الجامعة الافتراضية السورية

أمن الشبكات
Network and Infrastructure Security

د. محمد العصورة

Dr. Mohammed Assora

دكتوراه في امن شبكات الحواسب

PhD. In Computer Network Security

Wireless network Security

Objectives of Lecture

- Understand basics of physical layer options available for wireless transmission.
- Study the security issues arising in Wireless LANs
- Understand countermeasures available to further reduce threats in wireless networks.

wireless local area network (WLAN)

WLAN is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air.

WLAN has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing, and warehousing. Nowadays most, if not all, laptops and mobile phones around the world are equipped for WLAN.

It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced cost and scalability.

Regardless of the benefits mentioned above, WLAN have some security threats, in which anyone who use it should be aware of.

Wireless LAN (WLAN)

- IEEE 802.11 is a family of standards for wireless LANs
- 802.11b 5.5 Mbps and 11 Mbps.
  - Average throughput of ~4Mbps, range of 30-40m (indoor).
- 802.11g Supports up to 54Mbps
  - Average throughput of ~20 Mbps, range of 30-40m (indoor).
- 802.11n (Wi-Fi 4) Typical 75Mbps and maximum of 300Mbps.
  - Range of 70m (indoor).
- 802.11ac (Wi-Fi 5)Typical 433 Mbps up to several Gbps.
  - Range of 30-40m (indoor).
- 802.11ax (Wi-Fi 6): up to 9.6 Gbps,
  - range of 30m (indoor).

Interception

- Wireless LAN uses radio signal.
- Not limited to physical building.
- Signal is weakened by:
  - Walls;
  - Floors;
  - Interference.

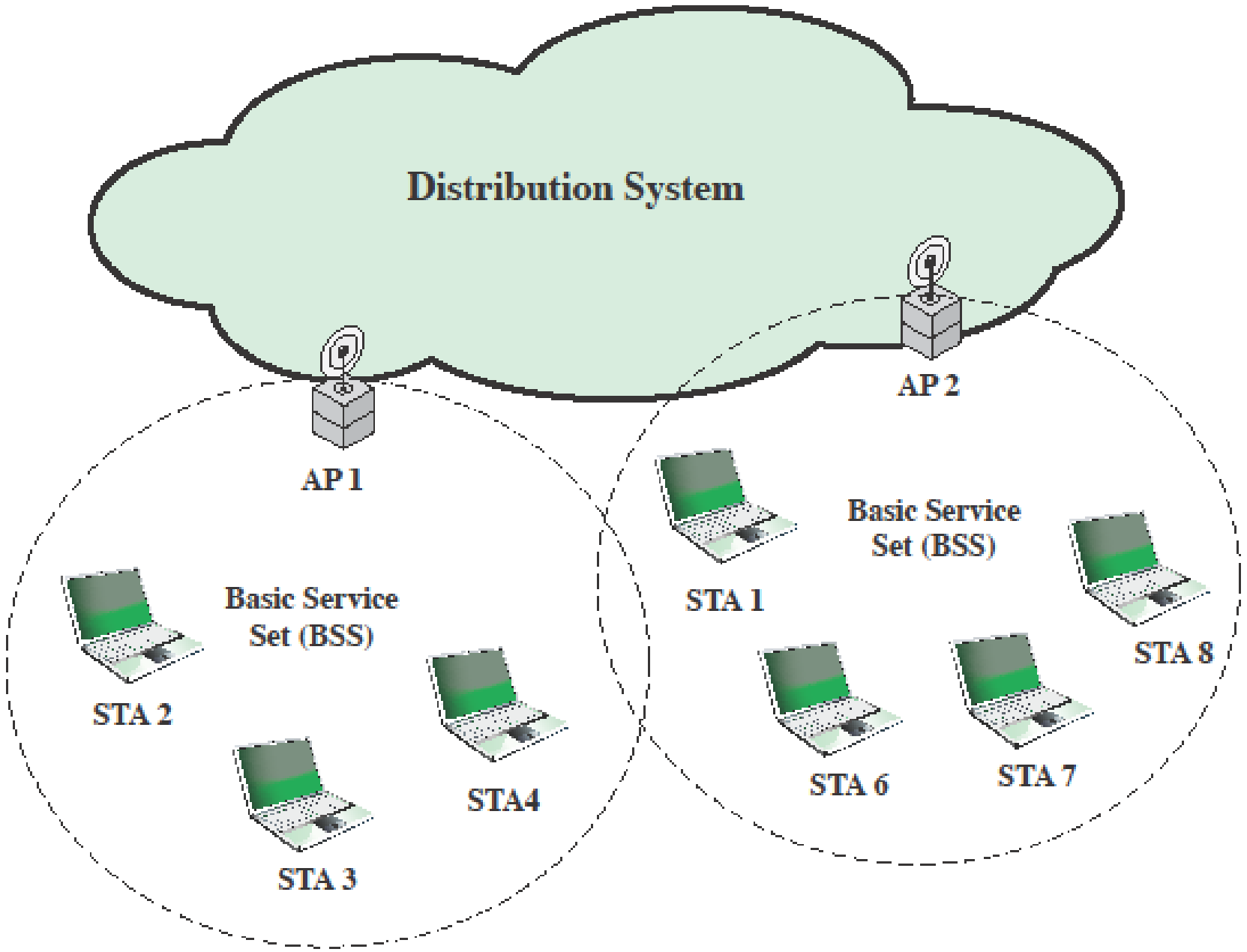
- Directional antenna allows interception over longer distances.

