Biometrics is a Win Win for both the Customer and the Security Integrator

Biometric technologies increase security, reduce risk and make us safer because knowing "who" matters if you are really serious about safety and security.

The use of biometric technologies is the most effective, secure and private means of identification available today. Biometrics identifies or verifies the identity of an individual based on physiological or behavioral characteristics. Examples include products that recognize faces, hands, fingers, signatures, irises, voices, fingerprints and dermis.

Commonly thought to be new technology, biometrics was used as early as 30,000 years ago, when authors of paintings on cave walls left their signature handprints to identify themselves. In 1891, Juan Vucetich started a collection of the fingerprints of criminals in Argentina, considered to be the earliest cataloging of fingerprints. The difference today is that technology is available that can collect data, such as the fingerprint patterns of live individuals, quickly convert the data into arithmetic codes and match in real time against a database record of authorized persons.

The common thread from 30,000 years ago to today is that it matters who I am. In both personal relations and business it matters who I am, both to myself and to the people with whom I have relationships with or conduct business with. With today's large and growing population, our relationships and transactions are no longer limited to the people in our village as in ancient times. According to our Census Bureau, the world population today is more than 7 billion with the US population in excess of 315 million. Our economy is global. And as terrific as our brain is, we cannot always remember names and faces. And, so it is that we apply our technology to this important question: who am I dealing with? How do I keep my personal information secure, so that only I can access it?

Biometric technology steps up to the task. Technology can quickly determine a person's identify by matching data from a live person, i.e. fingerprints, against a database of fingerprints, because fingerprints can be quickly converted into mathematical codes to become unique and secure identifiers. Determining what constitutes human identity is evolving and becoming more nuanced than our understanding even 5 years ago. And, at the same time, the stakes are becoming higher and higher, be it for law enforcement, counter-terrorism, defense, homeland security, healthcare, finance, e-commerce, the neighborhood school or the company on the corner.

Some of the unique qualities of biometrics to consider:

1. It's focused on the "who" – the individual – not the credential.
2. It's easy to use, simple to understand.
3. It's inclusive and egalitarian.
4. It improves security, lowers risks, and is more convenient.
5. It's a contemporary solution for a complex and rapidly changing digital world.

6. PIN numbers, passwords are ultimately obsolete.
7. Key cards can be quickly and easily cloned with inexpensive devices anyone can buy.
8. The job of the "who" is to make sure unauthorized persons are not granted access, services or use of assets.
9. Your face or fingerprint is your credential.

Is there a better alternative than biometrics?

All biometrics are not created equal: What are the elements that determine the robustness of a particular biometric product or technology? A quick review of the performance metrics:

- False acceptance rate or false match rate (FAR): This term measures the percent of invalid inputs or tries which are incorrectly accepted as correct.
- Threshold value: This setting determines the accuracy of the match.
- False rejection rate (FRR): The probability that the system failed to match a correct try to a matching template in the database.
- Equal error rate (EER): the rate at which both accept and reject errors are equal. In general, the device with the lowest EER is most accurate.
- Failure to enroll rate 9FTE): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs, example slight fingerprints.
- Failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- Speed of recognition: Speed is determined by the algorithm of the technology. The search methodic for the template record is key for speed, i.e. is the first record in the database a match or is it the last record in the database which of course takes longer.
- Minutiae Point Analysis: The most simple fingerprint comparison method and typically is combined with a second identifier such as a PIN or card.
- Pattern Recognition: Currently, the most robust recognition technology utilizing modern algorithms for fingerprints and faces and it stores a larger template than the minutiae point analysis' template.
- Eigenvectors and mapping: These are two major technologies first used for face recognition, either alone or in combinations. Mapping measures the distances between points on the human face and has two really weak features: (1) recognition distance in front of the camera is the same as the enrollment distance was and (2) daily changes in ambient light prevented recognition. Eigenvectors based face recognition technology is more robust with natural scaling which means that the camera can recognize the face as soon as the camera can see the facial features. However, the normal daily changes in ambient light was problematic. Currently, varying versions of these technologies are in use.

The current news in biometrics today is to report that the products work as advertised. In earlier days, security systems integrators often found that the biometric products despite their promises just didn't do the job they were advertised to do. Understandably, integrators concerned about their livelihood and reputation were reluctant to adopt biometric products for their customers. Many comments in this article will be related to access control, a common and popular security application with critical credential weaknesses that biometrics have alleviated, but biometrics is applicable to all kind of applications where the "who" matters.

Common characteristics of current biometric products:

- Operate on the network
- Template management
- Recognition on the unit
- Operates as long as power is available
- Operate as a single product
- Operate as a complete system with all functions
- Retrofit of existing third party systems
- Attach to third party systems
- No cards or PINs are required.
- Products accommodate thousands of fingerprints and facial images without cards or PINs

Types of current products available to installing security systems integrators and the benefits and efficiencies the end-user customers can enjoy. Currently, fingerprint technology is the most popular with facial recognition growing. Facial recognition is recommended for locations where fingerprints would not be practical because employees have dirty hands, carry things or the location itself is very clean such as clean rooms or surgical suites.

Access Control: The principal function of any biometric product is to verify the identity of an individual, the "who" because it matters. Access control in addition requires that the unit unlock a door, grant or deny access based on time restrictions and monitory door alarms. Products are available (1) that protect a single critical access point; (2) are a full state-of-the art systems; (3) that can be integrated into conventional access control systems; or (4) that can be added to the current conventional access control system.

