CSC429 – Computer Security

LECTURE 13
WIRELESS SECURITY

Mohammed H. Almeshekah, PhD
meshekah@ksu.edu.sa

Wireless Communication

- IEEE 802 is a dominant collection of networking standards developed by IEEE.
  - E.g. IEEE 802.3 specifies the physical and data link layer properties of Ethernet.
- IEEE 802.11 is a family of standards for wireless LANs.
  - Provides protocols at Layer 1 & Layer 2 of OSI model.

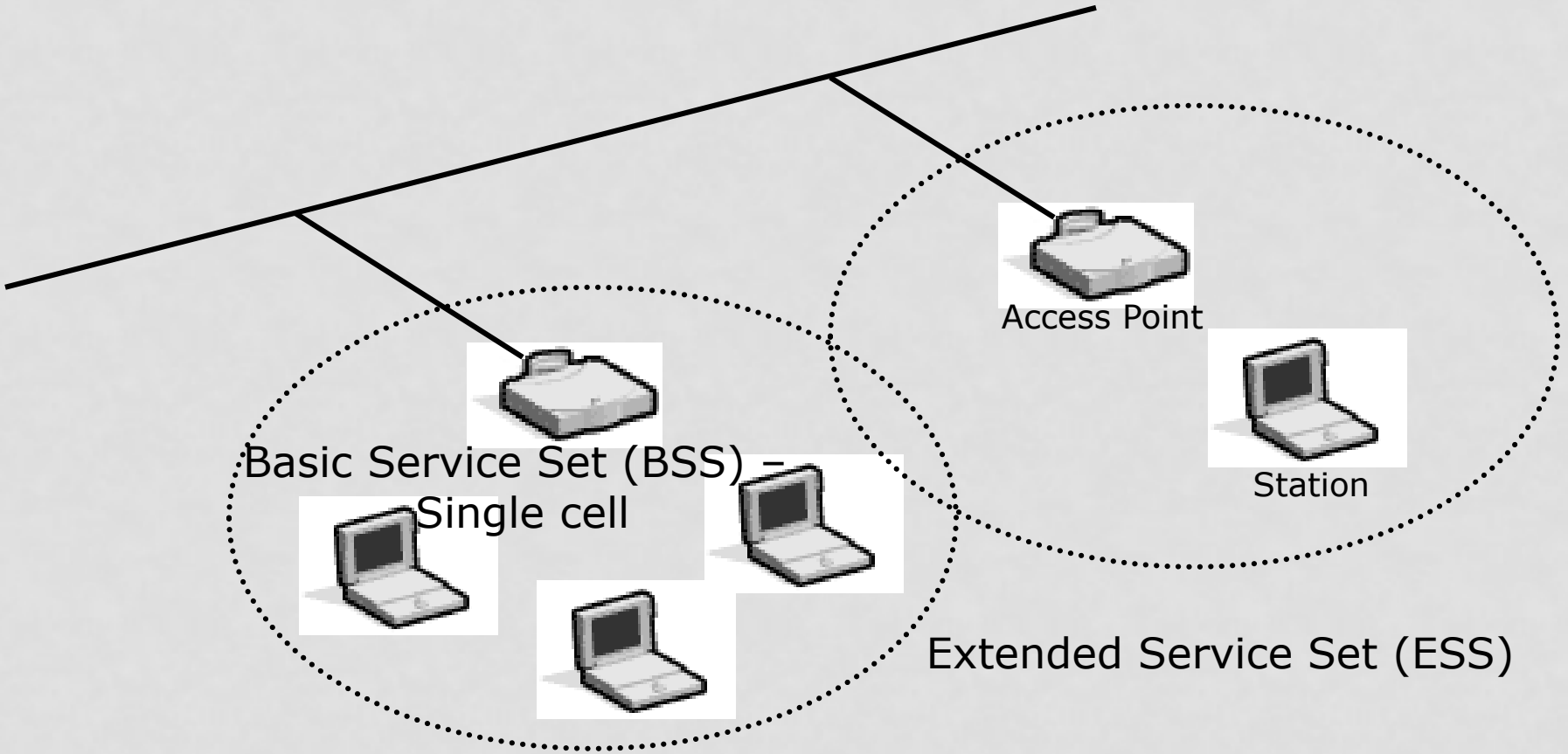
802.11 Components

- Two pieces of equipment defined:
  - Wireless station
    - A desktop or laptop PC or PDA with a wireless NIC.
  - Access point
    - A bridge between wireless and wired networks
    - Composed of
      - Radio
      - Wired network interface (usually 802.3)
      - Bridging software
    - Aggregates access for multiple wireless stations to wired network.

