Lecture 2
Secure Wireless LAN

Network security
(*19*265400 / 201000086)
Lecturers:

Aiko Pras
Pieter-Tjerk de Boer
Anna Sperotto
Ramin Sadre
Georgios Karagiannis

Acknowledgements

Part of the slides are based on the slides presentation:

"Wireless LAN Security", given by:

Matthew Joyce,

Rutherford Appleton Laboratory,

Council for the Central Laboratory of the Research Councils (CCLRC), UK

Lecture material

- To be found via Blackboard: Course information => Study material that can be downloaded:
  - wlan_pers_comm_05.pdf

    JYH-CHENG CHEN, MING-CHIA JIANG, AND YI-WEN LIU

    “WIRELESS LAN SECURITY AND IEEE 802.11i”,

    IEEE Wireless Communications, February 2005

    Also via: http://calypso.unicauca.edu.co/gntt/grupo/maestria/II-parte/CHEN.pdf
  - mobicom_borisov.pdf

    Nikita Borisov, Ian Goldberg, David Wagner

    “Intercepting Mobile Communications:

    The Insecurity of 802.11”

    Mobile Computing And Networking, July 16–21, 2001.

    Also via: http://cs.berkeley.edu/~daw/papers/wep-mob01.pdf
- Slides will be uploaded on Blackboard: Courses => Course materials

  (also on: http://wwwhome.cs.utwente.nl/~pras/netsec/)

Outline

- Goal of this lecture
- What's Wireless LAN
- Security History (WEP)
- Main WEP Vulnerabilities
- 802.11 safeguards
- WLAN security enhancements (WPA, WPA2, 802.11i)
- Summary & information homework assignments
- Appendix 1 (WLAN 802.11 for safeguards details): Not presented but will be considered for examination
- Appendix 2 (More WEP Vulnerabilities): Not presented but will be considered for examination

Goal of this lecture

- understanding current and future Wireless LAN security vulnerabilities and solutions

Outline

- Goal of this lecture
- What's Wireless LAN

  (more details on W-LAN in Mobile & Wireless Networking: 19262001)
- Security History
- Main WEP Vulnerabilities
- 802.11 safeguards
- WLAN security enhancements
- Summary & information homework assignments

What's Wireless LAN

- IEEE ratified 802.11 in 1997.
  - Also known as Wi-Fi
  - Last ratified version in 2007
- Wireless LAN at 1 Mbps & 2 Mbps
- WECA (Wireless Ethernet Compatibility Alliance) promoted Interoperability
  - Now Wi-Fi Alliance
- 802.11 focuses on Layer 1 & Layer 2 of OSI model.
  - Physical layer
  - Data link layer

What's Wireless LAN (Components)

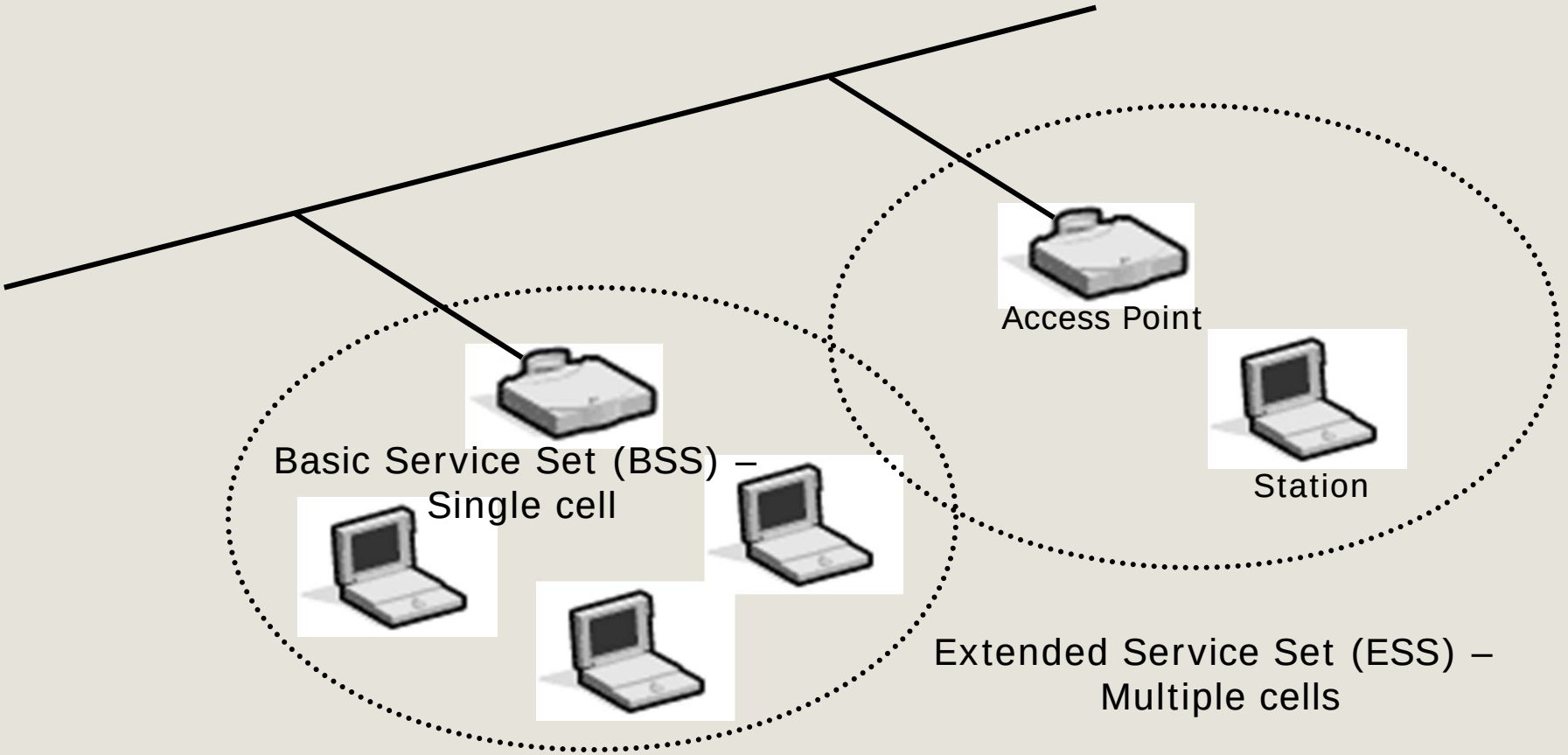
- Two pieces of equipment defined:
  - Wireless station
    - A desktop or laptop PC, PDA, or other wireless device with a wireless 802.11 NIC (Network Interface Card).
  - Access point
    - A bridge between wireless and wired networks
    - Composed of
      - Radio
      - Wired network interface (usually 802.3)
      - Bridging software
    - Aggregates access for multiple wireless stations to wired network.

