handicapped individuals. First people with impaired vision will have a problem with most graphical passwords particularly those employing images with many small details. Those users typically depend on a 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 mouse or any other similar pointing device and so may experience some difficulty in using graphical passwords particularly those based on selection of small subparts of an image, such as PassPoints. People with certain other types of visual problems such as colorblindness may also experience problems with graphical passwords dependent on colorful images [44].

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 memorization 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 can’t deal well with systems like PassFaces [31]. 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 the most of the more popular graphical password methodologies [45].

- In a Draw-a-Secret (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 to 3 strokes and are centered [26, 38]. 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. Additionally 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 [43].
- 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 then 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. So if demographic information about the user is available it becomes possible to greatly narrow the password space for a system like PassFaces. If the system does not permit users to select their own passwords it becomes more difficult for users to remember such faces as they are often from a different race, and so more difficult to distinguish and remember [11].

Another significant drawback of graphical passwords is the so-called shoulder surfing problem [47]. 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 GP. A person who observes a few login sessions could eventually realize what the password is or obtain information making the guessing of the password much easier. Sobrado et al. [35] propose a shoulder surfing secure graphical password schema, however it requires over a 1000 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. Additionally a lengthy, 10 step, sequence is required for secure authentication. A similar but somewhat modified approach is presented in Hoanca et al. [16] and a broad overview of solutions to the shoulder surfing problem is given by Li et al. [20].

IV. 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 [23]. 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 impossible to break with brute force alone.

The Traveling 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" [6]. Numerous approaches for solving the TSP exist, but only the brute force approach provides optimal solution, 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 utilization of the large search space inherent in the TSP problem and the ease of memorization 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 personalize 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. 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 memorization. Additionally 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 utilized 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.

At the PassMap creation stage also known as the enrollment 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 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.

A potential search space for classical passwords is considered to be secure as long as the users select passwords with equal probability from all possible combinations of characters. However in reality many short, simple passwords are used making it possible to guess them or to find them by a brute force attack. Perhaps a similar problem may take place with the PassMap system. Users may attempt to save time by making only minimal changes to the base map or not making any changes at all. The system should require a minimum number of atomic operations before a new PassMap is approved. PassMap created by making no changes to the base map, deleting or adding just one edge in the graph should not be allowed.

In the PassMap system of authentication the user is not required to memorize any difficult character combinations such as D@$0o#bk2. The user only needs to memorize the sequence of changes he makes to the base map. We argue that this is relatively easy since human memory is predisposed to memorizing routes [23]. Also the choice of the base map can be made to reflect the user's previous knowledge without sacrificing the security aspect of the system. In fact a system can be designed with customizable options for each user:

1. The default option is for all users to be presented with a common map. For example the map of USA can serve as a widely known base map example.
2. A user can select an option of having his user name associated with a particular map from a list of possible base maps (a more secure but less convenient option is for user to select a map from a larger list of maps).
3. Another option is for a user to provide his own base map file, but this might be a problem for login from remote systems, which may not have immediate access to the user's chosen base map file. The system might also encounter problems with converting a map file provided by the user to a proper complete graph format.

Perhaps an example is in order to demonstrate how the system works and what kind of PassMap users can generate. Due to the limited size of maps we can incorporate into this publication, the example is simple and manually produced [13]. Suppose the user is presented with a map of all 50 US states with their capitals and some routes indicated as shown in Figure 1. 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 utilize their personal information in generation of their password since someone who knows them well might be able to guess it.

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 memorizing 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.

