When To Use Biometrics

Hagai Bar-El
hagai@hbarel.com

Abstract

Biometric systems become common over the years. Their ease of use for the end user and their perceived security make them seem to be the best solution to any problem involving user authentication. Although biometric systems can provide fast and secure user authentication with minimal user intervention, they have several inherent limitations making them inappropriate for most environments where authentication is used. The focus of this paper is not the possible use-cases of biometry, but rather it is those limitations that are neither biometry-type specific nor implementation specific and that make biometric measures limited in their scope of possible uses.

1 Introduction

Secure user identification is a common requirement for almost every secure system. Transaction authentication, authorization, non-repudiation, validation and other building blocks of security require that a system knows the identity of the user who is accessing it, or who is generating a piece of data.

Three factors were defined for authentication of users, namely: "Something the user knows", "something the user has" and "something the user is". "Something the user knows" refers to passwords, passphrases, PINs and other information that the user is requested to provide the system with as a proof of his identity. "Something the user has" refers to physical possessions that the user introduces to the system in order to prove his identity. The best examples for these are keys, cards and tokens. "Something the user is" refers to biometry and to more-or-less unique biological properties that the user has and that can be verified by the system in an attempt to identify the user.

The advantages for using biometrics are quite straightforward. They require minimal user intervention in terms of remembering things and do not require the user to carry tokens. Also, biometric systems are perceived as highly robust. Science-fiction movies play a major role in the heroic perception of biometrics. Excitement from the new user-friendly-and-secure technology caused some of its disadvantages to be overlooked.

Some of the trivial obstacles to deploying biometry, such as the high cost involved in the dedicated hardware it requires, were always known. Recent studies demonstrate technical weaknesses that make most hardware devices susceptible to physical attacks, which appear to be much less hard to mount than previously thought. Lack of accuracy, as shown in false-positive and in false-negative rates, are also known and considered. These problems can be collectively called "technological problems".

The other group of problems, which is seldom considered, is the group of problems that are inherent to biometrics, and which cannot be solved by newer technology or by more accurate devices. These problems result from the ever-true fact that a person's biometric pattern, which may be unique for that person, is certainly not a secret. This fact, and the issues that result from it, narrow the range of applications and circumstances that can benefit from the deployment of biometrics, dramatically.

2 Technological problems

Although the group of problems that are considered to be technological problems is beyond the scope of this paper, I would like to present the biggest problems in brief.

Other than the high cost involved in the deployment of biometric systems, the biggest technological problem with biometrics seems to be lack of accuracy. The accuracy of biometric systems is represented by the false-positive and the false-negative rates of the system. The false-positive rate is the probability that the biometric system will identify someone as having an identity that he does not have. The false-negative rate is the probability that the biometric system will fail in identifying an individual as having the identity that he has. In many cases, the false-positive and false-negative rates are low enough for the system to be applicable. However, there

are circumstances in which even the lowest error rates known for biometric systems are still not low enough.

For example, let us take a biometric system that has 99.9 percent accuracy in terms of false-positives. In such a system, the probability of an arbitrary individual to be identified as someone he is not is one to a thousand. This definitely seems to be a low probability, and many biometric systems do not enjoy such high accuracy, but there are at least two cases in which this probability is still much too high.

The first case is the case of a high security facility. The probability of 1 to 1000 of an unauthorized person to succeed in identifying as someone else is much higher than the probability of a similar event when using cryptographic authentication with cryptographic tokens. The latter usually offers probability of 1 to 2^{100}, or even less, when functioning correctly.

The second case is where false-positive events have a less crucial impact but where many examinations are carried out. In the urge to improve airport security a new face recognition system was proposed. The system consisted of closed-circuit television cameras that were to be installed in airport terminal buildings. An intelligent face recognition program was set up to examine the images of the crowd and to alert in a case that it spots a terrorist among the people. With 99.9 percent accuracy and an airport that hosts 100,000 passengers a day we would experience an average of 100 false alarms per day. A hundred false alarms result in a hundred investigations, a hundred angry customers who miss their flight and an enormous hassle and cost. No airport can afford having one hundred such events per day, and unfortunately, the accuracy of face recognition today is still lower than 99.9 percent.

