Department of Computer Science

FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

CSE 4820: Wireless and Mobile Security

7. WEP Vulnerabilities

Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

Outline

WEP Security Analysis

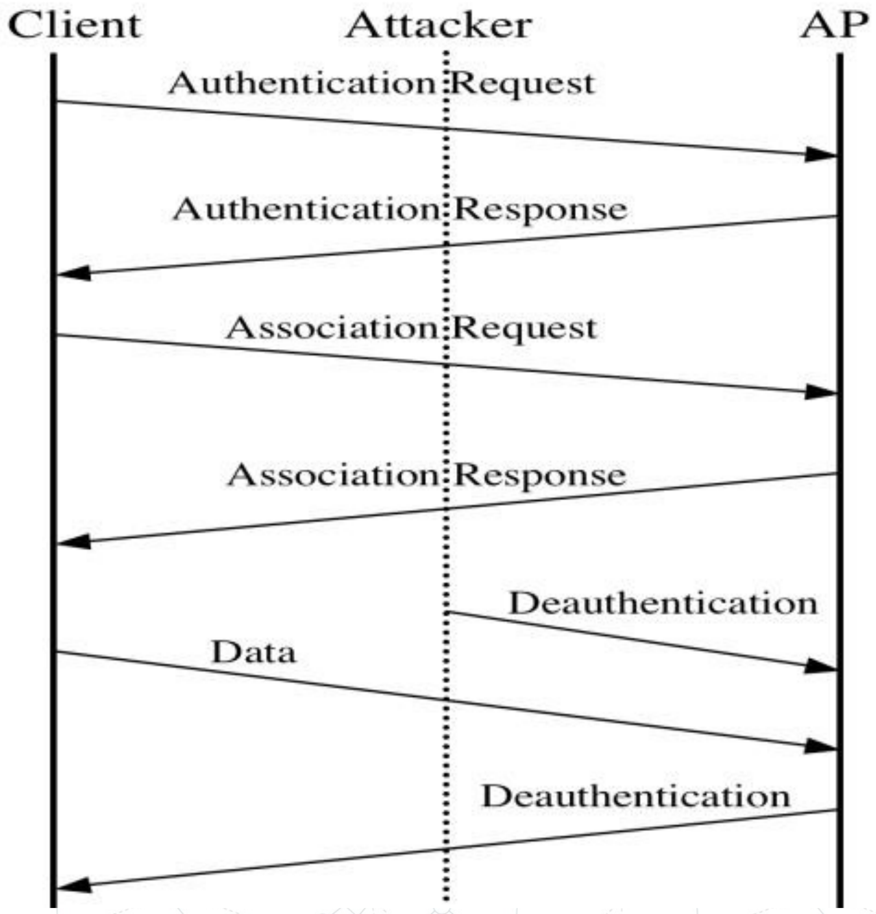
MAC Filtering

Recall: Security Through Obscurity

- Passive sniffers can easily take advantage of this behavior
  - If you sniff the network, you will get the SSID whenever someone joins the network
  - You may even force user's hand
    - How?

Recall: De-authenticating user

- Management frames in 802.11 are not authenticated
  - Send a packet to user that looks like coming from AP
  - The user can't tell the difference
  - Wireless driver will reconnect immediately
  - Reassociation request with the SSID in it will be sent



Recall: Protected Management Frames

- PMF provide protection for unicast and multicast management action frames
  - Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging
- PMF is required for all new certified devices
  - However, may not be implemented in all devices out there

Countermeasure for Deauthenticating User

- 802.11w amendment (2012 update) to support protection of both deauthenticate and disassociation frames
  - Using a message integrity check to identify spoofed frames
- Available only when WPA2 is used
- Newer OS support but some APs do not

Review WEP

- Weak Encryption Protocol
  - Authentication
  - Access control
  - Replay prevention
  - Message modification detection
  - Message privacy
  - Key protection

