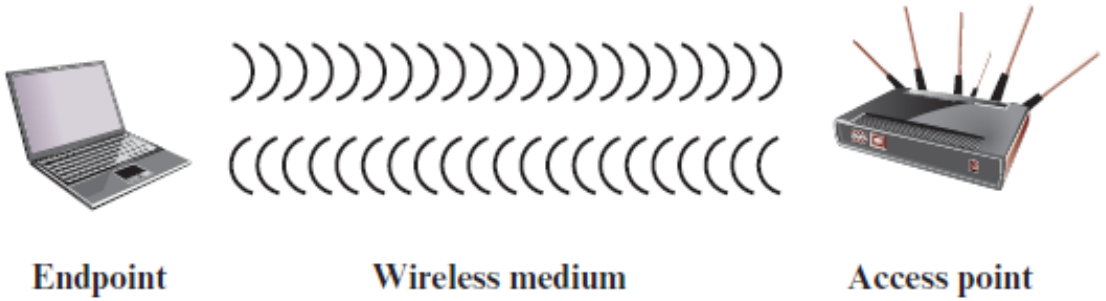
Wireless Security

Outline

- Threats against wireless systems.
- Wireless LAN - 802.11 standards.
- Wired equivalent privacy (WEP).
- Wifi Protected Access (WPA).
- IEEE 802.11i

Wireless Networking Components

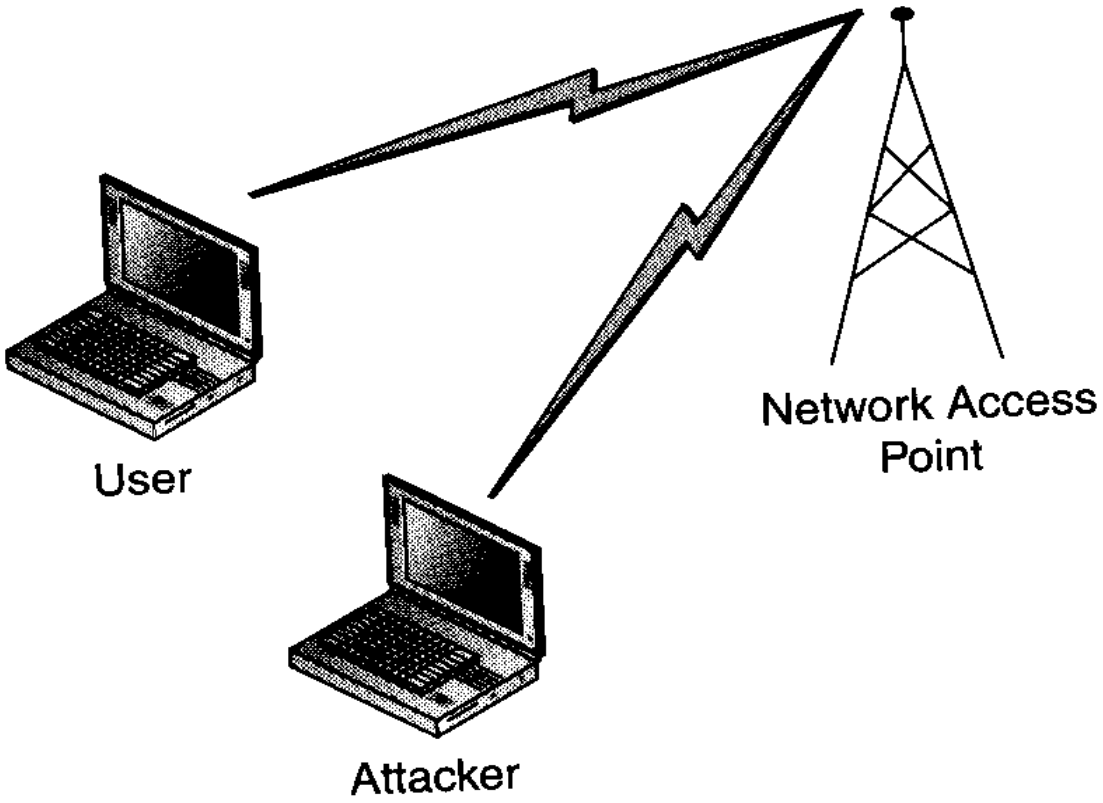


- Wireless client: cell phone, laptop, tablet, Bluetooth device, etc.
- Wireless access point provides a connection to the network or service. Examples: cell towers, Wi-Fi hotspots, access points to wired LAN or WAN
- Wireless medium carries the radio waves for data transfer.

