Course code	Course Name	L-T-P - Credits	Year of Introduction
CS472	PRINCIPLES OF INFORMATION SECURITY	3-0-0-3	2016
Module	**Contents**	**Hours**	**End Sem. Exam Marks**
V	Security in current domains: Wireless LAN security – WEP details. Wireless LAN vulnerabilities – framespoofing. Cell phone security - GSM and UMTS security. Mobile malware - Bluetooth security issues.	8	20%

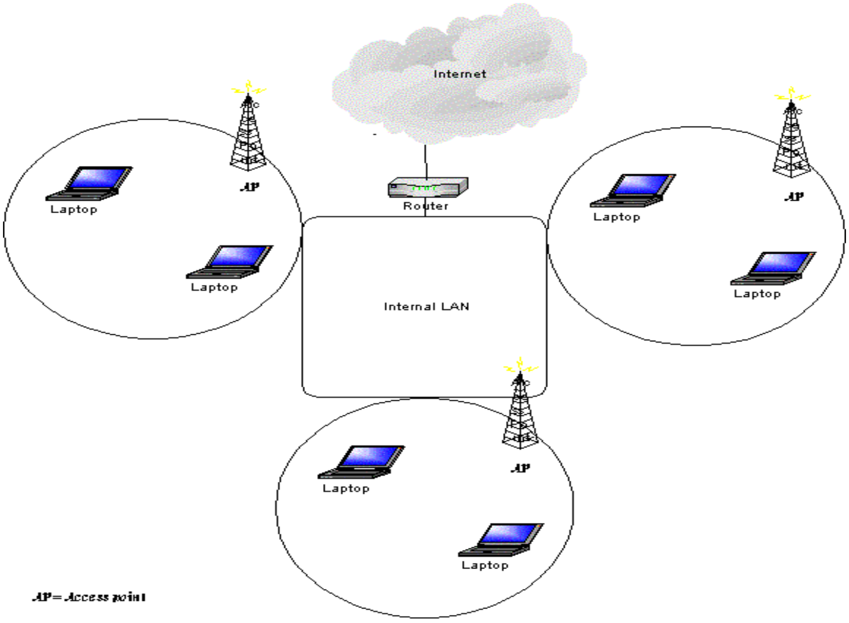
Wireless LANs:

- IEEE ratified 802.11 in 1997.
    - Also known as Wi-Fi.
- 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
- A local area network (LAN) with no wires
- Several Wireless LAN (WLAN) standards

802.11	- 1-2 Mbps speed, 2.4Ghz band
802.11b (Wi-Fi)	– 11 Mbps speed, 2.4Ghz band
802.11a (Wi-Fi)	- 54 Mbps speed, 5Ghz band
802.11g (Wi-Fi)	– 54 Mbps speed, 2.4Ghz band

802.11 Components

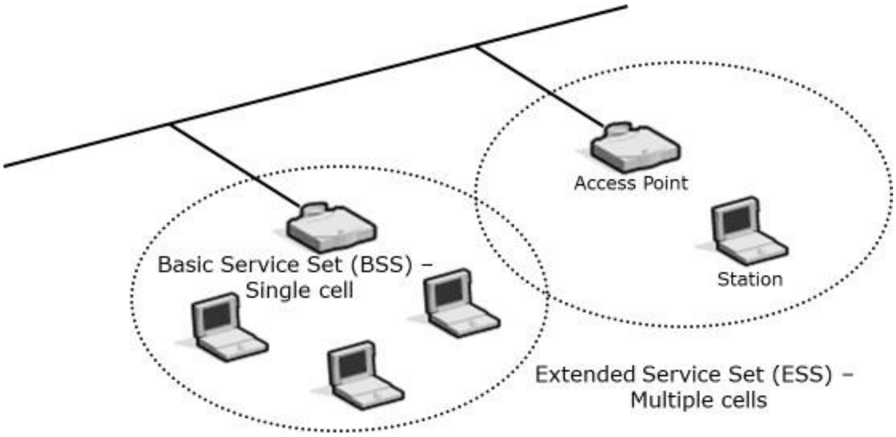
- Two pieces of equipment defined:
    - Wireless station
        - A desktop or laptop PC or PDA with a wireless NIC.
    - Access point
        - A bridge between wireless and wired networks
        - Composed of
            - Radio
            - Wired network interface (usually 802.3)
           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



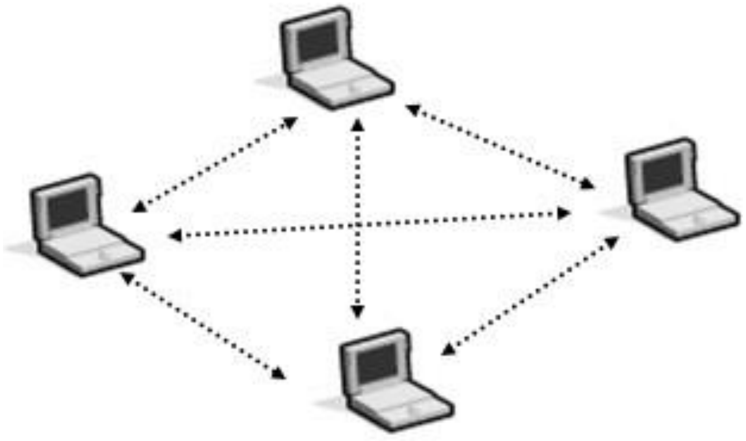
802.11 modes

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

Infrastructure mode


Access Point
Station
Basic Service Set (BSS) – Single cell
Extended Service Set (ESS) – Multiple cells

Ad-hoc mode



Independent Basic Service Set (IBSS)

802.11 Physical Layer

- Originally three alternative physical layers
  - Two incompatible spread-spectrum radio in 2.4Ghz ISM band
    - Frequency Hopping Spread Spectrum (FHSS)
      - 75 channels
    - Direct Sequence Spread Spectrum (DSSS)
      - 14 channels (11 channels in US)
  - One diffuse infrared layer
- 802.11 speed
  - 1 Mbps or 2 Mbps.

802.11 Data Link Layer

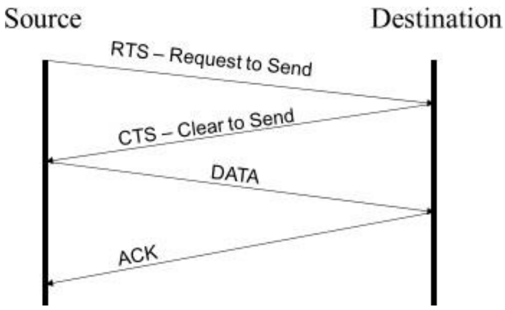
- Layer 2 split into:
  - Logical Link Control (LLC).
  - Media Access Control (MAC).
- LLC - same 48-bit addresses as 802.3.
- MAC - CSMA/CD not possible.
  - Can't listen for collision while transmitting.
- CSMA/CA – Collision Avoidance.
  - Sender waits for clear air, waits random time, then sends data.
  - Receiver sends explicit ACK when data arrives intact.
  - Also handles interference.
  - But adds overhead.
- 802.11 always slower than equivalent 802.3.

RTS / CTS

- To handle hidden nodes

- Sending station sends
    - “Request to Send”
- Access point responds with
    - “Clear to Send”
    - All other stations hear this and delay any transmissions.
- Only used for larger pieces of data.
    - When retransmission may waste significant time.

