

BANKING AUTHENTICATION METHODS

Authentication Methods Used for Banking

Seth Thigpen

East Carolina University

Abstract

Banks are storehouses of personal identifiable information. With identity theft on the rise, these organizations must take information security very seriously. There are multiple ways that banks can authenticate users—that is, make sure they are who they say they are. These methods range from username and password combinations to iris scanning. As technology continues to change, banks must adapt their security systems to effectively combat hackers and thieves. Selecting the right technologies for each organization cannot be generalized. However, knowing what authentication techniques are available is the first step in maintaining a secure environment. This paper gives insight into some of the more prevalent technologies currently being implemented in large organizations today.

Authentication Methods Used for Banking

Introduction

Millions of internet users access servers each day. Many of these servers are freely available to the public. They allow anyone to use the service. Google.com for example allows anyone to use its search features with no need to verify the user's identity. There are other circumstances, however, where the company needs to keep a vigilant watch over who can access services. These companies range from universities to gaming sites. Banking companies are a prime example of organizations that must authenticate users before allowing them access to critical resources.

Authentication is defined as "... the process by which a computer, computer program, or another user attempts to confirm that the computer, computer program, or user from whom the second party has received some communication is, or is not, the claimed first party."

(Wikipedia, 2005) In other words, someone has the need to verify that someone else is who they say they are. Authentication can be completed via the use of many different methods. Some of these methods are far superior to others, but are more difficult to implement and fund.

Authentication is not enough to grant users access on its own. Authorization is the next step in the procedure. Authorization is the process by which a computer system or individual grants access to a user for various reasons. The user must first authenticate himself to the system. The system will then check the user's authorization and decide if that user has sufficient access to the resource he is trying to access. Only then will the system grant the user access to the resource. However, this is still not the end of the process. Accounting must take place too.

Accounting is the process of recording access to a resource. Specifics on the accounting format may vary from system to system, but is a key part of the authentication process. It is always a good idea to know what user is accessing the system and when that user does so. This can aid in investigations if problems appear in the future.

Banks are organizations that must take the authentication process very seriously. Banks are storehouses of critical personal identifiable information. This information may include: social security numbers, physical addresses, phone numbers, email addresses, account numbers, credit histories, employment histories, and other information pertaining to the organization's clients and the employees.

Physical Security

Do not overlook the security regarding the organization premises itself. After all, if there is no physical security, there is no need for technical online authentication methods.

Documented procedures and multiple lines of defense are imperative to secure an organization's physical property.

The measures taken to secure property will vary greatly depending on the organization's needs. More security measures are required at locations which contain critical information or items of value. In regards to security for technical resources, documented procedures must be in place and available to employees.

Banks must have multiple security measures in place. The perimeter of a facility may require razor wire fencing. All property outside of the facility's structures should be well lit and may benefit from security patrols, guard dogs, or simple closed circuit security cameras.

“Security guards are one of the best mechanisms for ensuring physical security because they are flexible, provide good response, and are a very effective deterrent.” (Campbell et al, 2003)

Most facilities do not have such perimeter defenses keeping in mind that each organization has its own needs.

All building entrances should have proper locking mechanisms. These may range from ordinary preset locks to swipe cards or iris scanners. Here is where authentication really needs to be considered.

AAA

AAA (pronounced “triple A”) is an acronym meaning Authentication, Authorization, and Accounting (sometimes referred to as Access Controls, Authentication, Accounting). The AAA model was created to maintain control over user access. It is the framework underlying who has access to what resources, when, and for how long. AAA can be implemented in basic forms such as building access or in complex computer network systems.

Authentication “requires users ... to prove that they really are who they say they are.” (Roland, 2004) Authorization then takes place, and governs what the user can access. This can be accomplished via many different methods including operating system policies, network AAA servers, hard coded lists, etc. Finally, the entire process must be documented. Accounting can be thought of very much like finances in business. When did the user authenticate? What did the user access? How long did the user access the resource?

