ISRC Future Technology Topic Brief

Future Security Approaches and Biometrics

Prepared by: Serguei Boukhonine
under the supervision of Dr. Blake Ives

What is security?

To understand future security approaches, we turn first to the definition of security. The *Webster New World Dictionary* defines **security** as:

1 the state of being or feeling secure; freedom from fear, anxiety, danger, doubt, etc.; state or sense of safety or certainty

2 something that gives or assures safety, tranquility, certainty, etc.; protection; safeguard

3 *a*) protection or defense against attack, interference, espionage, etc. e.g. funds for national *security*, *b*) protection or defense against escape e.g. a maximum *security* prison, c) procedures to provide such protection or defense

Thus, security approaches in the computer world have both an objective component, i.e. a system that can show demonstrable results of providing protection, and a subjective component, i.e. the feeling of protection that such a system should engender. Unfortunately, feeling secure does not always correspond to objective measures of actual security.

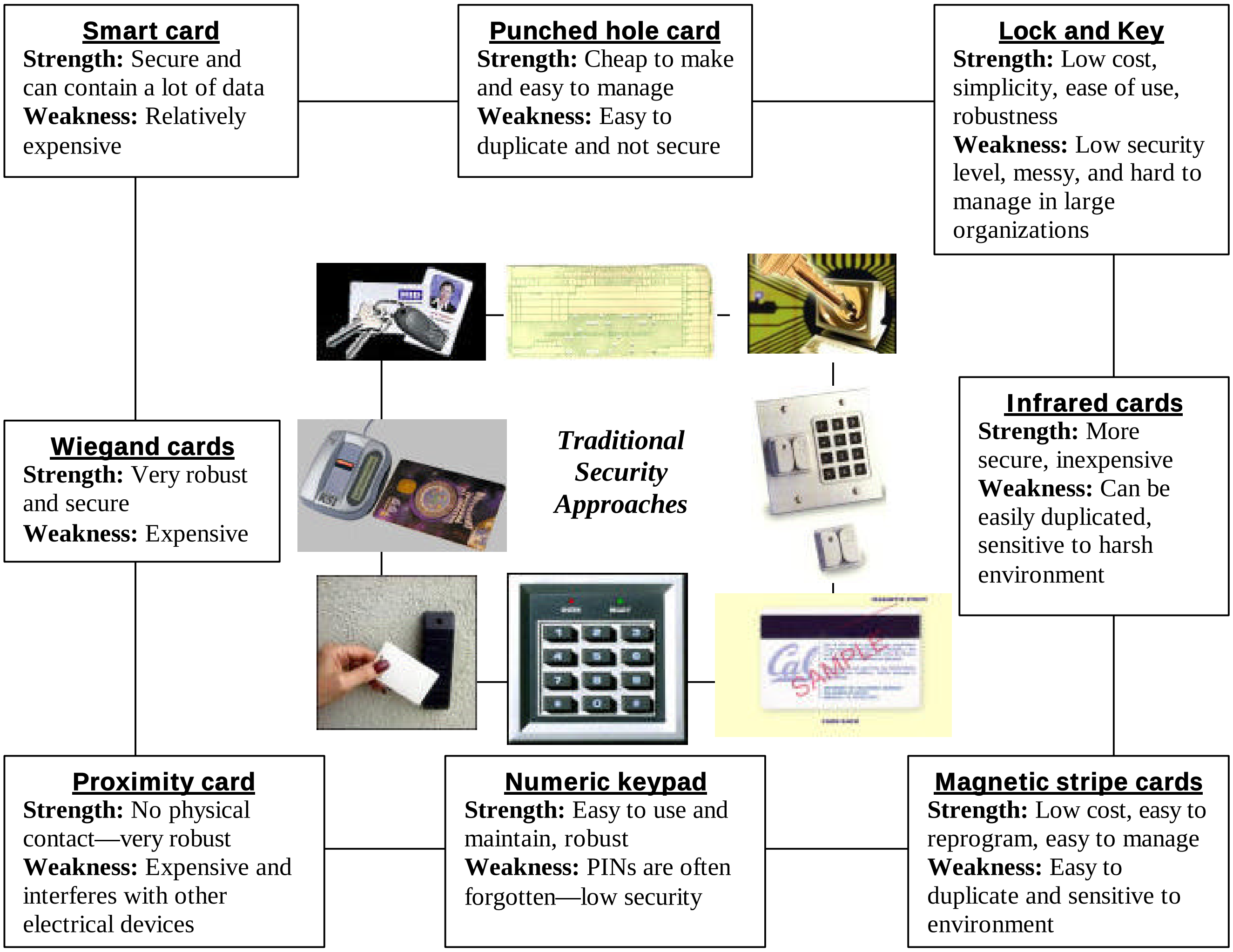
What is wrong with traditional security approaches?

