Biocryptography

Increasing the protection of biometric templates - part 2

by Ravi Das

In the first part of this article, which was published in the previous issue of this Journal, Ravi Das explained the scientific concepts of what a biometric template really is, and gave us an introduction to (bio)cryptography. In this second part he explains how the concepts of cryptography can be used to increase the protection of fingerprint and iris templates in three different types of network environments, and also gives a number of implications for further research.

***Ravi Das** is a technical writer for BiometricNews.net, an independent publisher and leading source of news and information about the Biometrics Industry. 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.*

In the first part of this article we have seen that mathematical functions are used for the encryption and decryption of the biometric template, while in transit across the network medium. A component which is central to these mathematical algorithms is a so-called 'key'. It is the key itself which is used to encrypt or lock the biometric template at the point of origination, and it is also used to unlock that same template at the receiving end.

The key itself is a series of mathematical values. There are many types of keys used in cryptography, such as signing keys and session keys, and the number of keys generated depends primarily upon the mathematical algorithms used. In the world of cryptography, there are two primary types of algorithms:

1. Symmetric algorithms.
2. Asymmetric algorithms (or Public Key Algorithms).

Symmetric algorithms

In symmetric algorithms, the same key is used to encrypt and decrypt the plaintext biometric template. As a result, their use possesses inherent risks and dangers, because the primary security here depends solely upon the key which is being used. If anybody divulges the secrecy behind the key, the security of it is 100% compromised.

Asymmetric algorithms

The alternative to the symmetric cryptography is asymmetric cryptography. In this process, two keys are generated: one for the encryption and one for the decryption of the plaintext biometric template.
The encryption key is known as the 'public key', and the decryption key as the 'private key'. The security strength is much greater than that of the symmetric algorithms, not only because two keys are being used, but also because the decryption key cannot be computed from the encryption key.

Public Key Infrastructure (PKI)

In businesses and corporations all over the world today, it is the asymmetric approach which is most commonly used, especially for client server network topologies, given its superiority over the symmetric approach.

One of the most popular, or commercial forms of the asymmetric cryptography is known as 'Public Key Infrastructure', or 'PKI' for short. It has been around since the 1970's and consists of the following components:

- The digital certificates.
  This is the PKI's version of the public and private keys. These certificates are kept within the biometric system itself (such as the fingerprint scanner or the iris scanner), and within the central server (which houses the database(s) of the fingerprint and iris templates, and the biometric template processing functions).
- The biometric devices (the actual hardware) and the servers.
- The LDAP/X.500 directories.
  LDAP stands for 'Lightweight Directory Access Protocol' and X.500 is its related network protocol for communications across the internet. These are the database structures in the central server in which the iris and fingerprint templates are housed.
- The Certificate Authority (CA).
  In smaller versions of PKI, the two keys are often generated from within the system itself. But in more complex systems, such as that of a biometric-based one, the two keys or the digital certificates are issued and verified by a third party known as the Certificate Authority or 'CA'. Although adding a CA is more expensive, it is often viewed as an 'unbiased third party', and as a result, the digital certificates are viewed with much more trust and confidence than if they were generated from within the system.

Using cryptography to protect fingerprint and iris templates

Biometric systems can involve quite an array of system designs, deployments and network architectures. To illustrate how the concepts of cryptography can be used with biometrics, three different types of network environments will be discussed in which biometrics can be stored. These environments are:

1. A stand-alone biometric system.
2. A client server setting, where the biometric devices are connected to a central server.
3. A hosted environment, where the biometric templates and processing functions are placed in the hands of a third party.

Please note that the three examples described and discussed below are theoretical in nature, they have not yet been proven in the real world, and it is assumed that much research will have to be conducted before these applications are put to the test on a commercial basis.

1. Stand-alone biometric system

With the biometric technology available today, most fingerprint recognition and iris recognition scanners consist of a database and a processing function integrated in a stand-alone unit. This means that enrolment and verification occur at one single point. There are obviously many advantages to having such a stand-alone system, with the biggest two being costs and time; the costs are relatively low and the enrolment and verification templates can be processed very fast.

Biometrics

In a stand-alone biometric system, cryptography can be used as follows to protect the iris and fingerprint recognition templates:

1. When the end-user wishes to gain physical or logical access with his or her fingerprint or iris scan, a verification template needs to be created. This template is either a binary mathematical file (for a fingerprint template) or an IrisCode (for an iris template).
2. Using the principles of symmetric cryptography, the verification templates are then encrypted with the key that is generated by the system. This takes place directly after the unique features from the fingerprint or the iris are extracted, and the template is created.
3. Once the verification template reaches database level, it is then decrypted with the same key, and the statistical correlations are computed between the verification and the enrolment templates. If this correlation is established within the bounds of the security threshold, then the end-user is granted physical or logical access by the biometric system.