WEP: Authentication

- The basic requirements for authentication in wireless LANs are:
  - Robust method of proving <u>identity</u> that <u>cannot be spoofed</u>
  - Method of preserving identity over subsequent transactions that <u>cannot be transferred</u>
  - Mutual authentication
  - Keys are independent from encryption's (and other purposes) keys

WEP: Authentication

- As a reminder, WEP authentication relies on a challenge-response mechanism
  - First, the AP sends a random string of numbers
  - Second, the mobile device encrypts the string and sends it back
  - Third, the AP decrypts the string and compares to the original string
  - It can then choose to accept the device and send a success message
- The key used for this process is the same WEP key used for encryption, thus breaking rule 4
  - Need independent keys

WEP: Authentication

- The operation does not authenticate the AP to the mobile device because a rogue AP can pretend it was able to check the encrypted string and send a success message without ever knowing the key
  - Hence rule 3 is broken
- Rule 2 is broken because there is no token provided to validate <u>subsequent transactions</u>, making the whole authentication process rather futile

WEP: Authentication

- During authentication the AP sends a random string of 128 bytes
  - The way in which this "random" string is generated is not defined
  - One would hope at least that it was different for each authentication attempt
- The mobile station encrypts the string and sends it back
- WEP encryption involves generating a sequence of pseudorandom bytes called the key stream and XORing it with the plaintext
- Thus, anyone watching this transaction now has the plaintext challenge and the encrypted response

WEP: Authentication

- Therefore, simply by XORing the two together, the enemy has a copy of the RC4 random bytes
- Authentication: `P ⊕ R = C     (Plaintext XOR Randombytes = Ciphertext)`
- And remember that XORing twice gets you back to the original value (that's decryption): `If P ⊕ R = C then C ⊕ R = P`
- By the same argument, XORing the ciphertext with the plaintext gives you the random key stream: `If P ⊕ R = C then C ⊕ P = R`

WEP: Authentication

- The attacker now knows the key stream corresponding to a given IV value
- Now the attacker simply requests authentication, waits for the challenge text, XORs with the previously captured key stream, and returns the result with the previously captured IV
- To check the result, the AP appends the IV (chosen by the attacker) to the secret key and generates the RC4 random key stream

WEP: Authentication

- These will be the same bytes that the attacker worked out because the key and IV are the same as last time
- Therefore, when the access point decrypts the message by XORing with the RC4 key stream, it matches
- The attacker is "authenticated" without ever knowing the secret key

WEP: Authentication

- Although an attacker can get authenticated in this way, can't communicate because frames are encrypted with WEP
  - Therefore, need to break WEP encryption as well
- The enemy needs a sample of matching plaintext and ciphertext
  - The WEP authentication method provides a 128-byte sample free of charge
  - Worse, it is a sample of the first 128 bytes of the key stream, which is the most vulnerable to attack
  - Assists the enemy to attack the encryption keys

Access Control

- Access control is the process of allowing or denying a mobile device to communicate with the network
  - It is often confused with authentication
  - All that authentication does is to establish who you are; it does not follow that, because you are authenticated, you should be allowed access
- In general, access is usually controlled by having a list of allowed devices
  - It may also be done by allowing access to anyone who can prove he has possession of a certificate or some other electronic pass

