Доц. д-р РАДОСЛАВ МИЛЧЕВ
Докторант инж. МЕЛИНА НЕЙКОВА
ЛЕСОТЕХНИЧЕСКИ УНИВЕРСИТЕТ, СОФИЯ

ИЗСЛЕДВАНЕ НА ВЪЗМОЖНОСТИ ЗА РАЗРАБОТВАНЕ НА РАМКОВО ПРИЛОЖЕНИЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ, ПРЕДНАЗНАЧЕНО ЗА ВГРАЖДАНЕ В ЛОКАЛНИ ПРИЛОЖЕНИЯ ЗА Е-БИЗНЕС

DEVELOPMENT AND INVESTIGATION OF AN AUTHENTICATION FRAMEWORK APPLICATION FOR INCORPORATION INTO LOCAL E-BUSINESS APPLICATIONS

Assoc. Prof. Dr.RADOSLAV MILTCHEV,
Eng. MELINA NEYKOVA, PhD Student
UNIVERSITY OF FORESTRY, SOFIA

Abstract: The present paper aims to investigate the main approaches to the development of tools for the management and authentication of user access to local e-business applications. The authors have investigated major trends in the field of user recognition and selected methods which ensure the security at minimum cost. A framework application has been developed, which enables its incorporation into various business applications, depending on the requirements of the organization and accepted security policy.

Keywords: authentication, security, e-business.

Introduction

In recent years information has become one of the main assets of modern organizations and business entities. At present an essential part of the development and implementation of contemporary security policies is providing a controlled access to the information resources and assets for the various levels of the organizations. The implementation and use of modern methods for user authentication, as well as their combination with existing traditional methods allow the improvement of the conditions for information security in the organizations and business entities. This enables the implementation of different measures to ensure the confidentiality, integrity and accessibility of information resources and assets as part of the development of the overall concept of e-business of the various sized organizations.

The development of a global market of innovative devices and security systems is stimulated by the massive increase in global security threats and the damage and losses related to them. The need for a properly chosen effective security policy to be implemented into a variety of operations such as bank payments, financial transactions, e-commerce, e-banking, online and mobile transactions, cash withdrawal from ATMs and POS (banking terminals), etc. accelerated immensely in response to currently existing or possible future global threats. Along with this there is an increased striving for the performance of more accurate personality identification in the process of user authentication and authorization. Traditional methods of controlling the access to protected areas and resources are increasingly unreliable, with a high level of risk and increasingly resort to the implementation and deployment of biometric systems and devices. At the moment the development of the biometric market is increasingly beginning to dominate over the market for token-based technologies to control access, the market growth of biometric technology in 2012 reached 5.2 billion USD and the tendency is for it to reach 16.7 billion USD by 2019 [Biometrics: Market Shares, 2014].

The increment of the range of devices to access the electronic resources of organizations and business entities leads to an expansion of the user opportunities for electronic interaction anywhere and anytime. According to the survey [Miltchev, R., 2013], this leads to continual development and implementation of innovative solutions linked to the concept of e-business in various entities based on the use of embedded computer systems of various types. At the same time we observe the maximization of the striving towards miniaturization of devices, increasing their functionality and the need of constant diversification of developed applications. According to the report of the National Research Council, the network systems of embedded computers radically change the way of interaction between society and the surrounding world [NRC, 2001]. Simultaneously the reduction in the cost of embedded systems and sensors, and their mass production are a prerequisite for the continuous generation to the market of portable, mobile devices such as tablets, smart phones, and increasingly available biometric devices and technologies.

In the present paper, the authors aim to explore the leading trends in the deployment and implementation of appropriate and innovative devices and the methods for user authentication for the different purposes of various sized organizations. Based on the conducted studies, analysis and an overview of Bulgarian and foreign authors, an appropriate range of software tools for authentication management have been developed in accordance with the existing policies on information security and technical support. The main goal is to achieve high levels of security and ensure access to e-business resources and information assets, which are part of used local e-business applications. In the study an attempt has been made to identify the existing security gaps and disadvantages related to the practices applied in the provision of access to the information assets in the organizations. The main advantage of the presented methods in the developed framework application is the ability to be applied by organizations and business entities to ensure user authentication and access, including through several levels of authentication, at minimum cost.