Threats against Wireless systems

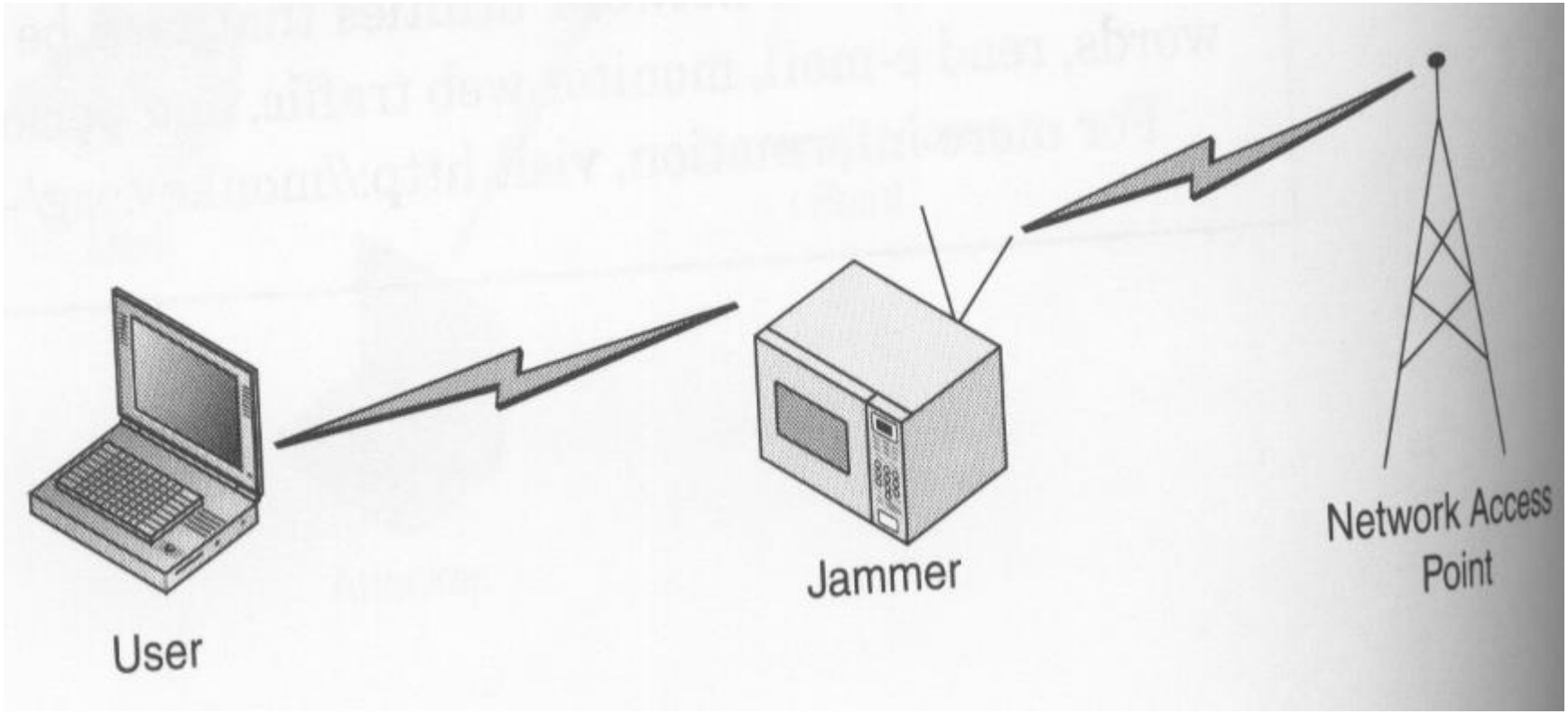
- Types of Threats:
  - Eavesdropping.
  - Communications jamming.
    - Denial of Service (DoS) jamming.
  - Injection and modification of data.
    - Man-in-the-Middle Attacks.
  - Rogue Access Point.
  - Cryptographic threats.
  - etc.

