

# CS 6v81 - Network Security

## Wireless LAN (802.11) Security

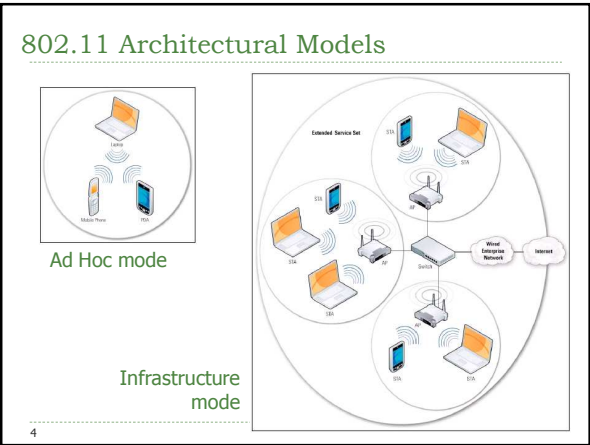
### IEEE 802.11 WLAN Technologies

IEEE Standard or Amendment	Maximum Data Rate	Frequency Band	Comments
802.11	2 Mbps	2.4 GHz (ISM)	Legacy technology that is minimally used
802.11a	54 Mbps	5 GHz (UNII)	Not compatible with IEEE 802.11b or IEEE 802.11g Provides better than 10Base-T Ethernet speeds
802.11b	11 Mbps	2.4 GHz (ISM)	Equipment based on IEEE 802.11b has been the dominant WLAN technology Provides close to 10Base-T Ethernet speeds Is generally combined with IEEE 802.11g as product offerings as IEEE 802.11b/g
802.11g	54 Mbps	2.4 GHz (ISM)	Backward compatible with IEEE 802.11b Provides better than 10Base-T Ethernet speeds Supported by most current WLAN products
802.11n	300 Mbps	2.4 GHz (ISM) and 5 GHz (UNII)	Backward compatible with IEEE 802.11a/b/g Provides better than 10Base-T Ethernet speeds

▶ All support WEP - Wired Equivalent Privacy

2

- ### Security in IEEE 802.11 WLAN Technologies
- ▶ WEP
    - ▶ Well-documented security problems
  - ▶ Wi-Fi Protected Access (WPA)
    - ▶ A short term enhancement/replacement on WEP
  - ▶ 802.11i – (WPA2)
    - ▶ Specifies a security framework that is compatible for existing 802.11 technologies
    - ▶ Includes many security enhancements that leverage mature and proven security technologies
      - ▶ Extensible Authentication Protocol (EAP), HMAC
    - ▶ Introduces concept of Robust Security Network (RSN)
      - ▶ RSNA – a logical connection b/w 802.11 entities established through 802.11i key management scheme
- 3



- ### WLAN Security
- ▶ Security objectives
    - ▶ Confidentiality
    - ▶ Integrity
    - ▶ Availability – can access a WLAN and its resources whenever needed
  - ▶ Threat classes
    - ▶ Those involving radio link between wireless devices
      - ▶ Intercept/inject messages
    - ▶ Deployment of rogue wireless devices, i.e., APs
      - ▶ Provides a backdoor to the network bypassing security measures, i.e., firewalls
    - ▶ DoS attacks – flooding/jamming
- 5

- ### WLAN Security
- ▶ Classification of attacks
    - ▶ Passive
      - ▶ Eavesdropping
      - ▶ Traffic analysis
    - ▶ Active
      - ▶ Masquerading – impersonating to gain unauthorized access to resources
      - ▶ Replay
      - ▶ Message modifications
      - ▶ DoS
- 6

## WLAN Security

### Major threats against WLAN security

Threat Category	Description
Denial of Service	Attacker prevents or limits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Man-in-the-Middle	Attacker actively impersonates multiple legitimate parties, such as appearing as a client to an AP and appearing as an AP to a client. Allows attacker to intercept communications between an AP and a client, thereby obtaining authentication credentials and data.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Misappropriation	Attacker steals or makes unauthorized use of a service.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants.

