Authenticating Users on Handheld Devices[1]

Wayne A. Jansen
The National Institute of Standards and Technology
Gaithersburg, Maryland, USA
Wayne.Jansen@NIST.Gov

Abstract - Adequate user authentication is a persistent problem, particularly with handheld devices, which tend to be highly personal and at the fringes of an organization's influence. Yet, these devices are being used increasingly in corporate settings where they pose a security risk, not only by the sensitive information they may contain, but also the means to access such information they may provide. User authentication is the first line of defense against unauthorized access to the contents of a lost or stolen device. Motivating users to employ common password mechanisms and periodically change their authentication information to meet corporate policy is always a challenge, and particularly so for handheld devices. This paper reviews mechanisms, which are compatible with the capabilities of handheld devices and designed to facilitate user authentication, as alternatives to using passwords.

Keywords: User Authentication, Handheld Devices, PDA Security

[1] Contribution of the National Institute of Standards and Technology

Authenticating Users on Handheld Devices

Introduction[2]

With the trend toward a highly mobile workforce, the acquisition of handheld devices such as Personal Digital Assistants (PDAs) is growing at an ever-increasing rate. These devices are relatively inexpensive productivity tools and are quickly becoming a necessity in today's business environment. Most handheld devices can be configured to send and receive electronic mail and browse the Internet over wireless communications. While such devices have their limitations, they are nonetheless extremely useful in managing appointments and contact information, reviewing documents, corresponding via electronic mail, delivering presentations, and accessing corporate data, and increasingly hold sensitive information.

Many manufacturers produce handheld devices using a broad range of hardware and software. Unlike desktops and notebook computers, handheld devices typically support a set of interfaces that are oriented toward user mobility. Handheld devices are characterized by small physical size, limited storage and processing power, and battery-powered operation.

This paper focuses on high-end Personal Digital Assistant (PDA) devices, having significant memory (at least 32MB flash and 64MB RAM) and processing speed (200Mhz or higher), aimed at corporate users. Usually, such devices come equipped with a one-quarter VGA touch screen and a microphone/ soundcard/ speaker, but lack a keyboard. One or more wireless interfaces, such as infrared or radio (e.g., Bluetooth and WiFi) are also built-in for communication over limited distances to other devices and network access points; so too are wired interfaces (e.g., serial and USB) for synchronizing data with a more capable desktop computer. Many high-end PDA devices also support Secure Digital (SD) and Compact Flash (CF) card slots for feature expansion. Over their course of use, such handheld devices can accumulate significant amounts of sensitive corporate information (e.g., medical or law enforcement data) and be configured to access corporate networks and resources via wireless and wired communications.

One of the most serious security threats to any computing device is impersonation of an authorized user. User authentication is the first line of defense against this threat. Unfortunately, management oversight of user authentication is a persistent problem, particularly with handheld devices, which tend to be highly personal and at the fringes of an organization's influence. Other authentication-related issues that loom over their use include the following items:

- Because of their small size, handheld devices are easily lost or stolen.
- User authentication may be disabled, a common default mode, divulging the contents of the device to anyone who possesses it.
- Even if user authentication is enabled, the authentication mechanism may be weak or easily circumvented.
- Once authentication is enabled, changing the authentication information periodically is seldom done.

Many handheld devices use a four-digit Personal Identification Number (PIN) for authentication, with a ten-digit (i.e., digits 0-9) numerical keypad. Because of their limited length and alphabet, PINs may be susceptible to shoulder surfing or systematic trial-and-error attacks. Passwords offer a significant improvement over PINS in both length of entry string and size of alphabet. Most PDA operating systems inherently support traditional alphanumeric passwords, which are entered character-by-character via the touch screen, using either handwriting recognition or a virtual keyboard window. While passwords are an improvement over PINs, they can be difficult to remember and prone to error when entered using a touch

[2] Certain commercial products and trade names are identified in this paper to illustrate technical concepts. However, it does not imply a recommendation or an endorsement by NIST.

screen. Both these conditions can lead to serious problems, up to and including the loss of access to information.

This paper reviews mechanisms, which are compatible with the capabilities of handheld devices and designed to facilitate user authentication, as alternatives to using passwords. Despite the strength of the authentication technique employed, given enough time and money, the contents of a device in the possession of a skillful attacker can be compromised, if necessary, through direct hardware manipulation. Therefore, encrypting the contents of a device is recommend as a complement to strong user authentication [Sto01].

