The Perception of Biometrics in the United States

A White Paper
written by Ravi Das

BiometricNews.net

And

M2SYS™
ACCELERATED BIOMETRICS

Table of Contents

A Definition of Biometrics

We all have unique physiological and behavioral characteristics that distinguish us from other people. Biometrics uses these unique characteristics (or identifiers) to ascertain and verify people's identity. Unique identifiers include distinct features such as fingerprints, various iris patterns, blood vessel patterns in the retina, voice inflections in speech, and hand shape/geometry. It also includes the way we sign our name or use a computer keyboard.

Brief Review of the Major Biometric Technologies

There are a total of seven major biometric technologies available today. They are:

- Fingerprint recognition
- Hand geometry recognition
- Facial recognition
- Iris and retina recognition
- Voice recognition
- Keystroke recognition
- Signature recognition
- Vascular recognition

Of these technologies, fingerprint recognition, hand geometry recognition and now vascular recognition are the most prevalent. Having said that, considerable time and effort is being invested in biometric technologies of the future, which include gait recognition (the way and manner in which somebody walks), earlobe recognition (examining the geometry of the earlobe) and DNA recognition (examining the unique strands found in DNA samples). A brief description of each biometric technology is provided below.

Fingerprint Recognition

Fingerprint recognition involves the location and determination of the unique characteristics of the fingerprint. The fingerprint is composed of various 'ridges' and 'valleys', which form the basis for the loops, arches and swirls on your fingertip. The ridges and valleys contain different kinds of breaks and discontinuities. These are known as 'minutiae'. It is from these minutiae that the unique features are located and determined. There are two types of minutiae: ridge endings (the location where the ridge actually ends) and bifurcations (the location where a single ridge splits into two ridges).

Hand Geometry Recognition

Hand geometry recognition involves looking for unique features in the structure of the hand. These features include the thickness, length and width of the finger, the distances between finger joints, and the hand's overall bone structure. A 3-dimensional image is taken of these unique characteristics. It should be noted that the hand does not contain as many unique characteristics as other identifiers.

Facial Recognition

Facial recognition involves taking many images (or pictures) of the face, and extracting the unique facial features and distances from -or between -the ears, nose, eyes, mouth and cheeks.

Iris and Retinal Recognition

Iris recognition entails examining the unique features of the iris. The iris is the colored section between the pupil and the white region of the eye (also known as the sclera). Its primary purpose is to control the size of the pupil (the part of the eye that allows light to pass through). The unique features of the iris include the trabecular meshwork (the tissue that gives the iris its 'radial' impression) as well as other physiological properties such as freckles, furrows, rings, and the corona. Retinal recognition involves examining the pattern of blood vessels in the retina, which is located at the back of the eye. The examination focuses on the juncture of the optic nerve (the area where the nerve leaves the brain and enters the eye).

Voice Recognition

With voice recognition, it is the unique patterns of an individual's voice as produced by the vocal tract which is examined. In order to capture the voice inflections, a text phrase is usually recited. The vocal tract consists of the laryngeal pharynx, oral pharynx, oral cavity, nasal pharynx and the nasal cavity.

Keystroke Recognition

Keystroke recognition works by examining the unique way in which an individual types on a computer keyboard. Variables include typing speed, the length of time that keys are held down, and the time taken between consecutive keystrokes.

Signature Recognition

Signature recognition examines the way and manner in which we sign our name. Unique characteristics include changes in timing, pressure and speed during the signing process. It is important to note that it is not the signature itself that is examined.

Vascular Recognition

Vascular Recognition is probably at the present time, the most recent of the Biometric Technologies available today. This technology is often referred to as Vein Pattern Recognition. In a manner similar to Retinal Recognition, it is the unique pattern of blood vessels which is examined. But in this instance, it is the blood vessel structure of the finger, the hand, and even the palm which is captured. What makes Vascular Recognition different from the other Biometric Technologies is that it requires no contact by the end user. Infrared light is used to transmit back (or reflect) the blood vessel pattern, and from there, the unique features are extracted.

The Differences Between Behavioral and Physical Biometrics

The above biometric technologies fall in two categories: behavioral biometrics and physical biometrics. In general, behavioral biometrics can be defined as the non-biological or non- physiological features (or unique identifiers) as captured by a biometric system. As behavioral biometrics also covers any mannerisms or behavior displayed by an individual, this category includes signature as well as keystroke recognition. Physical biometrics may be defined as the biological and physiological features (or unique identifiers) as captured by a biometric system. This category includes fingerprint recognition, hand geometry recognition, facial recognition, iris and retinal recognition, and voice recognition.