The reason for such a model is that organizations need to limit access to resources to trusted users. There may be a need for multiple levels of authorization such as differentiating between a C.E.O., a network administrator, or a teller. A C.E.O. may have access to all resources used in daily business, while a teller may only have access to basic computer terminal applications (such as email or financial software). Finally, everything must be recorded in case

future conflicts arise. If property is missing or a server configuration is changed, accounting logs can yield information concerning possible suspects.

Authentication Methods

Methods for authentication can be organized into a few basic categories. They can be one of several things directly related to the user. Basically, this is something the user knows, something the user possesses, the way the user behaves, or a physical characteristic of the user. The following figure categorizes some of the authentication methods. Note that this is not an exhaustive list.

Categorization of Authentication Methods

User Knows	User Possesses	User Behaviors	User's Physical Characteristics
Password	Swipe Card	Speech	Fingerprint/Palm print
PIN	Proximity Card	Signature	Hand Geometry
Identifiable Picture	USB Token One Time Password	Keyboarding Rhythm	Iris Features

Information the User Knows

Username and Passwords

Probably, the most basic form of user authentication is by a username password combination. This type of authentication is extremely weak. More and more problems are occurring with its use. The idea here is that a user possesses a unique identifier such as an employee number. He also has a secret phrase that is paired with the identifier. When the user authenticates, he provides his unique identifier and supplies his secret password. Since the user

is the only one who is supposed to know the secret password, he is authenticated and is the person he says he is.

Using passwords for authentication is the simple idea. Assign a unique identifier to a user and instruct that user to supply a password to correlate to that identifier. Administration is also pretty simple. Almost all computer systems have built-in applications to handle passwords. The user identifiers and passwords can be stored in a database allowing the entire process to be completed with the user as the only source of human input.

Surely many problems can be identified with this technique. Username and password combinations have a fundamental flaw stemming from human psychology. Passwords should be easy to remember and be easy enough to provide swift authentication. On the other hand, in terms of security the password should be difficult to guess, changed from time to time, and unique to a single account. (Wiedenbeck, 2005) Because of these requirements, many people feel the need to physically record their password (often times in close proximity to the authentication device). Furthermore, as technology increases, attacks targeting passwords are becoming easier to implement. High powered computers make it quite efficient to initiate dictionary and brute force attacks to obtain the password.

Passwords are highly susceptible to man in the middle attacks and if someone simply watches you enter the code. Since passwords are still vastly implemented in computer systems, there are some best practices for their creation. Passwords should be alphanumeric, meaning that they require both letters and numbers to be valid. They should also have a minimum length. Six characters seem to be a generally accepted minimum but more and more systems are moving to 8 characters minimum. For added security, passwords should also encompass special characters like the asterisk (*), semi-colon (;), or dollar sign (\$). Note that many computer systems do not

allow special characters in the password. This has held true with online banking computer systems.

PIN

A personal identification number (PIN) can be used in much the same way as a password. It is numerical in format and like a password should be kept secret. The most common use of the PIN is for automatic teller machines (ATM). “Most commonly PINs are 4-digit numbers in the range 0000-9999 resulting in 10,000 possible numbers, so that an attacker would need to guess an average of 5000 times to get the correct PIN.” (Personal Identification Number, 2005) This presents a problem, however. If a hacker is trying to guess a PIN, by statistical calculations it will take some time. If a computer does the work, it may take a matter of seconds. This is why most systems implementing a PIN have a lockout feature. If the user or anyone else enters the wrong PIN more than a predetermined number of times, the user account will be locked until an system administrator reactivates the account. This is usually the case with the previously discussed password system as well.