Time and Attendance: Most biometric time and attendance systems utilize fingerprints or faces as identifiers. The typical time and attendance system collects the work time and summarizes it according to the customer's parameters so that the time can be exported to the payroll service to prepare the pay checks. Customers that utilize biometric time clocks find that it saves significant money by eliminating time card fraud such as buddy punching and lost or stolen cards or forgotten passwords. Reducing overpayments for time of as little as ten minutes a day where

there is 100 employees can easily save as much as $150,000 each year and time of the administrator.

Muster Systems: Muster systems are recommended for crisis control such as locations with hazardous materials or dangerous processes. During an evacuation or accident, the muster system provides management and first responders with a real time list of missing persons. This information allows management and the rescuers to deploy their resources where they are needed and provides management information when making announcements or talking with the press.

Visitor Management: Visitor management works much like access control in that positive identification is required of the visitor and an electronic record is made of when, where and who the visitor is. This process greatly reduces record keeping and recording time of end-users.

Other common applications: Cabinet control, turnstile control, gate control and dock control: Positive identification of the operator is required before the person can open, operate the equipment, etc.

Successful applications: Ultimately the key to using biometric products successfully is to select the product that is appropriate for the application, for example fingerprint recognition would not typically be recommended for clean room access control.

Why Use Multimodal Biometric system: Multimodal biometric systems evolved in the business world due to a variety of reasons. (1) Because integrators and customers were uneasy about trusting a single biometric, manufacturers added a second identifier such as a PIN or card reader to increase the accuracy and reliability of the biometric products. (2) A second reason was that the identification technology be it fingerprints, faces, etc. was prone to false acceptance of invalid inputs/tries when only a small census of persons were enrolled and another identifier was added to prevent the false acceptance.

The authentication model, the key card reader, most often installed by security system integrators today was invented in the 1960s and is outdated and vulnerable and violates the promise of trust that the customers have bestowed on the integrators. The key card access control products so popular with integrators cannot provide the "who" with an acceptable degree of certainty. Furthermore, the cards, credentials, are easily lost, stolen and shared and now can be easily cloned with an inexpensive device that can be purchased for less than $20.00. The inherent ability of a card system to provide a true ID or identification of an authorized person is failure of the first degree.

Biometric products offer new revenue opportunities for system integrators and dealers.

There are biometric systems available to meet the needs of almost any commercial access control project and meet it economically. And integrators already know how to install the biometric

products if they have installed access control and card readers. Biometric devices offer practical solutions to reliably meet your clienteles' security needs. Common applications are:

- Upgrading the access control systems of their current customers.
- Suggesting biometric products to their customers that need a more secure solution.
- Installing time and attendance that will save your end-user just because of the accuracies and efficiencies of collecting work time as well as eliminate buddy punching.
- Install biometric muster systems to make the workplace safer and provide management with a real time missing person report should an event occur.

Biometric products provide an opportunity for the security systems integrator to provide their customers with products that actually can prevent unauthorized access via stolen or cloned card or PINs. Reduced costs for the routine replacement of cards and keys add up when the overall administrative costs of a key or card system are considered. And, because biometric products require minimal operator assistance, end-users can save money by assigning customer service personnel to other activities.

And, where are the best market niches for biometrics: Biometrics is needed in the same markets currently using access control. Today systems are available for a variety of tasks: access control, time and attendance and muster systems, visitor identification and OEM applications for cabinet controls or switches.

Challenges for security systems integrators selling biometric products: The role of the traditional integrator is changing as the market transitions to IP-based technology. This transition is attracting IT integrators with their lower equipment costs and higher service costs. This transition has required the installers to broaden their skillsets and to be more professional in project management. IMS Research predicts that physical security equipment sold through integrators and installers will reach more than $38 billion in 2016. And, the security integrators can expect IT providers to continue to move into this industry as they assist their customers with the purchase of security equipment.

Some customers will have privacy concerns. In some cases the employees of end-users will be concerned that their personal information or fingerprints or facial images will be available either to the employer or an outsider such as law enforcement. Employees need to be reassured that images of fingerprints and faces are not saved. The image is converted to a mathematical code for storage and even if the system is hacked, the code will be meaningless.

A serious liability problem awaits security systems integrators that continue to install card based systems now that it is common knowledge that the cards can easily and quickly be cloned which essentially renders the system useless and invalid. And, why would an integrator risk the safety and security of their customer by installing a system they know for a fact is easy to defeat with a cloned card.

The objective of an access control system is to manage where authorized people are granted access. Using your typical access control card access system, entry is granted if the card or credential as presented has the right number. Any person can be holding the card as the system does not care.

Card manufacturers' solution to this issue of inability to authenticate the identity of the user has been to produce new cards with more options that are more expensive but do not and cannot authenticate the identity of the holder of the card. Management is still dependent upon the honesty and integrity of the person that holds the card. More bells and whistles for this credential are not a cure.

The future for security is biometrics – THE ULTIMATE CREDENTIAL. Customers are increasingly aware that their card systems do not and cannot authenticate the identity of the user. Is the future of the security systems integrator going to be as a vendor that sells and installs sub quality systems, i.e. card reader systems, that will not and cannot authenticate the "who" of the card holder. Embrace biometric technologies and save customers money, increase security, reduce risk and make us safer because knowing "who" matters if you are really serious about safety and security.