CONCEPT OF BIOMETRIC SECURITY SYSTEM

Martin DRAHANSKÝ, Doctoral Degree Programme (4)
Dept. of Intelligent Systems, FIT, BUT
E-mail: drahan@fit.vutbr.cz

Supervised by: František Zbořil

ABSTRACT

This article is devoted to the description of the Biometric Security System concept. The biometric security system consists of the classical biometric system and cryptographic system. Both are connected and can cooperate. Further two processes in the biometric security system are described – namely process of certificate creation and certificate usage. At the end are introduced two possible proposals, in which the biometric security systems could be used.

1 INTRODUCTION

Authentication is a fundamental component of human interaction with computers. Traditional means of authentication, primarily passwords and personal identification numbers (PINs), have until recently dominated computing, and are likely to remain essential for years to come. However, stronger authentication technologies, capable of providing higher degrees of certainty that a user is who he or she claims to be, are becoming commonplace. Biometrics is one such strong authentication technology.

The classical biometric systems (here focused on fingerprint technology) are known for a long time. They are used for two different main tasks – access control and forensic. The second group is unimportant for our considerations, but the first one can be extended and this extension is connection with some cryptographic module. Let us call these conjoined systems – the Biometric Security Systems. Like many other technologies, the Biometric Security Systems have some advantages and disadvantages – see [1,2].

2 THE MAIN CONCEPT

The description of the main concept of the Biometric Security System follows. The biometric attributes (data) must not only serve to access or verification/identification, but can be used for data protection. We can ask, if it is possible to generate some art of key from the biometric data that can be used to encipher and/or decipher data. There is enough information entropy in the fingerprint to generate the key [3], which is suitable for symmetrical cryptography. The minimal entropy factor [3] is about 2^{240}, what is sufficient data amount for symmetrical cryptography. On basis of these statements, we introduced a Biometric Security

System, using the combination of key generation from the fingerprint and voice [4], and a corresponding cryptographic algorithm.

The following two subchapters describe concrete processes of the Biometric Security System. As the input biometric information could be used any of biometric attributes, as said in the introduction. The only requirement is the entropy power in the selected biometric attribute [3,4]. If there is not enough entropy information, it is impossible to generate strong cryptographic keys, even if the process of key generation is realizable.

2.1 CERTIFICATE CREATION PROCESS

In this process, the certificate, including the biometric information, is generated. The certificate may be based on the X.509 standard. The certificate has to be generated only by an administrator, who is possessing the certification authority key pair. Hereby is guaranteed that the whole process of key generation and certificate creation was successful and trustful. If the whole process was without problem and all steps of certificate generation were under control, then the content of the certificate can be signed by an administrator. The signed certificate warrants the correctness of all items (name, organization, department, personal number, biometric data, etc.). Important is, that this certificate creation is done only once. New certificate should be newly generated only if it is necessary (e.g. the certificate is not valid more). The same biometric attribute can be used in other applications, because the biometric data is not saved (not even as template) in the certificate and therefore can not be compromised. The main substeps of this process can be seen in the Fig. 1. In the phase of Acquirement the fingerprint is scanned, then the center of the fingerprint is computed and the minutiae sets (from 5) are assembled. The next phase is the Key Generation, composed of reference minutiae estimation, oriented closed graph creation, quantization and the last item is subgraph generation. Herewith the subvectors (biometric keys) are generated. The last phase is the Cryptomodule – beginning with hash computation (of each subgraph), following by secret encryption (extern input) and ending in certificate creation. This certificate can be stored on normal data token, with sufficient data capacity.

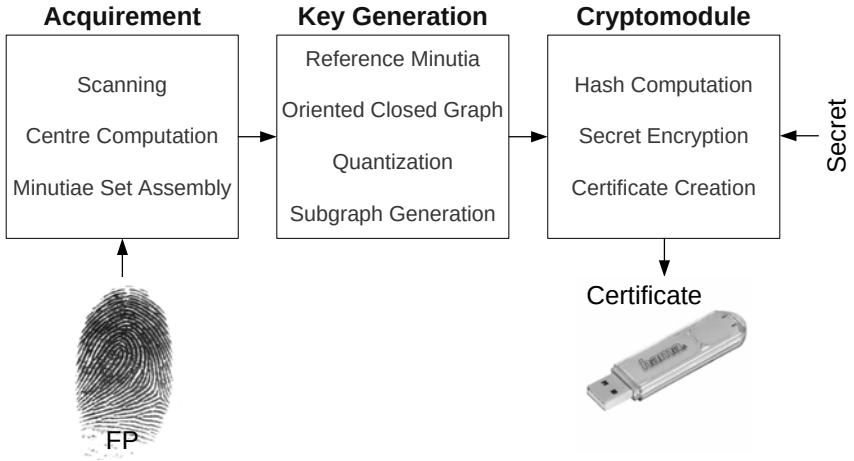

Fig. 1: *Certificate Creation Process*

2.2 CERTIFICATE USAGE PROCESS

The process describing the certificate usage is concerned on the daily usage of this

certificate, generated in the certificate creation process. The phase of usage can be applied repeatedly - it requires no action by the certification authority. The only condition is, if the confidentiality of the certificate may be proved, to get the possibility to obtain the public key of the certification authority, which has signed the certificate. The schema of this concept is shown in the Fig. 2. The phases are same, but the content of each phase is different. In the Acquirement phase only one (in relation to 5 by certificate creation) fingerprint is acquired. Then the center of this fingerprint is computed. The second phase is the Key Generation. The reference minutia is found here, the oriented closed graph is created, the whole graph is quantized and at the end only one subgraph is generated. In the last phase (Cryptomodule) the hash from the subgraph is retrieved, and this is compared with all hash values stored in the certificate. If the match is found, the subgraph (representing the biometric key) can be used to decipher the secret, which can be delivered further to the requesting application.

