Chapter 81
Applying Continuous Authentication to Protect Electronic Transactions

Silas Leite Albuquerque
University of Brasilia, Brazil

Paulo Roberto de Lira Gondim
University of Brasilia, Brazil

ABSTRACT

Perform a commercial transaction using the Internet or a mobile device (e.g., smart-phone) is quite common in today's world. Every moment increases the number of companies that offer their products and services through this virtual world. Thus, the security issues become evident and shown to be essentials for the parties involved in an electronic transaction feel safe when performing their actions. A fundamental security aspect to build trust among the parties is that they must be permanently authenticated to one another during the entire transaction. Then, conventional methods of authentication (username and password, digital certificates, etc.) do not provide the desired security level. At this moment, come into play continuous authentication processes that aim to maintain the parties' authenticity throughout the transactions period (ideally using methods transparent to users). Considering these requirements, one can realizes that some biometric recognition methods are well suited for providing this type of authentication.

In this sense, this chapter explores some possibilities for continuous authentication use to increase electronic transactions security and addresses issues such: Trust in electronic communications systems, conventional authentication models, continuous authentication concepts and biometrics.

DOI: 10.4018/978-1-4666-2919-6.ch081

INTRODUCTION

In a globalized world which is connected through the many communication networks in existence, the ability to do online commercial transactions is essential. More importantly, people who are in constant movement -between home, office, meetings and in traffic, wish to be able to perform these commercial transactions wherever they are and whenever they want. Therefore, electronic commerce and its variants (m-commerce, t-commerce, u-commerce) are more than mere possibilities; they are imposed by our daily needs. However, in order for this commerce to be considered reliable, it is necessary that some information security services be provided through these platforms. It is assumed that one potential executor of an electronic transaction demands, in terms of security, that the data used is accessed only by authorized people or entities (confidentiality), and that such data cannot be modified by intruders (integrity) and that the parties of the transaction recognize and trust the identity of their peers (authenticity). Only then a transaction can be considered reliable.

Specifically concerning authenticity, a very usual way to guarantee this is to use authentication processes of the involved parties. There are several authentication protocols globally recognized and created by several authors and standardized by various regulatory bodies, but almost all of such are concerned only with parties' authentication at a time immediately prior to the transaction completion. This is justifiable for situations in which the transaction has a small duration, but in cases of long sessions execution, where time interval is considerably larger, vulnerability to intruder attacks increase and it is no longer possible to guarantee that an earlier authentication (at the beginning of a transaction) is sufficient to ensure the authenticity of the parties. This lack of long-term guarantee can be found in the analysis of mechanisms used to protect such transactions, because they often use time intervals as limiting factors for the sessions validity, and once these ranges are exceeded, new authentication processes (usually explicit) should be triggered.

At this moment one must think of continuous authentication, which basically consists of constant repetition, throughout the transaction execution, regardless of duration, of procedures to verify the participants' identity.

After deeper analysis, other requirements present themselves alongside that of authentication continuity: transparency to users, so that the action of those users in the main process (buying, selling, banking, etc.) is not interrupted by an explicit re-authentication process, and the use of multiple and complementary authentication mechanisms (multimodal authentication) which enables greater process flexibility and allows the use of mobile equipment of reduced computational possibilities.

Biometric techniques have proven to be interesting alternatives for meeting the mentioned requirements. Whether in physiological or in behavioral aspects, biometrics constitutes more than identifying peers based on "something they have" or "something they know", it is identifying users (rather than pieces of equipment) by "what they are", i.e., based on something that is inherent to them and that uniquely identifies them.

All of these issues have been discussed in the academic community and various papers have been individually published which explore the many aspects addressed herein. It is therefore with the main objective of being a joint bibliographic reference that contemplates these several aspects that this chapter aims to:

Describe and analyze authentication processes that can be used continuously and transparently to increase the authenticity guarantee of the parties involved in an electronic transaction.

Furthermore, we intend to:

- Analyze trust aspects related to creating environments in which electronic transactions may happen and where application of continuous authentication appears somewhat promising;