

## **Business and Technical Factors To Be Taken Into Consideration Before Implementing a Biometric System At Your Place of Business**

Our past articles have examined the biometric technologies that are available today. These articles have been primarily technical in nature, placing particular emphasis upon how each biometric technology works.

Our next series of articles will now focus upon the actual use of biometric technologies in business-especially your place of business. The first article in this business series examines the factors, both business and technical, that you, as the business owner, need to take into account before adopting and implementing a biometric system.

As a business owner, you realize that there is a gap in your security policies. For example, you may have been impacted by a computer worm or virus, or worst, your place of business may have been broken into and vital information stolen. You have looked at various security tools and methodologies, and feel that a biometric system is best suited for your place of business. But how do you *really* know that a biometric system is best for you? Have you examined the benefits versus the risks of implementing a biometric system? More importantly, have you also examined the performance standards and metrics that measure the effectiveness of the various biometric technologies?

### *The Factors That Need To Be Taken Into Consideration*

First, before deciding upon which biometric system to implement at your place of business, it will be important to conduct an audit of your existing security infrastructure, and see how well it matches up against your current security policies (what exactly defines a “good security policy” will be the topic of a later article). If you, as the business owner are not sure how to conduct such an audit, it will probably be well worth the money to hire a security consulting firm to help you out.

As I have meetings with contacts and potential clients, the trend I keep hearing is that “Oh, yea, we do have a flaw in our security policies, we need to fix it!”. But when it comes time to actually spending the money needed to improve security, the reluctance then sets in. Keep in mind that conducting a security audit will cost some money, but would you rather spend the money now or wait until some security misfortune occurs which will then *really cost* you?

Second, the other reason for the importance of conducting a security audit is that it will give you the chance to know and understand your current business processes better. It is much easier to implement a biometric system in existence with other, current business processes, rather than implementing a system from ground up. As a result, your employees will be more accepting of a biometric system, which will make the training and learning curve a lot easier.

Third, after you have decided that you want to implement a biometric system, it is important that you get an understanding for the Rate of Return On Investment (ROI) you will be getting from it. In order to do this, you can first conduct a “Pilot Project”. For example, if your implementation calls for the deployment of five fingerprint scanners at five different access points at your place of business, first consider implementing only one fingerprint scanner at one primary access point, for a period of time (three months). By doing this, you can then quantify your ROI if you want to do a system wide implementation. Also, this will give you time to see how your employees will react to the use of a biometric system. You can always implement a system wide biometric deployment, but you run the risks of not knowing what your ROI will be, as well as your employee’s perception and acceptance of the new technology ahead of time.

Fourth, one of the cardinal rules in a good security policy is that never rely upon just one means of security as your only line of defense. You should have multiple layers of security. In biometric terms, this means having a “multi-modal” security system (a future article will specifically address the applications of “multi-modal” biometric security systems). Before you implement your biometric system, it is very important to examine to see how well you can implement it along side with your existing security systems (such as CCTV, card swipe, numeric keypad entry, etc.)

After you taken into account the above mentioned factors, you are probably asking yourself, as the owner of your business, what type of biometric system will work best for my place of business? This is a difficult question to answer, without having first conducted a security audit, and assessing your needs and budget. In general terms, biometric system applications fall into two areas for businesses: (1) Physical Access Entry Security; and (2) Computer and Network Security (this is also known as “Single-Single On Solutions”, in that your fingerprint becomes your password-this eliminates the need to remember multiple passwords-this will be the focal point of a future article) This article focuses upon physical access entry security. In these types of applications, hand geometry recognition technology and fingerprint recognition technology are deemed to be among the best. These two technologies also work together well in a “multi-modal” scenario. The hand geometry scanner can be used at the primary access entry points in your business, and the fingerprint reader can be used to provide for a second level of security for the more sensitive places within your business.

Biometric systems, like all other technologies, have performance standards or metrics which you must evaluate first before implementing them at your place of business.