Four-Way Handshake



802.11b

- 802.11b ratified in 1999 adding 5.5 Mbps and 11 Mbps.
- DSSS as physical layer.
    - 11 channels (3 non-overlapping)
- Dynamic rate shifting.
    - Transparent to higher layers
    - Ideally 11 Mbps.
    - Shifts down through 5.5 Mbps, 2 Mbps to 1 Mbps.
        - Higher ranges.
        - Interference.
    - Shifts back up when possible.
- Maximum specified range 100 metres
- Average throughput of 4Mbps

Joining a BSS

- When 802.11 client enters range of one or more APs
    - APs send beacons.
    - AP beacon can include SSID.
    - AP chosen on signal strength and observed error rates.
    - After AP accepts client.
        - Client tunes to AP channel.
- Periodically, all channels surveyed.
    - To check for stronger or more reliable APs.
    - If found, reassociates with new AP.

Roaming and Channels

- Reassociation with APs
    - Moving out of range.
    - High error rates.
    - High network traffic.
        - Allows load balancing.
- Each AP has a channel.
    - 14 partially overlapping channels.
    - Only three channels that have no overlap.
        - Best for multicell coverage.

802.11a

- 802.11a ratified in 2001
- Supports up to 54Mbps in 5 Ghz range.
    - Higher frequency limits the range
    - Regulated frequency reduces interference from other devices
- 12 non-overlapping channels
- Usable range of 30 metres
- Average throughput of 30 Mbps
- Not backwards compatible

802.11g

- 802.11g ratified in 2002
- Supports up to 54Mbps in 2.4Ghz range.
    - Backwards compatible with 802.11b
- 3 non-overlapping channels
- Range similar to 802.11b
- Average throughput of 30 Mbps
- 802.11n due for November 2006
    - Aiming for maximum 200Mbps with average 100Mbps

Security Issues and Solutions

- Sniffing and War Driving
- Rogue Networks
- Policy Management
- MAC Address
- SSID
- WEP
- Wired network limitations: physical, hard-wired infrastructure
- Wireless LAN provides
    - Flexibility
    - Portability
    - Mobility
    - Ease of Installation

Types of Wireless Topologies

- ❑ Independent Basic Service Set(IBSS)
- ❑ Basic Service Set(BSS)
- ❑ Extended Service Set(ESS)

WLAN Vulnerability

- ❑ Lack of Physical Security
- ❑ Invasion & Resource Stealing
- ❑ Traffic Redirection
- ❑ Denial of Service
- ❑ Rogue Access Point
- ❑ There are currently three main encryption technologies available to WLAN communication; WEP, WPA, and WPA2. These technologies attempt to provide Confidentiality, Integrity and Authentication. However, they do not all succeed at these tasks and introduce vulnerabilities into the WLANs.

- ❑ The first protection method and the easiest to use on wireless networks is Wired Equivalent Privacy (WEP). Although it appeared a successful invention, it could not survive for long and after only a period of two years, its RC4 was broken and this gave a bad reputation to wireless technology because of its perceived security flaw. The perceived flaws in the WEP saw the introduction of Wi-Fi Protected Access which is practically more efficient compared to WEP because it is much more complicated algorithm. As time went by, an improvement of WPA was made and that saw the introduction of WPA2.

Attacks on WLAN

- ❑ Passive Attack (Not harmful to the N/w)
- ❑ Active Attack (harmful to the N/w)
- ❑ Insider Attack (Malicious to N/W)
- ❑ Close-in Attack (Malicious Attack)
- ❑ Phishing Attack (User Information)
- ❑ Hijack Attack (User Information)
- ❑ Spoof Attack (Sensitive Information)
- ❑ Password Attack (to know password)

802.11 security features

- > Challenges
  - ➢ Beyond any physical boundaries
  - ➢ Encryption, Authentication and Integrity
- > Basic Security Mechanisms in 802.11
  - ➢ Service Set ID (SSID) – Acts like a shared secret, but sent in clear.

    - MAC Address Lists – Modifiable and also sent in clear.
    - Protocols (WEP,WPA,WPA2)

How to secure WLAN?

- ❑ WEP
- ❑ WPA
- ❑ WPA2

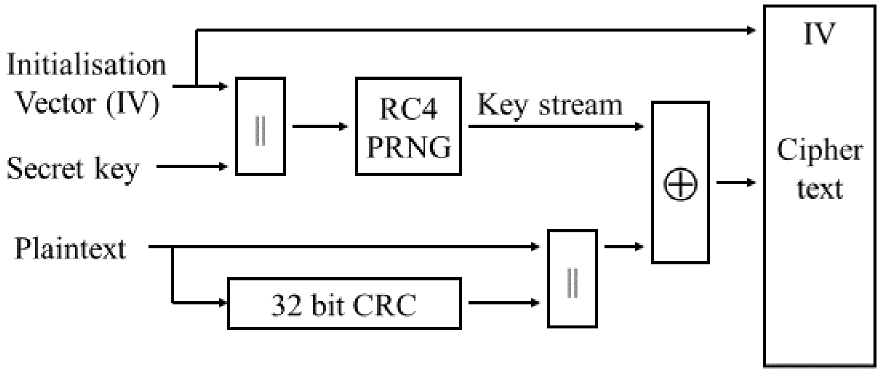
WEP

- Stands for Wired Equivalent Privacy
- Designed to encrypt data over radio waves
- Provides 3 critical pieces of security
    - Confidentiality (Encryption)
    - Authentication
    - Integrity
- Uses RC4 encryption algorithm
    - Symmetric key stream cipher
    - 64-bit shared RC4 keys, 40-bit WEP key, 24-bit plaintext Initialization Vector (IV)
- Shared key between
    - Stations.
    - An Access Point.
- Extended Service Set
    - All Access Points will have same shared key.
- No key management
    - Shared key entered manually into
        - Stations
        - Access points
        - Key management nightmare in large wireless LANs

WEP – Sending

- Compute Integrity Check Vector (ICV).
    - Provides integrity
    - 32 bit Cyclic Redundancy Check.
    - Appended to message to create plaintext.
- 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
        - 24 bit initialisation vector
- Ciphertext is transmitted.

WEP Encryption



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
        - > 24 bit initialisation vector (IV)
- > Check ICV
    - > Separate ICV from message.
    - > Compute ICV for message
    - > Compare with received ICV

Shared Key Authentication

- > When station requests association with Access Point
    - > AP sends random number to station
    - > Station encrypts random number
        - > Uses RC4, 40 bit shared secret key & 24 bit IV
    - > Encrypted random number sent to AP
    - > AP decrypts received message
        - > Uses RC4, 40 bit shared secret key & 24 bit IV
    - > AP compares decrypted random number to transmitted random number
- > If numbers match, station has shared secret key.

WEP Safeguards

- > Shared secret key required for:
    - > Associating with an access point.
    - > Sending data.
    - > Receiving data.
- > Messages are encrypted.
    - > Confidentiality.
- > Messages have checksum.
    - > Integrity.

- But management traffic still broadcast in clear containing SSID.

Initialisation Vector

- IV must be different for every message transmitted.
- 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.

Passive WEP attack

- If 24 bit IV is an ascending counter,
- If Access Point transmits at 11 Mbps,
- All IVs are exhausted in roughly 5 hours.
- Passive attack:
    - Attacker collects all traffic
    - Attacker could collect two messages:
    - Encrypted with same key and same IV
    - Statistical attacks to reveal plaintext
    - Plaintext XOR Ciphertext = Keystream

Active WEP attack

- If attacker knows plaintext and ciphertext pair
    - Keystream is known.
    - Attacker can create correctly encrypted messages.
    - Access Point is deceived into accepting messages.
- Bitflipping
    - Flip a bit in ciphertext
    - Bit difference in CRC-32 can be computed

Limited WEP keys

- Some vendors allow limited WEP keys
    - User types in a passphrase
    - WEP key is generated from passphrase
    - Passphrases creates only 21 bits of entropy in 40 bit key.
        - Reduces key strength to 21 bits = 2,097,152
        - Remaining 19 bits are predictable.
        - 21 bit key can be brute forced in minutes.