7

## Security of 802.11 WLAN Standards

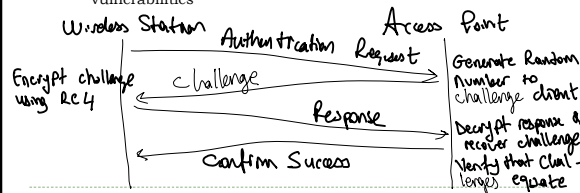
- WEP and WPA are two main security solutions for (legacy) 802.11 WLANs
- WEP designed for
  - Authentication, confidentiality, and integrity protection
  - No support for audit, authorization, replay protection, non-repudiation, and key management
    - Key management – how to generate, distribute, store, load, escrow, archive, audit, and destroy WEP keys
      - Source of many problems in WLANs

8

## Security of 802.11 WLAN Standards

### Authentication

- One way only – authenticating client to the AP
- Two methods
  - Open-system – only mandatory method but not a real authentication
  - Shared-key – cryptographic authentication
    - A simple challenge-response mechanism with significant vulnerabilities



9

## Security of 802.11 WLAN Standards

### Shared-key authentication

- Response computation
  - XOR AP's plaintext with key stream (from shared secret)
- Initial challenge and response is open to eavesdropping
  - Having challenge and response, can XOR to learn key stream and hence can authenticate to AP
- Bottom line
  - WEP provides no strong authentication scheme

10

## Security of 802.11 WLAN Standards

### Confidentiality

- WEP employs RC4 stream cipher alg with 40-bit WEP key *only*
- WEP uses 24-bit value as IV
- Though vendors implement optional use of longer keys, WEP implementation makes it inherently vulnerable to attacks despite the use of longer keys
- IV related WEP encryption problems
  - 24-bit IV sent in clear to AP
  - Knowing IV and eavesdropping a small amount of traffic enables one to recover the key
  - WEP does not specify how IV changes – some vendors make use of static known IVs
  - Even if IV changes for consecutive packets, it takes a few hours to exhaust IV space (17M IV values)

11

## Security of 802.11 WLAN Standards

### Confidentiality, cont'd

- Network analysis based attacks
  - Can learn which parties are communicating and when
  - Can learn nature of the communication: interactive, one way
  - Can learn OS related info based on length of certain frames
  - No attempt to make traffic analysis difficult

12

## Security of 802.11 WLAN Standards

- ▶ Integrity
  - ▶ WEP – simple encrypted checksum
    - ▶ 32-bit CRC encrypted along with payload using RC4
    - ▶ Vulnerable to certain attacks as CRC is not cryptographically secure
      - Bit flipping attacks

13

## Security of 802.11 WLAN Standards

- ▶ WPA – can be enabled via firmware upgrade
  - ▶ 802.1X – port based access control – allows the use of robust upper-layer authentication protocols
  - ▶ Temporal Key Integrity Protocol (TKIP) – four features to enhance 802.11
    - ▶ Extends IV space
    - ▶ Allows per-packet key construction
    - ▶ Provides cryptographic integrity
    - ▶ Provides key derivation and distribution
  - ▶ Provides protection against some of above attacks, replay and integrity attacks
  - ▶ Addresses critical need to periodically change encryption key
- ▶ However, has significant flaws and does not provide level of security that IEEE 802.11i does

14

## Threats and vulnerabilities

- ▶ Loss of confidentiality
  - ▶ Due to radio nature, no/minimal security at PHY layer – anyone can hear anyone else
  - ▶ Eavesdropping – sensitive/proprietary info, network IDs and passwords, configuration data, etc.
    - ▶ Once recovering two ciphertexts sharing same IV, both data integrity and confidentiality can be compromised
    - ▶ Once WEP key is recovered, can read any data over the WLAN
  - ▶ Having an AP connected to a Ethernet hub also makes data on wired network vulnerable to eavesdropping
    - ▶ Use of Ethernet switches alleviates these problems
  - ▶ Malicious/irresponsible user may insert a rogue AP into the network with no/minimal security configuration

15

## Threats and vulnerabilities

- ▶ Loss of integrity
  - ▶ Can be compromised by deleting/modifying data in an e-mail sent over a WLAN
  - ▶ Legacy 802.11 standards provide no strong integrity
- ▶ Loss of availability
  - ▶ Jamming or flooding
    - ▶ Can use bogus management frames to disassociate a client from an AP
    - ▶ Can flood bogus association frames to fill up association table at AP
    - ▶ Downloading large files to monopolize bandwidth resources on WLAN