Basic approaches and stages of user authentication.

Identification is the process of establishing the identity of an object (person or computer device), based on its unique identifying traits and characteristics. The process of authentication and verification of identity is associated with the proof of identity of the person according to the selected security policy. According to the results the e-business applications, computer system or online service can reject or accept requests for access. The main approaches for the implementation of authentication, as indicated by Bolle, R. [Bolle, R., 2004], can be separated into three groups:

- based on the possession of physical objects *(token - based approaches)* such as keys, identity documents (passports), smart cards, credit cards, tokens;
- based on knowledge-information *(knowledge – based approaches)* that must be kept secret - such as passwords, personal identification number (PIN), secret phrases, answers to secret questions;
- based on biometric identifiers - physiological (e.g. hands, fingers, face, eyes, DNA) or behavioral (e.g. signature, voice, gait) characteristics of the individual.

The identification of users through unique identifiers such as a username and password is a classical way of authentication. The main problems with this method are the ways of storing consumers' passwords, the security of the passwords and their storage, and ensuring access to the e-business applications. The study of the existing practices in this area shows a strong reluctance on the part of the end users to maintain and to meet the requirements of the security policy of the organization. Previous research has shown that this type of authentication does not fully guarantee the identity of the user, because the received authorization from the system is a result of the validation of an existing unique name and an identification string. This requires the implementation of subsequent levels of physical and logical access control, for example through a smart card or user's biometric data.

Identification based on a smart card not only confirms the identity of the party that performs the authentication, but also ensures the integrity and identity of the sent electronic document or made transactions. The smart card itself represents an active device for authentication with a high level of security providing information security by storing the private key and a corresponding user certificate (public key). The main advantage of smart cards is that the information stored on them cannot be copied, and the probability of the pair of keys (public and private) to be stolen is minimal. To be able to use the information on the smart card and to allow performance of a particular cryptographic operation, the user must first enter the appropriate PIN. The implementation of the process of authentication is accomplished by the interaction of the smart card with the public key infrastructure (PKI).

Biometric identification, according to Jain, A. [Jain, A., 1999] relates to the identification of an individual based on his/her distinguishing physiological or behavioral characteristics. A biometric system is essentially a recognition system of the biometric templates that are extracted on the basis of original patterns. They are matched with the corresponding records in a previously developed database. The initial input and processing of biometric information through a sensor and its transformation to a suitable form are performed by appropriate powerful algorithms and specialized software. The basic requirements for the biometric identifiers discussed in the same source are universality, uniqueness, permanence, measurability, performance, circumvention and acceptability from consumers. They characterize the effectiveness of the biometric trait to be used in biometric research and in a biometric authentication system.

There are a multitude of biometric methods and technologies which are applicable in the process of user identification and authentication. The more popular of these can perform identification on the base of biometric characteristics that are measurable and constant over time. These can include finger- and palm-print, iris and retina (eye-based methods), face, hand/finger, ear geometry, hand and finger veins, as well as DNA samples. Each of the represented biometric characteristics has its specific advantages and disadvantages, but none of the abovementioned identifiers meet all the performance requirements. What also needs to be taken into account is the existence of a specific case such as congenital or acquired disability or occupational burden on persons, as in certain circumstances it could hinder the process of authentication. Finally, it is necessary to make compromises when choosing a biometric technology, depending on its application.

One of the most popular biometric technologies at that time with a share of 43.6 % is the identification of users based on images of their fingerprints [Jung M., 2005]. Important deficiencies in this method are related to possible disruption of authentication as a result of dirt, moisture, fingerprint fogging in the process of aging or wear and tear associated with professional practice, and injuries of the individual.