Overview

Authentication refers to the process of confirming or denying an individual's claimed identity. Authentication mechanisms are based on one or more of the following three classes of procedure, whose sureties are commonly referred to as an authentication mode or factor:

- Proof by knowledge – an individual's claimed identity is established through information that can only be known or produced by the individual with that identity (e.g., a password).
- Proof by possession – an individual's claimed identity is established through the possession of an object associated with and exclusive to that identity (e.g., a smart card).
- Proof by property – an individual's claimed identity is established through the direct measurement of certain properties (i.e., biometrics), which match those of the individual with that identity (e.g., a fingerprint).

Password authentication is the most common example of a proof by knowledge procedure. Because of their simplicity and easy of implementation, password systems are the most ubiquitous form of user authentication. Though they are not completely free of problems, passwords nevertheless serve as the benchmark for assessing other authentication mechanisms.

Smart card authentication is perhaps the best-known example of a proof by possession procedure. These credit-card-size, plastic cards host an embedded computer chip with its own operating system, programs, and data, and can be imprinted with a photo and other information, as well as a magnetic strip, for dual use as a physical identification badge [Pol97]. Many corporate security infrastructures incorporate smart cards.

Fingerprint authentication is the oldest form of biometric verification and, thus, the best example of a proof by property procedure [Boe02]. A biometric is a unique, measurable characteristic of an individual, used to verify his identity. Biometrics, such as a fingerprint, by their very nature are impossible to forget and unlikely to be lost.

By applying two or more authentication procedures in combination, such as a proof by possession with a proof by knowledge, stronger authentication can be achieved. Automated banking tellers are an everyday example – a customer presents a magnetic stripe or a smart card containing identification information (first factor), which is then bound to the individual through a Personal Identification Number (PIN) (second factor). In addition to combining multiple factors, conditional constraints, such as time-of-day or location restrictions, may be applied.

An authentication system includes all of the hardware, software, and associated infrastructure needed to perform the authentication process. For broad user acceptance, the overriding considerations for any handheld device authentication mechanism are how convenient it is to use and how well its design utilizes the capabilities of the underlying hardware. For example, the time required to perform various functions, such as enrollment and verification, should be minimal and the procedure straightforward. Administration of the authentication system should also be simple, should devices change ownership, or authentication items are lost, stolen, damaged, or forgotten.

Translating desktop authentication solutions to handheld devices or implementing new solutions can be problematic. Any inconvenience due to cumbersome attachments, slow or erratic performance, or error-prone display interfaces is generally not acceptable. Some of the common obstacles faced include the following:

- If additional hardware is needed, a suitable device interface must be available, and a device driver must be developed for the processor architecture and operating system. Power consumed by any additional hardware must be minimal to avoid draining the battery of the device too quickly.

- Computationally intensive authentication applications, especially those involving floating point operations, can overwhelm the processor capabilities and produce sluggish behavior. This can, at a minimum, require the algorithms to be reworked and may completely prohibit use of the mechanism ultimately.

- Powering off a handheld device suspends all processes, rather than shutting the system down. Powering on resumes any suspended processes, instead of having to initiate a time consuming reboot of the system, as with a desktop computer. This behavior, while convenient to the user, requires the developer to assert the authentication mechanism when the device is powered on, as well as during system reboot.

- Because of their mobility, handheld devices may only on occasion be connected to a corporate network. This usage characteristic requires that the authentication mechanism can operate independently of the corporate security infrastructure when authenticating a user.

- The security of a PDA operating system may not always be as robust as a desktop counterpart [Kin01]. An operating system having a weak security architecture or unresolved vulnerabilities can completely undermine the security of the authentication mechanism.

Authentication mechanisms for PDAs can be divided into two broad classes: software-based and hardware-assisted. Software-based authentication mechanisms work in conjunction with the built-in hardware on the device and require no additional hardware components. They rely only on additional software to be installed on the PDA. In contrast, hardware-assisted authentication mechanisms use at least one additional hardware component connected to the PDA, along with software that captures and processes input from that peripheral and controls the authentication process. Because of the additional hardware required, hardware-assisted authentication solutions generally cost significantly more than software-based solutions.

The remainder of the paper discusses the details of various authentication mechanisms that have been designed or could be tailored for PDA devices, grouped into the three main classes of authentication procedures: proof by knowledge, possession, and property.