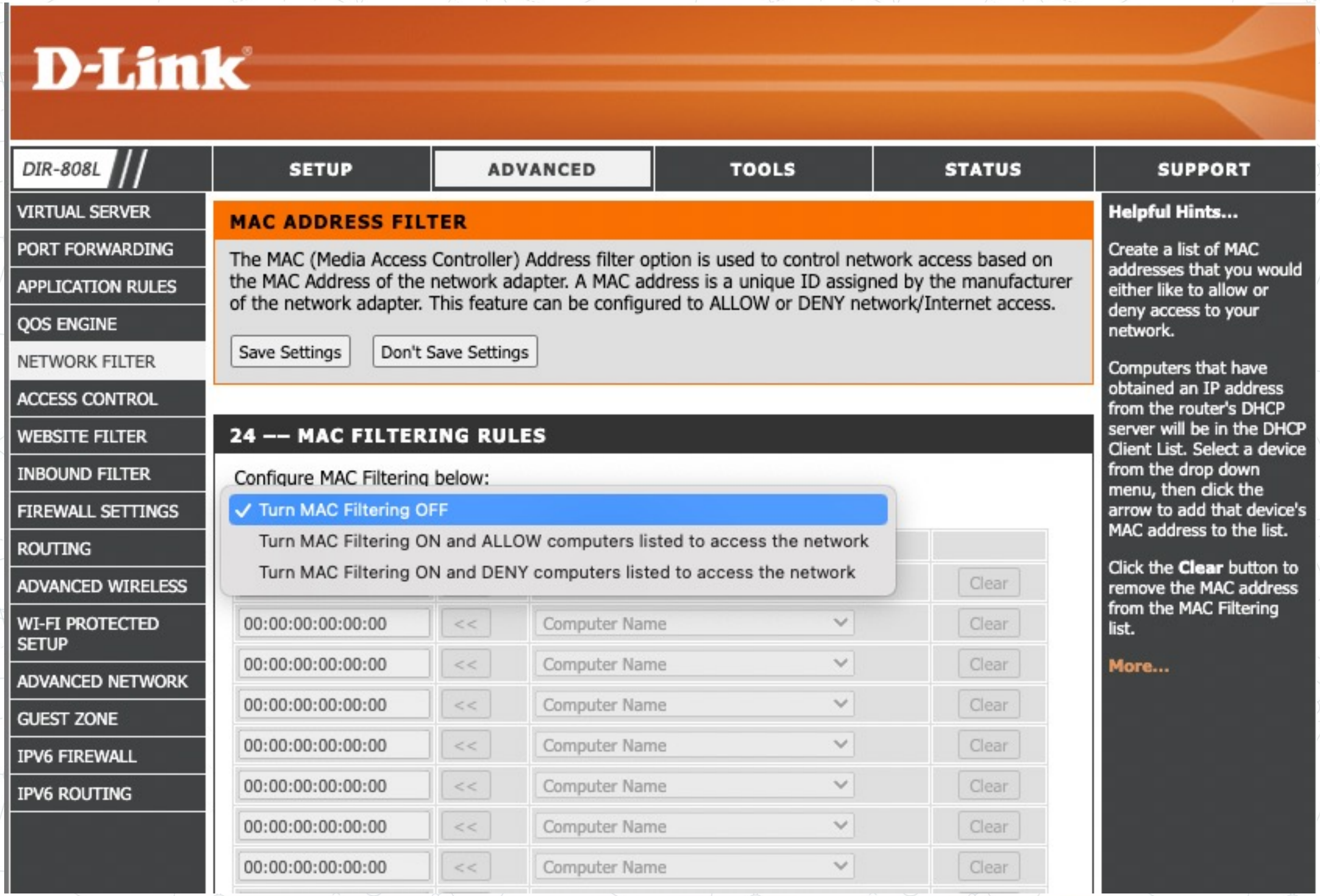
Access Control

- IEEE 802.11 does not define how access control is implemented
  - However, identification of devices is only done by MAC address, so there is an implication that a list of acceptable MAC addresses exists somewhere
- Many systems implement a simple scheme whereby a list of allowed MAC addresses can be entered into the access point, even when you are operating without WEP
- However, given the ease with which MAC addresses can be forged, this cannot be considered as a serious security mechanism

MAC Filtering

- Most APs allow MAC filtering
  - Trusted MAC Addresses to talk to
  - Rest ignored
- To beat it, you steal MAC address from someone already in the network:
  - Run passive scanner to get the address
  - The preferred way is to wait user to disconnect from the network
  - Or you kick them
    - DoS (deauthenticate) attack
    - Attempt to share MAC