Brute force key attack

- Capture ciphertext.
    - IV is included in message.
- Search all 2^{40} possible secret keys.
    - 1,099,511,627,776 keys
    - ~170 days on a modern laptop
- Find which key decrypts ciphertext to plaintext.

Key Scheduling Weakness

- Two weaknesses:
    - Certain keys leak into key stream.
        - Invariance weakness.
    - If portion of PRNG input is exposed,
        - Analysis of initial key stream allows key to be determined.

IV weakness

- WEP exposes part of PRNG input.
    - IV is transmitted with message.
    - wireless frame has reliable 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
        - First byte ciphertext XOR 0xAA = First byte key stream
        - Can determine key from initial key stream
- Practical for 40 bit and 104 bit keys
- Passive attack.
    - Non-intrusive.
    - No warning.

WPA/WPA2 - Wi-Fi Protected Access

- The design of WPA is based on a Draft 3 of IEEE 802.11i standard. It was proposed to ensure the release of a higher volume of security WLAN products before IEEE group could officially introduce 802.11i.

- Due to those weaknesses, WPA introduced some improvements. First, WPA can be used with an IEEE 802.1x authentication server, where each user is given different keys and it can also be used in a less secure "pre-shared key" (PSK) mode, where every client is given the same pass-phrase just like with WEP.

- In 2004, WPA2 standard was released to replace the less secure WEP and WPA. The final IEEE 802.11i standard not only adapts all the improvements included in WPA, but also introduces a new AES-based algorithm considered as fully secure.

- WPA includes two types of user authentication. One named WPA Personal with a pre-shared key mechanism similar to that of WEP and the WPA Enterprise, which uses 802.1X and derives its keys automatically.

- Nonetheless, the main improvement of the WPA was introduction of Temporal Key Integrity Protocol (TKIP) Instead of using a preshared key, which creates a key stream.
- It uses a pre-shared key to serve as the seed for generating the encryption keys. WPA also uses the RC4 stream cipher with a 128-bit key and a 48bit IV, which is similar to the WEP for data encryption. However, unlike the WEP, there is a major improvement for WPA to use the Temporal Key Integrity Protocol (TKIP), which is the heart of WPA.
- With a similar encryption process to WEP, implementation of the WPA is as simple as upgrading clients' software and updating the firmware of older access points.
- Like WPA, WPA2 offers two security modes: pre-shared key authentication based on a shared secret and authentication by an authentication server. Pre-shared key authentication is intended for personal and small office use where an authentication server is unavailable.

Wireless LAN Vulnerabilities

- Controlling access to be shared medium of a local area network is important enough to be handled by a separate layer called Medium Access Control Layer or MAC
- In the networks such as Ethernet and 802.11 LANs, there are well defined rules governing when a node should talk, how nodes handle collisions, etc.
- The smooth functioning of these networks depends on the stations on the LAN strictly obeying the rules.
- On wireless LANs, in particular, there is much scope for misbehaving the nodes to launch a variety of attacks.
- These include hogging network bandwidth by abusing features of the MAC protocol and disrupting communication between legitimate users by transmitting spoofed management and control frames.

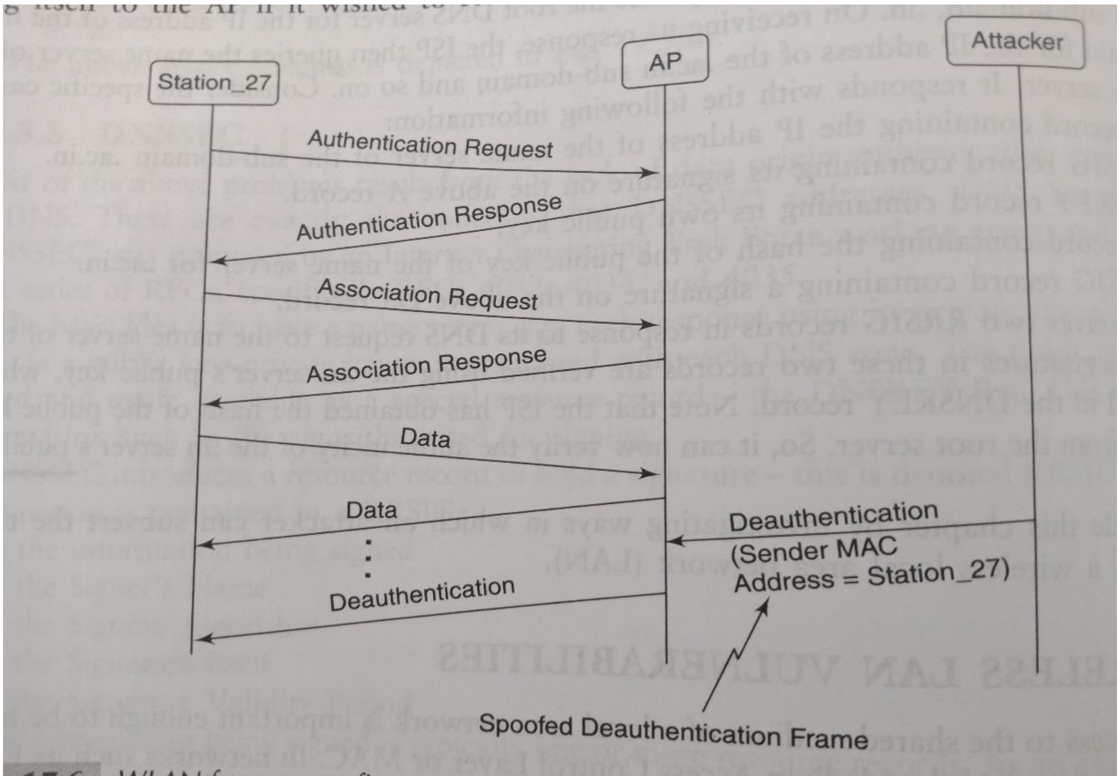
Frame Spoofing

Premature Termination of connections

- A number of management frames used in 802.11 wireless LANs such as the Beacon, Association and Authentication frames.
- A station needs to authenticate and then associate with an Access Point (AP) before they can exchange data frames with each other.
- Each party can, at any point in time, terminate the connection by transmitting a Deauthentication frames.
- The recipient of a management frame relies on the sender address field in the frame to identify the originator of the message.

- However, an attacker can spoof the sender address in the frame. For example, he can fabricate a deauthentication frame with

  Sender Address = Sataion_27
  Receiver Address = AP
- The address used are 48-bit MAC address. When the AP receives the above frame, it thinks that Station_27 wishes to terminate the existing connection to itself. The AP sets the state of the connection between itself and Station_27 to be "Unauthenticated and Unassociated"
- Station_27 would have to go through the time-consuming process of re-associating itself to the AP if it wished to resume the communication. The attacker could repeatedly transmit such Deauthentication frames to the AP thus effectively slowing down or even preventing communication between Station_27 and AP.



e 17.6 *WLAN frame spoofing*

Spoofing Power Management Control Frames

- A mobile station typically works on batteries. To save power, a mobile station powers off its transceivers.
- It informs the AP that it is in power saving modes so that the AP can buffer all frames intended for it.
- When the station wakes up, it informs the AP that it is now in the active state using a Poll Control Frame.

- On receipt of the Poll Control Frame, the AP delivers the station any frames that it had buffered for it while the station was in power saving mode.
- An attacker could spoof Poll Control Frames and make it appear that they were sent by a sleeping station that has just woken up.
- The AP, on receiving the spoofed poll control frame , would deliver any buffered frames to the sleeping station. But, since the receiver of the sleeping station is powered off, the frames would not be captured by the sleeping station.
- When sleeping station actually wakes up, it may send Poll Control frame to retrieve frames buffered for it while it was asleep.
- However, since all the frames buffered for it have already been transmitted by the AP, it will not receive the frames destined for it while it was asleep.