What's Wireless LAN (Modes)

- Infrastructure mode
  - Basic Service Set
    - One access point
  - Extended Service Set
    - Two or more BSSs forming a single subnet.
  - Most corporate LANs in this mode.
- Ad-hoc mode
  - Independent Basic Service Set
  - Set of 802.11 wireless stations that communicate directly without an access point.
    - Useful for quick & easy wireless networks.

What's Wireless LAN (Modes)

Infrastructure mode

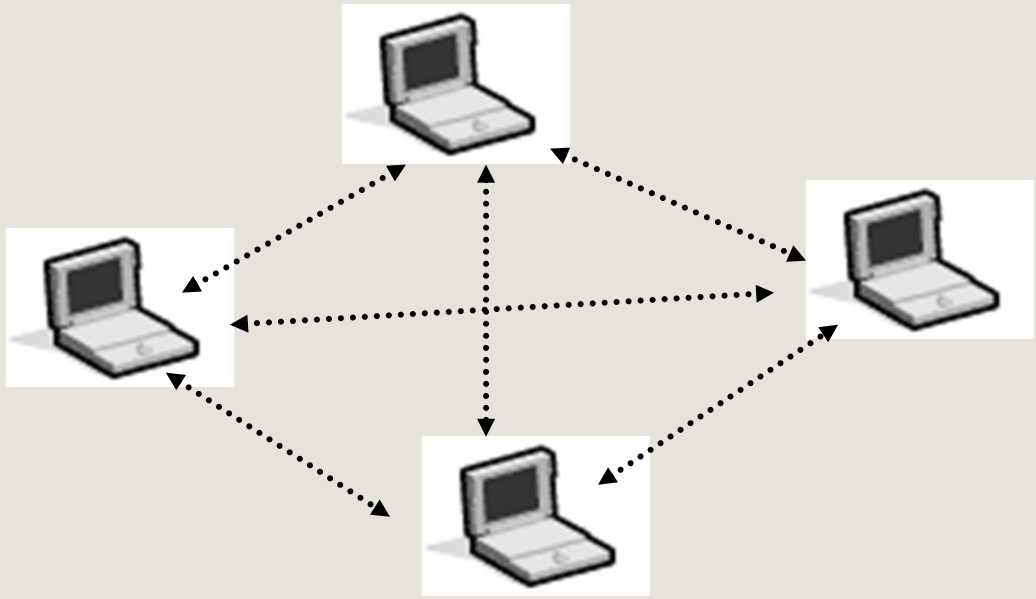


SSID (Service Set Identifier) attached to all packets belonging to a BSS

multiple APs with same SSID form Extended Service Set.

What’s Wireless LAN (Modes)

Ad-hoc mode



Independent Basic Service Set (IBSS)

What's Wireless LAN (IEEE protocol standards)

- IEEE 802.11
  - original standard in 2.4 GHz: 1 Mbit/s, optional 2 Mbit/s
- IEEE 802.11b
  - PHY Standard in 2.4 GHz: 3 channels :
    11 Mbps : Products are available.
- IEEE 802.11g
  - PHY Standard in 2.4 GHz
    3 channels
    54 Mbit/s
- IEEE 802.11i
  - Supplementary MAC
    Enhanced security
    (ratified June 2004)
- IEEE 802.11a
  - PHY Standard in 5 GHz: 8 channels : 54 Mbps : Products are available
- IEEE 802.11e
  - MAC Standard : QoS support
- IEEE 802.11f
  - Inter-Access Point Protocol
- IEEE 802.11u
  - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11n
  - Higher throughput improvements: 100+ Mbit/s
- IEEE 802.11p
  - Vehicular networks
- And more …..

Outline

- Goal of this lecture
- What's Wireless LAN
- Security History (WEP)
- Main WEP Vulnerabilities
- 802.11 safeguards
- WLAN security enhancements
- Summary & information homework assignments

WLAN security history (Attack practicality)

- Wireless LAN uses radio signal
- Attacker needs equipment capable of:
  - monitoring (passive attacks) and transmitting (active attacks) encrypted traffic
    - passive attacks can be carried out using off-the-shelf equipment by modifying driver settings
    - active attacks are more difficult but not beyond reach and easy when firmware (e.g., Orinocco) of PCMCIA cards can be upgraded
- Prudent to assume that motivated attackers have full access to link layer for passive and active attacks

WLAN security history (Attack practicality)

Attacker is using WarDriving: http://www.wardrive.net/

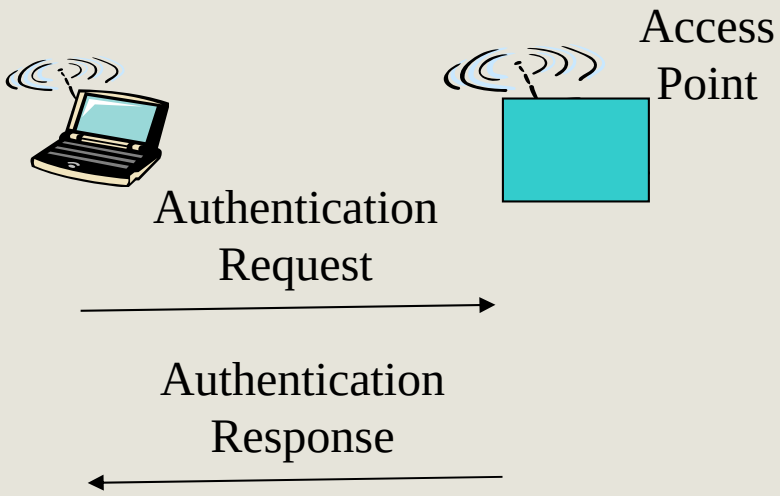
- driving around city searching for existence of Wireless LAN (802.11) Networks:
  - Wardriving software: http://www.wardrive.net/wardriving/tools
  - GPS (Global Positioning System) unit
- Logging of MAC address, network name, SSID, manufacturer, channel, signal strength, noise, (GPS – location)
- How to protect your Wireless Network from Wardrivers?
  - Solutions: http://www.wardrive.net (see also Appendix of this presentation):
  - important: authenticate wireless users with protocols like EAP & RADIUS or DIAMETER