Identifiable Pictures

A newer form of authentication has emerged promoted by the use of handheld devices (which are not as friendly to user input) and problems surrounding passwords and personal identification numbers. The idea behind using pictures in place of a password or a PIN is that users must recall a password; however, they recognize a picture. This allows the system to show multiple pictures and let the user recognize the correct picture that will provide access to the account. Studies have shown that this method of authentication can reduce the ability of a hacker to guess the correct authentication key and reduce a hacker's ability to record the correct

key (since it is a picture). (De Angeli, 2005) Some banks are beginning to integrate pictures as part of their authentication systems.

One-Time Password

Another related method is the one-time password. This is extremely similar to the basic username and password combination except that the password never travels through the public network. RFC 2289 explains one method for accomplishing a one-time password authentication. The system uses a client side generator and a server. Basically, the generator accepts a secret password from the user and concatenates it with information sent from the server in control of the authentication. Various computations and hashes are performed on the user's secret password which can be verified by computations by each end of the communication. This type of system can protect against passive attacks against which basic password systems may be vulnerable. (RFC 2289 - A One-Time Password System, 1998)

Items the User Possesses

Swipe Card

Anyone interested in modern banking is familiar with the common swipe card. One prime example is the credit card. Swipe cards are small and contain a magnetic strip holding information about the user's identity. This type of authentication can be used in conjunction with other authentication methods such as a PIN. (SafeNet, 1999) The card by itself is not a sufficient means of authentication since it is prone to theft. The data on the card can be duplicated by means of the proper equipment. This means that a third party could possibly create a card with the same information or simply use the information in a different method.

Proximity Card

Proximity cards work in much the same fashion as swipe cards but work from a distance which varies from vendor to vendor. The card contains information by which to authenticate that the person holding the card is the person who is authorized to access a certain resource or door. That individual simply places the card near the card reader and the information is exchanged wirelessly. The proximity card shares the same problems that magnetic swipe cards do, that is, with the proper equipment, the card can be duplicated or the information can at least be stolen. (He, 2003) These types of cards are used in numerous organizations including universities.

USB Token

The USB tokens are very much like their plastic card counterparts. The token contains information about a user's identity and serves a method for the user to access protected resources. The USB token must be plugged into a computer's USB port so that the computer has access to the information. Often times, software licensing information may be stored on these devices. This makes it easy to account for legal and financial records. As with other authentication items which users possess, USB tokens can be lost, stolen, or broken.

User Behaviors

Speech

Speech authentication is a modern approach to user authentication. Long have people wanted to simply tell their computer what to do. This is becoming a reality. A combination of voice authentication hardware and software can allow an organization to verify the identity of users by phone, wall mounted device, or the Internet. "Voice authentication captures a person's voice—the physical characteristics of the vocal tract and its harmonic and resonant frequencies—and compares it to a stored voiceprint created during an enrollment process." (Gilhooly, 2003) This means that a user first records his voice to store on the system. The

computer calculates different characteristics of that user's voice and stores the information.

When the user wants to authenticate, he speaks a predetermined phrase used in the initial recording, such as his name. The computer can determine if the voice patterns match and based on those calculations, grant or deny access to a resource. One drawback of this method of authentication is that if a user has severe laryngitis, the system may not recognize the user's voice. (Markowitz)

Signature

Signature authentication is yet another method to authenticate a user. Users are either required to register their signature before using the system or actively use it and let the system learn the signature over time. Signature authentication also usually requires a tablet on which the user can sign. "Penflow(TM) is currently deployed at leading banks and other financial institutions where signature authentication helps to reduce fraud and streamline workflow processes. Other industries that have already benefited from signature authentication include the government, Homeland Security, medical, telecommunications, energy, aviation, armed forces and the legal sectors." (Landon, 2004) Banks have to inspect signatures on a very large number of documents on a daily basis. Technology like this can prove to be an extremely resourceful time saver.

