Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/28/2022 8:23:11 pm • Time spent: 02:12

Score: 100% Passing Score: 80%

Question 1: ✓ Correct

Which of the following are examples of Something You Have authentication controls? (Select two.)

- ➡ ☑ Smart card
- ☐ Voice recognition
- ☐ PIN
- ☐ Handwriting analysis
- ➡ ☑ Photo ID
- ☐ Cognitive question

EXPLANATION

Something You Have authentication controls include physical items that you have on your possession, such as a smart card, photo ID, token device, or swipe card.

Something You Know authentication requires you to provide a password, PIN, pass phrase, or the answer to a cognitive question (such as your mother's maiden name).

Something You Are authentication uses a biometric system, such as a fingerprint, retina scan, voice recognition, keyboard, or writing recognition.

REFERENCES

6.2.3 Authentication Facts

q_authent_have_secp7.question.fex

Question 2: ✓ Correct

Which of the following identification and authentication factors are often well known or easily discovered by others on the same network or system?

➡ ● Username

○ PGP secret key

○ Biometric reference profile

○ Password

EXPLANATION

The username is typically the least protected identification and authentication factor. Therefore, usernames are often well known or easy to discover, especially by others on the same network or system. The key to maintaining a secure environment is to keep authentication factors secret. Often, usernames are constructed using a standard naming convention, such as first and middle initials plus the full last name, or the first name and last name separated by a period. If these simple construction conventions are known, building usernames from an employee list is very simple.

Passwords, your PGP secret key, and your biometric reference profile are less likely to be well known or easy to discover.

REFERENCES

6.2.3 Authentication Facts

q_authent_identity_secp7.question.fex

Question 3: ✓ Correct

Which of the following is a password that relates to things that people know, such as a mother's maiden name or a pet's name?

- ➡ ● Cognitive
- ○ One-time
- ○ Dynamic
- ○ Passphrase

EXPLANATION

Cognitive passwords relate to things that people know, such as a mother's maiden name or a pet's name.

Dynamic passwords change upon each consecutive login.

One-time passwords are only valid for a single use.

A passphrase is a password long enough to be a phrase.

REFERENCES

6.2.3 Authentication Facts

q_authent_know_01_secp7.question.fex

Question 4: ✓ Correct

What type of password is *maryhadalittlelamb?*

- ○ Static
- ○ Cognitive
- ○ Composition
- ➡ ● Passphrase

EXPLANATION

A passphrase is a password long enough to be a phrase, such as *maryhadalittlelamb*.

Cognitive passwords relate to things that people know, such as a mother's maiden name or a pet's name,

A static password is created by a user and overseen by an administrator.

Composition passwords are created by the system and are usually two or more unrelated words divided by symbols on the keyboard.

REFERENCES

6.2.3 Authentication Facts

q_authent_know_02_secp7.question.fex

Question 5: ✓ Correct

Match the authentication factor types on the left with the appropriate authentication factor on the right. Each authentication factor type may be used more than once.

PIN

✓ Something You Know

Smart card

✓ Something You Have

Password

✓ Something You Know

Retina scan

✓ Something You Are

Fingerprint scan

✓ Something You Are

Hardware token

✓ Something You Have

Passphrase

✓ Something You Know

Voice recognition

✓ Something You Are

Wi-Fi triangulation

✓ Somewhere You Are

Typing behaviors

✓ Something You Do

EXPLANATION

Something You Know authentication requires you to provide a password or some other data that you know. This is the weakest type of authentication. Examples of Something You Know authentication controls include:

- Passwords, codes, or IDs
- PINs
- Passphrases (long multi-word passwords)

Something You Have (also called token-based authentication) is authentication based on something users have in their possession. Examples of Something You Have controls include:

- Swipe cards
- Photo IDs
- Smart cards
- Hardware tokens

Something You Are authentication uses a biometric system. A biometric system attempts to identify a person based on metrics or a mathematical representation of the subject's biological attribute. Biometric systems are the most expensive and least accepted system type, but are generally considered the most secure form of authentication. Common attributes used for biometric systems include:

- Fingerprints
- Hand topology (side view) or geometry (top-down view)
- Palm scans
- Retina scans
- Iris scans
- Facial scans
- Voice recognition

Somewhere You Are authentication (also known as geolocation) is a supplementary authentication factor that uses physical location to verify a user's identity. Examples of implementations include:

- An account is locked unless the user has passed through the building's entrance using an ID card.
- If the user is within RFID range of the workstation, authentication requests are allowed.
- GPS or Wi-Fi triangulation location data is used to determine a device's location. If the user and the device are in a specified location, authentication requests are allowed. If not, the device is locked.

