Abstract:

We propose a design of a secure remote (internet) access system using biometric authentication. The secure access involves a communication scenario that employs a usual client-server network model, and includes biometric together with standard security mechanisms. The proposed access scenario enables to include the aliveness detection capability as well as the biometric replay attack prevention.

Keywords: Biometrics / remote access security

1 Introduction

Biometric authentication has recently matured enough to be applied in large scale applications. Biometric systems are still far from the ideal -- resistant to counterfeits, producing no authentication errors, immune to aging and diseases, bringing no social, religious, ethical, and other objections, and comfortable in use. A variety of biometric modalities have been investigated and applied to various access control scenarios, including fingerprints, iris, face, voice recognition, hand geometry, handwritten signatures, etc. At present, fingerprint methodology experiences its second youth, with iris-based systems features (see, e.g. [A1,A2] being the second runner.

We show how biometric methodology can be implemented into a secure remote access system. A prototype of such authentication device envisioned and built by NASK applied together with Biometrika optical fingerprint reader was tested with the use of an iris database.

2 Iris Verification for Remote Access

2.1 Remote Access Scenario

One of various authentication scenarios consists in granting the remote access to the network. The scenario we propose employs a common client-server network model, thus incorporating standard security mechanisms with biometric enhancements. The client terminal is designed as a biometric-based host, equipped with the capturing device and the processing unit that measures the biometric trait and calculates the features vector (biometric template). The client capabilities may be understood in a wider sense, thus enabling the client to be equipped with sensors related to more than one biometric modality. The proposed access scenario enables to include the aliveness detection capability and the biometric replay attack prevention. To insert the necessary elements into the communication flow, capture-dependent parameters will be retrieved by the client terminal prior to the biometric trait measurement.

A flexible solution of biometric remote authentication can be based on biometric enhanced EAP protocol included in RADIUS server. RADIUS can incorporate a number of authentication protocols, e.g., PAP, SPAP, CHAP, MS-CHAP, EAP, depending on the distribution. The EAP protocol (*Extensible Authentication Protocol*) – among those available – can be extended for additional authentication methodology. The proposed EAP packets - in case of the biometric remote authentication – are enriched with aliveness detection and biometric replay attack prevention. The

client terminal may require some volunteer-dependent parameters prior to the capturing process (e.g. position and size of the iris sectors for iris biometrics, fingerprint index or temperature data for fingerprint biometrics, etc.). These additional parameters may be used for biometric replay attack prevention, since the server may require different parts of the biometric traits in each transaction. Additionally, the same mechanism of using additional parameters may be useful in dynamic biometrics implementations (e.g., phrase-dependent voice verification), when the challenge-response mechanism is necessary. The above scenario is generic and may be applied to iris-based authentication, fingerprint systems, etc.

The client workstation can be established on Windows 2000 system and configured to enable for VPN connection to the remote network. Windows 2003 Server can be used as Network Access Server (NAS) for this purpose. The Radius biometric server can be installed on the same machine as NAS. The server may use MS SQL 2000 database for biometric templates storage. MS SQL database makes it easy to import biometric data from BioBase. MS SQL database interface must then be applied to Radius server. The enrolment station can be established on a remote Windows 2000 system. The next subsections depict the scenario elements.

2.2 Biometric Client Terminal

A biometric variant of EAP (BEAP developed by Telefonica I&D, may serve as an example) can be enhanced with a Biometric Module. We apply here the Iris Module developed by NASK. This enables to adapt Iris Recognition Device with Radius client and consequently to setup a remote access scenario based on iris pattern analysis. The Iris Module has the following proposed functionality:

- It controls Iris Imaging hardware and captures iris images with the desired quality and speed,
- It processes the acquired images, i.e., a) detects the inner and outer iris boundaries within the raw camera image, b) localizes the eyelids and specular reflections, c) extracts iris sectors based on the localized occlusions, d) transforms the iris sectors to the collection of stripes,
- It calculates the biometric template based on the representation of the iris image.

The Iris Module consists of the device library used for high-level hardware management and image capture, and the algorithms library, which deals with image processing, quality measurement, iris and occlusions detection, and features extraction. The entire Client Terminal structure is presented in Fig. 1.