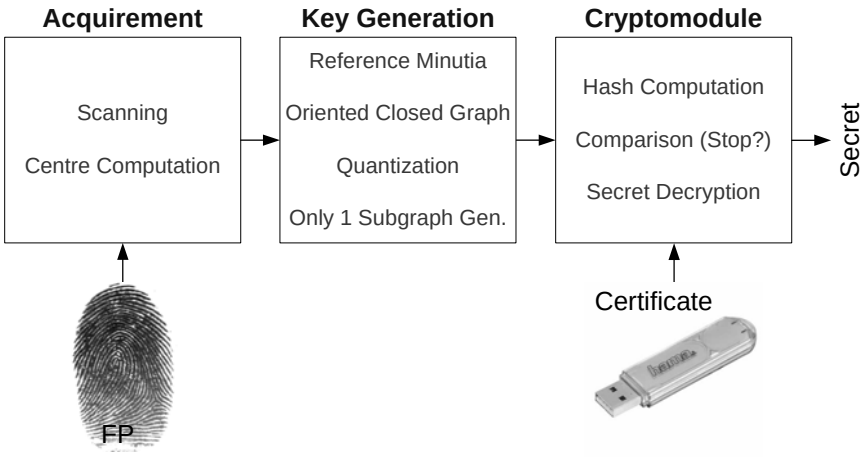

Fig. 2: *Certificate Usage Process*

3 CONCLUSION

In the previous chapters were sketched the processes of certificate creation and certificate usage. Now come two proposals of the disposal in the real world:

- *Private key protection*. The first possibility is the protection of some private key. Let us assume that some application has generated a cryptographic key pair. The public key is publicly accessible, but the private key has to be protected. One condition is that the private key can not be saved in open form or can not be readable from unauthorized person. These conditions are in our system guaranteed, while the secret is encrypted and saved only in encrypted form. The pairs – hash value from the biometric key and the encrypted private key – are saved in the certificate. When the private key is requested by another application, the fingerprint must be scanned and the biometric key is generated. The comparison of the hash value from this key with the saved hash values in the certificate is done. If the match is found, the biometric key corresponding to the hash value can be used to decrypt the private key, which will be delivered to the requesting application.

- *Personal document extension*. The second proposed possibility is important for new extension of the information in the personal documents, regarding biometrics. The personal document will include some smart chip, where all data can be stored. The certificate will be stored on this chip, including personal information and hash values of the subgraphs generated from the fingerprint of the user. As the secret will be taken the photography of the user. This photography is saved enciphered in the certificate. As an example of a usage could be discussed the passport control. The user gives his passport to the customs officer and he controls the data in the paper form. But moreover, during the manual control, the data stored in the chip are read. The user is claimed to authenticate – verify his identity with the identity information on the chip. He must let his finger to be scanned. This biometric information is processed and the subgraph is generated. If the match in the set of hash values is found, the photography of the user can be deciphered using this biometric key and compared visually with the photography scanned from the paper form and with the real visage of the user.

The Cryptomodule can combine two or more another biometric attributes. The encryption / decryption have to be done in a cascade – see [1,2]. Such combination of two different biometric attributes in the Cryptomodule is shown in the Fig. 3.

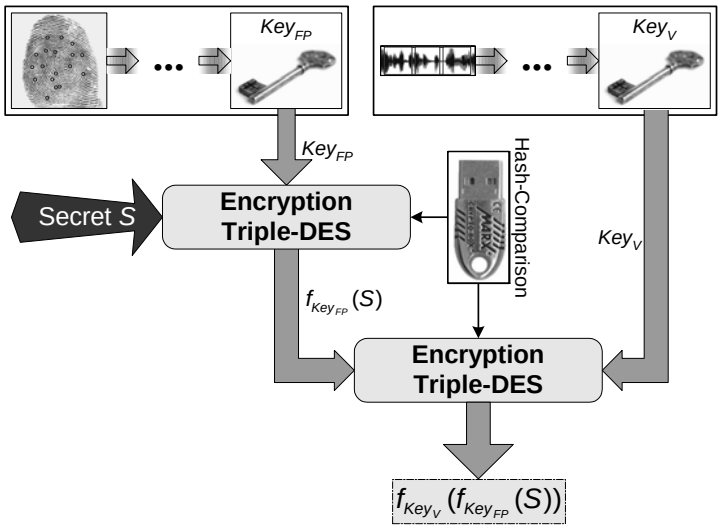

Fig. 3: *Combination of fingerprint and voice in the Cryptomodule*

REFERENCES

[1] Drahansky, M., Orsag, F.: Biometric Security Systems: Fingerprint and Speech Technology, In: Proceedings of the 1st Indian International Conference on Artificial Intelligence, Tallahassee, IICAI, 2003, p. 703-711, ISBN 0-9727412-0-8

[2] Drahansky, M., Orsag, F.: Biometric Security Systems: Robustness of the Fingerprint and Speech Technologies, In: BT 2004 - International Workshop on Biometric Technologies, Calgary, 2004, p. 99-103

[3] Drahansky, M., Smolik, L.: Entropic Numbers from the Fingerprint, In: BMWA – Workshop on Biometrics, London, 2004, p. 20

[4] Orsag, F.: Biometric Security Systems: Speaker Recognition Technology, Dissertation Thesis, FIT BUT, Brno, 2004