Image Authentication Using PDA'S

M.L.Kalavathi M.Tech 2nd Year Student, Dr.KISHORE KUMAR M.Tech, P.Hd, Guide, H.O.D Of Nist College

Abstract

Adequate user authentication is a persistent problem, particularly with mobile devices such as Personal Digital Assistants (PDAs), which tend to be highly personal and at the fringes of an organization's influence. Yet these devices are being used increasingly in military and government agencies, hospitals, and other business settings, where they pose a risk to security and privacy, not only from sensitive information they may contain, but also from the means they typically offer to access such information over wireless networks. User authentication is the first line of defence for a mobile device that falls into the hands of an unauthorized individual. However, motivating users to enable simple PIN or password mechanisms and periodically update their authentication information is difficult at best. This paper describes a general-purpose mechanism for authenticating users through image selection. The underlying rationale is that image recall is an easy and natural way for users to authenticate, removing a serious barrier to users' compliance with corporate policy. The approach described distinguishes itself from other attempts in this area in several ways, including style dependent image selection, password reuse, and embedded salting, which collectively overcome a number of problems in employing knowledge-based authentication on mobile devices.

Keywords: user authentication, mobile devices, computer

1 Introduction

The current trend toward a highly mobile workforce has spurred the acquisition of handheld devices such as Personal Digital Assistants (PDAs). Handheld

1 The identification of commercial firms or products does not imply recommendation or endorsement by the National Institute of Standards and Technology. devices are characterized by small physical size, limited computing resources and battery life, and the means for exchanging data with a more capable notebook or desktop computer. They also support interfaces oriented toward mobility, for example, a touch screen and a microphone in place of a keyboard. One or more wireless interfaces, such as infrared (e.g., IrDA) or radio (e.g., Bluetooth, WiFi, GSM/GPRS), are usually built-in for both local and wide area communications. Most handheld devices can be configured to send and receive electronic mail and browse the Internet. While such devices have their limitations, they offer productivity tools in a compact form and at relatively low cost, and are quickly becoming ubiquitous in today's business environment.

Security-related issues loom over the use of such devices, however, including the following items:

- Handheld devices gradually accrue sensitive information and over time gain access to wireless services and organizational intranets.

- Because of their small size, handheld devices may be temporarily misplaced, lost, or stolen, and thereby exposed to an unauthorized individual.

- If user authentication is not enabled, a common default, the device's contents and network services fall under the control of whoever possesses it.

- Even if user authentication is enabled, the authentication mechanism may be weak (e.g., a four number PIN) or easily circumvented [1].

- Once authentication is enabled, renewing the authentication information periodically is seldom user initiated.

Enabling user authentication and accurately verifying an individual's claimed identity is the first line of defence against unauthorized use of a handheld device. Three basic techniques commonly used to verify identity involve either some information known by an individual (i.e., knowledge-based authentication), something possessed by an individual (i.e., token-based authentication), or some measurement taken of an individual's physiological or behavioural traits (i.e., biometric-based authentication). Implementing authentication solutions on handheld devices can be problematic. For example, hardware tokens drain power and biometric scanners can be cumbersome to interface and use.

Knowledge-based mechanisms involving passwords are the oldest and most common form of authentication technique in use today. Password systems are straightforward to implement on most devices. While password systems can be effective, users tend to undermine them by using easily remembered character strings as their password (e.g., "password"), which an intruder may easily guess or systematically match against dictionaries of such commonly used strings [2, 3]. To combat weak passwords, organizations apply measures that compel users to include special, uppercase, and numerical characters in their password string, to change passwords regularly (e.g., every 90 days) with completely different strings, and to avoid common or easily guessed strings [4]. Unfortunately, the measures put in place to ensure strong passwords usually result in complex and meaningless passwords that users often need to record and keep near the computer system to recall quickly.

The method described in this paper authenticates a user to a device using a visual login technique called Picture Password. Its aim is to give users a simple and intuitive means of authentication through image selection that avoids the pitfalls of alphanumeric passwords, yet is as effective a mechanism.

