Exam Report: 3.3.5 Practice Questions - Section 3.3

Date: 11/24/2015 1:37:02 pm
Time Spent: 4:16

Candidate: Belskis, Tomas
Login: t0mas9lt

Overall Performance

Your Score: 40%

Passing Score: 80%

Certification Ranking

Within your class: Within your school: Nationally:

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

What type of key or keys are used in symmetric cryptography?

- A single key pair
- A shared private key
- Two unique sets of key pairs
- A unique key for each participant

Explanation

Symmetric cryptography uses a shared private key. Both communication partners must be in possession of the same key in order to exchanged encrypted data.

Asymmetric cryptography uses a unique key pair for each participant. This key pair consists of a public key and a private key.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm SP02_4-1 [13]]

Question 2: Correct

How many keys are used with symmetric key cryptography?

- One
- Two
- Four
- Five

Explanation

Private Key or Symmetric Cryptography uses a single *shared* key. Both communicating parties must possess the shared key to encrypt and decrypt messages. The biggest challenge to

Symmetric Cryptography is the constant need to protect the shared private key. This protection must be applied at all times, including the initial transmission of the shared key between the parties.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm SP02_4-1 [76]]

Question 3: Incorrect

Which of the following is **not** true concerning symmetric key cryptography?

- The key is not shared with other communication partners.
- Before communications begin, both parties must exchange the shared secret key.
- ~~Each pair of communicating entities requires a unique shared key.~~
- Both parties share the same key (which is kept secret).
- Key management is easy when implemented on a large scale.

Explanation

Key management is *difficult* when symmetric cryptography is implemented on a large scale. Because two users must share the same unique key to encrypt and decrypt data, even a small group of users would require the generation of a large amount of keys. The formula to determine the number of keys is n(n-1)/2.

With symmetric key cryptography:

- Both parties share the same key (which is kept secret).
- Before communications begin, both parties must exchange the shared secret key.
- The key is not shared with other communication partners.
- Each pair of communicating entities requires a unique shared key.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm SSCP-2 NEW [57]]

Question 4: Correct

Which of the following can be classified as a "stream cipher"?

- Twofish
- RC4
- Blowfish
- AES

Explanation

The most frequently used implementation of symmetric key stream ciphers is Ron's Code (or Ron's Cipher) v4, known as RC4. RC4 uses a variable key up to 256 bits and is commonly used with WEP and SSL. It uses the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA).

Blowfish, Twofish, and AES are all block ciphers.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm MCS11]

Question 5: Correct

You want to encrypt data on a removable storage device. Which encryption method would you choose to use the strongest method possible?

- RSA
- SHA-1
- AES
- 3DES

Explanation

AES is stronger and faster than 3DES when implemented with a large key size (256-bits). DES was one of the first symmetric encryption methods and is now obsolete (known weaknesses can be used to break the encryption). 3DES improves upon DES by applying the encryption three times. It is an acceptable alternative to DES.

RSA is an asymmetric encryption algorithm. Asymmetric encryption is typically not used for bulk encryption of data. SHA-1 is a hashing algorithm, not an encryption algorithm.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm SP08_5-1 8]

Question 6: Incorrect

Which of the following algorithms are used in symmetric encryption? (Select three.)

- [x] 3DES
- [ ] El-Gamal
- [ ] Blowfish
- [ ] Diffie-Hellman
- [x] AES

Explanation

3DES, AES, and Blowfish are symmetric encryption algorithms. 3DES is an update to the original DES algorithm and uses multiple keys and algorithm passes to improve security. AES is considered to be the replacement for the aging 3DES algorithm and was chosen by the National Institute of Standards and Technology (NIST) as the new government standard for encryption algorithms. The Blowfish algorithm is considered to be a very secure algorithm and uses a variable key length.

References

LabSim for Security Pro, Section 3.3.

[Questions.exm SP02_4-4 [76]]

Question 7: Incorrect

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

- [x] ~~Can easily be broken~~
- [x] Uses a 168-bit key
- [ ] Uses 64-bit blocks with 128-bit keys
- [ ] Is used in IPSec
- [ ] Uses the Rijndael block cipher

Explanation

Triple DES:

- Applies DES three times.
- Uses a 168-bit key.
- Used in IPSec as its strongest and slowest encipherment.

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

LabSim for Security Pro, Section 3.3.
[Questions.exm NEW [40]]

Question 8: Incorrect

Which of the following are true concerning the Advanced Encryption Standard (AES) symmetric block cipher? (Select two.)

- [ ] AES uses a variable-length block and key length (128-, 192-, or 256-bit keys).
- [x] ~~AES uses 8'128 bit keys in steps of 8 bits.~~
- [ ] AES uses the Rijndael block cipher.
- [ ] AES uses up to 16 rounds of substitution and transposition.

Explanation

AES is an iterative symmetric key block cipher that uses the following:

- The Rijndael Block Cipher, which is resistant to all known attacks.
- A variable-length block and key length (128-, 192-, or 256-bit keys).

Ron's Cipher v2 or Ron's Code v2 (RC2) uses 8'128 bit keys in steps of 8 bits. Twofish uses up to 16 rounds of substitution and transposition.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm NEW [74]]

Question 9: Incorrect

Which of the following symmetric block ciphers does **not** use a variable block length?