Overall, security approaches can be broken down into two approaches: passive and active. Passive approaches are like a shield **-** they protect against a clear and present danger such as a hacker attempting to access a computer system, while active approaches are more like prevention via a preemptive strike as in arresting terrorists before they plant a bomb.

Traditional security technologies are mostly passive and reactive. There are not many technologies suitable for active security. The only traditional way to proactively search for and identify lawbreakers has been by massive use of manpower such as detectives prowling the mean streets or security guards watching closed circuit television looking for known suspects. This approach is both expensive and vulnerable to human error, negligence, or willful sabotage.

Second, all cards, keys, and username/password combinations have a common flaw: anybody can use them if they have them. Credit cards can also be easily counterfeited and even the most sophisticated card can be lost, stolen or maliciously taken away. Use of PINs and passwords improves the situation somewhat, but the fundamental problem with PINs is that they identify a card but not its user. Obtaining both the card and the PIN might be more difficult than the card alone but is quite feasible, particularly if the owner of the card is forced to cooperate. Thus cards, PINs and passwords can hardly provide highly secure solutions. The same flaw applies to the username/password combination: the password really identifies the username, not the actual user!

Third, while all of the traditional approaches have their strengths, they also have corresponding weaknesses. The following figure presents the traditional security approaches, along with their strengths and weaknesses.



Smart card
Strength: Secure and can contain a lot of data
Weakness: Relatively expensive

Punched hole card
Strength: Cheap to make and easy to manage
Weakness: Easy to duplicate and not secure

Lock and Key
Strength: Low cost, simplicity, ease of use, robustness
Weakness: Low security level, messy, and hard to manage in large organizations

Traditional Security Approaches

Wiegand cards
Strength: Very robust and secure
Weakness: Expensive

Infrared cards
Strength: More secure, inexpensive
Weakness: Can be easily duplicated, sensitive to harsh environment

Proximity card
Strength: No physical contact—very robust
Weakness: Expensive and interferes with other electrical devices

Numeric keypad
Strength: Easy to use and maintain, robust
Weakness: PINs are often forgotten—low security

Magnetic stripe cards
Strength: Low cost, easy to reprogram, easy to manage
Weakness: Easy to duplicate and sensitive to environment

Fourth, whereas the requirement for physical access security has existed since time immemorial, computer threats and problems gained prominence during the 1990s due to the explosive growth of Internet, e-commerce and other computer technologies. The table below summarizes computer threats as perceived in 1992 and 2002. The table shows that the number and severity of threats to networked computers has caused into question traditional approaches to security and demands a new response from IT to deal with the e-world of tomorrow.

Perceived computer security threats comparison: 1992 versus 2002[13]