Cellphone security - GSM and UMTS security

Global System for Mobile communications (GSM) and
Universal Mobile Telecommunications System (UMTS) Security

Second Generation Mobile Phones – The GSM Standard

- Second generation mobile phones are characterised by the fact that data transmission over the radio link uses **digital** techniques
- Development of the GSM (Global System for Mobile communications) standard began in 1982 as an initiative of the European Conference of Postal and Telecommunications Administrations (CEPT)
- In 1989 GSM became a technical committee of the European Telecommunications Standards Institute (ETSI)
- GSM is the most successful mobile phone standard
  - 1.05 billion customers
  - 73% of the world market
  - over 200 countries

General Packet Radio Service (GPRS)

- The original GSM system was based on circuit-switched transmission and switching
  - voice services over circuit-switched bearers
  - text messaging
  - circuit-switched data services
    - charges usually based on duration of connection
- GPRS is the packet-switched extension to GSM
  - sometimes referred to as 2.5G
  - packet-switched data services

        - suited to bursty traffic
        - charges usually based on data volume or content-based
- Typical data services
    - browsing, messaging, download, corporate LAN access

GSM Security — The Goals

- GSM was intended to be no more vulnerable to cloning or eavesdropping than a fixed phone
    - it's a phone not a "secure communications device"!
- GSM uses integrated cryptographic mechanisms to achieve these goals
    - just about the first mass market equipment to do this
    - previously cryptography had been the domain of the military, security agencies, and businesses worried about industrial espionage, and then banks (but not in mass market equipment)

GSM Security Features

- Authentication
    - network operator can verify the identity of the subscriber making it infeasible to clone someone else's mobile phone
- Confidentiality
    - protects voice, data and sensitive signalling information (e.g. dialled digits) against eavesdropping on the radio path
- Anonymity
    - protects against someone tracking the location of the user or identifying calls made to or from the user by eavesdropping on the radio path

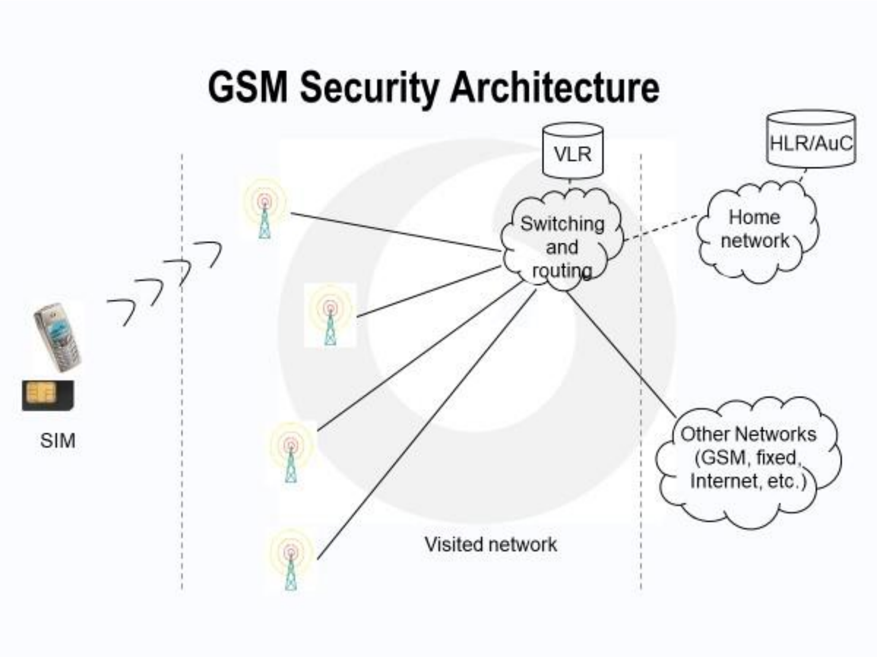
GSM Security Mechanisms

- Authentication
    - challenge-response authentication protocol
    - encryption of the radio channel
- Confidentiality
    - encryption of the radio channel
- Anonymity
    - use of temporary identities

GSM Security Architecture

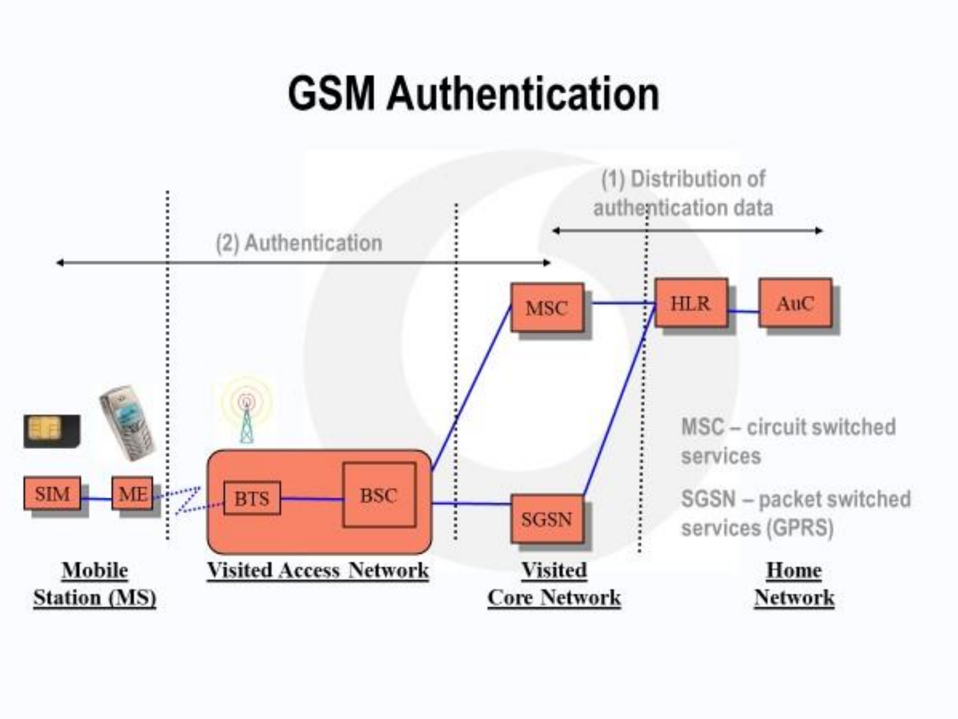
- Each mobile subscriber is issued with a unique 128-bit secret key (Ki)
- This is stored on a **Subscriber Identity Module (SIM)** which must be inserted into the mobile phone

- Each subscriber’s Ki is also stored in an **Authentication Centre (AuC)** associated with the HLR in the home network
- The SIM is a tamper resistant smart card designed to make it infeasible to extract the customer’s Ki
- GSM security relies on the secrecy of Ki
    - if the Ki could be extracted then the subscription could be cloned and the subscriber’s calls could be eavesdropped
    - even the customer should not be able to obtain Ki


GSM Security Architecture
VLR
HLR/AuC
Switching and routing
Home network
SIM
Other Networks (GSM, fixed, Internet, etc.)
Visited network

GSM Authentication Principles

- Network authenticates the SIM to protect against cloning
- Challenge-response protocol
    - SIM demonstrates knowledge of Ki
    - infeasible for an intruder to obtain information about Ki which could be used to clone the SIM
- Encryption key agreement
    - a key (Kc) for radio interface encryption is derived as part of the protocol
- Authentication can be performed at call establishment allowing a new Kc to be used for each call