WLAN security history (802.11b security services)

- Authentication
  - Open System Authentication
  - Shared Key Authentication
- Confidentiality, Access Control, Data integrity
  - Wired Equivalent Privacy (WEP)

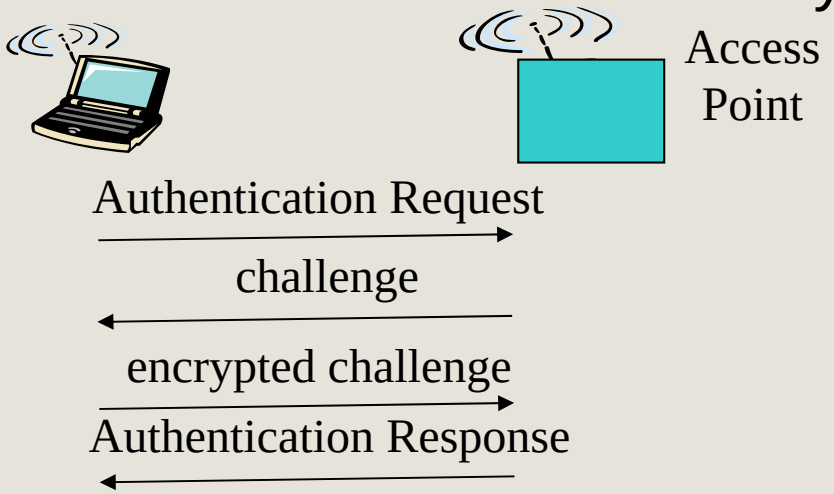
WLAN security history (Open system authentication)

- Authentication Request = Station ID
- Authentication Response = success or failure
- On success: both stations mutually authenticated



WLAN security history (Shared Key Authentication)

- When station requests association with Access Point
  - AP sends random number to station (challenge)
  - Station encrypts random number
    - Uses RC4
    - Encrypted random number (encrypted challenge) sent to AP
  - AP decrypts received message
    - Uses RC4
  - AP compares decrypted random number to transmitted random number
- If numbers match, station has shared secret key.



WLAN security history (Access control)

Access control:

- Can be achieved using WEP encryption:
  - optional feature used to discard packets not properly encrypted using WEP

WLAN security history (Wired Equivalent Privacy)

- Shared key, usually, between all:
  - Stations.
  - An Access Point.
- Extended Service Set
  - All Access Points will have, usually, same shared key.
- Usually, no key management
  - Shared key entered usually manually into:
    - Stations
    - Access points
    - Key management nightmare in large wireless LANs

WLAN security history (Ron’s Code number 4)

- Question: Can you list some main characteristics of the encryption mechanism RC4?

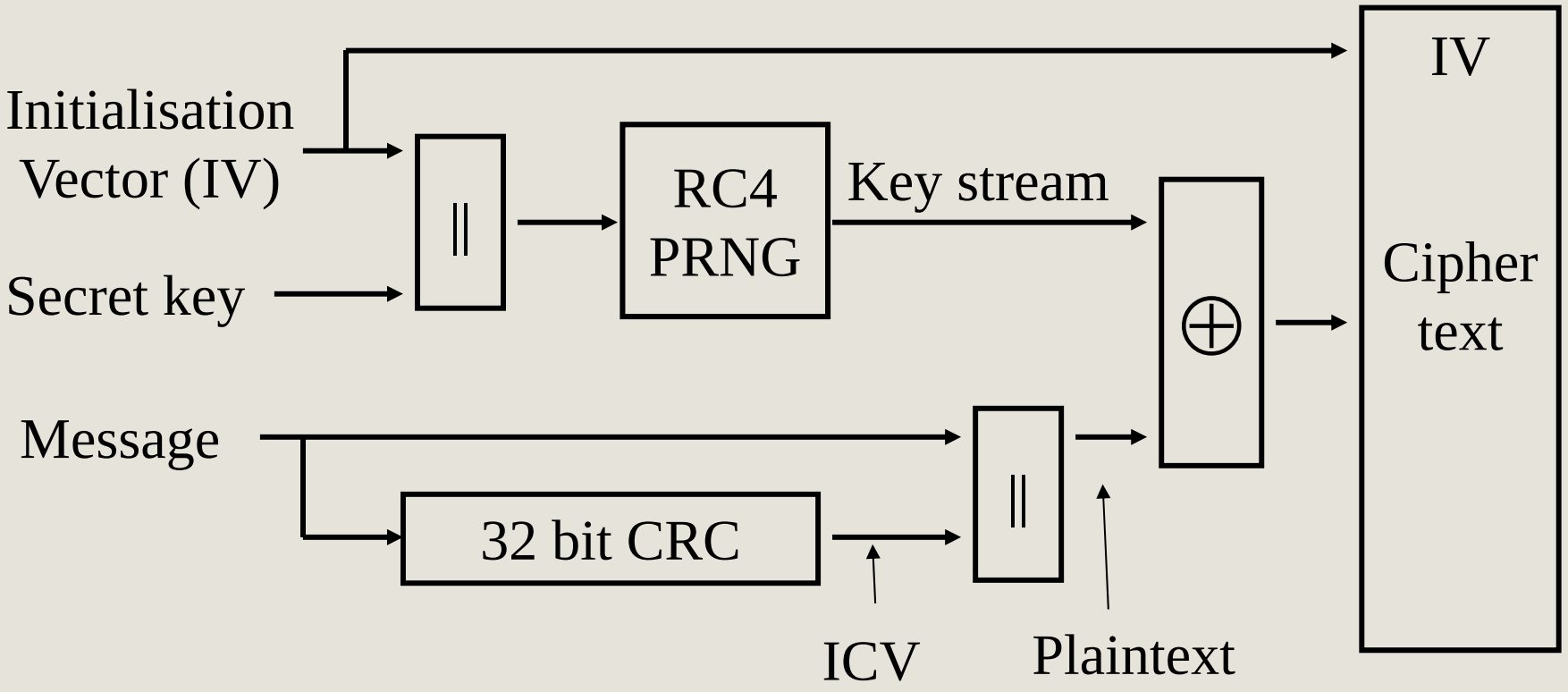
WLAN security history (Ron's Code number 4)

- Ron's Code number 4 (RC4)
  - Symmetric key encryption
  - RSA Security Inc.
  - Designed in 1987 by Ronald Rivest
  - Trade secret until leak in 1994.
- RC4 can use key sizes from 1 byte to 256 bytes
- Supports:
  - RC4-KSA (Key Scheduling Algorithm): translates key of length 1 byte to 256 bytes to initial permutations of numbers 0 to 255
  - RC4-PRNG: generates stream of pseudo random using initial permutation numbers
    - XORed with plaintext to create ciphertext.