Review of the Major Biometric Concepts

When examining the various biometric technologies and systems, it is important that one has a basic understanding of the key concepts that are associated with biometrics. Each of these concepts is explained below:

- Verification and identification
- Biometric templates
- The processes of enrolment, verification and authorization
- Biometric performance standards

Verification and Identification

The verification process aims to confirm or validate someone's claimed identity. When you first enroll into a biometric system, it assigns you an identifier, which is linked to your biometric template. The database containing your template is then searched on the basis of this identifier. If a positive match is established, you will be extended a given service or privilege.

Verification: Also referred to as a 1:1 relationship, this biometric identification process answers the question, "Are you who you say you are?" It substantiates an individual's identity by comparing a submitted biometric template against the biometric reference template of a single enrollee.

Identification: Also referred to as a 1:N relationship, this biometric identification process answers the question, "Who are you?" It substantiates an individual's identity by comparing a submitted biometric template sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. A biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity.

Biometric Templates

When you first enroll in a biometric system, it takes numerous images/recordings of your biological or non-biological data (including, for example, a voice recording or keystroke pattern). These raw images and recordings are subsequently consolidated into one main image, known as the 'biometric sample'. It is from this sample that the unique features (discussed above) are captured and extracted.

Next, they are converted to a 'biometric template', which, in turn, is used for the purposes of verification and identification. It should be noted that the biometric system does not contain actual images of the biological or non-biological data, they are a mathematical representation of the data points that a biometric algorithm extracts from the scanned biometric identifier. The identity template is simply a binary data file, a series of zeros and ones. The algorithm then uses the template to positively identify an individual during subsequent scans. No image is ever stored or transmitted across a network. In addition, the algorithm is "one way" which means that the template that is extracted is nearly impossible to be used to recreate the original biometric image. In other words, it is nearly impossible to reverse engineer the data that is sent to positively identify an individual and successfully “steal” their biometric identity. The type of mathematical file that is created depends on the biometric system in use. Whereas fingerprint recognition and hand geometry recognition systems create binary mathematical files, iris recognition systems generate hexadecimal files. In other words, the image of your fingerprint or hand becomes a series of 0s and 1s (e.g. - 00010101000011111111).

The Processes of Enrollment, Verification and Authorization

Imagine trying to enter a high-security area. To do so, your template must be included in a database, alongside those of other authorized individuals. In turn, this requires you to register your fingerprint. This process is known as enrolment. Several fingerprint images are taken, which are combined in a single biometric sample. Next, a mathematical formula or extraction algorithm is used to extracts the unique features from the biometric sample. These features are subsequently stored in a mathematical file known as an enrolment template, which is used for the purposes of verification.

The next step involves verification. In order to enter a high-security area, you are required to identify yourself by placing your finger on a fingerprint scanner. The scanner’s sensor will capture ‘an image’ of your print. The extraction algorithm subsequently extracts the unique features from the image, and stores these in a file known as the verification template.

The next stage involves comparing the verification template to the enrolment template in order to determine the extent to which they match. This is achieved with the assistance of a matching algorithm. The latter assigns a score, based on the amount of overlap between both templates. If this score is higher than an agreed value (or threshold) you are authorized to enter the area. If the score is lower than the threshold value, you are denied access (and the verification process may be repeated).

Although much happens during the enrolment, verification and authorization processes, they only take a few seconds to complete. At this point, it is important to remember that an enrolment template is never completely (100%) the same as a verification template.

Biometric Performance Standards

Biometric systems are rated on the basis of several performance standards. The most important are the False Rejection Rate (FRR), the False Acceptance Rate (FAR) and the Equal Error Rate (EER) (figure 1).

The FRR (also known as type 1 errors) can be defined as the probability of a registered user being wrongly rejected by the biometric system. In case of the above example: what is the likelihood of a legitimate, registered user being denied access to the high-security area on the basis of a fingerprint scan?

The FAR (also known as type 2 errors) can be defined as the probability of an impostor being wrongly authorized by the biometric system. In case of the above example: what is the likelihood of a legitimate, registered user (this could also be a non-registered user) being wrongly authorized to access to the high-security area on the basis of a fingerprint scan?)

