Chapter 82
Performance Metrics and Models for Continuous Authentication Systems

Ahmed A.E. Ahmed
University of Victoria, Canada

Issa Traoré
University of Victoria, Canada

ABSTRACT

Continuous Authentication (CA) systems represent a new class of security systems that are increasingly the focus of much attention in the research literature. CA departs from the traditional (static) authentication scheme by repeating several times the authentication process dynamically throughout the entire login session; the main objectives are to detect session hijacking and ensure session security. As the technology gains in maturity and becomes more diverse, it is essential to develop common and meaningful evaluation metrics that can be used to compare and contrast between existing and future schemes. So far, all the CA systems proposed in the literature were by default evaluated using the same accuracy metrics used for static authentication systems. As an alternative, we discuss in this chapter dynamic accuracy metrics that better capture the continuous nature of CA activity. Furthermore, we introduce and study diverse and more complex forms of the Time-To-Authenticate (TTA) metrics corresponding to the authentication delay. We study and illustrate empirically the proposed metrics and models using a combination of real and synthetic data samples.

INTRODUCTION

User authentication is the process of verifying whether the identity of a user is genuine prior to granting him access to resources or services in a computer system. Traditionally, authentication is performed statically at the point of entry of the system (e.g., login). However, the main issue with this approach is that a successful authentication at the beginning of a session does not provide any remedy against the session being hijacked later by some malicious user.

DOI: 10.4018/978-1-4666-4707-7.ch082

One of the solutions proposed to address these shortcomings is *continuous authentication (CA)* (de Lima & Roisenberg, 2006; Calderon et al., 2006; Liu et al., 2007; Azzini & Marrara, 2008). CA consists of the process of positively verifying the identity of a user in a repeated manner throughout a computing session. Different technologies can be used to develop a CA system, and examples of these include a face recognition camera on a computer that can detect when a user has changed, the sequence of commands entered by a user in a computing session (Lane & Brodley, 1999), keystroke dynamics (Gunetti & Picardi, 2005; Ahmed and Traore, 2008), mouse dynamics (Ahmed & Traore, 2007), and gait (Gafurov & Snekkeness, 2009) etc.

To this date, most of the CA applications proposed in the literature have been evaluated using classical accuracy metrics inspired by signal detection theory (Swets & Pickett, 1992). The existing evaluation framework fails to capture important characteristics of CA systems including the dynamic nature of underlying continuous monitoring activities and the implication of successive alarms being potentially generated in a login session.

A common characteristic of CA applications that the existing evaluation framework fails to capture is the need to generate timely alarms in case of unusual behavior. Here, unusual behavior corresponds to any deviation of a computed profile from an expected one. Not only is the accurate detection of unusual behavior important, but so is the time interval between the triggering of this behavior to its detection. Although the significance of this time interval may vary according to the kind of monitoring application considered, in general the shorter it is the better. For instance, in computer intrusion monitoring, ideally one would expect the monitor to be able to detect intrusive activity before the end of such activity. So the *time-to-recognize* accurately the user must be shorter than the time required by the intruder to succeed in his or her task. In contrast, in network forensics analysis, some flexibility can be allowed regarding the length of the *time-to-recognize*; the primary concern in this case is the gathering of reliable evidence that may be used against perpetrators, possibly after the fact.

Furthermore CA systems may generate multiple alarms that actually are of unequal importance; in general, only the first alarm is significant (Fawcett and Provost, 1999). In principle, after the first alarm appropriate action is taken, such as terminating the fraudulent activity. Subsequent alarms, if any, do not contribute anything new to the state of knowledge.

In this chapter, we introduce a new evaluation framework for CA applications that addresses the above concerns. Specifically, we define new accuracy metrics that capture the dynamic nature of CA systems. We also introduce and analyze various metrics that capture the length of an individual authentication period. The length of a single authentication period can be captured in terms of either the time or the amount of data involved. We identify and study various monitoring scenarios, and for each scenario we provide a formal definition of corresponding length metrics.

The remainder of the chapter is structured around 5 sections as follows. In the second section, we discuss related work on CA evaluation. In the third section, we introduce an abstract CA model and corresponding parameters, and discuss possible performance metrics for CA. In the fourth section, we introduce dynamic accuracy metrics and provide a corresponding formal definition. In the fifth section, we identify different monitoring scenarios and define formally corresponding length metrics. Finally, in the sixth section, we make some concluding remarks.

RELATED WORK

Continuous authentication has been the focus of several proposals in the recent literature (Ikehara & Crosby, 2004; de Lima & Roisenberg, 2006;