Chapter 13
Continuous Authentication in Computers

Harini Jagadeesan
Virginia Tech, USA

Michael S. Hsiao
Virginia Tech, USA

ABSTRACT

In the Internet age, identity theft is a major security issue because contemporary authentication systems lack adequate mechanisms to detect and prevent masquerading. This chapter discusses the current authentication systems and identifies their limitations in combating masquerading attacks. Analysis of existing authentication systems reveals the factors to be considered and the steps necessary in building a good continuous authentication system. As an example, we present a continual, non-intrusive, fast and easily deployable user re-authentication system based on behavioral biometrics. It employs a novel heuristic based on keyboard and mouse attributes to decipher the behavioral pattern of each individual user on the system. In the re-authentication process, the current behavior of user is compared with stored "expected" behavior. If user behavior deviates from expected behavior beyond an allowed threshold, system logs the user out of the current session, thereby preventing imposters from misusing the system. Experimental results show that the proposed methodology improves the accuracy of application-based and application independent systems to 96.4% and 82.2% respectively. At the end of this chapter, the reader is expected to understand the dimensions involved in creating a computer based continuous authentication system and is able to frame a robust continual re-authentication system with a high degree of accuracy.

INTRODUCTION

Security is a key concern in the internet age where an increasing number of transactions are made over an unsecured network and there is a greater chance for sensitive data to be misused. Authentication mechanisms usually form the first line of defense in an electronic system's security. They can be used for both initial authentication (verifying if a user is genuine) and re-authentication (continually verifying if the current user is the same as the logged-in user). Specifically, re-authentication or continuous authentication (CA) technologies are becoming

DOI: 10.4018/978-1-4666-2919-6.ch013

more prevalent due to continued login into systems like laptops, netbooks, mobile devices, etc. For example, if an authenticated user temporarily leaves a system unattended without exiting the application or webpage completely, the session can still be in use. These sessions can be used by intruders to gain access to sensitive information. Also, if traditional authentication mechanisms are broken via stolen passwords, PINs, hardware keys, etc., the computer system currently has no way to distinguish the hacker from the authentic user. This, in turn, would compromise the entire system's security if the authentication mechanisms consist only of traditional authentication methods.

Authentication of a user is generally performed at the beginning of a user session and during subsequent logout-logins. Although sufficient for one-time validation, it is ineffective in preventing masquerade attacks. Unlike user authentication, which attempts to determine if the person trying to enter the system via a controlled setting (e.g., typing of a password) matches the expected behavior, we try to determine if the user's uncontrolled behavior matches the expected behavior. Thus, a user re-authentication system aims to continuously check if the *current-user* is the *logged-in user*. The *logged-in user* refers to the user whose initial login information authenticated the session. The *current user* refers to the person who is presently using the system. In general, we expect that the *current-user* and the *logged-in user* are the same. However, imposters can intercept the system and become the *current user*. In such scenarios, the *current user* is not the same as *logged-in user* and should be identified. In computer system authentication, this scenario is known as *Masquerading*.

Identity thefts due to masquerading cannot be successfully prevented by traditional methods since the intruder has already broken the authentication system. Two major factors in masquerading effort are:

- **Accessibility to a user's session:** This is possible by stolen passwords, PINs, unsecure session exits, etc. and can be prevented by using a second (and possibly, third) layer of authentication which is accurate and has a high cost of cryptoanalysis. A search for such a layer of authentication points towards mechanisms that involve characteristics which are unique to a user. A user's biometric characteristics and to a certain extent, to her behavioral characteristics satisfy this requirement. For example, biometric characteristics like the iris print, finger print, DNA, etc. are unique and cannot be replicated easily. Similarly, a user's behavioral characteristics are very hard to imitate. Research shows that it is impossible for a person to demonstrate a set of behavioral characteristics that are different from her own. Such an exercise usually results in a mixed set of behavioral characteristics that borrows from both the original set and the new set. If a system is sensitive enough to identify the subtle differences in a user's behavior, it can easily identify the intruder despite masquerade attempts.
- **Time of access:** Gaining access to a user's session when it is in use by a genuine user (if the authentic user is away temporarily – without securely locking the system) is a common example for the time of access factor in masquerading efforts. As a security measure against this possibility, it is necessary for the authentication system to ensure that at any point of logged-in time, the current user is the same as the logged in user. This need is satisfied by continuous authentication of the user which ensures that the logged-in user's profile matches the current user's profile. When done periodically, they help mitigate the time of access factor in masquerading.

So the second layer of authentication should include non-intrusive real-time or continuous