WLAN Components

- Two pieces of equipment defined:
  - Wireless station: A desktop or laptop PC or PDA or Mobile phone 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.

WLAN Architecture Model

- There are three main types of WLAN architecture:
  - **Infrastructure WLAN** (basic service set (BSS)): BSS WLAN consists of wireless stations and AP.
  - **Independent WLAN** (ad hoc LAN): no infrastructure is required, and the stations are self-organized. Independent networks can be set up whenever two or more wireless adapters are within range of each other
  - **Microcells and Roaming** (extended service set (ESS): The installation of multiple access points is required in order to extend the WLAN range beyond the coverage of a single access. The WLAN system hands off roaming users to the access point with the strongest and highest quality signal


Distribution System
AP 1
AP 2
Basic Service Set (BSS)
STA 2
STA 3
STA4
Basic Service Set (BSS)
STA 1
STA 6
STA 7
STA 8

Security threats for WLAN

- the 802.11 standard family faces a common set of security vulnerabilities due to the open wireless medium.

- We focus here on the security threats related to the wireless link between the stations and the AP, which is in many cases the last hop in the end-to-end path.

- We do not consider the security compromise of an AP nor the attacks on the wired network portion.

Attacks targeting the network infrastructure

- **Channel jamming**: The attacker can jam the wireless channel in the physical layer and effectively deny network access to legitimate users

- **Unauthorized access**: When authentication is not turned on, the attacker cannot only gain free network usage but also use the AP to bypass the firewall and access the internal network.

- **Traffic Analysis**: The attacker can analyze the overheard wireless traffic to obtain useful information

Attacks against the communication between the station and the AP

- **Eavesdropping**: eavesdropping is the most significant threat because with advanced antennas, it is possible to monitor wireless traffic from a few miles away.
- **Message forgery**: When the link is not protected for message integrity, the attacker can inject forged messages into both directions of the communication.
- **Message replay**: Even when message integrity is enforced, the attacker can replay previously recorded messages, including authentication data.
- **Man-in-the-middle attack**: The attacker can manage to reside between the station and the AP, and intercept and modify the messages on-the-fly.
- **Session hijacking**