Eavesdropping



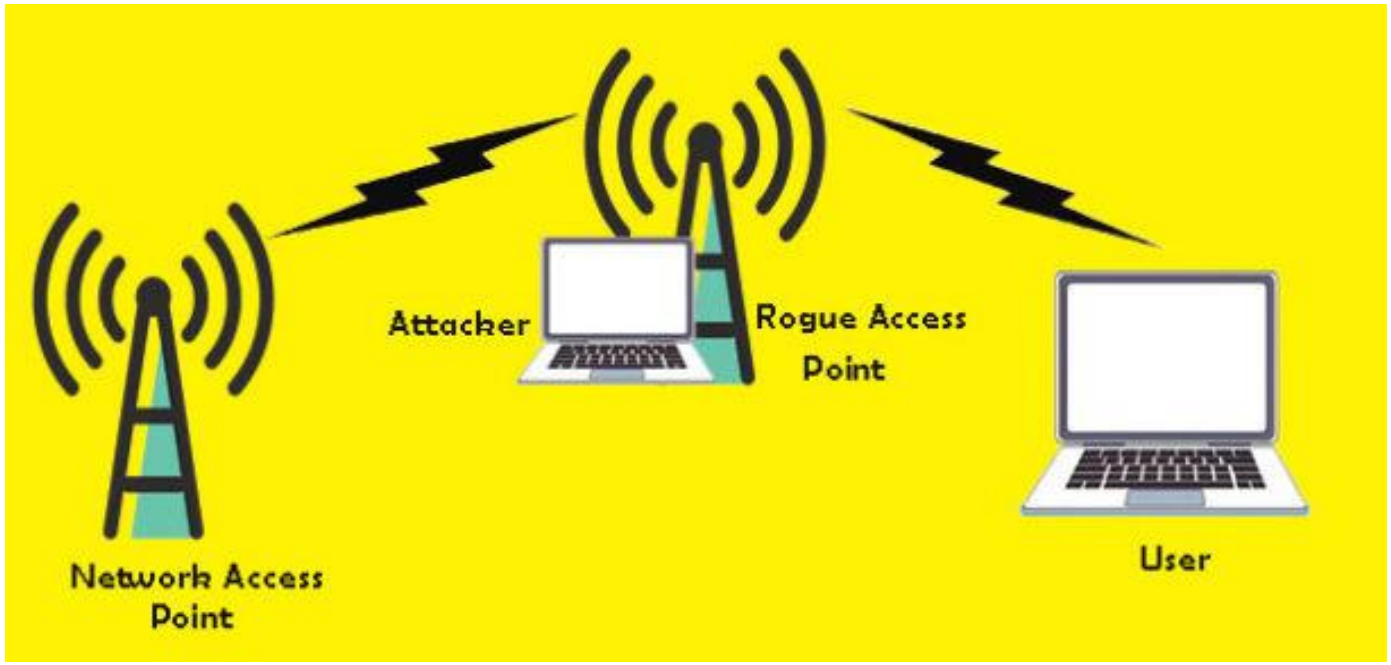
Listening in on communications.

Communications Jamming



Stopping legitimate users from accessing a network.

Rogue Access Point



One way to do this is to fool the user into linking to a rogue access point and then using the transmitted information to make a real login as that user.

Wireless LAN

- Primary benefits of Wireless LAN:
  - **Installation flexibility**:
    - The network can extend to areas that wires cannot reach, with significantly lower cabling cost.
  - **Scalability**:
    - Wireless LAN configurations can be easily changed.
  - **Installation Speed**:
    - A WLAN can be installed quickly enough to support mobile workgroups and assist in disaster recovery implementation.

802.11 for Wireless LANs

- IEEE 802.11 refers to a *family of specifications* for wireless local area networks (WLANs).
  - They have been developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).
- The 802.11 specification identifies an *over-the-air* interface between a wireless client and a base station, or between two wireless clients.

The 802.11 family

802.11 Standards	
802.11	The original WLAN Standard. Supports 1 Mbps to 2 Mbps.
802.11a	High speed WLAN standard for 5 Ghz band. Supports 54 Mbps.
802.11b	WLAN standard for 2.4 Ghz band. Supports 11 Mbps.
802.11e	Address quality of service requirements for all IEEE WLAN radio interfaces.
802.11f	Defines inter-access point communications to facilitate multiple vendor-distributed WLAN networks.
802.11g	Establishes an additional modulation technique for 2.4 Ghz band. Intended to provide speeds up to 54 Mbps. Includes much greater security.
802.11h	Defines the spectrum management of the 5 Ghz band for use in Europe and in Asia Pacific.
802.11i	Address the current security weaknesses for both authentication and encryption protocols. The standard encompasses 802.1X, TKIP, and AES protocols.

Wireless LAN Security

- The IEEE 802.11b standard defines an optional encryption scheme called Wired Equivalent Privacy (WEP), which includes a mechanism for securing wireless LAN data streams.
- The standard algorithm enables RC4-based, 40-bit data encryption with a 24 bit IV to prevent an intruder from accessing the network and capturing wireless LAN traffic.
  - WEP 2.0 uses a 104-bit key and a 24-bit IV.

