LAIKIPIA UNIVERSITY

CRSS 423: PHYSICAL SECURITY II

Topic 7: Biometric Authentication & Authorization

The underlying purpose of identity management in physical security is to verify the identity of individuals in order to provide access to those who are authorized and to deny access to those who are not authorized. Nearly all identification methods in use today are based on one or more tokens or identifiers:

- There are knowledge tokens such as passwords or PINs or relatively obscure personal information such as one's mother's maiden name.
- There are physical tokens such as badges, cards, passports, driver's licenses, and keys.
- There are behavioral or physiological biometric identifiers.

Each of these methods has its advantages and limitations, and each may be the appropriate solution in a given set of circumstances. But each method by itself offers only a single security factor. Strong authentication[1] demands a combination of authentication factors such as knowledge, tokens, or biometric authentication used to verify identity under security constraints. Although tokens can provide a proxy for an identity claim, they can be forgotten, lost, stolen, forged, or compromised, and they do not provide nonrepudiation. Token-based systems simply do not completely verify the identity of the user.

With regard to physical security, in order to enable entry by authorized individuals and to thwart the unauthorized ones, one's identity must be verified within an acceptable probability. Biometrics is arguably the only technology that can bind a person to a verification event, such as requesting entry into a secure facility. A biometric template could also be stored on a PIN-activated smart card (which might also serve as a badge) and, together, they would provide three-factor security. When strong three-factor security is used to secure physical access, the risk of fraud significantly declines, and assurance of legitimacy substantially increases.

Unmasking Biometrics

Biometrics means "life measurement." Biometrics refers to automated methods of recognizing an individual based on a measurement of his or her physical or behavioral characteristics. A biometric system is basically an automated pattern recognition system that either makes an identification from a database of many. Most non-surveillance, physical security applications employ identity verification methods.

Based on the use of unique and measurable characteristics, biometrics validates a professed identity, within a given probability. Physiological characteristics include, but are not limited to, a person's vein patterns, facial structure, ocular characteristics, hand geometry, or fingerprints. Behavioral characteristics are based on an individual's unique actions captured over a period of time, including such traits as signature dynamics, voice, gait, and keystroke dynamics. Biometrics is considered a natural and reliable solution for identity verification situations. Therefore, the inclusion of a biometric component for identity verification is a critical enhancement for many physical security systems.

There are a variety of biometric systems in use today. However, no single biometric type, referred to as the biometric modality, is best for all situations. The right biometric modality for a given application depends on many factors, including the task at hand, security risks, population of users, and user circumstances. Moreover, biometric modalities are in varying stages of maturity in terms of implementation experiences.

For physical security, a variety of biometric modalities come to mind, but the five most popular physical access modalities in use today are: (1) facial recognition, (2) fingerprint/palm print, (3) hand geometry, (4) iris recognition, and (5) vein pattern recognition.

Facial Recognition - Facial recognition is the most natural means of identity recognition. Facial recognition systems attempt to find recognizable facial characteristics, reduce the key features to digital representations, and match them against known facial templates. Although various techniques can be used, facial recognition systems tend to emphasize facial regions that are less susceptible to alteration, such as the areas surrounding the cheekbones, upper outlines of eye sockets, the distance between the eyes, and the sides of the mouth.

Facial recognition systems can process a two-dimensional or three-dimensional camera image, depending on the system. Face scanning can be accomplished at a distance for clandestine surveillance or in close proximity to the subject. Two-dimensional facial recognition systems have not achieved high accuracy relative to some other biometric techniques, but they are constantly improving. Three-dimensional facial recognition is not as dependent on lighting conditions or varied poses, including nonfrontal angles. Three-dimensional systems are still developing, but they have the potential for high accuracy.

The advantages of facial recognition include high public acceptance of the modality, commonly available sensors (e.g., cameras), not physically intrusive, and the ease with which humans can verify the results. A key advantage to facial recognition is that this biometric identifier can be used at any venue in which one can mount a camera. An interesting by-product of this biometric is that the system administrator can retrieve a visual record of unauthorized attempts at entry. The disadvantages include its susceptibility to "spoofing" in large databases, as the face can be obstructed; its sensitivity to lighting, facial expressions, and pose; its large templates (approximately 3,000 bytes or more); and the reality that faces do change with age.

