Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/7/2022 8:30:37 pm • Time spent: 03:59

Score: 70%

Passing Score: 80%

Question 1: ✔ Correct

Cryptographic systems provide which of the following security services? (Select two.)

- [ ] Cryptanalysis
- [x] Confidentiality
- [x] Non-repudiation
- [ ] Encryption
- [ ] Decryption

EXPLANATION

Cryptography is the science of converting data into a secret code to hide a message's meaning during transmission. Cryptographic systems provide the following security services:

- Confidentiality by ensuring that only authorized parties can access data.
- Integrity by verifying that data has not been altered in transit.
- Authentication by proving the identity of the sender or receiver.
- Non-repudiation by validating that communications have come from a particular sender at a particular time.

Encryption is the process of using an algorithm to transform data from plaintext to ciphertext in order to protect the confidentiality, integrity, and authenticity of the message.

Decryption is the procedure used to convert data from ciphertext into plaintext.

Cryptanalysis is the method of recovering original data that has been encrypted without having access to the key used in the encryption process.

REFERENCES

7.2.2 Cryptography Uses and Limitations Facts

q_cryp_limits_crypto_secp7.question.fex

Question 2: ✔ Correct

You have downloaded a file from the internet. You generate a hash and check it against the original file's hash to ensure the file has not been changed. Which information security goal is this an example of?

- Non-repudiation
- Authenticity
- Confidentiality
- Integrity

EXPLANATION

Creating a hash of a file can be used to validate that the file has not been altered. This validates the integrity of the file.

Applying a digital signature proves that the file is authentic and comes from the correct person.

Applying a digital signature provides non-repudiation. This means that the sender cannot later deny having sent the file.

Confidentiality is achieved through the encrypting of data or obfuscation of data.

REFERENCES

7.2.2 Cryptography Uses and Limitations Facts

q_cryp_limits_integrity_secp7.question.fex

Question 3: ✔ Correct

Which of the following are true of Triple DES (3DES)?

- Can easily be broken
- Uses 64-bit blocks with 128-bit keys
- Key length is 168 bits
- Uses the Rijndael block cipher

EXPLANATION

Triple DES:

- Applies DES three times
- Uses a 168-bit key

Advanced Encryption Standard (AES) uses the Rijndael block cipher.

DES can easily be broken.

International Data Encryption Algorithm (IDEA) uses 64-bit blocks with 128-bit keys.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

7.2.2 Cryptography Uses and Limitations Facts

q_cryp_limits_length_secp7.question.fex

Question 4: ✕ Incorrect

When a sender encrypts a message using their own private key, which security service is being provided to the recipient?

- Non-repudiation
- ~~Confidentiality~~
- Availability
- Integrity

EXPLANATION

When a sender encrypts a message using their own private key, the security service of non-repudiation is being provided to the recipient. The encrypted message can be freely decrypted using the public key. Because only the sender knows the private key, encrypting the message with the private key proves that only the sender could have sent the message.

Integrity is provided when hashing is used. Because the public key is freely available, the encryption does not provide confidentiality (anyone with the public key could read the message contents). Availability is not provided by any form of cryptography.

REFERENCES

7.2.2 Cryptography Uses and Limitations Facts

q_cryp_limits_non_rep_secp7.question.fex

Question 5: ✔ Correct

Which of the following is a direct integrity protection?

- Digital signature
- Digital envelope
- Asymmetric encryption
- Symmetric encryption

EXPLANATION

A digital signature is a direct integrity protection. It includes the use of hashing, which detects changes to integrity.

Digital envelopes, symmetric encryption, and asymmetric encryption do not provide direct integrity protection, nor do they use hashing to provide integrity protection.

REFERENCES

5.10.3 Network Application Facts

7.2.3 Combining Cryptographic Methods

7.2.5 Cryptographic Implementation Facts

q_comb_cryp_digital_01_secp7.question.fex

Question 6: ✔ Correct

What is the most obvious means of providing non-repudiation in a cryptography system?

- Shared secret keys
- Hashing values
- Public keys
- Digital signatures

EXPLANATION

Digital signatures, which are private keys from an asymmetric cryptographic system, are the most obvious means of providing non-repudiation. Only a single person is in possession of their private key. If a message is found with their digital signature, they are the only user who could possibly have created and transmitted it.

