School of Electrical Engineering and Computing

SENG2250/6250
SYSTEM AND NETWORK SECURITY
(S2, 2020)

Wireless Security

THE UNIVERSITY OF
NEWCASTLE
AUSTRALIA

Outline

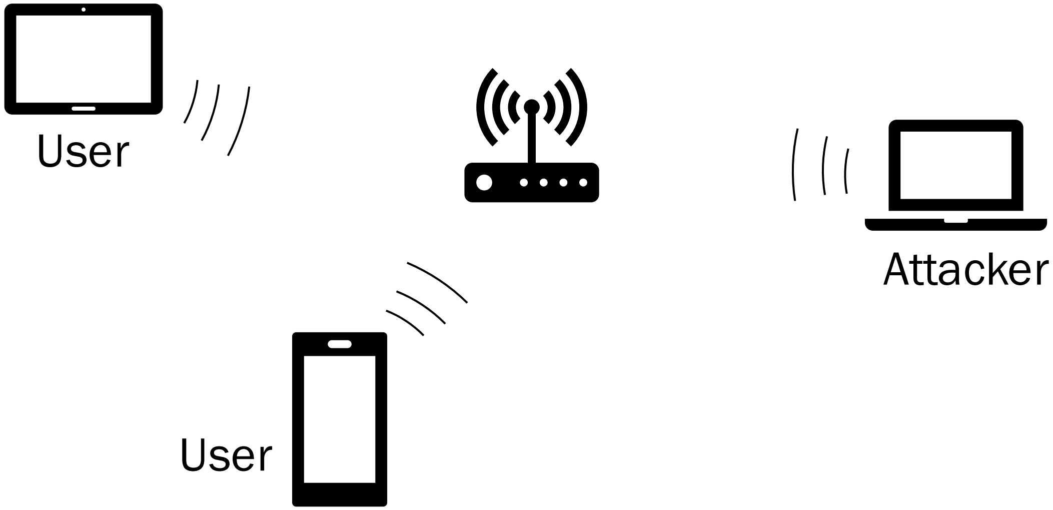
- Threats
- 802.11 Standards
- Operational Modes
- WEP
- WPA

Wireless Security Related Topics

- Wireless LAN 802.11
- Bluetooth
- Telecommunication Networks
  - *GSM/3G/4G/5G*
- Wireless Application Protocols (WAP)
- Radio Frequency IDentification (RFID)

Threats against Wireless Systems

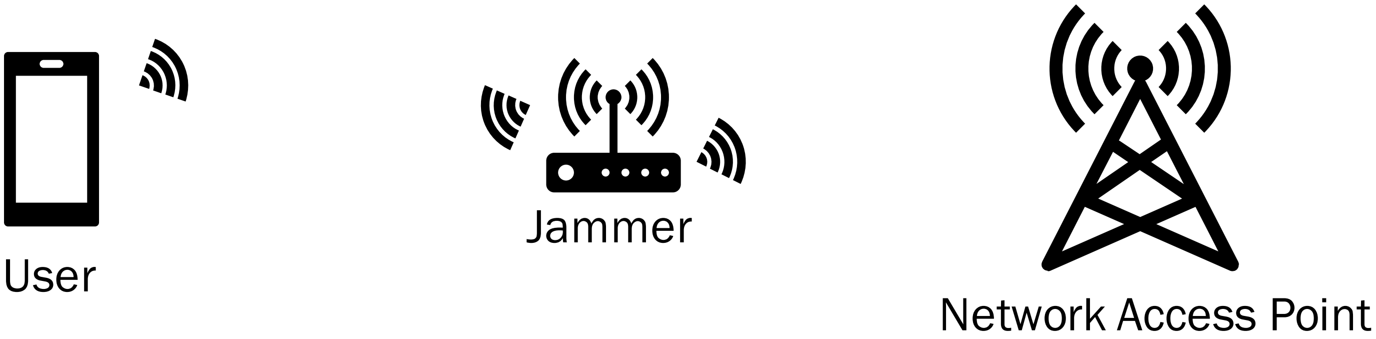
- Wireless networks are essentially more vulnerable to attacks as any device within radio range of a network could send or receive data, without being *physically* connected to the network.



Threats against Wireless Systems

- Eavesdropping
- Communications jamming
  - *E.g, DoS/DDoS*
- Injection and modification of data
  - *Man-in-the-middle attacks*
- Rogue clients
- Cryptographic threats