16

## WLAN security countermeasures

- ▶ Due to inherent vulnerabilities of legacy WLAN standards, difficult to achieve
- ▶ Involves
  - ▶ management,
  - ▶ operational and
  - ▶ technical countermeasures

17

## WLAN security countermeasures

- ▶ Management countermeasures
  - ▶ Having a wireless network security policy in place
    - ▶ Which users/groups are authorized to use WLANs
    - ▶ Who is responsible for installing/configuring APs
  - ▶ WLAN infrastructure security
    - ▶ Physical security of WLAN devices
    - ▶ Type of info that can be sent or not over WLANs
    - ▶ WLAN transmission protection policy – req's for use of encryption and crypto key management
  - ▶ WLAN client device security
    - ▶ When and where clients are allowed to use WLANs
    - ▶ Standard hw/sw configs
    - ▶ Guidelines for reporting loss of WLAN client devices
  - ▶ WLAN security assessment
    - ▶ Frequency and scope of WLAN assessment
    - ▶ Actions to be taken to address rogue/misconfigured devices

18

## WLAN security countermeasures

- ▶ Operational countermeasures
  - ▶ Physical security of WLAN devices
    - ▶ Personnel identification
    - ▶ External boundary protection
  - ▶ RF range for each AP in a legacy 802.11 WLAN
    - ▶ Range has to be limited to protected physical boundary of the organization's facilities
    - ▶ Use of site survey tools to measure range of AP devices
    - ▶ Helps protection against easy eavesdropping

19

## WLAN security countermeasures

- ▶ Technical countermeasures
  - ▶ Use of hw/sw solutions to help secure WLAN
- ▶ Confidentiality and Integrity Protection
  - ▶ WPA – temporary soln. an improvement over WEP
    - ▶ Via the use of TKIP and MIC
  - ▶ Use of VPNs – to protect sensitive communications
    - ▶ Between WLAN clients and a VPN end point beyond AP
  - ▶ Hybrid solution – use of WLAN security soln and VPNs
- ▶ Wireless IDS and IPS
  - ▶ Can help determine unauthorized access to the WLAN
  - ▶ Can help detect misconfigured WLAN clients, rogue APs, ad hoc nws, and other possible violations of WLAN policy

20

## WLAN security countermeasures

- ▶ AP Configuration
  - ▶ Should be done acc. to established security policy
  - ▶ Thick AP – handles encryption and overall management of client devices connected to it
  - ▶ Thin AP – processing of encryption and policy setting occurs in a centralized switch/controller
  - ▶ A thin AP is generally more secure than a thick one
  - ▶ Issues with AP management and WLAN configurations

21

## WLAN security countermeasures

- ▶ AP management
  - ▶ Configuring administrator access – do not use default password and default settings that come with the box
  - ▶ Controlling reset function – some devices have hw reset button which does not require any privileges to use
  - ▶ Use of SNMPv3 – instead of SNMPv1 or v2
  - ▶ Use of HTTP – has to be protected using SSL (HTTPS)
  - ▶ Enabling logging – helps ensure user accountability and records malicious activity

22

## WLAN security countermeasures

- ▶ WLAN configuration
  - ▶ Changing default channel and power output – to limit RF to protected boundary and minimize interference
  - ▶ Changing SSID – change from factory default to help prevent users from accidentally connecting to the wrong WLAN
  - ▶ Avoiding pre-shared keys (PSK) –
    - PSK = network name + SSID + passphrase
    - keys derived from passphrase shorter than 20 chars are weak
  - ▶ Using MAC ACL functionality
  - ▶ Use of DHCP – DHCP can assign an IP address to all including intruders – use static IP addresses instead
  - ▶ Maximize beacon interval – make it difficult to learn config. parameters for an intruder

23

## WLAN security countermeasures

- ▶ Client device security
  - ▶ Automatic connection – disable to avoid connecting to a malicious WLAN
  - ▶ Personal firewall – helps with unwanted connections from remote systems
  - ▶ Host-based IDS/IPS – monitors internal state of the client device and logs activities
  - ▶ Antivirus – helps assist spread of viruses, worms
  - ▶ Ad hoc mode – disable to avoid inadvertent or malicious connections to the client device
  - ▶ IEEE 802.11 radio mgmt – disable RF if not needed
  - ▶ Policy enforcement – client config should comply with security policy

24