In this example of a stand-alone biometric system, a number of key assumptions are made:

- Only verification or a 1:1 match is being used. Since it is being done at local level, the configuration needs are low, and therefore symmetric algorithms are the key choice of cryptography to be used. As a result, only one key is generated.
- Only the verification templates receive the added protection from encryption. This is because the fingerprint and iris recognition templates are created only once, and are later removed from the biometric system. In fact, in any biometric system, no matter what the magnitude of the application is, verification templates are used only once.
- The enrolment templates in the finger and iris biometric system receive no added encryption protection. This is unquestionably an inherent security risk, but one has to keep in mind that the database is being stored in the biometric device, instead of in multiple places, when the need for protection would be much greater.
- In a stand-alone verification application the processing power required is much less, compared to the client server or even the hosted approach, thus supporting the need for only the use of symmetric algorithms.

2. Client server biometric system

A traditional client server network topology consists of a series of computers connected to a central server via a network medium (for example, a hard-wired network or a wireless one). All the resources and applications the end-user needs access to, reside within this central server. The server often contains databases with all types and kinds of data, and is also the point where database querying and processing takes place.

This type of infrastructure can vary from very small (a Local Area Network, or LAN) to very large, covering great distances and international boundaries (a Wide Area Network, or WAN).

Biometrics

This type of setup can also be extrapolated to biometrics. Multiple biometric devices can be linked to a central server, in a very similar way as described above. However, the key difference in a biometrics client server system is that the primary application is solely used for verification and identification, (template processing/querying). Nowadays, typically the medium to larger-sized businesses are the ones that use biometric client server applications. Because many more resources are required, the costs are a lot higher than with a stand-alone biometric system.

In this type of configuration the most common biometric devices are hand geometry scanners, fingerprint scanners, iris scanners and facial recognition scanners. Different biometric devices (such as fingerprint scanners in conjunction with iris scanners) as well as the same devices (all fingerprint scanners) can be used together. In the end, it does not really matter which hardware is used, because they are all accessing the same resource: the central server.

Biocryptography

The security threats posed to this system are much greater than to a stand-alone system. Again, biocryptography can play a huge part to insure the protection of the biometric templates. For this configuration, asymmetric cryptography will be used, and both a public and as a private key will be generated.

The process of biocryptography would work as follows in a client server biometric system:

- The end-user's finger or iris is scanned, and each biometric system will create the usual verification templates (assuming that both iris and fingerprint scanners are being used simultaneously).
- The iris and fingerprint verification templates are encrypted by a public key.
- The newly encrypted verification templates will make their way across the appropriate network media, and finally to the central server.
- The biometrics database is stored in the central server, which contains the relevant iris and fingerprint enrolment templates. Here the private keys are stored and the templates decrypted.
- Once the public and private keys have been decrypted, the appropriate statistical measures will be applied to determine the degree of similarity between the verification and the enrolment templates.
- Based upon the results, the end-user will be granted or denied physical or logical access to the application.

An important point needs to be made about the biometrics client server system. As is the case in the stand-alone biometric system, the verification templates will be discarded along with their public keys, after they have been compared and evaluated. The enrolment templates will have to be decrypted as well, so that the comparison between the verification and the enrolment templates can be made. As the enrolment templates are stored outside the actual biometric device, however, they will have to be re-encrypted again to insure maximum security while stored in the central server's database. Thus, this type of configuration will need far more network resources and much more processing power. Also, there is no doubt that extra overhead and quite possibly further verification times will increase by a few more seconds (under normal conditions, these are less than one second).

3. Hosted biometrics environment

The world of information technology sees a shift towards a new type of application, known as 'cloud computing', or 'Software as a Service (SaaS)'. With cloud computing the entire IT infrastructure of a business can be outsourced to and managed by an independent third party, also known as a 'hosting provider'. This third party will set up the IT infrastructure hardware and software and manage, maintain, and upgrade it. Business owners only have to open an account with the hosting provider, and with a few mouse clicks, arrange the IT services they want.

The most important advantage of cloud computing is the total elimination of IT administrative headaches and hassles, as the hosting party is entirely responsible. Furthermore, a business only pays for the software/hardware services they have subscribed to, at a fixed monthly cost.

Biometrics

The cloud computing model can be extrapolated to the world of biometrics, and can then be termed 'Biometrics as a Service (BaaS)' or a 'Hosted Biometrics Environment'. It would be established as follows:

1. A business purchases the requisite biometrics hardware (fingerprint scanners and iris scanners).
2. After the biometrics hardware is installed, the business has to set up the services needed with their account, and all is set to go.
3. The responsibility for the servers, the databases containing the iris and fingerprint enrolment templates, the processing of the verification templates between the enrolment templates and formulating the match/non-match result rests entirely with the hosting provider.