### *Biometric Performance Standards and Metrics*

These performance standards, or metrics, are widely used by the biometric industry in order to gauge the effectiveness of the various biometric technologies. These standards are not particular to any specific biometric technology, they apply to all of the technologies. The standards are as follows:

- The False Acceptance Rate;
- The False Rejection Rate;
- The Equal Error Rate;
- The Failure To Enroll Rate;
- The Ability To Verify Rate

At the present time, there is no central, governing body which monitors and regulates the performance standards that are given out to the public by the various biometric vendors. As a result, there is controversy within the biometric industry over the performance standards claims by vendors of their products. For example, vendors can tend to overstate the results of these performance standards, without much questioning from the public. Although biometric vendors do use “real subjects” in evaluating their products, the test environment does not reflect real world usage and simulations. However, there has been a move to monitor these performance standards, with the creation of the International Biometric Industry Association and the BioAPI Consortium.

What are the implications of this to you, as the business owner? First, before you purchase and implement a biometric system, you must look beyond the performance standard numbers set forth by the vendor. Try and look up previous customers who have purchased and are currently using the system you want to implement. This can be done by asking for client testimonials. Also, as stated previously, implement a pilot project first to see if the biometric system you want to purchase will really be the best suited for your place of business. Second, these performance standards should not be used individually in order to gauge the effectiveness of the biometric system you are purchasing. Rather, you need to look at a combination of them in order to get a true picture of the security threshold you plan to implement or enhance at your place of business.

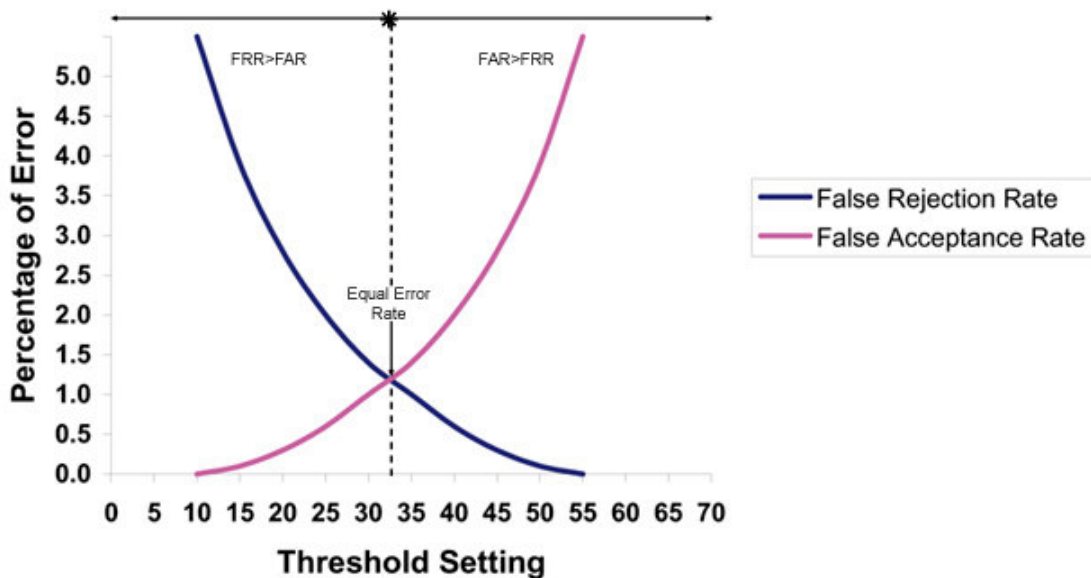
We will now explore in more detail each of these biometric performance standards:

The **False Acceptance Rate** is also referred to as FAR, or Type II Errors. This performance standard reflects the probability that the biometric system will falsely recognize an impostor as a regular employee of your business, and grant them access to entry.

The **False Rejection Rate** is also referred to as FRR, or Type I Errors. This performance standard describes the probability of a legitimate employee of your business being denied access to entry by the biometric system.

The **Equal Error Rate** reflects the probability of the FAR and the FRR being the same, or equal. The Equal Error Rate is also known as the “Crossover Rate”. This can be a misleading performance standard, and there are very few business applications which

require the FAR and FRR to be equal. The graph below depicts where the ERR is located at.



As you can see from the above graph, you have a wide range in which to establish a relevant security threshold for your place of business. The threshold you set is determined by what your security needs are, and how much of a compromise you, the business owner, are willing to accept. For example, if you do not want the biometric system to allow any imposters, you would establish a threshold setting of 10, but this would allow for a higher probability of legitimate employees of being denied access. However, if you absolutely do not want legitimate employees from being denied entry, you would set the threshold value at 55, but then this would allow for a higher probability of imposters to enter your place of business. Thus, there is a tradeoff which you must accept.