Communications Jamming



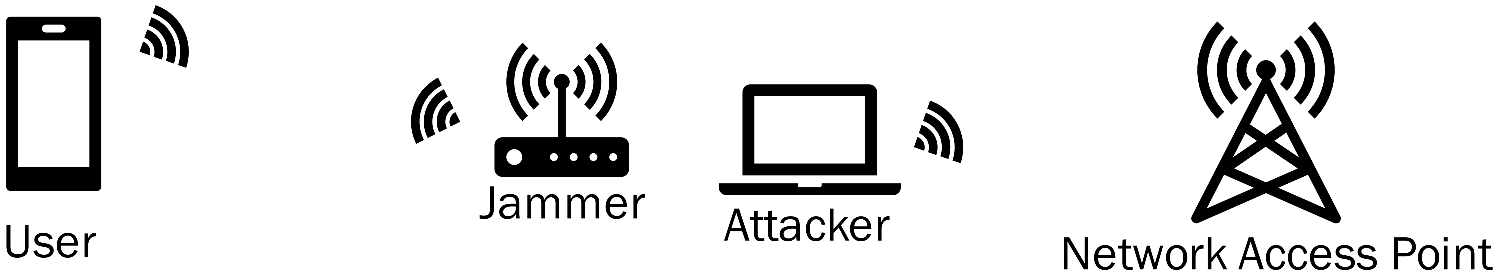
User

Jammer

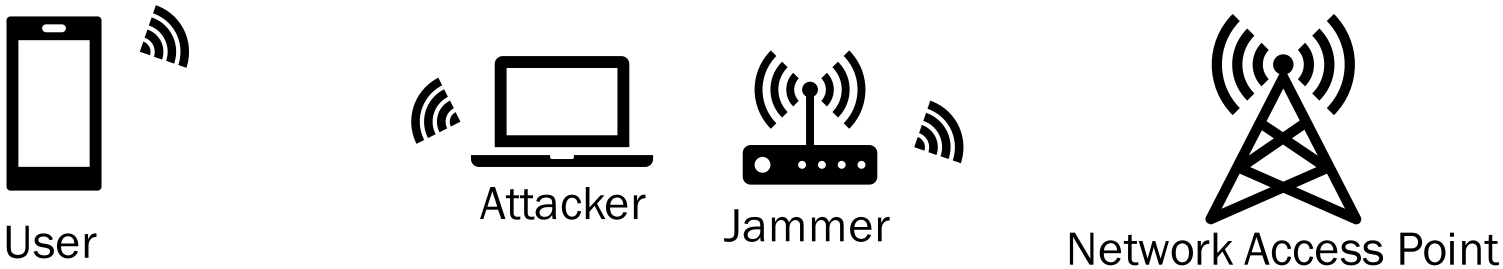
Network Access Point

Stopping legitimate users from accessing a network.

Jamming Attacks: Two Targets

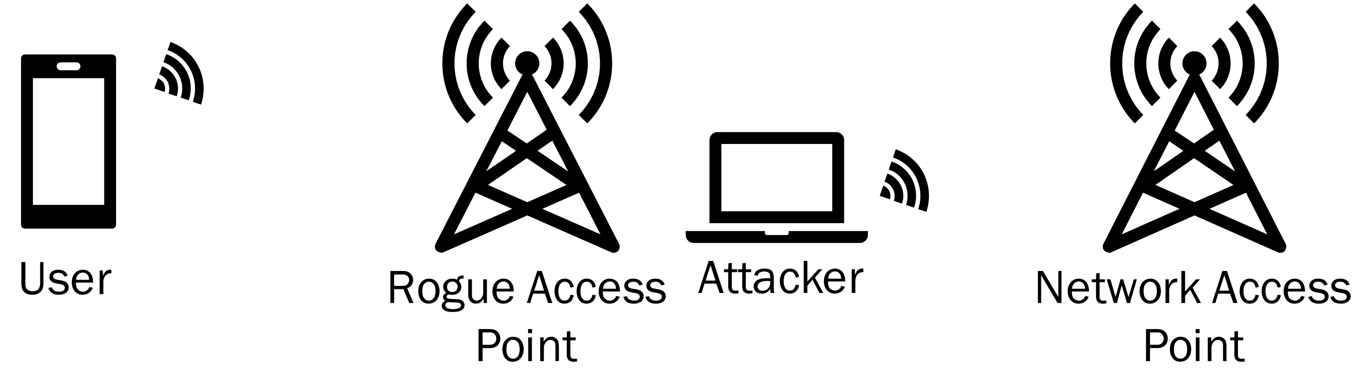


Jamming attack against client to hijack communications.