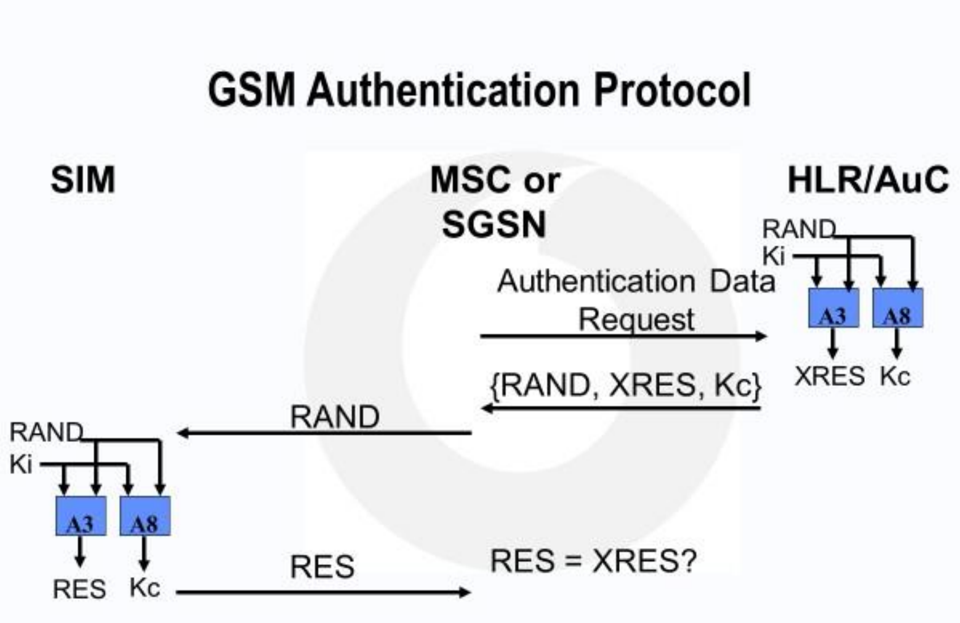
GSM Authentication

(1) Distribution of authentication data

(2) Authentication

MSC – circuit switched services

SGSN – packet switched services (GPRS)



GSM Authentication Protocol

GSM Authentication Parameters

Ki	= Subscriber authentication key (128 bit)
RAND	= Authentication challenge (128 bit)
(X)RES	= $A3_{Ki}$ (RAND)
	= (Expected) authentication response (32 bit)
Kc	= $A8_{Ki}$ (RAND)
	= Cipher key (64 bit)

Authentication triplet = {RAND, XRES, Kc} (224 bit) Typically sent in batches to MSC or SGSN

GSM Authentication Algorithm

- Composed of two algorithms which are often combined
  - A3 for user authentication
  - A8 for encryption key (Kc) generation
- Located in the customer's SIM and in the home network's AuC
- Standardisation of A3/A8 not required and each operator can choose their own

GSM Encryption

- Different mechanisms for GSM (circuit-switched services) and GPRS (packet-switched services)

Limitations of GSM Security

- Security problems in GSM stem by and large from design limitations on what is protected
  - design only provides *access security* - communications and signalling in the fixed network portion aren't protected
  - design does not address *active attacks*, whereby network elements may be impersonated
  - design goal was only ever to be *as secure as the fixed networks* to which GSM systems connect
- Failure to acknowledge limitations
  - the terminal is an unsecured environment - so trust in the terminal identity is misplaced
  - disabling encryption does not just remove confidentiality protection – it also increases risk of radio channel hijack
  - standards don't address everything - operators must themselves secure the systems that are used to manage subscriber authentication key
- Lawful interception only considered as an afterthought

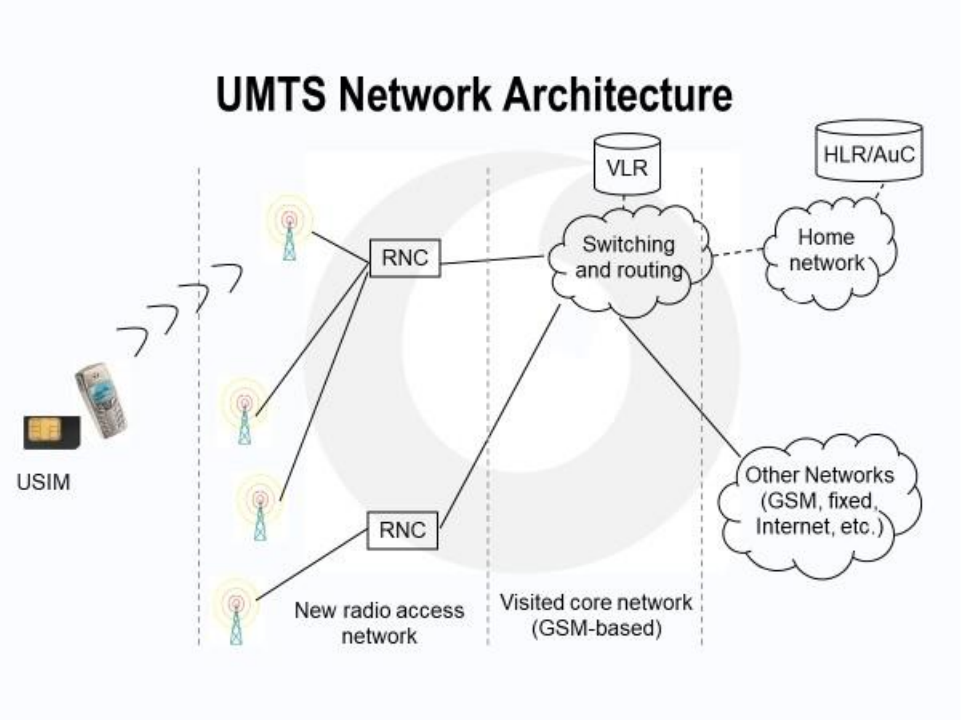
Third Generation Mobile Phones – The UMTS Standard

- Third generation (3G) mobile phones are characterised by higher rates of data transmission and a richer range of services
- Universal Mobile Telecommunications System (UMTS) is one of the new 3G systems
- The UMTS standards work started in ETSI but was transferred to a partnership of regional standards bodies known as 3GPP in 1998
  - the GSM standards were also moved to 3GPP at a later date
- UMTS introduces a new radio technology into the access network
  - Wideband Code Division Multiple Access (W-CDMA)

- An important characteristic of UMTS is that the new radio access network is connected to an evolution of the GSM core network

Principles of UMTS Security

- Build on the security of GSM
  - adopt the security features from GSM that have proved to be needed and that are robust
  - try to ensure compatibility with GSM to ease inter-working and handover
- Correct the problems with GSM by addressing security weaknesses
- Add new security features
  - to secure new services offered by UMTS
  - to address changes in network architecture


UMTS Network Architecture
VLR
HLR/AuC
RNC
Switching and routing
Home network
USIM
Other Networks (GSM, fixed, Internet, etc.)
RNC
New radio access network
Visited core network (GSM-based)

GSM Security Features to Retain and Enhance in UMTS

- Authentication of the user to the network
- Encryption of user traffic and signalling data over the radio link
  - new algorithm – open design and publication
  - encryption terminates at the radio network controller (RNC)
    - further back in network compared with GSM
  - longer key length (128-bit)
- User identity confidentiality over the radio access link
  - same mechanism as GSM