Keyboarding Rhythm

Many jobs today require the use of a keyboard. Since this is already the case, keyboard rhythm authentication can be easily integrated into the workplace. Keyboard rhythm authentication can be accomplished by measuring several distinct characteristics concerning a person's typing techniques. Latency between keystrokes, keystroke durations, finger positions, and the amount of pressure applied to keys can be combined to establish a unique identity to that

user. (Kacholia) The only necessary hardware needed for the user to authenticate is a standard keyboard networked into the authentication system. This authentication method may have profound advantages in future applications.

User's Physical Characteristics

Biometrics

There are many different types of authentication devices available today that take advantage of biometry. Merriam-Webster defines biometry as “the statistical analysis of biological observations and phenomena”. (biometry, 2005) They each have their benefits and shortcomings. “The most secure authentication methods include layered or ‘multi-factor biometric procedures’.” (Artemis Solutions Group LLC, 2004) Biometric characteristics are hard to counterfeit since each individual has unique physical properties based on heredity.

Fingerprint

No two humans on earth have the same fingerprint. Even each finger for the same person has a different pattern. This even holds true for identical twins. (Smith, 2005) Because of this fact, fingerprint authentication is an excellent way to differentiate users. Users are first required to scan a specific finger into a computer system. With that user's unique fingerprint on file, a wall mounted device can be deployed at any point that authentication is necessary. The user then applies his finger (the exact finger initially scanned) to the biometric reader. The system calculates a score based on the fingerprints on record and the currently scanned fingerprint. The system checks for similarities between the fingerprints and allows or denies access if the score is above or below a certain threshold. (Ratha, 2001) This technology can also be applied to palm prints.

An outstanding advantage of this system is that the user always has his means of authentication on his person at all times. He can never leave it at home. Another advantage as previously stated is that all fingerprints are unique. Fingerprints are almost impossible to counterfeit or recreate. Residual oil residue from a fingerprint can be found but takes a large amount of effort to transfer to the biometric device. Some drawbacks for the technology are that some people do not have fingerprints. Burn victims may have no finger prints at all. False-negatives may occur if the user does not orient their finger properly on the scanning device. Cuts and blisters can also cause false-negatives.

Hand Geometry

Hand geometry biometric scanners are devices that measure the properties of the human hand on which authorization is based. Like fingerprints, each human hand has differences in finger length, width, and thickness. A hand scanner uses a charge coupled device, infrared light, and light emitting diodes to scan a user's hand. It does not look at fingerprints or palm prints. The device uses mirrors to take measurements from two angles—top and side. This is known as orthographic scanning. (Zunkel) Adult hand geometry rarely changes. Injury to the hands could cause false-negatives to occur. Compared to fingerprint scanners, the wall mounted scanning device will be quite larger.

Iris Features

Iris scanners differentiate between users by measuring features of the eye's iris. "The iris contains many collagenous fibers, contraction furrows, coronas, crypts, color, serpentine vasculature, striations, freckles, rifts, and pits. Measuring the patterns of these features and their spatial relationships to each other provides other quantifiable parameters useful to the identification process." (Williams, 2001) Like other biometric techniques, the user must first

have his iris scanned into the system. The user can then use wall mounted scanning devices to access resources. The system works in much the same way as other biometrics, in that it calculates statistics of the physical differences of the human body. Since there are so many ways a person's iris can be different from another person's iris, the system can accurately authenticate individuals.

Conclusion

As mentioned earlier, Bank of America has incorporated a new authentication system for online users that takes advantage of a human's ability to recognize pictures. "Instead of the traditional user name-password setup, SiteKey users select one of a thousand different images, write a brief phrase and pick three challenge questions." (Nowell, 2005) Other banks are expected to follow suit. Banks in general are also incorporating various authentication methods to grant access to users. To this date, there is no single best solution for authentication. Multiple layers of authentication have proven to be the most effective.

Multifactor authentication is currently the most complete solution. An example of this would be to use a username and password combination with a proximity card. Another example would be to use both fingerprint and speech authentication. There are many combinations that can be implemented. The deciding factors on which methods to choose are cost, administration time, and ease of use for the users. No matter which methods are implemented, the system should integrate with little effects on the system's users. The authentication should be as seamless as possible.

