Wireless Security I
--Cellular Networks
Outline

- Wireless networks
- Wireless security challenges
- GSM security
  - current status, attacks and remedies
- 3GPP security
Classification of Wireless Networks

- WLAN: 802.11
- Cellular networks: GSM, 3GPP
- WWAN: WiMAX, 802.16
- Ad hoc networks
- Sensor networks
- WPAN: Bluetooth, Zigbee, 802.15
- Wireless mesh networks
Modern Wireless Networks

- **WWAN**
- **WLAN**
- **WPAN**
  - Bluetooth, Zigbee, 802.15
  - Low-Power Short Range
  - 802.11 and Similar Technologies
  - Medium Power Medium Range
  - Cellular & Related Technologies
    - High Power Long Range
Wireless Protocols

- Bluetooth
- 802.11a
- 802.11b
- 802.11g
- Others

<table>
<thead>
<tr>
<th>Transportation (SSL/TLS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network (IPSec, VPN)</td>
</tr>
<tr>
<td>MAC (WEP, WPA, WPA2, 802.11i)</td>
</tr>
</tbody>
</table>
Wireless Security Challenges

- A number of unsolved threats in wired networks
- Shared wireless medium
- Vulnerable protocol design
- Difficulty in identifying anomalies
- Physical loss or theft of mobile devices
- Resource constraints of mobile devices
- Lack of a centralized authority or administration
- More...
Cellular Networks

4G Architecture

Others

Mesh
WBAN
Bluetooth

IP Bone Network

802.11a
WLAN
802.11b

WCDMA
TDSCDMA

GPRS
CDMA1x
CDMA
GSM
2G/2.5G

3G

CDMA2000

2G/2.5G

4G Architecture
GSM

- **Global System for Mobile Communications**
  - GSM is most popular standard for mobile phones
  - The GSM Association estimates 82% of the global mobile market uses this standard
  - Two billion people across more than 200 countries use GSM

- **Services**
  - Voice Communication, Short Messaging Service, …etc.
GSM Architecture I

Diagram showing the components of the GSM architecture:
- Mobile Station
- Base Station Subsystem
- Network Subsystem
- Home Location Register
- Visitor Location Register
- Mobile Service Switching Centre
- Equipment Identity Register
- Authentication Centre

Interconnections and signals are depicted, including radio interface and base station controller.
GSM Architecture 2

Base Station Subsystem (BSS)  Network Switching Subsystem (NSS)

BTS  BSC  HLR  VLR  AuC
BTS  BSC  MSC  Public Networks
BTS  ME  SIM  MS
Mobile Station

- **Mobile Equipment**
  - International Mobile Equipment Identity (IMEI)

- **Subscriber Identity Module (SIM) card**
  - Smart Card containing identifiers, keys and algorithms
The SIM Card

- **SIM (Subscriber Identity Module)**
  - A small smartcard inserted into a GSM phone
  - Contains (at least)
    - IMSI – International Mobile Subscriber Identity
    - Ki – a 128-bit key obtained from AuC during registration, the long-term key used for authentication and cipher key generation
    - A3/A8 implementations
  - Protected by an optional PIN and a PUK (PIN Unlock)
  - Locked after a few invalid inputs of PIN (normally 3) and becoming permanently useless after a number of invalid inputs of PUK (normally 10)
Base Station Subsystem

- **Base Transceiver Station (BTS)**
  - A cell is formed by the radio coverage of a BTS
  - Provide the radio channels and handle the radio-link protocol

- **Base Station Controller (BSC)**
  - Manage the radio resources for one or more BTS
  - Handle channel setup and handovers
  - Connect to the mobile service switching center
Network Subsystem

- **Component in Network Subsystem**
  - MSC: Mobile services Switching Center
  - HLR: Home Location Register
  - VLR: Visitor Location Register
  - AuC: Authentication Center
  - EIR: Equipment Identity Register

- **Network Subsystem features**
  - Telephone switching function
  - Subscriber profile
  - Mobility management
GSM Basic Security Goals

- Subscriber authentication to protect the operator against the billing fraud
- Confidentiality on the radio path
- User anonymity/location privacy
GSM Security Design Requirements

- The security mechanism
  - MUST NOT
    - Add significant overhead on call set up
    - Increase bandwidth of the channel
    - Increase error rate
    - Add expensive complexity to the system
  - MUST
    - Use cost effective scheme

- How to Design?
GSM Security Features

- **Subscriber authentication**
  - The operator knows for billing purposes who is using the system

