Efficient Authentication Systems for a Small to Medium Sized Bank

By Cedrick Burrows

March 2007

Table of Contents

Introduction

Any time a person attempts access to a restricted resource the prerequisite is authentication. This is the safe guard of confirming a person is who he/she claims to be. Because of the many vulnerabilities associated with one factor authentication (passwords), many organizations are looking at better methods to identify individual's accessing their systems. Individuals should have access to only the resources applicable to their level of need to know. Organizations are becoming aware of the risk associated with password authentication and are looking at better methods to grant access to their resources. System security professionals need to understand the advantages and differences between the many products available.

The current authentication method used by the bank is passwords; this is a one factor solution. There are a few reasons this solution is not adequate. Passwords have to be reset because endusers forget their password, or they choose passwords that are easily guessed. Many tools are available today that can easily compromise a system.

The system chosen will alleviate these concerns because biopassword is based on individual keystroke rhythms. No two individual's type exactly alike, thus individuals cannot share, copy, or write down these unique attributes.

Overview of the bank

Since 1962, Bank Group has offered a level of service and responsiveness that the mega-banks, despite their posturing, can never hope to attain. The employees, from tellers to key decision makers, live in the communities served; Bank Group understands the needs of the communities and customers.

Bank Group, along with all the other banks and savings and loans, is subject to the provisions of the Community Reinvestment Act (CRA). This act was designed to ensure that

financial institutions demonstrate that their credit and deposit services are meeting the convenience and needs of the communities they serve. The primary focus is to ensure that institutions are reinvesting in their local communities through affirmative credit programs and ongoing community involvement.

Bank Group **Financial Highlights**

Years Ended December 31,

(Dollars in thousands, except per share data)

	2006	2005	2004	2003	2002
Net income	$ 25, 486	$23,658	$25,908	$17,932	$20,183
Per share earnings	58.93	54.82	59.90	41.46	46.67
Book value (1)	344,60	347,87	346,62	341,47	335,30
Net loans	1,091,747	1,046,125	1,074,215	1,128,816	1,093,376
Total assets	1,826,826	1,748,049	1,710,695	1,586,063	1,473,559
Deposits	1,639,666	1,569,742	1,529,931	1,420,256	1,309,720

DECEMBER 31, 2006 AND 2005
(Dollars in thousands)

The following are some of the financial highlights for Bank Group. Net income is calculated by starting with a company's total revenue.

- The per share earnings in 2002, increased from 46.67 to 58.93 by year 2006
- Net loans totaled 1,826,826 billion by the year 2006
- Total assets increased from 1,473,599 to 1,826,826 by the year 2006
- The total deposits in 2006 totaled 1,639,666
- Deposits totaled 1,639,666 in year 2006

Total assets is a metric used to measure a company's financial risk by determining how much of the company's assets have been financed by debt. Calculated by adding short term and long term debt and then dividing by the company's total assets. [34]

Bank Group currently has 850 full time employees. There are 109,502 bank account holders with Bank Group. Total accounts at Bank Group total 241,382. In the suburbs of Illinois Bank Group have thirty eight locations.

Access control

Access Control is the practice of authorizing end users, groups, and computers to access objects on the computer network. Notions that make up access control are permissions, user rights, and object auditing. [1]

In access control there are subjects and objects. Subjects request the information or access to objects. The subject is initiator, or formulating the action. The active entity, subjects can be the enduser, a program, or process taking on the task of making the request or action to carry out specific tasks. [35]

The object is the non requesting body. Objects contain the resources the subject want access for the resources contained within. Objects are the inactive entities and can be a computer, record, file, program, index, or field contained in a database. [35]

Identity Management

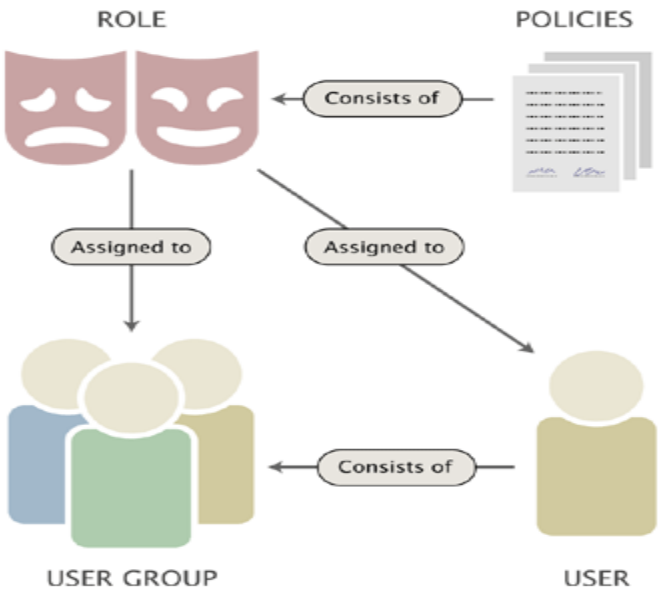
In a Windows environment identify management is connected to the management of an enduser's credentials (user name and password) and how they are permitted to gain access to the data/resources on a computer network. [2]

Both identification and authentication are the root method for just about all systems that control a person’s access to confidential data. Who you are is the undertaking of identifying yourself to a system. This is normally established by signing or logging-on using credentials or a

ID logon. This would create an end user logon access capability for the type of access on a system. [4]

The identification aspect is dependant upon a username that must uniquely identify the user and should not uncover the role in the organization, (such as human resources, president, or payroll officer). Ordinary or public accounts like admin, root or system should be avoided. [2]

If an end user has access to resource it should be determined the person is who he/she claims to be; the necessary credentials, and if he/she has the needed rights they are requesting. In most organizations policies are assigned to containers which can be named user or user groups. The below picture is an example of identity. [3]



Identity Management [1]

Authentication Methods

"Authentication is any practice by which you confirm that a person is who they declare they are. Authorization is every procedure in which someone is permitted to be present or gain access to where they set out to, or to gain information that they want possess". [36]