The problems that result from lack of accuracy could be eliminated as accuracy increases with new technology. Prices are also likely to go down with time. Even the most serious flaws that were discovered in some biometric systems are likely to be solved one day by this way or the other. What are not likely to ever be solved are the problems of the second group, presented in the next chapter.

3 Inherent problems

As mentioned, biometric patterns may be unique, but they are not secrets. The fingerprint of a person can easily be retrieved from anything that person touches. The face pattern of an individual can easily be deduced from a photo of that person. The voiceprint of a person can easily be recorded and replayed or analyzed. Therefore, a biometric pattern cannot be treated as a password or as any other authentication credential we know.

This single fact alone leads to difficulty when using biometrics, to the extent that in most cases their use is completely insecure when not deployed in combination with other mechanisms, which may just as well solve the authentication problem by themselves.

3.1 System security requirements

For biometrics to serve their purpose well, the system needs to take into consideration the fact that biometric patterns shall not be treated as secrets or as keys. The first and most obvious requirement is for the pattern that was read by the reader to be encrypted as it passes to the authenticating device. Sending a pattern in the clear is like sending a password in the clear with the only difference being that the biometric pattern of a person cannot be changed if a leakage is discovered. End-to-end encryption of some sort is therefore a must.

Furthermore, the authenticating device or server must be sure that the reader is a valid reader and that the pattern it receives indeed originated from that reader and was not injected by an adversary. Since the pattern itself is not a secret and shall be assumed to being available to anyone, the integrity and originator of each received pattern has to be assured. The authenticity signature or MAC has to be generated within the reader itself to prevent injection of a pattern by the host that the reader is connected to.

The only secure way to achieve confidentiality and integrity is by forming an authenticated and encrypted channel between the authenticating device (or server) and the reader. This means that key management facilities and effort must be put in place in order to issue and certify asymmetric key-pairs or to securely issue symmetric keys to all readers and possibly also to all authenticating devices. Having a single key for all readers and all authenticating devices (or servers) is too risky. No system can afford a complete collapse due to a single compromised reader. As for the authenticating device, the likelihood of the authenticating device to actually be a server makes the leakage of that key at some point of time a certain event. Therefore, the best

way to carry out such key distribution is probably using PKI (Public Key Infrastructure) having a CA, or a tree of CAs, certify individual keys that are installed in readers.

If all readers are certified and are capable of establishing an authenticated and integrity-protected session with all authenticating devices, and assuming the biometric pattern is not a secret anyway, the confidentiality requirement may be relaxed. This, however, does not eliminate the need for any of the components that were discussed.

In addition to the need for a massive key infrastructure involving all readers, the readers need to have cryptographic capabilities so they can take part in the authentication and encrypted tunnel establishment with the authenticating devices. The readers will have to support symmetric encryption, asymmetric encryption (if PKI is used) and probably random number generation as well. Additionally, each reader must be capable of storing its key (either private or shared) securely; hence tamper resistance for the reader is required. The last requirement alone might multiply the price of readers by a significant factor. Tamper-resistance is a hard enough problem in smartcards. Biometric readers, which are naturally larger and by far more complex in their hardware, may be impossible to protect to the same extent.

We end up with a biometric reader that has all the functionality of a smartcard, but which is much harder and most expensive to produce, offering an added value that is not obvious. After all, a tamper-resistant module with secure key storage and cryptographic capabilities, along with a key infrastructure consisting of individual keys for all entities, can form a highly secure authentication framework without involving biometrics at all. Furthermore, the higher false-positive rates of biometric measurements over cryptography may make this solution even less secure than the collection of the ingredients listed above without the biometric part but with a PIN and person-to-key binding instead.