Fingerprint - Fingerprinting is the oldest biometric method in use today; due to its significant head start, it is the most widely used biometric modality. Fingerprints are based on physical dermal structures defined before birth. The pattern of furrows and ridges on the surface of each finger (e.g., local ridge characteristics that occur at a ridge bifurcation or a ridge ending) and image density are unique to each individual. The print pattern of a finger's top joint (the distal interphalangeal joint) is the primary focus.

Fingerprint-based systems work by scanning the tips of one or more fingers and comparing the scans of the finger against known images—the pre-established fingerprint template created during program enrollment. Traditional fingerprint sensing systems use a variety of techniques to capture a fingerprint image including capacitive, ultrasound, and optical methods.

Fingerprint (FP) scanning has several advantages. Given its history and common use, most people understand the concept, and training is minimized. The sensors used in fingerprint applications tend to be quite small, allowing some very useful form factors for FP scanners. The FP templates are also small, enabling a greater volume of template storage in limited memory situations, as well as enabling a very fast retrieval process. Most types of FP scanning equipment are relatively inexpensive.

Fingerprint scanning does have an extensive set of limitations that should be considered. Biometric industry authorities indicate that between 2% and 5% of the general population has some physical limitation in regard to using fingerprint imaging technology. Fingerprint ridges deteriorate with age and wear. Some occupational activities, such as aggressively washing one's hands multiple times a day (e.g., surgeons) or constantly placing one's fingers in strong chemicals (e.g., hair beauticians), can erode one's fingerprints over time.

Very similar to fingerprint recognition, palm print recognition measures the prints in one's palm to verify identity. Palm print recognition also has a similar set of advantages and limitations. Since the palm is larger, more distinctive features can be acquired in comparison with fingerprints. On the other hand, palm print scanners tend to be bulkier than fingerprint scanners and are usually more expensive. Many commercial fingerprint system providers have added palm print scanning to their biometric lineup of products.

Hand Geometry - Biometric systems based on hand geometry focus on the physical structure (lengths, widths, thicknesses, and angles of the fingers and palm) of an outstretched hand. The human hand has 27 bones, and it provides adequate anatomical features for measurement to enable verification. Typically, a user places his or her hand on a reader that is studded with guide pegs. The advantages of hand geometry are that it is intuitively easy to use, it typically uses 9–20 bytes of data for its templates (the smallest template of any biometric modality), its error rates are very low for false reject and failure to enroll, and it has fewer privacy concerns than fingerprint or face recognition.

Hand geometry devices can function in extreme conditions, withstand wide temperature variances, and are not impacted by dirty hands or dusty environments. The modality is well suited for industrial locations such as warehousing or some manufacturing facilities (for physical access control and time and attendance applications), where its simplicity is a positive. Moreover, hand geometry can be readily combined with other biometrics, such as fingerprints and vein pattern recognition of the hand or fingers.

Iris Recognition - Iris recognition systems use small, high-quality, near-infrared cameras to capture a black and white, high-resolution, high-contrast photograph of the iris. The near infrared illumination reveals patterns even for dark irises with no discernible patterns during visible light. Once the image is captured, the iris's elastic connective tissue is analyzed, and the distinctive features are extracted and translated into a digital form. Iris-based systems are relatively nonintrusive and are hygienic.

The iris is the annular region of the eye bounded by pupil at its center and by the sclera (white of the eye) on its outer side. Every iris is distinct. An iris is highly stable over time, and it is less subject to wear or injury than most other measurable body parts. The iris offers a data-rich structure composed of fibrous and vascular tissue including freckles, furrows, pits, rings, corona, and striations—all of which can be measured and the intraspatial relationships gauged. The detail in the texture of the iris is established before birth, and it appears to be caused by random processes, referred to as chaotic morphogenesis.

