Behavioral Based Technologies for Enhancement of Login/Password Systems

Sérgio Tenreiro de Magalhães
Portuguese Catholic University, Portugal

Vítor J. Sá
Portuguese Catholic University, Portugal

INTRODUCTION

In the Information Systems, authentication involves, traditionally, sharing a secret with the authenticating entity and presenting it whenever a confirmation of the user's identity is needed. In the digital era, that secret is commonly a username/password pair and/or, sometimes, a biometric feature, both presenting difficulties of different kinds. The traditional pair username/password is no longer enough to protect infrastructures, having known vulnerabilities regarding the user privacy and the confidentiality of information, and the biometrics has many issues related to ethical and social implications of its use (Magalhães & Santos, 2005).

Password vulnerabilities come from their misuse that, in turn, results from the fact that they need to be both easy to remember, therefore simple, and secure, therefore complex. Consequently, it is virtually impossible to come up with a "good" password (Wiedenbeck et al., 2005). On the other hand, once users have not yet completely realized the need for securing their authentication secrets, even fairly good passwords become a threat when the security policies (if at all existing) fail to be implemented. The results of an inquiry made by the authors in 2004 to sixty Information Technology (IT) professionals show that, even among those that have technical knowledge, the need for passwords security is underestimated (Magalhães et al., 2006). This is probably one of the reasons why the governments increased their investment in biometric technologies after the terrorist attack of 9/11 (IBG, 2003).

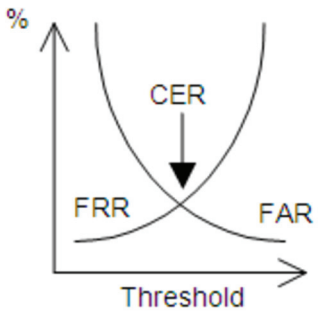
The use of biometric technologies to increase the security of a system has become a widely discussed subject but, while governments and corporations are pressing for a wither integration of these technologies with common security systems (like passports or identity cards), human rights associations are concerned with the ethical and social implications of its use. This situation creates a challenge to find biometric algorithms that are less intrusive, easier to use and more accurate.

The precision of a biometric technology is measured by its False Acceptance Rate (FAR), that measures the permeability of the algorithm to attacks, by its False Rejection Rate (FRR), that measures the resistance of the algorithm to accept a legitimate user, and by its Crossover Error Rate (CER), the point of interception of the FAR curve with the FRR curve that indicates the level of usability of the technology (Figure 1). For a biometric technology to be usable on a stand-alone base, its CER must be under 1%. As an algorithm gets more demanding, its FAR gets lower and its FRR gets higher; usually the administrator of the system can define a threshold and decide what will be the average FAR and FRR of the applied algorithm, according to the need for security – dependent of the risk evaluation and of the value of what is protected; also the threshold can be, in theory, defined by an Intrusion Detection System (software designed to identify situations of attack to the system).

Establishing the error rates of a biometric technology is a complex problem. Studies have been made to normalize their evaluation, but the fact is that the results are strongly dependent of the number of individuals involved in the process and, what is worst, of who is chosen. This means that, even with a large amount of data collected, the results can be very different if we change the evaluated group. The lack of trust in the precision evaluation methodologies and values is one of the reasons why the human rights

DOI: 10.4018/978-1-4666-5888-2.ch418

Figure 1. Crossover error rate



associations are opposing to the generalization of use of biometric technologies and their acceptance as standards for authentication procedures (Privacy International, 2004). Even so, in an inquire made by epaynews (www.epaynews.com) 36% of the users stated that they would prefer to use biometric authentication when using credit cards, a value only comparable to the use of Personal Identification Numbers (PINs) and much higher than the 9% obtained by the signature.

Considering all the advantages and disadvantages of the biometric procedures, it seems that the only way is to allow the user's choice. Being so, the traditional password systems must be enhanced both in the biometrical way and in another completely different way. On the biometric component we propose Keystroke Dynamics, a biometrical authentication algorithm that tries do define a user's typing pattern and then verifies in each login attempt if the pattern exiting in the way the password was typed matches the user's known pattern, once it's the only biometric technology that can be used with the existing login/password systems without requiring any extra hardware. On the non-biometric way we propose the use of a Graphical Authentication System, a login system that verifies the user's knowledge on specific images or parts of images to grant or deny him a successful login, because it has been proved that it provides a wither key space and because it can be used to generate complex secret strings, from simple passgraphs (the user's secret code to access a system protected by a graphical authentication system, constituted by a sequence of points where the user must click in order to obtain a successful login).

BACKGROUND

Keystroke Dynamics

As in many other problems, there have been two different approaches to the challenge of finding an algorithm for keystroke dynamics that minimizes the CER: machine-learning and deterministic algorithms.

Among the solutions based on the machine learning we can find the work presented by Ord and Furnell (Ord & Furnell, 2000) that tested this technology with a 14 people group to study the viability of applying it to the simple use of PINs (Personal Identification Numbers) typed on a numeric-pad. Unfortunately the results suggest that, for a large-scale use, the technology is not feasible. Deterministic algorithms have been applied to keystroke dynamics since the late 70's. In 1980 Gaines (Gaines, 1980) presented a report of his work to study the typing patterns of seven professional typists. The small number of volunteers and the fact that the algorithm is deducted from their data and not tested in other people later, results on a lower confidence on the FAR and FRR values presented. But the method used to establish a pattern was a breakthrough: a study of the time spent to type the same two letters (digraph), when together in the text. Since then, many algorithms based on Algebra and on Probability and Statistics have been presented. Joyce and Gupta presented in 1990 (Joyce & Gupta, 1990) an algorithm to calculate a value that represents the distance between acquired keystroke latency times and correspondent times previously stored. In 1997 Monrose and Rubin use the Euclidean Distance and probabilistic calculations based on the assumption that the latency times for one-digraph exhibits a Normal Distribution (Monrose & Rubin, 1997). Later, in 2000, they also present an algorithm for identification, based on the similarity models of Bayes (Monrose & Rubin, 2000), and in 2001 they present an algorithm that uses polynomials and vector spaces to generate complex passwords from a simple one, using the keystroke pattern (Monrose et al., 2001).

In 2005, Magalhães et al (Magalhães et al., 2005) presented an improvement of the Joyce and Gupta's algorithm and tested it with 170.391 attacks to 143 patterns obtaining a 0% FAR, with a FRR of 26%, and an estimated CER below 5%.