Proof by Knowledge

The fundamental operation of a knowledge-based system is accepting an input from the user and comparing that input against previously enrolled information. Because they are simple and inexpensive, password mechanisms are the most common form of authentication in use today. Organizational password policies usually demand at a minimum a random-like sequence of eight upper and lower case alphabetical characters and numeric values. Users tend to respond by either writing down complex passwords or choosing easy to remember passwords that may be vulnerable to attack. Moreover, when the prescribed password lifetime period ends, the replacement password is often very similar to its predecessor, increasing the risk of compromise [Lee01]. Dictionary attacks, involving pre-assembled collections of commonly used passwords to uncover a match, are the primary technique for defeating password systems.

Most password mechanisms rely on the 95 printable ASCII characters available on a traditional desktop keyboard. Thus, a 7-entry password has 95^7 possible values or a password space of size 69,833,729,609,375. Passwords are never stored in their original text form. Instead, when a password is entered, it is converted to a protected form, using a strong one-way cryptographic transformation [Man94].

Once the original input entered is discarded, only the protected form of the password remains. To improve their resistance to attack, should an intruder gain access to the protected form of the password, a randomly generated "salt" value is concatenated to the original password before cryptographic transformation. The addition makes it harder for the attacker to assemble pre-computed dictionaries of common passwords, but it requires the password system to maintain the salt value of each enrolled password.

Another example of a proof by knowledge method is a questionnaire [Pol97]. Individuals enroll answers to a list of questions and when subsequently challenged with a subset of those questions, whose answers are used to confirm the identity. The main weakness of a questionnaire mechanism is that someone who knows the user well could answer the questions correctly and impersonate him. Enrollment is also more time consuming that with a password system. Since the authentication system must retain the answer set for an individual, its protection is a matter of concern.

Visual Login

Visual login refers to a class of mechanisms that rely on the selection of icons or photo images to produce a password value. Visual login is a knowledge-based approach like passwords, but takes advantage of the device's built-in display and image selection capabilities. Instead of alphanumeric characters, users must remember image sequences. Studies indicate that human memory is well adapted for such tasks [Mel01]. For the visually inclined user, these mechanisms can be more intuitive than alphanumeric passwords. Ideally, a visual login system should be designed to be more convenient that entering passwords on a virtual keyboard, and as powerful as password system in terms of the size of password space and work effort needed to overcome them.

Perhaps the earliest general description of a system and method for applying graphical passwords appears in United States Patent 5,559,961 [Blo96]. The authentication mechanism described in the invention displays a set of image areas or cells that comprise a single graphical image. The user selects these predetermined areas of an image in a correct sequence, as a means of entering a password. The password is composed by allowing the user to position selected cells from the image in a location and sequence within the display interface. The mechanism stores the selected sequence of cells as a password. The cells are removed from the display when enrollment or verification is completed, leaving only the original image. One drawback appears to be that the cells, which in effect form the alphabet for composing a password, might offer a significantly smaller sized alphabet than that available with alphanumeric passwords. Alternatively, the cell size could be decreased in size to allow a larger alphabet, but might be made so small that it would be difficult to select one from another using a PDA touch screen.

A commercial product called visual Key [sfr00], from sfr GmbH, has many similarities to the aforementioned graphical password technique, insofar as it uses cells of a single predefined image as the password elements. The visual Key software forms a selection matrix by dividing a single image into cells and dynamically adjusts the grid so that cell centers align with the touch point during selection. A user must select a specific sequence of cells from the display to be granted access to the device. The strength of the password depends on the number of cells associated with the image, since they determine the effective size of the password alphabet. Approximately 85 distinct cells with a size of 30 x 30 pixels can fit on a standard size 240 x 320 pixel display of a PDA. Thus, a seven-entry visual Key password has approximately 85^7 possible values, resulting in a password space smaller than that available through an alphanumeric password. One other drawback is that during selection the cells are not made visible to a user, requiring her to remember which part of an object in the image to select (e.g., the upper left corner of a door or window), since the object might consist of more than one cell. Moreover, cells comprised of 30 x 30 pixels or less are a bit small, which can contribute to selection errors.