The claim that the biometry harms the security of the system due to its false-positive rates may be debated against, and depends on the specific technology, which is dependence I try to avoid in this chapter. Notwithstanding, it is easy to see that the biometric part of the authentication framework cannot possibly increase the security of the system beyond the security of the cryptographic authentication between the reader and the authenticating device. The robustness of the tunnel between the reader and the authenticating device forms an upper bound on the security of the overall system. This means that the biometric part of the authentication cannot lead to higher security.

Whereas biometry cannot increase the level of security provided by the required cryptographic layer underneath it, it can still assist in eliminating the PIN in cryptographic modules that require a PIN to unlock the private key they hold. In this case the reader itself evaluates the pattern and the only authentication performed with the server is a cryptographic one.

In order to establish a secure biometric authentication framework, the authenticating server (or device) must accept only fresh patterns only from authentic readers. This can be achieved, as shown above, by cryptographic means, but may also be achieved by direct physical connectivity. If the reader is installed in the same physical environment as the authenticating device (for example: a door or a gate), and the area is physically protected, so the reader cannot be tampered with, then biometrics can be used without the need for cryptography. This, however, cannot apply to systems that are distributed in any way, such as systems performing authentication over a local network.

3.2 Generation of key material

The second fundamental problem with biometrics relates to the process of deriving key data from user credentials. After the user is authenticated, key exchange often takes place. The key-exchange step is necessary when authentication is done as a part of secure channel establishment. Furthermore, secure protocols usually assure that the protocol data, which is sent after authentication, is cryptographically bound, directly or indirectly, to the credentials used for authentication. This is mainly to avoid man-in-the-middle attacks and session hijacking attacks. Most if not all of the protocols that separate authentication from key exchange are susceptible to these attacks.

In order to achieve successful binding, the session key used for secrecy or integrity must be a function of the users credentials and shall not be known to an opponent. Other requirements should be met as well, but the involvement of the users identity in a form that cannot be imitated by an adversary is one of the musts. Since the biometric pattern is not a secret, it cannot be considered as a good candidate for generating key material, unless when involving additional

information that is secret. The only secret credential that can be used for generating key material is the private, or shared, key of the reader. This key is a secret, but one which has nothing to do with the authenticated user.

Additionally, digital signatures, which are commonly generated by applications on behalf of the user, cannot be generated if user identification is done by biometric means. The generation of a digital signature requires at least one piece of information that is known only to the user who generates the signature. In a biometric authentication system there is no such piece of information. The only user-specific data is the biometric pattern, which is not a secret. Using the biometric pattern alone for signature generation will result in a signature that anyone can fake. On the other hand, using the readers private, or shared, secret for signature generation will result in a signature that it is impossible to link to the individual, and thus that cannot provide for non-repudiation.

4 Conclusion

Biometrics, like other authentication mechanisms, have their advantages and disadvantages. They provide high convenience for the user and can, in some circumstances, provide stronger authentication than offered by other applicable solutions. However, in some situations where user authentication is required, biometrics can offer adequate security only when integrated with cryptographic mechanisms, including a key infrastructure.

When biometrics are integrated with cryptography, the cryptographic layer in most cases assumes all responsibility for the security level of the system, thus making the biometric identification by the server plain unnecessary. In some specific cases integration of biometrics and cryptography can provide an added value on using cryptography alone. In some of the other cases, biometrics and cryptography together provide less in terms of security than the cryptographic layer (along with the key infrastructure) could provide by itself. Biometry can sometimes add security to the cryptographic module by replacing the local PIN that the module asks for. In this case, the authentication between the module and the server is a purely cryptographic one and biometrics are used for the local authentication between the device and the user.

The only environment in which biometrics can be applied as is, is a physical area where the reader and the authenticating device are physically connected and reside in a room which is supervised. All other environments require adding strong cryptographic capabilities both to the authenticating devices and to the readers, including adequate key management. These additional cryptographic capabilities, however, can often form an authentication framework by themselves, which is just as good.

Lastly, biometrics cannot be applied also in systems that require the generation of digital signatures.