MAC Filtering



Beating MAC Filtering

- Change your MAC on Linux:

  sudo ifconfig wlan0 down
  sudo ifconfig wlan0 hw ether 00:11:22:33:44:55
  sudo ifconfig wlan0 up

- IDS (Intrusion Detection System) may detect sharing MAC
  - But can't detect if the attacker waiting for user to disconnect
  - Thus, not much of additional security

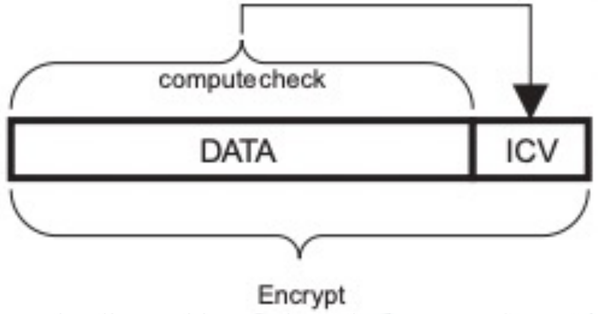
Access Control

- If you can't trust the MAC address, the only thing left to WEP is the encryption key
  - If the mobile station doesn't know the correct WEP key, then the frames it sends will produce an error when decrypted
  - Therefore, the frames will be discarded and, effectively, the device is denied access

Replay Prevention

- WEP has no protection against replay at all
  - It was just not considered in the design
  - There is a sequence number in the MAC frame that must increase monotonically
  - However, it is not included in the WEP protection so it is easy to modify the sequence number to be valid without messing with the encrypted portion on the frame
- Replay protection is not broken in WEP; it simply doesn't exist

Message Modification Detection



- To prevent tampering, WEP includes a checkfield called the integrity check value (ICV)
  - Compute a check value or CRC (cyclic redundancy check) over all the data to be encrypted, append the check value to the end of the data, and then encrypt the whole lot
- If someone <u>changes a bit in the ciphertext</u>, the decrypted data will not have the same check word and the <u>modification will be detected</u>
  - Because the ICV is encrypted, you cannot go back and correct its value to compensate for the other changes you have made
- It is only intended to provide protection to the ciphertext

Message Modification Detection

- If an attacker already knows the keys, he can modify the data and recompute the ICV before re-encrypting and forwarding the frame
- So use of the ICV protects the ciphertext from tampering?
  - Not quite
- ICV is called a linear method
  - You can predict which bits in the ICV (32-bits) will be changed if you change a single bit in the message

Message Modification Detection

- Let's suppose the message is 8,000 bits (1,000 bytes) and you flip bit position 5244
  - You can then compute which bits in the ICV will be changed as a result
  - It is typically not a single bit but a combination of bits that will change
- You don't need to know the actual value of the plaintext; you just need to know that if you flip the value of a certain bit in the data, you can <u>keep the ICV valid by also flipping a certain combination of its bits</u>
  - Because WEP works by XORing the data to get the ciphertext, bit flipping survives the encryption process
  - Flipping a bit in the plaintext always flips the same bit in the ciphertext, and vice versa

Message Privacy

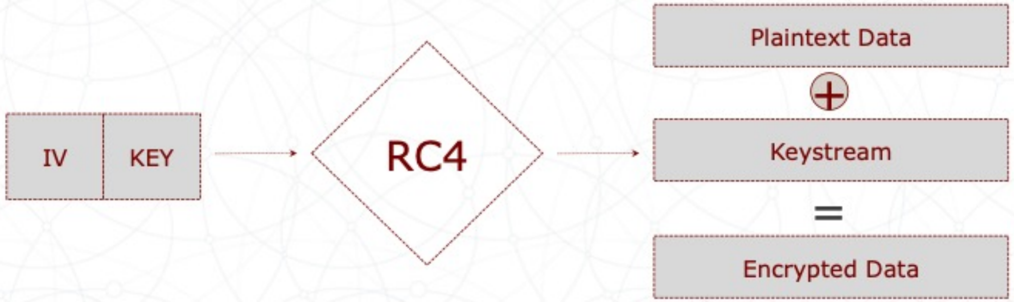
- Attacking the encryption method of WEP
  - If the encryption method holds up, then the attacker is very limited in what he can do
  - So far, it's just watching shadows or throwing rocks at the window; but if the encryption can be breached, the attacker is inside the house
- There are two main objectives in attacking the encryption: decode a message or get the keys
- The ultimate success is to get the keys
  - Once an attacker has the keys, he is free to explore and look for the valuables
- Possession of the keys doesn't automatically mean access to confidential information because there are other layers of security inside, such as server passwords and operating system protections
  - However, the issue of network access is put aside

