Security in IEEE 802.11 WLANs
IEEE 802.11 Architecture

Extended Service Set (ESS)

Basic Service Set (BSS)

AP$_1$

MS

AP$_2$

MS

AP$_3$

Distribution System

LAN Segment

Courtesy: Prashant Krishnamurthy, Univ Pittsburgh
Operational Details

- There are two modes of operation of IEEE 802.11
  - Infrastructure mode
  - Ad hoc mode

- Infrastructure Mode
  - All communications go through an AP
  - MS to MS communications does not happen
  - Specifies the BSS or ESS ID or SSID as it is sometimes called
  - Some systems filter MAC addresses – spoofing is easy
    - Registered addresses at BS
    - MAC address changeable in software.
  - We focus on this mode of operation

- Ad hoc mode
  - MSs communicate with each other in a peer-to-peer manner
  - MSs do not forward packets – there is NO multi-hop communications
  - MSs have to be in range of one another in order to communicate
Association

- To deliver a frame to a MS
  - The distribution system must know which AP is serving the MS

- Association
  - Procedure by which a MS “registers” with an AP
  - Only after association can a MS send packets through an AP

- How the association information is maintained in the distribution system is NOT specified by the standard.
  - Each vendor has proprietary method.
  - Non volatile memory at Access Point where a table is stored as to which MAC layer addresses are allowed and which mobile station is currently associated.
Re-association and Dissociation

- The **re-association** service is used when a MS moves from one BSS to another within the same ESS.
- It is always initiated by the MS.
- It enables the distribution system to recognize the fact that the MS has moved its association from one AP to another.

- The **dissociation** service is used to terminate an association.
- It may be invoked by either party to an association (the AP or the MS).
- It is a notification and not a request. It cannot be refused.
- MSs leaving a BSS will send a dissociation message to the AP which need not be always received.
Handoff in 802.11

1. Strong signal
2. Weak signal; Start scanning for handoff
3. Probe Request from MS
4. Probe response
5. Choose AP with strongest response
6. Reassociation Request
7. Reassociation Response
8. IAPP indicates reassociation to old AP

Beacon periodically

IAPP: Inter Access Point Protocol

Courtesy: Prashant Krishnamurthy, Univ Pittsburgh
Types of Messages in 802.11

- Control messages
  - Short messages – primarily ACKs

- Management messages
  - Messages between MSs and APs to negotiate set-up
  - Examples are association request and responses
  - Carries information about capabilities of the network (data rates, radio parameters, power saving flags, etc.)

- Data frames
  - Actual layer 2 frames transmitted by either the AP or the MS
Management Frames in 802.11

- **Beacon**
  - Timestamp, beacon interval, capabilities, ESSID, traffic indication map (TIM), { If no traffic as per TIM, MS will sleep for a beacon interval (to come)}

- **Probe**
  - ESSID, Capabilities, Supported Rates

- **Probe Response**
  - same as beacon except for TIM

- **Re-association Request**
  - Capability, listen interval, ESSID, supported rates, old AP address

- **Re-association Response**
  - Capability, status code, station ID, supported rates
Beacon

Beacon is a message that is transmitted quasi-periodically by the access point.
It contains information such as the BSS-ID, timestamp (for synchronization), traffic indication map (for sleep mode), power management, and roaming.
Beacons are always transmitted at the expected beacon interval unless the medium is busy.
RSS measurements are made on the beacon message.
Wired Equivalent Privacy – WEP

- **Background**
  - The only standard for WLAN security till 2000
  - Still used by a large number of legacy implementations

- **Objectives behind WEP**
  - “Reasonable” strength
    - Intended to make it difficult to break-in like a wired network
  - Self synchronizing
    - Each frame is encrypted independently of the others
  - Efficient
    - It must be fast and in software or hardware
  - Exportable
    - There must be no export restriction (1997) – use 40 bit keys
  - Optional

- **Specified tow options**
  - Open security and shared key options
RC4 Stream Cipher

- Stream cipher designed by Ron Rivest (the \textit{R} in RSA) in 1987
  - Encryption is by the byte
  - Period is greater than $10^{100}$
  - Very simple to implement in software or hardware
  - At least twice as fast as any comparable block cipher
- Algorithm was kept secret by RSA Security
  - RC4 was released anonymously in 1994
- Popular encryption scheme
  - Used in IEEE 802.11 Wired Equivalent Privacy (WEP), CDPD, SSL and many other applications
RC4 Algorithm (I)

- **Parameters**
  - A key K
    - Key length in bytes is variable from 1 to 256
    - In WEP, 40 bit key and 24 bit IV ==> K.
  - State vector S with 256 bytes
    - S = S[0], S[1], ..., S[255]
  - Temporary vector T
    - T = T[0], T[1], ..., T[255]