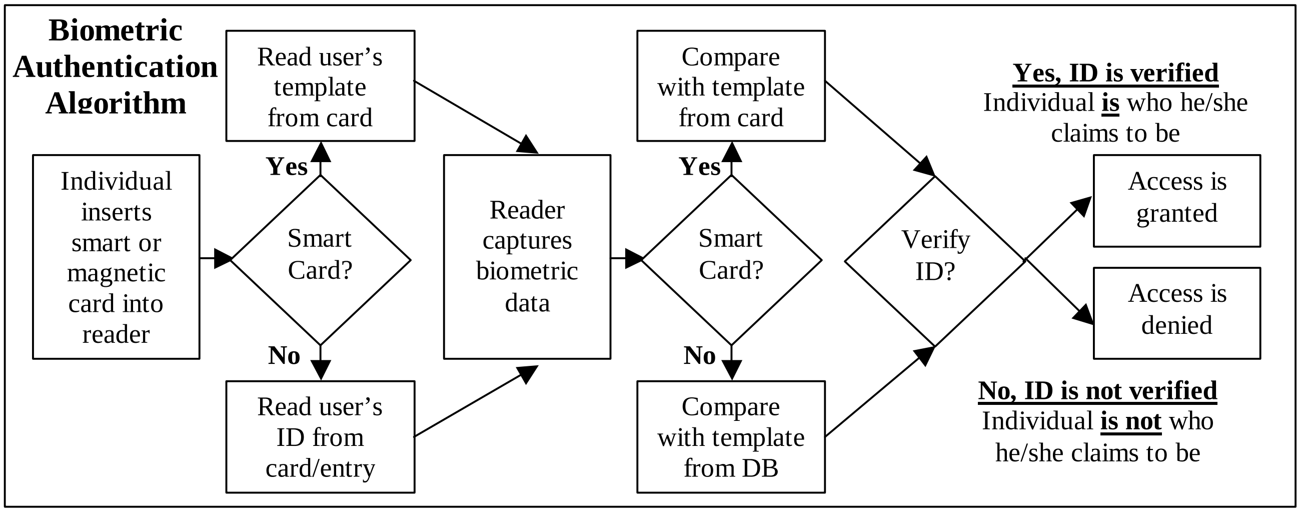
Most severe threats in 1992	Most severe threats in 2002	
1. Natural Hazards	1. Viruses	9. Infringement of IP rights
2. Inadequate control over media	2. System penetration: Hacking/ Espionage	10. Spoofing
3. Weak and Ineffective Controls	3. Fictitious people/ Perpetrators	11. Implied trust exploitation
4. Hacking	4. Denial of Service	12. Active Wiretap
5. Access to system by competitors	5. Insider abuse of net access	13. Sabotage
	6. Unauthorized access by insiders	14. Telecom Eavesdropping
	7. Credit card fraud	15. Repudiation
	8. Human Error	16. Natural Hazards

What is the next step in security?

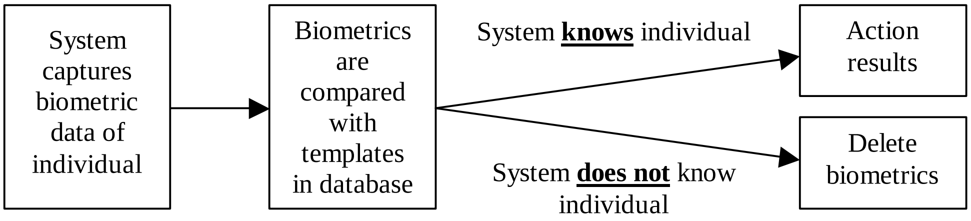
A new branch of science/technology called biometrics holds great promise to solve many security problems. Biometrics is a method of recognizing people based on unique physical or behavioral characteristics. In a contemporary context, biometrics could be defined as **computerized** methods of recognizing people based on unique physical or behavioral characteristics. Even in the ancient times people knew that some individual characteristics of human beings are unique. Ancient Babylonians used handprints to identify sculptors and artists. The first comprehensive biometric approaches were developed in the nineteenth century. Franz Joseph Gall and Cesare Lombroso developed the discipline of phrenology, which attempted, albeit unsuccessfully, to link criminal behavior with cranial shapes and sizes. Frenchman Alphonse Bertillon developed a system of identifying criminals by anatomical measurements called judicial anthropometry, which became popular in Europe and the U.S. The Czech Jan Evangelista Purkinje did scientific research on uniqueness of fingerprints. In 1901 Scotland Yard became the first police force to adopt a fingerprinting system. In 1904 the Argentinean policeman Juan Vucetich published a treatise on this new discipline of dactyloscopy. The fingerprinting technology, now used throughout the world, is the best known example of biometrics. Despite these developments, biometrics did not expand until the end of the twentieth century when computer and other new technologies finally made other approaches possible.