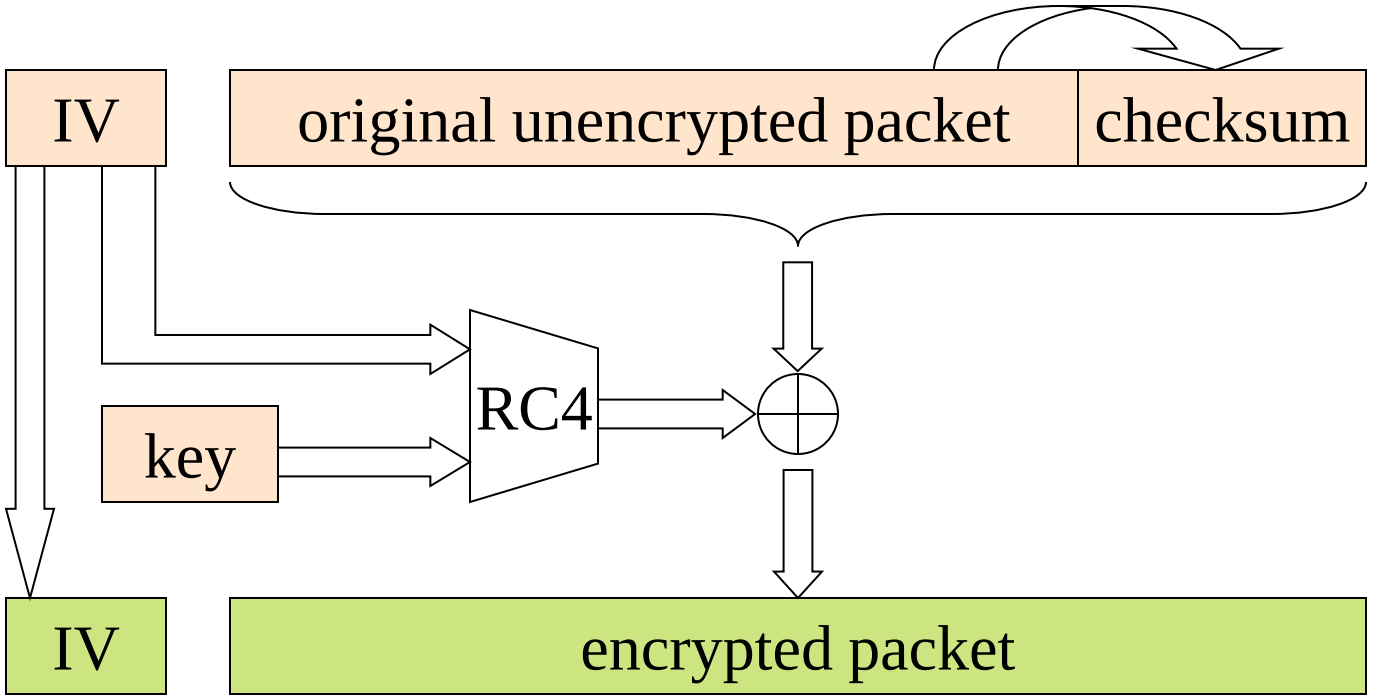
Wired Equivalent Privacy (WEP)

- WEP uses symmetric key cryptography.
- It aims to provide:
  - Access control: Only users with the correct WEP key can access the network.
  - Privacy: Protect WLAN data streams by encryption. Decryption is only possible by users who have the correct WEP key.

WEP security

- Two processes are applied to the plaintext:
  - One to add a checksum for the data.
  - One to encrypt the data & checksum.

WEP -- More Detail



WEP integrity

- To protect against unauthorised data, an integrity algorithm CRC-32 operates on the plaintext to produce the ICV.
- This is a (**non-cryptographic**) 32-bit checksum, or integrity check value (ICV).
- This expands the size of the encrypted message by 4 bytes above the length of the plaintext message.

WEP Encryption process

1. The 40-bit secret key is concatenated with an 24-bit initialisation vector (IV), resulting in a key with an overall length of 64-bits.
2. The resulting key is put into the pseudo-random number generator (PRNG), i.e., the stream cipher RC4.
3. The PRNG (RC4) outputs a pseudo-random key sequence based on the input key.
4. The resulting sequence is used to encrypt the data (M and ICV) by doing a bitwise XOR.

WEP Decryption process

1. The IV of the incoming message is used to generate the key sequence necessary to decrypt the incoming message.
2. The ciphertext, combined with the proper key sequence, yields the original plaintext and ICV.
3. The decryption is verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV to the ICV transmitted with the message.
4. If the ICV is not equal to the ICV received, the message has an error, and an indication is sent to the sending station.

Questions

- What is the purpose of introducing IV?

- What is the problem of using a short IV?

A Weakness of RC4

- Keystream leaks, under known-plaintext attack
  - Suppose we intercept a ciphertext C, and suppose we can guess the corresponding plaintext P
  - Let Z = RC4(K, IV) be the RC4 keystream
  - Since $C = P \oplus Z$, we can derive the RC4 keystream Z by

$$P \oplus C = P \oplus (P \oplus Z) = Z$$

- This is not a problem ... unless keystream is reused!

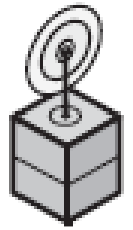
CRC32

- This is not a cryptographic checksum function
- It has a linear property

$$crc(P \text{ XOR } P') = crc(P) \text{ XOR } crc(P')$$

Will this property cause security problems?

Modification Attack



$(P||crc(P)) \oplus RC4(K)$

$(P||crc(P)) \oplus RC4(K) \oplus (P'||crc(P'))$

- CRC-32 is linear crc(P XOR P') = crc(P) XOR crc(P')

  $(P||crc(P)) \oplus RC4(K) \oplus (P'||crc(P'))$
  $= (P \oplus P')||((crc(P) \oplus crc(P')) \oplus RC4(K)$
  $= (P \oplus P')||(crc(P \oplus P') \oplus RC4(K)$

- The checksum on received packet is valid, but the message has been modified.

Weaknesses in WEP

Key management: A single secret key is used for both authentication and encryption.

