International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# X.1086

(11/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

## Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security

Recommendation ITU-T X.1086

ITU-T X-SERIES RECOMMENDATIONS

**DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY**

| | |
|---|---|
| PUBLIC DATA NETWORKS | X.1–X.199 |
| OPEN SYSTEMS INTERCONNECTION | X.200–X.299 |
| INTERWORKING BETWEEN NETWORKS | X.300–X.399 |
| MESSAGE HANDLING SYSTEMS | X.400–X.499 |
| DIRECTORY | X.500–X.599 |
| OSI NETWORKING AND SYSTEM ASPECTS | X.600–X.699 |
| OSI MANAGEMENT | X.700–X.799 |
| SECURITY | X.800–X.849 |
| OSI APPLICATIONS | X.850–X.899 |
| OPEN DISTRIBUTED PROCESSING | X.900–X.999 |
| INFORMATION AND NETWORK SECURITY | |
| General security aspects | X.1000–X.1029 |
| Network security | X.1030–X.1049 |
| Security management | X.1050–X.1069 |
| **Telebiometrics** | **X.1080–X.1099** |
| SECURE APPLICATIONS AND SERVICES | |
| Multicast security | X.1100–X.1109 |
| Home network security | X.1110–X.1119 |
| Mobile security | X.1120–X.1139 |
| Web security | X.1140–X.1149 |
| Security protocols | X.1150–X.1159 |
| Peer-to-peer security | X.1160–X.1169 |
| Networked ID security | X.1170–X.1179 |
| IPTV security | X.1180–X.1199 |
| CYBERSPACE SECURITY | |
| Cybersecurity | X.1200–X.1229 |
| Countering spam | X.1230–X.1249 |
| Identity management | X.1250–X.1279 |
| SECURE APPLICATIONS AND SERVICES | |
| Emergency communications | X.1300–X.1309 |
| Ubiquitous sensor network security | X.1310–X.1339 |

*For further details, please refer to the list of ITU-T Recommendations.*

# Recommendation ITU-T X.1086

## Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security


**Summary**

Recommendation ITU-T X.1086 defines the requirements of guidelines to provide security countermeasures for the telebiometrics protection procedures. This Recommendation defines the vulnerabilities and threats in operating telebiometric systems, and proposes a general guideline for security countermeasures, from both technical and managerial perspectives, in order to establish a safe environment for the use of telebiometric systems and to protect individual privacy.

This Recommendation describes countermeasures that allow the protection of biometric devices as related to their installation, removal, and delivery. Countermeasures are proposed for the protection of biometric systems as related to their operational procedures, as well as the roles and responsibilities of personnel involved in system design. It is expected that the proposed countermeasures will ensure the security and reliability of the flow of biometric information in a telecommunications environment.



**Source**

Recommendation ITU-T X.1086 was approved on 13 November 2008 by ITU-T Study Group 17 (2009-2012) under Recommendation ITU-T A.8 procedures.

**Keywords**

Telebiometrics authentication models, telebiometrics countermeasures, telebiometrics protection guideline, telebiometrics vulnerabilities.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

## CONTENTS

# Recommendation ITU-T X.1086

## Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security

### 1 Scope

This Recommendation proposes a general guideline for security countermeasures, from both technical and managerial perspectives, that would allow for the protection of biometric information against various threats, such as hijacking, modification and illegal access, from the point of its creation to its disposal in a telecommunications environment. Also this Recommendation proposes countermeasures for the protection of biometric systems as related to their operational procedures, as well as the roles and responsibilities of personnel involved in system design. From a technical point of view, this Recommendation proposes several countermeasures to ensure data integrity, mutual authentication, and confidentiality. From a managerial perspective, this Recommendation describes countermeasures that allow for the protection of biometric devices as related to their installation, removal, and delivery.

Not in the scope of this Recommendation is defining security requirements for biometric data and biometric security algorithms.

### 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1084] Recommendation ITU-T X.1084 (2008), *Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems*.

[ISO 19092] ISO 19092 (2008), *Financial services – Biometrics – Security framework*.

[ISO/IEC 19784-1] ISO/IEC 19784-1 (2006), *Information technology – Biometric application programming interface – Part 1: BioAPI specification*.

[ISO/IEC 19785-1] ISO/IEC 19785-1 (2006), *Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification*.

[ISO/IEC 19795-1] ISO/IEC 19795-1 (2006), *Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*.

[ISO/IEC 24761] ISO/IEC 24761 (2009), *Information technology – Security techniques – Authentication context for biometrics*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 biometric** [ISO/IEC 19785-1]: Pertaining to the field of biometrics.

NOTE – "biometric" should never be used as a noun.

**3.1.2 biometrics** [ISO/IEC 19785-1]: Automated recognition of individuals based on their behavior and characteristics.

**3.1.3 biometric data** [ISO/IEC 19785-1]: A biometric sample at any stage of processing, biometric reference, biometric feature, or biometric property.

**3.1.4 biometric product** [ISO/IEC 19785-1]: A software or hardware product or a combination of software and hardware, which is assigned a biometric product identifier by a CBEFF biometric organization called the biometric product owner of the biometric product.

**3.1.5 biometric sample** [ISO/IEC 19785-1]: Information obtained from a biometric device, either directly or after further processing.

**3.1.6 biometric system** [ISO 19092]: Automated system capable of capturing, extraction, matching and returning a decision (match/ non-match).

**3.1.7 biometric template** [ISO/IEC 19784-1]: A biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison.

**3.1.8 capture** [ISO/IEC 19785-1]: Acquisition of a biometric sample.

**3.1.9 enrolment** [ISO 19092]: Process of collecting biometric samples from a person and the subsequent generation and storage of biometric reference templates associated with that person.

NOTE – See also initial enrolment and re-enrolment.

**3.1.10 extraction** (feature extraction) [ISO/IEC 19785-1]: Process of converting raw biometric data into processed biometric for use in template comparison or reference template creation.

**3.1.11 identification** [ISO/IEC 19795-1]: Application in which a search of the enrolled database is performed, and a candidate list of 0, 1 or more identifiers is returned.

**3.1.12 registration** [ISO/IEC 19785-1]: The process in which a person shall prove their identity by presenting credentials to the biometric service provider before being allowed to enroll, and assigns an electronic identifier.

**3.1.13 score (scoring)** [ISO/IEC 19784-1]: Value indicating the degree of similarity or correlation between a biometric sample and a biometric reference template.

**3.1.14 template** [ISO/IEC 19785-1]: Data, which represents the biometric measurement of an individual, used by a biometric system to execute biometric matches.

**3.1.15 threshold** [ISO/IEC 19785-1]: Point above which the degree of similarity between two compared templates is sufficiently high to constitute a "match", and below which the degree of similarity between two compared templates is sufficiently low to constitute a "non-match".

NOTE – Thresholds can often be adjusted at an administrative level to decrease the false match rate or to decrease the false non-match rate.