The EER (or crossover rate) reflects the probability of the FAR and the FRR being (nearly) the same. There are also other biometric standards. For example, the Failure To Enroll rate (FTE), which defines the statistical probability that a person is simply unable to enroll in a biometric system. This may be attributable to the fact that the person in question does not have enough unique features for the system to capture.

The Ability To Verify rate (ATV) indicates the overall percentage of users that can be verified by a biometric system. The ATV can also be thought of as the combination of the FTE and the FRR. Mathematically, this relationship can be represented as follows:

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

The Perception of Biometrics in the U.S.

Biometrics is a technology which has been around for quite a long time. In fact, the first commercial uses can be seen in the 1970's with the hand geometry scanner which is still considered to be the oldest Biometric Technology in the world thus far. Since then, Biometrics has seen a lot of technological advancements with great and rapid progress being made in Research and Development. There are some very interesting Biometric Technologies which are being planned for the future, such as DNA Recognition, Gait Recognition (examining the unique features in the way we walk), and even Earlobe and Nose Recognition. Despite all of this, and the obvious benefits Biometrics brings to the security table, it still has not reached a very high level of acceptance here in the United States. Although we cannot speak for every country in the world, in comparison the perception of Biometrics is very low here in the United States.

There are a number of reasons for this, and they all will be discussed and reviewed separately.

Specifically, they are as follows:

1) The issues surrounding Privacy Rights
2) Our society is very reactive and lackadaisical about Security
3) The fear of the misuse of Biometric Information and Data
4) The lack of Standards for Biometrics
5) The fear of the National ID Card
6) The lack of training and support for Biometrics
7) The perceived costs and expenses associated with Biometrics

The Issues Surrounding Privacy Rights

This country was founded primarily upon the creation and enforcement of civil liberties, especially protecting our own rights as citizens. We live in the freest country in the world, and we can do pretty much whatever we please as long as it is in the bounds of the law and does not intrude upon the Civil Rights of others whom live in our society. As a result, we truly cherish the rights to our own privacy.

Biometrics is a security tool which examines and extracts the unique features of our physiological and biological being in order to identify who we are. In fact, no other security tool does this. So in a way, Biometrics can be considered an intrusive tool, it is invading our own body due to the physical process of capturing data with the perception that we have no control over the information and data which is being collected and analyzed.

Privacy concerns have a lot of other specific sub issues surrounding it, but the invasion of our own physiological structure and being, as well as the total loss of control of not knowing where the information and data is being stored is at the heart of the issue.

Our Society is Very Reactive and Lackadaisical about Security

We all remember the horrible day of September 11, 2001. As we gathered intelligence and information surrounding details and backgrounds of the terrorists involved, we learned the horrifying facts of the truth that in reality this tragedy could have conceivably been avoided.

For example, we learned of erratic behaviors the terrorists exhibited at schools from which they took flying lessons to the very poor security at the airports which could have caught them. It was only after these tragic events that we came together to become much more proactive about security, and utilized the various technologies which were available at the time to help fortify it.

The same can be said about biometrics. Here in the United States, we have not been proactive in learning about security tools available to protect us. If we were more security proactive as a society, we would be much more informed about biometrics, thus increasing our levels of acceptance of it like other security technologies. Immediately after September 11th, 2001, biometric identification soared in popularity then after awhile it died out. Since then the level of the interest and awareness about biometrics has never sustained captive interest with the public.

The Fear of Biometric Information and Data Misuse

Whenever we disclose personal information, such as our phone number, e-mail address or even our regular postal address, we are struck with the fear: Will this private information be acquired by a third party and misused in any way?

Fortunately various protective mechanisms have been put in place such as the No Call List, e-mail spam filters and even the credit card agencies are taking a much more proactive stance in protecting their respective cardholders. However, our biggest fear with the misuse of our personal information by third parties is the thought of identity theft, especially when we have to submit our Social Security number or other types of financial data, such as our Credit Card number and its associated three digit security code.

It is this very fear of identity theft which has caused the acceptance and perception of biometrics to be At low levels here in the United States. This fear resides in the fact that if a biometric device were to be hacked into and our biometric template was stolen, our identity would also be stolen forever .

The underlying cause for this fear is that biometric data are permanent physiological structures and cannot be changed unlike our credit card or Social Security number.

Compounded with this fear is the fact that biometrics also has a “Black Box” characterization associated with it which means when we present identification to a biometric device, there are a lot of processes which take place and data/information storage which we do not know about. Therefore we assume that all of this happens in a so called “vacuum,” and thus anyone with criminal intent can access and steal our biometric template.