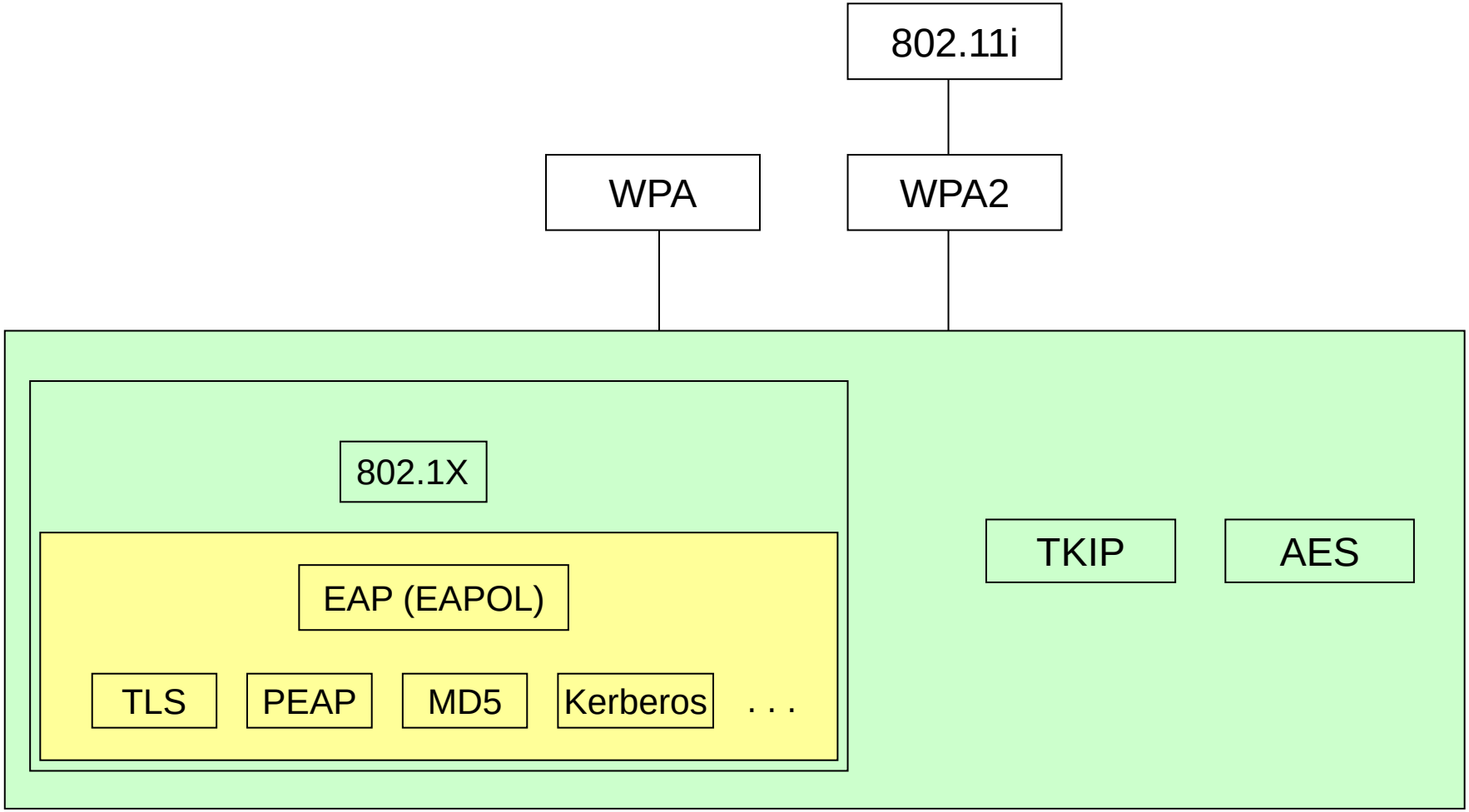
Integrity: It is possible to modify some bits in a message so that the resulting message still passes the ICV test.

Confidentiality: key size is too short (in version 1), Key stream reuse (IV is too short).

WEP should not be used anymore!

New Wi-Fi Security Standards

- Improved Security Standards:
  - 802.1x Authentication
    - Port-based Network Access Control
    - Extensible Authentication Protocol (EAP).
  - WPA (Wi-Fi Protected Access)
    - Temporal Key Integrity Protocol (TKIP).
  - 802.11i


802.11i
WPA
WPA2
802.1X
EAP (EAPOL)
TLS
PEAP
MD5
Kerberos
. . .
TKIP
AES

What is EAP?

- EAP (*Extensible Authentication Protocol*)
  - Authentication framework.
  - Supports multiple authentication methods.
  - Operates directly over the Data link layer.
  - Proprietary EAP types being developed by vendors, e.g., Cisco's Lightweight Extensible Authentication Protocol (LEAP).

What is IEEE 802.1X?

