The security of existing wireless networks

- Cellular networks
  - GSM
  - UMTS
- WiFi LANs
- Bluetooth
Security in Wireless Networks

- Wireless networks are more vulnerable to security issues:
  
  - **Broadcast communications**
    - Wireless usually means a radio channel which has a broadcast nature
    - Transmissions can be overheard by anyone in range (eavesdropping)
    - Anyone can generate transmissions: injecting bogus messages into the network is easy
    - Transmission may interfere with other nearby transmissions (jamming)
  
  - Altering the content of the messages is easier
  - Impersonating a legitimate identity is easier
  - Replaying previously recorded messages is easy
  - The radio channel can be overused (a solution is limiting the bit rate)
  - Denial of service can be easily achieved by jamming
  - The device can be tracked (location privacy)
  - Power limitation in small mobile devices
Wireless communication security requirements

- **Confidentiality**
  - messages sent over wireless links must be encrypted

- **Authentication**
  - the identity of any entities accessing to the services must be verified

- **Replay detection**
  - freshness of messages received over wireless links must be checked

- **Integrity**
  - modifying messages on-the-fly (during radio transmission) is not so easy, but possible
    - integrity of messages received over wireless links must be verified

- **Access control**
  - the service provider grants access to the resources for legitimate users
    (legitimacy must be checked regularly because logical associations can be hijacked)

- **Non-repudiation**
  - it should be possible for an operator to prove that a user has used a service

- **Availability**
  - fairly availability of the services to every users (e.g. emergency calls with a high priority must be always possible in cellular networks)
Principles of security in existing wireless networks

1.3.1 Cellular networks
1.3.2 WiFi LANs
1.3.3 Bluetooth
Cellular Networks

- Cellular networks are infrastructure-based networks
- The infrastructure consists of base stations and a wired backbone network which connects the base stations together, to the wired telephone system and to the internet (Base Stations are supervised by Base Station Controllers which in turn are connected to a Mobile Switching Center).

- A base station provides the service to the mobile stations (mobile phones) in its own physical area which is called a cell.

- The whole network, which typically is a country, is covered by the whole number of base stations.
- The backbone of the network can be connected to other networks through roaming agreements to provide continent-or even world-wide mobility to the users.

- **GSM** (Global System for Mobile Communications) and **UMTS** (Universal Mobile Telecommunications System) are European initiatives of cellular networks.
GSM Security

- The SIM card (Subscriber Identity Module)
  - A small smart card as the main component at the user side.
  - Protected by a PIN code (checked locally by the SIM)
  - Is removable from the terminal device

- Contains all data specific to the end user which have to reside in the Mobile Station:
  - IMSI: International Mobile Subscriber Identity (permanent user’s identity)
  - PIN
  - TMSI (Temporary Mobile Subscriber Identity)
  - K : User’s secret key
  - CK : Ciphering key
  - List of the last call attempts
  - List of preferred operators
  - Supplementary service data (abbreviated dialing, last short messages received,...)
GSM Security

- **main security requirement:**
  - **subscriber authentication** (for the sake of billing, e.g. who must be charged for using the network)
    - long-term secret key shared between the subscriber and the home network operator
    - challenge-response protocol:
      - **challenge:** an unpredictable random number sent from the home network to the subscriber
      - **response:** computed by the subscriber from the challenge and the long-term secret key
      - The long-term key is known exclusively to the home network and the subscriber: no one else can compute the correct response
      - The freshness of the response is ensured due to the unpredictability of the challenge
    - Supports **roaming** without revealing the long-term key to the **visited networks**
GSM Authentication Protocol (roaming to a foreign network)

Mobile Station

Visited network

Home network

- Communication between visited and home network happens through the backbone
- CK is a key which will be used to encrypt the messages sent between MS and the visited network
- CK= Cipher Key

The security of existing wireless networks
other security services provided by GSM

- confidentiality of communications and signaling over the wireless interface
  - encryption key (CK) shared between the subscriber and the visited network is established with the help of the home network as part of the subscriber authentication protocol

- protection of the subscriber’s identity from eavesdroppers on the wireless interface
  - The aim is to protect the subscriber from being tracked
  - usage of short-term temporary identifiers, TMSI, instead of IMSI
    - After each successful authentication the visited network sends a TMSI to the subscriber (encrypted with CK) which will be mapped to IMSI by the visited network and will be used for next authentications
Conclusion on GSM security