802.11 Modes

- Infrastructure mode
  - Basic Service Set (BSS)
    - One access point
  - Extended Service Set
    - Two or more BSSs forming a single subnet.
- Ad-hoc mode
  - Also called peer-to-peer.
  - Set of 802.11 wireless stations that communicate directly without an access point.
    - Useful for quick & easy wireless networks.

Infrastructure Mode



Joining a BSS

- When 802.11 client enters range of one or more APs:
  - APs send beacons.
  - AP beacon can include SSID.
  - AP chosen on signal strength and observed error rates.
  - After AP accepts client.
    - Client tunes to AP channel.
- Periodically, all channels surveyed.
  - To check for stronger or more reliable APs.
  - If found, may reassociate with new AP.

Wireless Security

Security of IEEE 802.11

Security of IEEE 802.11

1. Authentication and Access Control.
2. Interception.

3. Wired Equivalent Privacy (WEP).
4. WiFi Protected Access (WPA).
5. WPA2

Authentication & Access Control

Open System Authentication:

- Relies on Service Set Identifier (SSID).
- Station must specify SSID to Access Point when requesting association.
- APs can broadcast their SSID as a beacon.

Is it reliable authentication?

- i.e. you can only join if you know the SSID!

SSID Hiding

- AP can choose not to transmit SSID in its beacons.
- Can still attack APs that don't transmit SSID:
  - Send deauthenticate frames to client.
  - SSID then captured when client sends reauthenticate frames containing SSID.
  - Implemented in "essid_jack" tool.
- Open System Authentication only provides **trivial** level of security.

Authentication & Access Control

- Access points may have Access Control Lists (ACLs).
- ACL is a list of allowed MAC addresses.
  - E.g. only allow access to:
    - 00:01:42:0E:12:1F
    - 00:01:42:F1:72:AE
    - 00:01:42:4F:E2:01
- But MAC addresses are sniffable and spoofable.
- Hence MAC ACLs are of limited value.
  - Will not prevent determined attacker.

Interception

- Wireless LAN uses radio signal.
- Not limited to physical building.
- Directional antenna allows interception over longer distances.
  - Record is 304 kilometre for an unamplified wifi signal (using a 120 centimetre antenna).

Wireless Security

Wired Equivalent Privacy

Wired Equivalence Privacy (WEP)

- Shared key between stations and an Access Point.
  - All Access Points will have same shared key in ESS.
- Key used in stream cipher to encrypt WLAN traffic.
- No key management.
  - Shared key entered manually into wireless stations and Access points.
  - Key never expires.
  - Key management problems in large wireless LANs.