**3.1.16 verification** [ISO/IEC 19795-1]: Biometric measures are compared to the enrolled template for the claimed identity, and an accept or reject decision regarding the identity claim is returned.

NOTE – The claimed identity might be in the form of a name, personal identification number (PIN), swipe card, or other unique identifier provided to the system.

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 biometric data auditor**: An independent third-party auditing organization, or a member thereof, given the task of protecting privacy.

**3.2.2 biometric data manager**: A person who collects, manages, or utilizes biometric data.

**3.2.3 biometric data provider**: An individual who provides his or her biometric data for the purposes of personal identification.

**3.2.4 biometric feature**: Concise representation of information extracted from a biometric sample by applying a mathematical transformation.

**3.2.5 biometric reference**: One or more stored biometric samples, biometric templates, or biometric models attributed to a subject and used for comparison.

**3.2.6 managerial protection countermeasures**: Protection countermeasures regarding biometric data protection policies, biometric data protection organizations, outsider security, information property classification, information protection education and training, and business continuity management.

NOTE – A biometric data provider must prepare all the necessary procedures required to access and manage users' biometric data, and enforce relevant employees such that they understand and comply with them. The biometric data provider must assign a manager with the authorization to access the biometric data, and provide the ID and password to the manager when processing users' biometric information using computers. In this case, the service provider, etc., should periodically renew the respective password/s.

**3.2.7 technical protection countermeasures**: Human security, physical security, system development security, code control, access control, operation management, electronic transaction security, security accident administration, control of reviewing, monitoring and auditing.

NOTE – Examples are prevention of computer viruses by installing and operating a vaccine program, security countermeasures used to safely transmit personal information over a network by use of encoded algorithms, installation and operation of an access control device such as an entry blocking system, and other technical measures required to secure safety.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASP Application Service Provider

FAR False Acceptance Rate

PKI Public Key Infrastructure

TTP Trusted Third Party

USB Universal Serial Bus

## 5 Conventions

None.

## 6 Components and vulnerabilities of a biometric system

The first step in taking technological protection measures for biometric data is to accurately identify the target and scope that required protection. Thereafter, establishing biometric data policies is the second step. In order to be able to reflect the technological protection measures on the protection policies, technical staff who are able to entirely understand and implement the proposed policies, and decision-makers who have the authorization to execute these policies, must participate in the process and work together effectively.

When a biometric system is installed or organized including the mechanism for the protection of the biometric data, an authorized data auditor supervises the auditing process, and the audit results will be open to public in cases where the biometric system is to be used in a more complicated and extended manner than initially designed.

One or more sub-processes are executed on a biometric processing unit. And one or more biometric processing units become biometric verification processes. A biometric processing unit is the abstract concept of a security domain, such as a sensor, a smart card, a storage device, or software running on a personal computer. Appendix II describes the functions of five sub-processes in a biometric verification process model.

Figure 1 describes a biometric system through a network, illustrating how a client acquires personal information and biometric data, thereafter transmitting them to a server installed at the aforementioned biometric step.

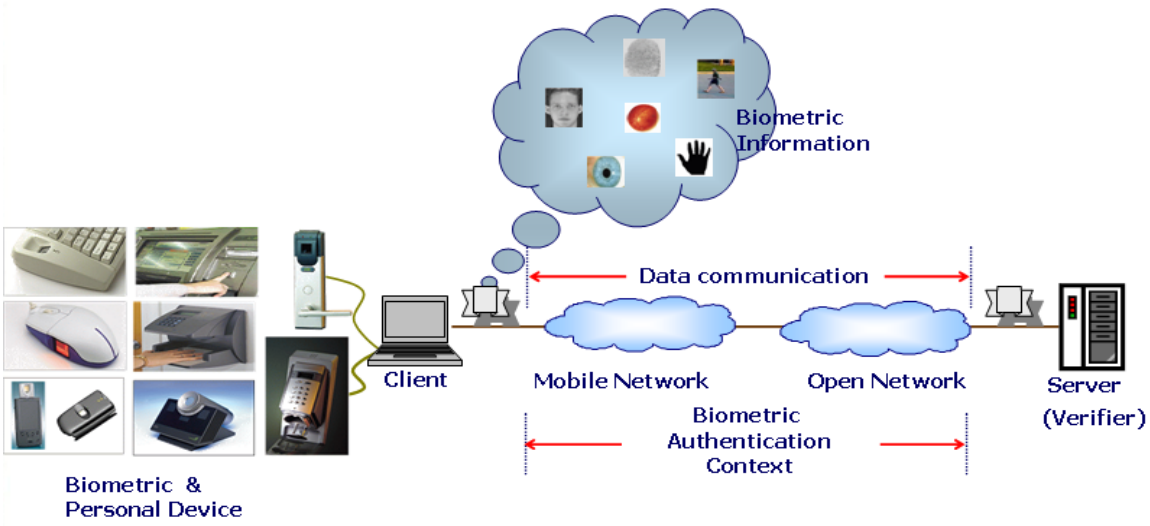


**Figure 1 – Telebiometric model**

Figure 2 illustrates the threats associated with the biometric component through a network in the biometric verification process model (see Appendix II). In this model, each component sends processed biometric data to the next component (see clause 5.1 of [ISO/IEC 24761]). Compared to a general biometric functional model, in a telebiometric functional model, processed biometric data can be transmitted between components through telecommunication media as denoted by *NW* in Figure 2. Figure 2 describes not only each component in the model but also the points where the transmission between the components is vulnerable to outside attacks. Examples of outside attacks are invasion when biometric data are delivered to the next step, or modification of processed biometric data.