PointSec for Pocket PC [Poi02] is a commercial product that includes several authentication-related components, able to be managed centrally. PicturePIN is a graphical counterpart to a numeric PIN system that uses pictograms rather than numbers for entering the PIN, via a keypad-like layout of 10 keys. The symbols, which are configurable, are intended to form a mnemonic phrase, such as the four-symbol sequence of woman/love/flowers/daily. They are also very large and able to be selected using a fingertip, instead of a stylus. The sequence of symbols can be between 4 and 13 symbols long, and to increase security against another individual observing their entry, the symbols are scrambled at each login. Should

the user attempt to re-access the device within a specified number of minutes after it is powered off (settable to between 30 and 300 seconds), a QuickPIN feature can be enabled to provide fast access. QuickPIN relies on a minimum of two pictogram symbols for the user to gain access to her PDA. Both the PicturePIN and QuickPIN systems can be set to lock a user out from her data after three to an infinite number of failed attempts occur in succession. By design, PicturePIN appears to support only a limited alphabet size, comparable to that of a numeric PIN. As an alternative, Pointsec for Pocket PC also supports traditional alphanumeric passwords.

Picture Password is a visual login technique developed by this author. It operates in a similar fashion to the two previous commercial products. Visual images are presented to the user for selection by tiling a portion of the user's graphical interface window with identically sized squares, grouped into a 5 x 6 matrix. The surface of each square displays a bit-mapped image or thumbnail of some picture supplied in a predefined digital format. Selecting the correct sequence of thumbnail images authenticates the user to the device. The thumbnail images are in a size easy-to-select and view (40 x 40 pixels) to minimize input errors. Figure 1 illustrates the PDA screen image for the Cats & Dogs theme, one of several default themes provided. Users can also configure their own photos or images into the matrix. Thumbnail images can also be combined to form a mosaic of a single a picture or graphic.

Figure 1: Picture Password Login Screen

Two styles of thumbnail element selection are provided: individual selection and paired selection. Individual selection requires choosing a single thumbnail, using, for example, a single tap with a stylus. Paired selection requires choosing and linking a pair of thumbnail elements, for example, dragging and dropping the first element onto the second. Conceptually, two thumbnail elements coupled this way represent one single 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 context, however, each thumbnail element can serve as a shift key for every other element, including itself. Having two styles of selection is a significant innovation since it significantly increases the effective size of the alphabet. The total number of alphabet elements is determined by the number of singly selectable thumbnail elements plus the number of paired thumbnail elements selectable, which for a 5x6 matrix is 30 + (30*30) or 930 elements. Thus, 7-entry long passwords have 930^7 possible values or a password space of approximately 6.017008e+20, which is an order of magnitude greater than that for 10-character long alphanumeric passwords at approximately 5.987369e+19. The general strength relationship between passwords formed using the 5x6 picture password matrices versus textual passwords formed from the 95 printable ASCII characters is approximately:

$$N_{pp} = \lceil {}^{2}/_{3} * N_{tp} \rceil,$$

where N_{tp} is the input character length required for alphanumeric passwords, N_{pp} is the corresponding input

sequence length required for picture password, and $\lceil x \rceil$ is the "ceiling" function, which results in the least integer greater than or equal to x.

Graphical Login

Graphical login refers to a class of authentication mechanisms that rely on the creation of graphical images to produce a password value. Graphical login is somewhat similar to visual login and possesses many of the same attributes.

Draw-a-Secret (DAS) is a scheme for graphical password input, targeted for PDA devices [Jer99]. The user draws a design on a display grid, which is used as the password. The design may include block text as well as graphical symbols. Strokes can start anywhere and go in any direction, but must occur in the same sequence as the one enrolled for the user. Figure 2 illustrates a five-stroke password entry. The numbered items indicate the order in which each stroke was drawn and point to starting end of each stroke. For this five-stroke example, there are 8! different ways it could have been drawn, taking into account both the possible ordering of strokes and, for the three strokes that begin and end in different cells, their possible forward and reverse directions

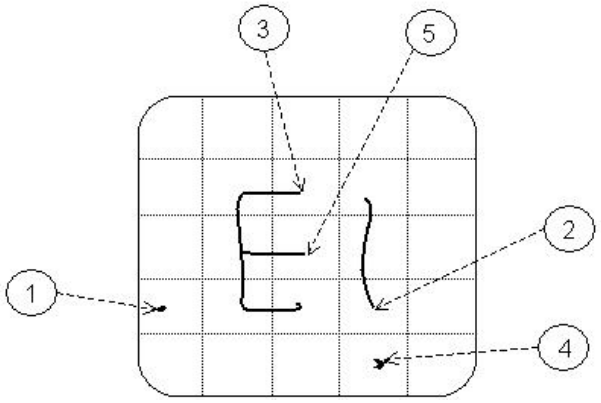

Figure 2: Draw-a-Secret Password Entry

Each continuous stroke is mapped to a sequence of coordinate pairs by listing the cells through which it passes, in the order in which it traverses the cell boundary. Since strokes that run along a cell boundary can cause ambiguity, the size of each cell must be sufficiently large to allow the user a degree of tolerance when drawing a password. 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 has been shown to be larger than that of alphanumeric passwords.