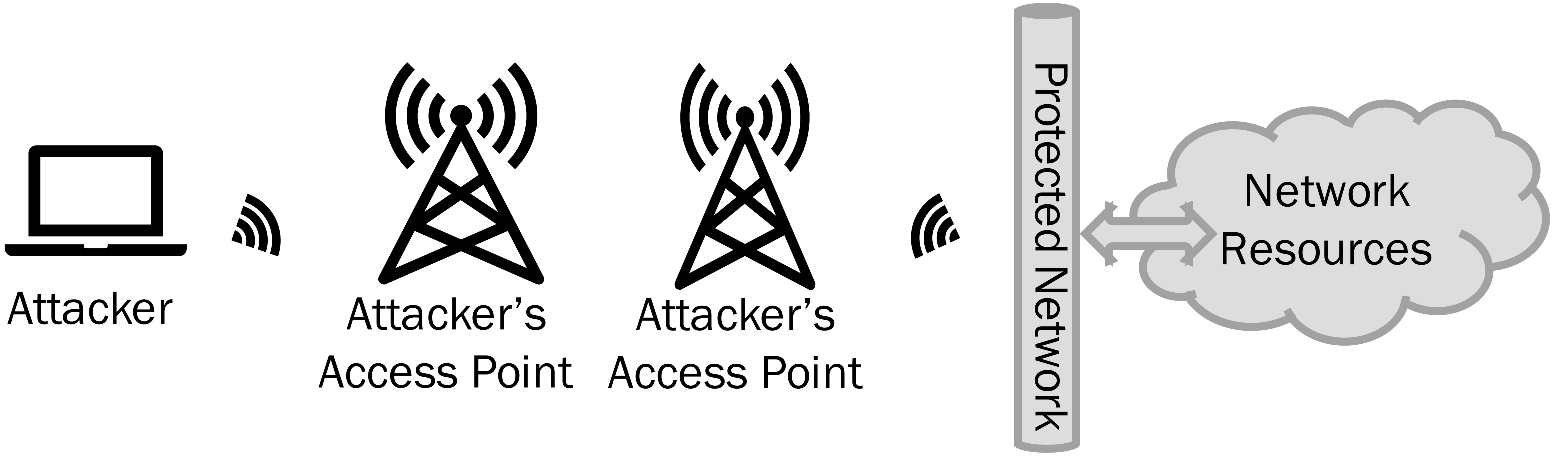
Jamming attack against access point to hijack communications.

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.

