Securing Wireless LANs: Part 2

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- J. Kurose, K. Ross, "*Computer Networking: A Top Down Approach*", Sixth Edition, Pearson Education, 2013
- J. Edney, W.A. Arbaugh, "*Real 802.11 Security: Wi-Fi Protected Access and 802.11i*", Pearson Education, 2004.
- B.L. Menezes, R. Kumar, "*Cryptography, Network Security, and Cyber Laws*", CengageLearning India Pvt.Ltd., 2018

Weaknesses in WEP

- Several weaknesses have been discovered in WEP
- We discuss some of them
- In wireless networks, usually *mutual* authentication is required:
  - the mobile device should be able to check that the AP is legitimate
  - since easy for an intruder to set up a decoy AP
- Under the WEP authentication scheme, can the mobile device check whether the AP is legitimate?
  - No; a decoy AP can send some value as the nonce and then falsely claim that it was able to verify the encrypted nonce without knowing the key

Weaknesses in WEP (contd.)

- Recall: it is good security practice to use different keys for authentication and for encryption
  - ❑ in particular, a long-term key for authentication and session keys for encryption
- However, under WEP, the key used for authentication is also used for encryption of data packets in each session
  - ❑ this is a weakness of WEP

Weaknesses in WEP (contd.)

- Recall: after authentication, the two parties should agree upon session keys
  - ❑ we discussed several procedures for agreeing upon session keys
- However, after WEP authentication, no session keys are agreed upon
- Instead, after WEP authentication, the AP and mobile device start exchanging data encrypted using their long-term secret shared symmetric key
- Hence, the authentication process is futile
  - ❑ provides no advantage over scenario where the AP and mobile device directly start exchanging data encrypted using their long-term secret shared symmetric key

Weaknesses in WEP (contd.)

- Next, we show how an intruder can authenticate itself to an AP without knowing the key
- Suppose intruder sniffs channel while a legitimate mobile device is authenticating itself
- Collects the following:
  - Nonce, say P, sent from AP to mobile device (in plaintext form)
  - Ciphertext, say C, obtained by encrypting P using WEP's encryption protocol and the IV that was used (these are sent from mobile device to AP)
- Intruder can recover the key value stream $k_1^{IV}, k_2^{IV}, k_3^{IV}$,…:
  - by taking XOR of P and C
- Can intruder use the information obtained so far to later authenticate itself?
  - Yes; intruder now knows the key stream corresponding to the above IV value
  - Intruder requests authentication, takes nonce, say P', sent by AP, XORs it with recovered key value stream and sends it back along with above IV value
- Thus, intruder can authenticate itself without knowing the secret key

Weaknesses in WEP (contd.)

- Consider an intruder who is trying to break WEP encryption
- While attacking an encryption algorithm, it is often useful for intruder to obtain some known plaintext blocks and their corresponding ciphertext blocks
  - e.g., when monoalphabetic cipher used, if intruder obtains the plaintext block "attack at noon" and corresponding ciphertext block "muumbf mu jkkj", then he/ she knows the ciphertext letters corresponding to the plaintext letters a, t, c, k, n, o
- Usually, it is hard for an intruder to obtain known plaintext blocks and their corresponding ciphertext blocks
- When WEP authentication is used, intruder easily obtains a known plaintext block and its corresponding ciphertext block:
  - since AP sends a 128-byte nonce in plaintext form and mobile device responds with the encrypted nonce
- Since same key used for authentication and encryption, these can be helpful to an intruder who is trying to break WEP encryption
- Summary: not only does the WEP authentication process not authenticate, but it can actually assist an intruder in attacking the encryption keys

Weaknesses in WEP (contd.)