Proof by Property

The fundamental operation of a biometric system is comparing a newly captured biometric image against a previously enrolled template [Pol97]. A template is the recorded biometric measurement of an individual's unique characteristics, which is extracted during enrollment and retained for later comparison against a new record captured during verification. All biometric techniques follow this same basic procedure.

Two main categories of biometric verification are physiological and behavioral techniques [Pol97]. Physiological techniques measure the physiological characteristics of an individual, such as a fingerprint, iris structure, or hand geometry. These characteristics are essentially unalterable and remain relatively stable over time. Behavioral techniques measure the behavioral characteristics of an individual, which are captured when some act is performed for verification purposes, such as signing one's signature, keying in some phrase, or speaking aloud a series of numbers [Boe02]. An individual usually acquires behavioral characteristics over time, and some can be controlled. However, they can change for a variety of reasons such as stress, illness, or normal aging, which makes them less reliable than physiological biometrics [Boe02]. While biometric systems that rely on physiological techniques are more accurate than those that use behavioral techniques, the devices are typically larger and more expensive [Pol97].

Biometric systems have variability when measuring human characteristics or behavior. A measure of variation is the false rejection and false acceptance ratios [Boe02]. The false rejection ratio indicates the percentage of authentication sequences that result in failure to authenticate a valid user. The false acceptance ratio indicates the ratio of authentication sequences that result in the authentication of an imposter. Ideally, both ratios should be as low as possible. Biometric systems usually have the means to set threshold levels tighter or looser to increase or decrease the level of security as required. A tight threshold setting reduces the likelihood for false acceptance errors, but increases the likelihood the false rejection errors. A loose threshold setting has the reverse effect.

The rates of error are critical to the system performance. Too high false rejection rates cause frustration and disuse, while too high false acceptance rates allow impersonation and fraud. Error rates can be graphed against a system's sensitivity threshold settings to obtain false acceptance and false rejection curves. At some threshold setting, these curves have an equal error rate and intersect each other, which is the point where false rejection and false acceptance errors are equally likely [Pol97]. The lower the equal error rate is, the more accurate the biometric system. However, these measurements depend on the population, application, and environment.

As mentioned earlier, templates typically contain only extracted information and not the original biometric image. Recorded templates can be stored in various places, including the memory of the biometric reader, the computer system, or a token [Pol97]. Wherever they are stored, they must be protected. Storing the templates in the memory of the reader device avoids any risk associated with their movement elsewhere. Storing the templates in the memory of a token allows individuals to carry their templates to other computing platforms for identification. The size of the template can be a factor in where it is stored. For example, templates for some biometrics can exceed the memory of some tokens.

While biometric systems eliminate the need for password management, enrollment and verification times can be an issue. Usually several biometric images are needed to create a template during enrollment. That process can be lengthened further by the occasional occurrence of a poor and unusable image, which also affects verification times negatively. .

Fingerprint Verification

Fingerprint verification is a quick and convenient method of establishing an individual's identity. Among all the biometric techniques, fingerprint-based identification is the oldest [Boe02]. A fingerprint is made of a series of lines, called ridges and the spaces between these ridges, called valleys. A fingerprint is matched for verification through the unique pattern of these ridges and valleys. Fingerprint uniqueness is determined by anatomic characteristics called minutiae. Minutiae are the locations on a fingerprint where the ridges stop, fork, or intersect. Minutia matching analyses the features of the fingerprint, such as the location and direction of the ridges. Some approaches use only minutiae for matching, while others include information such as the number of ridgelines between adjacent minutiae [Boe02].