2 Background

The strength of password systems lies in the large set of character strings possible, from which an intruder would have to identify the one needed to impersonate a specific user. For example, for an eight-character string populated from the set of 95 printable ASCII keyboard characters, the number of distinct strings is 95^8. Password controls that eliminate weak passwords reduce the size of the password space somewhat, and computer systems that support multiple users offer an even broader target base to an intruder. Nevertheless, passwords remain a cost-effective solution that serves as the benchmark for other authentication techniques. Researchers continually look at ways to improve password systems. Experimental results, suggesting human memory is well suited to visual and cognitive tasks involving the recall and selection of images, have stimulated the development of visual login techniques. Image selection inherently avoids traditional dictionary attacks and is especially relevant to PDAs and other devices that interact via a touch screen and stylus.

The earliest general description of a system and method for applying graphical passwords to a handheld device appears in United States Patent 5,559,961 [5]. The authentication mechanism displays a set of image areas or cells that comprise a single graphical image. To enter a password, the user selects and repositions some of the cells in a sequence with an area of the display. The mechanism then uses the selected sequence of cells as a password, though no details are given of how the mechanism uses this information. One drawback for small size screens is that the cells, which in effect form the alphabet for composing a password, may provide a smaller size alphabet compared with alphanumeric passwords. That is, while more cells result in a larger alphabet, their size is diminished, which at some point makes it difficult to select one from another using a pointing device, resulting in entry errors.

Visual Key [6] is a commercial product that also uses cells of a single graphical image as the password elements. A user selects a specific sequence of image areas (e.g., objects in the image) from the display to authenticate. A selection grid, kept hidden from the user, logically divides a single image into individual cells. During selection, the grid is dynamically adjusted so that cell centres align with their respective touch points. The strength of the password depends on the effective size of the password alphabet, which directly corresponds to the number of cells that make up the image. Approximately 85 distinct cells with a size of 30x30 pixels can fit on a standard size 240x320 pixel display of a PDA. This yields a smaller size alphabet than that available with alphanumeric passwords. Another limitation is that, because the cell boundaries are invisible, no visual cues exist to help determine areas of the image to select, if a selected object in the image encompasses more than one cell. Moreover, cells comprising 30x30 pixels or less are a bit small, which can contribute to selection errors.

PointSec for Pocket PC [7] is a commercial product that includes several authentication-related components that can be managed centrally. PicturePIN is

a graphical counterpart to a numeric PIN system, which uses pictograms rather than numbers for entering a code via a keypad-like layout of 10 keys. The symbols are intended to form a mnemonic phrase, such as the four-symbol sequence of - men / - love / - to listen / - to music. The sequence of symbols can be 4-13 symbols long. To increase security against a bystander observing hand motion and inferring the PIN, the symbols are scrambled at each login. PicturePIN, with a limited alphabet size of 10 items, is equivalent in strength to a numeric PIN. Even if more symbol keys populated the screen, the same tradeoffs between cell size, selection errors, and password strength would arise as with visual Key and result in the same upper limit on alphabet size. SafeGuard PDA [8] is another commercial product whose Symbol PIN authentication technique works nearly identically and with the same limitations.

3 Picture Password

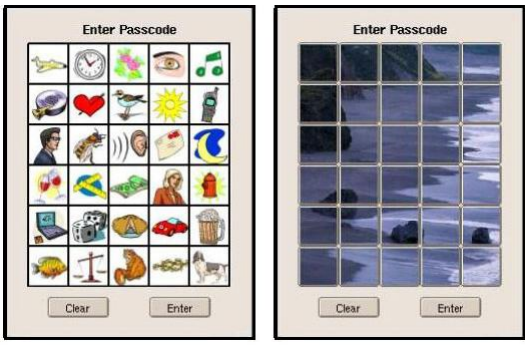
The visual login techniques described above face two main problems. First, due to screen size limitations, the size of the alphabet is smaller compared with traditional alphanumeric passwords, resulting in a weaker mechanism. Second, the user must select and remember a new set of images or image areas periodically whenever a password expires, which raises the level of difficulty for a user, especially if done within the context of the previous image set. Picture Password was devised to overcome both of these problems.

As with textual password authentication mechanisms, Picture Password uses elements of an alphabet to form a password entry of a given length. However, instead of the user having to remember a string of random-like alphanumeric characters, the sequence of images that form a passcode must be recalled and selected. Moreover, an image sequence that has some meaning or is of interest to the individual user (e.g., images of sport team logos in order of preference) can be used. If forgotten, the sequence may be reconstructed from the inherent visual cues.