How do biometric technologies work?

There are two different types of biometric technologies: authentication systems and identification systems. The objective of authentication is to determine if a particular person is who she claims to be, for instance to cash a check. Identification systems, by contrast, capture a person's biometric information, say at an airport boarding gate, and then compare it with templates stored in a database looking for a match. Authentication systems require active participation by the individual. Below is the general process for authentication systems. The individual inserts a smart or magnetic card into a reader (instead of a magnetic card the user may key in his or her username). If it is a smart card, the reader reads a biometric template from the card. Otherwise, the reader reads the username. Afterwards, the user's live biometric information is captured and compared with the template either read from the smart card or obtained from the database. If the system determines that the individual is who she claims to be, access is granted. Otherwise, access is denied. While the authentication process looks like security systems of today, biometric systems differ in several respects: biometric information identifies the user of the card and not the card, one cannot forget biometrics like a PIN, and a person's biometrics are unique. Authentication systems currently cost between $100 and $3,000, with applications including Physical Access Control, Logical Access Control, and Time and Attendance.


Biometric Authentication Algorithm
Individual inserts smart or magnetic card into reader
Smart Card?
Yes
Read user's template from card
No
Read user's ID from card/entry
Reader captures biometric data
Smart Card?
Yes
Compare with template from card
No
Compare with template from DB
Verify ID?
Yes, ID is verified
Individual is who he/she claims to be
Access is granted
Access is denied
No, ID is not verified
Individual is not who he/she claims to be

Identification systems are either passive to the individual (meaning they can be used without knowledge of a user) or they require the individual to provide biometric data. Below is the process for identification systems. The individual does not identify herself—the data is captured into the system and the database determines if the system knows or does not know the individual. If the individual is known, then action results, otherwise, the captured biometric data is deleted. Identification systems differ from authentication systems in two ways: 1) The ability to actively look for potentially harmful individuals without their knowledge, and 2) The individual does not need to carry a card or key in the username. Identification systems currently cost between $40,000 and $1 million and are typically used in law enforcement, but may also me used for access control applications (though at speeds considerably slower than authentication systems.


System captures biometric data of individual
Biometrics are compared with templates in database
System **knows** individual
System **does not** know individual
Action results
Delete biometrics

Biometric Identification Algorithm

Below is a picture of a human and the types of biometric technologies that can be used.

Eyes

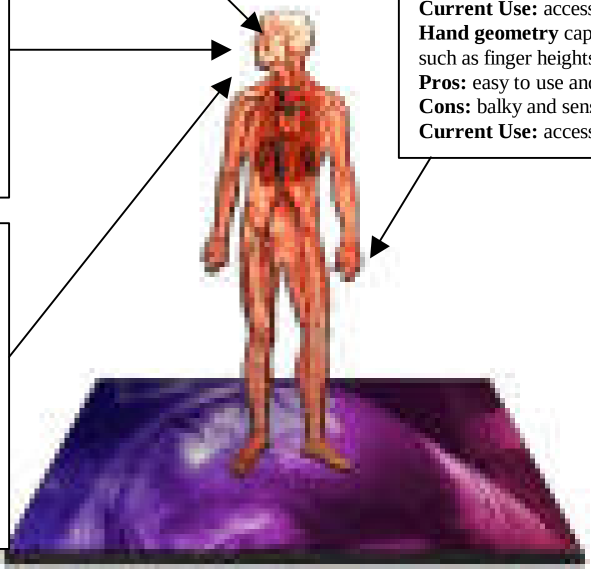
Both retina and iris scanning are used. **Retina** scanning captures unique pattern of blood vessels. It is extremely secure and accurate. However, it is expensive and requires perfect alignment and usually the user must look in monocular or binocular receptacle. **Iris** captures unique patterns of an iris. It is secure, does not need physical contact and non-intrusive. However, it is expensive and sensitive to environmental conditions. Suitable for high security applications in controlled environment.

