Exam Report: 9.3.4 Practice Questions

Date: 1/28/2020 3:49:50 pm
Time Spent: 8:07

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 67%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

What is the main function of a TPM hardware chip?

➡ ● Generate and store cryptographic keys

○ Perform bulk encryption in a hardware processor

○ Control access to removable media

○ Provide authentication credentials on a hardware device

Explanation

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard that stores and generates 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

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_01]

Question 2: Incorrect

Which of the following functions are performed by the TPM?

➡ ○ Create a hash of system components

○ Encrypt network data using IPSec

● ~~Provide authentication credentials~~

○ Perform bulk encryption

Explanation

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard and stores and generates 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 will have 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

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_02]

Question 3: Correct

Which of the following is a direct protection of integrity?

➡ ● Digital signature

○ Digital envelope

○ Asymmetric encryption

○ Symmetric encryption

Explanation

A digital signature is a direct protection of integrity, as 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

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_03]

Question 4: Correct

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

➡ ● Digital signatures

○ Public keys

○ Hashing values

○ Shared secret keys

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, then 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 for 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

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_04]

Question 5: Correct

When a sender encrypts a message using their own private key, what 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

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_05]

▼ **Question 6:** Incorrect

Which of the following statements is **true** when comparing symmetric and asymmetric cryptography?

● ~~Asymmetric key cryptography is quicker than symmetric key cryptography while processing large amounts of data.~~

○ Symmetric key cryptography should be used for large, expanding environments.

○ Symmetric key cryptography uses a public and private key pair.

➡ ○ Asymmetric key cryptography is used to distribute symmetric keys.

Explanation

Asymmetric key cryptography can be used to distribute symmetric keys. This is known as a *hybrid* cryptography system. A hybrid cryptography system combines the strengths of both the symmetric and asymmetric cryptography systems (meaning that symmetric systems can process large amounts of data relatively fast, and asymmetric systems can securely distribute keys).

Symmetric cryptography uses a single key pair, with each partner using the same key. Asymmetric cryptography uses a public and a private key pair. Symmetric key cryptography processing is about 1000 times faster than asymmetric cryptography. In large, expanding environments, managing keys with symmetric key cryptography is difficult.

References

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_06]