3.1 User Interface

The presentation of visual images to the user for selection is based on tiling an area of the graphical interface window with thumbnail images. Various ways exist to tile an area, the simplest being squares of identical size grouped into a

two-dimensional matrix. The surface of each tile displays a bit-mapped representation of some thumbnail image supplied in a predefined digital format. The goal is to strike a balance between providing clear recognizable and easily selectable images within the display area and having a sufficient number to enable the formation of strong passwords. Picture Password uses a template of 30 identically sized squares for its thumbnail images, grouped into a 5x6 matrix, as shown in the PDA screen shots in Figure 1.



A message area at the top of the display guides the user actions. The buttons at the bottom allow the user to clear out incorrect input or submit an entered image sequence for verification. When an image sequence is initially enrolled, users can choose from among several available predefined themes. An option exists to shuffle images between authentication attempts, where appropriate for the theme, to make input monitoring by a bystander difficult. While each thumbnail image is distinct and individually recognizable, several of them may be used collectively to form a larger mosaic image. Users may define new themes using a theme builder tool and their own images.

Image selection and other interactions are done with an available pointing device – a stylus in the case of most PDAs. Two styles of thumbnail image selection are provided: individual selection and paired selection. Individual selection requires choosing a single thumbnail, which represents one element of the alphabet. Paired selection requires choosing and linking a pair of consecutively selected thumbnail images, which when coupled this way also represent one

2 (Images at left) Copyright of Hemera Technologies Inc. All rights reserved. element of the alphabet. The idea is similar to using a shift key to select uppercase or special characters on a traditional keyboard. In this setting, however, each thumbnail image can serve as a shift key for every other image.

Individual selection is done with a quick single pick of the stylus on a thumbnail image. Paired selection requires a touch and hold of the stylus for the first image, such that the stylus rests on a thumbnail image until it is highlighted, followed by a quick single pick of the second image. Using similar but distinct styles of selection offers significant benefits. First, it greatly expands the effective alphabet. Second, the subtle differences in selection style make eavesdropping difficult, especially since the narrow viewing angle of most handheld device screens already limit the viewing ability of a bystander.

The number of alphabet elements that a user can select when enrolling an image sequence is determined by the number of singly selectable thumbnail images, n, plus the number of possible paired thumbnail images selectable, n*(n-1), if a thumbnail image is not paired with itself, or n*n, if self pairing is allowed. For the 5x6 image matrix used, the total number of selectable elements with self-pairing allowed is 30+(30*30) or 930 in total. The result compares favourably with the conventional 95 printable ASCII character alphabet and significantly overshadows virtual keyboard emulation used on many PDAs, where a touch screen and stylus often prove cumbersome for entering characters.

With an effective alphabet size of 930, the resulting password space becomes

extremely large. For example, 7-entry long passcodes have 930^7 possible values or a password space of approximately 6.017e+20, which is an order of magnitude greater than that for 10-character long passwords formed from the 95 printable ASCII character set whose password space is 95^{10} or approximately 5.987e+19. The general relationship between the password spaces of passwords formed these two ways can be represented using the following formula:

$$\lceil Lt \cdot Lp \times \rceil = 32, \quad (1)$$

where Lt is the required character length for textual password input, Lp is the corresponding passcode length required for Picture Password, and ⌈y⌉ denotes the ceiling function (i.e., the least integer greater than or equal to y). In simple terms this means that the length of a passcode formed using a 5x6 image matrix is approximately one-third less than that of a traditional alphanumeric password, yet results in a comparable password space. Table 1 gives a comparison of input lengths between the two methods over a range of sizes. Note that the values in the table presume that just as additional keystrokes are needed to select special and capital characters on a keyboard, a comparable number of additional strokes are used when forming a passcode involving paired image selections.