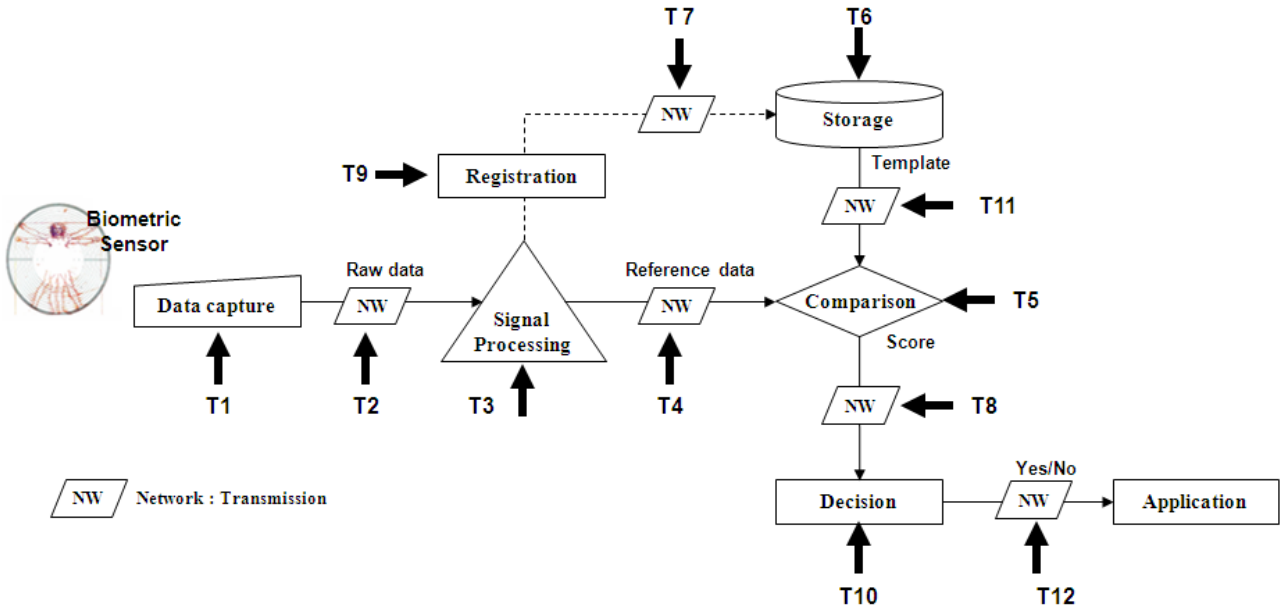


**Figure 2 – Vulnerabilities on the telebiometric functional model**

The threats associated with each component and transmission in the telebiometric functional model are listed and named as follows:

– T1: Threat on biometric input devices.

– T2: Threat on the process of transmitting biometric raw data to the signal processing component.

– T3: Threat on the signal processing component.

– T4: Threat on the process of transmitting the extracted biometric templates to the comparison component.

– T5: Threat on the comparison component.

– T6: Threat on the biometric storage component.

– T7: Threat on the process of transferring biometric templates from the registration component to the storage component.

– T8: Threat on the process of transmitting the matching score from the comparison component.

– T9: Threat on the registration component.

– T10: Threat on the decision component.

– T11: Threat on the process of transmitting the stored biometric template to the comparison component.

– T12: Threat on the process of transmitting the decision result to an application system.

Table 1 summarizes the relationships between the telebiometric components and the threats described above. For example, T1 can be a replay attack using artificial biometric samples in the data capturing process; and, T2 can be the hacking of biometric data being transmitted between the data capturing component and the signal processing component. Appendix III relates the vulnerabilities and the threats in the telebiometric system.

**Table 1 – Telebiometric system components versus threats**

| | Data Capture | Signal processing | Comparison/ Decision | Transmission | Storage | Registration |
|---|---|---|---|---|---|---|
| T1 | √ | | | | | |
| T2 | √ | √ | | √ | | |
| T3 | | √ | | | | |
| T4 | | √ | √ | √ | | |
| T5 | | | √ | | | |
| T6 | | | | | √ | |
| T7 | | | √ | √ | √ | |
| T8 | | | √ | √ | | |
| T9 | | | | | | √ |
| T10 | | | √ | | | |
| T11 | | | | √ | | |
| T12 | | | | √ | | |

The vulnerabilities and threats on telebiometric systems are identified by four groups: vendor, developer, user, and supervisor. The role of each group is as follows:

– Vendor: provides commercial telebiometric systems including input devices.

– Developer: develops a single or a set of telebiometric system components.

– User: uses the telebiometric system without the authority of supervision.

– Supervisor: supervises the users and manages the telebiometric system.

All the groups must be aware of not only the vulnerability of each component but also of the corresponding guidelines provided in this Recommendation. Appendix I provides as an example the checklist for usage of the telebiometric protection procedures.

## 7 Protection of biometric input devices

As illustrated in Figure 2, a telebiometric system is exposed to the threat of being hacked during the acquisition of biometric samples and their transmission to the signal processing component. The guidelines for protecting the acquisition process of biometric samples can be provided at three levels: device, transmission, and system. It is very important to acquire the first biometric samples from providers in a telebiometric system. The quality of the biometric data entered for the first time sometimes bears critical influence on the performance of the entire system treating biometric data. Thus, the protection of devices that acquire biometric data is significant.

In addition, since the acquired biometric data tend to be important original biometric data items, such as faces, fingerprints, irises, and voices, which should be treated as providers' private information, these data items are likely to be leaked outside and used in unauthorized places without appropriate permissions. Alternatively, incorrect data could be used through the use of unfair methods rather than as originally intended. Hence, such devices must be sufficiently protected.

### 7.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T1:

1) Manipulated biometric data, as opposed to the original biometric data of users, can be input through an unauthorized device.

2) Instead of the live-scanned biometric data, forged biometric data such as artificial fingerprints, facial photos, or recorded voice can be input.

3) Bad biometric data may be acquired as a result of device malfunction. Typical examples caused by device malfunction are low-contrast fingerprint images, defocused iris images, or yellowish face images.

4) Biometric raw data acquired from a capture device can be attacked and disclosed by illegal users before they are safely transmitted to the signal processing component.

### 7.2 Guidelines for protection

1) It is recommended that biometric capture devices be installed in safe and secure places, protected from physical attacks, such as disassembly or replacement. Further, biometric systems should provide a function to confirm whether the capture device is authorized or not. A possible way is to assign an encrypted unique device ID to each authorized device and check the ID at every data acquisition. The system administrator is responsible for creating, managing, and deleting the list of encrypted device IDs.

2) Biometric capture devices shall provide an appropriate method to check whether the acquired biometric sample is live-scanned or not. The method can be either software-based or hardware-based, or a combination of both. It should be noted that the liveness detection function in general increases the failure to acquire rate or the false rejection rate.

3) Biometric systems may be able to detect any device malfunction by implementing a function to test if the capture device is producing bad biometric raw data. A possible way of detecting bad biometric raw data is to measure the quality of biometric samples, which is under consideration by ISO.

4) In order to assure the integrity of the acquired biometric raw data, biometric capture devices may provide a function to encode the biometric raw data before transmitting them to the signal processing component. A possible encoding scheme is digital watermarking or encryption.

## 8 Protection of the process of transmitting biometric raw data

Biometric raw data acquired by a capture device must be safely transmitted to the signal processing component. Errors can occur in the course of transmission, or biometric data can be altered by external attacks. In particular, a protection measure may be prepared for transmission if the data are transferred via a telecommunications network or via wireless communication devices, such as a wireless LAN or Bluetooth. As biometric data correspond to private information, protection procedures should be developed against the problems of illegally leaking biometric data.

### 8.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T2:

1) Biometric raw data can be altered or intercepted by an attacker and used for illegal purposes when they are being sent to the signal processing component.

2) Biometric raw data can be damaged due to non-intentional transmission errors.