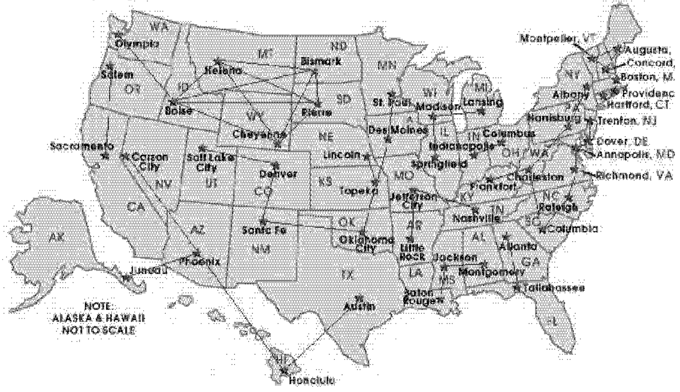


Fig 2. Given base Map.

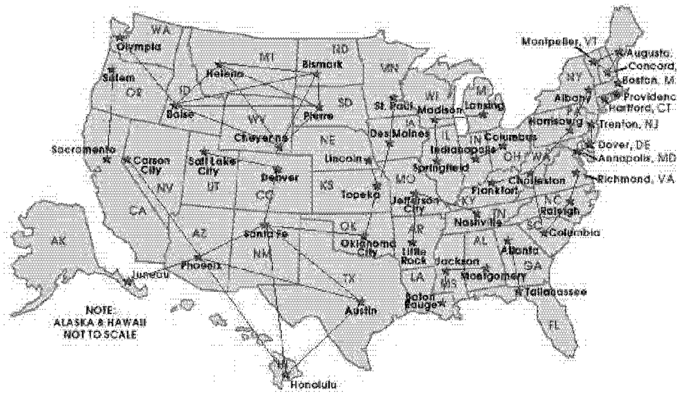


Fig. 2. PassMap example [13]

While the number of possible base map manipulations is truly enormous we would like to reiterate that memorizing 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 memorization 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. Additionally the PassMap technology is not very susceptible to "shoulder surfing" as can be clearly seen from Figure 1. Noticing a single new edge in a large graph or even an absence of some edge in the map is not a trivial task, for someone just passing by.

V. RESULTS AND CONCLUSIONS

It seems unfair to say that any n alphanumeric characters are equally easy to commit to memory. For example "Ffi0o" and the 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 memorize 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 [47]. With respect to our PassMap algorithm 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 and for the approach proposed in this paper [47].

TABLE 1
PASSWORD SPACE VS. PASSWORD LENGTH

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^{14}
PassPhrase[1]	50000	5 (words)	3.1×10^{23}
PassPoints[2]	373	5 (clicks)	7.2×10^{12}
PassPoints[3]	1925	5 (clicks)	2.6×10^{16}
PassPoints[4]	3928	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 x 5 grid	5 (elements)	5×10^{5}
DAS	5 x 5 grid	6 (elements)	1.7×10^{7}
DAS	5 x 5 grid	7 (elements)	6×10^{8}
Picture Password[7]	30	8 (selections)	6.5×10^{11}
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}
PassThought[9]	95	8 (chars)	6.6×10^{15}
PassMap[10]	10	2 (changes)	3.5×10^{13}
PassMap	25	3 (changes)	2×10^{90}
PassMap	50	3 (changes)	2^{1225}

0: see [44] for details. 1: 50000 dictionary words are taken as a working vocabulary of an adult. 2: image size 451 x 331 with grid size of 20 x 20 pixels [44]. 3: image size 1024 x 752 with grid size of 20 x 20 pixels [44]. 4: image size 1024 x 752 with grid size of 14 x 14 pixels [44]. 5: see [1] for details. 6: see [18] for details. 7: see [17] for details. 8: if OCR not possible see [2] for details. 9: proposed system currently not feasible [37]. 10: for N cities we have $2^{N(N-1)/2}$ password space.

Table 1 shows that the approach presented by us is both the most secure and the easiest to remember. At the same time, it is relatively fast to produce during an authentication procedure. 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 previous research [49, 46, 48] presents a system for continuous user verification based on user's behavior and promises to provide improved system security then coupled with the proposed user authentication approach. Integration of those two methodologies into a single security system is the next step in our continuing quest into making computers and computer networks more secure.

