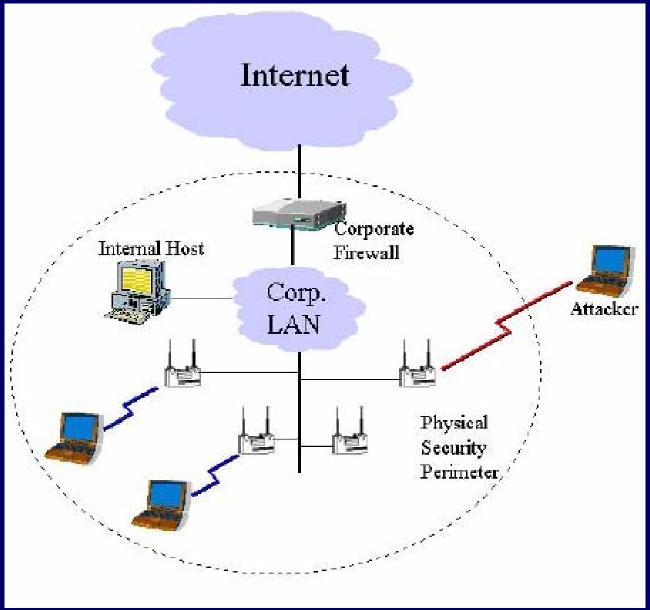
CS 395T

William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan



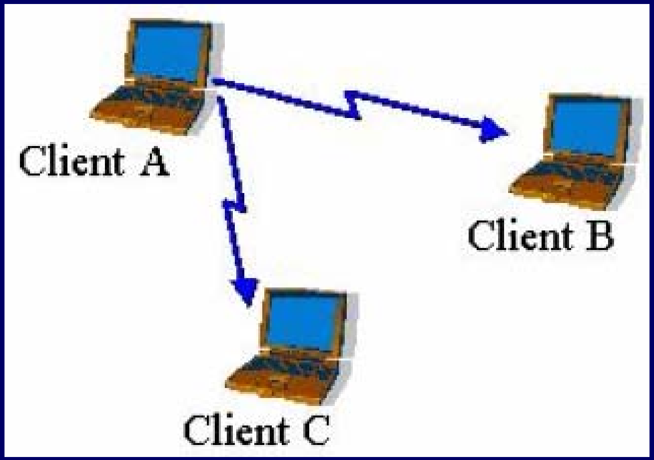
Intercepting Mobile Communications: The Insecurity of 802.11

Nikita Borisov, Ian Goldberg, David Wagner

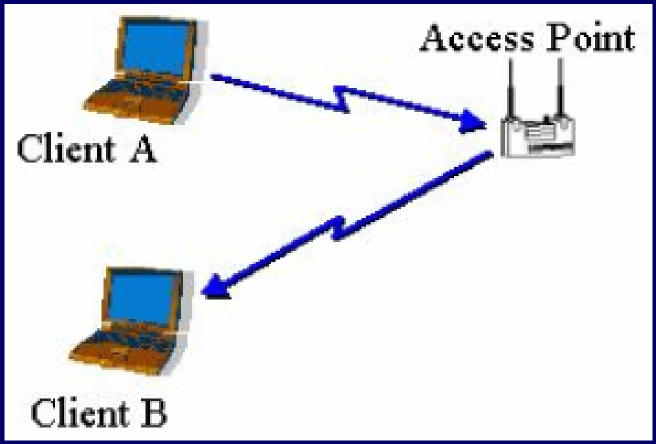
802.11 Wireless Networks

Two modes of operation :