Voice

Captures unique characteristics of voice.
Pros: Easy to use and understand, non-intrusive, accepted by users
Cons: Sensitive to background conditions such as noises.
Current use: automated call centers, e-commerce

Face

Face recognition captures characteristics of a face either from video or still image and translates unique characteristics of a face into a set of numbers.
Pros: Suitable for identification applications; relatively unobtrusive
Cons: Can be fooled by light conditions, sunglasses, facial hair, etc. Expensive
Current use: Identification (law enforcement) uses as well as identity authentication uses



Hands

Fingerprinting use unique patterns known as loops, arches, and whorls.
Pros: easy to use, inexpensive, large available database
Cons: not as reliable as retina or iris
Current Use: access control, computer access
Hand geometry captures unique characteristics such as finger heights (up to 90 characteristics)
Pros: easy to use and inexpensive
Cons: balky and sensitive to environment
Current Use: access control, computer access

In addition to these major techniques, other Biometric Techniques include vein pattern scanning, use of individual scent, measuring earlobes, individual keystroke dynamics, and signature verification. These methodologies are less developed and are not widely used. Individual keystroke dynamics, such as speed of typing, pauses between words, and intervals between individual characters, could potentially provide on-going identity verification rather just one time verification at the beginning of a session.

What are the projected benefits of biometric technologies?

Biometrics applications will be and already are providing tremendous benefits for both active and passive security applications.

Active (identification) applications

Biometrics will allow systems to be built that will be able to be active in nature and not simply passive. For example, face recognition, will allow law enforcement agencies to increase surveillance, tracking and apprehension of criminals to a previously unimaginable degree. There are working examples already. London's borough of Newham installed 206 surveillance cameras feeding information to the FaceIt® Surveillance, an FR technology developed by Visionics Corporation of Jersey City, NJ. Images of people are constantly matched against a database of suspects and known criminals. The system was installed in November 1998. A year later assaults were down 21 percent and burglaries and vehicle related crime dropped by 39 percent. Biometrics will also be useful for business security applications such as in casinos, shopping malls, and if the recent Super Bowl and Olympics are illustrative, for sporting events.

Passive (authentication) applications

In addition to the active applications, there are a number of passive applications, including:

- Physical access control. Reliability of such systems will be significantly increased.
- Time and attendance monitoring. Biometrics will cut down on cheating such as clocking in for other people.
- Benefit payment systems. Biometrics will reliably verify the identity of a benefits recipient. It will also prevent "double dipping" when an individual uses multiple identities to defraud the system. These have already been successfully used in Connecticut and Spain.
- Border control systems. Biometric data encoded in visas will verify foreigners' identities. Biometrics will allow frequent travelers to bypass lines and reduce border control expenses.
- PC/Network access control. Biometrics will reliably identity a user preventing unauthorized access.
- ATM applications. Biometrics will drastically reduce losses banks and consumers suffer due to fraud.
- Clubs. Biometrics will ensure that only those who belong to clubs may use them and do it without even being noticed by club members.
- National identity cards. If the U.S. gets serious about keeping illegal aliens out, this will be part of the solution.
- Internet verification for e-commerce and home workers. Identity theft will become a thing of the past. Consumers will shop on the Internet with confidence. E-commerce will flourish.
- Eventual elimination of physical id documents, debit and credit cards, keys, etc.

What are the potential problems with biometric technologies?

"The Big Brother" and Privacy Issues

While biometrics may offer the potential for greater security, civil libertarians warn that the emerging technology can also be used "passively" against us, and in places where terrorists are unlikely to tread[9]. "It's inevitable that once you install biometric technology in airports, it will be used in more and more places" says Jay Stanley of the American Civil Liberties Union. "Then we might just slip further down the slippery slope to a surveillance society." Dr. Frank Askin, a law professor and civil liberties expert at Rutgers University, also is wary of the surge in biometrics' popularity. "When you have a lobby that has an economic incentive in this, and when it's being fueled by concerns about terrorism, there's always the potential for going overboard," says Askin. Many people have the Orwellian fear that "…Big Brother will take the data from all those digital body and create the monster of all databases, capable of tracking every move from cradle to grave." And at the moment "…there are no substantial privacy laws to protect against misuse[8]."