However, a lot of these fears are just myths when examined from a technical standpoint and can be cleared up by opening a line of communication from the biometrics vendor to their customer. For example, suppose somebody does steal your fingerprint from a biometric device, as it turns out there is not a lot that they can do with it.

The Lack of Standards for Biometrics

As technology is introduced and matures throughout its product lifecycle, over the course of time it “grows” so that it meshes well with other technologies and related platforms and applications. For example, as a new software product is introduced into the marketplace, it is tested so it can work well with the other operating systems, such as Windows and/or Linux. However, in order for the software to mesh well with the other technologies, it is crucial that a set of Best Practices and Interoperability Standards be created so that the differing technologies can all work together upon a common platform.

A prime example of this are the various types of networking devices (such as routers and firewalls) working together on a common Internet Protocol, such as TCP/IP. A list of Interoperability Standards has to be created in order these networking devices to work in unison. As the biometrics market continues to mature, there are many types of modalities being released. For example, just this year alone, there have been a lot of technological advances made in iris recognition.

However, as these new biometric products and solutions are coming out, there is no established list of common Interoperability Standards. It is not that biometrics is a new technology, but rather, nobody had the initiative to come out with a list of Interoperability Standards. As a result, biometric vendors all over the world are making claims about their products and solutions with no solid baseline to be compared against. This causes confusion for the end user which basically diminishes the level of trust with biometric vendors, ultimately leading to low perception of biometrics here in the United States.

However, this low perception is not just with the end user or average consumer. Even more technical people (such as software developers) also have a rather low perception of biometrics from a development standpoint. This is due to the lack of Interoperability Standards between Biometric Vendors. Very often, software developers have a hard time developing applications which can interface with other technologies that are available.

Even on a more macro level, applications which require the use of biometrics in some type of fashion are also having a hard time getting off of the ground, exemplified by the National ID Card and the e-Passport. Governments around the world (including the United States) are trying to implement a National ID Card with biometric identification implemented into it. However, due to the absence of Interoperability Standards, it has been difficult for governments to get these new types of security documents off the ground.

For example, the National ID Card and the e-Passport have to work with legacy Information Technology systems worldwide in which they can be processed and accepted at points of entry and exit. This is especially true for the e-Passport because travelers will be using this security document all over the world making the need for Interoperability Standards even more paramount.

It's important to put a disclaimer here: With regards to the implementation of the National ID Card, and the e-Passport, there are many other logistical and operational reasons why they have been difficult to put into place—biometrics has been only part of these difficulties.

The Fear of the National ID Card

The last section mentioned the National ID Card and the e-Passport. Currently, here in the United States there is no common Security document across all fifty states which can identify an individual. Instead, each state has their own driver's license or state ID card and there is no uniformity among these cards. Plus, they can also be easily replicated. About the closest thing U.S. citizens have for a common document is the traditional Passport. But not all U.S. citizens have this type of Passport, only those whom travel abroad tend to go through the steps to obtain it.

After the events on September 11th, 2001, the movement for a National ID Card proliferated-so that there would be one standard in which to verify and/or identify people. The idea is that there would be an all inclusive security document, complete with a picture, fingerprint, and various types of other biometric templates, such as a facial scan or an iris scan. However the National ID Card has received, at best, an extremely lukewarm reception here in the United States. This is primarily because the public at large is afraid that the federal government will have control over our most private information which is contained in the National ID Card and in particular, our biometric templates.

As a result, this has led to an outcry of civil liberties violations, especially our privacy rights being compromised. Consequently, this has also led to suspicions of biometrics here in the United States and a general distrust of the government's intention to gather this type of information. It is important to note that other countries around the world have been successful or have been trying to implement some sort of a National ID Card infrastructure. Citizens of these various countries have been much more receptive and open to the thought of a National ID Card largely because fear of privacy rights violations is not as prominent and there are not groups like the American Civil Liberties Union here in the United States that are specifically organized to protect individual rights.

A key reason could be is that people in these countries are much more informed about biometrics and as a result, they are more proactive about their security.

It could also be that governments in these countries are conveying a much clearer message about how biometrics will be used on their citizens -- a key, fundamental human factor about biometrics -- conveying how the information/data will be used and for what purposes.