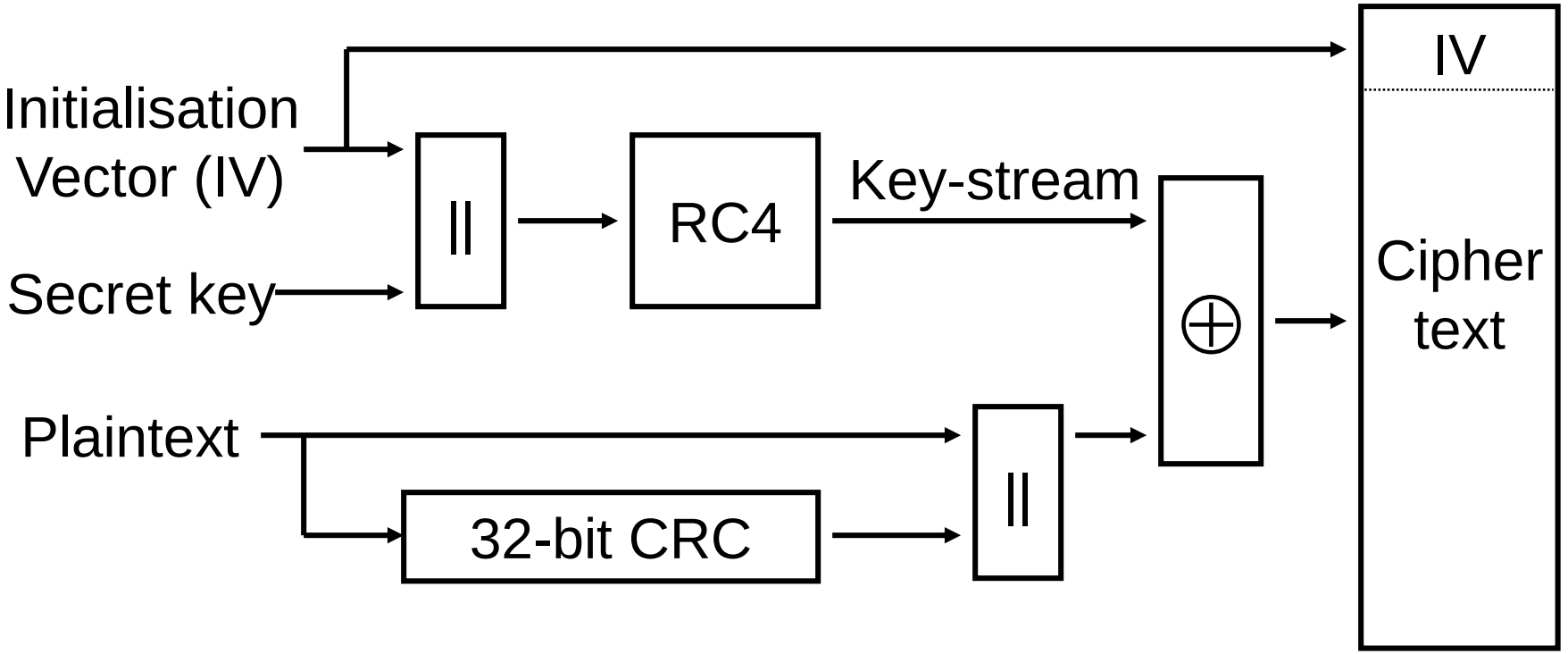
Securing Wireless transmissions

- Link-layer security mechanisms can provide strong information security by encrypting and integrity-checking.
- They also reduce network security threats by preventing unauthorized access.
- They do not address the jamming and traffic analysis attacks.
- Data communication over WLAN can also be protected at the network layer and above through end-to-end mechanisms (e.g., IPSec, VPN).
- These solutions cannot address wireless-specific attacks, such as unauthorized access or MITMA attacks.
- They can be used to complement link-layer mechanisms and further enhance end-to-end data security.