- **Signaling and user data confidentiality**

- **Subscriber identity protection/user privacy**
  - The transmission of the IMSI in plaintext over the air should be avoided wherever possible
  - Somebody intercepting communications should not be able to learn if a particular mobile user in the area

- **Key management is independent of equipment**

- **Detection of compromised equipment**
Crypto Algorithms in GSM

- **Authentication**
  - In the SIM
  - 128-bit RAND → A3 → 32-bit SRES
  - 128-bit Ki

- **Key generation**
  - In the SIM
  - 128-bit RAND → A8 → 64-bit Kc
  - 128-bit Ki

- **Encryption**
  - In the phone
  - Kc (from A8) → A5 → ciphertext
  - COUNT
  - user data
Crypto Algorithms in GSM

- A3/A8 left at the discretion of the operator
- COMP128 – ill-advised by GSM standards
  - Outputs a 128-bit result
  - First 32 bits producing the A3 output
  - Last 54 bits concatenated by 10 zeros producing the A8 output
  - Cracked in 1998 and still in use
Authentication

- **Authentication Goals**
  - Subscriber (SIM holder) authentication, protection of the network against unauthorized use
  - Create a session key for the next communication

- **Authentication Scheme**
  - Subscriber identification: IMSI
  - Challenge-Response authentication of the subscriber
  - Long-term secret key shared between the subscriber and the home network
  - Supports roaming without revealing long-term key to the visited networks
Authentication Parameters

- **Network Contains**
  - AuC: Authentication Center
  - HLR: Home Location Register

- **Algorithms**
  - A3: Mobile Station Authentication Algorithm
  - A8: Session (cipher) key generation Algorithm
  - PRNG: Pseudo-Random Number Generator

- **Random number, keys and signed response**
GSM Authentication Protocol

IMSI: International Mobile Subscriber Identity
RAND: Random Number
SRES: Signed Response
Ki: Stored in the HLR as well as in the SIM
Kc: Cipher Key
Authentication Procedure

- MS send IMSI to the network subsystem (AuC and HLR)
- The network subsystem received the IMSI and find the correspondent Ki of the IMSI
- The AuC generate a 128-bit RAND and send (RAND, SRES, Kc) to MS
- The AuC calculate the SRES with A3 algorithm
- MS calculates a SRES with A3 using Ki and the given RAND
- MS sends the SRES’ to the network
- The visited network compare the SRES and SRES’ for verification
A3 – Authentication Algorithm

- Goal
  - Generation of SRES response to random number RAND

```
RAND (128 bits) → A3
Ki (128 bits) → A3

SRES (32 bits)
```
A8 – Cipher Key Generation Algorithm

- Goal - Voice Privacy
  - Generation of Cipher key - Kc
Implementation of A3 and A8

- Both A3 and A8 algorithms are implemented on the SIM. It is independent of hardware manufacturers and network operators.
- COMP128 is keyed hash function, used for both A3 and A8 in most GSM networks.

```
COMP128

RAND (128 bits)  

Ki (128 bits)  

128 bits output

SRES = first 32 bits
Kc = last 54 bits
```
Confidentiality

• After the authentication protocol, cipher key $K_c$ is shared between the subscriber and the visited network.

• A5 is used as an over-the-air voice privacy algorithm
  ◦ A5 is a stream cipher
  ◦ Implemented very efficiently on hardware
  ◦ A5/1 – the strong version
  ◦ A5/2 – the weak version
Encryption Scheme

Mobile Station

FN (22 bits)  Kc (64 bits)  A5

114 bits

Data (114 bits)

XOR

BTS

FN (22 bits)  Kc (64 bits)  A5

114 bits

Data (114 bits)

FN : Frame Number
CK: Cipher Key
### A5/1 Shift Registers

<table>
<thead>
<tr>
<th>LFSR</th>
<th>Length in bits</th>
<th>Characteristic polynomial</th>
<th>Clocking bit</th>
<th>Tapped bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>19</td>
<td>$x^{18} + x^{17} + x^{16} + x^{13} + 1$</td>
<td>8</td>
<td>13, 16, 17, 18</td>
</tr>
<tr>
<td>2</td>
<td>22</td>
<td>$x^{21} + x^{20} + 1$</td>
<td>10</td>
<td>20, 21</td>
</tr>
<tr>
<td>3</td>
<td>23</td>
<td>$x^{22} + x^{21} + x^{20} + x^{7} + 1$</td>
<td>10</td>
<td>7, 20, 21, 22</td>
</tr>
</tbody>
</table>
Clock Controlling of A5/1

- Three clocking bits in the middle of register are extracted and their majority is calculated.
- Two or three registers whose bit agrees with the majority are clocked.