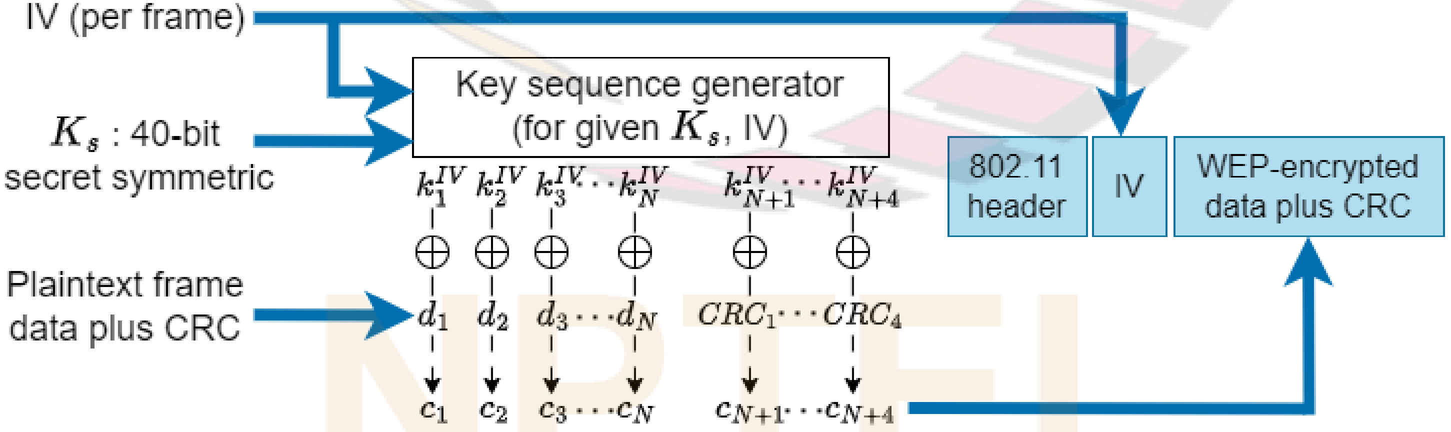
- Replay prevention:
  - ❑ suppose a legitimate mobile device exchanged some data packets with AP, which were recorded by an intruder
- Later, intruder can replay one or more of those packets
- Need a mechanism to prevent such replay:
  - ❑ recall: we discussed that sequence numbers can be used for this
- However, WEP provides no protection against replay:
  - ❑ there is a sequence number in 802.11 medium access control (MAC) header, which increases monotonically
  - ❑ but it is not encrypted, and no message authentication code is computed over the sequence number
- Hence, easy for intruder to modify the sequence number in a replayed packet to be valid

Message Integrity

- Recall: message integrity:
  - ❑ it should not be possible for an intruder to sniff a packet from sender, modify it and send modified version to receiver
- We earlier studied the following general method for achieving message integrity when Alice sends a message to Bob
- Alice performs the following actions:
  - ❑ computes checksum of m, say $c(m)$
  - ❑ concatenates m and $c(m)$ to get $(m, c(m))$
  - ❑ sends its encrypted version, $K_A(m, c(m))$, to Bob
- Bob finds $K_B(K_A(m, c(m))) = (m, c(m))$ and checks whether checksum of m equals $c(m)$
- We discussed that above method correctly achieves message integrity
- WEP uses above method for achieving message integrity
- However, above method applied in a way that makes it insecure

Message Integrity (contd.)

- Mechanism in WEP to provide message integrity:
  - ❑ suppose plaintext data is N bytes in length; 4-byte Cyclic Redundancy Check (CRC) computed for it
  - ❑ the 64-bit key used to generate a stream of key values (1 byte each), k_1^{IV}, k_2^{IV}, k_3^{IV},… using RC4 stream cipher
  - ❑ ciphertext obtained by XORing (plaintext data+CRC) with the key value stream



Weaknesses in WEP (contd.)

- Above mechanism for message integrity is not secure for following reasons
- Method used to compute the 4-byte CRC such that:
  - ❑ it is possible to predict which bits in the CRC will change if we change a single bit in the data message
- But recall that (message data+CRC) is XORed with key value stream, which is unknown to intruder
- Can an intruder still break message integrity of WEP?
  - ❑ Yes, since XOR has the property that if $x \oplus k = y$, then $\bar{x} \oplus k = \bar{y}$
  - ❑ So attacker can change some bits of ciphertext corresponding to message data, predict which bits of CRC should be changed to keep CRC valid, and change corresponding bits of ciphertext

Weaknesses in WEP (contd.)

- It was also shown that an attacker can find the secret key (used for encryption) in a small amount of time after eavesdropping on the network
- Depending on the amount of network traffic, a successful key recovery may take as little as one minute
- Automated tools are available on the Internet that implement above attack
- For details, see:
  - J. Edney, W.A. Arbaugh, "*Real 802.11 Security: Wi-Fi Protected Access and 802.11i*", Pearson Education, 2004.
  - S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," *Eighth Annual Workshop on Selected Areas in Cryptography*, Toronto, Canada, Aug. 2002.
- Due to above weaknesses, WEP was deprecated by IEEE
- In 2004, 802.11i, a more secure standard for 802.11 security was adopted