Multimodal biometric systems

How they can help to protect against physical and logical threats

by Ravi Das

Ever since the tragic events of 9/11, security has always been on the mind of both businesses and global leaders. At the time, the primary focus was on so-called physical access entry security. However, as the decade went on, a new threat from a logical angle became evident: identity theft. The answer to the question of how to protect oneself from both these threats lies, according to Ravi Das, in multimodal biometric solutions, which can also be used in less threatening circumstances, such as monitoring the time and attendance of personnel.

Unimodal versus multimodal biometric solutions

When one thinks of a security system, very often the image of a security guard standing by the turnstile, or some sort of ID badge recognition springs to mind. This type of scheme relies upon only one means of security, or just one layer of it, often referred to as a unimodal security solution. Using only one means of security is a clear violation of a strong policy. Under this scenario, only one question is answered: "What do you know?". A multimodal security solution, however, consists of several security solutions, and answers in addition to the former question also "What do you have?", and "What are you?". This concept of a multimodal security solution can be extended into biometrics with this formal definition: "... a biometric system that uses multiple biometric characteristics".[1] In this regard, there are two different types of biometric multimodal systems:

- synchronous systems;
- asynchronous systems.

'Synchronous' means that there are two or possibly more biometric systems being used at the same time, for the same authorisation process of the subject in question. In this scenario, imagine a fingerprint scanner and an iris scanner being used simultaneously.

'Asynchronous' means that there are two (again possibly even more) biometric systems that are being used, but the key difference here is that they are used in tandem with each other, or in a sequential fashion. Again imagine the fingerprint scanner and the iris scanner. The fingerprint scanner would be used first and immediately after, the iris would be scanned to confirm the identity of the subject in question.

There are two key points to remember, when using biometric multimodal systems:

- Using multiple systems increases the accuracy, although it does not increase the speed of the authorisation process.
- If one device does not work, the other systems will come into play as a fail safe, thus still assuring a strong level of security.

Applications of multimodal biometric solutions

Ever since 9/11, security has always been on the mind of businesses. At the time, the primary focus was on the so-called physical access entry security: protecting the actual physical assets of an organisation, such as buildings and confidential files.

Physical access entry application

With regards to physical access entry, it is typically businesses and organisations that use multimodal biometric solutions. Very often, there will be a strong presence of security at the main points of access and entry of a building, and within the office infrastructure itself other rooms and private areas will be protected also (see figure 1). At the main points of entry, a hand geometry scanner is used to verify and confirm the identity of individuals.

Along with this scanner, there could be other levels of security used in conjunction, such as a swipe card or smart card system. When the individual gains entry through the main point of access, the internal parts of the office remain protected, such as the client file room and the server room. Very often, in this extra layer of security, fingerprint recognition is used. This then formulates the multimodal biometric solution in this example, and as you can see, it is an asynchronous approach. Typically, this combination of security is a very powerful one.

Ravi Das *is a technical writer for BiometricNews.net, an independent publisher and leading source of news and information about the Biometrics Industry. He has been involved in the IT industry for 10 years and launched HTG's security solutions division in 2003. This division offers a complete security solutions package and uses biometric technology as its main product offering. Ravi holds a Master of Science Degree in Agribusiness Economics from Southern Illinois University and a Master of Business Administration (specialising in Management Information Systems) from Bowling Green State University).*