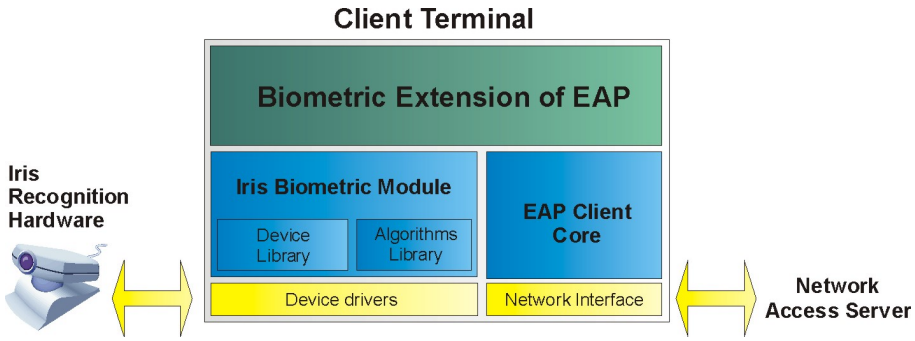

Figure 1. **The remote client terminal architecture**

.

2.3 Biometric Authentication Server

Radius server was configured to use MS-SQL BioBase server to store the templates. NASK BioBase Access Module add-on enables to make loading and storage of templates transparent to EAP Server Core. The server was also expanded by the iris matching algorithms, cf. Figure 2.

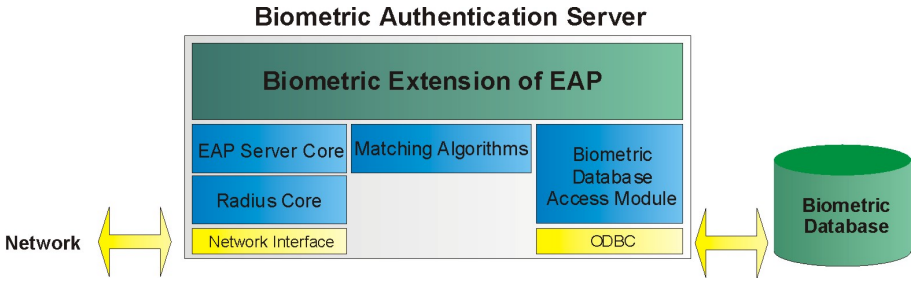

Figure 2. **Biometric Authentication Server based on Radius servers, with remote Biometric Database**

2.4 Enrolment Terminal

The Enrolment Terminal (cf. Fig. 3) uses the NASK Iris Module and BioBase Access Module. A separate application is developed that uses common elements of NASK biometrics modules, namely, the device library to control the hardware, and the algorithms library to process iris images and calculate iris features vectors.

The enrolment terminal captures a certain number of images of volunteer's eye. The raw image is processed to detect the inner and outer iris boundaries and eyelid occlusions. As an additional security mechanism, the occlusions may be used to determine volunteer-dependent free of occlusions (FOC) angular iris sectors, used for iris code construction in place of pre-set angles. The FOC angles can enhance the iris code. The enrolment hardware helps the user to position his or head correctly behind the camera.

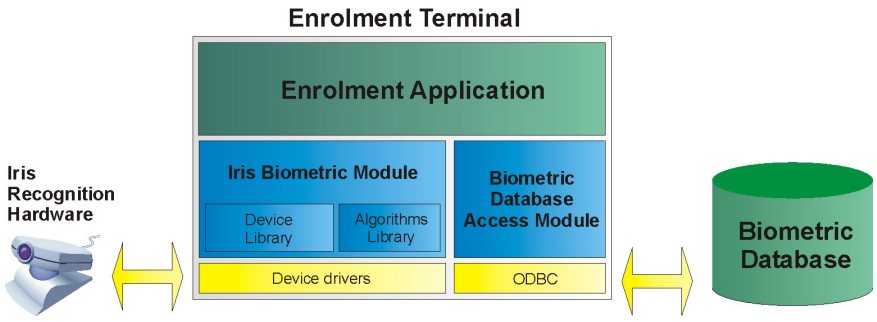

Figure 3. **Iris biometrics enrollment terminal, developed at NASK for use with the remote access scenario**

.

3 Conclusions

In the paper we described an application of a biometric verification to remote access security. The biometric used is based on iris coding with the optimal iris features selection. The proposed approach leads to zero false match and zero false non-match sample errors. This ideas were implemented in a secure remote access framework.

4 Acknowledgements

Most of the above results were obtained as a part of BioSec European integrated project IST-2002-001766.

References

[A1] John Daugman, “Biometric identification system based on iris analysis”, United States Patent 5.291.560, March 1, 1994

[A2] Adam Czajka, Andrzej Pacut, “Zak's transform for automatic identity verification”, Proceedings of the 4th International Conference on Recent Advances in Soft Computing RASC2002, 12-13 December 2002, Nottingham, United Kingdom, pp. 374-379, 2002

.