- Focused on the protection of the air interface and no protection on the **wired** part of the network
- The visited network has access to all data (except the secret key of the end user) while there is **no authentication for the base station**
- **Faked base stations:**
  - The authentication triplet can be reused later by a fake base station; the subscriber cannot check the freshness of the challenge
- **No data integration:** although modifying packets on-the-fly is quite challenging a fake base station can do that
- **Short length of the key** (54 bits only) + commonly used A3 and A8 algorithms ➔ Cloning of the SIM card has been also reported
UMTS Security Principles

- Reuse of 2\textsuperscript{nd} generation security principles (GSM)
  - Removable hardware security module
    - In GSM: SIM (Subscriber Identity Module) card
    - In UMTS: USIM (User Services Identity Module)
  - Radio interface encryption
  - Protection of the identity of the end user (especially on the radio interface)

- Correction of the following weaknesses of GSM:
  - Possible attacks from a faked base station (auth. data can be reused)
  - Cipher keys and authentication data transmitted in clear between and within networks
  - Data integrity not provided
Authentication in UMTS

User authentication request:

\[
\text{RAND} \parallel \text{AUTN}
\]

\[
\text{(AUTN} := (SQN \oplus AK) \parallel AMF \parallel MAC)
\]

\[
\text{(MAC} := f_1(SQN, AMF, RAND, K)
\]

User authentication response: RES

Compare RES and XRES

Will use CK for confidentiality and IK for integrity

Mobile Station

Visited Network

Home Network

K

AMF:

(Sequence Number)

SQN:

Generation of cryptographic material

Authentication vector

(RAND, XRES, CK, IK, AUTN)

XRES: expected response to RAND

AUTN: Authentication Token

K

IMSI/TMSI

User authentication request:

- Verify AUTN: calculate AK, decode SQN, verify MAC (to check if RAND is generated by home network)
- Verify freshness of SQN (greater than the last one stored)
- Compute RES

Will use CK for confidentiality and IK for integrity
Generation of the authentication vectors

\[
\begin{align*}
AUTN &:= (SQN \oplus AK) \parallel AMF \parallel MAC \\
AV &:= RAND \parallel XRES \parallel CK \parallel IK \parallel AUTN \\
MAC &:= f_1(SQN, AMF, RAND, K)
\end{align*}
\]

AMF: Authentication and Key Management Field
AUTN: Authentication Token
AV: Authentication Vector
MAC: Message Authentication Key
AK: Used to encrypt SQN
User Authentication Function in the USIM

- Verify MAC = XMAC
- Verify that SQN is in greater than the previous one

USIM: User Services Identity Module
Conclusion on UMTS security

- Some improvement with respect to 2\textsuperscript{nd} generation
  - CK and authentication data sent not in clear (thus a fake base station can not reuse them)
  - Integrity of the signalling messages is protected

- Visited network is not authenticated:
  - Although visited network can be authenticated by the home network but since home network does not inform the subscriber about the identity of the visited network the following attack is still possible:
    - Visited network X authenticates itself to the home network as x but masquerades to the subscriber as Y (which may be cheaper than X and the subscriber would the unexpected tariff on the bill at the end of the month)
Principles of security in existing wireless networks

1.3.1 Cellular networks
1.3.2 WiFi LANs
1.3.3 Bluetooth
AP: access point
STA: Mobile Station

- AP advertises its presence on several radio frequencies (channels)
- STAs listen on each channel to hear the beacons and request connection
- All communications (even between two mobile devices of same network) are through the AP

**Introduction to WiFi**

**beacon**
- MAC header
- timestamp
- beacon interval
- capability info
- SSID (network name)
- supported data rates
- radio parameters
- power slave flags

**association request**
**association response**

---

scanning on each channel

STA

“connected”

AP
Introduction to WiFi
WEP – Wired Equivalent Privacy

- Early versions of the IEEE 802.11 standard already featured a security architecture: WEP (Wired Equivalent Privacy)
- part of the IEEE 802.11 specification

- goal
  - make the WiFi network *at least as secure as a wired LAN* (that has no particular protection mechanisms)
  - WEP was never intended to achieve strong security

- services
  - access control to the network
  - message confidentiality
  - message integrity
WEP – Access control