Extending Range of Attacks by Chaining Access Points



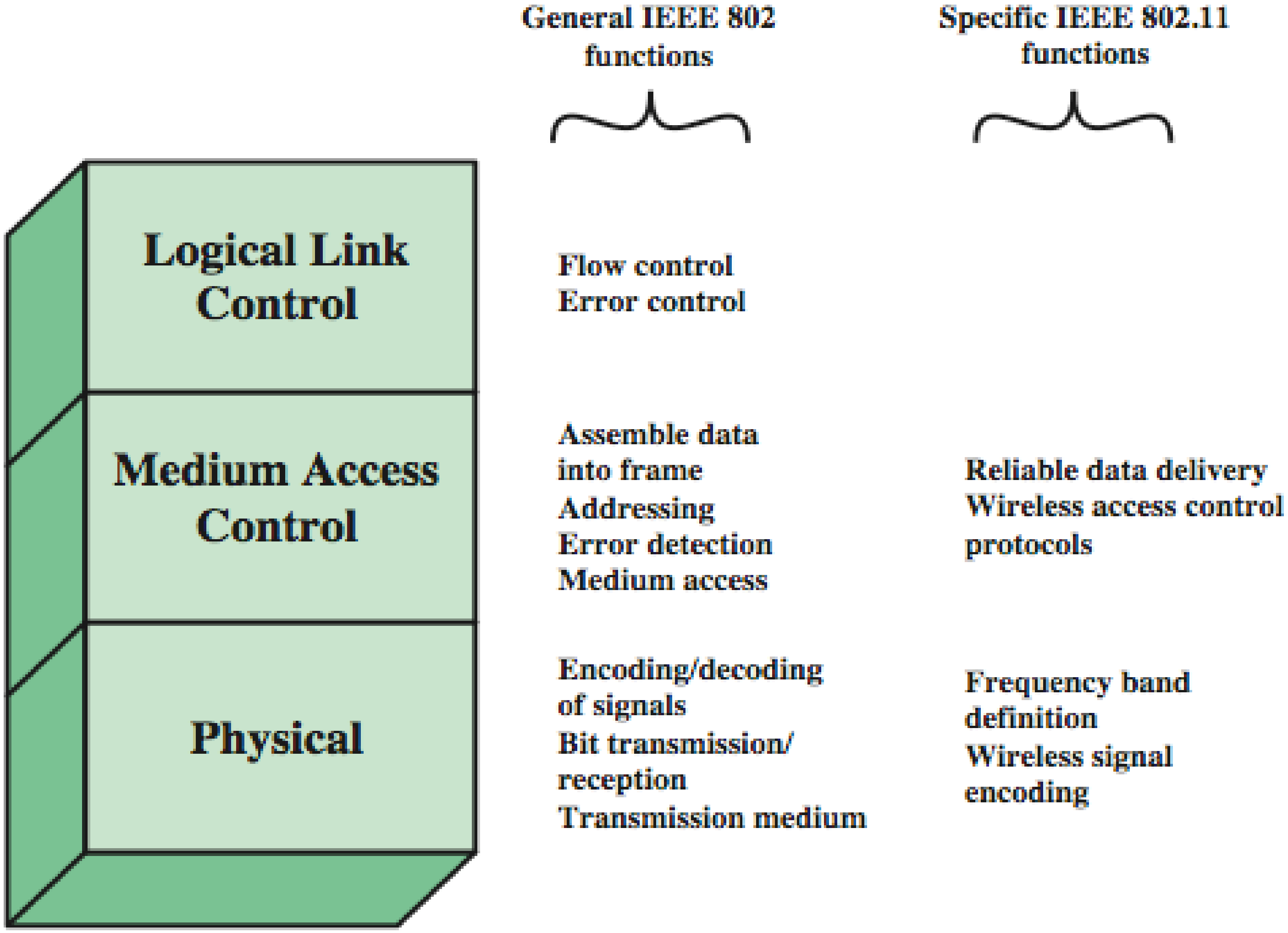
Cryptographic Threats: Examples

- CDMA and GSM cryptographic protection
  - *A5/1: A stream cipher used for providing private communication among the GSM cellular telephones.*
  - *Initially hidden but…*
    - General design leaked in 1994.
    - Reverse-engineered in 1999.
    - Broken. Various attacks against it.
    - In 2000, about 130 million GSM customers relied on A5/1; 4 billion by 2011.
- Wired Equivalent Privacy (WEP) for 802.11b
  - *Implementation flaws and key management issues:*
    - WEP becomes useless (kind of).
    - It is still used though!

Wireless LAN (WLAN)

- Use radio waves – super high to ultra high frequencies – microwaves.
- Primary benefits of WLAN
  - *Installation flexibility*
    - The network can extend to areas where wires cannot reach, with significantly lower cabling cost.
  - *Installation speed*
    - A WLAN can be installed quickly enough to support mobile workgroups and assist in disaster recovery implementation.
  - *Scalability*
    - WLAN configurations can be easily changed.

IEEE 802 Protocol Architecture



	General IEEE 802 functions	Specific IEEE 802.11 functions
Logical Link Control	Flow control Error control	
Medium Access Control	Assemble data into frame Addressing Error detection Medium access	Reliable data delivery Wireless access control protocols
Physical	Encoding/decoding of signals Bit transmission/ reception Transmission medium	Frequency band definition Wireless signal encoding

802.11 for WLAN

- IEEE 802.11 refers to a family of specifications for 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 mobile device wireless client and a base station, or between two mobile device wireless clients.

The 802.11 Family (Part of)

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.

802.11 Wireless Network Operational Modes

- IEEE 802.11 wireless networks operate in one of the two modes:
  - *Ad hoc mode*
  - *Infrastructure mode*

Ad hoc Mode

- In *ad hoc mode*, each mobile device client communicates directly with other mobile device clients within the network.
  - *No access point is required to connect to any wired LAN.*
  - *If a client in an ad hoc network wants to communicate outside of the cell, a member of the cell must operate as a gateway and provide a routing service.*

Infrastructure Mode

- In *infrastructure mode*, each mobile device client sends all its communications to a network device called an *access point* (AP).
- *The AP acts as an Ethernet bridge and forwards the communications to the appropriate network, such as a wired LAN or another wireless network.*

WLAN 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 key 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.*

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 keys.*

WEP Security

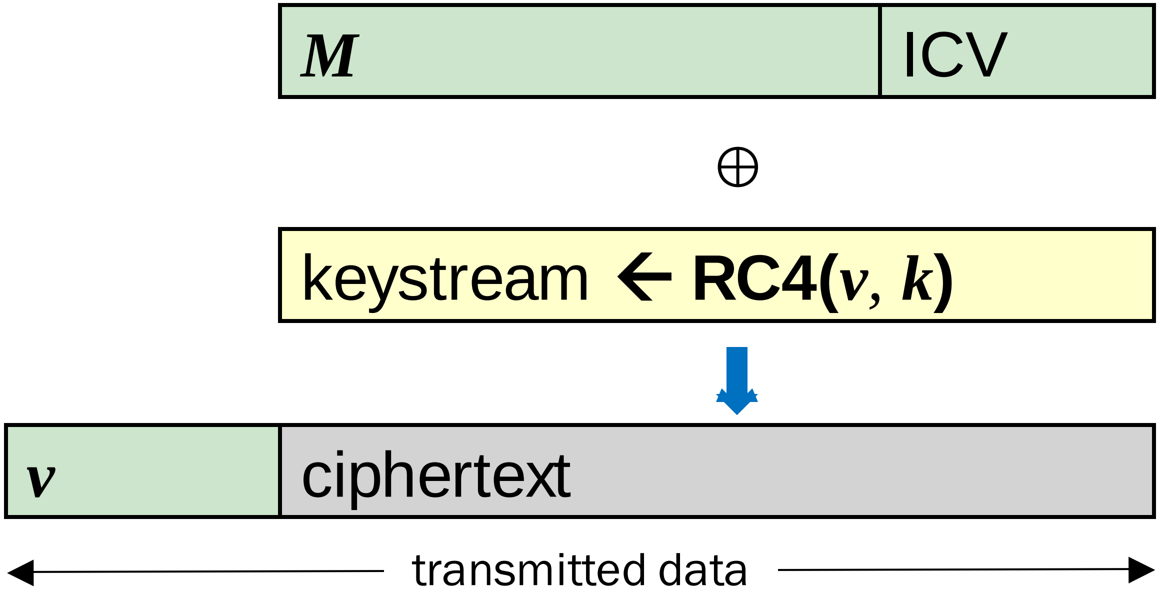
- Two processes are applied to the plaintext
  - *One to protect against unauthorized modification of the data.*
  - *One to encrypt the plaintext.*

WEP Integrity

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

WEP Confidentiality

- M – message
- v – current IV
- k – shared secret key



M ICV

$\oplus$

keystream ← **RC4(**v, k**)**

v ciphertext

transmitted data

WEP Encryption Process

1. The 40-bit secret key is concatenated with a 24-bit initialization 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 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.