Public keys are useful for restricting delivery, such as using them as digital envelopes, but they don't provide non-repudiation. Hashing values protect integrity, but they don't provide non-repudiation. Shared secret keys do not provide true non-repudiation because two entities hold copies of the shared key.

REFERENCES

5.10.3 Network Application Facts

7.2.3 Combining Cryptographic Methods

7.2.5 Cryptographic Implementation Facts

q_comb_cryp_digital_02_secp7.question.fex

Question 7: ✔ Correct

Which form of cryptography is best suited for bulk encryption because it is so fast?

- Public key cryptography
- Hashing cryptography
- Symmetric key cryptography
- Asymmetric cryptography

EXPLANATION

Symmetric cryptography is best suited for bulk encryption because it is much faster than asymmetric cryptography.

Hashing is not used for encryption; it is only used to verify the integrity of data. Public key cryptography, also known as asymmetric cryptography, is best suited for small amounts of data. Often, asymmetric cryptography is used to exchange symmetric cryptography keys, and then the symmetric cryptography keys are used to encrypt communication traffic.

REFERENCES

7.2.5 Cryptographic Implementation Facts

q_comb_cryp_encrypt_secp7.question.fex

Question 8: ✕ Incorrect

Your computer system is a participant in an asymmetric cryptography system. You've crafted a message to be sent to another user. Before transmission, you hash the message and then encrypt the hash using your private key. You then attach this encrypted hash to your message as a digital signature before sending it to the other user.

Which protection does the private key-signing activity of this process provide?

- Non-repudiation
- Confidentiality
- Availability
- ~~Integrity~~

EXPLANATION

Signing a digital signature with the private key provides non-repudiation.

A digital signature activity as a whole does not provide protection for confidentiality because the original message is sent in clear form. Hashing of any sort at any time, including within a digital signature, provides protection for integrity. No form of cryptography provides protection for availability.

REFERENCES

7.2.5 Cryptographic Implementation Facts

q_comb_cryp_non_rep_secp7.question.fex

Question 9: ✕ Incorrect

What is the main function of a TPM hardware chip?

- ~~Provide authentication credentials on a hardware device~~
- Perform bulk encryption in a hardware processor
- Control access to removable media
- Generate and store cryptographic keys

EXPLANATION

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard. This hardware is used to store and generate cryptographic keys. These keys are used for encryption and authentication, but the TPM does not perform the actual encryption.

A smart card is a hardware device containing a digital certificate. The smart card can be used for authentication. Special hardware processors perform bulk encryption in hardware rather than software. These processors typically encrypt data using AES or encrypt network traffic using IPsec.

REFERENCES

- 4.2.1 Operating System Hardening
- 4.2.2 Hardening Facts
- 4.2.3 Hardening an Operating System
- 4.2.4 Managing Automatic Updates
- 4.2.6 Configuring Microsoft Defender Firewall
- 4.2.8 Configuring Windows Defender with Firewall Advanced Security
- 7.2.4 Hardware-Based Encryption Devices
- 7.2.5 Cryptographic Implementation Facts
- 7.4.9 File Encryption Facts

q_comb_cryp_tpm_01_secp7.question.fex

Question 10: ✔ Correct

Which of the following functions are performed by a TPM?

- Provide authentication credentials
- Encrypt network data using IPsec
- Create a hash of system components
- Perform bulk encryption

EXPLANATION

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard. This hardware is used to store and generate cryptographic keys. The TPM also generates hash values of system components. The hash value verifies that startup components have not been modified. Because each system has a unique hash value, the hash can also be used as a form of identification for the system.

Keys generated by the TPM are used for encryption and authentication, but the TPM does not perform the actual encryption. A smart card is a hardware device containing a digital certificate. The smart card can be used for authentication. Special hardware processors perform bulk encryption in hardware rather than software. These processors typically encrypt data using AES or encrypt network traffic using IPsec.

REFERENCES

- 4.2.1 Operating System Hardening
- 4.2.2 Hardening Facts
- 4.2.3 Hardening an Operating System
- 4.2.4 Managing Automatic Updates
- 4.2.6 Configuring Microsoft Defender Firewall
- 4.2.8 Configuring Windows Defender with Firewall Advanced Security
- 7.2.4 Hardware-Based Encryption Devices
- 7.2.5 Cryptographic Implementation Facts
- 7.4.9 File Encryption Facts

q_comb_cryp_tpm_02_secp7.question.fex