### 8.2 Guidelines for protection

1) A detecting function, such as an encoding technique using a hash function, can be applied to check the validity of transferred biometric data. In addition, a challenge-response protocol shall be established between the capture device and the signal processing component for detecting any replay attack. A replay attack in biometrics is the resubmission of illegally intercepted data in order to fool the biometric system. An example of protecting biometric systems from a replay attack is the adoption of a challenge-response

protocol in transmission, where messages hold 'freshness' property by inserting nonce, timestamp or sequential numbers into the messages. See Appendix IV.

2) If any outside infringement is practically impossible because the system and devices are wire-connected in physical proximity, the data transmission is adequately safe within this segment of the system. However, if there is a router or any other transmission system between the capture device and the signal processing component, these systems should provide a conventional error-checking scheme.

## 9 Protection of the signal processing component

The main function of the signal processing component in a telebiometric system is to extract biometric features from the transmitted biometric sample. This component needs to provide not only the functions of validating the liveness and quality of transmitted biometric samples but also the functions of protecting the processed biometric data.

### 9.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T3:

1) Even though the capture device has liveness detection function, live-scanned data can be intercepted during the transmission and replaced by forged biometric data. This forged data can be input to the signal processing component.

2) If the capture device does not provide the quality-checking function, biometric raw data of bad quality may be input to the signal processing component, which will deteriorate the performance of the overall biometric system.

3) A biometric template extracted by the signal processing component can be manipulated, lost, or disclosed using an illegal program, such as a computer virus or spy-ware program.

4) A non-encoded biometric template can be externally disclosed, then analysed, or fabricated, before being transmitted to either the storage or the comparison component.

5) The raw biometric sample can be stored and illegally used by an outside attacker if it is not destroyed immediately after the extraction of the biometric reference data.

### 9.2 Guidelines for protection

1) A signal processing component shall provide an appropriate method to check whether the transmitted biometric sample is live-scanned or not. The method will be software-based.

2) The quality of biometric raw data is a very important factor in biometric systems in the sense that it is directly related to the performance of the biometric systems. The quality-checking function will prevent a bad sample from being processed for feature extraction. The quality score for each biometric sample is given by an integer between 0 (bad) and 100 (excellent). Consult the work of ISO/IEC JTC1 SC37 for more information.

3) In order to avoid the invasion of computer viruses or spy-ware programs, the computer system containing the signal processing component is recommended to be protected by a firewall and to be scanned by a vaccine program in a regular basis.

4) Since the processed biometric data in the signal processing component will be transmitted to either storage in registration or to the comparison component in authentication, they are recommended to be encoded before transmission to protect them from illegal hacking.

5) After the extraction of the biometric reference data, the raw biometric sample should be deleted completely by the signal processing component or by the computer system containing the signal processing component.

## 10 Protection of the process of transmitting extracted biometric templates

In certain telebiometric applications, it is possible that the signal processing component and the comparison component are installed remotely, in different platforms, where the processed biometric data (or extracted biometric feature data) will be delivered from the signal processing component to the comparison component. In this case, even safely processed biometric data may be disclosed or altered during the transmission process.

### 10.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T4:

1) Processed biometric data can be altered or intercepted by an attacker and used for illegal purposes when they are being sent to the comparison component.
2) Processed biometric data can be damaged due to non-intentional transmission errors.

### 10.2 Guidelines for protection

1) The processed biometric data must be encoded for transmission, and their integrity should be verified using a one-way function such as a hash function or the public key infrastructure (PKI), which prevent any alteration of the data during transmission.
2) If any outside infringement is practically impossible because the signal processing and the comparison components are wire-connected in physical proximity, the data transmission is adequately safe within this segment of the system. However, if there is a router or other transmission system between them, these systems should provide a conventional error-checking scheme.

## 11 Protection of the biometric template comparison component

The processed biometric data comparison component is one of the most important components of the biometric system. The processed biometric data comparison component generally accepts two biometric reference data, and compares their similarities based on probability. Even though a biometric template is valid for comparison, different results can be produced if the comparison component improperly processes it.

### 11.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T5:

1) If a biometric template for the comparison request is altered, incorrect matching results may be produced.
2) If comparison is attempted using the processed biometric data with the identical biometric template at all times, comparison can be successful.

### 11.2 Guidelines for protection

1) The comparison component that generally receives two biometric templates and compares their similarities may employ a method to inspect the validity of the biometric templates. The biometric template itself must be encoded, and the encoded data should be tested to check whether the entered biometric templates have been altered, and if their validity is legitimate. This may be accomplished by using a one-way hash function. If the entered data are not valid, the similarity value produced as a result will have no meaning, and the similarity result value used without such a test will bear critical influence on the overall comparison system. Therefore, the input values must be tested.
2) Given their characteristics, the original data acquired from live biometric data may be slightly different in each case. This will always lead to slightly different biometric

templates. However, if the biometric templates were extracted from the original data obtained from the processed biometric data, rather than from the live biometric data, the entered original data remain identical at all times, and will always produce identical biometric templates, due to their mathematical characteristics. Therefore, the comparison segment should recognize unauthorized inputs from the outside, rather than the normal comparison inputs in cases where completely identical biometric templates were consecutively entered. In addition, a time stamp data may be inserted in the biometric templates to identify valid data.

## 12 Protection of the storage

In general, biometric reference data for registration should be safely stored in a single storage, for later usage in comparison, where the matching process is carried out by comparing the input reference data with the stored biometric template. Since the storage usually contains a set of biometric template data, it also needs to be securely protected from an outside attack. Furthermore, biometric template data should be modified, used, and stored to operate only for a specific purpose within the biometric system, following a valid procedure by an authorized biometric data manager. And, they must be destroyed completely by the biometric data manager using a technical method after the date of expiration of valid use, or when a user requests the disposal of his or her biometric data.

### 12.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T6:

1) All the user's personal information and the biometric template data are stored in a single storage, and can be exposed, destroyed, damaged, or stolen in one single illegal invasion.
2) The stored biometric data can be abused by an outside attacker if they are not encoded.
3) The biometric template is not purged after the date of expiration of valid use or after the corresponding user requests its destruction.

### 12.2 Guidelines for protection

1) The vendor should provide a technical mechanism, such as firewall or a VPN, for protection against any type of attack through the network. The storage should be also protected physically by keeping it in a secure place, and the access to the storage should be restricted only to the biometric data manager.

   NOTE – Rather than storing a large amount of biometric templates in a single storage, a portable storage device, such as a smartcard or a USB memory stick, for each individual may be recommended to store the individual biometric template. However, protection procedures for portable storage devices are out of scope of this Recommendation.
2) Regardless of the storage method or media, biometric templates should be stored encoded so that they will not be illegally used even if the storage is hacked.
3) Whenever the use of a biometric template has expired or a user demands the destruction of his or her biometric template, the biometric data manager should be able to delete the biometric template completely so that it cannot be restored and reused without any notice to the biometric provider.

