Tamper-proof and privacy-protected fingerprint identification systems

Michael Schwaiger
secunet Security Networks AG
michael.schwaiger@secunet.com

Abstract: In this paper alternatives of tamper-proof and privacy-protected biometric identification systems are shown. One approach to secure such databases is to use cryptography. With its help it is possible to highly protect a system from any external attacker but an internal attacker still has direct access to all stored biometric data. This risk shall be avoided by using biometric encryption with another approach. In the following both approaches will be described and compared.

1 Introduction

Basically, it is possible to store biometric data on secure hardware (e.g. smartcards) which stays in possession of the owner. Nevertheless, there are lots of use cases where a central storage of biometric data in large databases is advantageous and preferred. Accordingly, interest in security of these databases arouses, too. Threats and possible points of attack [BCP+04] on biometric systems have to be taken seriously because misuse of biometric data can have serious and long-lasting implications. As opposed to passwords or cryptographic keys compromised biometric data cannot be changed. One main focus when collecting biometric data in large databases is data protection. According to national data protection laws in Europe biometric data need special protection as they allow other people to determine the identity of a person. Furthermore, they need suitable protection because it might be possible that sensitive information about the state of health of the corresponding person is extracted from the biometric feature.

This paper suggests two approaches to protect stored fingerprint data in identification systems. More detailed information regarding this topic can be found in [Sch09] and [MMJP03].

2 Conventional biometric solution

Biometrics itself does not offer any security mechanisms to protect captured and stored biometric data. One possibility is to use cryptography to protect the data. To ensure that only authenticated applications are communicating with the central database SSL/TLS
client authentication based on digital certificates is used. After the server’s authenticity is verified and the SSL/TLS handshake is finished successfully the communication to the database system is encrypted. While every user of the system has the possibility to authenticate himself to the system not every user shall be allowed to enrol, delete, or modify other users. This is the job of the biometric enrolment operator. He is in possession of a secure token holding a signature certificate. By signing the template and adding the digital signature to the template the integrity of the fingerprint template can be ensured. Furthermore, after transmitting the template via the encrypted SSL/TLS communication link to the central system the digital signature is verified. Thus, it is ensured that only biometric enrolment operators (which have a secure token with a valid certificate) can enrol, delete, and modify users. On identification, the digital signature, which was created during enrolment, of all possible candidates of the identification process is verified. Only if the signature is valid this user will be added to the candidate list. Returning the candidate list to the local application again is SSL/TLS encrypted. Attacking any software parts of the whole system might lead to serious implications. Therefore, all software is digitally signed by code signatures. Every single software part is only executed if the digital signature is valid and thus no modifications were done.

Another characteristic of the system is the one-way approach. It ensures that biometric data can only be accessed in one direction. Only biometric enrolment operators who are in possession of a token (and the stored certificate) are eligible to enrol, update, or delete users and their fingerprint features. It is not possible to get the stored biometric information from the database and return it to the application. This is achieved by disabling all functions from the according communication interface which can read data from the database. Thus, once biometric data is stored in the database it does not leave the central system anymore. Only a unique identifier of the identified candidate is returned to the application.

The afore described architecture has been realised with a biometric middleware approach – secunet biomiddle [BNS07]. secunet biomiddle implements among other things the standardised BioAPI 2.0 Framework [ISO06] which is a modular interface for biometric devices and algorithms. The client application communicates with the biomiddle server which invokes calls to Biometric Service Providers (BSP). They implement the actual behaviour of the attached device or algorithm.