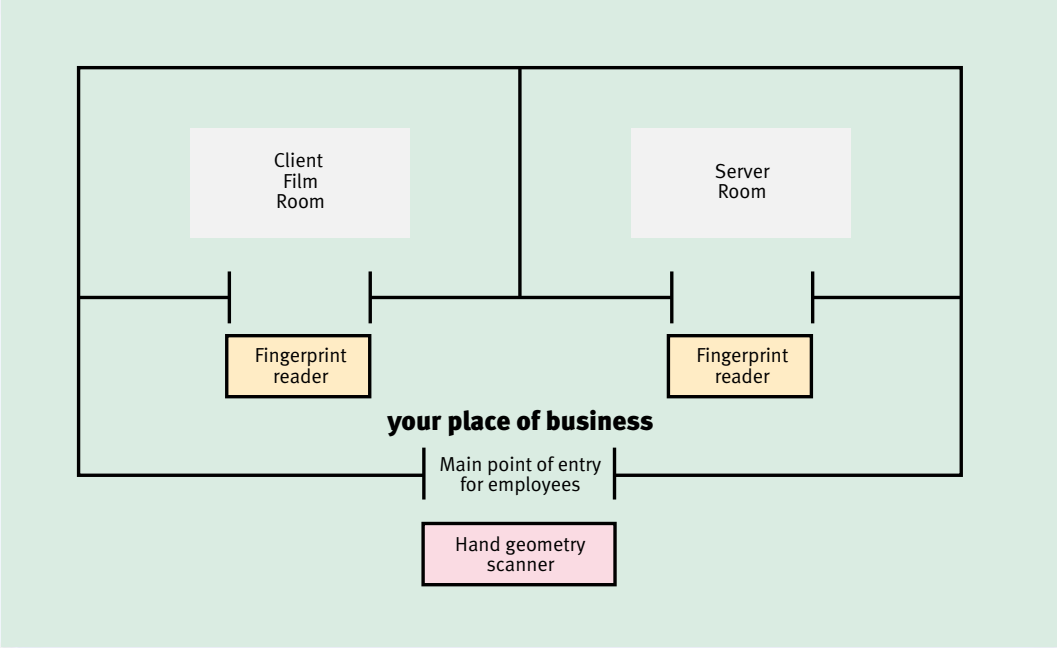


Figure 1
Example of physical access entry.

Other types of biometric devices can be used in lieu of fingerprint recognition, such as facial and iris recognition. Nowadays, vein pattern recognition is starting to be used extensively as a component of a multimodal biometric package.

However, as the decade went on, a new threat became evident, and perhaps on an even grander scale: identity theft. This is a threat from a logical angle.

Logical access application

Passwords have long been the traditional means of security when logging onto a computer or a corporate network. But as has become clear with the proliferation of the identity theft threats, passwords can be cracked and hacked very easily. Thus, organisations and businesses are constantly faced with enforcing stronger password policies, frustrating the end-user even more. But even here, biometrics is emerging as a much favoured security solution over the password. Nowadays, you can log into your network or computer with the single swipe of a finger or even a picture of your iris.

Today, new laptops often contain a small fingerprint sensor on the keyboard. While durable, significant damage can occur to it if the laptop is dropped, or exposed to harsh environmental conditions. To counter this, a secondary biometric system can be used, such as iris recognition. For example, when logging on to their laptop, an individual's identity could firstly be confirmed with a quick swipe of the finger, and then for extra protection, their iris could be scanned and verified via a built-in camera, before full access is granted. An example of this is portrayed in figure 2.[2]

As is the case with physical access entry applications, here also vein pattern recognition is emerging as the top choice in multimodal biometric solutions. In the world of logical access the cardinal rule of having two or more means of identity verification is just as important, if not more.

There are, however, less threatening circumstances in which multimodal biometric solutions can be used. One example is the time and attendance of personnel.