1) Independent Basic Service Set (IBSS), aka *ad-hoc* mode

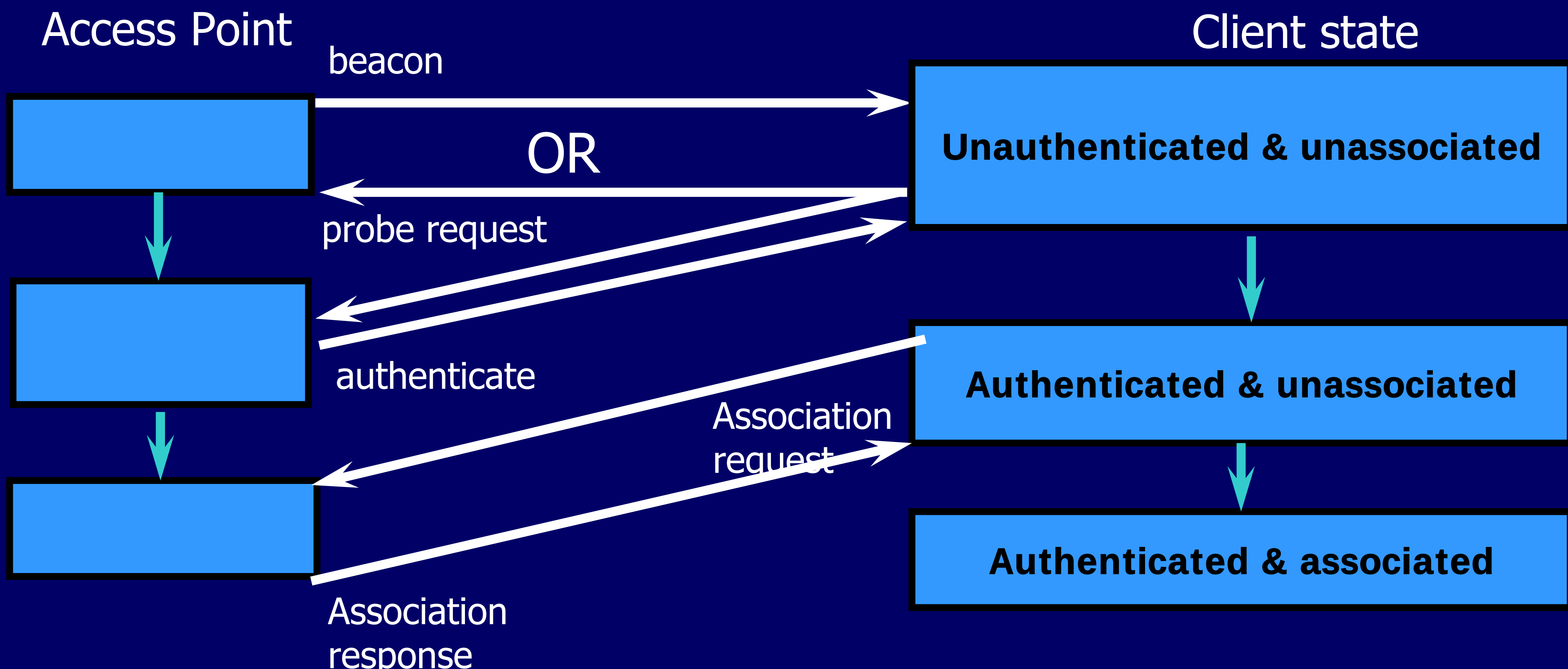


1) Basic Service Set (BSS), aka *infrastructure* mode

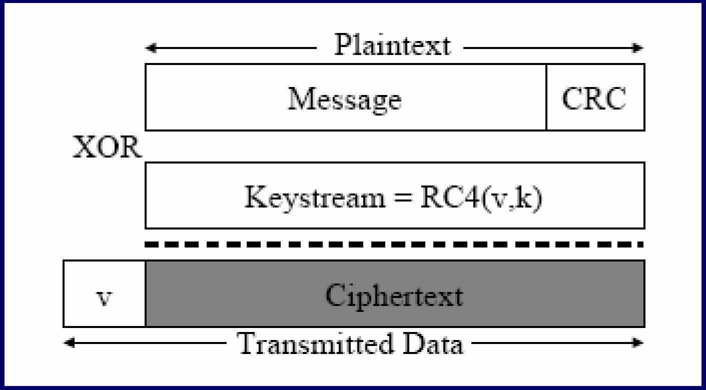


802.11 Wireless Networks cont'd

Prior to communicating data wireless clients and access points exchange management frames to establish an *association*



Wired Equivalent Privacy (WEP) Protocol



- K is secret key between communicating parties
- V is initialization vector (IV) for RC4
- keystream is long sequence of pseudorandom bits

$$P' = C \text{ XOR } RC4(v, k)$$
$$= (P \text{ XOR } RC4(v, k)) \text{ XOR } RC4(v,k)$$
$$= P$$