WLAN security history (WEP - Sending)

- Compute Integrity Check Vector (ICV)
  - 32 bit Cyclic Redundancy Check.
  - Appended to message to create plaintext.
  - Provides integrity
- Plaintext encrypted via RC4
  - Provides confidentiality.
  - Plaintext XORed with long key stream of pseudo random bits.
  - Key stream is function of
    - 40-bit secret key (vendors extended this to 104-bits)
    - 24 bit Initialisation Vector (IV)
- Ciphertext is transmitted.

WLAN security history (WEP - Encryption)



PRNG = Pseudo Random Number Generation
(note: RC4-KSA also part of RC4 PRNG block)

WLAN security history (WEP - Receiving)

- Ciphertext is received.
- Ciphertext decrypted via RC4
  - Ciphertext XORed with long key stream of pseudo random bits.
  - Key stream is function of
    - 40-bit secret key (or 104-bit secret key)
    - 24 bit initialisation vector (IV)
- Check ICV
  - Use plaintext and separate ICV from message.
  - Compute ICV for message
  - Compare with received ICV

WLAN security history (WEP Safeguards)

- Shared secret key required for:
  - Associating with an access point.
  - Sending data.
  - Receiving data.
  - Distribution of keys not defined:
    - external mechanism is required to populate a globally shared array of 4 keys
    - each message contains key identifier field specifying index in the key array
    - usually a single key for entire network
- Messages are encrypted: Confidentiality
- Messages have checksum (ICV): Integrity
- But typically:
  - management traffic still broadcasted in clear containing SSID

WLAN security history (Initialisation Vector)

- IV must be different for every message transmitted (but not mandatory in specification).
- 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.

Outline

- Goal of this lecture
- What's Wireless LAN
- Security History
- Main WEP Vulnerabilities (see Appendix 2 for more WEP vulnerabilities)
- 802.11 safeguards
- WLAN security enhancements
- Summary & information homework assignments

WEP vulnerabilies (Passive WEP attack)

- Question: How is it better to calculate IV?

WEP vulnerabilies (Passive WEP attack)

- If 24 bit IV is an ascending counter,
  - If Access Point transmits at 11 Mbps and packet length approx. 1500 bytes
  - All IVs are exhausted in roughly 5 hours.
- If 24 bit IV uses a random generator:
  - due to birthday paradox, and assuming that probability of sequnce number match is 50% then a number of collisions occur after transmitting approx. 5000 packets, recovered within a transmission of few minutes
  - Birthday paradox equation, see also Appendix B in:

http://betterexplained.com/articles/understanding-the-birthday-paradox/

$$n \approx \sqrt{-2 * \ln(1-m)} * \sqrt{T}$$

Where:

n = number of packets before a collision occurs

m = probability of match (that two packets use the same sequence number)

T = Maximum number of packets with different sequence number

WEP vulnerabilies (Passive WEP attack)

- Passive attack:
  - Attacker collects all traffic
  - Attacker could collect two messages:
    - Encrypted with same key and same IV
    - Xoring two ciphertexts causes keystream to cancel out and result is the XOR of two plaintexts
    - each of the XORed plaintexts can be calculated when there is partial knowledge of some part of the plaintexts:
      - statistical attacks to reveal plaintext

WEP vulnerabilities (IV weakness)

- Paper from Fluhrer, Mantin, Shamir (FMS), 2001:
  http://wiki-files.aircrack-ng.org/doc/rc4_ksaproc.pdf
- Passive attack on WEP able to retrieve entire secret key in relatively small amount of time (4.000.000 packets)
- get information about all key bytes when PRNG input is known:
  - Capture packets with weak IV
    (specific IV values that easy calculation of a key byte when previous key bytes are known)
  - First output byte ciphertext per IV is known:
    Every wireless frame has reliable and known first byte
    - Sub-network Access Protocol header (SNAP) used in logical link control layer, upper sub-layer of data link layer.
    - First byte is 0xAA

WEP vulnerabilies (Active WEP attack)

- If attacker knows plaintext and ciphertext pair
  - Keystream for IV values are known.
    - Plaintext XOR Ciphertext = Keystream
    - Build decryption dictionaries as tables of
      - Keystream value ⇔ IV value
  - Attacker can create correctly encrypted messages.
      - keystream XOR plaintext = cyphertext
      - cyphertext sent together with known IV
  - Access Point is deceived into accepting messages.
- Message authentication using CRC checksum not secure enough, e.g. Bitflipping, for integrity check:
  - Flip a bit in ciphertext
  - Bit difference in CRC-32 can be computed due to linear property:
    - checksum(M XOR Diff) = checksum(M) XOR checksum(Diff)

WEP vulnerabilies (Active WEP attack)

Message Modification Attack

- Change destination address in encrypted packet into attackers wired node
- Unencrypted packet delivered by AP to the attackers wired node

WEP vulnerabilities (Chopchop attack)

Succesful on 64 bit and *128 bit* WEP

- Allows attacker to interactively decrypt last m bytes of plaintext of encrypted packet:
  - Step 1: Sniff an encrypted packet
  - Step 2: Chop one byte from the end (that we want to reveal)
  - Step 3: During first iteration suppose chopped secret byte was 0
    - Correct checksum (using e.g., bitflipping)
  - Step 4: repaired packet sent to Access Point
  - Step 5: If AP broadcasts packet, then secret last byte found (go to step 7)
  - Step 6: If not, try to repair the checksum using values 1 then 2, 3 ... and repeat step 3 until AP broadcasts packet
  - Step 7: Go to step 2, chop the next secret byte from the end