Authentication can be achieved by the following methods:

1. "Something you know, such as a password, or personal identification number" [8]
2. "Something you have, such as a credit card or token" [8]
3. "Something you are, biological trait" [8] Biometrics include "Physiological trait-unique fingerprint, retina, voice, or iris characteristics" [9] and "Behavioral, characteristic – keystroke, signature pattern" [9]

Passwords

End user recognition together with a password is the means of confirming he/she is who they profess to be. A password along with other identification such as a user name is the most widespread form of identification and authorization to a system. A password is a undisclosed, protected data string of lettering used to give access to an end user attempting to gain access to a system. Passwords notwithstanding the name do not have to be exact words. If the end user uses passwords made up using characters and words it is much harder for the intruder to guess, this can also be harder to remember for end users to remember. [7]

Password attacks

Below are some of the password attacks

Electronic monitoring: This is a passive technique used by gathering network traffic, utilizing software such as a snuffer. This particular software that can capture packets as it travels

thru the network. In most instances the information gathered will be used later in an attack that can infiltrate a network. [29]

In the Windows environment acquiring access to the Security Accounts Management (SAM) database; often done on the authentication server. In this database are the end user passwords. Access to this database by an intruder would cause a great deal of damage. The Security Management database (SAM) database should be protected with good access control measures, in addition to encryption. [29]

Social engineering, another type of a password attack is a method done by using non-technical intrusion. Social engineering is accomplished by human interaction and often involves deception; using the end user to effectively breach security procedures. Social engineering evolves using a con game. An example would be an attacker erroneously persuading the end user who is authorized to use a system to give him restricted information; pretending he/she is someone he is not. [30]

Brute force attack

This assault is made to a single system, and usually the last resort due to the time it takes to perform this kink of attack. When all other method of entry fail to breach a system. The assailant time after time attempts to gain access to the system making changes in the attack each time, in the expectancy that the attack will eventually succeed; each penetration attempt is a test to gain acceptable authentication credentials.

The attack is a method of obtaining an end user's authentication credentials. This method is generally performed through the usage of usernames and passwords. Acquiring the password may give the attacker assurance the end user is valid. Each end user first chronicled, or is registered by an administrator using an assigned or self-stated password. On each consequent try,

the end user must know and use the formerly declared password. Using brute force, attackers attempt various mixtures of character set in order to find a definite grouping that achieve access to the allowed system. [10]

Dictionary Attacks

This approach is an attempt to crack account passwords. This method is achieved by using every possible word in the dictionary as a possible encrypted string. It is possible because of end user choice of simple easy to remember passwords. Frequently when using this kind of attack the attacker will need a copy of the Security Accounts Management (SAM) file. Using this file, it will be up loaded on a system, and then use a utility called a password cracker; will try to gain end user account passwords. [11]

One of the regular protection methods against password guessing attacks is a feature named blacklisting. This measure limits the amount of successive failed login attempts. Generally a login attempt counter is set to zero after a good login and incremented thereafter if any unsuccessful login are attempted. When the counter reaches the blacklist clipping level; usually between 3 and 7 attempts, account login is disabled. Not even the correct authentication would be allowed after the level is exceeded. [66]

Imposters may use blacklisting as the starting point for another kind of attack. When they cannot gain entry break to a system, they can in effect deny access to users with a blacklist attack, this sort of attack can effectively deny legitimate access to all endusers by intestinally blacklisting them. One measure to prevent system-level accounts from being blacklisted by an intruder, most operating systems will allow logins to accounts from the operator's console even if the account is in blacklist status. [66]

Another likely attack would be to thieve a system's password file; this is quite a simple thing to accomplish when the system is not afforded the right access protection controls. Even though passwords are just about always kept in some encrypted or hashed form in a file, they are nonetheless prone to attack using a dictionary attack. This attack uses large numbers of words encrypted with the operating systems' encryption method in an attempt to acquire a password equal to the inside the file. Several studies find that there is a near 99 percent probability of successfully cracking at least one password in a file holding as little as 16 passwords. Utilizing high-speed processors available today on the desktop at simple cost, almost anyone with a spell checker can embark on a dictionary attack. [61]

An additional method of compromising a system is called logon spoofing. This can be mostly successful in public terminal rooms at educational institutions. In this set-up the attacker uses a program that displays what appears to be a valid login screen. When another enduser attempts to login, the program makes the normal prompt for the username and password, extracts the information to a file, displays an "Invalid login" message, and then logs the attacker out. The lawful enduser, believes they must have made a mistake inputting the credentials, tries again to login and succeeds. This method of attack is often successful and, if fortunate, the intruder finds a user who has a high amount of system access. [60]

Another attack is to examine the traffic between the enduser and computer. When this method is used, the attacker may be gain usernames and passwords in plain text. In a network, this type of attack involves the intruder gain physical access to the lines of transmission or wiring closet. Using the Internet, an attacker may simply have to observe the packets used for Telnet, the internet or other password protected accounts. [62]

When successful acquiring valid usernames and passwords; attackers can employ a replay attack. Using this attack the attacker resends the valid authentication data to a target system to gain access. Most systems that use constant identification, and/or authentication information are susceptible to such as attack. [63]

Because nearly all computer systems amass passwords in some encrypted form, imagine the password like a means to a cryptographic system. Cryptographic method pass on more security as the key size multiply, implying that passwords are more secure as they gain in size. This is true to a certain degree; however, a longer password is not as resilient when compared to a shorter password as you might think. Often because of the limitations inflicted by some computers and the way most endusers choose their passwords. A password made up using case-insensitive characters. There are 26 letters in the alphabet. Using 26 would give 26 to the 7^{th} (8,031,810,176 or 8,031E9) characters. Using one of the processors available today it would be considerably less time. Combining numbers and special characters, (&#*) would include to the complexity of the password, thus making it harder, although not unachievable to crack. Passwords with characters less then seven could be simpler to compromise using the expression above 26 to the $4/5^{th}$ an so on. [65]