![Clocking Diagram]

How about?

```
0 1 0 1
1 0 0 1
0 0 0 1
```
A5/1 Architecture
Description of A5/1

1. Set all LFSRs to 0 \((R_1 = R_2 = R_3 = 0)\).
2. For \(i := 0\) to 63 do
   (a) \(R_1[0] = R_1[0] \oplus \text{Key}[i]\)
   (b) \(R_2[0] = R_2[0] \oplus \text{Key}[i]\)
   (c) \(R_3[0] = R_3[0] \oplus \text{Key}[i]\)
   (d) Clock all three registers (i.e., for \(j > 0\) \(R_i[j] \leftarrow R_i[j - 1]\), and \(R_i[0]\) is set to the result of the primitive polynomial on the previous value of \(R_i\)).
3. For \(i := 0\) to 21 do
   (a) \(R_1[0] = R_1[0] \oplus \text{Frame}[i]\)
   (b) \(R_2[0] = R_2[0] \oplus \text{Frame}[i]\)
   (c) \(R_3[0] = R_3[0] \oplus \text{Frame}[i]\)
   (d) Clock all three registers.
4. For \(i := 0\) to 99, clock the cipher by its regular majority clocking mechanism, and discard the output.
Anonymity

- Protection of the subscriber’s identity from eavesdroppers on the wireless interface
- Usage of short-term temporary identifiers
Subscriber Identity Protection

- **TMSI** – Temporary Mobile Subscriber Identity
  - TMSI is used instead of IMSI as an a temporary subscriber identifier.
  - TMSI prevents an eavesdropper from identifying of subscriber.
  - A 32-bit pseudo-random number only valid in a particular Location Area
Subscriber Identity Protection

- Usage
  - TMSI is assigned when IMSI is transmitted to AuC on the first phone switch on.
  - TMSI is used by the MS to report to the network, and network uses TMSI to communicate with MS.
  - The VLR is in charge of TMSI issuance and update.
  - Updated at least every location update procedure; or changed by the VLR at any time.
  - The new TMSI is sent in encrypted form whenever possible so that an attacker cannot map it to an old one and “follow” a user.
  - On MS switch off TMSI is stored on SIM card to be reused next time.
Subscriber Identity Protection

- MS (Mobile Station)
- VLR\textsubscript{new}
- VLR\textsubscript{old}
- HLR/AuC (Home Location Register/Authentication Center)

- TMSI\textsubscript{old}
- Query TMSI\textsubscript{old}
- IMSI\textsubscript{old}+(RAND, SRES,Kc)s
- IMSI
- A5(Kc,TMSI\textsubscript{new})
- ACK
-ACK
- Cancellation
Key Management Scheme

- **Ki – Subscriber Authentication Key**
  - Shared 128 bit key used for authentication of subscriber by the operator
  - **Key Storage**
    - Subscriber’s SIM (owned by operator, i.e. trusted)
    - Operator’s Home Locator Register (HLR) of the subscriber’s home network

- **SIM can be used with different equipment**
  - Subscribers can change handsets without compromising security
Detection of Compromised Equipment

- **International Mobile Equipment Identity (IMEI)**
  - Identity allows to identify mobile phones
  - IMEI is independent of SIM
  - Used to identify stolen or compromised equipment

- **Equipment Identity Register (EIR)**
  - Black list – stolen or non-type mobiles
  - White list – valid mobiles
  - Gray list – local tracking mobiles
Overview of GSM Security Flaws

- Cryptanalysis attacks against A3/A5/A8/COMP-128 algorithm
- Over-the-air interception using fake BTS
- Only air interface transmission is encrypted
- Ciphering key (Kc) used for encryption is only 54 bits long
- Key recovery allowing SIM cloning
Security Flaws in GSM

- Network does not authenticate itself to a phone
  - The most serious fault with the GSM authentication system
  - Leading to the man-in-the-middle attack
Security Flaws in GSM

- Common implementation of A3/A8 is flawed
  - COMP128 is used for both A3 and A8
  - Goldberg and Wagner (UC Berkeley) took 8 hours to break COMP128 in 1998
    - Require physical access to the target SIM, an off-the-shelf card reader and a computer to direct the operation
    - Send $2^{19}$ challenges to the SIM and analyze the responses to obtain the Ki stored in the SIM
  - IBM researchers cracked COMP128 in less than one minute in 2002
- Aftermath
  - The victim SIM can be cloned!!!
Security Flaws in GSM

- Another deliberate flaw in COMP128
  - The lease significant 10 bits of the 64-bit Kc is always set to 0
  - Security is reduced by a factor of 1024

