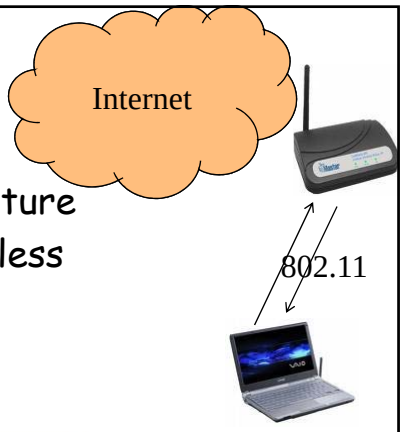
Last-Hop Wireless Networks

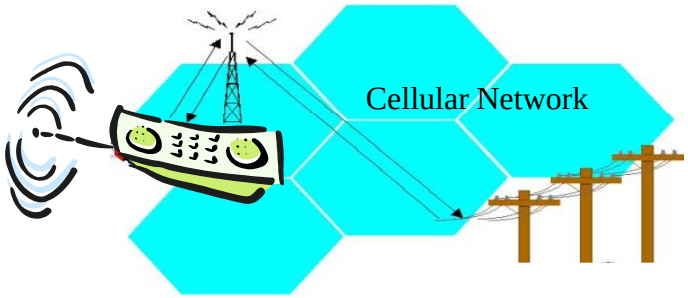
Wireless LANs (e.g., 802.11x)
Cellular (e.g., GSM)
Bluetooth, Infrared, RFID, etc.

1

Last-Hop Wireless



- Rely on extensive infrastructure
- Usually, only last hop is wireless
- Only end-node is mobile



2

What security needed?

- End-node access control
- End-node ←→ infrastructure authentication
- Encrypted, authenticated communication
- Anonymity/Pseudonymity: who is this end-node? Where does he move from/to?
  - From infrastructure?
  - From others (eavesdroppers)?

3

802.11 security (Kurose/Ross Ch. 8)

- *war-driving:* drive around your city/neighborhood, see what 802.11 networks available?
  - Many are accessible from public spaces
  - Most don't use encryption/authentication
  - Packet-sniffing and various other attacks are easy!
    - Eavesdropping, spoofing, bw consumption (DoS), framing!
- securing 802.11
  - encryption, authentication
  - first attempt at 802.11 security – Wired Equivalent Privacy (WEP): a failure
  - current approach: 802.11i

4

Wired Equivalent Privacy (WEP):

- Simple authentication:
  - host requests authentication from access point
  - access point sends 128-bit nonce (random number)
  - host encrypts nonce using shared symmetric key
  - access point decrypts nonce, authenticates host
- no key distribution mechanism
- authentication: knowing the shared key is enough (assumed host already knows shared key)

5

WEP data encryption

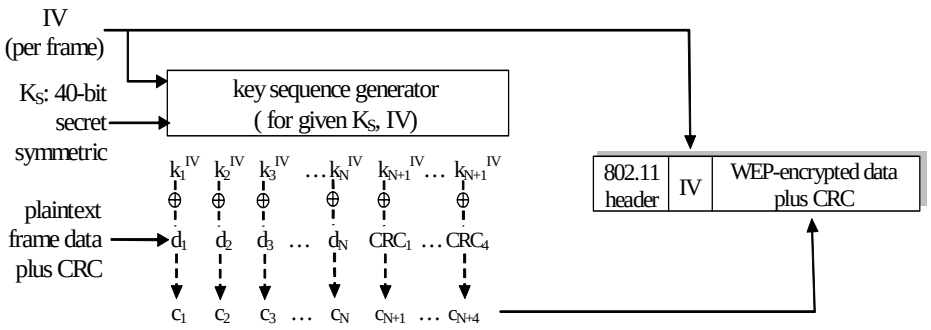
- Host & AP share a 40-bit symmetric key
- In each frame, host appends a 24-bit initialization vector (IV) to create a 64-bit key
- 64-bit key used to generate a key-stream: k_i^{IV}
- k_i^{IV} used to encrypt i-th byte, d_i, in frame:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV and encrypted bytes, c_i sent in frame

6

802.11 WEP encryption



Sender-side WEP encryption

Breaking 802.11 WEP encryption

security hole:

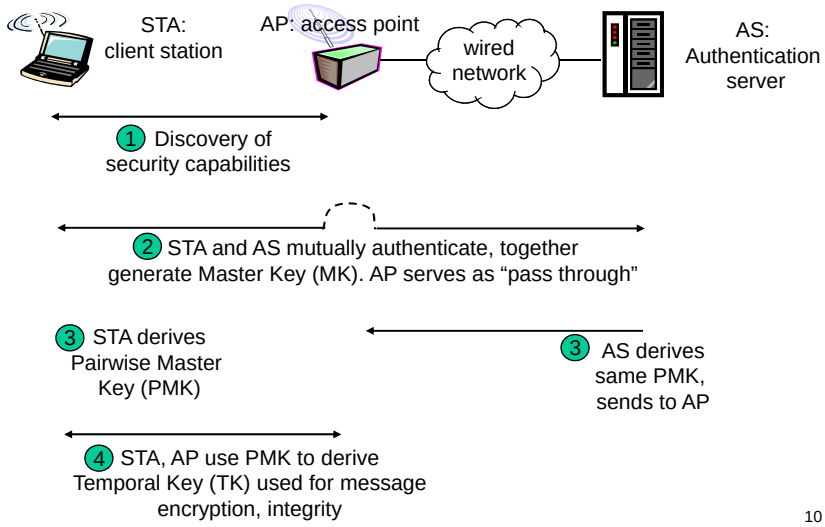
- 24-bit IV, one IV per frame → IV-s eventually reused
- IV transmitted in plaintext → IV reuse detected
- attack:
  - Eve causes Alice to encrypt known plaintext: d_1 d_2 d_3 d_4
  - …
  - Eve sees: $c_i = d_i$ XOR k_i^{IV}
  - Eve knows c_i d_i, so can compute k_i^{IV}
  - Eve knows encrypting key sequence k_1^{IV} k_2^{IV} k_3^{IV} …
  - Next time same IV is used, Eve can decrypt!