## 13 Protection of the process of transmitting data from the registration to the storage

In certain telebiometric applications, where the signal processing component and the storage component have been installed remotely, in different platforms, the processed biometric template data will be delivered from the signal processing component to the storage component. In this case, even safely processed biometric data may be disclosed or altered during the transmission process.

### 13.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T7:

1) Biometric template data for registration can be altered or intercepted by an attacker, and used for illegal purposes, when they are being sent to the storage.

2) Biometric template data for registration can be damaged due to unintentional transmission errors.

### 13.2 Guidelines for protection

1) Biometric template data for registration must be encoded for transmission, and their integrity should be verified by a one-way function, such as a hash function or the public key infrastructure (PKI), which prohibits any alteration of the data during transmission.

2) If any outside infringement is practically impossible because the signal processing component and the storage are wire-connected in physical proximity, the data transmission is adequately safe within this segment of the system. However, if there is a router or other transmission system between them, these systems should provide a conventional error-checking scheme.

## 14 Protection of the process of transmitting results from the comparison component

In certain telebiometric applications where the comparison component and the decision component have been installed remotely, in different platforms, the output score from the comparison component will be transmitted to the decision component. In this case, the output score may be disclosed or altered during the transmission process.

### 14.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T8:

1) The output score from the comparison component can be intercepted and replaced by a malicious outsider during transmission to the decision component.

2) The output score from the comparison component can be damaged due to unintentional transmission errors.

### 14.2 Guidelines for protection

1) The output score from the comparison component must be encoded for decision, and their integrity should be verified by a one-way function such as a hash function or the public key infrastructure (PKI), which prohibits any alteration of the data during transmission.

2) If any outside infringement is practically impossible because the comparison component and the decision component are wire-connected in physical proximity, the data transmission is adequately safe within this segment of the system. However, if there is a router or other transmission system between them, these systems should provide a conventional error-checking scheme.

## 15 Protection of the registration

The registration is a procedure that transmits the reference data from the signal processing component to the storage. The recognition performance of the overall biometric system is heavily dependent on the quality of the registered biometric reference data. Hence, the registration procedure must be performed by a well-trained supervisor when the user's biometric data is registered in the central biometric database, in order to guarantee the quality of the registered data.

### 15.1 Vulnerability

The following can be considered a possible vulnerability that corresponds to threat T9:

1) Biometric reference data of poor or bad quality are entered, due to the lack of training of the supervisor of the registration process.

### 15.2 Guideline for protection

1) The vendor must provide a manual and a training session for registration, and the supervisor must complete the training session before the telebiometric service begins.

## 16 Protection of the biometric template decision component

In verification, the decision component decides either PASS or FAIL by comparing the matching score delivered from the comparison component against a preset threshold value. The threshold value is provided by the vendor and may vary depending on the level of security in verification. This threshold value must be protected from any unauthorized external access because the decision result will change if the threshold value is changed.

### 16.1 Vulnerability

The following is a possible vulnerability that corresponds to threat T10:

1) The threshold of the decision component can be changed by a malicious outsider.

### 16.2 Guideline for protection

1) The threshold of the decision component should be protected by a technical method such as auditing or accounting.

## 17 Protection of the process of transmitting the stored biometric templates

In most of the telebiometric applications with a central storage of biometric reference data, the storage component and the comparison component are installed remotely, in different platforms, where the processed biometric data (or extracted biometric feature data) will be transmitted from the storage component to the comparison component. In this case, even safely processed biometric template data may be disclosed or altered during the transmission process.

### 17.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T11:

1) Processed biometric data can be altered or intercepted by an attacker, and used for illegal purposes, when they are being sent to the comparison component
2) Biometric data can be damaged due to unintentional transmission errors.

### 17.2 Guidelines for protection

1) The processed biometric data must be encoded for transmission, and their integrity should be verified by a one-way function, such as a hash function or the public key infrastructure (PKI), which prohibits any alteration of the data during transmission.
2) If any outside infringement is practically impossible because the storage and the comparison component are wire-connected in physical proximity, the data transmission is adequately safe within this segment of the system. However, if there is a router or other transmission system between them, these systems should provide a conventional error-checking scheme.

## 18 Protection of the process of transmitting results from the decision component

In certain telebiometric applications where the decision component and the application are remotely installed in different platforms, the result from the decision component will be transmitted to the application. In this case, the decision result may be disclosed or altered during the transmission process.

### 18.1 Vulnerabilities

The following list enumerates the possible vulnerabilities that correspond to threat T12:

1) The result from the decision component can be intercepted and replaced by a malicious outsider during its transmission to the application.

2) The result from the decision component can be damaged due to unintentional transmission errors.

### 18.2 Guidelines for protection

1) The result of the decision component must be encoded, and its integrity should be verified by a one-way function, such as a hash function or the public key infrastructure (PKI), which prohibits any alteration of the data during transmission.

2) If any outside infringement is practically impossible because the decision component and the application are wire-connected in physical proximity, the data transmission is adequately safe within this segment of the system. However, if there is a router or other transmission system between them, these systems should provide a conventional error-checking scheme.

# Annex A

## Check list for usage of telebiometric system mechanism

(This annex forms an integral part of this Recommendation)

The following is based on [ITU-T X.1084]:

In telebiometrics, there are various biometric communication devices for the end-users. [ITU-T X.1084] specifies biometric authentication protocols and profiles for telebiometric systems. It defines nine telebiometrics authentication models for open network environments. Some of the nine models utilize a trusted third party (TTP) for authenticating user's public keys, registered biometric reference information, and the security evaluation result, based on the common criteria scheme for biometric devices. A TTP can also perform biometric comparison.

[ITU-T X.1084] takes into account the two perspectives below to divide models into nine classifications according to the locations of the storage of biometric templates and the biometric comparison component. Table A.1 expresses the vulnerabilities of the nine models defined in [ITU-T X.1084] using the threats defined in this Recommendation.

**Table A.1 – Expression for vulnerabilities of [ITU-T X.1084] versus threats identified in this Recommendation**

| Threats / Models of TSM | T1 | T2 | T3 | T4 | T5 | T6 | T7 | T8 | T9 | T10 | T11 | T12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Local | √ | | √ | | √ | √ | | | √ | √ | | √ |
| Download | √ | | √ | | √ | √ | √ | | √ | √ | √ | √ |
| Attached | √ | | √ | √ | √ | | | | √ | √ | √ | |
| Centre | √ | | √ | | √ | √ | | | √ | √ | | |
| Reference management on TTP for local | √ | | √ | | √ | | | | | √ | | √ |
| Reference management on TTP for Centre | √ | | √ | √ | √ | | | | | √ | | |
| Comparison outsourcing by client | √ | | | | | √ | | | √ | | | √ |
| Comparison outsourcing by server | √ | √ | | | | √ | √ | | √ | | | |
| Storage and Comparison outsourcing | √ | | | | | | | | | | | |

NOTE – This table assumes that in general, the models in [ITU-T X.1084] have the data capture component and the signal processing component in the same location. However, for the models with the outsourced comparison, the signal processing component is located in the same component as the comparison component. It is also assumed that the comparison and the decision components are combined in the same module. Furthermore, TTP guarantees the safety and security of biometric template data both stored and transmitted.