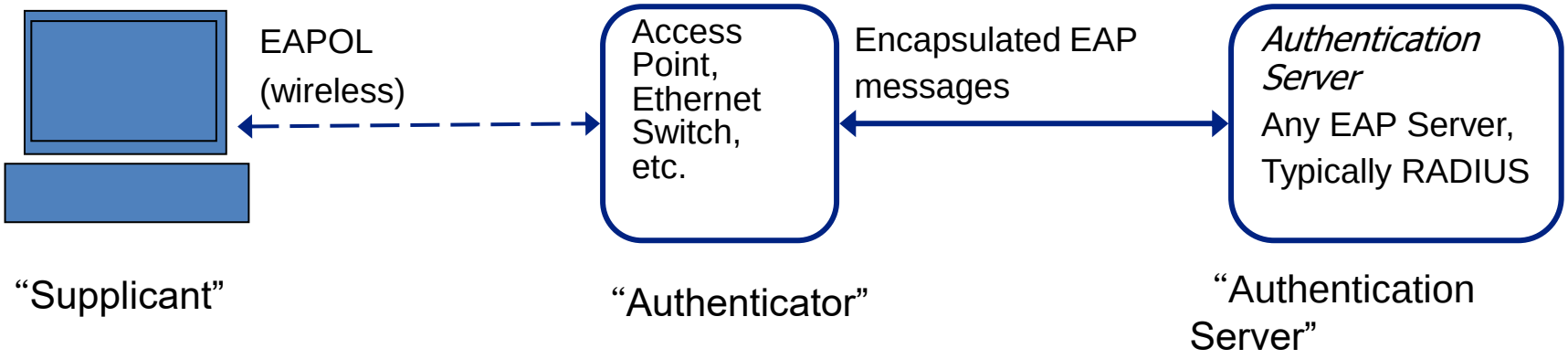
- A standard for passing EAP (*Extensible Authentication Protocol*) messages over a wired or wireless LAN.
- Port based network access control.
- Intended to provide:
  - **strong authentication.**
  - **access control.**
  - **key management**.

Essential Components

- **Supplicant** - Wireless terminal, basically the user or client
- **Authenticator** - Access Point, responsible for communication with Supplicant, submits information received from Supplicant to Authentication Server, which can then check Supplicant credentials for correct authorization.
- **Authentication Server** - provides authentication services to Authenticator to determine whether Supplicant is authorized to access services provided by the Authenticator.
  - The authentication server function *can be* located in the same entity as the authenticator function, but is typically in an external server (e.g. Remote Dial-in User Service – RADIUS Server).