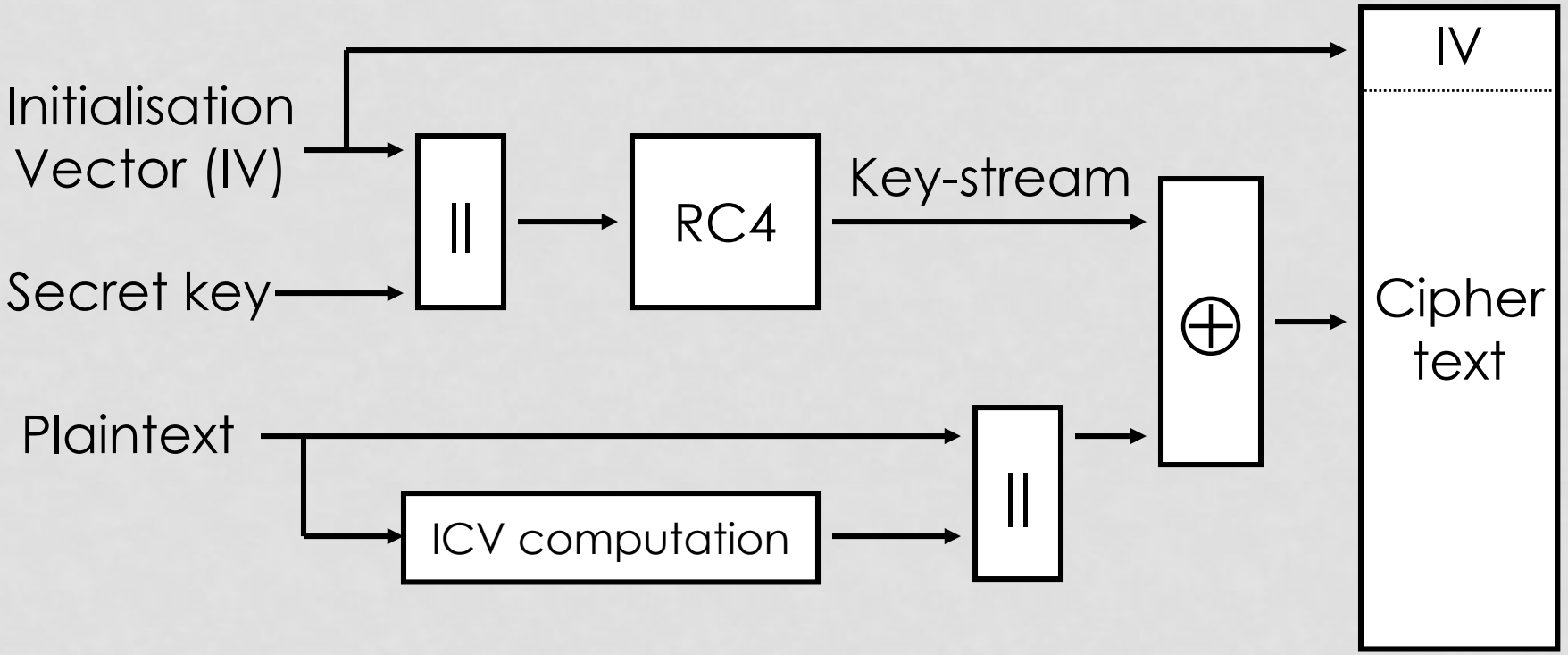
WEP Stream Cipher

- WEP uses RC4 stream cipher
  - Proprietary to RSA Security Inc.
  - Designed in 1987 by Ron Rivest.
  - Trade secret until reverse-engineered in 1994.
- RC4 can use key sizes from 1 bit to 2048 bits.
  - WEP typically uses 40-bit key.
- RC4 algorithm generates a stream of pseudo-random bits.
  - Using key and Initialisation Vector (IV) as input.
  - Called the key-stream.
  - Key-stream is XOR'd bit-by-bit with frame data.

WEP – Sending

- Compute Integrity Check Vector (ICV).
  - 32-bit Cyclic Redundancy Check (CRC).
  - Keyless algorithm, specified in IEEE standard.
  - Appended to message to create plaintext for encryption.
- Plaintext then encrypted using RC4 stream cipher.
  - RC4 is initialised with
    - 40-bit secret key
    - 24-bit initialisation vector (IV)
  - RC4 generates the key-stream as function of these 64 bits.
  - Key-stream XOR'd with plaintext to generate ciphertext.
- Ciphertext is transmitted along with IV.

WEP Encryption



WEP – Receiving

- Ciphertext is received.
- Ciphertext decrypted using RC4 stream cipher.
  - RC4 initialised with:
    - 40-bit secret key;
    - 24-bit initialisation vector (IV) from start of ciphertext.
  - RC4 generates key-stream as function of these 64 bits.
  - Key-stream XOR'd with ciphertext to recover plaintext.

- Check ICV
  - Separate plaintext to obtain ICV and message.
  - Compute expected ICV for message.
  - Compare with received ICV.

Shared Key Authentication

- Station requests association with AP.
- AP sends challenge to station.
- Station encrypts challenge using WEP to produce response.
  - Uses RC4, 40-bit shared secret key & 24-bit IV selected by station.
- Response received by AP, decrypted by AP and result compared to initial challenge.