Weakness in WEP

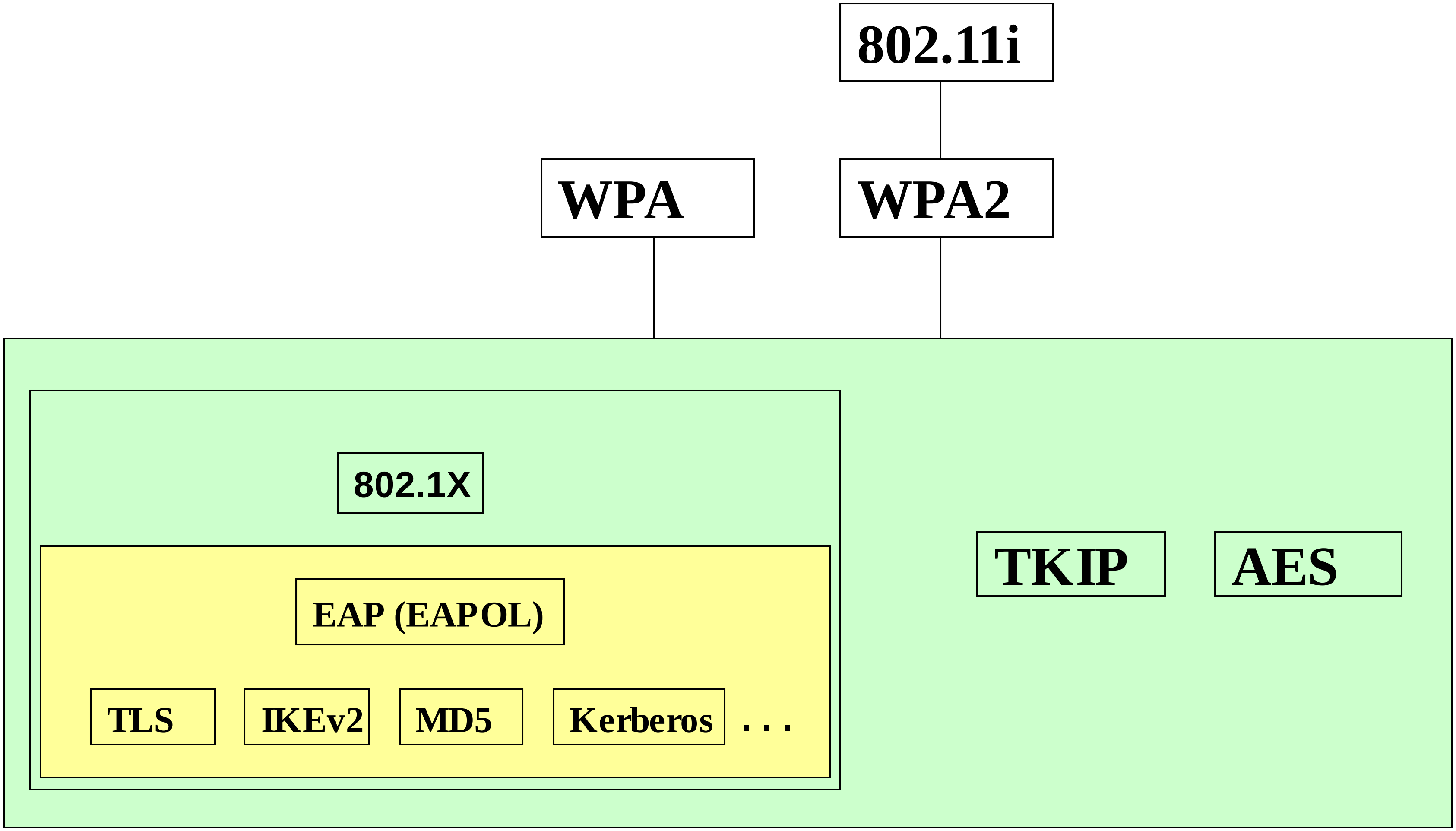
- Key management and key size
  - *The same shared secret key is used for both authentication and encryption, and key size is too short.*
- Authentication
  - *Only one-way authentication. That is, AP is not authenticated to the client.*
- Integrity
  - *It is possible to modify some bits in a message so that the resulting message still passes the ICV test.*

Access Point Security

- Some guidelines for AP
  - *Configure the AP with nondefault settings.*
    - Leaving devices on the manufacturers default is a very dangerous thing to do.
  - *Use MAC address filtering.*
  - *Use sniffing tools and Intrusion Detection Systems (IDS)*

You shouldn't use WEP!