REFERENCES

[1] A. D. Angeli, L. Coventry, G. I. Johnson and M. Coutts., *Usability and user authentication: Pictorial passwords vs. PIN., Contemporary Ergonomics, pages 253–258.*, Taylor & Francis, London, 2003.

[2] E. Bekkering, M. Warkentin and K. Davis, *A Longitudinal Comparison of Four Password Procedures, Proceedings of the 2003 Hawaii International Conference on Business*, Honolulu, HI, June 2003.

[3] BioPassword, *Biopassword*, Available at: www. biopassword.com/bp2/welcome.asp, Retrieved October 24, 2005.

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

[5] M. Bishop, *Proactive Password Checking, 4th Workshop on Computer Security Incident Handling*, Available at: citeseer.ist.psu.edu/bishop92proactive.html, August 1992.

[6] P. E. Black, *Traveling salesman from Dictionary of Algorithms and Data Structures*, Available at: www.nist.gov /dads/HTML/travelingSalesman.html, Retrieved October 22, 2005.

[7] G. E. Blonder, *Graphical Passwords, United States Pattent 5559961*, 1996.

[8] A. Brostoff, *Improving Password System Effectivness, PhD Dissertation*, Department of Computer Science University College London, September 30, 2004.

[9] S. Brostoff and M. A. Sasse, *Are Passfaces More Usable Than Passwords? A Field Trial Investigation, Proceedings of CHI 2000, People and Computers XIV, pp. 405 - 424*, Springer, September 2000.

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

[11] D. Davis, F. Monrose and M. K. Reiter, *On user choice in Graphical Password Schemes, In Proceedings of the 13th USENIX Security Symposium*, San Diego, August 2004.

[12] R. Dhamija and A. Perrig, *Deja Vu: A User Study. Using Images for Authentication, Proceedings of the 9th USENIX Security Symposium*, Denver, Colorado, August 2000.

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

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

[15] N. I. G. T. Force., *Player id, age verification and border control technology forum.*, Available at: www.nevadaigtf.org/TechnologyForum.html., Retrieved October 23, 2005.

[16] B. Hoanca and K. Mock, *Screen oriented technique for reducing the incidence of shoulder surfing, The 2005 Internation Conference on Security and Management*, Las Vegas, June 20-23, 2005.

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

[18] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, *The Design and Analysis of Graphical Passwords, Proceedings of the 8th USENIX Security Symposium*, Washington, D.C., August 23-36, 1999.

[19] D. V. Klein, *Foiling the cracker: A survey of and improvements to password security, USENIX Conference Proceedings*, 1990.

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

[21] J. Liddell, K. Renaud and A. D. Angeli, *Using a Combination of Sound and Images to Authenticate Web Users, 17th Annual Human Computer Interaction Conference. Designing for Society*, Bath, England, 8-12 Sept, 2003.

[22] D. L. McDonald, R. J. Atkinson and C. Metz, *One Time Passwords In Everything (OPIE): Experiences with Building and Using Stronger Authentication, Proceedings of teh Fifth USENIX UNIX Security Symposium*, Sal Lake City, Utah, June 1995.

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

[24] F. Monrose, M. K. Reiter and S. Wetzel, *Password Hardening based on Keystroke Dynamics*, *International Journal of Information Security, 1(1):69--83*, 2001.

[25] R. Morris and K. Thompson, *Password Security: a Case History*, *CACM*, 1979, pp. 594--597.

[26] D. Nali and J. Thorpe., *Analyzing User Choice in Graphical Passwords., Tech. Report TR-04-01, School of Computer Science Carleton University*, Canada, 2004.

[27] J. Pierce, J. Wells, M. Warren and D. Mackay, *Conceptual Model for Graphical Authentication*, *1st Australian Information Security Management Conference*, Edith Cowan University, Australia, 2003.

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

[29] S. Porter, *Stronger Passwords through Visual Authentication: handwing*, *University of Glasgow.*, Available at: http://www.dcs.gla.ac.uk/~porters/thesis.pdf, Retrieved November 4, 2005.