802.11i: improved security

- numerous (stronger) forms of encryption possible
- provides key distribution
- uses authentication server distinct from access point

9

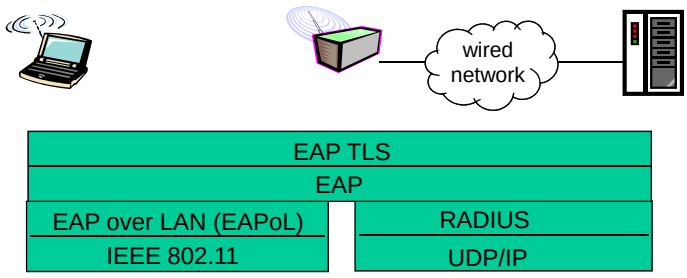
802.11i: four phases of operation



10

EAP: Extensible Authentication Protocol

- EAP: end-end client (mobile) to authentication server protocol
- EAP sent over separate "links"
  - mobile-to-AP (EAP over LAN)
  - AP to authentication server (RADIUS over UDP)



11

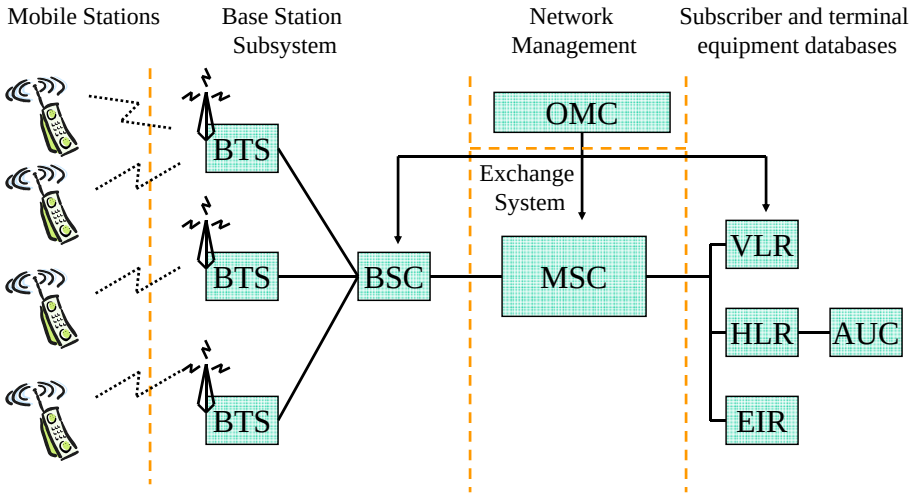
GSM Security

- Good overview of GSM Security:

http://www.cs.huji.ac.il/~sans/students_lectures/GSM%20Security.ppt

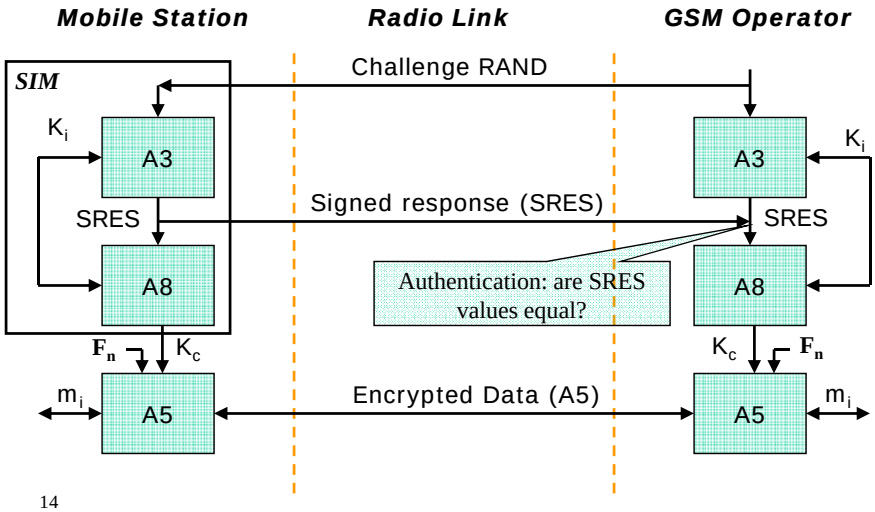
12

GSM Architecture



13

Authentication & Encryption



14