- Flaws in A5
  - A5/1: originally used in Europe
  - A5/2: a deliberately weakened version of A5/1 created for export and used in the United States
  - A5/3: strong encryption algorithm created by 3GPP
Security Flaws in GSM

- Flaws in A5
  - Biryukov, Shamir and Wagner cracked A5/1 under one second on a typical PC in 2000
  - Goldberg, Wagner and Green broke A5/2 in 1999 in about 10 ms
  - Barkhan, Eli Biham and Keller showed an attack on A5/2 within a few dozen milliseconds in 2003, and also described attacks on A5/1 and A5/3
  - A5/3 has not been broken yet but may be soon
Security Flaws in GSM

- Vulnerabilities in the subscriber identity confidentiality mechanism
  - If the network somehow loses track of a particular TMSI, it must ask the subscriber its IMSI sent in plaintext over the radio link
  - An attacker can utilize this to map a TMSI to its IMSI
Security Flaws in GSM

- Ciphering occurs after FEC
  - FEC (forward error correction) is used over the radio link to assist in correcting errors from noise or fading
  - FEC works by adding redundancy to the data stream, thus increasing the amount of bits to transfer
  - In GSM ciphering occurs after FEC
  - The known redundancy patterns of FEC could be used to assist in a cryptanalytic attack
    - Attackers know part of the plaintext and the full ciphertext
Attacks on GSM Security

- Attacks on A3/A8, A5/1
  - Through air interface
  - With possession of mobile equipment
- False base station
  - GSM does unilateral authentication
- Attacks on SIM card (SIM Editor, SIM Scanner)
- DoS (Denial of Service)
  - Jamming the signal
  - Preventing the MS from communicating
Attacks on GSM Security

The network is not authenticated!

No privacy for network signals!
IMSI Catcher (Fake Base Station)

- IMSI-catchers are used by law enforcement and intelligence agencies.
Cracking Long Term Key

- Over-the-air cracking of Ki and cloning of the SIM
  - By imitating a legitimate GSM network, the attacker can learn the IMSI and Ki of a user and clone its SIM card over the air.
SIM Card Cloning
Conclusion

- GSM fails to deliver most of the security criteria described in GSM 02.09
- GSM’s faults result from designing algorithms in secret and deliberately weakening the system
  - This lesson tells us that security algorithms should be exposed to public scrutiny before deployment
- None of the attacks are easily carried out, so
  - For most average users, the security concerns may not be that great
  - Those using GSM for highly sensitive information should think twice however
Countermeasures

- **New A3/A8 implementation**
  - COMP128-2 and COMP128-3
    - Still developed in secret (security through obscurity)
    - A rather slow migration from COMP128-1 to COMP128-2/3
  - 3GPP have defined brand-new authentication algorithms for use with the UMTS system

- **A5/3**
  - Added by GSM in 2002
  - Only few networks and handsets support A5/3 currently

- **GPRS/UMTS**
  - Ciphering before FEC
Countermeasures

- **UMTS Security (3GPP)**
  - Improved, stronger and open crypto algorithms
  - Support network authentication to phone
    - The network sends to the mobile the RAND and an Authentication Token to prove its knowledge of Ki
    - The AUTH includes a sequence number (SN) encrypted using Ki and a message authentication code (MAC) generated also with Ki
    - The mobile decrypts the SN and recalculates the MAC
    - If the result matches with what the network sent, it considers the network legitimate and then returns an XRES
    - The network authenticates the mobile if the XRES is correct
3GPP Security

- The 3rd Generation Partnership Project, built on GSM
- Mutual authentication
- Data Integrity
- Better algorithms
  - KASUMI (A5/3)
3GPP Introduction

• 3G features exceeding over 2G provide
  ◦ Higher data rate, massive network capacity
  ◦ Interactive multimedia service, QoS
  ◦ Global roaming

• 3G communications standards
  ◦ CDMA2000 (USA), W-CDMA (Europe/Japan), TD-SCDMA (China)

• Applications
  ◦ Multimedia Message Service (MMS), Email, Video phone
  ◦ Video streaming, Services from the Internet
3GPP Architecture

UTRAN: UMTS Terrestrial Radio Access Network
RNC: Radio Network Controller
MSC: Mobile Service Switching Center
VLR: Visitor Location Register
GMSC: Gateway MSC
HLR: Home Location Register
SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Support Node
GPRS: General Packet Radio Service
UMTS: Universal Mobile Telecommunications System
3GPP Security Principles

- Reuse of 2G (GSM) security principles:
  - Removable hardware security module, SIM based Authentication
    - In GSM: SIM card
    - In 3GPP: USIM (User Services Identity Module)
  - Radio interface encryption
  - Protection of the identity of the end user (especially on the radio interface)
3GPP Security Principles