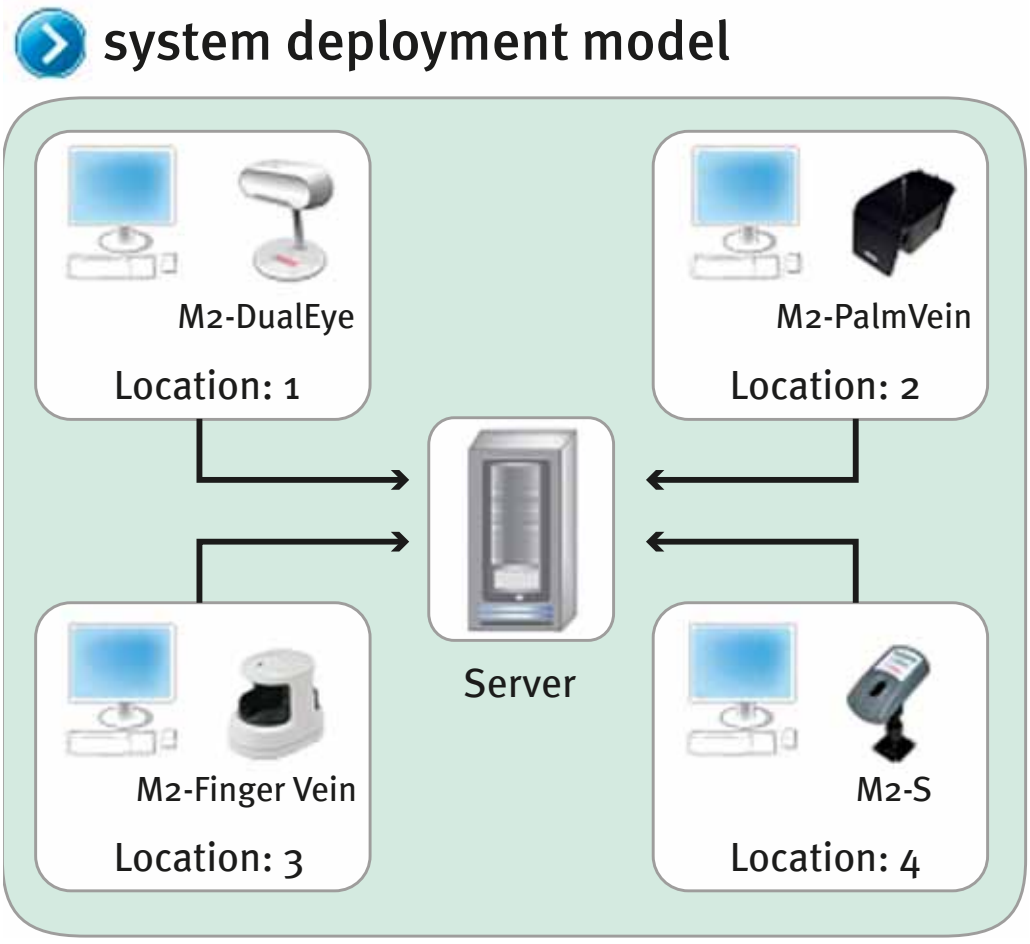
Time and attendance of personnel

Another major application of a multimodal biometric system is the time and attendance of personnel. This will be explained using a brief case study about the real estate firm Yarco Company, Inc.. This company were in need of a much more efficient method of keeping track of the time worked by their employees, but they also wanted to eliminate the problem of what is known as 'buddy punching', when one worker claims the hours of another employee.

The portfolio value of the real estate holdings encompassed more than USD 600 million. The method traditionally used to keep track of billable hours and hours worked was a manual, labour intensive process, spanning across over 100 real estate properties. It could take up to two days to process all the related paperwork, and there was no formal system in place to confirm the validity of the hours worked. Thus, a newer, and much more efficient method was needed: a multimodal biometric system.

The new application consisted of both a web-based approach and vein pattern recognition (figure 3).

Figure 2
Example of logical access.



The internet aspect was required for the biometric templates to be transferred smoothly and quickly, as well as for the payroll processing to happen at server level. The biometric component was used for employees to clock in and out using their vein pattern, thus eliminating the need for the traditional time card.

Results of the use of this multimodal biometric system were seen immediately. This once multifaceted process has reached a 90% increase in efficiency, compared to the old method. Much of the administrative overhead has also been reduced, thus allowing the HR staff to focus on more important issues.

Considerations and strategic benefits

In the past, implementing a multimodal biometric system was an expensive endeavour, as a biometric system would have to be implemented on top of, or with, an existing legacy security system. This would very often mean a major overhaul in the organisational infrastructure. However, the past decade has seen an evolution in biometrics technology as well as in multimodal systems. One unit or device can now house different technologies. Nowadays, multimodal biometric solutions are not just available as hardware, but can be obtained as a software development kit (SDK). This approach has become known as a 'hybrid' biometric system, where fingerprint, iris and vein pattern recognition is primarily used.

