Exam Report: 9.4.3 Practice Questions

Date: 1/28/2020 4:35:08 pm
Time Spent: 4:33

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 14%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

Which of the following attacks typically takes the longest amount of time to complete?

○ Dictionary attack

○ Replay attack

○ Impersonation attack

➡ ● Brute force attack

Explanation

A brute force attack typically takes the longest amount of time. A brute force attack is a form of attack that attempts every possible key or password pattern for a message, login prompt, or security file. To combat or protect against brute force attacks, always use strong, complex passwords and wisely use the keyspace of your cryptosystems.

A dictionary attack, replay attack, and impersonation attack all take considerably less time than a brute force attack and are often used as shortcuts to a brute force attack.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_09]

Question 2: Incorrect

Why are brute force attacks always successful?

○ They are platform independent.

➡ ○ They test every possible valid combination.

○ They are fast.

● ~~They can be performed in a distributed parallel processing environment.~~

Explanation

Brute force attacks are always successful because they test every possible valid combination. Thus, they will eventually discover the actual key, password, or code that was used.

Brute force attacks are not fast, they are usually platform and application-specific, and while they can be deployed in distributed parallel processing environments in order to make them faster, this does not necessarily make them successful.

References

LabSim for Security Pro, Section 9.4.

[All Questions SecPro2017_v6.exm CRYPTO_ATT_11]

Question 3: Incorrect

If a birthday attack is successful, meaning the attacker discovers a password that generates the same hash as that captured from a user's login credentials, which of the following is true? (Select two.)

➡ ☐ A collision was discovered.

☑ ~~The discovered password is always the same as the user's password.~~

☐ The user is forced to change their password at their next login attempt.

➡ ☑ The discovered password will allow the attacker to log in as the user, even if the discovered password is not the same as the user's password.

Explanation

The discovered password will allow the attacker to log on as the user, even if the discovered password is not the same as the user's password. This is because the birthday attack (password cracking) will discover a collision. A collision is when two messages produce the same hash. A collision does not guarantee that the two messages are the same. Therefore, another password could be discovered that has the same hash as the original user's password. Since the authentication system checks only for matching hashes, the attacker could log on with a different password as long as it produces the correct hash.

The discovered password might not be the same as the user's password, since collision only ensures that two messages produce the same hash, not that the two messages are the same. The attack component of the birthday attack is collision, not collusion. Collusion is when two or more people agree to work together to commit a security violation. The act of an attacker discovering a user's password does not automatically force the user to change their password upon the next login attempt. Instead, this is a good security practice to implement if the security team discovers or suspects a password compromise.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_14]

Question 4: Incorrect

Which of the following is a mathematical attack that targets the complexity of a cryptosystem's algorithm?

○ Replay attack

➡ ○ Analytic attack

○ Brute force attack

● ~~Birthday attack~~

Explanation

An analytic attack is a mathematical that targets the complexity of a cryptosystem's algorithm. The goal of an analytic attack is to break the algorithm.

A birthday attack is focused on hashing algorithms, but not on the algorithm itself. Instead, a birthday attack exploits a statistical anomaly of collusion when two different messages using the same algorithm produce the same message digest. A brute force attack tries all possible combinations of keys to decipher an encrypted message. A replay attack attempts to re-transmit encryption session keys in hopes of accessing the resource in a de-encrypted mode.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_01]

Question 5: Incorrect

Your company produces an encryption device that lets you enter text and receive encrypted text in response. An attacker obtains one of these devices and starts inputting random plaintext to see the resulting ciphertext.

Which type of attack is this?

➡ ○ Chosen plaintext

● ~~Chosen cipher~~

○ Brute force

○ Known plaintext

Explanation

A *chosen plaintext* attack is where the attacker chooses the plaintext to be encrypted. This event can occur when a worker steps away from the computer and the attacker sends a message and captures the resulting cipher text. The attacker can select plaintext that will produce clues to the encryption key used.

A brute force attack is where the attacker tries every known combination. A chosen ciphertext is where the attacker produces ciphertext and then sends it through a decryption process to see the resulting plaintext. A known plaintext attack is where an attacker has seen the plaintext and the resulting ciphertext.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_05]

Question 6: Incorrect

Which form of cryptanalysis focuses on weaknesses in software, the protocol, or the encryption algorithm?

○ Ciphertext only attack

➡ ○ Implementation attack

○ Statistical attack

● ~~Analytic attack~~

Explanation

An implementation attack exploits implementation weaknesses, such as in software, the protocol, or the encryption algorithm.

A statistical attack exploits weaknesses in the computing platform, such as the inability to produce random numbers or CPU floating point errors. An analytic attack focuses on weaknesses in the algorithm itself. A ciphertext only attack is a solution attack where material supplied by the attacker is decrypted by the victim, revealing the key.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_03]

Question 7: Incorrect

Which of the following best describes a side-channel attack?

● ~~The attack targets the key containing a small data set.~~

○ The attack exploits weaknesses in a cryptosystem, such as inability to produce random numbers or floating point errors.

➡ ○ The attack is based on information gained from the physical implementation of a cryptosystem.

○ The attack targets a weakness in the software, protocol, or encryption algorithm.