Adding a fourth part, something you do, is further introduced to this list. Something you do would be typing your name using a keyboard. Something you do can be the same as something you are. [64]

Strengths and weaknesses of passwords

Passwords are a ubiquitous means of identification and authentication using keystrokes to gain system access. Its use can be seen from the use personal of identification numbers at automatic teller machines (ATM), credit cards, and calling cards. To the more complex letters

and numbers combined passwords that protect files, computers, and network equipment. Passwords are generally used because they are cheap, easy to setup. Because they are easy to use, passwords are recognized as being difficult to maintain. Network administrators may have thousands of passwords accounts to manage; with just lone account need be negotiated to give an intruder a path into the network. Skilled attackers may gain a way into a machine and not execute any malicious activity; simply gain access to use the system as a way to commence attacks to other distributed systems. Toda with the millions of internet interrelated systems. A calamity could be damaging to a great extent. [12]

According to the Gartner Group, "approximately 20% to 50% of all help desk calls are for password resets. Forrester Research states that the average help desk labor cost for a single password reset is about $70. [36]

The main reason passwords are compromised is because they are a weak form of protection. The single reason for this weakness is due to the fact that passwords depend on the relation in the network string of defense the "end user". Most end users are not attentive to the security rules and procedures, and how significant they are to the many systems and network. [13]

Intruders launch attacks on systems attempting to gain access; there are many ways this can be done. One of the more widespread forms of entry is password guessing. End users many times choose their own name, username, cell phone number, or some variation as their password. Other methods; they choose the name of relatives, friends, pets, special interests, or something similar. Intruders find this much of this information, all too often in many situations, it's easy. [14]

"A password should be like a toothbrush. Use it everyday, change it regularly; and DON"T share it with friends" [6]

Authentication; method used to identify a person is, who they say they are to a computer or system. This process requires end users, or in some cases systems, to provide information to prove their identity. [15]

One-factor authentication mechanisms use one of three types for authentication. Something you know, between a workstation station and an individual, such as a password. Something you have, the possession of a physical token; or ATM card. [16]

“Something you are”, a physical attribute; biometric characteristic, information generated from an individual by digitizing dimensions of a bodily traits such as fingerprint, facial geometry, voice pattern, or a retinal pattern. A two factor process would obtain two of the three types of information”. [16]

Two factor authentications would be an ATM card and PIN. The end user's PIN something you know and the end user's ATM card something you have are both needed to access an ATM machine. [16]

Passphrase

A passphrase is a collection of words or characters used just like a password to grant entry to a system. Passphases are comparable to passwords, except are longer in length. The longer the passphrase the less the success the attacker will have cracking. Because pass phrases are longer it makes them troublesome to enter. Passphases share the same problems with passwords. [16]

Strengths and Weakness of Pass phrase

Passphrases are generally longer than passwords. Passwords can often be as little as 6, 8, or sometimes less characters. Passphrases are longer and, most often passphrases are between 20 or 30 characters or longer; because they are longer this makes brute force attacks impossible to

carry out. Because of the longer length often means stronger security. Attackers will find it very difficult to break a 25-character passphrase than one that has only 8 digit password. When passphases are chosen well, it should not be a phase, quote or in the dictionary. This would dictionary attacks useless. Passphases can be something easy to remember, thus ensuring the end user will not have to jot it down on paper. [16]

Most organizations have rules for using a valid passphrases. Some systems that have shorter passwords will most often not use words or names. Using these as password is, short of having good security. Using this password is typically clear random succession of characters. The longer the length of a pass phrase, by contrast this will allow end users to create an easily memorized phrase rather than a secret sequence of letters, numbers, and or symbols. [17]

End uses normally choose passphases they can remember, by doing so it makes the passphase easier to guess. End users will also write it down or share the pass phase. Entering pass phases can be wearying. To circumvent system controls end users will use simple non secure passphases. [18]

Biometrics

"Biometrics verifies with an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification". [26]

When comparing different biometric systems the crossover error rate (CER) is the most important factor to consider. A percentage of both represent the point where the false rejection rate (FRR) equals the false acceptance rate (FAR). The lower the number value the more accurate the system; a value or 2 would be more accurate then a value rating of 4. [27]

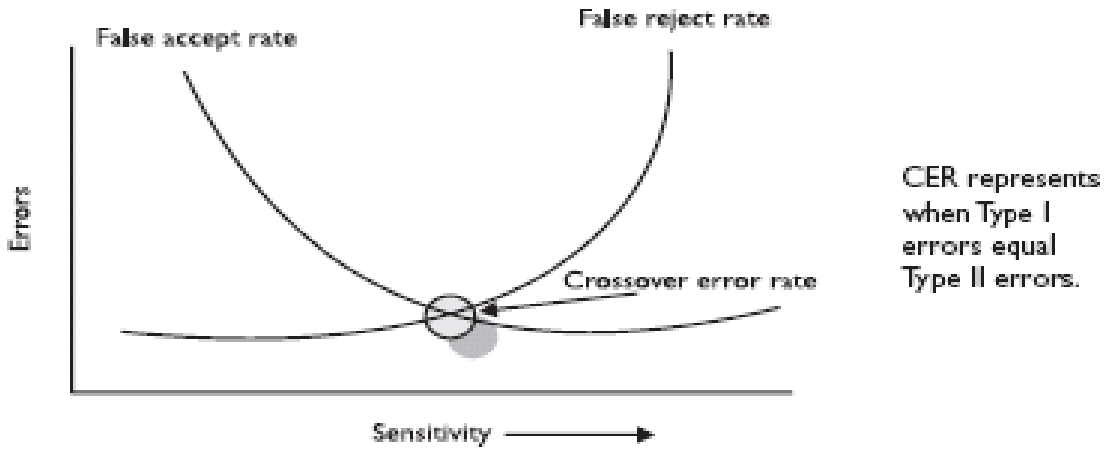
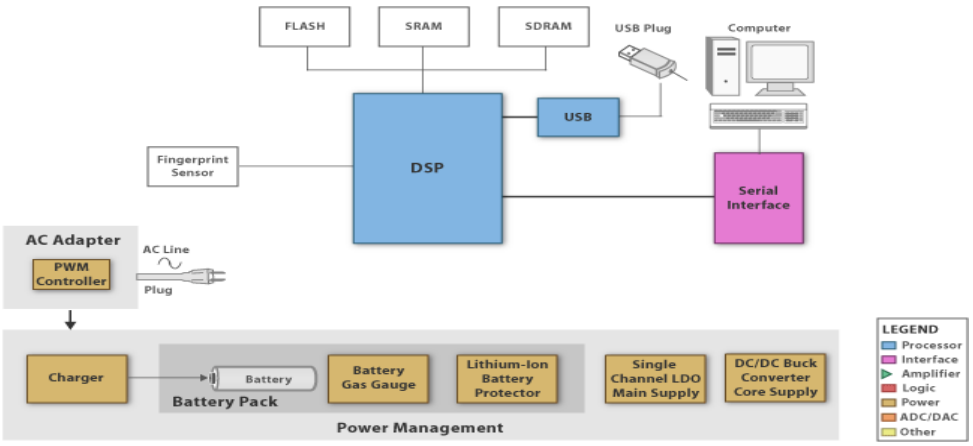