Considerations

Before you are going to implement either a hardware or a software multimodal biometric system, there are some key questions to be taken into consideration:

- As a business owner, are you trying to protect the physical or the logical aspects of your business?
- Which biometric system will work best for your particular multimodal system? As mentioned, you will have an entire array of technologies to choose from, such as:
  - fingerprint recognition;
  - hand geometry recognition;
  - facial recognition;
  - iris recognition;
  - vein pattern recognition.
- Will the new multimodal biometric system be layered with the existing security infrastructure, or will it be used as an addition? Probably the best way to answer this question, as well as the first two, is to conduct a comprehensive security audit.

- What are the costs, and what is your budget? Although in today's harsh economic times, IT budgets are the first to be trimmed, it is good to keep in mind that, compared to a decade ago, biometric solutions have become much cheaper, and thus more affordable for small and medium enterprises (SMEs).
- What kind of software applications, if any, will need to be developed to support a new multimodal biometric system? It should be noted that biometrics is not just about hardware and devices, the software component is equally important.

Strategic benefits

After evaluating some of these major factors, it will soon become apparent that a multimodal biometric solution offers a number of strategic benefits. Some of these include:

- A fortified level of security. Rather than having just one layer of security, you will now have multiple layers. Not only will there be a fail-safe mechanism in place, but should a perpetrator break through one line of defence, they will most likely be caught deeper in. In other words, an SME can retain a very high security threshold with this scheme.
- There are many metrics that are included in evaluating the effectiveness of a biometric system, for example the False Accept Rate (FAR), the False Reject Rate (FRR) and the Equal Error Rate (ERR). By using a multimodal biometric system, the reliability of the verification process is greatly increased.
- Some systems experience difficulties enrolling and verifying people of different ethnic origins, but a multimodal biometric system can capture the unique characteristics of a much larger and varied population. A read rate of almost 100% can be guaranteed.
- In biometrics, there is always the theoretical issue that a system can be spoofed. By having extra layers of biometrics, this issue has become, over time, much less prevalent.
- As mentioned previously, a newer version of the multimodal system is known as the hybrid approach. This permits for more than one biometric technology to be used within one component. An example of this is a SDK, which allows for the different recognition technologies to be all used together, independent of the actual hardware being utilised.
- From a business and financial point of view, a multimodal biometric system also offers the end-user:
  - the ability to customise their application and have it based upon environmental and/or ethnicity factors, as well as a host of other variables which are required by the deployment environment;
  - the flexibility to add to or transfer from one biometric modality to another as newer technologies evolve;

Figure 3
An example of a vein pattern recognition device.[2]

  - a quick return on investment, and a vast reduction of the cost of ownership, as a combination of biometrics can be virtually realised for the cost of just one full biometric implementation.

Conclusion

As discussed at the beginning of this article, one should never rely upon just one means of security for asset protection, but always upon multiple levels of it. A multimodal biometric system offers such an approach. As we progress over time and well into the future, we will continue to see the evolution of new biometric technologies and related software. Naturally, this means that the cost of existing biometric technologies will only come down further, thus making a solution available to SME's that, at one time, only the largest of corporations could afford. Another interesting trend in the biometrics industry will be the one offering solutions through a hosted approach, or through the 'cloud', in which multimodal biometric solutions will play a very important role as well - a topic for another article.

1 Hong, L. & Jain, A.K. Multimodal Biometrics. Article in Biometrics: Personal Identification in Networked Society by Jain, A.K., Bolle, R. & Pankati, S.
2 Figures 2 and 3 and the case study provided by M2SYS, LLC. Permission was obtained to use images and case study.

If you would like to respond to the contents of this article, please send an email to kjd@keesingreferencesystems.com