Table 1: Input Length Comparison

Password Length							
Visual Passcode Length	4	5	6	6	7	7	8
Textual	6	7	8	9	10	11	12

3.2 Password Derivation

It is relatively straightforward to use the indices of the image matrix to form the elements of an alphabet and, in turn, compute an associated password value based on the images selected, in much the same way as textual passwords are computed. A one-way cryptographic hash applied iteratively to the clear text password value formed by concatenating individual alphabet values produces the cipher text value of the password. While a visual login technique inherently avoids dictionary attacks associated with textual passwords, it may be possible for an intruder to compile commonly used image sequence selections (e.g., the four corners of the image matrix) and use them in an attack. To ward off specialized dictionary attacks, the clear text password value can be prepended with a random value, called a salt, before the applying the hash. Adding a salt significantly increases the work factor for the intruder, in proportion to the size of the salt and whether both a public and a secret salt are applied [9, 10].

Many organizational policies require users' passwords be replaced after some period of use. Password expiration stymies an intruder, who somehow obtains the cipher text value of the password, from cracking it and determining the input string, over an indefinite lifetime of use. Though the

safeguard is effective, it is also a nuisance for the user, who must follow this practice on numerous systems. Ideally, the user would prefer to continue using the same image sequence indefinitely. The solution is to allow the same image sequence to be used during a password change over, but generate a completely new password value.

Providing this type of password reuse required the addition of a value matrix with the same dimensions as the image matrix. The value matrix holds the values to be applied when the corresponding image is selected. Each entry in the value matrix is randomly assigned a value from the set of alphabet values normally associated with the entries in the image matrix. Instead of using the indices of an image sequence to derive the clear text password, the corresponding elements of the value matrix are used. As before, the alphabet values are concatenated together in the sequence the images were selected to form the clear text password. The value matrix is retained by the authentication mechanism, and remains constant from one authentication attempt to another. Only during password changeovers are the elements of the value matrix automatically updated with randomly reassigned values. Thus, the value matrix allows users to retain the same theme and image sequence over multiple password changeovers, yet produce completely different password values.

One additional use for the value matrix is to hold individual salt values for each element of the alphabet, rather than prepending the clear text value of the password with a single salt value. This can be particularly advantageous when the memory allocated for each value matrix element is larger than that needed to hold the values of the alphabet. In such situations, the unneeded bits can be populated with random values each time a new password is enrolled. This, in effect, creates a new way of salting the password through the embedding of salt values within the alphabet value entries of the value matrix.

3.3 Organization

Picture Password has two main parts: enrolment and verification. Figure 2 gives an overview of these functions. For mobile devices, normally only a single user exists that needs to be authenticated. During start up, the system prompts the user to login or, if an image sequence is not yet enrolled, to enrol one as the passcode. Unlike desktop systems, powering off a handheld device suspends all processes, rather than stopping them and shutting down the system. Powering on the device simply resumes any suspended processes without having to initiate a time-consuming system boot up. To be effective, the authentication mechanism must assert itself at device power on as well as at system boot up, turning the power button into a secure attention key for establishing a trusted path to the authentication mechanism.

Figure

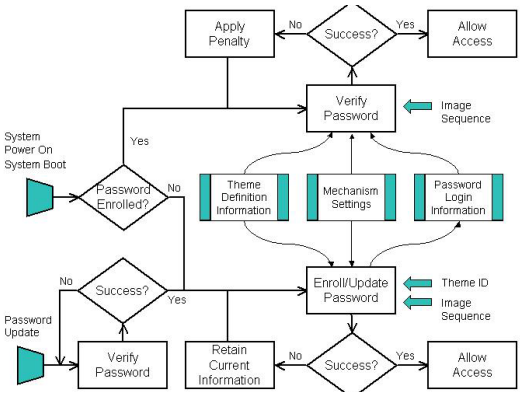


Figure 2: Functional Flow Diagram

Enrolling the password requires the user to select a theme and image sequence, and repeat the sequence a second time to ensure accuracy. If a discrepancy arises, the user can continue the process until successful. Enrolment uses several files. The theme definition information file identifies each theme, the images to display, and other related information. Similarly, the mechanism settings file contains information related to computing the password, such as the number of login attempts to allow, restrictions on passcode length, and the number of hash iterations to apply. When a successful enrolment occurs, the theme identifier and image sequence entered by the user are saved away within the password login information file, along with the value matrix and salt information generated, and the user gains access to the device.