- **Initialization**
  - Set S to have values from 0 to 255
    - S[0] = 0, S[1] = 1, ..., S[255] = 255
  - Transfer K into vector T
    - Repeat K till it fills up T
    - Suppose K has 10 bytes – K[0], K[1], ..., K[9]
RC4 Algorithm (II)

- **Initial permutation of S**
  - Swap the elements of S according to T
  - Initialize an index j to zero
  - For i = 0 to 255
    - Compute \( j = (j+S[i]+T[i]) \mod 256 \)
    - Swap(S[i], S[j])

- **Stream generation**
  - i = 0;
  - j = 0;
  - i = i + 1 \mod 256
  - j = j + S[i] \mod 256
  - Swap(S[i], S[j])
  - t = (S[i] + S[j]) \mod 256
  - k = S[t] (the key which is used to XOR with data)
  - Go to A
Strength of RC4

- RC4 is strong if long key sizes are used (e.g., 128 bits)
- There are several attacks for small key sizes
  - Fluhrer, Mantin and Shamir (FMS) attack
    - Can predict key stream with small number of steps
- WEP has its own flaws that are independent of RC4, but can be exploited in conjunction with RC4
WEP Keys

- Characteristics
  - Keys are either 40 or 104 bits long and symmetric
  - Keys are static – they never change unless manually reconfigured
- Two types – default and key mapping keys
  - Default key
    - All MSs and APs use a single set of keys
    - Also called shared key, group key, multicast key or simply key by vendors
    - Possible to have more than one default key (up to 4 values)
      - The default key in use is called the active key
      - Directional usage of keys is also possible
  - Key mapping keys – not widely deployed
    - Each MS has a unique key (also called per-station or individual key)
    - AP keeps a table of MSs and keys
    - Need a separate key for multicast/broadcast messages that is shared by all MSs
- Both types of keys can be allowed simultaneously in a WLAN
WEP Encryption Process

- Data is broken up into fragments suitable for transmission on an 802.11 frame.
- An ICV is attached to the data fragment:
  - ICV = integrity check value
  - Uses a CRC
  - It is used as an alternative to a message authentication code!!
- Process:
  - Station selects an IV
  - Appends IV to the secret key
  - Initializes RC-4 algorithm
  - Creates key stream
  - Encrypts Data || ICV

- Station appends:
  - 24 bits IV and Key ID (specifies default key number) to encrypted part
  - Attaches MAC header informs the receiver that the packet is encrypted
WEP Authentication

- **Open authentication**
  - AP accepts connections from all MSs
  - MSs connect to any available AP that is willing to accept a connection

- **Shared key authentication**
  - Uses a version of the challenge response protocol
    - sent as clear text.
  - There is NO key exchange as part of the protocol
  - Easy to hijack sessions after authentication is performed if subsequent encryption is not used
    - You can observe both challenge and response (response simply XORs the challenge with key stream) and regenerate key stream.
  - Used primarily to eliminate confusion for honest MSs
  - Most systems do not implement any authentication at all
WEP Authentication

- **Idea**
  - Allow the AP to know that the MS possesses the right secret key

- **Process**
  - The AP sends a 128 byte arbitrary challenge text
  - The MS responds by encrypting the random message with the correct key
  - Algorithm used in RC-4

- The authentication is NOT mutual.
WEP Confidentiality

- Data packets are all encrypted using RC-4 stream cipher
  - You should NOT use the same key with a stream cipher to encrypt two message (why?)
  - Each packet in IEEE 802.11 is encrypted separately
  - There is only one key shared between the MS and AP
  - How can we avoid the problem with stream ciphers?

- Idea in WEP
  - Combine the secret key with a 24-bit initialization vector (IV) that changes for every packet
  - This increase the key “size” from 40 to 64 bits
  - For proprietary implementations, the key size goes up from 104 to 128 bits (with 24 bit IV).
WEP Confidentiality - Weakness

- To be effective, the same IV must never be used twice –
  - $2^{24} = 16,777,216$
  - No. of packets/sec at a busy AP = 700
  - Time taken to capture $2^{24}$ packets = $2^{24}/700 = 23968$ secs. = 399 mins = 6.65 hours

- Many systems
  - Start with the same IV value after shutting down
  - Change IVs in a pseudorandom manner that is predictable
  - Make all MSs start the same sequence of IVs
Attacks against WEP - 1

- **Authentication**
  - Necessary to authenticate each packet -- but not the case.
  - It allows offline key guessing
    - Remember how RC-4 works
    - Oscar can authenticate himself ANYTIME
  - No session key is exchanged and subsequent messages are not authenticated
  - The AP is not authenticated – easy for Oscar to mount a man-in-the-middle or reflection attack