Diagram shows the point where FAR equals FRR [28]

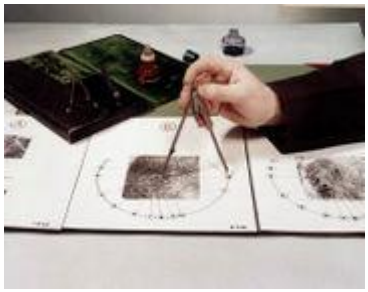
Information technology uses biometric authentication technologies that will measure, and analyzes physical and behavioral characteristics for purposes of authentication. Biometric identification it the lone method to uniquely identify an individual based on physiological or behavioral characteristics. Examples of physical, or physiological, or biometric characteristics include, eye retinas and irises, facial patterns, and hand geometrics. Behavioral biometric characteristics include data taken from actions or indirectly measure characteristics of a human body. Voice, signature, gait and keystrokes are characteristics or behavior. Behavioral biometric characteristics have physiological components; on the other hand physical characteristics have a behavioral element. [19]



Fingerprint system block diagram

“The fingerprint in biometrics is a depression of friction ridges or any part of the finger. A friction ridge is a raised portion of the epidermis on the palm and fingers or sole and toes skin, consisting of one or more connected ridge units of friction ridge skin. These ridges are sometimes known as "dermal ridges" or "dermal papillaeFingerprint scans are the most widespread biometric in use today. Finger identification compares friction skin ridge impressions from fingers, palms, and toes. These impressions compared to see if it matches other finger, palms or toes. Because of the flexibility of ridge skin means that there are no two fingers or palm prints that are exactly alike; in no way identical in every detail”. [20]

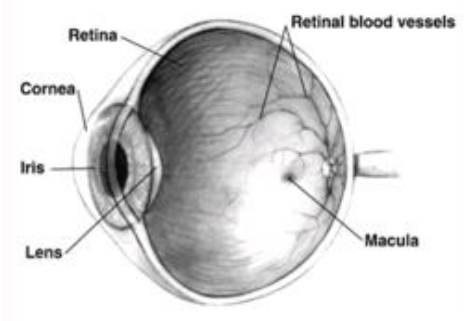
Captured fingerprint normal fingerprint [21]



Measuring a fingerprint [23]

“Retinal scanning analyses the layer of blood vessels at the back of the eye. Scanning involves using a low-intensity light source and an optical coupler and can read the patterns at a great level of accuracy. It does require the user to remove glasses, place their eye close to the

device, and focus on a certain point. Whether the accuracy can outweigh the public discomfort is yet to be seen." [24]



Retina [23]

At present there is no known way to duplicate a retina. When a human being expires the retina deteriorates too quickly to be useful, therefore no extra safety measures need been taken with retinal scans to be sure the user is a living human being. In human beings the retina remains constant from life to death. Due to the constancy, the retina remains the most accurate biometric method to measure person's identity. [25]

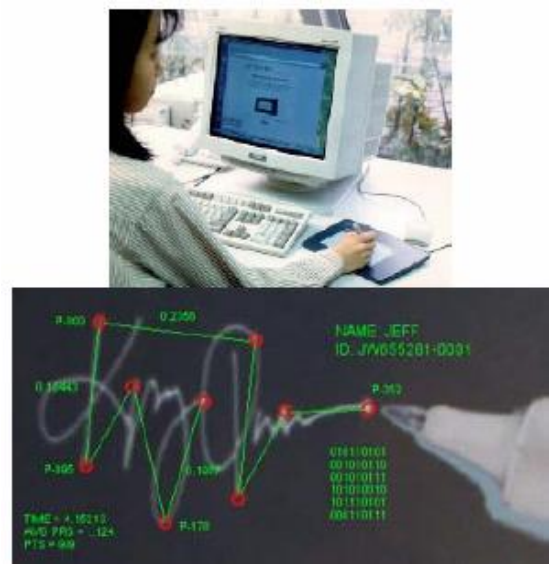
Retina scan processes are the most precise biometric authentication method used today. The stability of the retinal pattern all through life and the difficulty in duplicating such a machine also make it a good lasting, protection option. [25]

Example of retina scans [26]

The pure cost alone of the implementing the hardware is one of the reasons it is not widely used today, as well as the low end user acceptance of such a mechanism. It also has the reputation of being possibility being harmful to the eye, and difficult to use. [26]