- before association, the STA needs to authenticate itself to the AP
- authentication is based on a simple challenge-response protocol:
  - STA \(\rightarrow\) AP: authenticate request
  - AP \(\rightarrow\) STA: authenticate challenge \((r)\) // \(r\) is 128 bits long
  - STA \(\rightarrow\) AP: authenticate response \((e_k(r))\)
  - AP \(\rightarrow\) STA: authenticate success/failure

- once authenticated, the STA can send an association request, and the AP will respond with an association response
- if authentication fails no association is possible
WEP – Message confidentiality and integrity

- WEP encryption is based on RC4 (a stream cipher developed in 1987 by Ron Rivest for RSA Data Security, Inc.)
  - operation:
    - for each message to be sent:
      - RC4 is initialized with the shared secret (between STA and AP)
      - RC4 produces a pseudo-random byte sequence (key stream)
      - this pseudo-random byte sequence is XORed to the message
    - reception is analogous
  - it is essential that each message is encrypted with a different key stream
    - RC4 generator is initialized with the shared secret and an IV (initial value) together
      - shared secret is the same for each message
      - 24-bit IV changes for every message
    - Otherwise an attacker could eavesdrop two messages \((M1 \oplus K)\) and \((M2 \oplus K)\) and XOR them together to achieve \((M1 \oplus M2)\); since messages are far from pseudo-random sequences the attacker will be likely to succeed to open it.

- WEP integrity protection is based on an encrypted CRC (Cyclic redundancy check) value
  - ICV (integrity check value) is computed and appended to the message
  - the message and the ICV are encrypted together
WEP – Message confidentiality and integrity

Message confidentiality and integrity in existing wireless networks like WEP involves several steps. For encryption (encode), a pseudo-random sequence \( K \) is generated. This sequence is used in a stream cipher, such as RC4, to generate a keystream. The IV (Initial Value) is combined with the secret key to encrypt the message. The resulting encrypted message is then supplemented with a CRC (Cyclic Redundancy Check) value. For decryption (decode), the same non-secret \( K \) is generated and used to decrypt the message, which is then compared to the calculated CRC value to verify integrity.

- **K**: Pseudo-random sequence
- **IV**: Initial Value
- **ICV**: Integrity Check Value (\( = \text{CRC}(M) \oplus K \))
WEP – Keys

- two kinds of keys are allowed by the standard
  - default key (also called shared key, group key, multicast key, broadcast key, key)
  - key mapping keys (also called individual key, per-station key, unique key):
    - is more complicated on the AP side

- in practice, often only default keys are supported
  - the default key is manually installed in every STA and the AP
  - each STA uses the same shared secret key → in principle, STAs can decrypt each other’s messages
WEP flaws – Authentication and access control

- authentication is one-way only
  - AP is not authenticated to STA
  - STA is at risk to associate to a rogue AP

- the same shared secret key is used for authentication and encryption
  - weaknesses in any of the two protocols can be used to break the key

- A STA is authenticated only at connection time
  - An attacker can send messages using the MAC address of the STA
  - Although, correctly encrypted messages cannot be produced by the attacker but replay of the STA messages (also of any other STAs due to the common default key) is still possible
WEP flaws – Authentication and access control

- STA can be impersonated:
  - As authentication is based on a challenge-response protocol:
    - AP $\rightarrow$ STA: $r$
    - STA $\rightarrow$ AP: IV $\mid$ $r \oplus K$
    - where $K$ is a 128 bit RC4 output on IV and the shared secret

- an attacker can compute $r \oplus (r \oplus K) = K$

- then it can use $K$ to impersonate STA later (uses the same $K$ and IV as in the overheard message without need to have the secret key of the STA to compute $K$ from IV):
  - AP $\rightarrow$ attacker: $r'$
  - attacker $\rightarrow$ AP: IV $\mid$ $r' \oplus K$
WEP flaws – Integrity and replay protection