Finger vein recognition represents another attractive biometric authentication technology, which can be implemented in various sized organizations and business entities. The veins are a network of blood vessels in the hypodermic areas of the human body, which are unique for each individual. Unlike fingerprint or iris scans, they do not change over time and they are immutable under influences such as aging, moisture, dirt and wear. Technology for contactless authentication through finger vein recognition is suitable for implementation in environments with high hygiene requirements. It is suitable for users who do not want to come in contact with equipment for public use. According to Hitachi ICT Solutions [Security Solutions, 2014], the biometric characteristics of finger veins offer the highest level of security and make forgery difficult. In the same source has made a qualitative comparison between finger vein recognition and the other popular biometric methods (iris patterns, palm vein patterns, fingerprint patterns, facial contours and features), the result of which confirmed that the finger vein patterns have the convenience of fingerprints and the accuracy is comparable to iris patterns. In this context, the technology for finger vein recognition has the advantages of fingerprint devices, such as low cost, high processing speed and compact size, while overcoming some of their disadvantages.

DEVELOPMENT OF AN AUTHENTICATION FRAMEWORK FOR LOCAL E-BUSINESS APPLICATIONS.

Based on the conducted studies it can be concluded that the best practices for increasing security and access control demonstrate the need to use two or more ways of identification in the process of authentication. In the present study a multilevel user authentication is proposed, which is achieved as a result of the combination of different methods of authentication, depending on the goals adopted in the security policy of organizations or business entities.

During the first stage of user authentication a conventional recognition technique is applied through a username and password, which are suitably encrypted in order to increase the level of security. The second level of authentication is performed using a smart card and a smart card reader (ACR 38, illustrated in Fig. 1). The development is consistent with the popular device models that have been applied to other activities in the organizations. In order to provide a higher level of authentication of a user's identity biometric authentication is applied, which is implemented by fingerprint and finger vein scanning devices. The proposed biometric identification is a more reliable method for authentication of the individual than those presented in the first two stages, because conducted studies in the organization have shown that it is possible to provide the passwords, as well as smart cards to third parties, especially in the event of an emergency, most often related to the absence of the employees and the need for their tasks to be performed. The used fingerprint or finger vein patterns are a unique personality trait that cannot be replaced.

Figura.1. Smart card reader (ACR 38)

Two types of biometric technologies for the authentication of individuals have been integrated and applied into the developed application for authentication management: a device to scan the fingerprint patterns and a device for contactless finger vein recognition (Hitachi H-1 Reader, Fig.2).

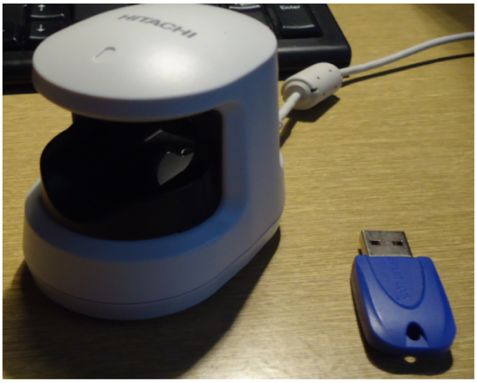


Figura.2. A smart card and Hitachi H-1 Reader for multilevel authentication.

The process of designing and developing the application for multilevel authentication took into account the existing hardware and software that were accepted and used by the organization. For that reason, the application was developed by the resources of Microsoft Visual Studio, in the form of .NET application designed to work in a Windows operating system environment. Also, there are applied techniques which allow the use and the functioning of the framework application either independently or as a component for subsequent installation into computer applications developed for the e-business of the organization. For the purposes of authentication and in order to improve the application security, the framework application communicates with a separate encrypted database, which supports only the necessary information for authentication.In the developed framework application data structures are supported. They give access to the stored user information, which is implemented through four selected authentication methods: traditional access, based on the use of a username and password, access through a smart card, fingerprint and finger vein recognition (Fig. 3). The application has pledged methods that allow encryption according to AES, 3DES and RSA procedures. Procedures for both adding new users and verifying the rights of existing users in the system have been developed.

The appearance of the graphical user interface for testing the ability of the framework application is shown in Fig. 4. The buttons which allow testing different mechanisms for user authentication are located at the top of the window. The opportunities for adjusting the security requirements in the process of user authentication are located at the bottom of the window. Different policies can be tested: from traditional methods which are based on the use of a username and password, through the use of smart cards, to the application of the biometric methods for identification.