The **Failure To Enroll Rate** also referred to as FTE, describes the probability that a person simply cannot enroll into a biometric system. The likely cause of a Failure To Enroll Rate is that the person just does not have enough unique features for the biometric system to capture. For example, an employee of your business may not be able to enroll them self into your biometric system because they just do not have enough unique fingerprint or hand geometry data for the system to capture. Although the FTE is usually a small percentage, it is important to have a manual back up system in case you have any employees that simply cannot enroll into the biometric system.

The **Ability To Verify Rate** is also known as the ATV. This performance standard demonstrates the probability of the overall percentage of users that can be verified by a biometric system. For example, the total percentage of employees at your business that be successfully authenticated by the biometric system in order to gain access to entry. The ATV can also be thought of as the combination of the FTE and the FRR. Mathematically, this can be represented as:

$$ATV = [(1-FTE) * (1-FRR)]$$

It is important to maintain a high ATV, and as a result, this performance standard is more important than the FTE.

*Other Biometric System Considerations*

Apart from the biometric standards and metrics reviewed, there are other aspects which you need to take into consideration before implementation of your biometric system.

First, you need to be concerned with the enrollment and verification times of the biometric technology you are planning to purchase. In broad terms, enrollment can be defined as the process of registering your employees into the biometric system, and verification can be defined as the biometric system actually confirming the identity of your employee, and granting them access to entry. For a more detailed review about these two biometric processes, please see the article “An Introduction to Biometric Technology”

([www.htgadvanceystems.com/Advance/articles/Biometrics\\_Introduction.pdf](http://www.htgadvanceystems.com/Advance/articles/Biometrics_Introduction.pdf)).

You want to acquire a biometric system which will result in very rapid verification times. Otherwise, you could potentially have employees that will be waiting in line to be verified, which could then cause them to have disdain for the system. The enrollment process usually takes longer than the verification process, because your employees will have to enroll a few times, in order to insure enough unique features from their biometric is captured by the system.

The following matrix displays the enrollment and verification times of some leading products.

<i>Product</i>	<i>Enrollment Time</i>	<i>Verification Time</i>
HandKey II (Hand Geometry Scanner, Manufactured by Recognition Systems, Inc.	N/A	<1 Second
Fingerscan V20 (Fingerprint Scanner, manufactured by Identix, Inc.	<5 Seconds	<1 Second
FingerKey DX (Fingerprint Scanner, manufactured by Recognition Systems, Inc.)	N/A	<2 Seconds
Indoor Morpho Access Biometric Terminal (Fingerprint Scanner,	N/A	<1 Second

Manufactured by SAGEM MORPHO, Inc.		
V-STATION (Fingerprint Scanner, Manufactured by Bioscrypt)	<5 Seconds	<1 Second

NOTE: The above products are used primarily for physical access entry applications

Another aspect you need to take into consideration is if your biometric system will operate in either a standalone or networked mode. For example, suppose you have purchased and installed four fingerprint scanners at four different access entry points at your place of business. In a stand alone mode, the fingerprint devices will act like their own computer-each device will conduct its own enrollment and verification transactions, as well have its own database for storage of the biometric data. In a networked environment, all of the fingerprint scanners will be connected to a central server, where the enrollment and verification transactions will take place, as well as storage of the biometric data.

In a stand alone mode, enrollment and verification will usually happen very quickly. But in a networked environment, enrollment and verification will be much slower, because transmission of data over the network will increase the transaction times. This will be a focal point in the article which will review “multi-modal” biometric security systems.

Finally, as the business owner, you need to choose a biometric system which is least susceptible to privacy rights issues. This could very well be an issue with your employees as the biometric system is implemented. For physical access entry applications, with respect to small and medium sized businesses, hand geometry scanners and fingerprint scanners will probably be suitable enough. Also, these two biometric technologies are the least prone to privacy rights issues, as they have been around the longest. However, if you are planning to implement a higher scale biometric system such as facial scanning or iris scanning, the privacy rights issues will be much greater among your employees.

In summary, we have looked at some of the factors you need to take into consideration before you implement a biometric system at your place of business. Our next article will look at the role a biometric system can play in enhancing the Information Technology and Network Security at your business.