Exam Report: 3.1.5 Practice Questions - Section 3.1

Date: 11/23/2015 12:36:57 am
Time Spent: 2:18

Candidate: Belskis, Tomas
Login: t0mas9lt

Overall Performance

Your Score: 60%

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 is the cryptography mechanism which hides secret communications within various forms of data?

- ○ Codes
- ➡ ◉ Steganography
- ○ Signals
- ○ Polyinstantiation

Explanation

Steganography is the cryptography mechanism which hides secret communications within various forms of data.

Codes and signals are pre-arranged meanings behind words, phrases, images, etc. Codes and signals are not usually considered a form of steganography, since the communication is not imbedded in the code or signal, but is a pre-established meaning for something. Polyinstantiation is a security feature of databases which allows duplicate objects to exist at different levels of security.

References

LabSim for Security Pro, Section 3.1.
[Questions.exm CISSP-511 NEW [7]]

Question 2: Correct

Which of the following encryption methods combines a random value with the plain text to produce the cipher text?

- ➡ ◉ One-time pad
- ○ Transposition
- ○ Steganography
- ○

Elliptic curve

Explanation

A *one-time pad* is a cryptography method in which the plain text is converted to binary and combined with a string of randomly generated binary numbers (referred to as the *pad*). It is a form of substitution.

A *transposition cipher* (also called an *anagram*) changes the position of characters in the plain text message. *Steganography* is a cryptography method that uses digital pictures, video clips, or audio clips to hide a message or some type of data. Steganography tools encode the message into the Least Significant Bit (LSB) of the binary coding. *Elliptic curve cryptography* (ECC) is an approach to cryptography that uses a finite set of values within an elliptic curve (an algebraic set of numbers).

References

LabSim for Security Pro, Section 3.1.
[Questions.exm SP08_5-3 7]

Question 3: Correct

Which type of cipher changes the *position* of the characters in a plain text message?

- Substitution
- Transposition
- Block
- Steam

Explanation

A *transposition* cipher changes the position of characters in the plain text message. It is also referred to as an *anagram*.

A substitution cipher replaces one set of characters with symbols or another character set. A block cipher takes a fixed-length number of bits, referred to as a block, and encrypts them all at once. A stream cipher creates a sequence of bits that are used as the key.

References

LabSim for Security Pro, Section 3.1.
[Questions.exm NEW [7]]

Question 4: Incorrect

The Enigma machine, a cryptographic tool introduced in 1944 and used in WW2, encrypted messages by replacing characters for plain text. Which type of cipher does the Enigma machine use?

- ~~Transposition~~
- Substitution
- Block
- Steam

Explanation

The Enigma machine uses a substitution cipher. A substitution cipher replaces one set of characters with symbols or another character set.

A transposition cipher changes the position of characters in the plain text message. It is also referred to as an *anagram*. A block cipher takes a fixed-length number of bits, referred to as a block, and encrypts them all at once. A stream cipher creates a sequence of bits that are used as the key.

References

LabSim for Security Pro, Section 3.1.
[Questions.exm NEW [15]]

Question 5: Correct

In a cryptographic system, what properties should the initialization vector have? (Select two.)

- [ ] Predictable
- [x] Unpredictable
- [x] Large
- [ ] Short
- [ ] Uniform

Explanation

For security, the initialization vector should be *large* and it should be *unpredictable*. When the initialization vector is large and unpredictable, an encryption algorithm can generate secure keys or encrypt data that is difficult to decrypt.

If the initialization vector is short, predictable, or uniform, the generated keys may not be secure and encrypted data may be easily decrypted by attackers.

References

LabSim for Security Pro, Section 3.1.
[Questions.exm NEW [31]]

Question 6: Incorrect

Which of the following is a form of mathematical attack against the complexity of a cryptosystem's algorithm?

- ( ) Replay attack
- (•) ~~Brute force attack~~
- ( ) Birthday attack
- ( ) Analytic attack

Explanation

An analytic attack is a form of mathematical attack against 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 will 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 3.1.
[Questions.exm SP [587]]

Question 7: Correct

Which form of cryptanalysis focuses on the weaknesses in the supporting computing platform as a means to exploit and defeat encryption?

- (•) Statistical attack
- ( ) Implementation attack
- ( ) Ciphertext only attack
- ( ) Analytic attack

Explanation

A statistical attack attacks 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, thus revealing the key. Implementation attack focuses on poor programming and seeks out a software bug that can be exploited.

References

LabSim for Security Pro, Section 3.1.
[Questions.exm CP [619]]

Question 8: Correct

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

- ( ) Brute force
- ( ) Chosen plaintext
- (•) Known plaintext
- ( ) Chosen cipher

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 ability of the attacker 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 3.1.
[Questions.exm NEW [130]]

Question 9: Correct

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 plain text to see the resulting cipher text. What type of attack is this?

- Known plaintext
- Chosen plaintext
- Brute force
- Chosen cipher

Explanation

A *chosen plaintext* attack is where the attacker chooses the plain text to be encrypted. This 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 plain text that will produce clues to the encryption key used.

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. A known plaintext attack is where an attacker has seen the plain text and the resulting cipher text.

References

LabSim for Security Pro, Section 3.1.
[Questions.exm NEW [138]]

Question 10: Incorrect

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

- Statistical
- Key clustering
- ~~Replay~~
- Analytic

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 3.1.
[Questions.exm NEW [146]]

Question 11: Incorrect

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

- 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 the key containing a small data set.
- ~~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 3.1.
[Questions.exm NEW [154]]

Question 12: Correct

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 3.1.
[Questions.exm NEW [141]]

Question 13: Incorrect

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

- Replay attack
- Brute force attack
- Impersonation attack
- ~~Dictionary attack~~

Explanation

A brute force attack will typically take the longest amount of time. A brute force attack is a form of attack that attempts every possible key or password pattern against a message, a logon prompt, or a 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 the brute force attack.

References

LabSim for Security Pro, Section 3.1.
[Questions.exm SP [480]]

Question 14: Correct

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

- Asynchronous
- Dictionary
- Salami
- Brute force

Explanation

A dictionary attack is a type of password attack that employs a list of pre-defined passwords that it tries against a logon 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, industry, interests, etc., then the dictionary can be customized to focus on words, terms, and acronyms related to those topics.

References

LabSim for Security Pro, Section 3.1.
[Questions.exm SP [496]]

Question 15: 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, code, etc. 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, that does not make them always successful.

References

LabSim for Security Pro, Section 3.1.
[Questions.exm CP [512]]