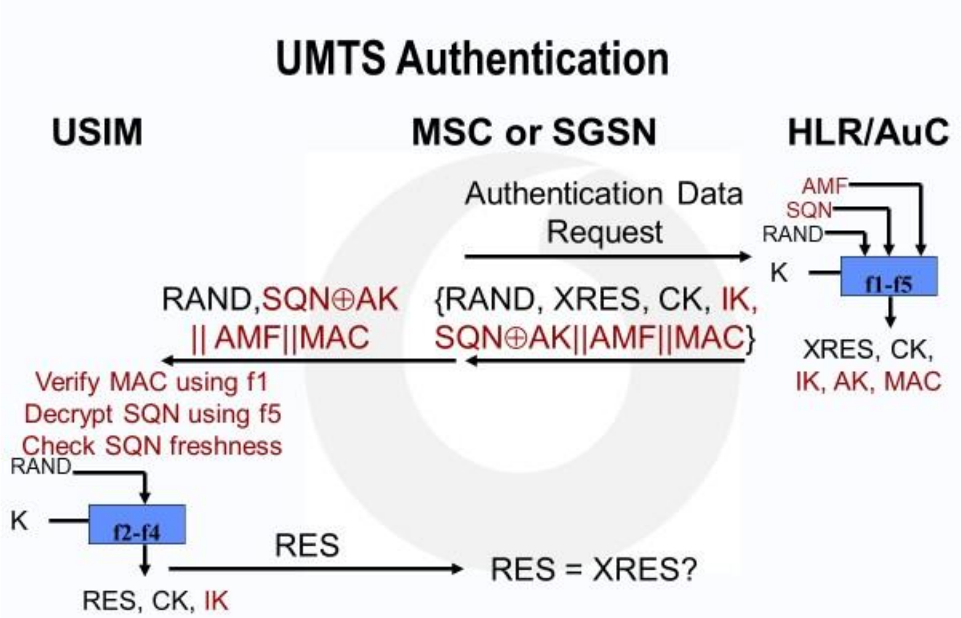
New Security Features for UMTS

- Mutual authentication and key agreement

    - extension of user authentication mechanism
    - provides enhanced protection against false base station attacks by allowing the mobile to authenticate the network
- Integrity protection of critical signalling between mobile and radio network controller
    - provides enhanced protection against false base station attacks by allowing the mobile to check the authenticity of certain signalling messages
    - extends the influence of user authentication when encryption is not applied by allowing the network to check the authenticity of certain signalling messages

UMTS Authentication : Protocol Objectives

- Provides authentication of user (USIM) to network and network to user
- Establishes a cipher key and integrity key
- Assures user that cipher/integrity keys were not used before
- Inter-system roaming and handover
    - compatible with GSM: similar protocol
    - compatible with other 3G systems due to the fact that the other main 3G standards body (3GPP2) has adopted the same authentication protocol



UMTS Authentication Parameters

K = Subscriber authentication key (128 bit)

RAND = User authentication challenge (128 bit)

SQN = Sequence number (48 bit)
AMF = Authentication management field (16 bit)
MAC = $f1_K$ (SQN||RAND||AMF) = Message Authentication Code (64 bit)
(X)RES = $f2_K$ (RAND)
= (Expected) user response (32-128 bit)
CK = $f3_K$ (RAND) = Cipher key (128 bit)
IK = $f4_K$ (RAND) = Integrity key (128 bit)
AK = $f5_K$ (RAND) = Anonymity key (48 bit)
AUTN = SQN⊕AK|| AMF||MAC = Authentication Token (128 bit)
Authentication quintet = {RAND, XRES, CK, IK, AUTN} (544-640 bit)

UMTS Mutual Authentication Algorithm

- Located in the customer's USIM and in the home network's AuC
- Standardisation not required and each operator can choose their own
- An example algorithm, called MILENAGE, has been made available
    - open design and evaluation by ETSI's algorithm design group, SAGE
    - open publication of specifications and evaluation reports
    - based on Rijndael which was later selected as the AES

UMTS Encryption Principles

- Data on the radio path is encrypted between the Mobile Equipment (ME) and the Radio Network Controller (RNC)
    - protects user traffic and sensitive signalling data against eavesdropping
    - extends the influence of authentication to the entire duration of the call
- Uses the 128-bit encryption key (CK) derived during authentication

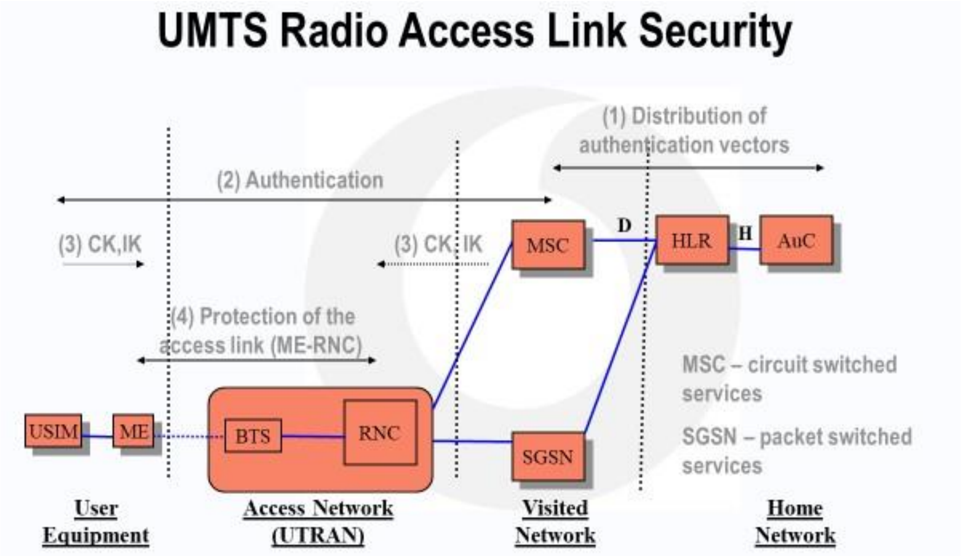
UMTS Encryption Mechanism

- Encryption applied at MAC or RLC layer of the UMTS radio protocol stack depending on the transmission mode
    - MAC = Medium Access Control
    - RLC = Radio Link Control
- Stream cipher used, UMTS Encryption Algorithm (UEA)
- UEA generates the keystream as a function of the cipher key, the bearer identity, the direction of the transmission and the 'frame number' - so the cipher is re-synchronised to every MAC/RLC frame
- The frame number is very large so keystream repeat is not an issue

UMTS Encryption Algorithm

- One standardised algorithm: UEA1
    - located in the customer's phone (not the USIM) and in every radio network controller

- standardised so that mobiles and radio network controllers can interoperate globally
- based on a mode of operation of a block cipher called KASUMI


UMTS Radio Access Link Security
(1) Distribution of authentication vectors
(2) Authentication
(3) CK,IK
(3) CK, IK
(4) Protection of the access link (ME-RNC)
MSC
D
HLR
H
AuC
USIM
ME
BTS
RNC
SGSN
MSC – circuit switched services
SGSN – packet switched services
User Equipment
Access Network (UTRAN)
Visited Network
Home Network

Mobile malware - bluetooth security issues

- Bluetooth is a wireless radio specification, design to replace cable as the medium for data and voice signal between electronics device.
- Bluetooth design on small size, low power consumption and low cost.
- Mostly it uses in Laptop computers, cellular phones, PDA's, Headset, keyboards, as well as in digital camera and other consumer electronics devices.
- Uses the radio range of 2.45 GHz
- Theoretical maximum bandwidth is 1 Mb/s
- Several Bluetooth devices can form an ad hoc network called a "piconet"
  - ✓ In a piconet one device acts as a master (sets frequency hopping behavior) and the others as slaves.
  - ✓ Example: A conference room with many laptops wishing to communicate with each other.
- Range < 10m.
- Piconets: 1 master and up to 7 slaves.
- The original architect of Bluetooth, named after the 10th century "Danish King" HARALD BLUETOOTH.
- The original Architect was the Ericsson Mobile Communication.

- In 1998, IBM, Intel, Nokia and Toshiba formed the Bluetooth

SIG (Special Interest Group).

- Standardize within the IEEE 802.15 Personal Area Network (PAN) Working Group.