Once enrolled, subsequently powering on or booting up the device prompts the user to enter a correct image sequence for verification. The verification process uses information from the password login information file to display the correct theme and from the mechanism settings file to compute the clear text password for the image sequence. It then applies the hash algorithm as prescribed in the mechanism settings file. A correct match against the enrolled value in the password login information file results in successful authentication and access is granted to the device. If too many authentication failures occur, the user account is locked temporarily to prevent unrestricted password guessing.

Any time after gaining access, a user can update the password by using an available icon to launch the process and entering the correct image sequence for verification, which then follows the same steps described earlier for verification at power on or boot up. In Figure 2, the "Verify Password" box associated with password update does not show the information flows discussed earlier, which are present implicitly. Successful verification allows the user to select a theme and enrol a new image sequence. Choosing the same theme and image sequence produces a completely different password value. A successful enrolment updates the password login information file and the user regains access to the device.

As with any authentication mechanism, Picture Password relies on the security of the operating environment to protect critical pieces of authentication information, including the salt value, the value matrix, and the enrolled password value. Strict file access control settings ensure the confidentiality and integrity of this information. The binaries of the authentication mechanism must also be protected against unauthorized replacement or deletion. Additional

system policy controls can be added to enforce these restrictions and lock down the device until authentication successfully completes [11].

4 Related Work

Draw-a-Secret (DAS) is a scheme for graphical password input, targeted for PDAs [12]. Rather than selecting images, a user draws them on a display grid for use in generating a password. The size of each cell of the grid must be sufficiently large to allow the user enough tolerance when making a stroke to avoid cell boundary ambiguities. Each continuous stroke is represented as the sequence of cell grids encountered. Strokes can start within any cell and go in any direction, but must occur in the same sequence as the one enrolled for the user. Each continuous stroke maps to a sequence of coordinate pairs by listing the cells in the order in which the stroke traverses cell boundaries. The grid sequences for each stroke that composes a drawing are concatenated together in the order they were drawn to form a password. The size of the password space for graphical passwords formed using this scheme on a 5x5 grid is argued to be better than that of textual passwords.

5 Summary

Picture Password is a visual login technique that matches the capabilities and limitations of most handheld devices and provides a simple and intuitive way for users to authenticate. Besides user authentication, Picture Password may also be used in other security applications where conventional passwords have been used traditionally. While the solution is particularly well suited for handheld devices, it can also be used in a wide range of computing platforms.

References

[1] Kingpin and Mudge, Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats, Proceedings of the 10th USENIX Security Symposium, August 2001.

[2] Robert Morris, Ken Thompson, Password Security: A Case History, Communications of the ACM, 22(11), pp. 594-597, November 1979.

[3] Daniel Klein, Foiling the Cracker: A Survey of, and Improvements to, Password Security, Proceedings of the 2nd USENIX Unix Security Workshop, pp. 5-14, August 1990.

[4] Eugene Spafford, OPUS: Preventing Weak Password Choices, Computers & Security, 11(3), pp. 273-278, May 1992.

[5] Greg E. Blonder; Graphical Password, US Patent 5559961, Lucent Technologies Inc., Murray Hill, NJ, August 30, 1995.

[6] visual Key – Technology, sfr GmbH, 2000, http://www.viskey.com/technik.html.

[7] Pointsec for Pocket PC, Pointsec Mobile Technologies, November 2002, http://www.pointsec.com/news/down

load/Pointsec_PPC_POP_Nov_02.pdf.

[8] SafeGuard PDA, Utimaco Safeware AG, March 2003, http://www.utimaco.com/eng/content_pdf/sg_pda_eng.pdf.

[9] Udi Manber, A Simple Scheme to Make Passwords Based on One-Way Functions Much Harder to Crack, Computers & Security, 15(2), pp. 171-176, 1996.

[10] Martın Abadi, T. Mark A. Lomas, Roger Needham, Strengthening Passwords, SRC Technical Note 1997-033, Digital Systems Research Center, December 1997.

[11] Wayne Jansen, Tom Karygiannis, Michaela Iorga, Serban Gravila, Vlad Korolev, Security Policy Management for Handheld Devices, International Conference on Security and Management (SAM'03), June 2003.

[12] Ian Jermyn, Alain May, Fabian Monrose, Michael Riter, Avi Rubin, The Design and Analysis of Graphical Passwords, Proceedings of the 8th USENIX Security Symposium, August 1999.