The Lack of Training and Support for Biometrics

Whenever we are introduced to a new piece of technology, especially in the workplace, there is often a training, workshop or just tutorial to get you acquainted with the new software. You may not embrace the new technology you now have to work with, but with the proper training you are probably at least willing to accept it. Most technology vendors are aware of this and recognize the fact that training their end users is one of the most important ingredients for acceptance of their products.

Traditionally, biometric vendors were not effective with providing adequate tools and resources to end users on proper use and maintenance of biometric software systems and the accompanying hardware devices. However, as the industry has evolved, most vendors have rewritten training materials that are easier to understand and offered additional multimedia training resources to help ensure a smooth launch and ongoing use of the biometric system.

Unfortunately, due to the reputation that the industry developed as being subpar on training by early adopters of the technology, some end users have become frustrated and developed a defeatist attitude towards biometrics because of their poor training on how to use it right the first time.

This also contributes to the low perception of biometrics based simply on lack of understanding and training. To make matters worse, with most of the technology tools available on the Internet, an end user can look up information via a simple Google search. However, this is not even the case with biometric technology. There is even concern amongst the Federal Government of the lack of training, especially with the Department of Homeland Security.

There are also purported biometric consulting companies out there in the marketplace and the main line of their business is to provide consulting services to their clients whom are interested in implementing biometrics at their place of business or organization, and are in the decision making phase of what they will need and what to get. Very often, on the part of the Biometric Consulting Company, fancy buzzwords and techno jargon is used, but once again, there seems to be the fundamental lack of understanding here as well about the lack of educating the customer about biometrics. For instance, the customer not only needs to understand about what biometric device they will need to acquire, but they also need to understand and be educated about the perceived benefits and the perceived ease of use of the particular piece of biometric technology they are interested in.

Clearly understanding the benefits and user friendliness are important components in the overall reputation of biometrics. It sounds very easy to simply say that in order to help increase the acceptance of biometrics, all a biometric vendor has to do is to provide training to their end user after the sale. However, biometrics vendors also need to realize that training is just one component. The end user also to be educated and fully understand what specific type of Biometric System will work best for their needs. For example, consumers often can't recognize what type of hardware is best for their needs and may end up purchasing the wrong modality leading to frustration and an ultimate lack of confidence in biometrics.

The Perceived Costs And Expenses Associated With Biometrics

When one thinks about biometrics, the image of something surreal and James Bondish always gets conjured up. With these mental images come the perceptions and notions of fancy gizmos which are extremely expensive. As a result, because Biometrics is often associated with a "black box phenomenon", there is the view that it is only used by the biggest of the corporations, which instills the image that Biometrics is very expensive technology.

There is no doubt that Biometric technology can be expensive-but, one has to bear in mind that the more elaborate a setup is and the more sophisticated type of application it is being used for, the higher the cost, and expense. At one point in time, all biometric devices were very expensive, but just like computer hardware, the prices have reduced substantially. For example, today, simple biometric devices such as Single Sign On Solutions for your computer or network are reasonably affordable, costing anywhere between $100 - $200. You can even buy a rudimentary Biometric Device at your local office supply store (such as Office Max or Office Depot) for less than $50.

As we see the number of biometric vendors increasing across the market, the law of economics that an increase in supply leads to a decrease in price holds true. Furthermore, as there are continual technological breakthroughs in biometrics, the size of the hardware is also coming down. For example, very small fingerprint recognition sensors are being used on netbooks and even wireless devices to verify/confirm the identity of the person using it.

However, biometric vendors need to do a much better job at communicating their prices, especially to the end user. The Vendors tend to focus on the much more specialized markets rather than just the average consumer, or end user. In other words, Vendors need to educate consumers with more content driven collateral to stress affordability:

1. Case Studies
2. White Papers
3. Testimonials
4. Blog Posts

Conclusion

In conclusion, this has been a comprehensive White paper looking at Biometrics from a number of different perspectives. First, a formal definition was provided, as well as a review of the major Biometric Technologies which are available, both in terms of Physical Biometrics (including Fingerprint, Hand Geometry, Facial, Iris/Retina, Vascular, and Voice) and Behavioral Biometrics (including Keystroke and Recognition). Second, a review of the major concepts of Biometrics was explored (such as verification/identification; Biometric Templates; the processes of Enrollment; Verification and Authorization; and Biometric Performance Standards). Third, an examination of the perception of Biometrics in the United States was analyzed, and numerous reasons were provided as to why the United States has a lower adoption rate of Biometrics when compared to the rest of the world (which include Privacy Rights; a reactive attitude towards Security; misuse of Biometric Data; a lack of Standards; lack of training to the customer; and the perceived costs and expenses).