Message Privacy

- If an attacker can get the keys, he can probably go undetected, which is important to buy the time to find useful information
  - If an attack is detected, the WEP keys can be changed, putting the attacker back to square one
- The next best thing to getting the keys is to be able to get the plaintext
  - If you can get the plaintext in a reasonably fast and reliable way, you have access to a range of other types of attacks using message modification and replay
  - That information can also be used as a stepping-stone to getting the keys
- There are three weaknesses in the way RC4 is used in WEP:
  - IV reuse
  - RC4 weak keys
  - Direct key attack

WEP Keys

- Protects eavesdropping by preventing repetition of RC4 Key



- IV is 24 bits; so total IVs = 224 = 16,777,216

- Probability of IV Repetition after 5,000 frames = 50 %

IV Reuse

- Instead of using a fixed secret key, the secret key is appended to a 24-bit IV value and then the combined IV / secret is used as the encryption key
- The value of the IV is sent in the frame so the receiving device can perform the decryption
- One purpose of the IV is to ensure that two identical messages don't produce the same ciphertext

IV Reuse

- Let's suppose for a moment that there was no IV and only the secret key is used for encryption
  - For every frame, the RC4 algorithm is initialized with the key value prior to the start of the pseudorandom key stream generation
  - But if the key were to remain fixed, the RC4 algorithm would be initialized to the same state every time
  - Therefore, the key stream produced would be the same sequence of bytes for every frame
  - This is disastrous because, if the attacker can figure out what that key stream is, he can decode every frame simply by XORing the frame with the known sequence
    - He doesn't need to know the key

IV Reuse

- By adding the IV value to the key each time, RC4 is initialized to a different state for every frame and so the key stream is different for each encryption
  - Let's review that statement because there is an implicit assumption: The IV value is different for every frame
  - If the IV is a constant value, you are no better off than in the static key case
- The constant IV is useless and using a different IV for every frame is a good idea
  - There are a limited number of possible IVs, so it is acceptable to use a different IV for most frames but eventually start reusing IVs that have been used in the past
  - The simple answer is that this is not acceptable, but it is precisely what WEP does

IV Reuse

- In reality a collision is likely much sooner because there may be many devices transmitting, each incrementing a separate IV value and using it with the same key
- Implementation errors can compound the problem
  - Wi-Fi LAN manufacturer may initialize the IV counter to 0 when the system is started up
- Imagine that ten users come into work and start up their laptops
  - Depending on who does what, the IV counter of some will get ahead of others, but there will be a rich harvest of IV collisions to be had by an observer

Direct Key Attacks

- The method can be tuned to attack each secret key byte in turn so eventually the entire secret key can be extracted
  - Note that increasing the key size from 40 bits to 104 bits means that it takes 2.5 times longer to extract the key (linear, not exponential)
- All the previous weaknesses of WEP pale into insignificance compared to this attack
  - Remember that extracting the keys is the ultimate goal of an attacker, and here is a method that directly extracts the keys in linear time
  - This attack blew apart the remnants of WEP security
  - Because it used a fairly mechanical approach, it was feasible to create a script tool that would do the job unattended
- Within months, some "helpful" person invested their time into generating a cracker tool

Thank you.
Questions?

Dr. Abdullah Aydeger