[30] N. Provos and D. Mazieres, *A Future-Adaptable Password Scheme*, *USENIX Annual Technical Conference*, Monterey, California, USA, June 6-11, 1999.

[31] K. Renaud, *Quantifying the Quality of Web Authentication Mechanisms. A Usability Perspective*, *Journal of Web Engineering, Vol. 0, No. 0,* Rinton Press, Available at: http://www.dcs.gla.ac.uk/~karen/Papers/j.pdf, 2003.

[32] K. Renaud and E. Smith, *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 2001.

[33] S. Ross, *Is It Just My Imagination?* Available at: http://research.microsoft.com/displayArticle.aspx?id=417, Retrieved November 4, 2005.

[34] A. D. Rubin, *Independent one-time passwords*, *Proceedings of the 5th Security Symposium USENIX Association*, Berkeley, CA, June 1995.

[35] L. Sobrado and J.-C. Birget, *Graphical passwords*, Available at: http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm, Retrieved November 3, 2005.

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

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

[38] J. Thorpe and P. v. Oorschot, *Graphical Dictionaries and the Memorable Space of Graphical Passwords*, *13th USENIX Security Symposium*, pp. 135–150.

[39] J. Thorpe and P. v. Oorschot, *Towards Secure Design Choices For Implementing Graphical Passwords*, *20th Annual Computer Security Applications Conference*, Tucson, Arizona, December 6-10, 2004.

[40] C. Varenhorst, *Passdoodles; a Lightweight Authentication Method*, Available at: http://people.csail.mit.edu/emax/papers/varenhorst.pdf, July 27, 2004.

[41] D. Weinshall and S. Kirkpatrick, *Passwords you'll never forget, but can't recall*, *Available at:* ***http://www.cs.huji.ac.il/~kirk/Imprint_CHI04_final.pdf***, Retrieved October 24, 2005.

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

[43] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy and N. Memon, *Authentication using graphical passwords: effects of tolerance and image choice*, *ACM International Conference Proceeding Series; Vol. 93, Proceedings of the 2005 symposium on Usable privacy and security*, Pittsburgh, Pennsylvania, 2005.

[44] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy and N. Memon, *PassPoints: Design and Longitudinal Evaluation of a Graphical Password System*, *International Journal of Human-Computer Studies, Volume 63, Issues 1-2*, Elsevier Science, July 2005.

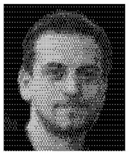
[45] R. V. Yampolskiy, *Analyzing User Password Selection Behavior for Reduction of Password Space*, *The IEEE International Carnahan Conference on Security Technology (ICCST06)*, Lexington, Kentucky, October 17-19, 2006.

[46] R. V. Yampolskiy, *Behavior Based Identification of Network Intruders*, *19th Annual CSE Graduate Conference (Grad-Conf2006)*, Buffalo, NY, February 24, 2006.

[47] R. V. Yampolskiy, *Secure Network Authentication with PassText*, *4th International Conference on Information Technology: New Generations (ITNG 2007)*, Las Vegas, Nevada, USA, April 2-4, 2007.

[48] R. V. Yampolskiy and V. Govindaraju, *Similarity Measure Functions for Strategy-Based Biometrics.*, *International Conference on Signal Processing (ICSP 2006)*, Vienna, Austria, December 16-18, 2006.

[49] R. V. Yampolskiy and V. Govindaraju, *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 2006.



Roman V. Yampolskiy holds an MS in Computer Science degree from Rochester Institute of Technology (2002) and is a PhD candidate in the department of Computer Science and Engineering at the University at Buffalo. His studies are supported by the National Science Foundation IGERT fellowship. Roman's main areas of interest are artificial intelligence, behavioral biometrics and intrusion detection. Roman has a number of publications describing his research in neural networks, genetic algorithms, pattern recognition and behavioral profiling.