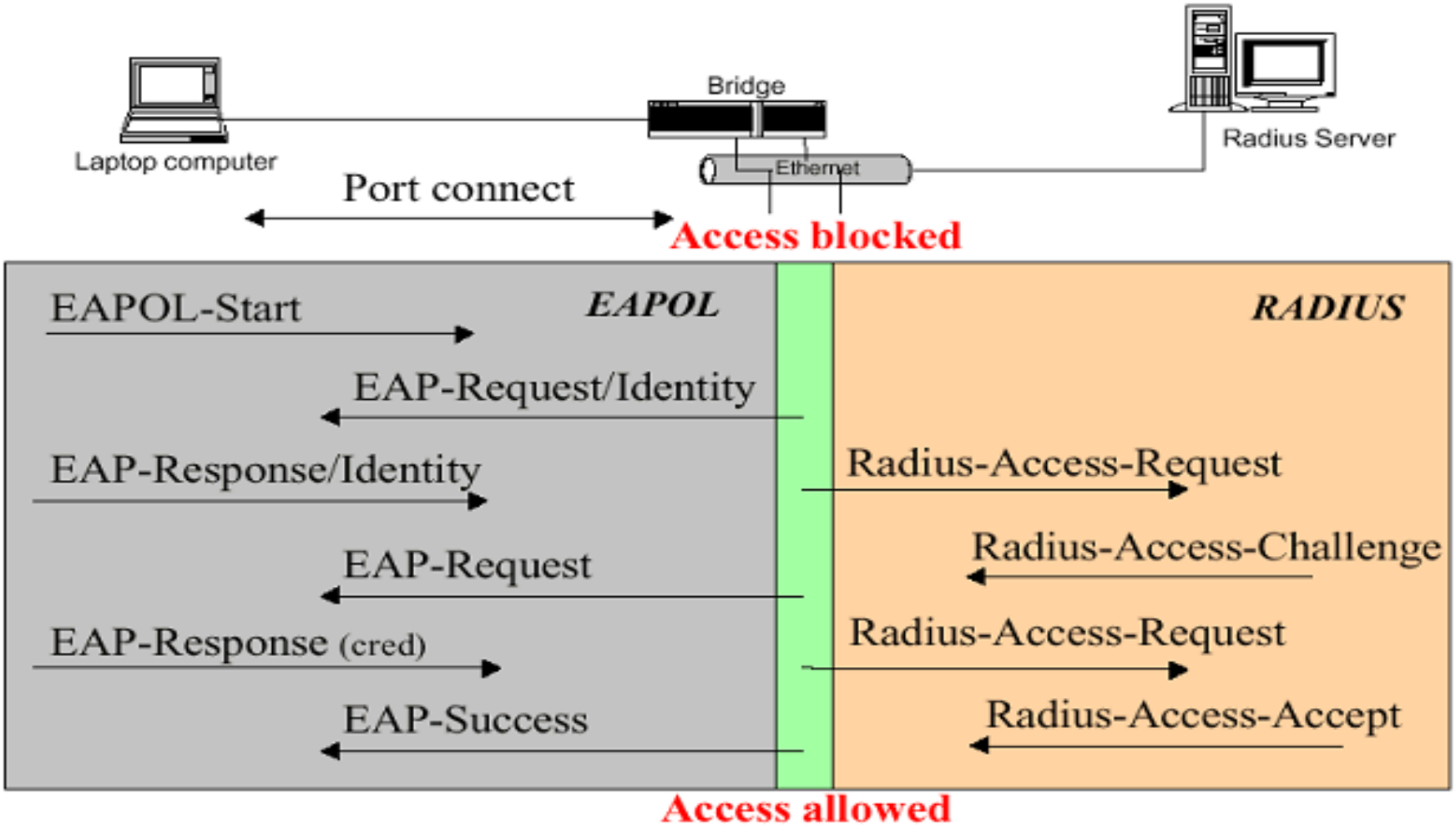
Setup

- IEEE 802.1X setup:
  - Supplicant authenticates via Authenticator to central Authentication Server.
  - Authentication Server confirms Supplicants credentials.
  - Authentication Server directs Authenticator to allow the Supplicant access to services after the successful authentication.



Handshake

- EAP and RADIUS messages in 802.1X authentication session.



Key Management

- Two sets of keys are generated:
  - **Pairwise Master Key** (**PMK**) is unique to an association between an ***individual Supplicant*** and the ***Authenticator*****.**
    - Derived from the 802.1X protocol
    - PMK + nonces ➔ encryption & authentication keys
  - **Groupwise Key:** shared among ***all Supplicants*** connected to same Authenticator.
    - Distributed by Authenticator in encrypted format

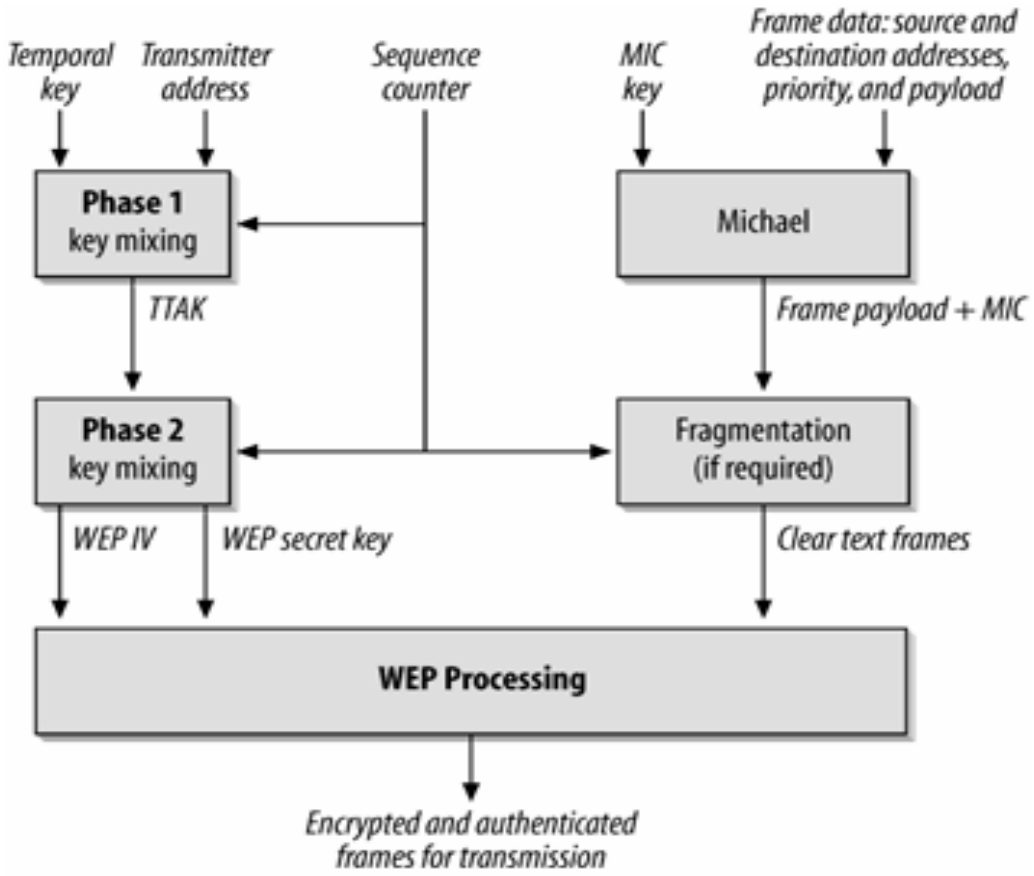
Pre-Shared Key (PSK)

- Home or Office environment, **easily configured** by home or office user.
- **No** centralised authentication server or EAP framework available.
- Requires the home or office user to **manually enter the password** to the Access Point or Wireless Gateway and have the same password in each PC that is allowed access to that wireless network.
  - Used as the PMK

TKIP

- WPA uses *Temporal Key Integrity Protocol* (TKIP) to provide stronger data encryption and address known vulnerabilities in WEP:
  - ─ Quick fix to overcome the reuse of encryption key problem in WEP.
  - ─ Uses existing device calculation capabilities to perform the encryption operations.
    - In particular, this means it is a relatively cheap method of improving security.
    - It is more like a patch though, rather than a new version.