Improved Security Standards



IEEE 802.1X

- A standard for encapsulating EAP (Extensible Authentication Protocol) over a wired or wireless LAN.
- Port-based Network Access Control
- Authentication mechanism to devices wishing to attach to a LAN or WLAN.
- Three parties are necessary to complete an authentication exchange.
  - *Supplicant: This is an entity wanting access to somewhere.*
  - *Authentication Server: This does the authentication.*
  - *Authenticator: This is the in-between system, such as a wireless access point.*

Essential Components

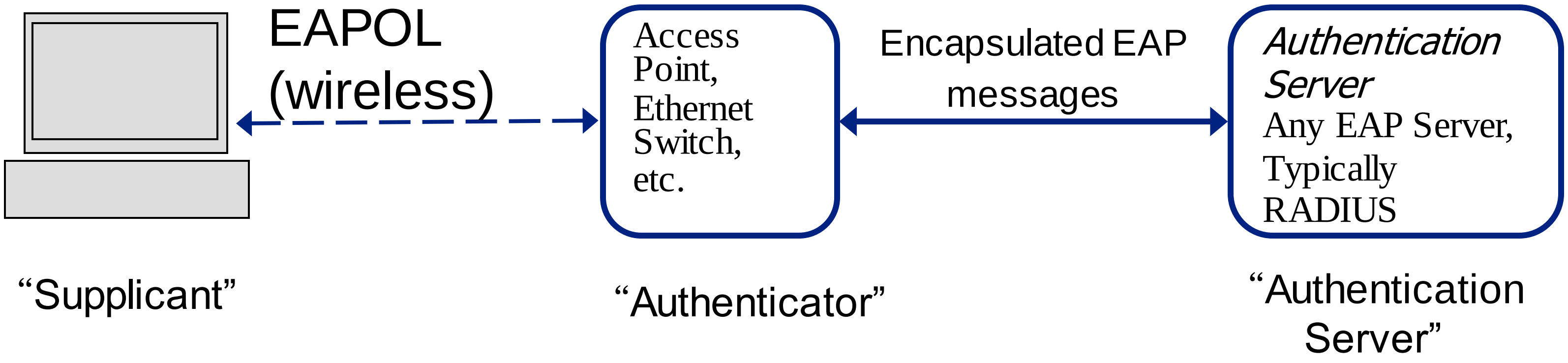
- **Supplicant** – Wireless terminal, basically the user or client.
- **Authenticator** – Access point, responsible for communication with Supplicant, submits information received from Supplicant to Authentication Server, which can then check Supplicant credentials for correct authorization.
- **Authentication 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)*

EAP

- Extensible Authentication Protocol
  - *Authentication framework.*
  - *Supports multiple authentication methods.*
    - EAP authentication types include EAP-MD5, EAP-TLS, EAP-SIM, etc.
  - *Operates directly over the data link layer.*
  - *Proprietary EAP types being developed by vendors, Cisco's Lightweight Extensible Authentication Protocol (LEAP).*

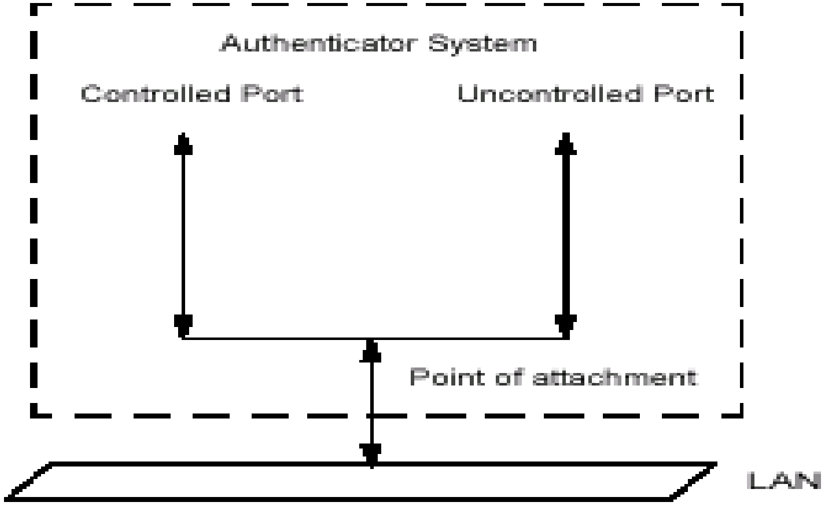
Setup

- 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.*


EAPOL
(wireless)
Access Point, Ethernet Switch, etc.
Encapsulated EAP messages
Authentication Server
Any EAP Server, Typically RADIUS
“Supplicant”
“Authenticator”
“Authentication Server”

Port-based Access Control

- Controlled Port: accepts packets from authenticated devices.
- Uncontrolled port: only passes 802.1X packets.



- Point of attachment: association between Wireless Terminal and Access Point.