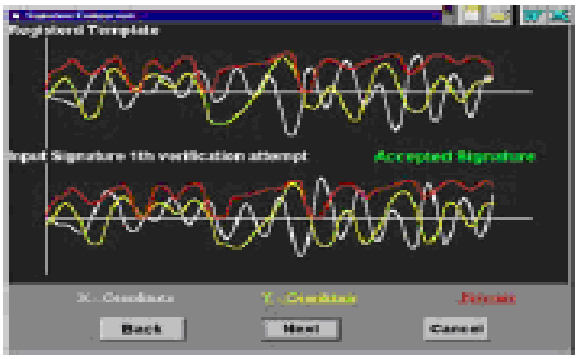
Voice: There are very faint unique patterns in people's speech sounds and patterns. Biometric systems capture a voice tone and compare it to the information contained in a reference file can distinguish one person from another. During the sign-up procedure a person is given a script with different words. Signing into a system a person needs to be authenticated; the biometric system mixes words and introduces them to the individual. At this point the person says the sequence of words given during enrollment. This is used as a preventive measure, so that intruders won't try to record the session to play back at another time, in anticipation of acquiring unauthorized access. [51]

Signature Dynamics: When a person signs he/she will generally do so using the same speed with each new signature. Signing a signature creates electrical signals that can be obtained by a biometric system. The bodily movement present when someone is signing a paper creates these electrical signals. The signals give an exclusive characteristic that can be used to differentiate one human being from another. Signature dynamics impart more information than a static signature, so there are more things to verify when validating a persons identity and more guarantee that this person is who he/she claims to be. [40]



Dynamic Signature Depiction [40]

Signature dynamics is distinctive from a digitized signature. A digitized signature is merely a electronic duplicate of a someone's signature, not a biometric system that acquires the tempo of signing the way the person holds the marker, and the weight the signer puts forth to produce the signature. [40]



Graphic Depiction of Dynamic Signature Characteristics [40]

Keyboard Dynamics: Signature dynamics is a process that obtains the electrical signals when an individual signs a signature. Keyboard dynamics captures electrical signals when a person types a certain expression. When an individual types a certain saying, the biometric system

obtains the quickness and motions of this act. Every person has a definite manner and speed that transforms into unique signals. This method of authentication is better in terms of effectiveness then typing in a password, due to passwords are easily obtainable. Repeating individuals typing style is much harder to repeat then it is to obtain a password. [40]

Iris Scan A persons iris is the colored section of the eye that encircles the pupil. The iris has distinctive, rifts, colors, rings, coronas, and furrows. The distinctiveness of each of these features within the iris is obtained by a camera and compared with the information assembled during the enrollment period. [51]

Palm Scan: The palm holds an abundance of information, and has many features that are used to verify an individual. On a persons palm there are creases, ridges, and grooves allover that are only found to a specific person. Palm scans also comprise the fingerprints of individual fingers. Individual place their hand on a biometric device, which scrutinize and gathers the information. This data is linked to a reference profile and the identity is verified or rejected. [52]

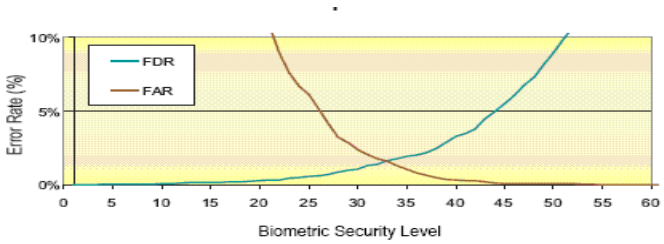
Hand Geometry: this biometric device obtains information based on the shape of an individuals hand; the length and width of the hand and fingers, this data characterizes how hand geometry is defined. Individual features differ substantially among people and is utilized in various biometric systems to confirm identities. To engage this device one would place his/her hand on a device that contains channels for individual fingers. This device obtains the geometry of each finger, and the hand entirely, to the information in a reference database to confirm that person's identity. [53]

Facial Scan: Biometric device that gathers facial attributes and characteristics into account. Individual have dissimilar skeletal structures, nose rim, eye thickness, forehead dimension, and chin contours. This information is all captured throughout a facial scan and

compared to an earlier obtained scan held within a reference database. When the content matches the data the person is positively identified and allowed access to the system. At the same time, passwords are also widely considered a tremendously inadequate form of protection. Password problems are difficult to administer since a single computer system have hundreds or thousands of password guarded accounts and just one needs to be negotiated to give an attacker access to the local system or network. Today because of the interconnected Internet, the problems are would-be devastating on a yet larger scale. [54]

Biopassword

This solution combines one factor authentication "passwords", with a biometric method something you are "keystroke dynamics". This takes in to account the typing rhythm using the study of keystroke dynamics. "Keystroke dynamics is the technology that measures "key up" and "key down" event timings as endusers type a line of characters in a field". [67]



Biometric level threshold [67]

Biopassword protects against social engineering, phishing, pharming, inherent password, lost, stolen, shared, or weak passwords, brute force attacks and keystroke loggers. This is possible because it uses a typing rhythm to authentication endusers. If the attacker has the password he/she will be unable to access the account unless he/she is able to mimic the typing technique of the authorized persons. This is impossibility, no two people type using the same keystroke dynamics. [50]

Biopassword keyboard dynamics [49]

Token based Devices

The token device, also known as a password generator, is typically a device held in the hand. It has an LCD viewer and may also have a keypad. This hardware device is apart from the system the enduser is trying to authenticate to, or access. The token device and authentication device will have to synchronize in order to be authenticated to the enduser. A token device confronts the end user with a listing of characters that need to be inputted as a key when signing onto a system. The only two devices, the token and authentication service discern value of these characters. When the two are in sync, the token device generates the exact password the authentication service is waiting for. This is a one-time password, also called a token. Once used, it is no longer applicable after first use. [55]