When one looks at a spectrum of the Security Technologies which are available today (for example, ranging from routers to network intrusion devices to CCTV Cameras), it is Biometrics which receives the most scrutinization, both from a positive and negative perspective. This is so because it is a piece of our own individuality which is being explored in order to confirm our identity. Biometrics has this perception of being a “black box” type of technology, meaning one can witness the input and the output, without having a clue as to how the internal processes work. But really, there is nothing magical as to how all this happens. The internal processes are just a series of high level mathematical algorithms at work. In the end, Biometrics is just another piece of Security Technology, which can be used to fortify our businesses or other critical assets, from a logical and physical standpoint. Really, there is nothing magical about Biometrics.

It is this basic understanding (or lack of) of what Biometrics is really about which influences the adoption rate of it in any geographic location. For example, throughout the entire world, we have seen a greater adoption rate of Biometrics primarily in the developing regions such as Africa and Asia, than the developed nations of Europe and the United States. Why is this so? It is because in these parts of the world, the populations have a strong desire to be counted as individuals and citizens in the eyes of their own governments. Because of the corruption which is faced by traditional methods, Biometrics provides irrefutable proof of who the citizens are, and the entitlements and the benefits they deserve. In these societies, survival day to day is the most common concern, not privacy rights or civil liberties.

But here in the United States, as well as in Europe, we are afforded, to a very large degree, of being recognized by our own governments, and receiving the benefits that are due upon us. This is something we take for granted on a daily basis. Therefore, we can be much more concerned about the fears of privacy being violated, or personal liberties being taken away by the use of Biometrics. Perhaps it is when our governments go deeper into debt and we no longer receive our benefits and entitlements, will we know what it means not to be recognized as individuals. Then, we will truly understand the need for Biometrics not just from a Security perspective, but from the social perspective as well.

Copyright and Profiles

Copyright

This White paper is our opinion of the perception of biometrics in the U.S.

About Ravi Das (BiometricNews.net)

Ravindra Das (aka "Ravi") is a technical writer for BiometricNews.net, and is also the Editor of the blog site "Biometrics Security News and Information" (biometricnews.typepad.com). He has held numerous positions in IT ranging from Software Configuration Management to Database Administration to CRM Software. He has been in the IT area for some 12 years now. A native of West Lafayette, Indiana, Ravi has a Master of Science degree in Agribusiness Economics (thesis in International Trade) from Southern Illinois University, Carbondale, and an MBA from Bowling Green State University, with a specialization in Management Information Systems (thesis in e-Commerce).

Apart from being a technical writer, Ravi is also active in other parts of life. He loves working out at the gym, and has a deep passion for the martial arts. In fact, just recently, he became a certified and licensed 1st Degree Black Belt in Taekwondo, by the World Taekwondo Federation in Seoul, South Korea. Ravi is also currently training for his 3rd Black Belt (2nd Degree). He is also training for his Blue Belt in Brazilian Ju Jitsu.

BiometricNews.net was founded as a technical writing business to provide education to the end user on Biometrics; to increase the public awareness and perception of Biometrics; and to be that constant line of communications and interactions between the technology and the end user.

About M2SYS Technology

M2SYS provides affordable multi-modal biometric solutions that enable our customers and partners to easily utilize or integrate the right form of biometric technology for their needs. Our core focus is identity management for enterprise software applications in workforce management and healthcare together with a biometric software development kit (SDK) that allows developers to instantly add biometric recognition to any software application. Our technology accelerates the adoption of biometric identification leading to a faster and more widespread delivery of its many benefits.

The hub of our biometric technology platform is the M2SYS **Hybrid Biometric Platform™**, a client/server multi-modal biometric software system that supports several types of **biometric devices**, including **fingerprint**, **finger vein**, **palm vein**, and **iris recognition**. Using M2SYS' patent-pending **Bio-Plugin™** middleware integration methodology, software developers can seamlessly integrate Hybrid Biometrics™ in a matter of hours and immediately have the ability to deploy the form of biometric technology that best neutralizes varying user, demographic, and environmental conditions. This flexibility produces near 100% read rates with a single integration into a single biometric software system and eliminates the risks that are associated with being locked in to one particular form of biometrics or a single biometric reader.