----------CH2----------

Wireless networks, it is extremely difficult to implement uniformed security.

Wireless communication is the process of communicating information in electromagnetic media.

Security is the combination of processes, procedures and systems used to ensure the confidentiality, integrity, or availability of information.

The algorithms used for authentication in 2G cellular networks are A3 and A8, both of which are based on cryptographic algorithm COMP128.

The data encryption algorithm A5/3.

Mutual authentication became required in the 3G along with improved security algorithms for both data confidentiality and integrity.

In 3G networks, data confidentiality is protected using algorithm f8 and integrity is preserved using algorithm f9, based on KASUMI cipher.

Wired Equivalent Privacy (WEP) secures the transmission between the clients and APs using:

CRC-32, RC4, Secret key

24-bit Initial Vectors (IVs) used in WEP

(TKIP) in WPA helps overcome the vulnerability found in WEP.

The security requirements of WLANs essentially fall into the following five areas:

1. Confidentiality: Confidentiality prevents the disclosure of the data or information to unauthorized
2. Authentication: Authentication provides a service that verifies and confirms the authenticity of a sender or receiver's
3. access control enables an authority to grant authorized users the corresponding access right to the resources in the WLANs.
4. integrity: Integrity assures the consistency of the data when it is transmitted in the WLANs
5. intrusion detection and prevention.

Wi-Fi Protected Access (WPA) supports:

- Pre-Shared Key (PSK)
- Remote Authentication Dial in User Service (RADIUS).

The Temporal Key Integrity Protocol (TKIP) in WPA helps overcome the vulnerability found in WEP.

WMANs

WMANs are based on the IEEE 802.16 standards WMANs are based on the IEEE 802.16 standards.

In WiMAX, Message authentication is done by using Hashed Message Authentication Code (HMAC).

authentication is based on digital certificates and Secure Socket Layer/Transport Layer Security (SSL/TLS)

Data confidentiality is implemented using:

1. RSA
2. DES-CBC
3. AES with CBC-MAC(CCM)

Data integrity is implemented using:

1. HMAC
2. CMAC

Bluetooth

Bluetooth are relatively simple and data volume is much less and therefore the security complexity is reduced.

Bluetooth applications may require secure authentication, data encryption and integrity check.

Bluetooth cannot use SSL/TLS.

Each Bluetooth version supports one or multiple (not all) security modes.

four security modes were designed and implemented.

Each Bluetooth version supports one or multiple (not all) security modes.

Bluetooth Authentication makes use of a challenge-response.

Data confidentiality is implemented by Exclusive-ORing plaintext with keystream.

WSNs

Wireless Sensor Networks (WSNs) are a type of Mobile Ad Hoc Networks

(MANETs) that consist of a large number of resource-constrained sensor nodes.

Security is one of the most important issues in WSNs mainly because WSNs are usually deployed in hostile or remote environments and work in an unattended manner.

Standard cryptographic ciphers, such as Digital Signature Algorithm (DSA) and Elliptic Curve Cryptography (ECC), can also be applied to secure WSNs

RFID

Technology consists of small, inexpensive, computational devices, with wireless communication capabilities.

will play an important role in the proposed Internet-of-Things (IoT)

The difficulty in securing RFID lies in the resource constraints of the RFID tags, which makes it impossible to adopt existing security solutions

----------CH3----------

A cellular network is a radio network with many fixed location transceivers.

1G use analogue signals.

2G use digital signals.

2G use Error-correcting codes.

The improvements of the 3G networks over the 2G:

- mutual authentication.
- Improved security algorithms.
- Different radio frequency ranges.

The temporary user equipment identity in 3G networks is named as globally unique temporary identity (GUTI).

When a mobile user tries to connect, it first sends its IMSI serving as its identity to a nearby eNodeB.

HLR which has an authentication center.

VLR, which is composed of a collection of base stations.

HLR is responsible for issuing each mobile user a unique identity (ID)

All this information is held by the authentication center in a secure database.

On the user side, the information is kept in the SIM card.

The base station collects the information from the user, sends it to a processing unit.

The HLR serves as an authentication center.

TMSI is to provide privacy protection of the IMSI to certain degree.

A3 used for authentication.

A8 used for generating a session key.

A5 used for data encryption is a stream cipher.

The A5/3 changed the philosophy of “security by obscurity”. Instead, it used an algorithm KASUMI.

home subscriber server (HSS) which has similar functionalities as an HLR.

