Chapter 9
Biometric Authentication in the Digital Age:
Rights, Risks, and Responsibilities

Raymond Anthony
University of Alaska – Anchorage, USA

Bogdan Hoanca
University of Alaska – Anchorage, USA

Kenrick Mock
University of Alaska – Anchorage, USA

ABSTRACT

The increased use of biometric traits to digitally authenticate people has the potential to conveniently and accurately grant or deny individual access to information and services. Unlike passwords or smart cards that are also used to authenticate a user, biometrics are not replaceable if lost or stolen—yet there are no universal rights protecting people against unauthorized use of their biometrics. Moreover, there are no clear accommodation rights for users who might not be able to provide some biometrics, for example due to cultural reasons or because of a disability. If users cannot be guaranteed the recovery of stolen biometrics, do people have a right to only provide those biometrics that cannot be stolen? While biometric technology by itself does not raise intrinsic ethical issues, the authors identify a number of extrinsic ethical arguments about the ethical status of applications of this technology and its consequences, namely, those that are linked to distributive justice issues and risk. They explore some of these concerns and discuss strategies to mitigate them within the context of balancing the rights of individuals and the need to ensure collective security.

DOI: 10.4018/978-1-4666-0891-7.ch009

INTRODUCTION

Whether we are still in the Internet Age or beyond it, the Internet continues to be ever more present and indispensable in daily life. As the volume of electronic communications grows, the electronic communications channels become increasingly attractive targets for malicious users: an ever-growing number and variety of attacks on Information Systems (ISs) are reported in the media on a regular basis (Bradley, 2011). Most of these attacks involve at some level the theft of a user's identity, to gain access to computing resources, to private data, or ultimately to financial resources. Despite incredible advances in IS over the past half a century, identifying (or authenticating) users on an IS relies most often on techniques from the early days of IS: passwords. User identification is a one to many process of looking up a user in a database given a certain user-identifying feature. Authentication is somewhat more limited in scope, and is only a one-to-one comparison, intended to confirm the claim of a given user name based on an associated user-identifying feature. At the most basic level, for correct identification users need to have distinct features, while authentication works even if some users might have similar or identical identifying features. While most of what we discuss in this chapter applies to both identification and authentication, we will mainly refer to authentication, for simplicity.

Single and Multiple Factor Authentication Schemes

There are three user identifying features (usually called factors) that are commonly used: "something you know" (passwords), "something you have" (smart cards or tokens), or "something you are" (biometric traits or biometrics). Most information security experts agree that multiple factor authentication—combining two or more of the three ways to authenticate users—is a key tool for mitigating security risks in authentication. The basic premise is that it is considerably more difficult for an attacker to acquire multiple forms of authentication that are required to work in concert. This has been only partly true, as multiple factor authentication schemes have also been breached by determined attackers.

Since the 1970s many secure authentication systems required users to enter both a password and a key code generated by hardware token (Denning, 1979). For physical access, user authentication often involves scanning a badge or smart card and entering a Personal Identification Number (PIN)—e.g., for staff-only security doors at airports. The use of biometrics has been somewhat more limited, for reasons related to cost, user discomfort, and privacy. These reasons will be described in detail in the remainder of the chapter. At the same time, biometric traits are expected to be the most user-friendly among the three authentication factors, again, for reasons we will detail in the chapter.

The remainder of the chapter starts with a description of the general features and limitations of the most common biometrics. Chief among the limitations of biometrics are privacy concerns, which raise ethical concerns about the harvesting and use of such traits. As such, we propose a new set of user rights to respond to the challenges posed by the use of biometrics, and we discuss appropriate uses of biometrics that would respect the users' rights.

Biometrics for User Authentication in Information Systems

While most people are familiar with the use of fingerprints to identify crime scene suspects, the use of biometric traits to identify users on ISs is less well understood. Fingerprint scanners for personal computers became commercially available in 1984 (Willis, 2008) but the first laptop with an integrated fingerprint reader was not available until 2004 (Lenovo). While electronic devices with integrated fingerprint scanners are