- checksum c(M') re-computed to ensure only frames with valid checksums are accepted

WEP cont'd: security goals

Security "relies on the difficulty of discovering the secret key through a brute-force attack"

1) Confidentiality – prevent eavesdropping
2) Access control
   a. 802.11 provides option to discard all packets not properly encrypted not using WEP
3) Data integrity - checksum

WEP cont'd: flavors

- classic, or standard, with 40-bit keys
  - Meets US Government export regulations
  - Susceptible to brute-force attacks
- Extended "128-bit" version
  - 104-bit keys

WEP documents state "Eavesdropping is a familiar problem to users of other types of wireless technology"

Keystream reuse

If $C_1 = P_1 \oplus \mathrm{RC4}(v, k)$

and $C_2 = P_2 \oplus \mathrm{RC4}(v, k)$

then

$$\begin{aligned} C_1 \oplus C_2 &= (P_1 \oplus \mathrm{RC4}(v, k)) \oplus (P_2 \oplus \mathrm{RC4}(v, k)) \\ &= P_1 \oplus P_2. \end{aligned}$$

- If one plaintext known other's immediately attainable
  - Real world plaintexts have enough redundancies that this isn't even necessary
- *depth n* problems – n ciphertexts that all reuse the same keystream
  - WEP standards recommend, but do not require, a per-stream IV to combat this
  - Some PCMCIA cards reset IV to 0 each time they're re-initialized and increment by 1, so expect reuse of low-value IVs
  - WEP only uses 24-bit IVs → "birthday paradox" if it's random

Keystream reuse cont'd

- Other ways to recover plaintext
  - IP traffic can be predicted since protocols use well-defined structures in messages; ex. login sequence
  - If you know plaintext beforehand compare with encrypted form to learn keystream
- Once a keystream is learned other messages using same IV can be decrypted
  - Table can be built for keystreams of each IV
  - Since IV size is fixed larger keys won't help
- 802.11 relies on external mechanism to populate globally shared array of 4 keys
  - Each message's key identifier is index into array
  - Most installations use single key (!), increasing chance for IV collisions

Message Authentication

- Message Modification since WEP checksum (CRC-32) is linear function of message
  - Assume arbitrary modification Δ

$$\begin{aligned} C' &= C \oplus \langle \Delta, c(\Delta) \rangle \\ &= \mathrm{RC4}(v,k) \oplus \langle M, c(M) \rangle \oplus \langle \Delta, c(\Delta) \rangle \\ &= \mathrm{RC4}(v,k) \oplus \langle M \oplus \Delta, c(M) \oplus c(\Delta) \rangle \\ &= \mathrm{RC4}(v,k) \oplus \langle M', c(M \oplus \Delta) \rangle \\ &= \mathrm{RC4}(v,k) \oplus \langle M', c(M') \rangle. \end{aligned}$$

  - Attacker doesn't need full knowledge of M

- Message Injection
  - If you know plaintext and ciphertext, keystream will be revealed and can be reused to create new packets
  - Receiver has to take it since 802.11 doesn't say IVs can't be reused
  - Using MAC instead of WEP checksum doesn't help against replay; besides, MAC can be reprogrammed and hence spoofed

Message Authentication cont'd

- Authentication spoofing
  1) Mobile station requests shared-key authentication
  2) Access point sends it a *challenge*, a 128-byte random string, in cleartext.
  3) Mobile station responds with the same challenge encrypted using WEP.
  4) If authentication successful, roles are reversed and process repeated for mutual authentication
  - Ability to generate encrypted version of the challenge is considered proof of key possession
  - Monitoring such a sequence, adversary can learn keystream

Message Authentication cont'd: Message Decryption

- IP redirection
  - Adversary modifies destination address to itself and lets access point handle decryption
  - Adversary needs to make sure IP checksum is correct; new checksum $x' = x + D'_H + D'_L - D_H - D_L$
  - 1) If x is known, straightforward
  - 2) trial and error
  - 3) x = x' and modify another field so checksum holds

Countermeasures

- Place wireless networks outside organizational firewall, and no routes to outside Internet exists on wireless Intranet
  - Use VPN