Biocryptography

As the iris and fingerprint templates are placed at the hands of the hosting provider, their security becomes the prime concern. There is yet another cryptography tool which would work perfectly here: a Virtual Private Network or 'VPN' for short. This is how it would work with a BaaS type of application:

1. The end-user has their fingerprint or iris scanned to create a verification template, which gets broken down into a separate data packet. This data packet is then further encapsulated (or encrypted) into another data packet, so it eventually becomes invisible as it traverses across the various network media, making its way to the servers of the hosting provider.
2. To ensure the integrity of this double-layered data packet, it also contains headers with information about the size and type of the verification template. Upon receipt of the data packet, the headers serve as a confirmation to the hosting provider that none of the iris or fingerprint template data has been altered or changed en route.
3. To create another layer of protection, a dedicated VPN channel can be created. This is a direct line from the point of origin of the fingerprint or iris scanner all the way to the servers of the hosting party. This is known as 'IP Tunneling'. The channel cannot be seen by other people accessing the internet via the same network media across which the data packets are also travelling.

Box 1

RSA Algorithm

To further illustrate the sheer power of asymmetric cryptography and its use in a biometric client server system, a popular algorithm which could work perfectly in biocryptography is known as the 'RSA Algorithm'. It was developed in 1978 by Ron Rivest, Adi Shamir, and Leonard Adelman. RSA Data Security owns all the intellectual property rights associated with this algorithm, which nowadays is the major asymmetric algorithm. The strength behind the RSA methodology is that it uses the power of prime numbers and the effort associated with factoring large numbers. The public and private keys which encrypt and protect the verification and enrolment templates are direct mathematical functions of a pair of very large prime numbers (over 200 digits). The logic behind this is that it is very difficult to work backwards from the created product to discover these large prime numbers. It would take a very long time to figure out, and as a result, a hacker would most likely give up in frustration.

4. Once the data packet has arrived at the servers of the hosting provider, it is decrypted and the verification and enrolment template are compared.
5. After a match or non-match has been determined, the result is sent back to the place of origin of the iris or fingerprint scanner, after which the end-user is allowed or denied access to the resources or applications they have requested.

IPSec

To further fortify the VPN between the place of business and the hosting provider, a protocol known as 'IPSec' can be used, which also uses digital certificates (public and private keys). The IPSec protocol is a major security enhancement to the TCP/IP protocols which are used by everybody nowadays to gain access to the internet. One specific type of IPSec mode, the so-called 'IPSec Tunneling', helps to provide maximum security for the data packet housing the verification template. In this IPsec mode the header and the verification templates are further encrypted at a much deeper level.

Some points of attention need to be made about BaaS:

- Although this type of application is still very new (thus far only voice biometrics has been used as a BaaS), it could very well be the wave of the future. The reason for this is that the biometrics security technology is still perceived to be very expensive.

With a hosted approach, however, these high costs will be considerably reduced: the business owner only needs to purchase the required biometric hardware, and then pay a fixed monthly cost.

- With BaaS, the verification times and presentation of the match/non-match result could take time, because the template processing and matching will take place at the hosting provider. The speed will be a direct result of the hardware and software used, and of the network bandwidth.
- Although BaaS holds great promise, one of the biggest obstacles it faces is the issue of privacy rights which constantly plagues the entire biometric industry. In the case of BaaS, this privacy issue will only proliferate, as the biometric templates are in the hands of an outside third party.

Conclusions and implications for further research

In summary, this article has examined how the principles of cryptography and biometrics can be used together to provide maximum security for the biometric templates that are created and stored. Biocryptography is still very much an emerging field, and some observations have to be noted:

- The three types of network environments discussed above could become very complex, if proven to be viable in the real world. The reason for this is that two types of security technology become one, and from that, many variations of all kinds and types could be created. It is therefore very important that right from the outset attention is paid to the actual analysis and design of the biometric systems, in order to ensure a smooth and streamlined process with regards to troubleshooting and support.
- Another area which has haunted and plagued the biometrics industry is that of the sheer absence of a standards and best practices list for the technology, both in its current state and as it is being developed. As biocryptography emerges into the forefront of security, such a list is an absolute must in order to avoid duplication of efforts, which would result in unneeded and bloated overhead. Also, as businesses and entities start to adopt biocryptography, a standards and best practices list will help to provide the groundwork needed to create security applications, rather than having to re-invent the wheel every time.
- Although biocryptography can be used for any kind or type of biometrics application, there will be two primary drivers which will cause this emerging field to proliferate and expand: the continuing trend of adopting multimodal biometric solutions, and the sheer explosion of wireless communications and technology, in particular the smartphone.
- Finally, it is the author's point of view that biocryptography should be developed in an open model type of forum, where all parties involved, ranging from the private sector to academia to government level can collaborate and discuss new ideas with the goal of open communications and an open dialogue. An open model would help minimise any potential security threats and risks, because answers and solutions can be thought of very quickly. This is best demonstrated by the use of the open source model for software development versus the closed source model.