Synchronous token devices will have to synchronize with the authentication service by using time, or a counter as the center piece of the authentication process. When the synchronization is using a time based system, the token device and the authentication service will have to maintain the identical time within their internal timer. The time rate on the token device and a secret key are used to create the one-time password. This will be displayed to the enduser to input. The user inputs this value and a user ID into the system. This is then sent to the server running the authentication service. The authentication service decrypts the value and

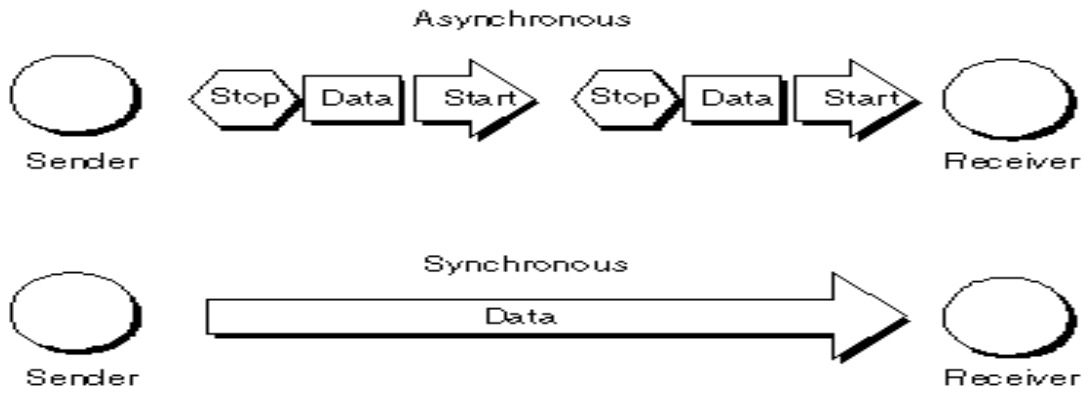
compares it with the value that expects. When the two match, the enduser is authenticated and given access to the system and allowed the system resources. [56]

When the token device and authentication service use counter-synchronization, the enduser will have to begin the logon cycle on the system and press a button on the token device. This allows the token device and the authentication service to move ahead to the next value. This value and a base secret are hashed and given to the enduser. The enduser should then enter this number together with a user ID in order to gain access. In whichever time or counter based synchronization, the token device and authentication service have to split the matching secret base key used for encryption and decryption. [56]

Asynchronous token devices that employ asynchronous tokens producing process use a challenge response design to authenticate the enduser. In this situation, the authentication server gives the enduser a challenge, which is a random value, which is called a nonce. The user inputs this random value into the token device. The token encrypts it and gives back a value that the enduser uses as a one-time password. The user forwards this value, together with a username, to the authentication server. If the authentication server is able to decrypt the value and it's identical to the challenge value that was sent before, the enduser allowed access. [57]

Asynchronous and synchronous token devices

Asynchronous communication does not synchronize the data in a steady stream. In its place the data is sent in bits and pieces. Case in point the internet, data packets are sent to the destination by a good authentication. Yet this type of system is not vulnerable to electronic eavesdropping, sniffing, or password guessing. [57]



How synchronous and asynchronous devices transfer data [13]

"Asynchronous a token device that is using an asynchronous token-generating method uses a challenge/response scheme to authenticate the user. In this situation, the authentication server sends the user a challenge, a random value also called a nonce. The user enters this random value into the token device, which encrypts it and returns a value that the user uses as a one-time password. The user sends this value, along with a username, to the authentication server. If the authentication server can decrypt the value and it is the same challenge value that was sent earlier, the user is authenticated". [32]

"Synchronous, occurring at regular intervals syn-, meaning "with," and chronos, meaning time" [31] "A synchronous token device synchronizes with the authentication service by using time or a counter as the core piece of the authentication process. If the synchronization is time based, the token device and the authentication service must hold the same time within their internal clocks. The time value on the token device and a secret key are used to create the one-time password, which is displayed to the user.

The user enters this value and a user ID into the computer, which then passes them to the server running the authentication service. The authentication service decrypts this value and compares it to the value that it expected. If the two match, the user is authenticated and allowed to use the computer and resources. If the token device and authentication service use counter-

synchronization, the user will need to initiate the logon sequence on the computer and push a button on the token device. This causes the token device and the authentication service to advance to the next authentication value. This value and a base secret are hashed and displayed to the user". [32]

Smart Cards

A smart card looks a lot like a credit card in dimension and silhouette, but internally they are entirely different. If you were able to take a smart card apart, you would see it has a microprocessor internally. These internal circuits can process data. Credit cards don't contain processors, they have magnetic strips. The microprocessor is beneath a gold contact pad contained on one side of the card. The main purpose of the microprocessor imbedded in smart cards is for security reasons. The computer and card reader communicate with the microprocessor. The microprocessor implements or starts access to the data on the card. [57]

Today the use of magnetic stripe cards is in use throughout the country. Although the information on the stripe can be read very easily, written, erased or changed with tools that can be found in most electronic stores. Consequently, magnetic stripes are in fact not the number one choice when it comes to storing confidential data. Due to the easily manipulated cards, in order to protect consumers companies have devoted large amounts of money into widespread online mainframe based networks for verification and processing. [58]

Most smarts cards have eight-bit processor, 16KB read-only memory, and 512 bytes of random-access memory. Smart card use serial interfaces that get there power from external sources like a card reader. The processor uses a limited instruction set for applications such as cryptography. [33]

There are two kinds of smart cards: contact and contact less. One difference is memory cards hold non-volatile memory storage elements. Smart cards contain a microprocessor and have volatile memory and a microprocessor. The contact smart card is imbedded with a gold seal on the front of the card. At the time the card is placed into a card reader, electrical impulses rub against the card, in the precise spot that the chip contacts are positioned. When this sequence is initiated this gives the power needed to supply power and data I/O to the chip for authentication function. The contact less smart card has antenna wire that encircles the border of the card. At the time the card moves within an electromagnetic area of the reader, the antenna inside the card produces adequate energy to power the inner chip. When this process takes place the broadcast goes through the antenna and starts process of authenticating the enduser. Authentication is finalized when the one time password, challenge, response or inputting the endusers private key. This takes place if in a public key setting. [33]