Bluetooth Security

- ***Authentication:*** Verifies the identification of the devices that are communicating in the channel.
- ***Confidentiality:*** Protecting the data from the attacker by allowing only authorized users to access the data.
- ***Authorization:*** Only authorized users have control over the resources.

Security Mode of Bluetooth

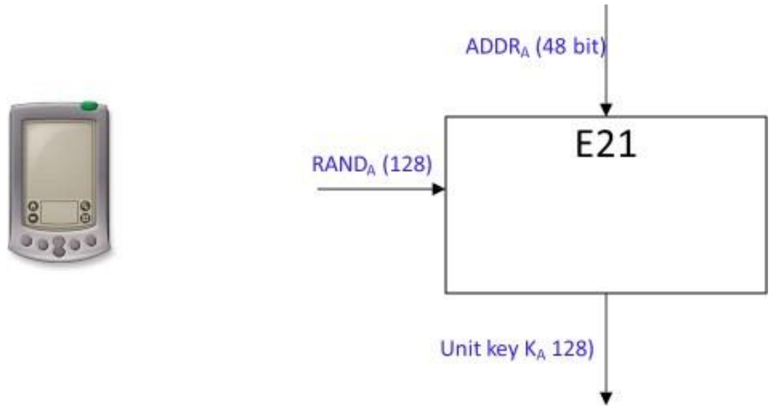
- ***Security Mode 1:*** No-Secure Mode, (There won't be any authentication or encryption in this mode. Bluetooth device can easily be connected with the other devices).
- ***Security Mode 2:*** Service level security mode, (The management of the access control and interfaces with other protocols and device users is handled by the centralized security manager, it includes Authentication, Configuration and Authorization).
- ***Security Mode 3:*** Link-level security mode, (This is a built in security mechanism that offers the authentication (unidirectional or mutual) and encryption based on the secret key shared by the pair of devices).

Protocols in Bluetooth

1. Generation of unit key.
2. Generation of initialization key.
3. Generation Combination Key.
4. Authentication.
5. Generation of encryption key.
6. Generation of key stream.
7. Encryption of data.

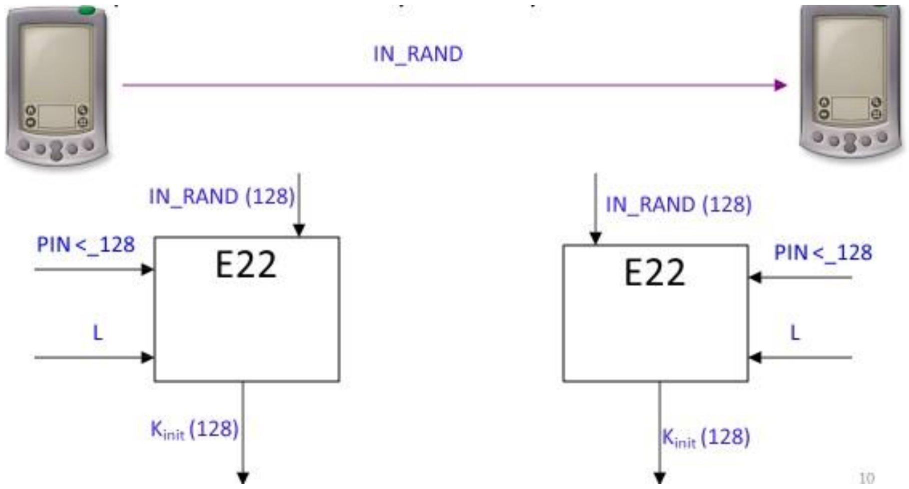
1. Generation unit key

- ✓ It is a Semi permanent Key.
- ✓ Bluetooth Device Operated for the First time.
- ✓ $ADDR_A$ (48 bit)



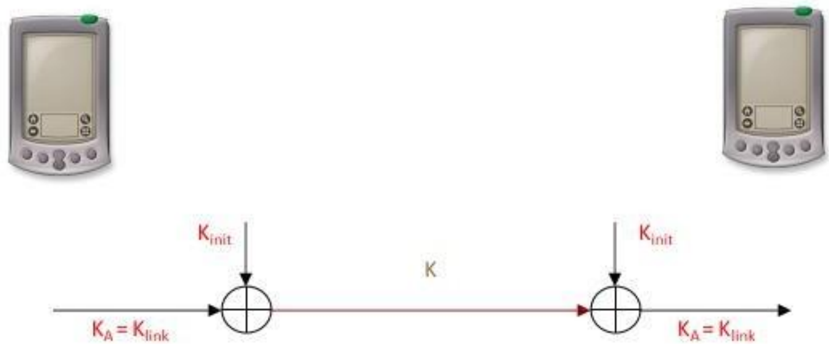
2. Generation initialization key

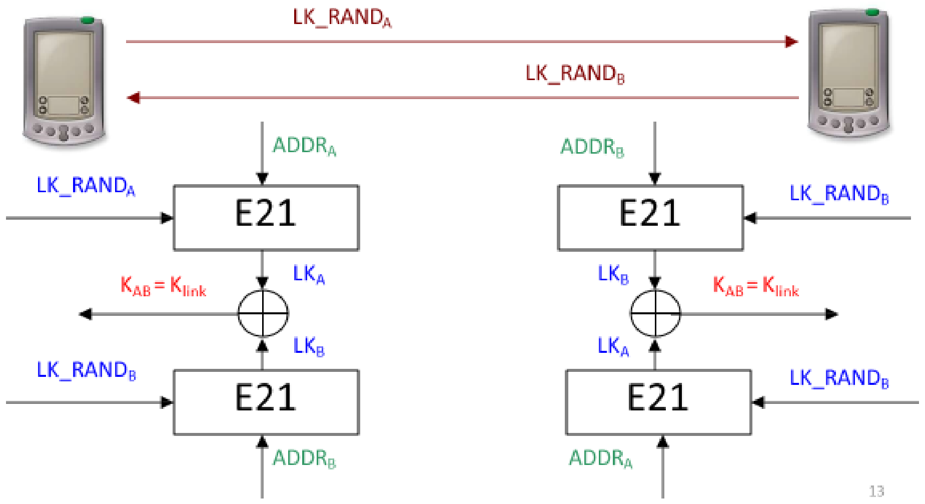
- ✓ it's a temporarily Key.
- ✓ Communication between two Device (P'=PIN + BD_ADDR).
- ✓ XOR Operation. Here Unit key = Link key.



3. Generation Combination Key

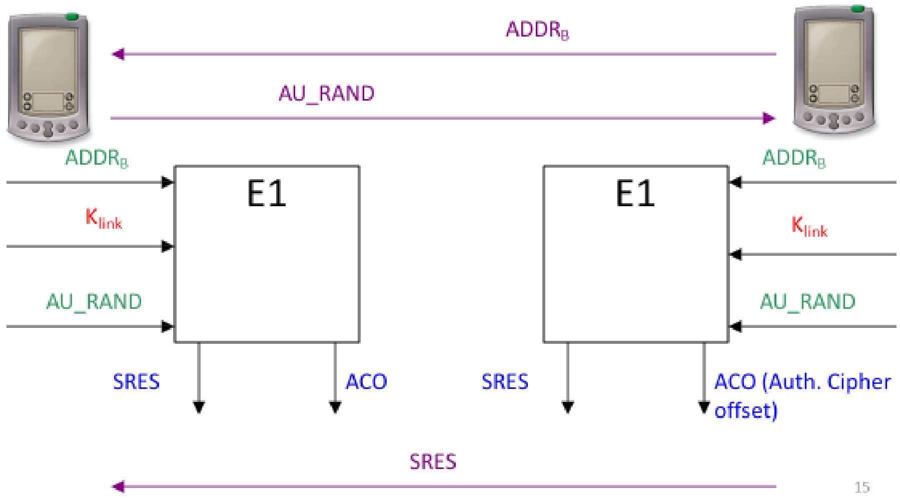
- The Combination key is the combination of two generated in a device A and B, Respectively.
- Each device generates a random no. LK_RAND$_A$ and LK_RAND$_B$.
- Then utilizing E$_{21}$ they generate LK_K$_A$ and LK_K$_B$ respectively.
- LK_K=E$_{21}$ (LK_RAND, BD_ADDR)
- LK_K$_A$ and LK_K$_B$ are XORed with the current link key.
- Device A calculate LK_RAND$_A$ LK_RAND$_B$.
- K$_{AB}$ is calculated simply by XORing LK_K$_A$ and LK_K$_B$.