Explanation

A *side-channel* attack is where an attack is based on information gained from the physical implementation of a cryptosystem rather than theoretical weaknesses in the algorithms, such as the length of time required during encryption or decryption.

A *mathematical* attack is an attack on a key containing a small data set. An *implementation* attack exploits implementation weaknesses, such as in software, the protocol, or the encryption algorithm. A *statistical* attack exploits weaknesses in a cryptosystem, such as inability to produce random numbers or floating point errors.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_07]

▼ **Question 8:** Incorrect

Which of the following is **not** a countermeasure against dictionary attacks?

○ Avoiding common words

➡ ○ Using short passwords

○ Using three or four different keyboard character types (lowercase, uppercase, numerals, and symbols)

● ~~Avoiding industry acronyms~~

Explanation

Using short passwords is not a direct countermeasure against dictionary attacks. All too often, a short password is a simple common word. A dictionary attack is designed to quickly discover passwords that use common words. Dictionary attacks can be customized for the intended victim. If the attacker knows a few details about the victim, such as hobbies, sports interests, education, or industry, then the dictionary can be customized to focus on words, terms, and acronyms related to those topics.

Avoiding common words, using three or four different keyboard character types, and avoiding industry acronyms are all good countermeasures against dictionary attacks.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_12]

▼ **Question 9:** Incorrect

Which of the following is an example of a statistical attack against a cryptosystem?

○ Attempting every possible key pattern

● ~~Intercepting messages between two communication partners and modifying the content~~

○ Exploiting faulty implementation of an algorithm in software

➡ ○ Exploiting a computer's inability to produce random numbers

Explanation

An example of a statistical attack against a cryptosystem is exploiting a computer's inability to produce true random numbers. Another example is to exploit the floating point errors in a processor. A computer system's inability to produce true random numbers makes the possibility of the re-use of keys probable, if not likely.

Attempting every possible key pattern is a form of brute force attack. Exploiting faulty implementation of an algorithm in software is an implementation attack. Intercepting messages between two communication partners and modifying the content is a form of man-in-the-middle attack.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_02]

▼

Question 10: Incorrect

If two different messages or files produce the same hashing digest, then a collision has occurred. Which form of cryptographic attack exploits this condition?

● ~~Statistical attack~~

○ Adaptive chosen ciphertext attack

○ Meet-in-the-middle attack

➡ ○ Birthday attack

Explanation

Birthday attacks exploit collisions. Birthday attacks exploit the probability that two messages using the same hash algorithm will produce the same message digest.

An adaptive chosen ciphertext attack is used to discover the encryption key. A meet-in-the-middle-attack is used to determine the algorithm used. A statistical attack is used to exploit computer-based cryptosystems, such as the inability to produce true random numbers.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_13]

Question 11: Incorrect

Which of the following password attacks adds appendages to known dictionary words?

○ Analytic

● ~~Dictionary~~

➡ ○ Hybrid

○ Brute force

Explanation

A *hybrid* attack adds appendages to known dictionary words (for example, 1password, password07, and p@ssword1).

A *brute force* attack works through all possibilities until the password is cracked. A *dictionary* attack tries known words (such as from a dictionary). An *analytic* attack uses an algebraic manipulation to reduce the complexity of the algorithm.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_08]

Question 12: Correct

When an attacker decrypts an encoded message using a different key than was used during encryption, what type of attack has occurred?

○ Analytic

○ Statistical

○ Replay

➡ ● Key clustering

Explanation

A *key clustering* attack is where the attacker decrypts an encoded message using a different key than was used during encryption.

A statistical attack exploits weaknesses in a cryptosystem, such as inability to produce random numbers or floating point errors. An analytic attack uses an algebraic manipulation to reduce the complexity of the algorithm. A replay attack attempts to re-transmit encryption session keys in hopes of accessing the resource in a de-encrypted mode.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_06]

▼ **Question 13:** Incorrect

Which type of password attack employs a list of pre-defined passwords that it tries against a login prompt or a local copy of a security accounts database?

➡ ○ Dictionary

○ Brute force

● ~~Asynchronous~~

○ Salami

Explanation

A dictionary attack is a type of password attack that employs a list of pre-defined passwords that it tries against a login prompt or a local copy of a security accounts database. A dictionary attack is designed to quickly discover passwords that use common words. Dictionary attacks can be customized for the intended victim. If the attacker knows a few details about the victim, such as hobbies, sports interests, education, or industry, then the dictionary can be customized to focus on words, terms, and acronyms related to those topics.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_10]

▼ **Question 14:** Incorrect

In which type of attack does the attacker have access to both the plaintext and the resulting cipher text, but does not have the ability to encrypt the plain text?

● ~~Chosen plaintext~~

○ Chosen cipher

➡ ○ Known plaintext

○ Brute force

Explanation

A *known plaintext* attack is where an attacker has seen the plaintext and the resulting cipher text. The attacker can make conclusions about the encrypting key and will have validation if the encrypting key is discovered.

A chosen plaintext attack is where the attacker chooses the plaintext to be encrypted. The main difference between known plaintext and chosen plaintext is the attacker's ability to select random plaintext and run it through the encrypting mechanism.

A brute force attack is where the attacker tries every known combination. A chosen cipher text is where the attacker produces cipher text and then sends it through a decryption process to see the resulting plaintext.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_04]