Strengths and Weakness of smart cards

One of the disadvantages of to using smart cards is associated with the cost of readers plus the operating cost of card generation, the same with memory cards, even if this cost is decreasing. Smart cards alone are higher priced than memory cards. This is due to the added extra integrated circuits and microprocessor on the cards themselves. [59]

Smart cards and memory cards are susceptible to masquerading if the enduser gives his ID or username; as a consequence the token device is shared or stolen. Tokens devices may also experience battery failure or other technical malfunction. [59]

These technologies are not perfect and no measure is, but they have significant benefits over the typically password, and are developing into more effective means when in combination. Password use will be around for a long time because they are easy to use, and most businesses

don’t want to spend the money for better security measures. Today’s organizations that want to manage system access to their data and systems will want to think about stronger procedures of authentication instead of the common easily compromised use of passwords. [48]

Current Authentication Methods

Currently one factor authentication is place in the form of user name, and password. When an enduser has forgotten his/her password loss prevention is able to reset all passwords to systems. There are many different applications in use, in order to gain access, the enduser has to authenticate to each system. This has been a problem because of the security policy.

Passwords have to be at least seven characters, and must contain special characters and in addition to the choice of character from the alphabet. Password must be changed every thirty days; previous passwords cannot be used when selecting a new password.

Problem with Current Authentication Methods

One factor authentication is not very secure. This is because of the many attack options available to attackers attempting access an organizations resources for the purpose of financial profit. The time it takes to reset all the passwords Password resets are a problem by the volume of resets. On a daily basis there are approximately 30 to 40 resets or more. There is no data on the actual cost associated with password resets. However, according to the Gartner Group, approximately 20% to 50% of all help desk calls are for password resets. Forrester Research states that the average help desk labor cost for a single password reset is about $70”.[36]

Because they are sometimes had to remember endusers write their password down on paper and place them under the keyboard. Password age is set to thirty days; hence passwords for users expire after 30 days. Because users have to form new passwords every 30 days, they now have to remember new passwords. Also, previous passwords cannot be reused because of the

security policy. This creates a situation where password use because very difficult to manage. [48]

Possible solutions to the problem of passwords:

One time password:

One possible answer to avoid against compromising a system would be the use of one time passwords. A one time password can only be used once, so if an attacker were to obtain the password it would be useless, because one time passwords only work once. After initial use they are not valid. This may offer the greatest protection. If the same password is identical at each and every login it's identified as static password. Passwords that require changing at each logon is identified as a dynamic password. One time passwords would work in most situations, but because Bank Group has many passwords to different systems, there would be problems getting the different systems to use this kind of authentication method. Another complication with one time passwords is if an attacker gained the password he/she would have access to all applications because only one password would give access to the entire network. [59]

Passphase:

Passphrase function the using the same rule as passwords, and are used in precisely the same way. Most of the identical issues you have with passwords are connected with the passphases; forgotten, enduser may write it down, or share it.

Biometric:

"Biometric authentication is only warranted for high-risk systems where the cost of the breach would be greater than the cost of the system, if there is a system with large amounts of customer information or high-value money transfers, then biometric devices may be appropriate". [45]

Fingerprint:

Most biometric systems would be a good replacement for the current solution, but are very expensive, and the amount of time for enrollment exceeds what would be considered acceptable. Implementing a fingerprint system would require quite a few hardware items.

Retinal scan

Although this type of access control device is very accurate, it is one of the more expensive, and is mostly used in restricted high end security applications. Because of the very high cost and use mostly in restricted areas this method would not be practical. [39]

Signature dynamic:

Another possible good biometric solution, but because endusers may not always sign their signature the same way each time, this could be a problem. Some people sign their signature different at different times, or if a physical problem occurred with where the signing hand was injured the signature would not be the consistent, the enduser would have to go through the process of initiation again. When there are hundreds of employees at an institution this could be a huge problem. [41]

Iris scan

Most people consider this system to be to intrusive, damaging to the eye and time consuming for enrollment. Not to mention the cost to implement an Iris systems. Iris systems are some the most costly compared to other biometric systems.

"Retinal scanners are not at present good candidates for widespread use. First they are expensive. Second, in order to work, users must permit light beams to be shone directly into their eyes for 10 to 15 seconds. The sensation is unpleasant and intrusive enough to make widespread

acceptance among the general public unlikely. Additionally, diseases such as cataracts can cause the retina to change over time". [43]

Hand geometry:

Because of the lack of uniqueness with this type of biometric system, it would not be a good choice to implement because identification is one of the key aspects needed for any authentication system. Organization want to insure a person who is attempting access to their systems is in fact who he/she claims to be. [44] "Unlike fingerprints, the human hand isn't unique. One can use finger length, thickness, and curvature for the purposes of verification but not for identification". [44]

Facial scan

This solution is not quite as good as some of the other biometric solutions. Early reports by the Palm Beach airport, testing was not good because of were not adequate. Early test showed out of several employee scans of about one thousand only 15 were matches. These were early tests, but there are no posted reports of the current statistics. [46]

This solution is also not good because of the cost of hardware. Every person would have to have a camera on their monitors. A facial system is better suited at entrance to high security area, not desktops. [46]

"Fingerprints can be spoofed, and images of them can be stolen, just like user IDs and passwords. The same can be said for a system based on facial recognition. A photograph of the user could be used to fake out the system." [45]

Smart cards

Smart Cards are used for payphones, mobile Communications, banking & retail. This solution is not recommended for general use authenticating enduser for system access. Smart

cards are not used to authentication enduser access in a Domain Active Directory structure. Having every endusers carry a smart token would add additional problem into the scenario, not to mention the cost alone of purchasing the many tokens that would be needed.

