Biometrics, A Critical Consideration in Informaiton Security Management

Paul Benjamin Lowry
Brigham Young University, USA

Jackson Stephens
Brigham Young University, USA

Aaron Moyes
Brigham Young University, USA

Sean Wilson
Brigham Young University, USA

Mark Mitchell
Brigham Young University, USA

INTRODUCTION

The need for increased security management in organizations has never been greater. With increasing globalization and the spread of the Internet, information-technology (IT) related risks have multiplied, including identity theft, fraudulent transactions, privacy violations, lack of authentication, redirection and spoofing, data sniffing and interception, false identities, and fraud.

Many of the above problems in e-commerce can be mitigated or prevented by implementing controls that improve authentication, nonrepudiation, confidentiality, privacy protection, and data integrity (Torkzadeh & Dhillon, 2002). Several technologies help support these controls, including data encryption, trusted third-party digital certificates, and confirmation services. Biometrics is an emerging family of authentication technologies that supports these areas.

It can be argued that authentication is the baseline control for all other controls; it is critical in conducting e-commerce to positively confirm that the people involved in transactions are who they say they are. Authentication uses one or more of the following methods of identification (Hopkins, 1999): something you know (e.g., a password), something you have (e.g., a token), and something about you (e.g., a fingerprint). Using knowledge is the traditional approach to authentication, but it is the most prone to problems, because this knowledge can be readily stolen, guessed, or discovered through computational techniques. Physical objects tend to be more reliable sources of identification, but this approach suffers from the increased likelihood of theft. The last approach to authentication is the basis for biometrics. Biometrics refers to the use of computational methods to evaluate the unique biological and behavioral traits of people (Hopkins, 1999) and it is arguably the most promising form of authentication because personal traits (e.g., fingerprints, voice patterns, or DNA) are difficult to steal or emulate.

BACKGROUND

A given biometric can be based on either a person's physical or behavioral characteristics. Physical characteristics that can be used for biometrics include fingerprints, hand geometry, retina and iris patterns, facial characteristics, vein geometry, and DNA. Behavioral biometrics analyze how people perform actions, including voice, signatures, and typing patterns.

Biometrics generally adhere to the following pattern: When a person first "enrolls" in a system, the

target biometric is scanned and stored as a template in a database that represents the digital form of the biometric. During subsequent uses of the system the biometric is scanned and compared against the stored template.

The process of scanning and matching can occur through verification or identification. In verification (a.k.a. authentication) a one-to-one match takes place in which the user must claim an identity, and the biometric is then scanned and checked against the database. In identification (a.k.a. recognition), a user is not compelled to claim an identity; instead, the biometric is scanned and then matched against all the templates in the database. If a match is found, the person has been "identified."

The universal nature of biometrics enables them to be used for verification and identification in forensic, civilian, and commercial settings (Hong, Jain, & Pankanti, 2000). Forensic applications include criminal investigation, corpse identification, and parenthood determination. Civilian uses include national IDs, driver's licenses, welfare disbursement, national security, and terrorism prevention. Commercial application includes controlling access to ATMs, credit cards, cell phones, bank accounts, homes, PDAs, cars, and data centers.

Despite the promise of biometrics, their implementation has yet to become widespread. Only $127 million was spent on biometric devices in the year 2000, with nearly half being spent on fingerprinting; however, future growth is expected to be strong, with $1.8 billion worth of biometrics-related sales predicted in 2004 (Mearian, 2002). Clearly, the true potential of biometrics has yet to be reached, which opens up many exciting business and research opportunities. The next section reviews specific biometrics technologies.

BIOMETRICS TECHNOLOGIES

This section reviews the major biometrics technologies and discusses where they are most appropriate for use. We examine iris and retina scanning, fingerprint and hand scanning, facial recognition, and voice recognition.

Retina and Iris Scanning

Considered by many to be the most secure of all biometrics, eye-based biometrics have traditionally been utilized in high-security applications, such as prisons, government agencies, and schools. Eye scanning comes in two forms: iris scanning and retina scanning. The first biometric eye-scanning technologies were developed for retina recognition. Retinal scanners examine the patterns of blood vessels at the back of the eye by casting either natural or infrared light onto them. Retina scanning has been demonstrated to be an extremely accurate process that is difficult to deceive because retinal patterns are stable over time and unique to individuals (Hong et al., 2000).

Iris scanning is a newer technology than retina scanning. The iris consists of the multicolored portion of the eye that encircles the pupil, as shown in Figure 1. Iris patterns are complex, containing more raw information than a fingerprint. The iris completes development during a person's first two years of life, and its appearance remains stable over long periods of time. Irises are so personally unique that even identical twins exhibit differing iris patterns.

Two differences between retina and iris scanning are the equipment and the procedures. The equipment for retina recognition tends to be bulky and complex and the procedures tend to be uncomfortable. Users must focus on a particular spot for a few seconds and their eyes must be up close to the imaging device. Figure 2 shows an iris scanner sold by Panasonic. Unlike retinal scanning, iris recognition involves more standard imaging cameras that are not as specialized or as expensive. Iris scanning can be accomplished

Figure 1. Depiction of an iris from www.astsecurity.com