Port-based Access Control

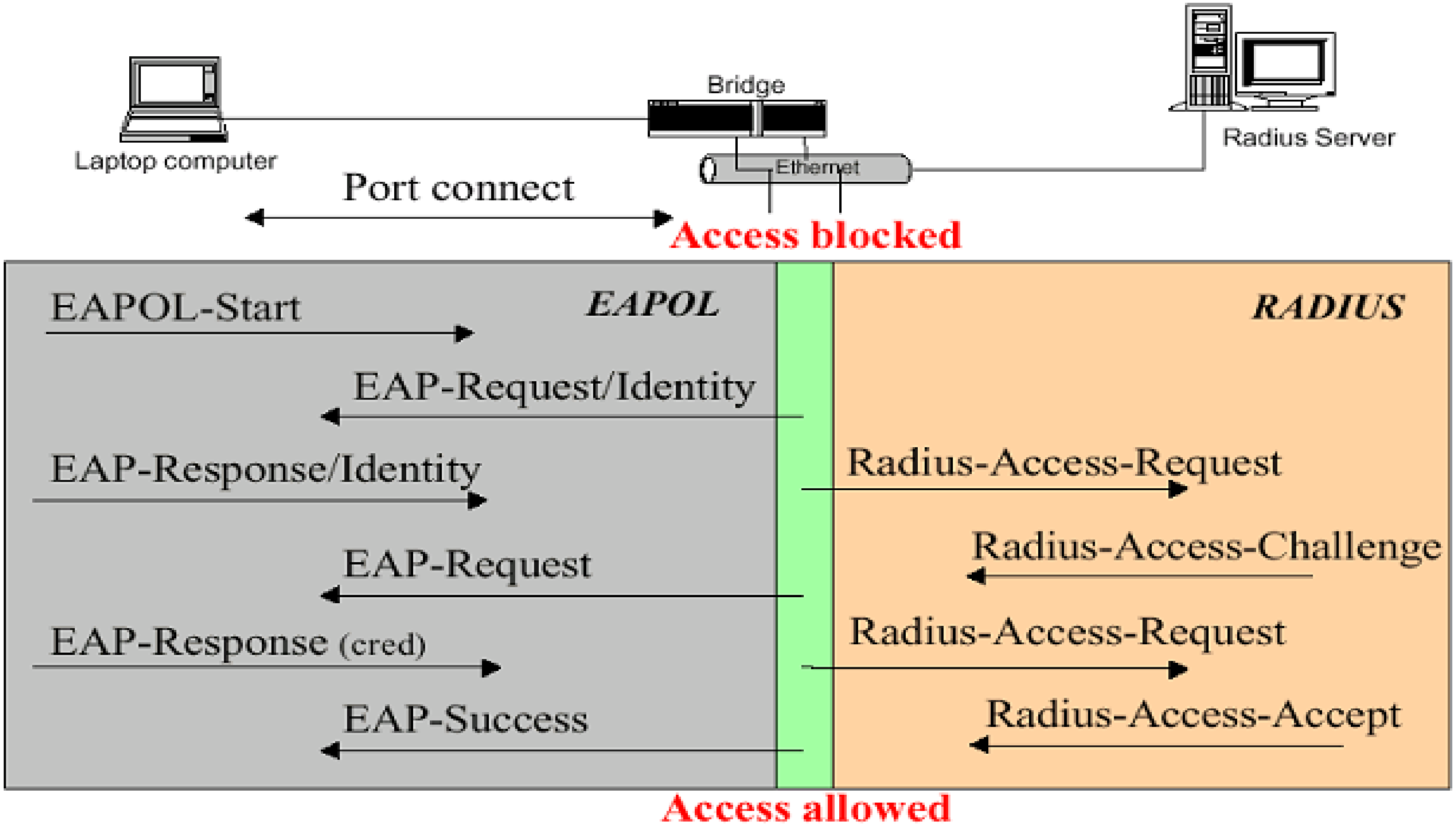
- Port-based access control (Authenticator)
  - ***Controlled Port*** *and* ***Uncontrolled Port*** *are two* ***logical*** *entities, but are the same* ***physical connection****, or point of attachment.*
  - *The point of attachment is an association between the Supplicant and the Authenticator.*

How does the authentication work?

- On detection of a new supplicant, the port on the authenticator is enabled and set to the “unauthorized” state. In this state, only 802.1X traffic is allowed, other traffic is dropped.
- To initiate authentication the authenticator will periodically transmit EAP-Request Identity frames. The Supplicant, on receipt of EAP-Request Identity frame, responds with an EAP-Response Identity frame containing an identifier for the Supplicant such as a User ID.
- The authenticator then encapsulates this Identity response in a RADIUS Access-Request packet and forwards it on to the authentication server.

4-Way Handshake

EAP and RADIUS messages in 802.1X authentication session.



Encryption Keys

- Two sets of encryption keys are generated
  - ***Pairwise Master Key*** *(PMK) is unique to an association between an individual Supplicant and the Authenticator.*
  - ***Groupwise Key:*** *shared among all Supplicants connected to same Authenticator.*
- PMK used to generate additional encryption and authentication keys.