In Table A.1, the models defined in [ITU-T X.1084] include the transmission of information related to telebiometrics and are exposed to the vulnerabilities originated in any type of attack from outside. So, the system developer and the supervisor must provide the protection methods or procedures based on the guidelines for protection specified in this Recommendation.

# Appendix I

## Check list for the application of telebiometric protection procedures

(This appendix does not form an integral part of this Recommendation)

The following is based on [ITU-T X.1084]:

### I.1 Definition of check list

This Recommendation presents the guidelines for operating telebiometric systems safely. Systems must make sure they prevent attacks from outside when the telebiometric system is utilized. Checking items for security differs depending on the purpose of the utility. This Recommendation presents a checklist to help check aspects related to the model of the telebiometrics system mechanism.

The telebiometrics system mechanism specifies biometric authentication protocols and profiles for telecommunication systems. This Recommendation defines nine telebiometrics authentication models for the environment. And it defines the negotiation protocol for the policies and device environments using the models.

This Recommendation defines threats from both the technical and managerial perspectives in order to establish a safe environment for using the telebiometric systems. Items on the check list are organized based on the guidelines for protection defined in [ITU-T X.1084]. Therefore, the check list is organized into subjects to check both the viewpoints of the developer, the vendor and the supervisor.

Vendors, developers and supervisors can use the check list to safely organize the system. The check list must provide a complete check for all threats that originate in attacks coming from outside the telebiometric system. Vendors provide commercial telebiometric systems, including input devices. They will be able to concentrate on the reliability of the input device and on the precision of the algorithm. Therefore, vendors check the specific algorithm, input devices and storage devices. Developers provide a single or a set of telebiometric system components. Since they have the technical view of the system, they check the threats from the technical perspective. The user uses the telebiometric system without access to the supervisory functionality. The supervisor supervises the users and manages the telebiometric system. They check the threats in the managerial part of the system.

As an example of practical usage of this Recommendation, this appendix specifies a checklist for a local model of [ITU-T X.1084].

### I.2 Check list of items

The local model of [ITU-T X.1084] assumes that the server side cannot bear the biometric-processing load and the user terminal-side is given sufficient processing resources, as shown in Figure I.1 of the telebiometrics systems mechanism. This model can be used when the server side trusts the client-side processing.

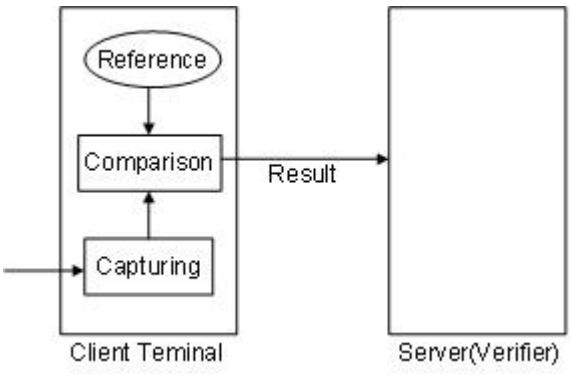


**Figure I.1 – Local model**

This is practical in access control systems that verify each process and transfer and save a log to the server. These attack-check items are organized according to the managerial perspective relative to the security of the telebiometric system components of the local model.

Within the check lists, there are further headings that group the countermeasure list used to protect against those attacks. All the individual items in the check list are described in terms of the guidelines for protection described in this Recommendation, and that should be taken into account in order to satisfy or minimize the threats represented by each item. A question format has been used, with the intention that a user checking the items will know that the appropriate measures have been taken if the answer to the question uses the words "must", "should" or "may".

### I.2.1 Protection items at the client

1) Vendor checklist
   - Did the vendor provide a technical mechanism such as a firewall or a VPN for protection against any type of attack through the network?
   - Is the storage protected physically by keeping it in a secure place?
   - Is the access to the storage restricted only to the biometric data manager?
   - Did the vendor provide a manual and a training session for registration, and had the supervisor completed the training session before the telebiometric service opened?

2) Supervisor checklist
   - Is a biometric capture device installed in a safe and secure place from physical attacks such as disassembly or replacement?
   - Is the system administrator responsible for creating, managing, and deleting the list of encrypted device IDs?
   - Is the biometric data manager able to delete the biometric template completely so that it cannot be restored and reused without any notice to the biometric provider?

3) Developer list
   - Does the biometric system provide a function to confirm whether the capture device is authorized or not?
   - Does the biometric system provide a possible way to assign an encrypted unique device ID to each authorized device and check the ID at every data acquisition?
   - Does the biometric capture device provide an appropriate method to check whether the acquired biometric sample is live-scanned or not?
   - Does the biometric system implement any function to detect any device malfunction producing bad biometric raw data?

– Does the biometric system provide any sample quality measure to detect bad biometric raw data?
– Does the biometric capture device provide a function to encode the biometric raw data before transmitting?
– Does the biometric system provide any detecting function to check the validity of transferred biometric data?
– Is a challenge-response protocol established between the capture device and the signal processing component for detecting any replay attack?
– Does the biometric system provide a conventional error-checking scheme if there is a router or other transmission system between the capture device and the signal processing component?
– Is the computer system containing the signal processing component protected by a firewall and scanned by a vaccine program on a regular basis?
– Are the biometric templates stored through encoding so that they cannot be illegally used even if the storage is hacked?
– Are the biometric templates for registration encoded for transmission, and their integrity verified by a one-way function?
– Is the output score from the comparison component encoded for decision, and their integrity verified by a one-way function?
– Is the threshold of the decision component protected by a technical method such as auditing or accounting?

### I.2.2 Protection items at server

1) Developer list

– Does the system provide any technique to monitor the biometric system's operations?
– Is the result of the decision component encoded, and its integrity verified by a one-way function such as a hash function or the public key infrastructure (PKI)?