When the fingerprint image is analyzed, the minutiae points are extracted and translated into a code that serves as a template. The template is initially encrypted and stored in local memory, in the scanning device itself, or on a smart card. Templates usually have a size of between 40 and 1000 bytes, often around 256 bytes [Boe02]. The original fingerprint cannot be recreated from the minutia data stored on the template. During verification, an image of the fingerprint is captured and translated into a template of minutiae, and then compared with the stored template. Authentication is successful and an identity established when the two match. Several technologies exist that can be used to obtain a digital image of the fingerprint, including capacitance, thermal, and optical sensing [Boe02].

The BioHub, a commercial product from Biocentric Solutions Inc., is a small CF module that incorporates a fingerprint-imaging sensor with a 250 dpi image density [Bio02]. An optional, higher resolution 500 dpi sensor can be made available to support the collection of better quality fingerprint information in the field. The module requires at least a type I CF card slot on the device. The sensor portion of the module extends beyond the CF slot when inserted. Software controls biometric enrollment, matching, and access to a PDA. It also supports an option for file encryption. The enrollment process can create a template from one or

more fingers. The template is encrypted and stored on the PDA's memory. Five selectable security levels determine the number of matching minutiae needed for the live fingerprint. Figure 3 is a photo of an early version of the device. The company also produces a related product called the BioSentry, which operates in a similarly to the BioHub, but whose sensor is built into an expansion sleeve designed specifically to fit an iPAQ PDA. The expansion sleeve also incorporates a CF slot for the device.

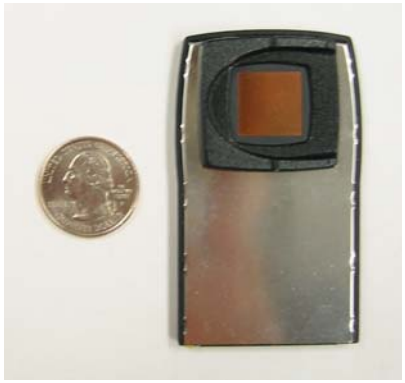

Figure 3: BioHub CF Reader

BioTouch is another fingerprint reader solution from Identix Inc., targeted mainly for notebook computers [Ide02]. The hardware module incorporates a 380 x 420 dpi optical fingerprint sensor into a type II PCMCIA Card. The sensor can be popped out of the card when needed. Figure 4 is a photo of the reader with the sensor extended. Software controls the logon and enrollment process. Enrollment creates a template of minutiae points from the fingerprint image, which is encrypted and stored on the PDA. The template size is up to 512 bytes. PDAs that incorporate a type II PCMCIA slot are extremely rare. Though not currently available as a released product, Identix has a prototype solution for iPAQ PDAs, whose expansion options currently include both single and double PCMCIA slot expansion sleeves.

Figure 4: BioTouch PCMCIA Reader

Fingerprint readers are also beginning to appear as built-in hardware on some PDA devices. For example, on HP's iPAQ H5450, the reader appears as a small strip beneath the navigation button.

Signature Verification

Signature verification is a technology where the dynamics of signing and not the signature image itself are captured and compared to a stored template for authentication [Boe02]. Dynamic characteristics include

speed, acceleration, direction, pressure, stroke length, sequential stroke pattern and the time and distance when the pen is lifted away from the surface. Several types of dynamics can be monitored and captured using a PDA touch screen, but not all. As with every biometric technology, a template is created during an enrollment process and subsequently used during the verification process. The user interface is very simple, needing little more that a signature box on the display in which to sign, such as that illustrated in Figure 5.

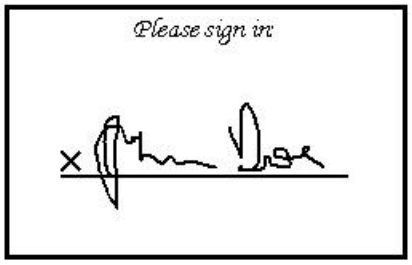

Figure 5: Example Signature Screen

Sign-On for Pocket PC is a commercial signature verification product from Communication Intelligence Corporation, which replaces the standard Pocket PC password logon process [CIC01]. Once installed on the device, the software forms a template based on the dynamics captured from seven signature samples, which is then encrypted and stored on the device. Subsequently, during user authentication, the software requests a signature and an optional PIN to verify identity. Both a signature and a PIN are required before synchronization with a desktop computer can proceed.

PDALok is a similar product from Romsey Associates, Inc. [Rom01]. Software captures, verifies, and encrypts a signature directly on a PDA. Six signature samples are needed for enrollment. A signature takes up less than 1K of memory and requires only a millisecond to be verified. The entire signature database is about 4k, depending on signature complexity. An encryption algorithm and one-way encoding protect the signature template.