Something You Do is a supplementary authentication factor that requires an action to verify a user's identity. Example implementations include:

- Analyzing a user's handwriting sample against a baseline sample before allowing authentication.
- Analyzing a user's typing behaviors against a baseline sample before allowing authentication.

REFERENCES

6.2.3 Authentication Facts

q_authent_multifactor_secp7.question.fex

Question 6: ✓ Correct

A smart card can be used to store all but which of the following items?

- ○ Digital signature
- ○ Identification codes
- ➡ ◉ Biometric template original
- ○ Cryptography keys

EXPLANATION

A smart card cannot store biometric template originals, as those are physical components of the human body.

A smart card can store digital signatures, cryptography keys, and identification codes.

REFERENCES

6.2.3 Authentication Facts

q_authent_smart_secp7.question.fex

▼ Question 7: ✓ Correct

Which of the following are disadvantages of biometrics? (Select two.)

- □ Biometric factors for identical twins are the same.
- ➡ ☑ When used alone, they are no more secure than a strong password.
- □ They can be circumvented using a brute force attack.
- ➡ ☑ They have the potential to produce numerous false negatives.
- □ They require time synchronization.

EXPLANATION

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 based on physical harm (such as cutting off a finger), but can include a wide variety of realistic reproductions that fool the biometric reader device.

When a biometric device's sensitivity is set too high, it results in numerous false rejections, or false negatives, (when authorized users are not recognized and are therefore rejected).

The advantage of biometrics is that no two people have the same biometric characteristics. Most characteristics, such as retinal patterns, are unique, even among identical twins. A password can be discovered using a brute force attack, but there is no such attack against biometrics.

REFERENCES

6.2.7 Biometrics and Authentication Technologies Facts

q_sso_biometrics_01_secp7.question.fex

Question 8: ✓ Correct

What is the MOST important aspect of a biometric device?

- ○ Size of the reference profile
- ➡ ● Accuracy
- ○ Enrollment time
- ○ Throughput

EXPLANATION

The most important aspect of a biometric device is accuracy. If an access control device is not accurate, it does not offer reliable security.

Enrollment time is how long it takes for a new user to be defined in the biometric database. Typically, an enrollment time less than two minutes is preferred. The size of the reference profile is irrelevant in most situations. Throughput is how many users a biometric device can scan and verify within a given time period. Typically, a throughput of 10 users per minute is preferred.

REFERENCES

6.2.7 Biometrics and Authentication Technologies Facts

q_sso_biometrics_02_secp7.question.fex

Question 9: ✓ Correct

Which of the following defines the crossover error rate for evaluating biometric systems?

○ The rate of people who are given access when they should be denied access.

○ The number of subjects or authentication attempts that can be validated.

○ The rate of people who are denied access when they should be allowed access.

➡ ● The point where the number of false positives matches the number of false negatives in a biometric system.

EXPLANATION

The crossover error rate, or the equal error rate, is the point where the number of false positives matches the number of false negatives in a biometric system.

A false negative (or Type I error) occurs when a person who should be allowed access is denied access.

A false positive (or Type II error) occurs when a person who should be denied access is allowed access.

The processing rate, or system throughput, identifies the number of subjects or authentication attempts that can be validated.

REFERENCES

6.2.7 Biometrics and Authentication Technologies Facts

q_sso_crossover_secp7.question.fex

▼ Question 10: ✓ Correct

Which of the following terms is used to describe an event in which a person who should be allowed access is denied access to a system?

- ➡ ● False negative
- ○ False acceptance
- ○ False positive
- ○ Error rate

EXPLANATION

A false negative occurs when a person who should be allowed access is denied access.

A false positive occurs when a person who should be denied access is allowed access.

The processing rate, or system throughput, identifies the number of subjects or authentication attempts that can be validated.

The crossover error rate, also called the equal error rate, is the point where the number of false positives matches the number of false negatives in a biometric system.

REFERENCES

6.2.7 Biometrics and Authentication Technologies Facts

q_sso_false_rej_secp7.question.fex