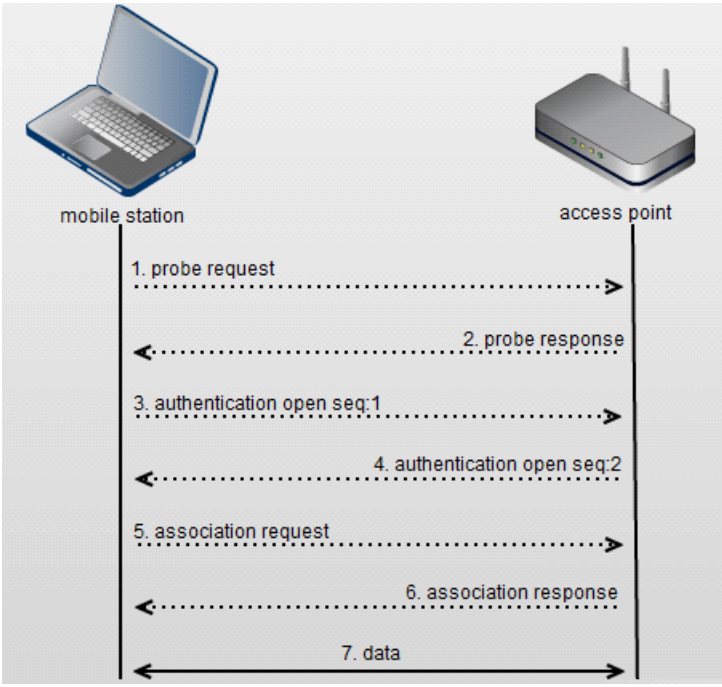
Wired Equivalent Privacy (WEP)

Thursday, May 14, 2020 10:18 PM

- Privacy protocol specified in IEEE 802.11 to provide wireless LAN users protection against casual eavesdropping
- Intent to provide a privacy service to wireless LAN uses similar to that provided by the physical security inherent in a wired LAN
- When WEP is active --> each 802.11 packet is encrypted separately with an RC4 cipher stream generated by a 64 bit RC4 key
    - Key composed of a 24 bit initialization vector (IV) & 40 bit WEP key
    - Encrypted packet is generated with a bitwise exclusive OR (XOR) of the original packet & the RC4 stream
    - IV is chosen by the sender & should be changed so that every packet won't be encrypted with the same cipher stream
    - IV is sent in the clear with each packet
    - Additional 4 byte Integrity Check Value (ICV) is computed on the original packet using the CRC-32 checksum algorithm & appended to the end
    - ICV is also encrypted with RC4 cipher stream
- Process



Key management & key size

Friday, May 15, 2020 11:26 AM

- Key management is not specified --> keys to be long-lived and of poor quality
- Usually have 1 single WEP key shared between every node on the network --> AP & client are programed with the same WEP key
- Tedious to synchronize the change of keys --> seldom change
- Size of key : 40 bits
    - Easy to attack using brute force
    - Vendors would usually implement a de facto standard by extending the key size to 104 bits with excellent interoperability
        - Known as 128-bit WEP key
- RC4 encryption key includes a 24-bit IV

Initialization Vector is too small

Friday, May 15, 2020 11:26 AM

- Size : 24 bits
  - Provides for 16 777 216 different RC4 cipher streams for a given WEP key for any key size
  - After 2^{24} or around 16.7M packets
  - Equation to calculate the time taken to exhaust IV space in a busy network
    - Formula: (number of bytes the AP send in a packet * 8) / (data rate in Mbps * 10^6) * 2^{24}
      - Theoretical rate is usually longer since:
        - Might take a longer time for the IV to be reuse due to overhead and packet collisions causing the observed rate to be much lower
        - Packets are also not at the Ethernet maximum of 1500 bytes
- Sent in clear text
- IV is reuse
  - Able to decrypt the subsequent packets that were encrypted with the same IV or forge packet as long as the attacker knows what key stream was used to encrypt that packet
    - Doesn't need to know the WEP key to decrypt the packets
- Doesn't state how IV is chosen
  - Start from 0 then increment for each packet
  - Chose randomly
    - Leads to 50% chance of reuse after less than 5000 packets
- Methods used to discover the cipher stream for a particular IV
  - given two encrypted packets with the same IV, the XOR of the original packets can be found by XORing the encrypted packets
    - If the victim is on the Internet, the attacker can simply ping the victim or send an email message
    - If the attacker is able to send the victim packets and observe and analyse those encrypted packets, he can deduce the cipher stream

