HW-Module14 Results for BRANDEN BARNES

Score for this attempt: 100 out of 100
Submitted Apr 21 at 11:09pm
This attempt took 387 minutes.

Question 1
20 / 20 pts

In IEEE 802.11, open system authentication simply consists of two communications. An authentication is requested by the client, which contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.

a. What are the benefits of this authentication scheme?
b. What are the security vulnerabilities of this authentication scheme?

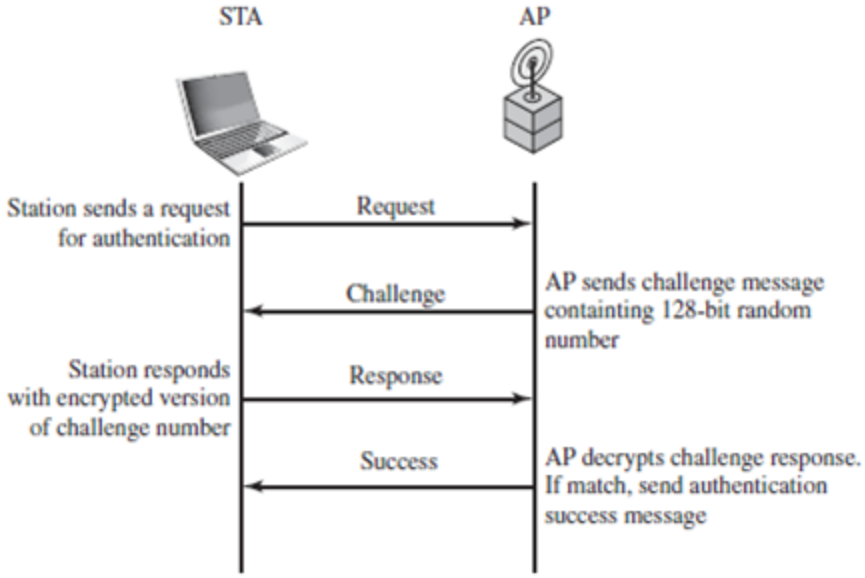
Your Answer:

a. The benefit of this authentication scheme is its ease of implementation. It also protects against simple attacks against Wi-Fi LAN cards and accidental wrong-network connections.

b. This authentication scheme has some security vulnerabilities such as MAC spoofing. This may allow attackers to intercept target-destined frames. This scheme also relies on both parties to work honestly.

Question 2
35 / 35 pts

Prior to the introduction of IEEE 802.11i, the security scheme for IEEE 802.11 was Wired Equivalent Privacy (WEP). WEP assumed all devices in the network share a secret key. The purpose of the authentication scenario is for the STA to prove that it possesses the secret key. Authentication proceeds as shown in the figure below. The STA sends a message to the AP requesting authentication. The AP issues a challenge, which is a sequence of 128 random bytes sent as plaintext. The STA encrypts the challenge with the shared key and returns it to the AP. The AP decrypts the incoming value and compares it to the challenge that it sent. If there is a match, the AP confirms that authentication has succeeded.



a. What are the benefits of this authentication scheme?

b. This authentication scheme is incomplete. What is missing and why is this important? Hint: The addition of one or two messages would fix the problem.

c. What is a cryptographic weakness of this scheme?

Your Answer:

a. The benefit of this authentication scheme is ease of access and shared secret key authentication through challenges.

b. Once the Shared Key authentication is successful, the same static process will be used to encrypt the 802.11 data frames. This encryption is important so no one can capture the clear-text challenge phrase.

c. The weakness of this scheme stems from the clear-text challenge frame. If someone were to capture this and then capture the encrypted challenge phrase, then the WEP key could become compromised. If the key becomes compromised then all the data frames can be decrypted.

Question 3
45 / 45 pts

For WEP, data integrity and data confidentiality are achieved using the RC4 stream encryption algorithm. The transmitter of an MPDU performs the following steps, referred to as encapsulation:

1. The transmitter selects an initial vector (IV) value.
2. The IV value is concatenated with the WEP key shared by transmitter and receiver to form the seed, or key input, to RC4.
3. A 32-bit cyclic redundancy check (CRC) is computed over all the bits of the MAC data field

and appended to the data field. The CRC is a common error-detection code used in data link control protocols. In this case, the CRC serves as a integrity check value (ICV).

4. The result of step 3 is encrypted using RC4 to form the ciphertext block.
5. The plaintext IV is prepended to the ciphertext block to form the encapsulated MPDU for transmission.

a. Draw a block diagram that illustrates the encapsulation process.

b. Describe the steps at the receiver end to recover the plaintext and perform the integrity check.

c. Draw a block diagram that illustrates part b.

If you want to attach a document with your solution, use the next question for the attachment.

Your Answer:

b.

1. The IV of the incoming message is concatenated with the secret key and through RC4 PRNG algorithm to produce a key sequence.
2. The plaintext and ICV are obtained by doing a bitwise XOR with ciphertext and the key sequence.
3. Even when the decrypted plaintext is obtained, the decryption needs to be verified by performing the integrity check algorithm comparing the output ICV' with the ICV obtained in step 2. If the two ICV are not equal, there is an error in the received message and the package is sent back to the sending station

Question 4

0 / 0 pts

This is a dummy question so you can attach a document with your solution for the above question (question #3).

Mod 14.docx (https://canvas.odu.edu/files/33895935/download)

Quiz Score: 100 out of 100