- Elliptic Curve (EC)
- ~~Advanced Encryption Standard (AES)~~
- Ron's Cipher v5 (RC5)
- International Data Encryption Algorithm (IDEA)

Explanation

International Data Encryption Algorithm (IDEA) does not use variable block lengths. In addition to IDEA, the following symmetric block ciphers also do not use variable block lengths:

- Data Encryption Standard (DES)
- Ron's Cipher v2 or Ron's Code v2 (RC2)
- Blowfish
- Twofish
- SkipJack

AES uses variable block lengths. RC5 uses 32-, 64- or 128-bit block lengths. Elliptic Curve (EC) is an asymmetric cipher.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm NEW [82]]

Question 10: Incorrect

Which of the following encryption mechanisms offers the *least* security because of weak keys?

- AES
- ~~IDEA~~
- DES
- TwoFish

Explanation

DES offers the least encryption security from the cryptography systems in this list. DES has a limitation of 56-bit keys, the weakest of those listed here. The strength of a cryptosystem lies not only in long keys but in the algorithm, initialization vector or method, the proper use of the keyspace, and the protection and management of keys.

AES (128, 192, 256 bit keys), TwoFish (up to 256 bit keys), and IDEA (128 bit keys) all support stronger keys than that of DES.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm SP [202]]

Question 11: Incorrect

Which version of the Rivest Cipher is a block cipher that supports variable bit length keys and variable bit block sizes?

- RSA
- RC2
- ~~RC4~~
- RC5

Explanation

RC5 is a block cipher that supports variable bit length keys and variable bit block sizes.

RC4 is a stream cipher. RC2 is limited to 64 bit blocks. RSA is not a Rivest Cipher, rather it is an asymmetric cryptography system developed by the same organization.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm SP [210]]

Question 12: Correct

Bob Jones used the RC5 cryptosystem to encrypt a sensitive and confidential file on his notebook. He used 32 bit blocks, a 64 bit key, and he only used the selected key once. He moved the key onto a USB hard drive which was stored in a safety deposit box. Bob's notebook was stolen. Within a few days Bob discovered the contents of his encrypted file on the Internet.

What is the primary reason why Bob's file was opened so quickly?

- Too small of a block size
- The decryption key was used to decrypt the files
- A birthday attack was used
- Weak key

Explanation

The primary reason for the quick failure of Bob's intended encryption protection was the use of a weak key. 64-bit RC5 keys can be broken in a very short amount of time, usually less than three days on a fast computer or a small network of distributed cracking agents. Bob should have used a larger key, at least 128 bits.

The birthday attack is used against hashing algorithms, not symmetric cryptography systems. The block size may have had some effect on the weakness of the protection, but not as much as the weak key. The decryption key was not used because it was moved to a removable device that was secured at a bank.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm SP [579]]

Question 13: Incorrect

You are concerned about the strength of your cryptographic keys, so you implement a system that does the following:

- The initial key is fed into the input of the bcrypt utility on a Linux workstation.

- The bcrypt utility produces an enhanced key that is 128 bits long.

The resulting enhanced key is much more difficult to crack than the original key.

Which kind of encryption mechanism was used in this scenario?

- Perfect forward secrecy
- DHE
- ~~Ephemeral keys~~
- Key stretching

Explanation

Key stretching has been used in this scenario. Key stretching strengthens weak encryption keys against exhaustive key search attacks. Using key stretching, the initial key is fed into an algorithm to create a stronger key. The enhanced key is usually at least 128 bits long, making it almost impossible to crack. Several commonly used key stretching algorithms include the following:

- PBKDF2
- bcrypt
- scrypt

Ephemeral keys are generated every time the key establishment process is executed and only exist for the lifetime of a specific communication session. *Perfect forward secrecy* can be implemented in public-key cryptography system so that random public keys are generated for each session. *DHE* refers to a Diffie-Hellman key exchange.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm RT-3.3-2]

Question 14: Incorrect

Which of the following is considered an out-of-band distribution method for private-key encryption?

- Copying the key to a USB drive
- ~~Using a private fiber network~~
- Using a key distribution algorithm
- Sending a secured e-mail

Explanation

Out-of-band distribution involves manually distributing the key, such as copying the key to a USB drive and sending it to the other party.

Sending an e-mail, using a key distribution algorithm, or using a private fiber network are all considered in-band distribution methods.

References

LabSim for Security Pro, Section 3.3.

[Questions.exm KMC 6.1-6]

Question 15: Correct

Match the symmetric key distribution mechanism on the left with the appropriate description on the right. Each distribution mechanism may be used once, more than once, or not at all.

The sender's key is sent to a recipient using a Diffie-Hellman key exchange.

✔ In-band distribution

The sender's key is copied to a USB drive and handed to the recipient.

✔ Out-of-band distribution

The sender's key is sent to the recipient using public-key cryptography.

✔ In-band distribution

The sender's key is burned to a CD and handed to the recipient.

✔ Out-of-band distribution

Explanation

Before communications can begin using symmetric encryption, both parties must exchange the shared secret key using a secure channel. Symmetric key encryption can use the following key distribution methods:

- *Out-of-band distribution* involves manually distributing the key, such as copying the key to a USB drive and sending it to the other party.
- *In-band distribution* can use a key distribution algorithm, such as Diffie-Hellman, to send the key to the recipient. It can also use asymmetric encryption technology to encrypt the key for distribution.

References

LabSim for Security Pro, Section 3.3.
[Questions.exm RT-3.3-1]