Integrity Check Value (ICV) algorithm is not appropriate

Friday, May 15, 2020 11:26 AM

- Based on CRC-32
  - Algorithm used for detecting noise & common errors in transmission
  - Excellent checksum for detecting errors
  - Awful choice for cryptographic hash
  - Better to use algorithms such as MD5 or SHA-1 for ICVs
- CRC-32 ICV is a linear function of the message --> able to modify an encrypted message & easily fix the ICV so the message appears authentic
  - e.g. attacker can easily make the victim's wireless AP decrypt packets for him
    - Capture an encrypted packet stream, modify the destination address of each packet to be the attacker's wired IP address, fix up CRC-32 & retransmit the packets over the air to the AP
    - AP then decrypt the packet & forward them to the attacker

Use of RC4 is weak

Friday, May 15, 2020 11:26 AM

- Weak key = more correlation between the key & the output than there should be for good security
- Easy to determine which packets were encrypted with weak keys since 1st 3 bytes of the key are taken from the IV that is sent unencrypted in each packet
    - Exploit using passive attack
- Just require one machine to use weak keys for the attack to succeed
- How it can be done
    - Attacker would need to capture enough "interesting packets", filtering for IV that suggest weak keys
        - Would have to capture between 2000 & 4000 packets to determine 104 bit WEP key
    - Analyze the packets & try a small number of keys to gain access to the network
        - All original IP packet starts with a known value --> easy to know when it's the right key

Authentication message can be easily forged

Friday, May 15, 2020 11:26 AM

- 2 forms of authentication
  - Open system (no authentication)
    - No authentication by default
    - Allows administrators to use other authentication protocol such as 802.1x to handle the task of properly authenticating wireless users
  - Shared key authentication
    - User has to prove knowledge of the shared WEP key --> more secure than no authentication
      - Done by encrypting a challenge
      - Advantage
        - Reduces the ability of an attacker to create a denial-of-service attack by sending packets encrypted with the wrong WEP key into the network
        - Allows wireless client to quickly determine if they know the correct WEP key
          - User-friendly but allows malicious client to try a dictionary attack on the wireless network
      - Attack method
        - Monitoring attack
          - Used to observed both the challenge & encrypted response --> determine the RC4 stream used to encrypt the response & stream to encrypt any challenge the attacker received in the future
        - Statistical attack
          - Attacker collect 2 ciphertext packets that ae encrypted with the same key stream --> match a ciphertext message with its associated plaintext & conduct a XOR operation to reveal the key
            - Educated guess about the contents of a plaintext message and exploiting the predictable nature and redundancy would be required if the threat cannot understand all of the contents
          - Passive attack

Active attack

Friday, May 15, 2020 11:26 AM

- What can they do with the information they have obtain
    - Generate the key stream
    - Threat can be built correctly encrypted packets by constructing a message, calculating its CRC-32 & executing an XOR operation with the newly discovered key stream --> ciphertext is then sent to the AP or mobile station to deceive it into thinking that it is a valid packet (affects integrity of the packet)
- If the attacker speculates about the frame's header --> making an educated guess of the destination IP address based on the information he/she got from the frame header --> modify appropriate bits to transform the destination IP address to send the packet to a machine in his control via a rogue mobile station -->