- There’s no replay protection at all
  - IV is not mandated to be incremented after each message
- The attacker can manipulate messages despite the ICV mechanism and encryption ($M$ to $M+\Delta M$ for any $\Delta M$)
  - Encrypted message can be written as: $(M||CRC(M)) \oplus K = (M\oplus K)||ICV$
  - CRC is a linear function with respect to XOR:
    $$CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$$
  - attacker observes $(M || CRC(M)) \oplus K$ where $K$ is the RC4 output
  - for any $\Delta M$, the attacker can compute $CRC(\Delta M)$
  - hence, the attacker can manipulate the message by computing:
    $$((M || CRC(M)) \oplus K) \oplus (\Delta M || CRC(\Delta M)) =$$
    $$((M \oplus \Delta M) || (CRC(M) \oplus CRC(\Delta M))) \oplus K =$$
    $$((M \oplus \Delta M) || CRC(M \oplus \Delta M)) \oplus K$$

  without being noticed by the AP
WEP flaws – Confidentiality

- **IV reuse**
  - IV space is too small
    - IV size is only 24 bits → there are 16,777,216 possible IVs
    - after around 17 million messages, IVs are reused
    - a busy AP at 11 Mbps is capable for transmitting 700 packets per second → IV space is used up in around 7 hours
  - in many implementations IVs are initialized with 0 on startup
    - if several devices are switched on nearly at the same time, they all use the same sequence of IVs
    - if they all use the same default key (which is the common case), then IV collisions are readily available to an attacker

- **weak RC4 keys** *(most serious flaw of WEP: finding the secret key itself)*
  - for some seed values (called weak keys), the beginning of the RC4 output does not look random: one can infer the bits of the seed
  - if a weak key is used, then the first few bytes of the output reveals a lot of information about the key → breaking the key is made easier
  - for this reason, crypto experts suggest to always throw away the first 256 bytes of the RC4 output, but WEP doesn’t adopt that
  - due to the use of IVs, eventually a weak key will be used, and the attacker will know that because the IV is sent in clear
  - → WEP encryption can be broken by capturing a few million messages !!!
WEP – Lessons learnt

1. Engineering security protocols is difficult
   – One can combine otherwise strong building blocks in a wrong way and obtain an insecure system at the end
     • Example 1:
       – stream ciphers alone are OK (RC4)
       – challenge-response protocols for entity authentication are OK
       – but they shouldn’t be combined
         (- K in authentication is a 128 bit RC4 output on IV and the shared secret)
     • Example 2:
       – encrypting a message digest to obtain an ICV is a good principle
       – but it doesn’t work if the message digest function is linear wrt to the encryption function
       – Don’t do it alone (unless you are a security expert)
         • functional properties can be tested, but security is a non-functional property → it is extremely difficult to tell if a system is secure or not
       – Using an expert in the design phase pays out (fixing the system after deployment will be much more expensive)
         • experts will not guarantee that your system is 100% secure
         • but at least they know many pitfalls
         • they know the details of crypto algorithms

2. Avoid the use of WEP (as much as possible)
Overview of 802.11i

- After the collapse of WEP, IEEE started to develop a new security architecture → 802.11i

- Main novelties in 802.11i compared to WEP
  - access control model is based on 802.1X
  - flexible authentication framework (based on EAP – Extensible Authentication Protocol)
  - authentication process results in a shared session key (which prevents session hijacking)
  - different functions (encryption, integrity) use different keys derived from the session key using a one-way function
  - integrity protection is improved
  - encryption function is improved
Overview of 802.11i

- 802.11i defines the concept of RSN (Robust Security Network)
  - integrity protection and encryption is based on AES cipher (and not on RC4 anymore)
  - nice solution, but needs new hardware → cannot be adopted immediately

- RSN uses AES-CCMP → needs new hardware to support AES

- To adapt the solution faster 802.11i also defines an optional protocol called TKIP (Temporal Key Integrity Protocol)
  - integrity protection is based on Michael (we will skip the details of that)
  - encryption is based on RC4, but WEP’s problems have been avoided
  - runs on old hardware (after software upgrade)

- TKIP → WPA (WiFi Protected Access): the manufacturers adopted TKIP in WPA specification (before 802.11i was finalized) by containing a subset of RSN which can also run on old devices that only support RC4 cipher.

- Only the mechanisms used for integrity and confidentiality is different between WPA and RSN (authentication, access control and key management are the same)
802.1X authentication model

- The **supplicant** requests access to the services (wants to connect to the network)
- The **authenticator** controls access to the services (controls the state of a port)
- The **authentication server** authorizes access to the services
  - The supplicant authenticates itself to the authentication server
  - If the authentication is successful, the authentication server instructs the authenticator to switch the port on
  - The authentication server informs the supplicant that access is allowed
Mapping the 802.1X model to WiFi

- supplicant → mobile device (STA)
- authenticator → access point (AP)
- authentication server → server application running on the AP or on a dedicated machine
- port → logical state implemented in software in the AP