Voice Verification

Voice verification, also know as speaker recognition, determines the identity of the speaker. Enrollment requires an individual to say a set of specific words, typically a numeric value, in succession and usually repeated several times. A template is extracted from this input using an acoustic model, which defines the characteristic of the voice [Boe02]. Once enrolled, authenticating to the system is done by prompting the individual to speak into a microphone and vocalize a randomly drawn set of digits, as they appear in the display.

While many PDAs incorporate a built-in sound card and microphone, they typically lack the processing power (i.e., floating point hardware) to perform the needed calculations quickly enough. The main reason for this is that voice-modeling algorithms rely heavily on floating point arithmetic, whose execution must be emulated in software. Other drawbacks to this type of solution include environmental sounds, individual speaker variability in pronunciation (e.g., for the number 12, saying one-two versus twelve), the significant amount of time needed for enrollment compared to other biometric mechanisms, and the larger size templates that are needed.

Proof by Possession

Security tokens are small hardware devices that their owners carry with them. The device may be in the form of a commonly used object such as a key fob that attaches to a key ring or credit card that fits in a wallet. A device driver and the software application to control user login usually accompany the token. The fundamental operation of a token system is determining the presence of some object needed to authorize access. Token are very effective in combination with a knowledge or biometric factor (i.e., two-factor authentication) [Boe02].

As mentioned earlier, the power consumed by the token can be an issue. The size of the token can also be a concern, as well as the manner in which it interfaces with the PDA. The distribution, use, and administration of tokens typically require more extensive overhead than with the other authentication methods discussed previously. For example, like passwords, tokens can be lost or stolen. They can also be damaged. A lost or damaged token necessitates the issuance of a replacement, a manual operation, as well as the revocation of the missing token as the means for establishing an individual's identity. Though many token products exist for the desktop, they have been slow to filter toward handheld devices.

Generally, security tokens come in two variants [Boe02]:

- A network authenticator for remote access
- A smart card for authentication, stored value, and other applications

The first variant is outside the scope of this paper, since it relates to the user authenticating through a handheld device over a communications network to some remote system. The second variant, smart cards, is quite relevant, however.

Smart cards are credit-card-size, plastic cards with embedded computer chips, ranging from simple memory cards that provide storage only, to microprocessor cards that have their own operating system, programs, and data [Pol97]. The card is designed to protect the information it contains, and it usually requires a PIN to verify the user's identity before granting access. The computer chip on the card requires a smart card reader to obtain power and to communicate with some more capable computing platform. Once contact is made with the reader, a smart card communicates with software running on the computing platform using a half-duplex serial interface. The capabilities and form factor of smart cards are compatible with some handheld devices, provided that a reader with a suitable interface and a driver for the platform's operating system is available.

A number of manufacturers produce smart card reader hardware modules that fit into a type II PCMCIA Card slot. These readers accept standard size smart cards, which can be obtained separately. A platform, such as an iPAQ PDA, whose expansion options include both single and double PCMCIA slot expansion sleeves, can readily accept such readers and operate them, once a suitable driver is found and installed. For example, a driver for the Pocket PC operating system that runs on the iPAQ is available for the Schlumberger Reflex 20 reader. Similarly, an open source Linux driver that works with ARM processors, including the iPAQ platform, is available for the Gemplus GemPC400 smart card reader [Gem03], which is shown in Figure 6.

Figure 6: PCMCIA Smart Card Reader

A more elegant solution for the iPAQ is the Blue Jacket from Axcess Mobile Communications, which is a special purpose expansion sleeve that incorporates a smart card reader and supports an optional Bluetooth communications module and compact flash slot (type II) [Blue]. Figure 7 is a photo of the Blue Jacket Sleeve with the full option set. Software needed for the Pocket PC operating system installs automatically from on-board memory on the sleeve.

Figure 7: Blue Jacket Expansion Sleeve

Smart cards come in other form factors. For example, an iButton is a 16mm computer chip contained in a stainless steel shell, able to be mounted in jewelry (e.g., ring, bracelet, necklace) [Dal02]. Capabilities range from a simple memory token to a microprocessor and arithmetic accelerator able to support a Java Card 2.0-compliant Virtual Machine. However, a button receptacle incorporated into the device or easily added (e.g., via a compact flash card) is needed to facilitate their use with PDA devices.