Temporal Key Integrity Protocol (TKIP)

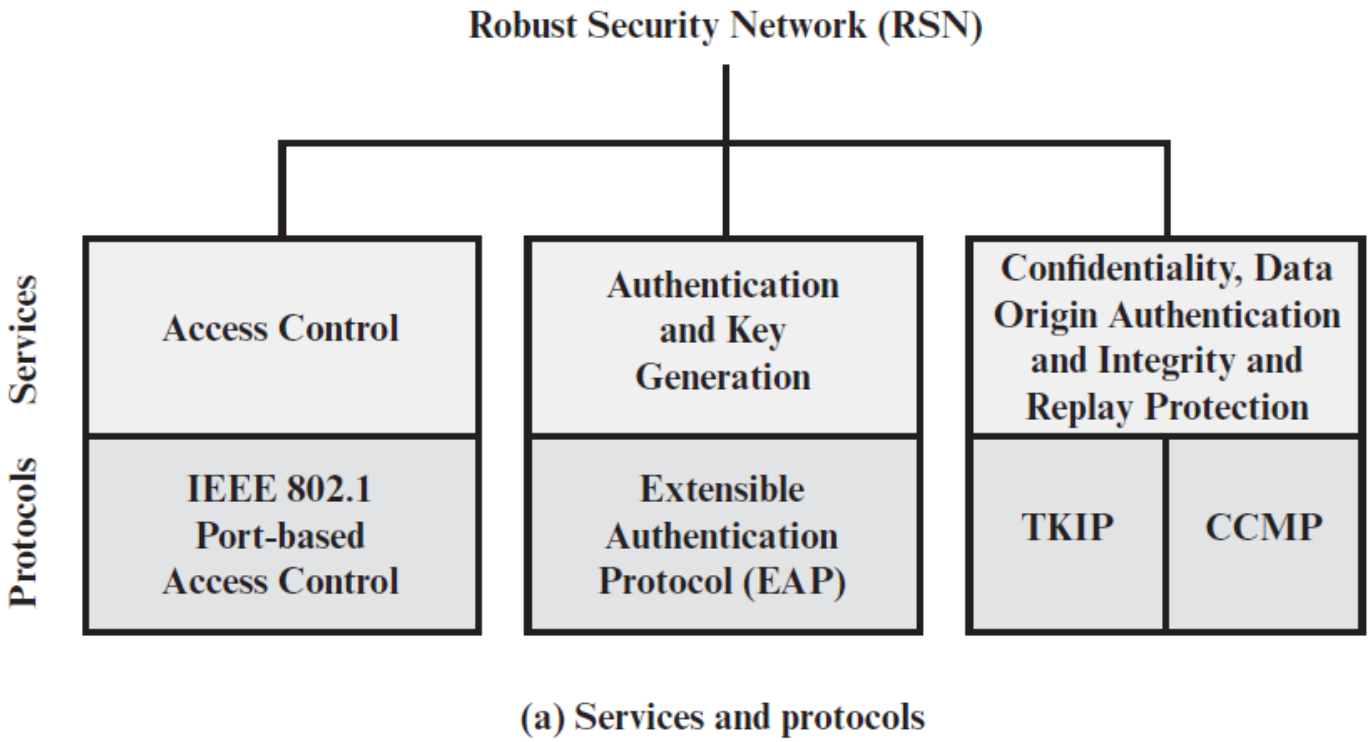


Matthew Gast, 802.11 Wireless Networks: The Definitive Guide

Data Encryption

- TKIP Sequence Counter (**TSC**): 48 bits
- **Temporal** and **MIC Keys** derived from **Pairwise Master Key** (**PMK**) - PMK derived as part of 802.1X exchange.
- *Message Integrity Check* (**MIC**):
  - Cryptographic **checksum** (called Michael) designed to make it much more difficult for an attacker to successfully intercept and alter data.

IEEE 802.11i



(a) Services and protocols

IEEE 802.11i Security Protocol

- *CCMP: Counter Mode with Cipher Block Chaining MAC Protocol*
  - CCMP is intended for newer IEEE 802.11 devices that are equipped with the hardware to support this scheme. As with TKIP, CCMP provides two services:
    - Message integrity: CCMP uses the cipher-block-chaining message authentication code (CBC-MAC).
    - Data confidentiality: CCMP uses the CTR operation mode with AES for encryption.