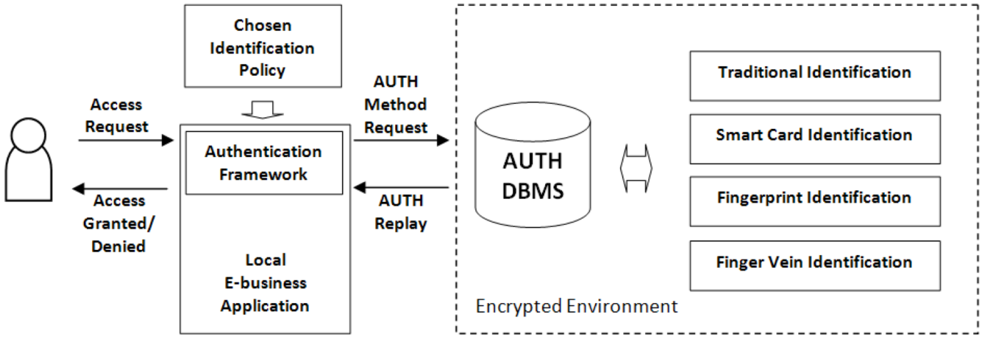
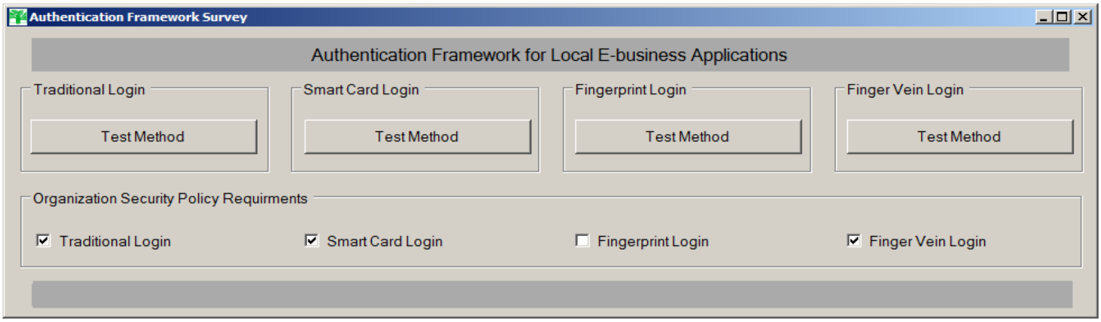

Chosen Identification Policy
Access Request
Access Granted/ Denied
Authentication Framework
Local E-business Application
AUTH Method Request
AUTH Replay
AUTH DBMS
Traditional Identification
Smart Card Identification
Fingerprint Identification
Finger Vein Identification
Encrypted Environment

Fig.3. Structure of the developed and tested environment.

The effectiveness of the developed framework application was tested using the graphical user interface which is presented in Fig. 4. The results returned by the developed framework application were examined depending on the adopted security policy on multilevel user authentication. The results when a user successfully passes through all required levels of authentication are shown on the left of Fig. 5, and the results when access is denied for a user who used the user access provided by a colleague, including a username, password, PIN code and digital certificate, but he/she did not successfully pass the process of biometric identification are shown on the right.



Authentication Framework for Local E-business Applications

Traditional Login

Smart Card Login

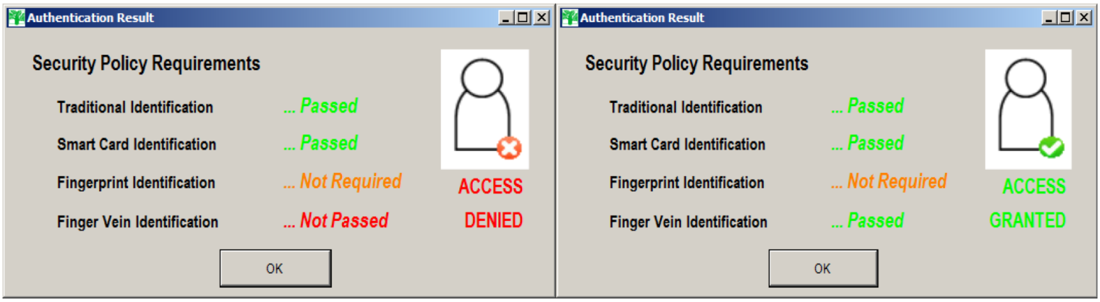
Fingerprint Login

Finger Vein Login

Organization Security Policy Requirments

☑ Traditional Login ☑ Smart Card Login □ Fingerprint Login ☑ Finger Vein Login

Figura.4. Authentication Framework Applicati on interface.



