Chapter 1
Introduction to Continuous Authentication

Issa Traoré
University of Victoria, Canada

Ahmed A.E. Ahmed
University of Victoria, Canada

ABSTRACT

Continuous Authentication (CA) systems represent a new generation of security mechanisms that continuously monitor user behavior and use this as basis to re-authenticate periodically throughout a login session. CA has been around for about a decade. As a result a limited amount of research work has been produced to date, and the first commercial products have only recently started reaching the market. We attempt, in this chapter, to provide some general perspectives in order to help achieve some common and better understanding of this emerging field. The chapter introduces basic CA concepts and terminologies, discusses the characteristics of CA data sources, and identifies major areas of application for CA systems.

INTRODUCTION

Identity Assurance (IA) is a set of mechanisms and strategies allowing an organization to minimize the business risk related to identity impersonation and misappropriation of authentication credentials. Some of the most serious threats to IA include session hijacking and masquerade attacks (Garg et al., 2006). A successful authentication at the beginning of a session, also referred to as *static authentication*, does not provide any remedy against the session being hijacked later by some malicious user, even when a strong authentication mechanism such as a biometric technology is used. Session hijacking involves an intruder seizing control of a legitimate user session after successfully getting a valid authentication session identifier while that session is still in progress. A possible remedy against such a scenario, referred to as *continuous authentication (CA),* consists of re-authenticating the user repeatedly throughout the lifetime of the session (de Lima and Roisenberg, 2006; Calderon et al., 2006; Liu et al., 2007; Azzini and Marrara, 2008). By repeatedly checking

DOI: 10.4018/978-1-4666-2919-6.ch001

the authentication credentials of the user while the session is still in progress, CA has inherently the capability to detect misappropriation of these credentials resulting from session hijacking.

Continuous authentication represents a subclass of activity monitoring. The field of activity monitoring was originally investigated by Fawcett and Provost (1999) as a new class of Knowledge and Data Discovery (KDD) problems, which consists of observing the behavior of a large number of entities or individuals with the purpose of detecting unusual events requiring immediate actions. Activity monitoring applications greatly vary in terms of the kinds of data streams involved. Nonetheless, Fawcett and Provost have attempted in their study to provide a general and common representation for activity monitoring tasks. These tasks vary from fraud detection to intrusion detection, or news story monitoring systems. As a subclass of activity monitoring, the field of application of CA is narrower and broadly fall under the category of intrusion detection.

This chapter provides some general perspectives on CA as an emerging discipline by defining fundamental concepts, discussing the characteristics of underlying data sources, and outlining some major applications. The goal of this chapter is less about presenting some concrete research results and more about providing some insight and laying down some ground for a better understanding of this emerging discipline. The rest of the chapter is articulated around four main sections as follows.

Firstly, we present a conceptual framework for CA where basic concepts and terminologies are introduced. We also outline a generic architecture for CA as part of this framework.

Secondly, we present the characteristics of the data needed for continuous authentication. Although this is not an absolute requirement, most of the data sources that exhibit such characteristics can be classified as biometrics. We give an overview of biometrics technologies, in general, and present examples of suitable biometrics technologies for continuous authentication.

Thirdly, we identify and discuss major application areas for CA systems, and finally, in the last section, we make some concluding remarks.

CONCEPTUAL FRAMEWORK FOR CONTINUOUS AUTHENTICATION

Terminologies and Concepts

In this section, we present and discuss the fundamental characteristics of CA systems. More specifically we consider CA systems from different perspectives and outline key terminologies and concepts that characterize CA activity and mechanism.

Static vs. Continuous Authentication

Static authentication is a binary decision process consisting of three sub-processes: *enrollment*, *presentation*, and *evaluation* (see Figure 1). During the enrollment sub-process information is collected about the individual, processed and stored as a template or a profile to be used subsequently as basis for authentication. The presentation sub-process is executed when an individual wants to use the system. When prompted by the system,

Figure 1. Static authentication process