Self-Assessment Quiz Answers

Self-Assessment Quiz 1

Question 1

Alice shared an important video that she signed with her signature key to prove it is valid. After sharing, she became worried about that the connection with her identity may cause issues in the future. She intentionally published her private signature key to expose it, so that anyone else could have signed the video. This achieves the privacy property of:

Answer: Repudiation

Question 2

The Tanenbaum-Torvalds debate surrounds the principle of:

Answer: Least Privilege

Question 3

In 2020, many Twitter accounts were hijacked. In STRIDE, this threat would be known as:

Answer: Spoofing / Escalation of Privilege

Question 4

In cryptosystem design, what should be secret?

Answer: The keys

Question 5

The poor design of password policies is due to:

Answer: Misunderstanding how human memory works.

Self-Assessment Quiz 2

Question 1

Which of the following attacks is effectively prevented by WˆX?

Answer: Using a format string vulnerability to overwrite the return address to point to instructions on stack *(Any attack that attempts to redirect control flow towards the stack is prevented by WˆX.)*

Question 2

A privileged program (setuid root) does the following on a temporary file:

1. Create a temporary file after checking the filename is unused.
2. Lock the temporary file.
3. Write user input data to the temporary file.
4. Close the temporary file.

An attacker attempts to launch a TOCTTOU attack against it by overwriting the temporary file as a symbolic link to a privileged file (e.g. the password file), then giving user input to the program to overwrite the root file with what the attacker wants (e.g. their own password). Will this attack work?

Answer: It will work if the attack is timed between 1 and 2. *(Once it is locked, it is too late for the attacker to redefine the file.)*

Question 3

A buffer overflow attack attempts to overwrite a variable in stack which controls user authorization. (For example, it may be the "authorized" variable in the class demo.) This is effectively prevented by:

Answer: None of the other choices. *(Address Space Layout Randomization, Canaries, WˆX)*

Question 4

One of the first worms was the Morris worm, written by then Cornell PhD student (now MIT professor) Robert Morris. Morris was the first person to be convicted under the US Computer Fraud and Abuse Act.

The worm used a remote buffer overflow attack against the vulnerable "fingerd" service, which was a background daemon, to escalate privilege and take over the target. It would then automatically attempt to spread to other devices. It could also remotely guess common usernames and passwords. It is called a worm because:

Answer: It spreads quickly and automatically with no user interaction.

Question 5

Ransomware almost always uses cryptocurrency because:

Answer: It is not possible to block the transaction.

Question 6

Which of the following is a useful defense against network-spreading malware like Blaster?

Answer: Air gap

Question 7

A covert channel is most useful when:

Answer: The victim has a firewall, and the attacker has taken control of the victim's data.

Self-Assessment Quiz 3

Question 1

An attacker has obtained a number of WEP messages with the same key and IV. What technique can they use to compromise these messages?

Answer: Crib-dragging

Question 2

Suppose Alice sends an encrypted message (without integrity checking) to Bob, and a malicious MITM changes one bit of the ciphertext. Which of the following is a FALSE statement about the plaintext Bob receives after decryption?

Answer: If the algorithm is AES under CBC with a block size of 128, up to 128 bits of the plaintext can be altered. *(Because AES-CBC xors the previous ciphertext block with each plaintext block for encryption, one bit flip can affect every plaintext block after it.)*

Question 3

Which of the following is NOT a desirable property for an encryption function Enc(K, M), where K is the key and M is the message?

Answer: Given Enc(K, M), M and M2, it should be hard to find Enc(K, M2). *(Note that achieving this property requires the use of an IV in stream ciphers.)*

Question 4

Suppose you have a strong password with 40 bits of entropy. The server has stored its SHA-256 hash without a salt, and the hash has been stolen. SHA-256 is the version of SHA-2 that outputs 256 bit digests. The approximate number of hashes the attacker would need to compute to guess your password is:

Answer: 2^{40}.

Question 5

Considering the above question, would it be beneficial for the server to hash your password with a salt?

Answer: Yes, it defeats pre-computed tables. *(While the total computation time for a specific hash is not changed, pre-computed rainbow tables still* *save the attacker's effort because a single SHA-256 table can be used for any SHA-256 password database, and they are defeated by salting.)*

Question 6

A good defense against the Logjam attack is:

Answer: Each server should generate its own large prime.

Question 7

Which of the following correctly describes the relationship between Public Key Encryption (PKE) and Symmetric Key Encryption (SKE)?

Answer: Both PKE and SKE keys should be short-lived.