# Appendix II

## Biometric verification process model

(This appendix does not form an integral part of this Recommendation)

The following is based on clause 5.1 of [ISO/IEC 24761]:

The specification of authentication context for biometrics, based on a biometric verification process, consists of the following five sub-processes:

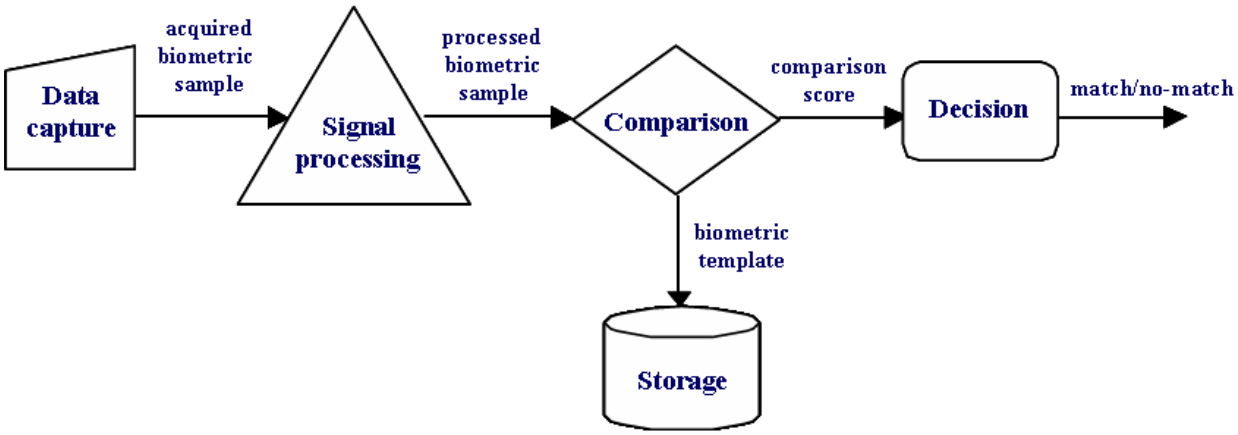


**Figure II.1 – Biometric verification process model**

a) Data capture

This sub-process captures the biometric information from the claimant and converts the information to the acquired biometric sample. The acquired biometric sample is then transmitted to the signal processing sub-process.

b) Signal processing

This sub-process receives the acquired biometric sample from the data capture sub-process, and transforms the acquired biometric sample into the processed biometric sample of the form required by the comparison sub-process. The processed biometric sample is then transmitted to the comparison sub-process.

c) Storage

This sub-process maintains the biometric template, of the form of the acquired biometric sample or of the processed biometric sample, for the claimant. The biometric template is transmitted to the signal processing sub-process or to the comparison sub-process, respectively. This sub-process achieves a management function of the data, with a storage component. The management function accomplishes the recording, modification, storage, and destruction functions.

d) Comparison

This sub-process receives the processed biometric sample generated by the signal processing sub-process, and the biometric template from the storage sub-process, or from the signal processing sub-process that processed the acquired biometric template originally maintained in storage. It then compares the two data, scoring the similarity of the data, referred to as the comparison score. The comparison score is then transmitted to the decision sub-process.

e) Decision

This sub-process receives the comparison score from the comparison sub-process, evaluates the score under certain rules, decides the validity of the claimant's identity, and outputs the resultant binary match/no-match result to the verifier.

# Appendix III

## Comparison between vulnerabilities and threats

(This appendix does not form an integral part of this Recommendation)

The following is based on studies currently active in ISO/IEC JTC1 SC27:

The security evaluation in the biometrics document describes vulnerabilities at the component, system, and application levels. The potential vulnerabilities are, therefore, specified at each level. Vulnerabilities are divided into N/A, basic, and extended types. The vendor should provide an evaluator of the requirements for the protection of vulnerabilities.

The requirements are that vendors and evaluators meet to ensure that any potential vulnerability cannot easily be exploited, and to provide explanations of attack processes in combination with other potential vulnerabilities. It is required that vendors and evaluators meet to ensure that the target systems are sufficiently resistant to attacks. The document does not describe problems that may occur during the transmission of information.

A security evaluation of the biometrics document includes an explanation of the potential vulnerabilities and related attack processes, as well as measures that vendors and evaluators should take to ensure that the potential vulnerability cannot easily be exploited. Explanations of attack processes in combination with other potential vulnerabilities and related requirements will be discussed at the meeting to ensure that the target system is appropriately resistant to attack.

This Recommendation defines the threats and vulnerabilities in operating a telebiometric system, and proposes a general guideline for security countermeasures from both technical and managerial perspectives, in order to establish a safe environment for using telebiometric systems, and to protect individual privacy.

Threats and potential vulnerabilities can be considered similar in terms of attack types. Attacks on drafts can be considered from different viewpoints. Threats occur in the process of telebiometrics and during the transmission of information. Attack occurrence points are defined from T1 to T12.

A potential vulnerability occurs at the processing stage of the biometric system, but the potential vulnerability does not address the vulnerability that occurs during the actual transmission of information.

Table III.1 presents a comparison of threats and vulnerabilities. During the biometrics process, threats and vulnerabilities may arise. For example, imitation could lead to impersonation in the use of a biometric product, and could also permit a backdoor to be created during enrolment. T1 indicates an attack at the data acquisition step. Therefore, imitation and T1 occur at the same stage. Unexpected high FAR, required to be explained in the security evaluation of the biometrics document, is similar to T8 in terms of being defined in this Recommendation. T2 and T4 of this Recommendation can be expressed by vulnerability of the telebiometrics data transmission. Therefore, the security evaluation of the biometrics document may need to address this transmission problem. If the subject of security against potential vulnerabilities during the transmission of data is added, the document should refer to the guidelines for these types of transmissions mentioned in this Recommendation.

For the assertion of protection, the vendor should provide the requirement documents to the evaluator, and the evaluator shall also then be required to perform a state-of-the-art examination so as to reveal the existence of any other vulnerabilities.

**Table III.1 – Comparison of vulnerabilities and threats**

| Threats / Vulnerabilities | T1 | T2 | T3 | T4 | T5 | T6 | T7 | T8 | T9 | T10 | T11 | T12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Imitation | √ | | | | | | | | | | | |
| Mimicry | √ | | | | | | | | | | | |
| Deficient liveness check | √ | | | | | | | | | | | |
| Impossibility of concealing biometric characteristics | √ | | | | | | | | | | | |
| Similarity | √ | | √ | | | | | | | √ | | |
| Special biometric characteristics | √ | | | | | √ | √ | | | | | |
| Synthesized biometric samples | | | √ | | √ | | | | | | | |
| Unexpected environment | | | | | √ | | | | | | | |
| Configuration | | | | | √ | | | | | √ | | |
| Enrolment process | | | | | | √ | √ | | √ | | | |
| Leakage and alteration of biometric data | √ | | | | √ | √ | √ | | | | | |
| Biometric data transmission | | √ | | √ | | | √ | | | | √ | |
| Data replacement | | | | | | | | √ | | | | √ |

# Appendix IV

## Replay attacks on telebiometrics

(This appendix does not form an integral part of this Recommendation)

### IV.1 Definition of a replay attack

A replay attack is performed by replaying a previously stored message in order to fool the system into accepting the message as legitimate. Establishing the authenticity (and therefore the origin), of the data, not only consists of verifying the presence of authentication data but also involves their validation. In fact, even without knowledge of the implemented authentication system, an attacker may potentially 'steal' biometric or biometric feature sets from the communication channel in order to later send them back again to the device in charge of matching them against a database, thus performing a so-called replay attack.