On the other hand, many in the biometrics industry believe that biometrics, if used properly, will increase privacy, since if you have somebody's biometric, you do not need other information such as race, gender, SS#, etc. They say that the problem is underlying database management, not biometrics[8].

It is imperative that privacy concerns be addressed. The biometrics industry as well as privacy advocates favor adoption of comprehensive regulations that would prevent possible biometric abuses and protect privacy and civil rights while allowing the industry to develop.

The "Living Person" Issue

In sci-fi or thriller movies, bad (or good) guys sometimes manage to outwit the biometrics authentication systems by neat tricks such as cutting off somebody's finger and using it at a fingerprinting system, using a tape recorded voice password, or even specially doctored contact lenses.

The biometrics industry takes such issues seriously and is working on possible solutions e.g. iris-scanning can detect if there is a pulse in the eye which would take care of attempts to use a prosthetic eye (or something more grisly) and fingerprint technology can measure the finger temperature to prevent that latex finger from being used; it is very difficult to fool a biometric system by a tape recording as one would need professional studio quality audio equipment, not a Walkman. Unfortunately, additional features like this make the technology more expensive and tend to increase time necessary for verification. Other solutions include combining several biometric technologies as well as using biometrics in conjunction with other authentication technologies. However, as chips become ever more powerful, the time for verification will continue to fall, even as further confirmation authentication functionality is added.

When will biometric technologies be available?

Most biometric technologies are already commercially available. The fingerprint technology is by far the most widely available and the cheapest too. All kinds of fingerprint readers, mice, trackballs and cards are available with prices of around one hundred dollars for devices such as ID Mouse Professional from Siemens[11], U.areU. Fingerprint-identification system from DigitalPersona[10] and Access Key and Biometrics PC Card from Compaq. Hand geometry readers, voice recognition, iris and retina scanning and face recognition technologies are all available from a number of vendors.

Driven by increased security concerns, biometric applications will thrive in the near future. Dropping hardware prices in conjunction with improved software will tremendously increase popularity of biometrics system and put

them within reach of most businesses and consumers. Iridian Technologies recently introduced an entry-level iris scanning technology Authenticam to be sold for $299 a unit[12].
In addition to improvements to currently available technologies, futurists predict use of instant DNA testing and brain wave pattern scanning for authentication and identification purposes. In 10 to 20 years these technologies may present a practical alternative for instant identity verification.

DNA testing is extremely accurate but currently requires specially equipped laboratories and takes time. It is extensively used for both identification and authentication purposes in law enforcement but currently is not a practical option for real time security applications.

Iowa-based neuroscientist Lawrence Farwell invented the so called "brain fingerprinting" that may help establish innocence or guilt in a courtroom[15]. His method focuses on a specific electrical brain wave, called a P300, which activates when a person sees a familiar object. The subject wears a headband of electrodes and faces a computer screen, which flashes photos. This technique provides a potential window into someone's past visual experience. If a person looks at random pictures of weapons, without activating a P300 wave, these objects are presumably unknown to him. But if the murder weapon is shown, and a P300 wave activates, then the person clearly has some experience with that weapon.

There are ways to use “brain fingerprinting” for identity verification. Upon being granted access to a restricted area, an individual might be demonstrated a series of unique pictures that would be not be seen by anybody else (e.g. randomly generated by a computer). In the process if authentication, these pictures could be played back to the individual. Only the authorized person’s brain would emit the right response.

Kirsch[16] proposes use of brain scanning in conjunction with iris scanning for identification of terrorists. The gist of his proposal is as follows: after an individual’s identity is established by a biometric such as iris scanning, the individual is shown a series of pictures presumably familiar to terrorists such as weapons while his brain is being scanned. While Americans may be exempted, this procedure may be made mandatory for foreign visitors to the U.S.

How can my organization become involved in biometric technologies?