- **Other weaknesses**
  - WEP has no protection against replay
  - WEP encrypted messages can be modified easily because the CRC used for the ICV is linear and encryption is just XOR
  - If you “flip” a bit of the ciphertext, you can predict which bits in the ICV part need to be flipped as well
Attacks against WEP – II

- IV Reuse
  - Collisions in IV’s are likely to occur sooner than $2^{24}$ packets
  - If Oscar knows the key stream corresponding to a particular IV, he can also decode all packets with the same IV

- Weak RC-4 keys
  - Some keys used in RC-4 are weak keys (for some keys swaps become obvious or have a predictable pattern)
  - Since the IV is transmitted as a plaintext, it is easy for Oscar to detect a packet that has been encrypted with a weak key
    - To overcome this problem, it is better to drop the first several bits of the key stream (256 bytes is suggested) -- some randomness is introduced.
  - Fluhrer, Mantin and Shamir showed that Oscar can get the first 8 bits of a key with just 60 messages and subsequent bytes in the same way
    - Attack is linear, not exponential so that longer keys do not help much
Recent Trends in 802.11 Security

- Several WLAN hotspots
  - Coffee shops, airports, hotels …
- Wi-Fi Protected Access (WPA)
  - Security is based on 802.1x and EAP (Extensible Authentication Protocol)
    - Allows many protocol within a common framework
  - Example
    - Authenticate the access point using a variation of SSL
- Use VPNs (IPSec or SSL)
- IEEE is coming up with a standard (802.11i)
  - Use AES instead of RC4 for better security
802.11i and WPA

- The IEEE 802.11 Working Group handles standardization of 802.11
  - They have several task groups that deal with different aspects of the standard
  - The Task Group I deals with security issues
- Idea in 802.11i
  - Authentication followed by a limited-life security context
    - Define a new wireless network called robust security network (RSN)
    - Allow WEP as well as enhanced security in a transitional security network (TSN)
- Wi-Fi Protected Access (WPA)
  - Subset of RSN that has been adopted for legacy systems NOW
More on the standards

- Keys in RSN/WPA
  - Keys have limited lifetimes and created in real-time (temporal keys)
  - Most of the keys are NOT known prior to authentication
  - Each device in the network has a master key that enables it to create the temporal keys and identify the device

- Security layers
  - Wireless LAN layer
    - Deals with raw communications, advertising, associations, etc.
  - Access control layer
    - Manages the security context (decides who is legitimate and who is not based on their status)
  - Authentication layer
    - Accepts or rejects proof of identity
    - Delegates power to the access control layer once a MS is authenticated
Implementation of layers

- 802.11 deals only with the MAC layer
  - Hence WEP was completely integrated into the MAC

- In RSN/WPA, other security standards are used
  - Use 802.1x for the access control layer
  - Use EAP for authentication
    - No mandatory authentication mechanism
    - Make use of SSL and other standards.
Entities in RSN/WPA

- **Supplicant**
  - Entity that wants access to the WLAN

- **Authenticator**
  - Entity that controls the point of access

- **Authentication Server**
  - Entity that decides whether or not to allow access to the supplicant

- **Process**
  - Supplicant request access from the authenticator
  - Supplicant identifies itself
  - Authenticator requests the authentication server to authorize access for the supplicant
  - Authentication server says YES or NO
  - Authenticator allows or blocks access

- **Protocols**
  - Mandatory – IEEE 802.1x and EAP
IEEE 802.1X

- **Idea**
  - Implement access control at the point of access to the network (AP, port in a hub in a LAN, etc.)
  - Uses the supplicant, authenticator, authentication server paradigm

- **Procedure**
  - Treats each wireless connection (association) as independent
  - The authentication server may be a simple list in the AP or in a separate database + server elsewhere
  - It is a one-time operation that is not completely suitable for 802.11
    - Session hijacking is a problem
    - IP address is assigned (one time) -- if this address can be spoofed, then, illegitimate users can gain access.

- It is important to bind the access control operation by including message authentication
  - Some changes to 802.1x have been made
  - A new 802.1AA standard is being considered
EAP

- A generalization of the C-R protocols
  - It does not specify what protocol should be used for identification
    - Examples: TLS (transport layer security) can be used with EAP
    - Cisco uses Light EAP or LEAP based on CHAP with mutual authentication (CHAP -- Challenge handshake authentication protocol --password based).
    - If a new method for authentication is invented, it can also be used with EAP
  - It only provides the “format” and “procedures” for requesting authentication information, accepting a legitimate user or rejecting a failed authentication
    - Request, Response, Success, Failure message are specified