Chapter 11
Continuous User Authentication Based on Keystroke Dynamics through Neural Network Committee Machines

Sérgio Roberto de Lima e Silva Filho
Bry Tecnologia S.A., Brazil

Mauro Roisenberg
Federal University of Santa Catarina, Brazil

ABSTRACT

This chapter proposes an authentication methodology that is both inexpensive and non-intrusive and authenticates users continuously while using a computer keyboard. This proposed methodology uses neural network committee machines. The committee consists of several independent neural networks trained to recognize a behavioral biometric characteristic: user's typing pattern. Continuous authentication prevents potential attacks when users leave their desks without logging out or locking their computer session. Some experiments were conducted to evaluate and to calibrate the authentication committee. Best results show that a 0% FAR and a 0.15% FRR can be achieved when different thresholds are used in the system for each user. In this proposed methodology, capture system does not need to concern about typing errors in the text. Another feature of this methodology is that new users can be easily added to the system, with no need to re-train all neural networks involved.

INTRODUCTION

Currently, lots of people are using computers and their networks in order to simplify their lives, get remote services and stay connected with other people. So, users are increasing their dependency on computers and Internet (Monrose & Rubin, 1997; Obaidat, 1995; Obaidat & Sadoun, 1997). Such dependency results in more critical informa-

DOI: 10.4018/978-1-61350-129-0.ch011

tion being stored in computers that become a prime target for frequent attacks. Those attacks may cause some serious problems such as classified documents being disclosed and critical information being deleted, falsified or stolen (Anagun & Cin, 1998; Capuano, Masella, Miranda & Salerno, 1999; Obaidat, 1995; Obaidat & Sadoun, 1997).

Many users do not concern enough or do not know the dangers of the misuse of personal, confidential or critical information stored in their computers. So, imagine a user that stores a bank account password into a file on the computer. An unauthorized person can gain access to this computer, get the password and use the Internet banking to transfer money to another account. Same problem occurs when a credit card number is stored in the computer. Intruders could use credit card number to buy what they want via online shops.

In order to assure that only valid users will be able to access computer resources and the information stored in them, authentication mechanisms try to prevent non-authorized users to disguise themselves as valid users and then access those restricted resources (Brown & Rogers, 1993; Coltell, Bada & Torres, 1999; Monrose, Reiter & Wetzel, 1999; Obaidat & Sadoun, 1997).

User authentication mechanisms are a very promising area of research and in recent years many authentication mechanisms have been proposed. However, those schemes have a common drawback as they only authenticate a user at the login procedure. If a user leaves the desk without logging out or locking computer session, an intruder has an occasion to use the system (Coltell, Bada & Torres, 1999).

An authentication scheme that overcomes such deficiency must continuously authenticate the user who is using the computational resource. So, users are authenticated all the time, starting at the very moment they access the resources to the moment they are no longer using the computer. If users have to leave their desks for a short break or to attend a meeting, they do not have to worry about non-authorized access to the computer because it will remain protected from any attack of non-authorized people.

Analyzing which feature should be used to provide that continuous authentication, we can conclude that continuous authentication is impracticable using passwords because would be extremely tiring for the user having to repeatedly typing same password to get access to computer. Same problem occurs when a smartcard is used for authentication. If a system asks all the time for a smartcard to authenticate the user, it probably would cause the user to leave the smartcard connected to the computer. On the occasion of an oversight, an intruder could gain access to the system.

Given these drawbacks for conventional authentication features to be used in a continuous authentication mechanism, many researchers have considered using biometric characteristics in continuous authentication schemes. However, in a continuous authentication environment we can discard some biometric characteristics that have been commonly used in a human authentication context, like fingerprint recognition, eye scan of iris or retina, voice recognition, face recognition using the geometry of the face and signature dynamics. For example, it would be totally impractical for a user to constantly put the thumb in a fingerprint reader or continuously talk in a speech recognizer.

Looking for an appropriate biometric characteristic to be used continuously, we found that two behavioral characteristics are present most of the time a user is using a computational resource: keystroke and mouse usage dynamics. As keyboard and mouse devices are constantly used for interacting with the system, their dynamics can be used as viable features for user authentication throughout the work session even after the access control phase has been passed (Bergadano, Gunetti & Picardi, 2002).

Therefore, the objective of this study is to investigate and develop a user authentication