Chapter 9

Multi–Factor Authentication and Dynamic Biometric Signatures

Vladimír Smejkal
Brno University of Technology, Czech Republic

ABSTRACT

Multi-factor authentication is a necessity for the adequate security of information systems. Dynamic biometric methods, which are increasingly being used, are based on the use of behavioral characteristics that are unique to each person. The authors of this paper will discuss the issue of the uniqueness of Dynamic Biometric Signatures (DBS) in relation to the characteristic behavior of individuals under different conditions and situations and hence the validity of the parameters required within user identification and authentication models in the world of electronics. The conclusions are based, amongst other things, on the results of experiments using dynamic biometric signatures. Attention has also been paid to the legal aspects of the DBS, including Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

INTRODUCTION

Contemporary trends in security components and processes in the ICT environment involve a wide area of tasks with regard to their implementation. This article provides a description of one main requirement for information system security; aspects of electronic authentication and authorization. It is necessary to be aware of the impossibility of realizing correct information security, not only due to the inclusion of integrity and confidentiality, but also due to the sophisticated authentication process which constitutes a very important part of the information or asset security solution. It is possible to commence the authorization process in order to allow an identified person to use the ICT services on the basis of the successful and trustworthy authentication of subjects.

The applied authentication procedures should react to and fulfil the variability requirements based on the possible differences in the types of used technology and from point of view of the user. In addition to the aforementioned topics, the design solution also has to allow the authorized user to communicate and perform the tasks associated with the conclusion of regular contracts or the realization of innocent transactions. Finally, the important factor related to other topics is the relationship and compliance of the new authentication methods with the legal rules.

DOI: 10.4018/978-1-5225-0703-1.ch009
TRENDS IN ELECTRONIC AUTHENTICATION

In the case of user authentication, information technology secures the same conditions in comparison with transactions and services provided in written form, i.e. the exchange of data among authorized users, including the required user’s nonrepudiation. In case of personal contact, i.e. if both people can see each other and are in direct contact, the principle of identification and authentication is established on the basis of the real intercommunication between them. This decision-making procedure seems very trustworthy, nevertheless there are potential risks that arise from the concept of the entire process.

During direct contact in the case of authentication based on a different attribute than personal knowledge, the security of the authentication process is directly proportional to the maturity of the applied procedure. While the evaluation of the signatures written on credit cards is considered to be an example of a minimum guarantee, the authentication risks based on the verification of personal documents depend on the quality of the work undertaken by the inspecting body and the possibility of the forgery of these documents.

In the case of remote communication or human/machine (or machine/machine) communication, the situation looks more difficult because of the high probability of identity fraud. In the case of voice communication (phone banking), the level of risk differs significantly within a large scale; from high risks in the case of identification based on the repetition of passwords or their weaknesses (e.g. the limited number of digits obtained from the personal number) to insignificant ones (use of a one-time pad or authentication calculators). When technological tools are used, the level of risk is usually medium or high, where the risk is a function of either the used methods or the tool parameters and the conditions of their use, the behavior of the users etc.

In each of the situations described above, the following necessary conditions should be adhered to in each process of remote authentication and authorization:

- The design and the solution should be neutral from the point of view of the technology,
- The authentication policy should be separate from the security policies related to the area of data protection,
- The technological solution should respect modularity in order to allow the effective improvement of the security models,
- The proposed solution should respect the requirements of the present legal regulations and adhere to the conditions of the internal instructions,
- The proposed solution should be user friendly and cost-effective.

More advanced authentication methods refer to the use of two parameters. These parameters can be linked with:

- **Ownership:** Something that we have, such as a token, a smart card or an authentication calculator.
- **Knowledge:** Something that we know, such a password.
- **Features:** Something that we are, such biometric information.

A successful solution depends on (to some extent) a sophisticated process for the utilization of these authentication parameters. The present orientation is leading towards strong or multi-parameter authentication.