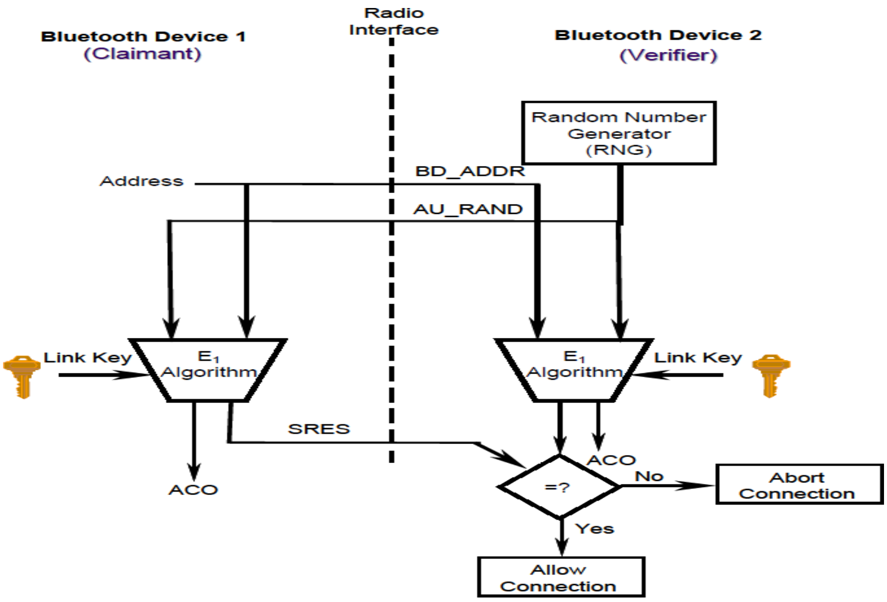




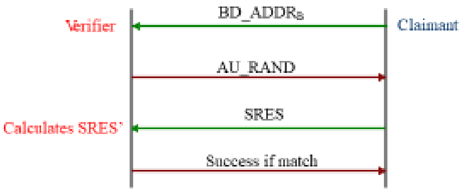
4. Authentication

- Both device A & B use the common link key for authentication, they don't need generate a new $K_{init.}$ During each authentication a new AU_RAND$_A$ is issued.
- Authentication uses a challenge-response scheme in which a claimant's Knowledge of a secret key is checked through a 2- step protocol using symmetric secret key.
- It return SRES to the verifier.
- When the authentication attempt fails, for each subsequent authentication failure with the same Bluetooth Device address, the waiting interval is increased exponentially.





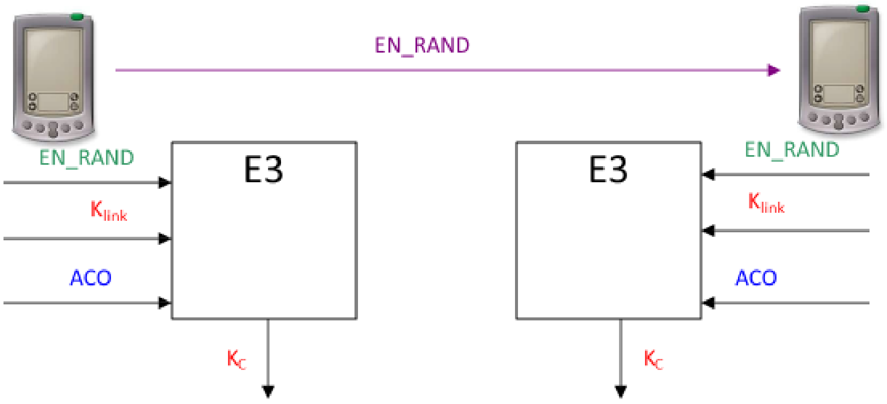
Authentication Summary



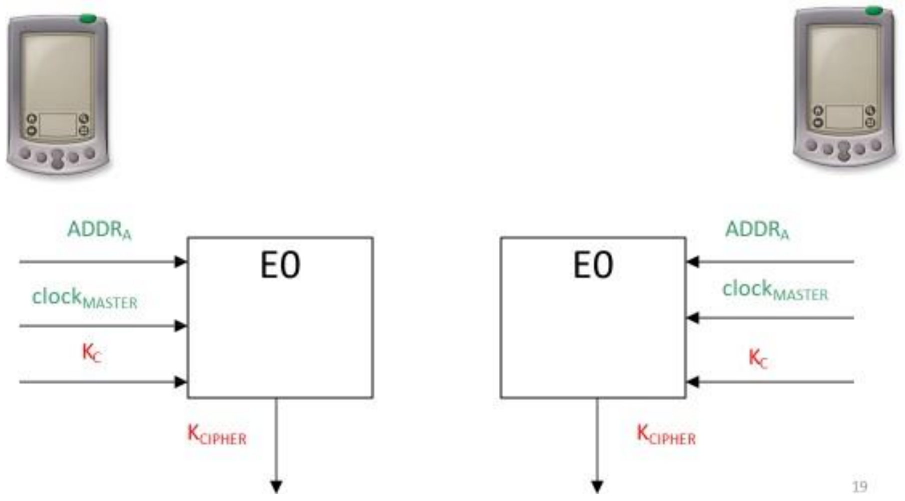
Authentication Process

Parameter	Length	Secrecy parameter
Device Address	48 Bits	Public
Random Challenge	128 Bits	Public
Authentication (SRES) Response	32 Bits	Public
Link Key	128 Bits	Secret

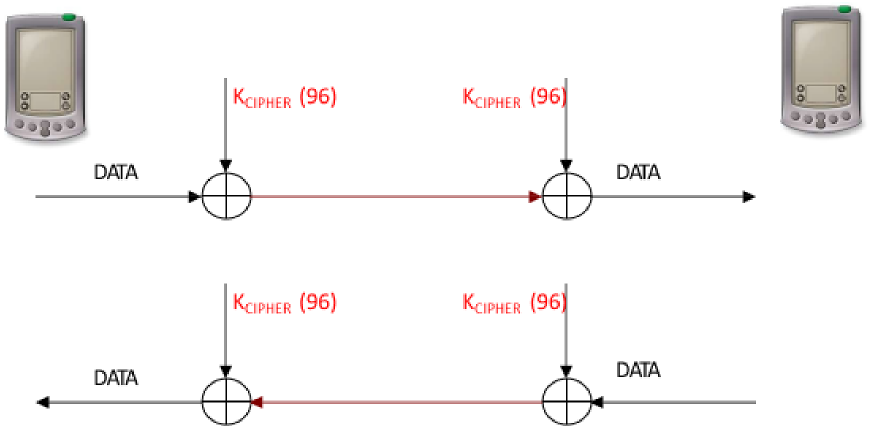
5. Generation encryption key



6. Generation key stream



7. Encryption of data



Most important security weaknesses

- Problems with E0
- Unit key
- PIN
- Problems with E1
- Location privacy
- Denial of service attacks