Wired Equivalence Privacy (WEP)

- Shared key between stations and an Access Point.
- 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 Encryption

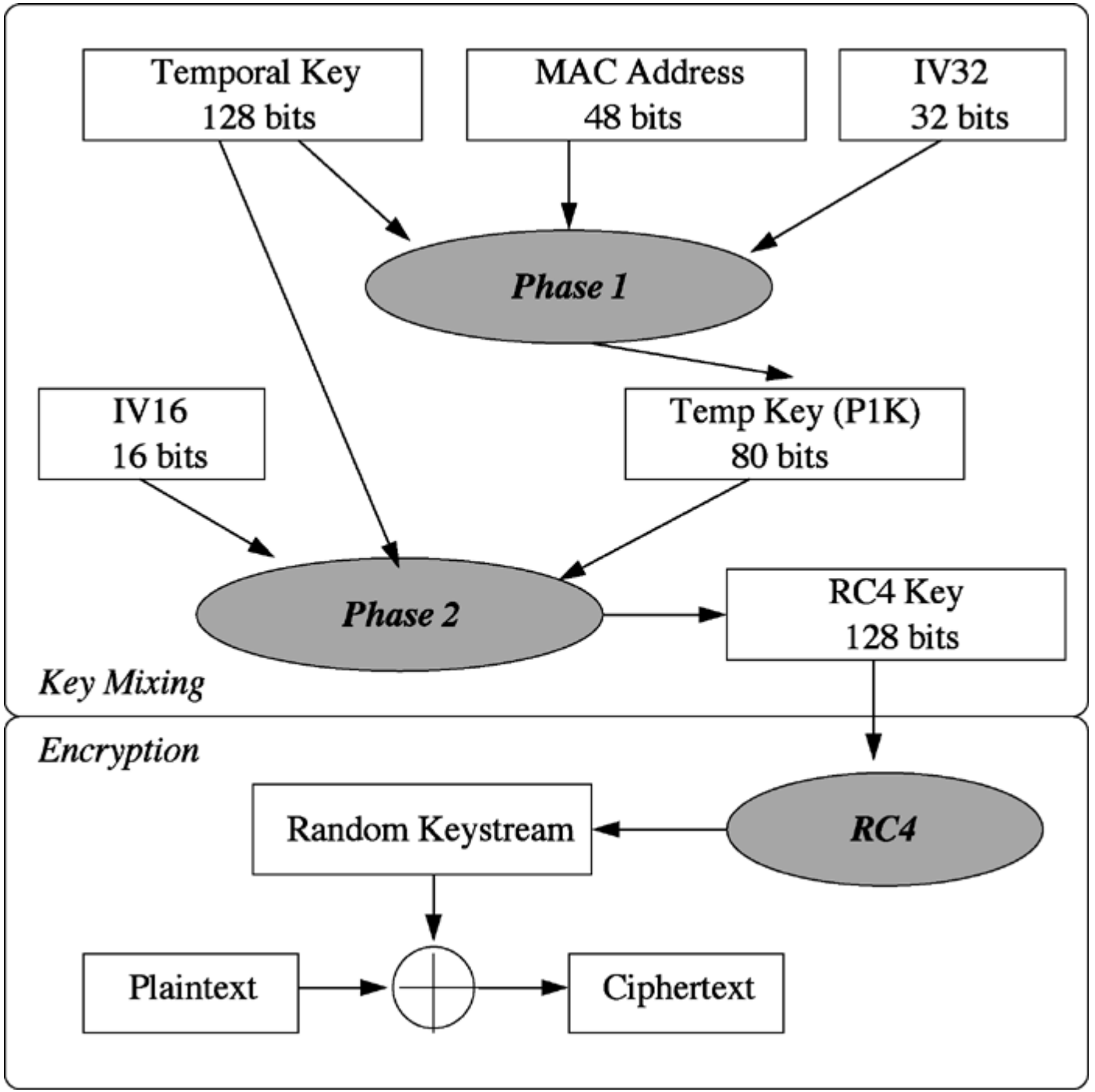


Insecurity of WEB

- Keystream reuse: key stream reuse means the same keystream being used to encrypt multiple messages
- Linear checksum: Linear checksum can be exploited to modify messages in arbitrary ways.
- Weak RC4 keys: Real implementations show that it requires only 20000 packets to recover the key, which takes less than 1 min in a loaded AP.