Many mobility management entities (MME), which have similar functionalities as the VLRs.

it first sends its IMSI serving as its identity to a nearby eNodeB

TMSI has setup a secure communication channel in 2G.

GUTI has setup a secure communication channel in 3G.

f0 is a pseudorandom number generator.

f1 generate a message authentication code (MAC), input AMF, SQN, RAND

f1∗ is used for the resynchronization of message authentication.

f2 used to generate the expected response (XRES)

f3 generate CK encryption data.

f4 generate an integrity key IK ,

f5 generate an anonymity key AK.

f0 ~ f5 for authentication vectors

f6 is the process for encryption.

f7 is the inverse.

f8 is a stream cipher that encrypts.

f9 generate (MAC) for the signaling messages.

f0, f1∗, f6 and f7 most security functions take KASUMI and AES

KASUMI is a block cipher.

output feedback (OFB) mode of KASUMI to build a stream cipher from a block cipher.

KASUMI has some security problems revealed [T]

There is no security provision in the first generation of cellular communication networks[T]

----------CH4----------

(WLAN) is a flexible data communications system implemented as an extension.

WLAN consists of two main categories of components:

- Wireless-enable clients
- Access Points

The main functions of (AP) are to receive and transmit radio frequencies for the wireless clients.

802.11 for the implementations of WLANs include both **radio standards** and **networking protocol standards**.

All the components belonging to the WLAN are referred to "**Station.**"

Set of stations called basic service set "BSS".

The stations in the basic service set communicate with each other obeying the same networking protocol under the same, shared wireless medium, which may generate medium access "collisions".

Every BSS has a unique identification (ID) called BSSID.

Each ESS also has an ID called service set identifier (SSID).

Multiple BSSs connected through a "wired" or "wireless" distribution system can form an extended service set (ESS).

WLANs can be divided into two categories:

- infrastructure-based WLANs
- Ad Hoc WLANs

WLAN Attacks:

- **Deauthentication**: The attackers can steal legitimate wireless users.
    - **MAC Spoofing**: By modifying the wireless client's MAC address.
    - **IP Spoofing**: By modifying the source IP address contained in the packet header.
    - **Rogue Access Points**: Rogue access points are unauthorized access points that are deployed in the WLANs.
- **Eavesdropping and interception**
    - **Traffic Eavesdropping**: Attackers can break the confidentiality of the data by eavesdropping the whole WLAN Due to the broadcasting nature.
    - **Man-in-the-middle Attacks**: an attacker can sit in the middle of the two-way communicating parties.
    - **Network Injection:** an attacker can inject bogus network traffic into the legitimate traffic.
    - **Session Hijacking**: an attacker can steal a legitimate authenticated conversation session ID
- **Traffic jamming**
    - **Denial of Service (DoS) Attacks:** Denial of service attacks are also easily applied to wireless networks.
    - **Spam Attacks:** attackers can launch spam attacks by flooding spam.
- **Brute force attacks**
- **Attacks against security protocols**
- **Misconfiguration**

The base stations (APs) in the WLAN are usually connected through high bandwidth wired connections[T]

Ad Hoc network can offer the service to users without the constraints[T]

WLANs enable physical network portability [T]

(61%) of people consider security as the second most important WLAN characteristic after reliability[T]

----------CH5----------

The main goal of the WEP protocol is to guarantee the authentication, confidentiality, and integrity.

WEP protocol is used only to protect link level data.

WEP protect data communication security between the clients and the access points.

WEP protocol is implemented from the initial connection between the clients and the APs.

Only the receivers who own the correct decryption key.

(Confidentiality → Encryption) using **Rc4 stream cipher.**

(Integrity → Checksum) using **CRC** [PT][CRC] That mean CRC appended with plain text.

(Access control → Authentication) using **challenge response** and we have the pre-shared key used with the challenge response.

Two key sizes

- 802.11 64-bit**(24IV+40KEY)**
- 802.11b 128-bit**(24IV+104KEY)**

WEP authentication uses a simple challenge-response scheme based on whether a client/AP has the knowledge of a shared secret key.