A breach of security in which information is stored without authorization and then retransmitted to trick the receiver into performing unauthorized operations, such as false identification, authentication, or a duplicate transaction is possible. For example, messages from an authorized user logging onto a network may be captured by an attacker to be resent (replayed), the next day. Even though messages may be encrypted, and the attacker may not know what the actual keys and passwords are, the retransmission of valid logon messages may be sufficient for gaining access to the network.

### IV.2 Countermeasures for replay attack

Like any large problem, identifying all possible vulnerabilities of a biometric system is a complex task when viewed holistically. The framework allows the analyst to partition the task, focusing on each potential threat point individually.

The general biometric framework will assume the context of threat point T2 in Figure 2, which is the communication channel between the sensor and the feature extractor. One obvious way to thwart such an attack is to encrypt the transmission. Although this may be effective, there are drawbacks, the relevance of which may vary from system to system.

Encryption may be computationally intensive, depending on the algorithm used. Depending on the processing requirements, this could potentially raise the cost and size of the sensors, an undesirable outcome. Furthermore, depending on the number of sensors, there may be a need to manage a large number of keys, which could potentially introduce other vulnerabilities. If the symmetric key used to encrypt the transmission of data from the sensor to the feature extractor does not change with each transmission, the encryption will have no effect in thwarting a replay attack of this nature. The attacker can simply replay the encrypted message, as if it were generated by the sensor.

Replay attacks are a real threat, and countering them may not be as straightforward as it appears. The sensor and feature extractor modules may reside in the same vicinity or at separate locations altogether. The communication channel may be a small network or it may be the Internet. If the modules are forced to communicate over the Internet, the number of devices that can snoop around transmitted packets is large, greatly increasing the threat level. Encryption may solve some security problems, but it is not foolproof. A better method is required to ensure that a message has originated at the sensor and is not a replay.

Attackers can sometimes capture old messages and replay them at later times. By replaying such legitimate, but stale, messages, attackers may either impersonate other parties to gain access to some secrets, or obtain some useful responses from the target party to perform other attacks. To prevent replay attacks, a message in the protocol should contain some 'freshness' property. If the freshness of a message is maintained, (e.g., nonce, sequence numbers, and timestamp of each

message), a receiving party can immediately detect replay attacks by examining the nonce, timestamp, and sequence numbers of the messages.

Three strategies for defeating replay attacks

a) Nonces: random numbers. (Typically a large random number, since this makes it more difficult for attackers to guess them.)

*Nonce*: A number chosen at random from a range of possible values.

i) Each generated nonce is valid only once.

In a challenge-response protocol, nonces are used as follows:

i) The verifier chooses a (new) random number and provides it to the claimant.

ii) The claimant performs an operation on it, expressing knowledge of a secret.

iii) This information is bound inseparable to the random number and returned to the verifier for examination.

iv) A timeout period is used to ensure 'freshness.'

b) Sequence numbers

i) Sequence numbers provide a sequential or monotonic counter on messages.

ii) If a message is replayed and the original message was received, the replay will have an old or excessively small sequence number, and be discarded.

iii) This method cannot detect a forced delay.

iv) It is difficult to maintain in the event of system failures.

c) Timestamps

i) The claimant sends a message with a timestamp.

ii) The verifier checks that it falls within an acceptance window of time.

iii) The last timestamp received is held, and identification requests with older timestamps are ignored.

iv) This method is appropriate only if clock synchronization is close enough for the acceptance window period.

### IV.2.1 Preventing simple replay attacks

After a protocol session of an initiator A and a responder B, an intruder I stores all the messages sent in the session. Then, I attempts to re-send the packets to B, impersonating A. If I can trick B into finishing its session in the belief it is talking to A, then the protocol is flawed and is discarded. Similarly, I can launch the simple replay attack to A as well. The purpose of such an attack is to check whether nonces, timestamps, or sequence numbers are used in a correct manner. The intruder does not try to encrypt or decrypt messages, nor alter the received messages, and hence, is very efficient.

### IV.2.2 Challenge-response

Much like an artificial biometric is used to fool the sensor, an artificial message can be used to fool the feature extractor, (replay attack). Challenge-response can be used to check the 'liveness' of a message. Challenge-response in the traditional sensor has been used in applications such as credit card inquiries over the phone to increase security. Typically, the customer is asked for their mother's maiden name to ensure that there is not an imposter on the other end of the line. The same principle can be applied to the communication protocol between the sensor and the feature extraction module.

### IV.2.3 Watermarking scheme for challenge-response

Establishing the authenticity, (and therefore, the origin), not only consists of verifying the presence of authentication data but also involves their validation. In fact, even without knowledge of the implemented authentication system, an attacker could potentially 'steal' biometric or biometric feature sets from the communication channel to later on send it back again to the device in charge of matching it against a database, thus performing a so-called replay-attack.

If the authentication only verifies the presence of the watermark, (e.g., extracting it, due to the key, and checking that the hidden message corresponds to the serial number of the known device), then the authentication system is not particularly strong. The only difference is that the stolen image would need to have been stolen from that same system, which is most likely what an attacker would do, even if he or she was not aware of that small requirement. This is why the watermarking scheme must embed some data that cannot be replayed. A common technique for this is to perform a so-called challenge-response. This challenge is different every time, and usually consists of embedding the current timestamp and checking, at the recovery stage, that the difference between the current time and the hidden timestamp is relevant, (i.e., that it does not exceed a threshold determined by the expected time it takes for image to 'travel' from the sensor to the recognition device). Therefore, if an attacker steals an image at time t and tries to replay it at time t+N, (N being above the defined threshold), the deception can be automatically detected and, possibly, recorded so as to warn the person in charge of the biometric system of a security threat. A remaining requirement for this challenge-response process is to ensure the detection of replay-attacks is that an attacker, aware of the watermarking technique, cannot reset the timestamp. This is why hidden data have to be locked by a key-based mechanism, so that only the intended recipient can gain access to them, thereby preventing an attacker from evading the protection by updating the timestamp to the current time of the attack.

### IV.2.4 One time password authentication (OTP)

S/KEY is a one-time password system developed for authentication in Unix-like operating systems. A user's real password is not directly transmitted across the network. Rather, the real password is combined with a short set of characters and a decrementing counter so as to form a single-use password. As the single-use password is only used once, passwords intercepted by a password sniffer or keyboard logger are not useful to an attacker. Because the short set of characters does not change until the counter reaches zero, it is possible to prepare a list of single-use passwords, to be carried and used in order by the user. Alternatively, the user may present the password, characters, and desired counter value to a local calculator in order to generate the appropriate one-time password that can then be transmitted over the network in clear. The latter form is more common, and practically amounts to challenge-response authentication.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Telephone transmission quality, telephone installations, local line networks |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| **Series X** | **Data networks, open system communications and security** |
| Series Y | Global information infrastructure, Internet protocol aspects and next-generation networks |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2010