Wi-Fi Protected Access (WPA)

- The primary goal of WPA is to amend the known security flaws in WEP yet retain backward compatibility with legacy WEP devices.
- By keeping the underlying cryptosystem intact, the new features in WPA can be incorporated into legacy WEP devices through software or firmware updates.
- WPA addressed the security flaws in WEP through the following primitives:
  - Temporal Key Integrity Protocol (TKIP), a new data encryption protocol that defeats the keystream reuse and weak key attacks;
  - message integrity codes (MICs), which defeat the message forgery attacks;
  - 802.1x authentication, which achieves strong authentication, authorization, and key management.


Temporal Key
128 bits
MAC Address
48 bits
IV32
32 bits
Phase 1
IV16
16 bits
Temp Key (P1K)
80 bits
Phase 2
RC4 Key
128 bits
Key Mixing
Encryption
Random Keystream
RC4
Plaintext
Ciphertext

Robust Security network (RSN) WPA2 program

The IEEE 802.11 Task Group proposed RSN (or 802.11i), a new security standard for WLANs.

802.11i was adopted as the next-generation WPA, (WPA2). All WPA features, such as TKIP/Michael, are retained in 802.11i.

The new cryptosystem used in 802.11i is (AES). The benefit of using AES is increased security in the long run.

However, AES operations typically require a 64-bit coprocessor to improve the performance. As a result, the legacy WEP/WPA devices, especially the APs, can hardly be upgraded to 802.11i without hardware upgrade

Basic security primitives in 802.11i

- TKIP/Michael: TKIP and Michael are retained in 802.11i for data encryption and MIC computation, respectively.
- AES-CCMP: AES in Counter mode with CBC-MAC Protocol (AES-CCMP) is a new protocol for data encryption and MIC computation.
- 802.1x Authentication: 802.1x is used to authenticate the stations and distribute the keying materials.

Securing Wireless LANs (1)

Set and Enforce WLAN Policies:

- Every enterprise network needs a policy for WLAN. The policy management should define access requirements.
- Who needs access to what and when?
- WLAN policies should begin with the basics of forbidding unauthorized access points and ad hoc networks
- policies should be in place to forbid the reconfiguration of access points to alter their features.
- WLAN security is greatly increased with policies that limit WLAN traffic to operate on set channels, and only during select hours.
- Although policies are necessary, they can be useless paperweights without enforcement.

Securing Wireless LANs (2)

- **Configuring the wireless access points correctly:** Wireless access points are the network's central control units and are therefore responsible for their safety. these are the most important configuration steps:
- **Step 1:** Create individual administrator access
- **Step 2:** Select WPA2 as the encryption method.
- **Step 3:** Create a secure WLAN password.
- **Step 4:** Specify an unidentifiable network name.
- **Step 5:** Turn on automatic firmware updates.

Securing Wireless LANs (3)

- **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!
  - Sniff 802.11 packets,
  - Identify IP addresses,
  - Detect signal strength,
- Wireless Intrusion Detection
  - AirMagnet, AirDefense, Trapeze, Aruba,…

Securing Wireless LANs (4)

- **Wireless IDS/IPS**
- Sensors deployed in WLAN.
- Monitoring to detect:
  - Unauthorised clients by MAC address;
    - Accidental
    - Malicious
  - Ad-hoc mode networks;
  - Unauthorised access points;
  - Policy violations.
- Possible to identify approximate locations.