For more details see: http://dl.aircrack-ng.org/breakingwepandwpa.pdf

Outline

- Goal of this lecture
- What's Wireless LAN
- Security History
- Main WEP Vulnerabilities
- 802.11 safeguards
- WLAN security enhancements
- Summary & information homework assignments

WLAN 802.11 safeguards (see also Appendix 1 for details)

- Security Policy & Architecture Design
  - Define use of wireless network
  - Holistic architecture and implementation
- Treat as untrusted LAN (extra autentication required)
- Discover unauthorised use (check latest wardriving tools)
- Access point audits

  (check security configuration, use highest level security WPA, 802.11i)
- Station protection (vpn station to intranet, use TLS/HTTPS)
- Access point location (centre of buildings)
- Antenna design (directional antenna)

Outline

- Goal of this lecture
- What's Wireless LAN
- Security History
- Vulnerabilities
- 802.11 safeguards
- WLAN security enhancements
- Summary & information homework assignments

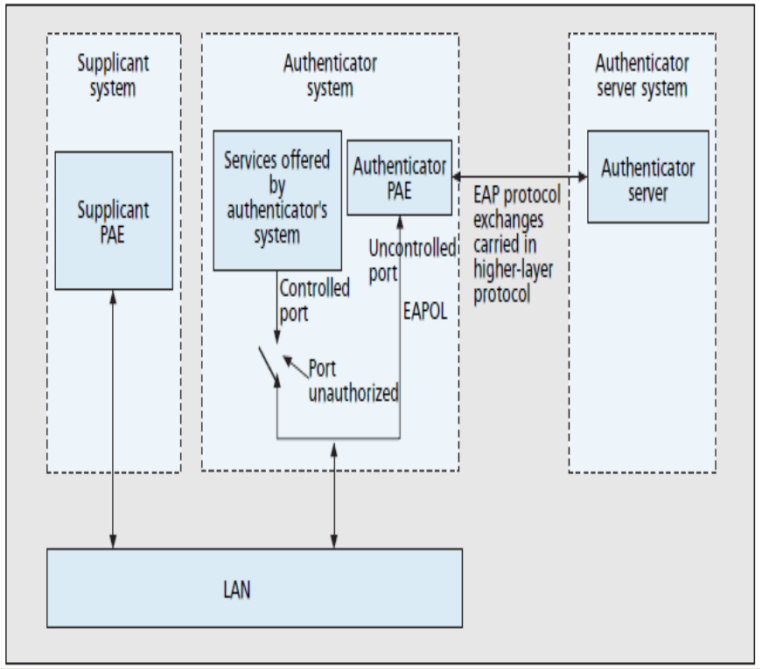
WLAN security enhancements (IEEE802.1x)

- defines security framework in upper OSI layers to provide compatible authentication & authorization for IEEE 802 LAN
- distributes keys for 802.11 and enabling authentication and encryption between APs and wireless stations

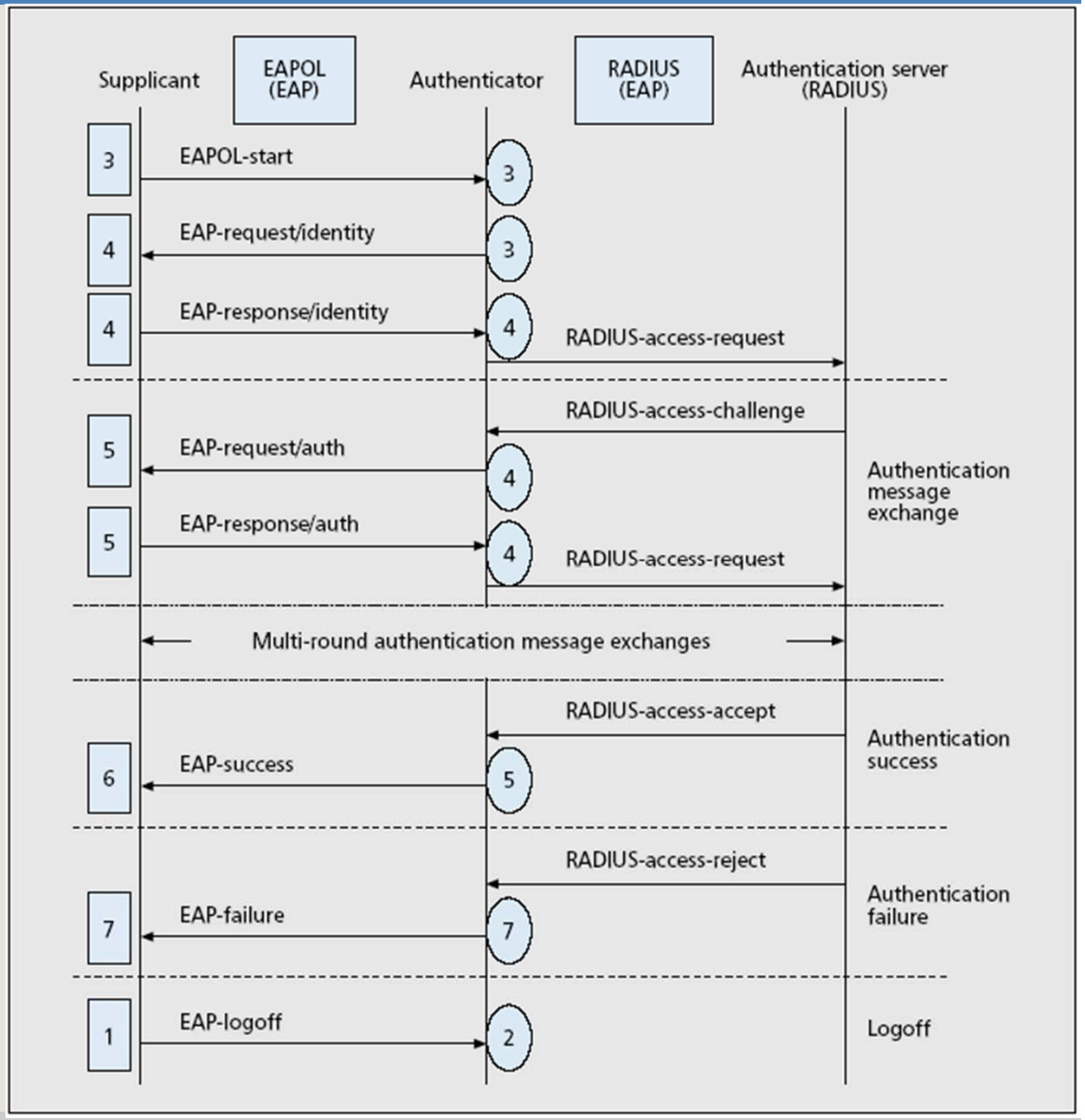
Main components:

- Supplicant (*wireless station*)
- Authenticator (*access point*)
- Authentication server (RADIUS or DIAMETER)
- EAP (RFC2284):
  - MD5, TLS, Tunelled TLS (TTLS), Protected EAP (PEAP), EAP SIMs
  - only supplicant & authentication server need understand authentication mechanisms
- EAP over LANs (EAPOL): encapsulates EAP messages between Supplicant & Authenticator

WLAN security enhancements (IEEE802.1x)



- IEEE 802.1x : port-based network access control



WLAN security enhancements (IEEE802.1x)

Supplicant Roaming

- supplicant should re-authenticate with Authenticator or Authentication Server when roaming to another 802.1X-enabled network
- Intra-subnet roaming:
  - moves from one Authenticator to another within the same IP subnet
- Intersubnet roaming:
  - Moves from one Authenticator to another Authenticator located in another IP subnet (Supplicant has to change its IP address)
  - Use IETF Mobile IP to support mobility management in the IP layer
- More info on IEEE 802.1X:
  - http://www.ieee802.org/1/files/public/docs2000/8021xSecurity.PDF

WLAN security enhancements (WPA)

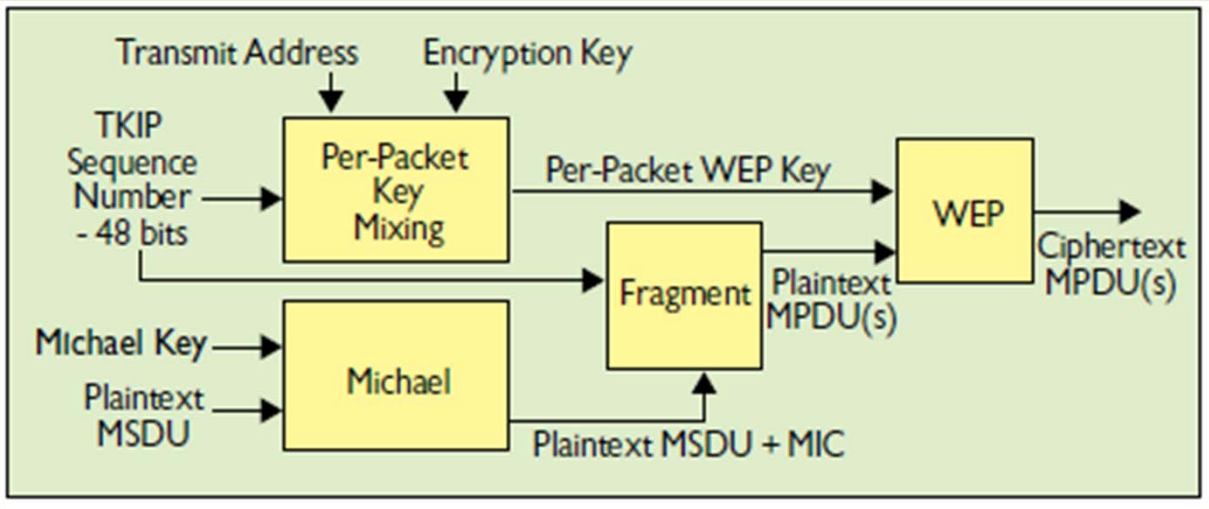
Wi-Fi Protected Access (WPA)

- Pre-shared mode: home environment, use Pre-shared keys (PSK)
- Enterprise mode: use
  - 802.1X authentication & key management
  - EAP & (RADIUS or DIAMETER)

Encryption:

- TKIP (Temporal Key Integrity Protocol) or WEP2
  - 128-bit secret key
  - RC4 session-based dynamic encryption keys, with 32 CRC as ICV
  - 48b TKIP sequence counter (TSC) is used to generate IV and
    - avoid replay attack (verify sequence order of MPDU); reset to 0 on new key and incremented.
    - IV reuse is prevented by changing WEP key on IV recycling
  - Michael 8 byte key: a non-linear message integrity code (MIC) in addition to 32 CRC
  - Longer IV + Per-Packet Key mixing => Per-Packet WEP Key + MIC

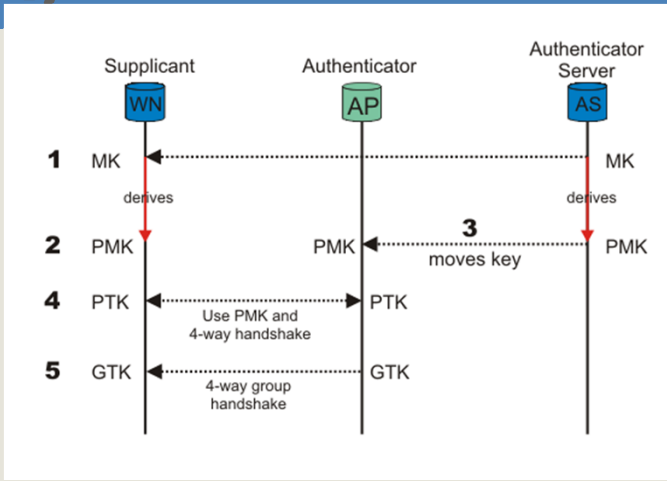
WLAN security enhancements (WPA)



- Taken from: http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf

WLAN security enhancements (WPA)

- Key management and establishment
  - Manual
  - Automatic: 802.1X used for support key management:
    - After 802.1X Supplicant & Authentication server using Master Key (MK) obtain independently the Pairwise Master Key (PMK)
    - Authentication Server sends PMK to Authenticator
    - Supplicant & Authenticator use PMK & more.., to generate each:
      - Pairwise Transient Key (PTK) using four way handshake, consists of:
        - » EAPOL-Key Confirmation Key (KCK)
        - » EAPOL-Key Encryption Key (KEK)
        - » Temporal Key (TK 1 & 2) used for encrypting wireless traffic; TK is further computed using MAC address and IV to produce unique security key per wireless station and per packet
      - Group Transient Key (GTK) for encrypting broadcast message