Security Policy Requirements

Traditional Identification ... Passed

Smart Card Identification ... Passed

Fingerprint Identification ... Not Required

Finger Vein Identification ... Not Passed

ACCESS DENIED

Security Policy Requirements

Traditional Identification ... Passed

Smart Card Identification ... Passed

Fingerprint Identification ... Not Required

Finger Vein Identification ... Passed

ACCESS GRANTED

Fig.5. Result from the multilevel user authentication process.

With the experience gained in the process of developing a presented framework application, it can be easily modified in order to be used not only for local e-business applications, but for a variety of online applications available on different types of networks. In this case, it will be necessary to use methods and instruments to secure the traffic between the server where the electronic business applications are and the customers who make requests to its information resources through the public networks. The proposed framework application can be easily extended to meet specific environmental requirements of other operating systems, because there are available drivers and libraries provided by the developers of the hardware devices.

Conclusion

The contemporary computer and information systems that are connected to the Internet, Extranet or Intranet are increasingly looking for approaches for the implementation and provision of various security measures, including by performing multifactor authentication. Biometric technology can be defined as a natural extension in the development of innovative technologies for identification and authentication. At present, increasing attention is being paid to the implementation of biometric systems and applications for precise user identification both in the activities of organizations and business entities and in the overall development of their e-business concept. Based on the conducted studies and specific requirements of the organization that wants to improve the possibilities for authentication of their users, a framework application for managing and testing the process of authentication of individuals has been developed. The developed application is consistent with the requirements of the organization to provide opportunities for operation and reconciliation with existing systems and resources. During the development process, existing gaps and deficiencies have been identified in the practices applied by the organization to provide user access, including user names and passwords, digital signature carriers and PIN codes. The developed computer application was designed to remove and minimize these practices and their impact on the security of the managed assets by providing user access through multilevel authentication. The main advantage of the presented methods in the developed framework application is the ability to be applied by the organizations and business entities to ensure user authentication and access, including through several levels of authentication, at minimum cost of investment.

Acknowledgment This document was supported by the grant No BG051PO001-3.3.06-0056, financed by the Human Resources Development Operational Program (2007 – 2013) and co-financed jointly by the European Social Fund of the European Union and the Bulgarian Ministry of Education and Science.

REFERENCES

[1] Bolle, R., Connell, J., Pankanti, S., Ratha, N., Senior, A. (2004). *Guide to biometrics*. Springer.

[2] Jain, A.K., Bolle, R. & Pankanti, S. (Eds.). (1999). *Biometrics: Personal Identification in Networked Society*. Kluwer, New York.

[3] Jung M. Biometric Market and Industry Report (2005). *International Biometric Group*. Retrieved Sep. 15, 2014, from http://www.wcoomd.org/fr/events/event-history/2005/~/~/media/ 96665922235 E422E8 B7BA8FA9CD8CA0E.ashx.

[4] Miltchev, R. & Neykova, M. (2013). Major trends in the development and the use of embedded computer control systems. *Journal of Management and Sustainable Development,* (in print, in Bulgarian).

[5] National Research Council. (2001). *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers*. Washington, DC: The National Academies Press.

[6] Biometrics: Market Shares, Strategies, and Forecasts, Worldwide (2013 to 2019). Available from http://www.reportsnreports.com/reports/270180-biometrics-market-shares-strategies-andforecasts-worldwide-2013-to-2019.html. [Accessed September 15, 2014].

[7] Security Solutions: Hitachi ICT Solutions. *Finger Vein Biometric Systems*. Retrieved Sep. 15, 2014, from http://www.hitachi.com.sg/ict-solutions/solutions/fingerVein.html