References

- Wikipedia, (2005). Retrieved Jul. 04, 2005, from Authentication Web site:
<http://en.wikipedia.org/wiki/Authentication>.
- Campbell, P., Calvert, B., & Boswell, S. (2003). *Security+ Guide to Network Security Fundamentals*. Toronto, ON: Thomson.
- Authentication, (2004). Glossary of Common Biometric Terms. Retrieved Jul. 14, 2005, from Biometric Glossary of Terms Web site:
http://www.biometricsdirect.com/Content/Biometric_Terms.htm.
- Roland, J. (2004). *CCSP Self-study: Securing Cisco IOS networks (SECUR)*. Indianapolis, IN: Cisco Press.
- Wiedenbeck, S., Waters J., Birget J., Brodskiy, A., & Nasir Memon (2005). Passpoints: Design and Longitudinal Evaluation of a Graphical Password System. *International Journal of Human-Computer Studies*, 63(1-2), 102-127.
- Wikipedia, (2005). Personal identification number. Retrieved Jul. 16, 2005, from
http://en.wikipedia.org/wiki/Personal_Identification_Number.
- De Angeli, A., Coventry L., Johnson G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*, 63(1-2), 128-152.
- Network Working Group, (1998). RFC 2289 - A One-Time Password System. Retrieved Jul. 16, 2005, from RFC 2289 (RFC2289) Web site: <http://www.faqs.org/rfcs/rfc2289.html>.
- SafeNet, (1999). Retrieved Jul. 16, 2005, from Personal Authentication and The PKI Security Process – Benefits of the iKey Web site:
http://www.nasscom.org/download/PersonalAuthentication_PKI.pdf.
- He, R. C. (2003, Dec 9). Proximity MIT Card Raises, Allays Security Concerns. *The Tech*, 123(62).
- Computerworld Inc., (2003). Voice authentication: making access a figure of speech . Retrieved Jul. 16, 2005, from <http://www.computerworld.com/printthis/2003/0,4814,86897,00.html>.
- J. Markowitz, Consultants, (n.d.). Frequently asked questions. Retrieved Jul. 16, 2005, from <http://www.jmarkowitz.com/about.html>.
- Landon, B. (2004). Security Biometrics Integrates Biometric Signature Authentication Into Mainstream Business Applications . Retrieved Jul. 16, 2005, from http://www.pdatoday.com/more/1242_0_1_0_M/.

Kacholia, V., & Pandit, S. (2005). "Biometric Authentication using Random Distributions (BioART)." Department of Computer Science and Engineering, Indian Institute of Technology Bombay, Powai. Retrieved Jul. 16 2005
<http://www-2.cs.cmu.edu/~shashank/papers/bioart/paper.pdf>.

Merriam-Webster Online Dictionary, (2005). biometry. Retrieved Jul. 17, 2005, from
<http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=biometric&x=0&y=0>.

Crystal Guides Ltd, (2005). Why are everyone's fingerprints unique?. Retrieved Jul. 17, 2005, from uknetguide answerbank Web site:
<http://www.theanswerbank.co.uk/Article1388.html>.

Ratha, N. K., Connell, J. H., & Bolle R. M. (2001). Enhancing Security and Privacy in Biometrics-Based Authentication Systems. *IBM Systems Journal*, 40(3), 614-634.

Zunkel, R. L. (n.d.). Hand Geometry Based Verification. Retrieved Jul. 17, 2005, from
<http://www.cse.msu.edu/~cse891/Sect601/textbook/4.pdf>.

Williams, G. O. (2001). Iris Recognition Technology. Retrieved Jul. 17, 2005, from
http://www.rycom.ca/services_solutions/IrisWhitepaper.pdf.

Nowell, P. (2005, July 13). Bank of America Adds New Online Security. *The Associated Press*.