By using all mentioned security features many points of attack on biometric identification systems can be obviated. The use of SSL/TLS ensures that an attacker cannot read and change the data while transmitting it to the central system and back to the client application. It ensures authenticated access to the system and prevents attackers from replaying identification decisions. Creating and storing the digital signature of the minutiae template guarantees the integrity of the biometric data in the database. Furthermore, using code signatures prevents manipulating all applications and obviates Trojan horse attacks on feature extraction and matching algorithms. Finally, the one-way approach does not allow external attackers to get stored biometric data from the database. Nevertheless, an internal attacker who already has access to the database can read and misuse the stored biometric data. Encrypting the stored data would be one solution but is not feasible when using an identification system. As a result, only by using the mentioned cryptographic
mechanisms it is not possible to secure the biometric data in such a way that internal attackers cannot misuse the data. For this reason, some approaches which consider this issue were developed. Biometric encryption is one way to solve this problem.

3 Approach using biometric encryption

Biometric encryption can also protect the stored biometric data from an internal attacker. When using biometric encryption a verification string is stored as a reference instead of the biometric template. As an advantage the original biometric data cannot be reconstructed from the verification string. This feature is achieved by a function which cannot be calculated in the other direction. Only if the user is presenting his biometric feature which is similar to the enrolled feature he can be authenticated. Additionally, some of the biometric encryption approaches also offer the possibility to extract a cryptographic key from the data.

One of these schemes is the BioKey approach [KMN09] which was designed and implemented by the German Federal Office for Information Security (BSI) and secunet Security Networks AG. It is a variant of the Fuzzy Vault scheme of Juels and Sudan [JS02]. The BioKey approach has some modifications compared to the original Fuzzy Vault scheme. Firstly, the entropy of one fingerprint is too low to design an approach which is resistant against known attacks [Mih07]. Thus, the system is designed to work with eight different fingerprints. To compensate rotations and translations of the fingerprint image instances an internal matching algorithm determines so called reliable minutiae within the given fingerprints during enrolment. A reliable minutia is a minutia which appears in a configurable amount of instances of the same fingerprint. As a result, minutiae which do not appear regularly in the captured fingerprint images (e.g. minutiae in edge regions of the image) will not be processed. This increases the authentication rate because minutiae which do not appear in every instance of the captured fingerprint image will be omitted during authentication. Secondly, there is a minimum limit of reliable minutiae per finger needed for a successful enrolment. Investigations showed that the matching rate increases drastically by using this requirement. Nevertheless, this results in a higher rejection rate during enrolment.

As an example, the BioKey approach was integrated to the conventional biometric solution. Now, an internal attacker who wants to misuse the stored verification biometric solution only succeeds with a certain probability. When choosing the right parameters of the algorithm this probability is less than $2^{-100}$ for each attempt. This is too low to start efficient attacks on the BioKey approach.

4 Summary and outlook

By using cryptography it is possible to achieve a high security level for biometric systems. As shown in the conventional approach, the integrity of the data and the authenticated
access to it as well as the encryption of the communication links between local and remote systems can be ensured. With the one-way approach it is not possible anymore to get the stored biometric data from the database. The approach using biometric encryption, however, adds more security to the system. The stored data itself is now protected against misuse, too. No more biometric raw data needs to be stored. Thus, the privacy of the biometric data is ensured as according to data protection laws. Nevertheless, there are some security concerns about this biometric encryption system as described in [Sch09] and [Mih07]. Also disadvantages in practicality of the BioKey approach need to be considered. Long template generation and identification time as well as a high failure to enrol rate are the major disadvantages. When designing and implementing a tamper-proof and privacy-protected fingerprint identification system these facts have to be taken into account. On the one hand more security and privacy for the stored data can be achieved; on the other hand the practicality is much lower than using the conventional approach. To establish biometric encryption for public usage, some more research has to be invested. The German Federal Office for Information Security (BSI) and secunet Security Networks AG are now optimising the developed approach regarding reliability and speed of the algorithm.

So far the BioKey approach is not fast enough and error-prone to be used as a privacy-protected identification solution. Nevertheless, the conventional approach offers high security for the stored biometric data as well. Many of these security features will also be necessary in the approach using biometric encryption, even if the BioKey algorithm will be optimised to be used in a real scenario.

References


