Biometrics Security

Stewart T. Fleming
University of Otago, New Zealand

INTRODUCTION

Information security is concerned with the assurance of confidentiality, integrity, and availability of information in all forms. There are many tools and techniques that can support the management of information security and systems based on biometrics that have evolved to support some aspects of information security. Biometric systems support the facets of identification/authorization, authentication and non-repudiation in information security.

Biometric systems have grown in popularity as a way to provide personal identification. Personal identification is crucially important in many applications, and the upsurge in credit-card fraud and identity theft in recent years indicates that this is an issue of major concern in society. Individual passwords, PIN identification, cued keyword personal questions, or even token-based arrangements all have deficiencies that restrict their applicability in a widely-networked society. The advantage claimed by biometric systems is that they can establish an unbreakable one-on-one correspondence between an individual and a piece of data.

The drawback of biometric systems is their perceived invasiveness and the general risks that can emerge when biometric data is not properly handled. There are good practices that, when followed, can provide the excellent match between data and identity that biometrics promise; if not followed, it can lead to enormous risks to privacy for an individual.

Biometric Security

Jain et al. (2000) define a biometric security system as: …essentially a pattern-matching system which makes a personal identification by establishing the authenticity of a specific physiological or biological characteristic possessed by the user. An effective security system combines at least two of the following three elements: "something you have, something you know or something you are" (Schneier, 2000). Biometric data provides the "something you are"—data is acquired from some biological characteristic of an individual. However, biometric data is itself no guarantee of perfect security; a combination of security factors, even a combination of two or more biometric characteristics, is likely to be effective (Jain et al., 1999). Other techniques are needed to combine with biometrics to offer the characteristics of a secure system—confidentiality (privacy), integrity, authentication and non-repudiation (Clarke, 1998).

Biometric data come in several different forms that can be readily acquired, digitized, transmitted, stored, and compared in some biometric authentication device. The personal and extremely sensitive nature of biometric data implies that there are significant privacy and security risks associated with capture, storage, and use (Schneier, 1999).

Biometric data is only one component in wider systems of security. Typical phases of biometric security would include acquisition of data (the biological characteristic), extraction (of a template based on the data), comparison (with another biological characteristic), and storage. The exact design of biometric systems provides a degree of flexibility in how activities of enrollment, authentication, identification, and long-term storage are arranged. Some systems only require storage of the data locally within a biometric device; others require a distributed database that holds many individual biometric samples.

BACKGROUND

Biometric security systems can be divided logically into separate phases of operation—separating enrollment of a biometric from extraction and coding into a template form to authentication where a sample acquired from an individual at some time is compared with one enrolled at a previous time. The

enrollment and comparison of biometric data are done by some biometric authentication device, and a variety of biometric data can be used as the basis for the authentication. The characteristics of a number of different devices are described, and then the particular risks and issues with these devices are discussed in the main part of this article.

Types of Biometric Devices

Several types of biometric data are commonly in use. Each of the following types of devices captures data in a different form and by a different mechanism. The nature of the biometric data and the method by which they are acquired determines the invasiveness of the protocol for enrollment and authentication. The method of acquisition and any associated uncertainties in the measurement process can allow a malicious individual to attack the security of the biometric system by interfering with the capture mechanism or by substituting biometric data.

- **Fingerprint Scanner:** Acquires an image of a fingerprint either by optical scanning or capacitance sensing. Generation of biometric templates is based on matching minutiae—characteristic features in fingerprints.
- **Retinal/Iris Scanner:** Both are forms of biometric data capture based on scanning different parts of the eye. In a retinal scan, a biometric template is formed by recording the patterns of capillary blood vessels at the back of the eye. Iris scanning can be performed remotely using a high-resolution camera and templates generated by a process similar to retinal scanning.
- **Facial Scanner:** Facial recognition works by extracting key characteristics such as relative position of eyes, nose, mouth, and ears from photographs of an individual's head or face. Authentication of facial features is quite sensitive to variations in the environment (camera position, lighting, etc.) to those at enrollment.
- **Hand Geometry:** Scanners generate templates based on various features of an individual's hand, including finger length. Templates generated can be very compact, and the method is often perceived by users to be less invasive than other types of biometric devices.
- **Voiceprint:** Voiceprint recognition compares the vocal patterns of an individual with previously enrolled samples. An advantage of voiceprint techniques over other forms of biometric is the potential to detect duress or coercion through the analysis of stress patterns in the sample voiceprint.
- **DNA Fingerprint:** This method works by taking a tissue sample from an individual and then sequencing and comparing short segments of DNA. The disadvantages of the technique are in its overall invasiveness and the speed at which samples can be processed. Due to the nature of the process itself, there is an extremely low false acceptance rate, but an uncertain false rejection rate.
- **Deep Tissue Illumination:** A relatively new technique (Nixon, 2003) that involves illumination of human tissue by specific lighting conditions and the detection of deep tissue patterns based on light reflection. The technique is claimed to have less susceptibility for spoofing than other forms of biometric techniques, as it is harder to simulate the process of light reflection.
- **Keystroke Pattern:** Technique works by detecting patterns of typing on a keyboard by an individual against patterns previously enrolled. Keystroke biometrics have been used to harden password entry—to provide greater assurance that a password was typed by the same individual that enrolled it by comparing the pace at which it was typed.

Typically, the raw biometric data that are captured from the device (the measurement) are encoded into a biometric template. Extraction of features from the raw data and coding of the template are usually proprietary processes. The biometric templates are normally used as the basis for comparison during authentication. Acquisition, transmission, and storage of biometric templates are important aspects of biometric security systems, as these are areas where risks can arise and attacks on the integrity of the system can be made.

In considering the different aspects of a biometric system, we focus on the emergent issues and risks concerned with the use of this kind of data.