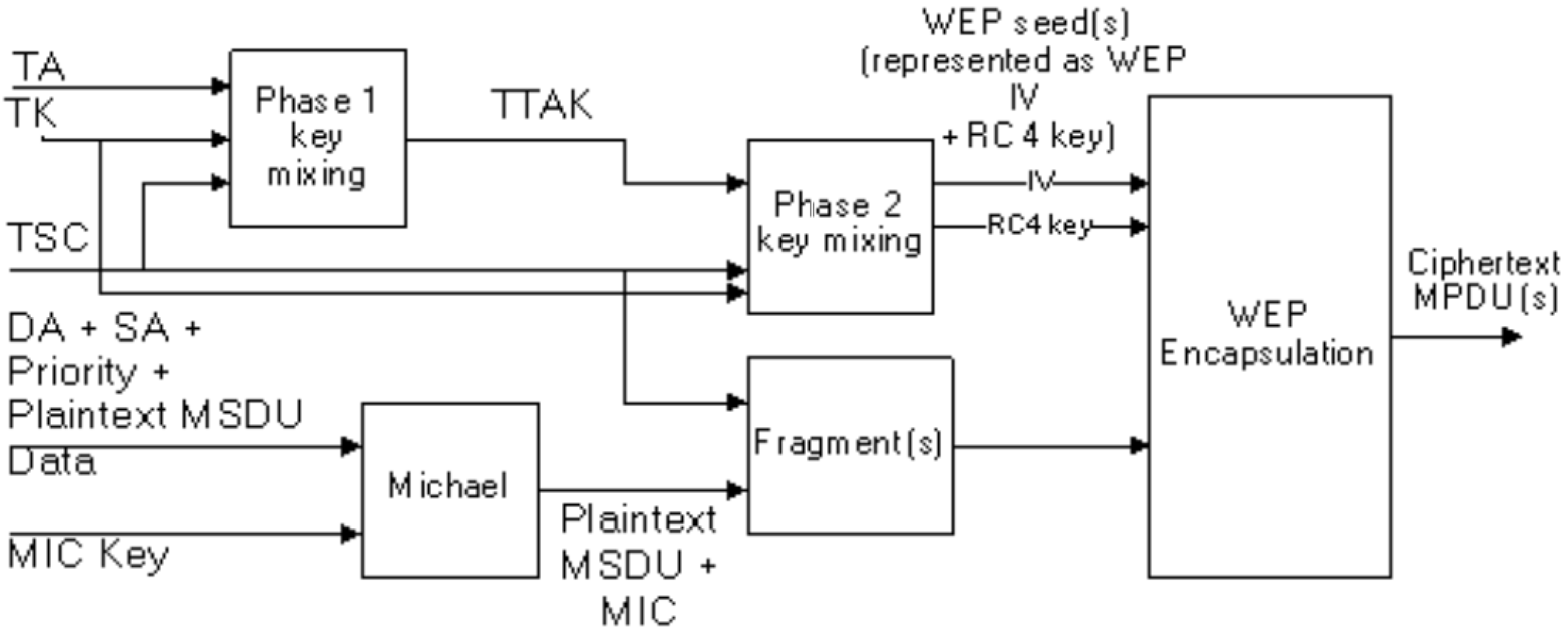
Wi-Fi Protected Access (WPA)

- IEEE developed the 802.11i standard for enhanced wireless security, to address weak data encryption and user authentication within the existing 802.11 standard.
- The WPA standard is a joint effort between Wi-Fi Alliance and IEEE:
  - *WPA is a subset of IEEE 802.11i standard.*
  - *It was designed to fill the gap between WEP and a longer term final 802.11i.*
- WPA provides stronger data encryption (weak in WEP) and user authentication (largely missing in WEP).
- WPA ≈ 802.1X + TKIP (RC4)

TKIP

- WPA uses *Temporal Key Integrity Protocol (TKIP)* to provide stronger data encryption and address known vulnerabilities in WEP
  - *Quick fix to overcome the problem with WEP.*
  - *Use 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.

How does it work?



DA – Destination Address   TKIP – Temporal Key Integrity Protocol   SA – Source Address

ICV– Integrity Check Value   TSC – TKIP Sequence Counter   TA – Transmitter Address

MPDU – Message Protocol Data Unit   TK – Temporal Key

TTAK– Result of phase 1 key mixing of Temporal Key and Transmitter Address

MSDU – MAC Service Data Unit   RSN – Robust Security Network

WEP – Wired Equivalent Privacy   IV – Initialisation Vector

Data Encryption

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

User Authentication

- Authentication and Key Management are based on IEEE 802.1X.
- WPA supports two authenticated key management protocols.
  - *802.1X and EAP authentication*
    - Enterprise environments through centralized authentication server.
    - Mutual authentication is required to prevent users from joining rogue networks.

User Authentication

- Pre-Shared Key (PSK) authentication
  - *Home or office environment, easily configured by home or office user.*
  - ***No** centralized authentication server.*
  - *Requires the home or office user to **manually enter the password** (Master Key) to the Access Point or Wireless Gateway and have the same password in each PC that is allowed access to that wireless network.*

WPA – Short Summary

- WPA effectively address WLAN security requirements and provides an immediate and strong encryption & authentication solution.
- WPA replaces WEP as standard Wi-Fi security mechanism.
- Wi-Fi Alliance adopted the full 802.11i standard as version 2 of WPA.