Chapter 13
Biometric Security in the E-World

Kunal Sharma
DOEACC Centre, India

A.J. Singh
H.P. University, India

ABSTRACT

The rising number of networked computers and the evolution of the WWW have witnessed the emergence of an E-World where the users are often referred to as e-people. In the new e-world, the evolution of WWW and Internet applications has become a focal point to the question of sustainable competitive advantage (Brennan & Johnson,2001).The increase in information access terminals along with the growing use of information sensitive applications such as e-commerce, e-learning, e-banking and e-healthcare have generated a real requirement of reliable, easy to use, and generally acceptable control methods for confidential and vital information. On the other hand, the necessity for privacy must be balanced with security requirements for the advantage of the general public. Current global events have shown the significance to provide the police, airport area, and other exposed area, new reliable component security tools such as biometrics. Access to systems that need security from unauthorized access is generally restricted by requesting the user to confirm her identity and to authenticate. Payment systems are undergoing radical changes stirred largely by technical advancement such as distributed network technology, real-time processing and online consumers' inclination to use e-banking interfaces making the study of biometrics even more important in this new E-World.

INTRODUCTION

There are many tools and techniques that can sustain the management of information security and systems based on biometrics that have developed to support some attributes of information security. Identity authentication and verification practices such as keys, cards, passwords, and PIN are commonly employed security applications. Still, passwords or keys may frequently be forgotten, divulged, altered, or stolen. Biometrics is an identity authentication technique which is being

DOI: 10.4018/978-1-61520-783-1.ch013

used currently and is more dependable, contrasted to conventional techniques. The phrase biometrics originated from the Greek words *"bios"* viz. life and *"metrikos"* viz. measure, ie. it is "the measurement of life". Sir Francis Galton, author of the book *Fingerprints* (Stigler,1995) was an English scientist well acknowledged for his theories on improving the human race through eugenics which is the application of the principles of genetics to the development of humankind and can be considered as the father of biometrics. Exactly speaking, biometrics means a science encompassing the statistical analysis of biological features (Zhang, 2000). A good quality of biometric characteristics is that they are founded on something you are or something you do, so you do not necessitate to memorize anything neither to hold any token.

Biometrics is accordingly defined as the automated way of identifying or authenticating the identity of a living individual, based on physiological or behavioral features. The phrase "biometrics" is used to elucidate two diverse facets of the technology: attributes and procedures. Biometrics as "attributes" refers to quantifiable organic (anatomical and physiological) or behavioral characteristics of the individual that can be employed for automated recognition. Biometrics as "procedures" refers to automated techniques of identifying an individual based on quantifiable biological (anatomical and physiological) and behavioral distinctiveness.

Physiological features used in biometrics include features such as face, fingerprint, and iris. Behavioral traits comprise signature, gait, and voice. This technique of identity verification is favoured over conventional passwords and PIN-based methods for different grounds, such as (Jain *et. al.*, 1999; Jain *et. al.*, 2004):

- The individual to be identified is required to be physically present for the identity authentication.
- Identification based on biometric procedures averts the need to remember a password or carry a token.
- It cannot be misplaced or forgotten.

SECURITY CHALLENGES IN THE E-WORLD

Potentially there are numerous reasons for the growth in security attacks; but one trend that is undeniable is the growth in the number and sophistication of cracking tools (Adams,2003). Thus, security becomes one of the biggest issues we face today. Crackers have been utilizing the recent technological advances, freely accessible over the WWW, to access important information resources from anyplace in the world. The two most sophisticated tools to crack passwords are L0phtcrack and Pwdump3.With the growing reliance of business organizations on information networks, the security aspects of such networks is becoming necessary, particularly with the surfacing of E-Commerce over Intranets, Extranets, and the Internet. Security challenges to these networks have different unwanted business impacts on organizations, such as: business embarrassment, financial loss, degradation of competitiveness, and legal problems (Rolf,2002;Rao,2004).

Security is an important issue. The penetration of personal computers, local area networks and distributed computing has radically changed the way we administer and control information resources. Internal controls that were efficient in the centralized, batch-oriented mainframe environment of yesteryears are insufficient in the distributed computing environment of today. Protection of distributed computing environment is of great importance in any enterprise information system (Caelli, 1994). Attacks on computer systems are on the rise and the sophistication of these attacks continues to rise to startling levels. Throughout much of the academic and practitioner literature, trust, privacy of information and systems