- Correction of the weaknesses of 2G:
  - Possible attacks from a faked base station ➔ Mutual Authentication
  - Data integrity not provided ➔ Integrity protection of signalling message
  - Use of stronger encryption
  - Assurance that authentication information and keys are not being re-used (key freshness)
3GPP Authentication and Key Agreement (AKA)

Mutual Authentication

MS

IMSI (Challenge 1) → HLR

Generate Authentication Vector = RAND||XRES||CK||IK||AUTN

AUTN (Response 1) ← RAND (Challenge 2)

RES (Response 2)

Verify AUTN
Calculate RES

Verify OK if RES = XRES
Generation of Authentication Vector

Generate SQN
Generate RAND

SQN: Sequence Number
RAND: Random Number
AMF: Authentication and Key Management Field
K: Shared Key
MAC: Message Authentication Code
XRES: Expected Response
CK: Cipher Key
IK: Integrity Key
AK: Anonymity Key
AV: Authentication Vector
AUTN: Authentication Token

Generate: $AV = \text{RAND} \| \text{XRES} \| \text{CK} \| \text{IK} \| \text{AUTN}$
Send: $\text{AUTN} = \text{SQN} \oplus \text{AK} \| \text{AMF} \| \text{MAC}$
Verification on Mobile Station

**Verify AUTH:**

- **MAC = XMAC**?
- **Verify that SQN is in the correct range**

**Key Terms:****
- **AUTN**: Authentication Token
- **RAND**: Random Number
- **K**: Shared Key
- **SQN**: Sequence Number
- **AK**: Anonymity Key
- **AMF**: Authentication and Key Management Field
- **MAC**: Message Authentication Code
- **XMAC**: Expected MAC
- **RES**: Response
- **CK**: Cipher Key
- **IK**: Integrity Key
Mutual Authentication in 3G

- Subscriber can authenticate the network by the secret $K$ using $f_1(K, SQN, AMF, RAND)$
- $SQN$ is introduced to prevent replay attacks
- $AK$ is used to conceal $SQN$
- Cipher Key and Integrity Key are generated after the authentication (Key Agreement)
Data Integrity in 3GPP

**Sender**  
(Radio Network Controller or Mobile Station)

**Receiver**  
(Radio Network Controller or Mobile Station)

- **COUNT-I**  
- **DIRECTION**  
- **MESSAGE**  
- **FRESH**

- **IK**  
- **f9**  
- **MAC-I**

- FRESH: Connection Nonce  
- COUNT-I: Integrity Sequence Number
**Data Integrity in 3GPP**

- **Data Integrity**
  - COUNT-I and FRESH are used to prevent replay attack
  - DIRECTION specifies the direction of the transmission (User to Network or Network to User)
- **Secure network elements interconnection**
- **F9 uses Kasumi to form CBC-MAC**
Ciphering Method in 3GPP

**Sender**
(Mobile Station or Radio Network Controller)

**Receiver**
(Radio Network Controller or Mobile Station)

LENGTH: Length of Keystream Block
BEARER: Bearer Identity
COUNT-C: Ciphering Sequence Number
Problems of 3GPP Security

- IMSI is sent in cleartext when allocating TMSI to the user
- Signal jamming: physical layer attacks are hard to solve
Further Reading

References to 3GPP Security

- **Principles, objectives and requirements**
  - TS 33.120 Security principles and objectives
  - TS 21.133 Security threats and requirement

- **Architecture, mechanisms and algorithms**
  - TS 33.102 Security architecture
  - TS 33.103 Integrity guidelines
  - TS 33.105 Cryptographic algorithm requirements
  - TS 22.022 Personalization of mobile equipment

- **Lawful interception**
  - TS 33.106 Lawful interception requirement
  - TS 33.107 Lawful interception architecture and functions

- **Technical reports**
  - TR 33.900 A guide to 3G security
  - TR 33.901 Criteria for cryptographic algorithm design process
  - TR 33.902 Formal analysis of the 3G authentication protocol
  - TR 33.908 General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms

- **Algorithm specifications**
  - Specification of the 3GPP confidentiality and integrity algorithms
    - Document 1: f8 & f9
    - Document 2: KASUMI
    - Document 3: implementer's test data
    - Document 4: design conformance test data
References

- Eli Biham and Orr Dunkelman “Cryptanalysis of the A5/1 GSM Stream Cipher”, INDOCrypt 2000
- 3GPP (Third Generation Partnership Project), http://www.3gpp.org/