- one more thing is added to the basic 802.1X model in 802.11i:
  - successful authentication results not only in switching the port on, but also in a session key between the mobile device and the authentication server
  - the session key is sent to the AP in a secure way
    - this assumes a shared key between the AP and the auth server
    - this key is usually set up manually
Protocols – EAP, EAPOL, and RADIUS

- **EAP** (Extensible Authentication Protocol) [RFC 3748]
  - carrier protocol designed to transport the messages between the STA and the authentication server
  - very simple, four types of messages:
    - EAP request – carries messages from the supplicant to the authentication server
    - EAP response – carries messages from the authentication server to the supplicant
    - EAP success – signals successful authentication
    - EAP failure – signals authentication failure
  - authenticator doesn’t understand what is inside the EAP messages, it recognizes only EAP success and failure

- **EAPOL** (EAP over LAN) [802.1X]
  - used to encapsulate EAP messages into LAN protocols (e.g., Ethernet)
  - EAPOL is used to carry EAP messages between the STA and the AP

- **RADIUS** (Remote Access Dial-In User Service) [RFC 2865-2869, RFC 2548]
  - used to carry EAP messages between the AP and the auth. server
  - MS-MPPE-Recv-Key attribute is used to transport the session key from the auth. server to the AP
  - RADIUS is mandated by WPA and is optional in RSN
Key hierarchies

802.1X authentication

PMK (pairwise master key):
The session key established between the STA and the AP in the authentication procedure

PTK (pairwise transient keys):
- key encryption key
- key integrity key
- data encryption key
- data integrity key
(four keys (PTK) derived from PMK) (128 bits each)

GTK (group transient keys):
- group encryption key
- group integrity key

key generation in AP

Sent to every STA

protection

unicast message trans. between STA and AP

broadcast messages trans. from AP to STAs

key derivation in STA and AP

The security of existing wireless networks

Georg-August University Göttingen
Four-way handshake

- PMK is established between AP and the mobile device
- To derivate PTK the MAC addresses of the parties as well as two random numbers generated by them is used as input besides the PMK
- AP and the mobile device exchange their random numbers through the four-way handshake protocol to be used in the generation of PTK
- The protocol also proves that AP also knows the PMK (result of authentication)
- The messages are carried by the EAPOL protocol

protocol:

- AP: generate ANonce
  AP \rightarrow STA: ANonce
- STA: generate SNonce and compute PTK
  STA \rightarrow AP: SNonce | MIC_{KIK}
  AP: compute PTK, generate GTK, verify MIC (using computed KIK, to verify that the STA has the PMK too)
  AP \rightarrow STA: ANonce | KeyReplayCtr | \{GTK\}_{KEK} | MIC_{KIK}
  STA: verify MIC and install keys
  STA \rightarrow AP: KeyReplayCtr+1 | MIC_{KIK}
  AP: verify MIC and install keys

MIC_{KIK}: Message Integrity Code (computed by the mobile device using the key-integrity key)
KeyReplayCtr: the start of a sequence number used to prevent replay attacks in data transmission, KEK: key encryption key
TKIP

- runs on old hardware (supporting RC4)
- WEP weaknesses are corrected:
  - **Integrity:**
    - new message integrity protection mechanism called Michael
    - use IV as sequence number \(\text{----> to prevent replay attacks}\)
    - IV incremented for each message (if the received IV is smaller than the smallest stored IV the message will be dropped; if larger than the largest one the message will be kept and the stored IVs will be updated; if between the smallest and the largest one it will check if the same IV is stored, if so the message will be dropped and otherwise the message will be kept and the new IV will be stored)
  - **Confidentiality:**
    - increase IV length to 48 bits in order to prevent IV reuse
    - Each message is encrypted with a different key to prevent attacks based on weak keys (the attacker can not observe enough number of messages encrypted with the same (weak) key) \(\text{----> the message keys are generated from the data encryption key of the PTK}\)
TKIP – Generating RC4 keys

- The message keys are generated from the data-encryption-key of the PTK.
- The problem is that the IV is modified to have 48 bits while the WEP hardware still accepts 128 bit-long RC4 seed values.
- So the 48 bit IV and the 104 bit key must somehow be compressed to have a total length of 128 bit.
TKIP – Generating RC4 keys

