Chapter 42
Biometric Authentication Techniques in Online Learning Environments

Jack Curran
Open University, UK

Kevin Curran
Ulster University, UK

ABSTRACT

The deployment of online e-learning can lead to many security risks, such as confidentiality loss, exposure of critical data, availability and destruction of publicly available information services. Security and proper authentication is critical in any online learning environment because any flaws can affect perceptions of its trustworthiness. Biometric authentication is increasingly being used in the newer generation of online learning environments for authentication of remote learners. Biometrics scan unique physiological characteristics in humans to identify people. These include fingerprints, iris, retina, voice, face, gait, and odor. The authors look at the state of biometric authentication techniques applicable to online learning environments and provide a more in-depth examination of face- and iris-based authentication systems for proper identification of learners.

BACKGROUND

There is becoming close to 100% adoption of e-learning environments in education institutions. Online learning environments are by their nature subject to all the attacks that online systems are vulnerable to (Adams & Blandford, 2003). Their 'low risk' nature on roll-out however leave many of the online learning environment content management more open than usual (Chen and He, 2013). Educational institutions tend to underestimate their attack surface and implications of being penetrated (Zuev, 2012). There is also the added weakness of Denial of service attacks which render e-learning environments unavailable to students. Commons risks however are unauthorized modification or deletion of educational materials,

DOI: 10.4018/978-1-7998-8047-9.ch042

and the equally dangerous problem unique to remote e-learning models of identity theft, impersonation, and weak authentication (Ayodele et al., 2011). The roll-out of online e-learning can lead to many security risks, such as loss of confidentiality, the exposure of critical data, availability and destruction of publicly available information services (Srivastava & Sinha, 2013). Security & proper authentication is critical as a means to retain user trust in any online learning environment because any risk can affect perceptions of its trustworthiness (Weippl & Ebner, 2008). Therefore, it is crucial to try to identify any underlying factors that lead to security issues in online learning and identify the limitations of security in place (Yao et al., 2011). The next step of course is to develop mitigations for any weaknesses uncovered.

Authentication is a key aspect for online learning (Raitman et al., 2005). There are several ways to achieve this. They can use knowledge-based authentication where users enter passwords or pins. They can use token-based authentication with key card, smart-phones or some security token or they can use biometric based authentication such as fingerprints, palm print, a retinal scan, or a face scan (Alotaibi & Argles, 2011; Garfinkel & Spafford, 1996). Among these authentication methods, user logins are the simplest means for providing identity and access services while retinal or face scans are the more difficult - but seen as the stronger (Song et al., 2013). In fact, biometric authentication seems to be increasingly used in the newer generation of online learning environments for authentication (Wang et al., 2013).

Humans possess many unique physiological body and shape characteristics that distinguish one from another. Some of these biometric characteristics in humans include fingerprints, iris, retina, voice, face, Palm prints and palm veins (Li & Kot, 2013). Some are more unique and secure than others. The uniqueness of a biometric feature that nearly every human possesses is determined by how many possible combinations can exist. Such a measure maximizes between-person random variations while at the same time minimizes within-person variability (Teoh et al., 2004). A biometric with many combinatorial possibilities means the possibility of two individuals in possession of identical patterns becomes increasingly less probable, therefore making it more secure as a biometric authenticator. There are two categories of biometrics. One deals with the physiological aspect, such as patterns, prints and physical features and the other is behavioural concentrating on aspects such as typing patterns, walking gaits, mannerisms, voice and computer usage patterns (Ratha & Zhang, 2010). An example of an insecure biometric authenticator would be the colour of people's eyes. If someone had brown eyes and they were enrolled on a database, everyone else with brown eyes who were to attempt to enrol themselves would be authenticated as being the first individual which was scanned originally (Pfleeger & Pfleeger, 2007). Therefore, this is insecure as anyone with brown eyes can be an imposter to the original individual who was enrolled. If, however there was a biometric feature with the probability of having the same pattern with another human being 1/1,000,000,000, then this would be considered secure as it is almost impossible to have two individuals with the same biometric pattern.

Biometric scans can be passive or contact. Passive scanning means no physical contact is required e.g. in iris scanning, where a user is told to stand a certain distance from the camera. Contact biometrics is when contact with a physical object is needed e.g. finger print scanning, when a user is asked to place their specified finger upon a scanning surface (Farooq et al., 2007). Compared with traditional password or token-based authentication, biometrics are considered more secure when executed correctly. Password and token-based methods can only authenticate a person possesses a token or knows a password. However, biometrics can check that a person is who they claim to be. Deployment of proper biometric solutions should significantly reduce identity thefts with great benefits for the economy by eliminating passwords from the equation in place of more reliable solutions. Trust is particularly important for financial institutions and merchants as well as consumers (identify theft, account blocking inconvenience) alike so we