WLAN security enhancements (practical WPA attacks)

- Dictionary attack on pre-shared key mode
  - CoWPAtty, Joshua Wright

    http://www.securiteam.com/tools/6L00F0ABPC.html
- Denial of service attack
  - If WPA equipment sees two packets with good ICV check and invalid MICs check in 1 minute:
    - All clients are disassociated
    - All activity stopped for one minute
    - Access Point rekeys TKIP session key

WLAN security enhancements (Beck&Tews WPA attack)

- Beck & Tews WPA attack:

  see: http://dl.aircrack-ng.org/breakingwepandwpa.pdf

  - detect encrypted ARP (Address Resolution Protocol) request or response
    - most parts of plaintext of packet are known, e.g., Ethernet source and destination addresses, etc.
    - Not known:
      - last byte of IP source and last byte of IP destination addresses
      - last 12 bytes of plaintext (MIC and ICV checksum)
- Use chopchop attack to reveal unknown bytes

WLAN security enhancements (Beck&Tews WPA attack)

- Avoid anti-replay TSC counter by using chopchop attack on another channel (with low TSC) than channel where packet was received
- guessed byte is sent to client:
  - wrong ICV check => packet is discarded by client
  - good ICV check, but wrong MIC check => a MIC failure report sent by client
- attacker needs to wait with continuation chopchop for at least 1 minute after receiving MIC failure report
- Question: Why does the attacker has to wait for at least 1 minute?
- last 12 bytes (MIC and ICV) decrypted in 12 minutes
- last byte of IP source and last byte of IP destination need to be decrypted
- after MIC and plaintext known, attacker can reverse MICHAEL algorithm to recover MIC key
- MIC key and RC4 keystream from AP for one TSC (IV) to client known:
  - send a custom packet on every channel where TSC counter channel lower than value used by captured packet

WLAN security enhancements (IEEE802.11i)

- Defines Robust Security Network (RSN) used to create a RSN Associations (RSNAs) that includes four way handshake mechanism for robust security key management
- Depends on 802.1X for authentication services and deliver key management services
- Two modes:
  - RSN is compatible with WPA2 ratified by Wi-Fi Alliance
    - Supports RSNA
    - Supports and extends WPA
    - RSN capable nodes include a RSN IE to carry RSN security information and capabilities in beacons, probe response, (re)association request and second and third message in four way handshake
  - Pre-RSN
    - IEEE 802.11 entity authentication
    - WEP

WLAN security enhancements (IEEE802.11i)

- RSN Authentication enhancement:
  - Similar to WPA that utilizes 802.1X for authentication and key management
- RSN Key management and establishment
  - Manual
  - Automatic: 802.1X used similar to WPA, but AES (Advanced Encryption Standard) keys are installed instead of TKIP keys

WLAN security enhancements (IEEE802.11i)

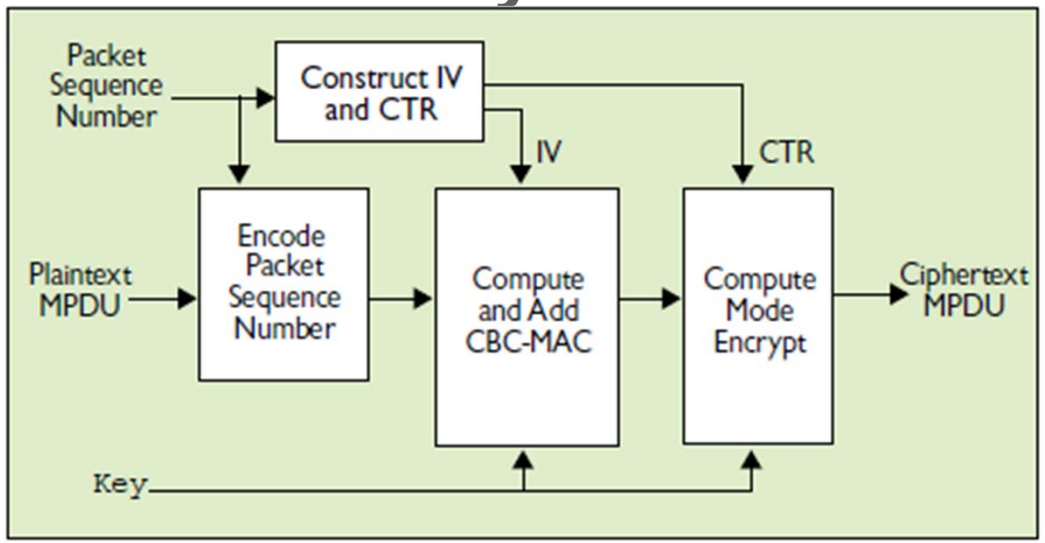


Figure taken from:
http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf

RSN Encryption and MIC enhancement

- **Mandatory and long term (requires new hardware):**
  - Based on a mode of AES, with 128 bits keys and 128 bit block size of operation, 48 bit IV and no per packet key derivation
  - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) [RFC3610]:
    - Counter mode (CTR) => data encryption
    - CBC-MAC => computes a MIC used also as ICV that protects header & payload from modification
  - Temporal Key (TK) for AES fresh every session & when packet number repeated

WLAN security enhancements (IEEE802.11i)

RSN Encryption and MIC enhancement

- **Optional and short term (called Transient Security Network)**
  - WPA's TKIP (requires only software upgrade)
    - Based on a mode of RC4, with 128 bits keys, 48 bit IV and 32 CRC ICV
    - Michael message integrity code (MIC) that protects payload and as well as source and destination address from modification

More details on WPA vs. WPA2:

- http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf
- http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf

WLAN security enhancements (WPA2 attack)

WPA 2 Hole196 Vulnerability:

- buried on last line of page 196 of 1232-page IEEE 802.11 Standard (version 2007)
- attack on GTK shared by all WPA2 authorized clients in WPA2 network
- standard considers that only AP transmits group-address data traffic using GTK and clients supposed to decrypt that traffic using GTK
- nothing in standard stops a malicious (authorized) client to inject spoofed GTK-encrypted packets:
  - insider (authorized user) can sniff and decrypt data from other authorized users as well as scan their Wi-Fi devices for vulnerabilities, install malware and possibly compromise those devices