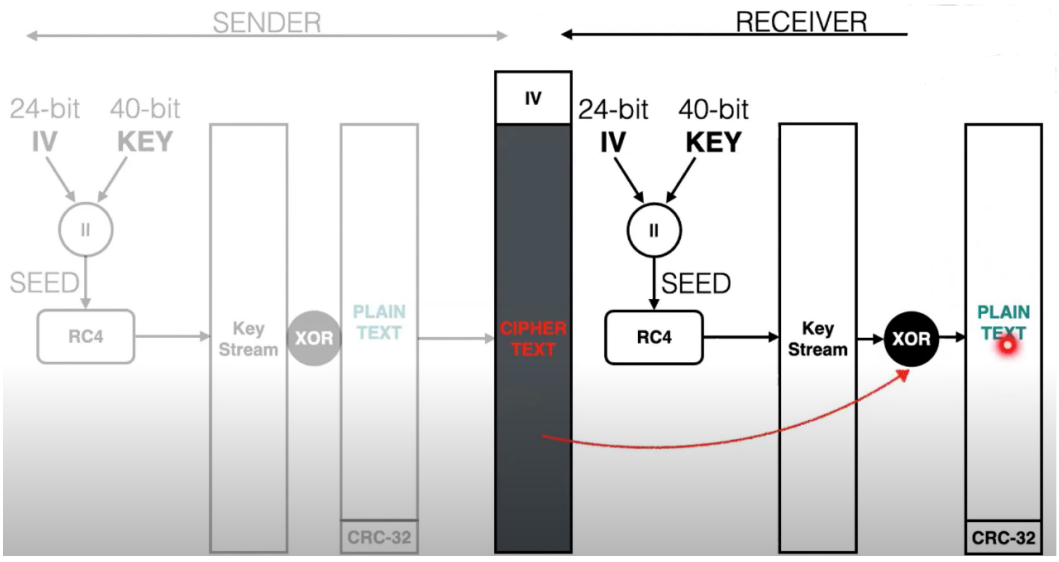
Two processes are applied to plaintext data:

- Encrypts the plaintext.
- Protects it from unauthorized modification.

The RC4 algorithm outputs a key sequence of equal in length to the plaintext input

Thus, the same plaintext may generate different cipher text at different times.

IV=Random 24 bit



Attacks on WEP:

- Brute force attack
- Key Stream Re-uses
- Weak IV attacks

Weaknesses of WEP

- IV in WEP is only 24 bits long.
- static WEP keys
- non-cryptographic cyclic redundancy check (CRC)
- No protection against replays

WEP does not provide end-to-end security [T]

----------CH6----------

In Personal mode, it utilized Pre-Shared Key (PSK) containing the network SSID.

In Enterprise mode, WPA functions as a Remote Authentication Dial in User Service RADIUS server

Use RADIUS for both authentication and key distribution.

What do you use for authenticating in WPA-Personal?
pre-shared key.

One major improvement in WPA is the TKIP which dynamically changes keys as the system is used.

WPA achieves the goal of designing a more secure wireless standard by using TKIP and MIC

In the TKIP protocol, it has two different keys:

128-bit key

64-bit key message integrity

in addition, every key in the TKIP has its own fixed lifetime.

TKIP compute MIC (Message Integrity Code) transmitted with the message.

WP2 encryption use CCMP.

48-bit Initial Vectors (IVs) used in WPA

Authentication:

- Uses PSK (Pre-Shared Key) -> WPA-Personal.
- Uses 802.1x EAP mutual authentication -> WPA-Enterprise.

Data encryption: TKIP

Data integrity: MMIC (Michael Message Integrity Check)

MIC is to prevent an attacker from

- Capturing.
- re-sending.

Changes from WEP to TKIP

- Message Integrity
- IV selection and reuse
- IV size
- Per-Packet Key Mixing
- Key Management

TKIP uses three distinct keys:

- Temporal keys
- key encryption keys
- master keys

Requires two distinct key encryption keys:

- To encrypt the distributed keying material
- To protect the re-key messages from forgery

WPA Vulnerabilities

- temporal key recovery attack
- sniffing the wireless communication channel
- dictionary attack on the keys

WPA Attacks

- dictionary attack
- DoS attack

WPA-Enterprise should only be used when a RADIUS server is connected for client authentication[T]

WPA Enterprise requires Authentication server[T]

When combined the much larger IV, this defeats the well-known key recovery attacks on WEP[T]

MIS use shift and add operations instead multiplication[T]

MIS uses a different key than encryption[T]