Recommended solution

Bio password this solution uses the endusers keyboard based on how he/she types; keystroke and rhythm. In combination with the typical user name and password coupled with biopassword to verify a person is who he/she says they are. Biopassword has a 99% FAR acceptance rate.

Why choose this solution:

Using Biopasswords eliminates the need for endusers writing down of passwords, phishing, password sharing, shoulder surfing, and key loggers. These are eliminated because keystroke dynamics are the only way a person has access to a system. The only way to gain access to a system with Biopassword enabled is to use the same rhythm of an authorized person. It is very unlikely for two people to type using the identical typing method or rhythm.

According to the manufacturers of Biopassword, their solution is 99% effective. This solution is also practical in that it integrates with Windows Active Directory. Biopassword is also compatible with all of the current applications at Bank Group. Because biopasswords work anywhere there is a keyboard, it can also be used with a cellular phone.

Additionally, the cost of using Biopassword is lower then any of the other solutions, and the rate of effectiveness is just as good as the best biometric system. The cost for Biopassword in increments of 50 employees using the Enterprise Edition is $2,500 for licensing fees.

The annual cost of maintenance after initial implementation is estimated to be only $450.00. Thus, the total annual cost to the organization is only $2,950.

References:

[1] http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci213757,00.html
[1] http://ez.no/doc/ez_publish/technical_manual/3_6/concepts_and_basics/access_control
[2] CISSP Exam Guide Shon Harris
[2] CISSP for Dummies pg 32.
[3] CISSP Certification Shon Harris
[4] The CISSP Prep Guide pg. 49
[5] The CISSP Prep guide pg. 49
[6] CISSP for Dummies pg. 31
[7]CISSP certification Shon Harris pg. 133
[8] CISSP certification Shon Harris pg. 133
[9] CISSP for Dummies pg. 30.
[10] The (ISC) CISSP CBK review seminar v5.0 student manual pg.105
[10-1] CISSP Prep guide pg. 109
[11] CISSP for Dummies pg. 158
[12] CISSP for Dummies pg. 154
[13] CISSP Prep guide pg. 49
[14] CISSP Prep Guide pg. 49
[15] CISSP All in one 3rd edition Shon Harris electronic pg 129
[15] CISSP Prep Guide pg. 50
[15] CISSP Prep Guide pg. 50
[16]
http://www.certmag.com/articles/templates/cmag_department_sec.asp?articleid=322&zoneid=43
[16] CBK review seminar pg. 101
[17] CBK review seminar pg. 103
[18] CISSP for Dummies pg. 31, 32
[19] CISSP for Dummies pg. 34
[20] CISSP for Dummies pg. 37
[21] http://en.wikipedia.org/wiki/Image:Fingerprintonpaper.jpg
[22]http://en.wikipedia.org/wiki/Image:Measuring_fingerprints_w_compass_RCMP.jpg
[23] http://en.wikipedia.org/wiki/Image:Human_eye_cross-sectional_view_grayscale.png
[24] http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.html
[25] CISSP Prep guide pg. 107
[26] ISC CBK review seminar pg. 106
[26] CISSP certification by Shon Harris pg. 131
[27] CISSP certification by Shon Harris pg. 131
[28] CISSP certification by Shon Harris pg. 131
[29] http://support.microsoft.com/kb/310105
[29] http://www.windowsecurity.com/articles/Passwords-Attacks-Solutions.html
[30] CISSP ALL IN ONE Shon Harris pg. 136
[31] CISSP Exam Guide Shon Harris pg. 140
[32] CISSP Exam Guide Shon Harris pg. 140
[33] http://java.sun.com/products/javacard/smartcards.html
[34] http://www.investopedia.com/terms/n/netincome.asp
[35] CISSP EXAM ALL IN ONE Shon Harris pg. 143

[36] http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm
[37] http://focus.ti.com/vf/docs/blockdiagram.tsp?family=vf&blockDiagramId=6020#
[38] http://focus.ti.com/vf/docs/blockdiagram.tsp?family=vf&blockDiagramId=6020#
[39] http://www.wisegeek.com/how-does-a-retinal-scan-work.htm
[40] http://www.biometrics.gov/docs/dynamicsig.pdf
[41] http://www.biometricnewsportal.com/signature_biometrics.asp
[42] http://news.bbc.co.uk/1/hi/uk_politics/4580447.stm
[43] http://terrorism.about.com/od/controversialtechnologies/g/RetinalScans.htm
[44] http://biometrics.cse.msu.edu/hand_geometry.html
[45] http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1242775,00.html
[46] http://www.wired.com/politics/security/news/2002/05/52563
[47] http://web.mit.edu/ecom/Spring1997/gr12/2USES.HTM
[48] http://www.certmag.com/articles/templates/cmag_department_sec.asp?articleid=322&zoneid=43
[49] http://www.biopassword.com/demo1/
[50] http://www.biopassword.com/authentication-software-news.php
[51] http://ctl.ncsc.dni.us/biomet%20web/BMIris.html
[52] http://www.gadgetreview.com/2005/12/biometric-vein-palm-scanner.html
[53] http://ctl.ncsc.dni.us/biomet%20web/BMHand.html
[54] http://www.biometricgroup.com/
[55] http://whatis.techtarget.com/definition/0,,sid9_gci796060,00.html
[56] http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci213080,00.html
[57] http://computer.howstuffworks.com/question332.htm
[58] http://money.howstuffworks.com/credit-card2.htm
[59] http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1265056,00.html
[60[http://www.cs.rochester.edu/~sandhya/csc256/lectures/lecture18-security.pdf
[61] http://www.thepcspy.com/read/passwd_files
[62] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci499492,00.html
[63] http://www.pcmag.com/encyclopedia_term/0,2542,t=replay+attack&i=50439,00.asp
[64] http://www.eff.org/wp/biometrics-whos-watching-you
[65] http://www.garykessler.net/library/password.html
[66] http://www.securityfocus.com/archive/1/402758
[67] http://biopassword.com/partnerportal/BP%20Tolly%20Report.pdf