- IV
  - upper 32 bits
  - lower 16 bits
- data encryption key from PTK
- key mix (phase 1)
- key mix (phase 2)
- MAC address
- message key
  - 3x8 = 24 bits
  - 104 bit
- RC4 seed value

- 48 bits
- 128 bits

TKIP (Temporal Key Integrity Protocol)

TKIP includes the following enhancements to WEP:

- IV (initialization vector)
  - upper 32 bits
  - lower 16 bits

- Key mix (phase 1)
- Key mix (phase 2)
- Message key
- RC4 seed value

TKIP uses a key mix algorithm to generate a 128-bit data encryption key from a pair of 128-bit PTKs (Pairwise Transient Keys). The key mix algorithm involves mixing the two PTKs together using a special algorithm to produce a new key.

- The resulting key is then used to encrypt the data using the RC4 stream cipher.

- The IV is used to ensure that each packet is encrypted with a different key, which enhances security.

- The IV is generated by combining the first 24 bits of the MAC address with a random 24-bit value.

- The RC4 seed value is used to initialize the RC4 stream cipher, ensuring that each packet is encrypted with a different key.
AES-CCMP

- Is used in RSN
- Was easier than TKIP to design because does not have to work on old hardware
- RC4 is replaced with AES block cipher
Summary on WiFi security

- Security has always been considered important for WiFi
- Early solution was based on WEP
  - Seriously flawed
  - Not recommended to use
- The new security standard for WiFi is 802.11i
  - Access control model is based on 802.1X
  - Flexible authentication based on EAP
  - Improved key management
  - TKIP
    - Uses RC4 → runs on old hardware
    - Corrects WEP’s flaws
    - Mandatory in WPA, optional in RSN (RSN is also called WPA2)
  - AES-CCMP
    - Is used in RSN
    - Needs new hardware that supports AES
Principles of security in existing wireless networks

1.3.1 Cellular networks
1.3.2 WiFi LANs
1.3.3 Bluetooth
Bluetooth

- Short-range communications, master-slave principle
- One unit acts as master and the others as slaves for the lifetime of the network

Eavesdropping is difficult:
- Frequency hopping (over 79 channels, frequency change with the rate of 1600 times/sec in a pseudo-random manner)
  - Master determines hopping pattern, slaves have to synchronize
  - All devices in the network hop together
- Communication is over a few meters only: the attacker must be very close to the victim to eavesdrop the messages

Security issues:
- Authentication of the devices to each other
- Confidential channel
- based on secret link key
When two devices communicate for the first time:

- Set up the temporary initialization key.
- \( L = \) length of the PIN
- Usually PIN is a 4-digit number with the default value of 0000
- Pairing (sharing PIN): the user can input a random PIN to both devices
Bluetooth

- Setting up the link key:
  - If one of the devices has memory limitations, it would send its long-term key to the other device encrypted with \( k_{\text{init}} \) to be used as the link key.
  - If none of the devices has memory limitations:
    - Link key = \( K_{\text{link}} \),  
    - \( BD\_\text{ADDR} \): the unique device address.
Bluetooth

- The authentication protocol:
  - BD_ADDR = Device address of the claimant
  - ACO = Authentication Offset
- Generation of the encryption key and the key stream:
  (EN_RAND= a random number generated by the master device)
  (The key stream generated by the stream cipher E0 using encryption key is XORed to the data sent between the devices)
Weaknesses

- The strength of the whole system is based on the strength of the PIN:
  - PIN: 4-digit number, easy to try all 10000 possible values.
  - PIN can be cracked off-line: having the challenge-response pairs overheard from authentication execution, each guessed PIN and the K_link given by that can be tested off-line (to find the PIN after checking max 10000 PINs).
  - many devices use the default PIN.

- For memory-constrained devices: the link key = the long-term unit key of the device:
  - An attacker can obtain the long-term unit key of a memory limited device just by establishing a link key with it.
  - It also can decrypt the messages transmitted between the memory limited device and other devices.

- Fixed and unique device addresses: privacy problem
  - The attacker can track the device by tracking the use of the given device address

- Weaknesses in the E₀ stream cipher:
  - The encryption key can be broken with much less effort than brute force attack
Conclusion

- Security issues of wireless networks:
  - wireless channel: easy to eavesdrop on, jam, overuse
  - Users are usually mobile:
    - privacy issues (which is unique to mobile networks) besides classical security requirements

- Mobile devices:
  - Limited resources
  - Lack of physical protection

- Roaming of users across different networks