Most organizations deal with issues of physical access control, time and attendance monitoring, computer/network security, and remote access by telecommuting employees on a daily basis. Fortunately, fingerprinting and other biometric technologies already offer reliable, manageable and reasonably priced solutions for most applications. Biometrics should definitely be considered if an organization has very high security areas such as power plants, classified research labs, etc. There are a variety of information sources that are listed at the end of this paper. Biometrics does not as yet offer financially competitive solutions to tasks such as ATM identity verification although experiments are underway. Face recognition technology is in the process of refinement. Nevertheless, Moore’s Law guarantees these teething problems will go away in just a few years. Below is a checklist of questions that might help your organization to assess possible uses of biometric technologies:

- How does my organization currently deal with physical access restrictions? At what risk?
- How does my organization deal with computer networks and remote access issues? At what risk?
- How does my organization deal with time and attendance issues?
- How does my organization deal with individual customers or online business partners?
- Which technologies are currently used for the above applications?
- What security procedures do we use for online payments?
- Are there biometric solutions to these problems?

- Are there things we could do online if we had better security?

Who (locally) is involved with biometric technologies?

Interactive Controls Inc. is a Houston security company providing biometric solutions. Interactive Controls is upgrading GTE Mobilnet's existing biometric security system at the company's switch offices in Houston. The biometrics system will have one central database holding fingerprint templates and serving several facilities. According to CEO Ben Smith, the company is also beginning to work on time and attendance applications.

Houston's Bank United is experimenting with iris scanning technology from Iridian Technologies[12]. According to Ron Coben, Bank United's executive vice president for community banking, Bank United is testing "EyeTMs" in Houston, Dallas and Fort Worth since 1999. He also says "…iris recognition is consumer-friendly and easy to use."

Biometric Access Corporation has been working with Houston area Kroger and HEB stores on testing fingerprint technologies in a retail environment.

Houston's own Compaq Computer sells fingerprinting technology such as USB Biometric ID Device and Biometric PC Card that use integrated BioLogon™ software fingerprint authentication package.

NASA has been testing a biometric security plan that would allow engineers to control unmanned space flights from their home computer using both facial scanning and fingerprint readers.

Researchers at Rice work on solving problems associated with biometrics use such as replay attacks (e.g. recorded voice password or latex finger). They work on the challenge-response algorithms for biometrics such as voiceprint and keystroke dynamics when an individual is asked to provide a new response (e.g. say a new phrase) when prompted.

For More Information

Online resources

1. The International Biometrics Industry Association site at www.ibia.org
2. Wide range of biometrics information from Visionics Corporation at www.visionics.com
3. Wide range of biometrics information from Viisage Technologies at www.viisage.com
4. U. are U. fingerprint reader for PC from Digital Persona at www.digitalpersona.com
5. ID Mouse Professional from Siemens at www.siemens.com/biometrics
6. A range of fingerprinting PC products from Compaq at www.compaq.com
7. Wide range of fingerprinting technologies from AuthenTec, Inc. at www.authentec.com
15. Brain scanning information at *http://news.nationalgeographic.com/news/2001/07/0705_wirelies.html*
16. Brain scanning combined with other biometrics at http://www.skirsch.com/politics/plane/ultimate.htm

Articles

8. Winter, Christine, "Biometrics: Safeguard or Invasion of Privacy?" *Sun-Sentinel*, October 29, 2000
9. Masterson, Ursula O., "Biometrics and the New Security Age," MSNBC.com, November 20, 2001
10. Mossberg, Walter S., "Sophisticated Security Technology Now Works With Individual's PCs," *Wall Street Journal*, November 8, 2001
11. Currid, Cheryl, "Biometric Mouse Uses Fingerprints to Guard PC Access," *Houston Chronicle*, December 5, 2001
12. Edwards, John, "They Want Your Body," *CIO Magazine*, February 1, 2001
13. Mehta, Manjari and George, Beena, "Security in Today's E-World," Proceeding of…

Important Books To Read

14. Ashbourn, Julian, "Biometrics: Advanced Identity Verification," Springer-Verlag, 2000

Local Contacts

Currid & Co. is a Houston technology-consulting firm that can be reached at www.currid.com.

Nova Marketing is an exclusive Texas distributor of AuthenTec[7] products that can be reached at (281) 240-6082.

Biometric Access Corporation (Austin) (512) 246-3760, 1-800-873-4133, sales@biometricaccess.com

Biometrics research at Rice University www.owlnet.rice.edu/~jlbrick/comp527/statusreport.htm