6.2.7 Biometrics and Authentication Technologies Facts

This lesson covers the following topics:

- Biometric authentication
- Authentication technologies

Biometric authentication is based on a unique physical attribute or characteristic. This type of authentication requires capturing and storing a unique physical attribute with a biometric system. This initial capture is known as enrollment. Subsequent authentication attempts are tested against the stored biometric template. For biometric authentication to be a viable security mechanism, it must conform to the following parameters:

Parameter	Description
Universal	Does each person have the physical attribute being measured?
Unique	Is the physical attribute distinctive enough that it can be used to distinguish between individuals?
Permanent	How well does the specified attribute hold up to aging?
Collectible	How easy is it to acquire this measurable attribute?
Circumvention	Can the attribute be easily circumvented?
Accuracy	Are the results accurate? Accuracy is extremely critical in a biometric system. Most devices can be configured for increased or reduced sensitivity. Note the following as it relates to biometric accuracy: ▪ False rejection (or false negative) occurs when a person who should be allowed access is denied access. The false rejection rate (FRR) is a measure of the probability that a false negative will occur. ▪ False acceptance (or false positive) occurs when a person who should be denied access is allowed access. The false acceptance rate (FAR) is a measure of the probability that a false positive will occur. False positives are more serious than false negatives and represent a security breach because unauthorized persons are allowed access. ▪ A crossover error rate, also called the equal error rate, is the point at which the number of false positives matches the number of false negatives in a biometric system. It is advisable to select the system with the lowest crossover error rate within your budget.

Biometric information can be collected for each of the following:

Method	Description
Fingerprints	Fingerprints are made up of patterns of ridges and valleys. Fingerprint scanners analyze these patterns and convert them into a numerical format that can be stored for future comparison.

Retina	A retina is the back portion of the eye that is sensitive to light. Numerous capillaries move blood to the retina and these capillaries create a unique pattern. A retinal scanner shines infrared light into an eye and measures the amount of reflection. The vessels in the retina absorb infrared light so that the reflection pattern can be stored for future identification.
Iris	The iris is the colorful portion of the eye around the pupil. Infrared light lights up the iris, and the scanner captures images of its unique patterns.
Facial	Facial scanning creates a map of 80 points on an individual's face. The distances measured on this map can be used to identify the person in the future. Measurements could include the distance between eyes, the shape of a nose, the size of the cheekbones, etc.
Voice	Voice recognition systems analyzes a person's voice for things like pitch, intensity, and cadence. These systems can be text dependent or text independent. Text-dependent authentication requires a specific phrase to be spoken. This could be a pre-determined phrase, or it could be randomly generated. Text-independent authentication uses any speech content.
Vein	Vein recognition scanners use infrared light to determine the vein pattern in your palm. Like a fingerprint, this pattern differs from one person to the next and does not change. The scanner converts the collected data into a code that is encrypted and assigned to you. The benefits of vein biometrics are: ▪ Veins are internal so they cannot be altered or covered as easily as hands or a face could be. ▪ Because a palm is larger than an eye or a finger, more data points can be collected. This provides a higher rate of accuracy. ▪ Because veins are internal, they are harder to replicate and can only be captured in close proximity.
Gait	Gait recognition analyzes the way that people walk. Each person has a unique way of walking. Several factors determine your gait, including: ▪ Height, weight, and body proportions ▪ Age ▪ Health (diseases or disorders) ▪ Personality or emotions When analyzing gait, the following are measured: ▪ Stride ▪ Step ▪ Speed ▪ Hip and foot angle ▪ Cadence Data is gathered using sensors, cameras, or wearable devices. The gait recognition system creates a digital signature that can be stored or compared to existing data. Gait recognition systems are still fairly new and, as with most biometric systems, should not be used as a stand-alone method of identification.

If you are considering implementing biometrics, keep in mind the following:

- Some biometric factors are unique. This is true even between identical twins.
- When a biometric is used by itself, it is no more secure than a strong password. A single successful attack can subvert a biometric in much the same way that a single successful attack can subvert a password.
- Biometric attacks need not be physically harmful (such as cutting off a finger) but can include a wide variety of realistic reproductions that fool the biometric reader device.
- The most important consideration for a biometric device is accuracy.
- When a biometric device has its sensitivity set too high, it can result in numerous false-negative rejections where authorized users are not recognized.
- To use a biometric, new users must go through a physical enrollment process that is more complex and time consuming than the enrollment process for a password-only system.
- Biometric enrollment requires new users to prove their identity to a user administrator. The new user must then provide the first example of their biometric to a reader device under the supervision of the user administrator. This first example is digitized and stored as a reference template. All future uses of the biometric compare the contemporary biometric sample offered with the historically recorded template.

Authentication Technologies

The following chart reviews several technologies that can be used for multifactor authentication:

Technology	Description
Short Message Service (SMS)	Short Message Service (SMS) authentication uses SMS messaging to send a one-time code or password to a known user of an account in order to verify their identity. This requirement can be requested at every login, at every time the user signs into a new device or browser, or at timed intervals.
Phone Call	Similar to SMS, the user receives a phone call with the one-time code or password.
Authentication Applications	Authentication applications are third-party tools that organizations use to authenticate their users, especially those working remotely. An authenticator app, typically installed on a smartphone, provides a new six-to-eight digit code every 30 seconds. This passcode, along with your username and password, provides additional verification that you are who you say you are. Another similar method that you may have used is a one-time password. Some banks use this method to allow ATM withdrawals without using a debit card. An application or token creates a one-time password. This password only works for a single login. After that, the password expires. There are two different methods for creating one-time passwords: ▪ HMAC-based one-time password (HOTP): This type of one-time password uses a mathematical algorithm to create a new password based on the previous password that was generated. ▪ Time-based one-time password (TOTP): This one-time password is generated by sending a shared secret key and the current time through an algorithm. This generated password is valid for only a short period, typically thirty seconds. After that, a new one-time password is generated using the same method.
Push Notifications	Push notifications can also be used to grant access to an account. Whenever you log into your account, you enter your username. But instead of a password, you receive an access request notification on your mobile device. You can choose to either approve or decline this request.