Iris scanners can measure the characteristics in the iris at a distance of a meter or more. The muscles in the iris control the amount of light entering the pupil and thus regulate the size of the pupil. The iris reacts to the stimulus of light with involuntary reflexes throughout the iris muscles. Some iris systems use this in a challenge/response effort to guarantee a living eye and not an artificial image. Iris scanning was specifically designed for physical access control applications.

Vein Pattern Recognition - Based on the unique patterns of veins in one's finger or hand, vein pattern recognition (VPR), also referred to as vascular pattern recognition, provides ease of use, a high level of accuracy, small readers, and a secure and hygienic approach. It uses near-infrared light generated from a bank of LEDs projected through an individual's skin to enable a high-contrast matching of vein patterns (e.g., vein branching points, branching angles, etc.) in one's hand or finger.

VPR systems scan the deoxygenated veins in one's palm, back of the hand, or fingers; extract key pattern features via contactless near-infrared optical sensor systems; digitize the extracted pattern recognition; and then match the transaction templates to the respective pre-established enrollment template. By measuring the veins under the skin with near-infrared spectroscopic imaging, it is very difficult for unauthorized persons to observe or capture this pattern, rendering VPR a highly secure method of identity verification.

VPR systems have some very powerful advantages. Vein pattern sensors look below the skin and they generally do not have issues with minor cuts and moisture. VPR systems reveal no significant performance degradation when measuring sweating or mildly dirty hands. They demonstrate very high accuracy rates and they are very difficult to spoof since blood needs to flow to register an image. Only a slight portion of the hand makes contact with the scanning device or its guideposts in order to align the finger or hand for consistent imaging. Since users do not touch the sensor surface and some vein pattern scanners are totally contactless, they are considered hygienic. VPR systems are easy to use and require only a moderate level of training on the part of the user.

As with all biometrics, VPR systems have their limitations. They can be impacted by direct sunlight or other ambient bright light; that is why some VPR systems have been positioned primarily for indoor use. However, many VPR system providers have designed coverings for outside access systems; some even have semitransparent coverings to limit ambient light indoors.

Multibiometric Systems - The concept of multibiometric systems has been used commercially since the late 1990s. A multibiometric system is one that uses multiple biometric sources to improve its overall performance. using a multibiometric system can increase security (e.g., by improving accuracy) or broaden support for and acceptance by the user population by offering alternatives. Multiple biometric techniques can be integrated into one security system to achieve better the stringent performance requirements imposed by some high-security applications, to identify imposters more readily, and to decrease the opportunities for imposters to spoof the system.

Multibiometric system might use any of the following six scenarios (starting at the top and continuing clockwise):

- Multiple sensors producing multiple samples of a single biometric trait to assuage noisy sensor data so that different sensors (e.g., optical and chip-based sensors for fingerprinting) for the same biometric identifier might be used to improve performance

- Multiple representations from the same biometric trait (e.g., minutiae-based vs. filter-based fingerprint systems) involving different approaches to feature extraction and matching

- Multiple samples of the same biometric trait using the same instance (e.g., same finger or same hand)

- Multiple identifiers, usually referred to as multimodal biometrics (e.g., using fingerprint and finger vein pattern recognition). Multimodal systems are arguably the most powerful type of multibiometric system. Indeed, multimodal systems analyze the evidence from multiple sources for verifying an individual's identity or for identifying an individual from a database, and generally multimodal systems provide superior recognition performance over unimodal biometric systems.

- Using "soft biometrics" such as gender, height, or eye color as a way to strengthen performance and accelerate processing time.

- Sampling multiple instances within the same modality (also called intramodal) such as different fingers or both palms for vein pattern recognition, which can help avoid spoofing in a challenge/response authentication.

Multimodal systems usually require more time and effort for users to enroll and to verify themselves. They also introduce a new level of complexity. Due to considerations of information integration, total cost, and end-user training, past successes with multimodal systems have been limited primarily to high-security facilities where cost issues are not a prime consideration and where users are motivated to master these systems.

The choice of multiple integration strategies depends primarily on an enterprise's requirements as well as the types of applications supported, the correlations among the biometric identifiers, and, of course, the costs incurred. These techniques provide multiple corridors of security checks that can be performed simultaneously or sequentially. Multiple biometric techniques combine multiple factors of evidence to enable better decisions.