A popular format emerging for smart cards is a USB key fob. This chewing-gum-pack sized hardware component has a USB connector at one end, and is built as a printed circuit board within a plastic housing that encases a processor and memory. Many manufacturers produce USB devices that are technologically identical to smart cards and eliminate the need for a reader. Currently, however, very few PDA devices support host USB ports, which are needed to interface to these peripherals.

Summary

Handheld devices, being designed for mobile workers, offer unique opportunities for user authentication. Several suitable authentication mechanisms exist as password replacements for PDA devices. Perhaps the most promising authentication mechanisms are visual login, signature verification, and fingerprint verification. For organizational security infrastructures that rely on smart cards, a limited number of possibilities also exist to apply them to handheld devices. Software only solutions that take advantage of built-in hardware are less costly to purchase than those requiring additional hardware and generally more available. However, each authentication system has its own infrastructure and cost implications that must be taken into consideration. As the trend toward more powerful and expandable handheld devices continues, the opportunity and need for strong authentication mechanisms also increases.

References

[Bio02] BioHub - Biocentric Security for Portable Applications, Biocentric Solutions, 2002, <URL: http://www.biocentricsolutions.com/media/BioHub.pdf>.

[Blo96] Greg E. Blonder, Graphical Password, US Patent 5559961, Lucent Technologies Inc., Murray Hill, NJ, August 30, 1995.

[Blue] Blue Jacket Product Information, Axcess Mobile Communications, <URL: http://www.axcess-mobile.com/products/BlueJacketFlyer.pdf>.

[Boe02] Nicky Boertien, Eric Middelkoop, Authentication in Mobile Applications, CMG, Telematica Instituut, The Netherlands, January 2002, <URL: https://doc.telin.nl/dscgi/ds.py/Get/File-23314/VH_authenticatie.pdf>.

[CIC01] Sign-On for Pocket PC, Communication Intelligence Corporation, 2001, <URL: https://secure.cic.com/product_details/signonpocket_details.asp>.

[Dal02] iButton Overview, Maxim/Dallas Semiconductor Corp, 2002, <URL: http://www.ibutton.com/ibuttons/index.html>.

[Gem03] GemPC400, Gemplus SA, 2003, <URL: http://www.gemplus.com/products/gempc400/>.

[Ide02] BioTouch PC Card, Identix Incorporated, 2002, <URL: http://www.identix.com/products/pro_info_fp_biotouch_pc.html>.

[Jer99] Ian Jermyn et al., The Design and Analysis of Graphical Passwords, 8th USENIX Security Symposium, Washington, D.C., August 23–26, 1999.

[Kin01] Kingpin and Mudge, Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats, USENIX Security Symposium, August 2001.

[Lee01] Jennifer 8. Lee, And the Password Is . . . Waterloo, The New York Times, Circuits, Thursday, December 27, 2001, Late Edition - Final, Section G, Page 1, Column 1, <URL: http://www.nytimes.com/2001/12/27/technology/circuits/27PASS.html?ex=1028105054&ei=1&en=4c3ce4a63682fecc>.

[Man94] Udi Manber, A Simple Scheme to Make Passwords Based on One-Way Functions Much Harder to Crack, Computers and Security, 15(2), pp.171-176, 1996.

[Mel01] David Melcher, The Persistence of Visual Memory for Scenes, Nature, 412(6845), p. 401, July 2001.

[Poi02] Pointsec for Pocket PC, Pointsec Mobile Technologies, November 2002, <URL: http://www.pointsec.com/news/download/Pointsec_PPC_POP_Nov_02.pdf>.

[Pol97] Despina Polemi, Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification And Authentication, Institute of Communication and Computer Systems, National Technical University of Athens, April 1997, <URL: ftp://ftp.cordis.lu/pub/infosec/docs/biomet.doc>.

[Rom01] PDALok Frequently Asked Questions, Romsey Associates, 2001, <URL: http://www.pdalok.com/pda_security_faq/pda_security_faq.htm>.

[sfr00] visual Key – Technology, sfr GmbH, 2000, <URL: http://www.viskey.com>.

[Sto01] Wolfgang Stockner, Mobile Security Concepts, Software Competence Center Hagenberg, Austria, August 2001, <URL: http://www.scch.at/research/projects/moved/moved/projectdocuments/d41.pdf>.