WEP Safeguards

- Shared secret key required for:
  - Associating with an access point.
  - Sending data.
  - Receiving data.
- Messages are encrypted.
  - Confidentiality.
- Messages have checksum.
  - Intended to provide integrity.

WEP Vulnerabilities

1. Insecure Authentication Protocol.
2. IV Vulnerabilities.
3. Passive Attacks.
4. Active Attacks.
5. Limited WEP Keys.
6. Brute-force Attacks.

Insecurity of Shared Key Authentication

- Rogue station records run of authentication protocol.
- Uses known plaintext (challenge) to compute portion of key-stream for the (known) IV.
  - Recall that C = P XOR key-stream.
- Rogue station can now respond to *any* future authentication challenge from AP.
  - Rogue receives fresh challenge.
  - Wireless station gets to choose IV in protocol.
  - But same IV (and same secret key) means that RC4 produces the same key-stream bits.
  - Hence rogue who repeats IV can reuse old key-stream portion to encrypt, producing correct response.
- Moral: A stream cipher is a very poor choice as an encryption primitive in an challenge-response protocol.

Initialisation Vector

- IV should be different for every message transmitted.
- But 802.11 standard doesn't specify how IV is calculated.
- Wireless cards use several methods:
  - Some use a simple ascending counter for each message.
  - Some switch between alternate ascending and descending counters.
  - Some use a pseudo-random IV generator.

Passive WEP Attack

- If 24-bit IV is an ascending counter, and if Access Point transmits at 11 Mbps, then all IVs are exhausted in roughly 5 hours.
- Passive attack:
  - Attacker collects all traffic.
  - Attacker will eventually collect two messages encrypted with same key and same IV.
  - Statistical attacks may then reveal plaintext:

    XOR of ciphertexts = XOR of plaintexts.
  - Hard to extract plaintexts this way in reality.
  - Much better attacks are available against WEP…

Active WEP Attacks

- If attacker knows plaintext/ciphertext pair and IV:
  - Corresponding key-stream is then known.
  - Now attacker can create correctly encrypted messages by repeating IV.
  - Access Point is deceived into accepting messages.
  - And short key-streams are obtained for free by observing runs of the authentication protocol!

Limited WEP Keys

- Some vendors allow limited WEP keys.
  - User types in a pass-phrase.
  - WEP key is generated from pass-phrase.
  - Pass-phrases creates as few as 21 bits of entropy in 40-bit key.
    - Reduces key strength to 21 bits; 2^{21} = 2,097,152.
    - 21-bit key can be brute forced in minutes.

Brute Force Key Attack

- Capture ciphertext.
  - IV is included in message.
- Search all 2^{40} possible secret keys.
  - A few days on a modern laptop.
- Select key that decrypts ciphertext to a meaningful plaintext.
  - WLAN logical link control layer frames have well-defined format.
  - E.g. first two bytes are always AA, AA (hex).
  - Automated recognition of correct key is possible.
- 40-bit keys do not provide adequate security.

Brute Force Key Attack

- Vendors have extended WEP to 128-bit keys.
  - 104-bit secret key.
  - 24-bit IV.
- Brute force now infeasible.
- Effectively safeguards against brute force attacks.
- But …

The FMS Attack

- Paper from Fluhrer, Mantin, Shamir, 2001.
  - *www.isoc.org/isoc/conferences/ndss/02/papers/stubbl.pdf*
- Detailed analysis of several features of RC4 key scheduling algorithm.
- Main result of interest to us:
  - If the RC4 key is composed from a known IV and an unknown secret part by concatenation;
  - And if the attacker knows the first byte of key-stream for enough different IVs;
    - Then the *whole* RC4 key can be determined in a statistical attack.
    - Attack only makes use of some of the IVs – so-called "weak" IVs.

Automated Tools to Break WEP

- Wepcrack
  - First tool to demonstrate FMS attack using IV weakness.
  - http://wepcrack.sourceforge.net/
- Aircrack-ng
  - Automated tool for mounting FMS attack
  - http://www.aircrack-ng.org/doku.php

WEP – Last Words

- The WEP authentication protocol is trivially breakable.
- The WEP encryption method is severely weakened by FMS and related attacks.