For details see:

- http://www.airtightnetworks.com/fileadmin/pdf/WPA2-Hole196-Webinar-Presentation.pdf
- http://www.airtightnetworks.com/fileadmin/pdf/WPA2-Hole196-vulnerability-FAQs.pdf

Outline

- Goal of this lecture
- What's Wireless LAN
- Security History
- Vulnerabilities
- 802.11 safeguards
- WLAN security enhancements
- Summary & information homework assignments

Summary & information homework assignments

Understand

- WLAN security concepts
- currently deployed WLAN security vulnerabilities
- WLAN security enhancements

Summary & information homework assignments

Homework assignments Lecture 2:

- To be found via:

http://wwwhome.cs.utwente.nl/~pras/netsec/assignments/lecture_2.html

- answers to homework exercises need to be sent by email to following email address before Monday 17 September at 24:00!
- Please Include "Lecture number and the number of the exercise(s)" in the title/subject line of the email?

Email address: network.security@ewi.utwente.nl

Appendix 1: WLAN 802.11 safeguards

- Security Policy & Architecture Design
  - Define use of wireless network
  - Holistic architecture and implementation
- Treat as untrusted LAN
- Discover unauthorised use
- Access point audits
- Station protection
- Access point location
- Antenna design

Appendix 1: WLAN 802.11 safeguards

Security Policy & Architecture

- Define use of wireless network
  - What is allowed
  - What is not allowed
- Holistic architecture and implementation
  - Consider all threats.
  - Design entire architecture
    - To minimise risk.

Appendix 1: WLAN 802.11 safeguards

Wireless as untrusted LAN

- Treat wireless as untrusted.
  - Similar to Internet.
- Firewall between WLAN and Backbone.
- Extra authentication required:
  - Authenticate wireless users with protocols like EAP together with RADIUS or DIAMETER
- Intrusion Detection
  - at WLAN / Backbone junction.
- Vulnerability assessments

Appendix 1: WLAN 802.11 safeguards

Discover unauthorised use

- Search for unauthorised access points, ad-hoc networks or clients.
- Port scanning
  - For unknown SNMP agents.
  - For unknown web or telnet interfaces.
- Warwalking: test regularly security of wireless network using the latest Wardriving Tools
  - Sniff 802.11 packets
  - Identify IP addresses
  - Detect signal strength
  - But may sniff your neighbours…
- Wireless Intrusion Detection
  - AirMagnet, AirDefense, Trapeze, Aruba,…

Appendix 1: WLAN 802.11 safeguards

Access point audits

- Review security of access points.
- Are passwords and community strings secure?
  - change default Administrator password
- Use Firewalls & router ACLs
  - Limit use of access point administration interfaces.
- Standard access point config:
  - SSID
  - WEP keys
  - Community string & password policy
- Use highest level of WEP/WPA (WPA2/802.11i strongly preferred)

Appendix 1: WLAN 802.11 safeguards

Station protection

- Personal firewalls
  - Protect the station from attackers.
- VPN from station into Intranet
  - End-to-end encryption into the trusted network.
  - But consider roaming issues.
- Host intrusion detection
  - Provide early warning of intrusions onto a station.
- Configuration scanning
  - Check that stations are securely configured.
- For all user applications use strong encryption over the wireless network, e.g., use SSH and TLS/https

Appendix 1: WLAN 802.11 safeguards

Location of Access Points

- Ideally locate access points
  - In centre of buildings.
- Try to avoid access points
  - By windows
  - On external walls
  - Line of sight to outside

Appendix 1: WLAN 802.11 safeguards

Antenna design

- Use directional antenna to “point” radio signal.

Appendix 2: WEP vulnerabilities (Brute force key attack)

- Capture ciphertext.
  - IV is included in message.
- Search all 40 bit combinations for possible secret keys.
  - 1,099,511,627,776 keys
  - ~170 days on a modern laptop
- Find which key decrypts ciphertext to plaintext.

Appendix 2: WEP vulnerabilities (using 128 bit WEP)

128 bit WEP

- Vendors have extended WEP to 128 bit keys.
  - 104 bit secret key.
  - 24 bit IV.
- Brute force takes 10^19 years for 104-bit key.
- Effectively safeguards against brute force attacks.

Appendix 2: WEP vulnerabilities (RC4 key scheduling weakness)

- Paper from Fluhrer, Mantin, Shamir (FMS), 2001:
  http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps
- Passive attack on WEP able to retrieve entire secret key in relatively small amount of time (4.000.000 packets)
- get information about all key bytes when PRNG input is known:
  - IV is known
  - First output byte ciphertext per IV is known

Appendix 2: WEP vulnerabilities (IV weakness)

- WEP exposes part of PRNG input.
  - IV is transmitted with message.
  - Every wireless frame has reliable and known first byte
    - Sub-network Access Protocol header (SNAP) used in logical link control layer, upper sub-layer of data link layer.
    - First byte is 0xAA
  - Attack is:
    - Capture packets with weak IV

      (specific IV values that easy calculation of a key byte when previous key bytes are known)
    - First byte ciphertext XOR 0xAA = First byte key stream
    - Can determine key from initial byte key stream
- Practical for 40 bit and 104 bit keys

Appendix 2: WEP vulnerabilities (IV weakness)

Wepcrack: http://wepcrack.sourceforge.net/

Airsnort: http://airsnort.shmoo.com/

Appendix 2: WEP vulnerabilities (IV weakness)

Avoid the weak IVs

- FMS (Fluhrer, Mantin, Shamir) described a simple method to find weak IVs
  - Many manufacturers avoid those IVs after 2002
  - Therefore Airsnort and others may not work on recent hardware
- However David Hulton (KoreK attack)
  - Properly implemented FMS attack which shows many more weak IVs
  - Identified IVs that leak into second byte of key stream.
  - Second byte of SNAP header is also 0xAA
  - So attack still works on recent hardware
  - And is faster on older hardware
  - http://packages.debian.org/unstable/net/aircrack-ng
  - http://weplab.sourceforge.net/
- PTW attack (uses Korek attack and RC4-KSA permutation)