Deploying Biometrics

Prior to deploying a biometric system, one must plan how the system will be used and must render some decisions on the best way to effect template storage, proper enrollment techniques, and daily biometric transaction use. And one should always build in privacy-enhancing features from the beginning.

Enrollment registers an individual to a biometric database for the first time. This is the process in which a user presents a biometric sample for the system to convert to a reference template and to store it in the biometric system database along with a proxy for his or her identity. The user's initial biometric sample is collected, assessed, processed, and stored. To a large degree, enrollment helps determine the ultimate accuracy of future matches.

Generally, no two reads from any biometric reader are exactly the same, and thus no two templates from the same person are exactly the same. Small variations in one's positioning, the distance from the sensor to an individual's identifying feature, the subject's interface with the sensor, and environmental conditions (humidity, temperature, sunlight, etc.) contribute to rendering a template unique. Each time biometric data are extracted, they are used to create a unique sample template for comparison to the reference template. The quality of each template is critical to the success of the overall system. The better the quality of the templates is, the more accurate will be the overall system and the lower the error rate.

Enrollment is the most crucial stage of the biometric process. Nothing can influence the successful use of the biometric system more than a proper enrollment. If one fails to capture the biometric trait properly and create an accurate reference template, then subsequent attempts to match templates will fail, and that will continue through the biometric life cycle for that individual. Thus, a weak enrollment process may lead to system inaccuracies and inconsistencies, as well as inadvertently creating an unreliable authentication infrastructure.

During the enrollment process a user record is created. That user record consists of an identifier and the biometric template, both of which should be encrypted (Figure 11.8). The identifier links the template and the user. A single user can be associated with various identifiers, which may lead to multiple roles in the biometric system for the attribution of rights and privileges. This also prevents an attacker from taking someone else's user credential by attempting to link his identifier to it.

A *verification transaction* is any application that requires individuals to authenticate a claimed identity. Moreover, verification activities tend to be self-service based, transaction oriented, and unsupervised. The biometric system captures an individual's biometric image and then extracts the unique characteristics from the individual's image to create the user's sample template. The biometric system then compares the sample template to the template stored at enrollment (e.g., the reference template), and in most systems, a numeric matching score is generated based on the percentage of similarity between the sample and reference templates.

Depending on the predetermined threshold value, the identity verification score may or may not meet the probability threshold for a match. Comparison of sample data and reference templates results in a biometric system match decision—that is, a yes or no match. Verification tasks are considered to be relatively simple and straightforward. The entire process for a verification application generally takes only a few seconds, depending on the biometric modality employed and the specific implementation. Some systems allow multiple sample retakes to produce a match. If an individual is denied, human interaction may be needed, and the denied person may need to follow a manual process for authentication.

Privacy

Although biometric technology can enhance and support most commonly held notions of privacy, it cannot guarantee it. Clearly, the topic of biometrics often raises the public's angst regarding privacy. There has long existed within some groups an inherent discomfort with biometrics; they have a perception that biometrics represents privacy intrusiveness. As we have mentioned previously, we leave our fingerprints on everything we touch, and there are limited prohibitions against someone taking our photographs or recording our voices, each of which can be accomplished legally without our awareness or consent, depending on the circumstances.

At the vortex of most privacy issues are concerns about the potential misuse of biometrics, such as a biometric system pointing to other information pertaining to an individual. Thus, an intrusion on one's privacy tends to originate from the inherent misuse of the technology, not from the biometric application itself. Identity verification applications may be less threatening to privacy (than, say, surveillance applications) simply because the individual knowingly enrolls in a given system and thereby gives permission to use his or her biometric characteristics for a specific purpose. However, that information can still be misused.

Biometrics can be privacy threatening if safeguards are not designed into biometric systems from the beginning. It really depends on how the biometric system is deployed, how the biometric templates are stored, and the strength and vigilance of the safeguards that are put in place to guard against third-party access or linking inappropriately to other systems.