GSM Security Concerns

• Operators
  – Bills right people
  – Avoid fraud
  – Protect Services

• Customers
  – Privacy
  – Anonymity

• Make a system at least secure as PSTN
GSM Security Goals

- Confidentiality and Anonymity on the radio path
- Strong client authentication to protect the operator against the billing fraud
- Prevention of operators from compromising of each others’ security
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
    • Cost effective scheme
  – Define security procedures
    • Generation and distribution of keys
    • Exchange information between operators
    • Confidentiality of algorithms
GSM Security Features

- **Key management is independent of equipment**
  - Subscribers can change handsets without compromising security

- **Subscriber identity protection**
  - not easy to identify the user of the system intercepting a user data

- **Detection of compromised equipment**
  - Detection mechanism whether a mobile device was compromised or not

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

- **Signaling and user data protection**
  - Signaling and data channels are protected over the radio path
GSM Mobile Station

• Mobile Station
  – Mobile Equipment (ME)
    • Physical mobile device
    • Identifiers
      – IMEI – International Mobile Equipment Identity
  – Subscriber Identity Module (SIM)
    • Smart Card containing keys, identifiers and algorithms
    • Identifiers
      – $K_i$ – Subscriber Authentication Key
      – IMSI – International Mobile Subscriber Identity
      – TMSI – Temporary Mobile Subscriber Identity
      – MSISDN – Mobile Station International Service Digital Network
      – PIN – Personal Identity Number protecting a SIM
      – LAI – location area identity
GSM Architecture

Mobile Stations

Base Station Subsystem

Network Management

Subscriber and terminal equipment databases

BTS

BTS

BTS

BSC

OMC

Exchange System

MSC

VLR

HLR

AUC

EIR
Subscriber Identity Protection

- **TMSI** – Temporary Mobile Subscriber Identity
  - **Goals**
    - TMSI is used instead of IMSI as an a temporary subscriber identifier
    - TMSI prevents an eavesdropper from identifying of subscriber
  - **Usage**
    - TMSI is assigned when IMSI is transmitted to AuC on the first phone switch on
    - Every time a location update (new MSC) occur the networks assigns a new TMSI
    - TMSI is used by the MS to report to the network or during a call initialization
    - Network uses TMSI to communicate with MS
    - On MS switch off TMSI is stored on SIM card to be reused next time
  - The Visitor Location Register (VLR) performs assignment, administration and update of the TMSI
Key Management Scheme

- **$K_i$** — 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
Detection of Compromised Equipment

• International Mobile Equipment Identifier (IMEI)
  – Identifier allowing to identify mobiles
  – 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

• Central Equipment Identity Register (CEIR)
  – Approved mobile type (type approval authorities)
  – Consolidated black list (posted by operators)
Authentication

• Authentication Goals
  – Subscriber (SIM holder) authentication
  – Protection of the network against unauthorized use
  – Create a session key

• Authentication Scheme
  – Subscriber identification: IMSI or TMSI
  – Challenge-Response authentication of the subscriber by the operator
Authentication and Encryption Scheme

**Mobile Station**
- **SIM**
  - $K_i$
- **A3**
- **SRES**
- **A8**
- $F_n$
- $K_c$
- **A5**
- $m_i$

**Radio Link**
- Challenge RAND
- Signed response (SRES)
- Encrypted Data

**GSM Operator**
- **A3**
- $K_i$
- **A8**
- $K_c$
- $F_n$
- **A5**
- $m_i$

Authentication: are SRES values equal?
Authentication

• **AuC** – Authentication Center
  – Provides parameters for authentication and encryption functions \((\text{RAND, SRES, } K_c)\)

• **HLR** – Home Location Register
  – Provides MSC (Mobile Switching Center) with triples \((\text{RAND, SRES, } K_c)\)
  – Handles MS location

• **VLR** – Visitor Location Register
  – Stores generated triples by the HLR when a subscriber is not in his home network
  – One operator doesn’t have access to subscriber keys of the another operator.
A3 – MS Authentication Algorithm

- Goal
  - Generation of SRES response to MSC’s random challenge RAND

\[
\text{RAND (128 bit)} \quad \downarrow \\
\text{K_i (128 bit)} \quad \rightarrow \quad \text{A3} \\
\downarrow \\
\text{SRES (32 bit)}
\]
A8 – Voice Privacy Key Generation Algorithm

• Goal
  – Generation of session key $K_s$
    • A8 specification was never made public

```
RAND (128 bit)

K_i (128 bit)  A8

K_C (64 bit)
```
Logical Implementation of A3 and A8

• Both A3 and A8 algorithms are implemented on the SIM
  – Operator can decide, which algorithm to use.
  – Algorithms implementation is independent of hardware manufacturers and network operators.
Logical Implementation of A3 and A8

- COMP128 is used for both A3 and A8 in most GSM networks.
  - COMP128 is a keyed hash function

\[
\text{RAND (128 bit)} \\
\text{K_i (128 bit)} \\
\text{COMP128} \\
\text{128 bit output} \\
\text{SRES 32 bit and K_c 54 bit}
\]
A5 – Encryption Algorithm

- A5 is a stream cipher
  - Implemented very efficiently on hardware
  - Design was never made public
  - Leaked to Ross Anderson and Bruce Schneier

- Variants
  - A5/1 – the strong version
  - A5/2 – the weak version
  - A5/3
    - GSM Association Security Group and 3GPP design
    - Based on Kasumi algorithm used in 3G mobile systems
Logical A5 Implementation

**Mobile Station**

- \( F_n \) (22 bit)
- \( K_c \) (64 bit)

\[ \xrightarrow{A5} \]

- Data (114 bit)

\[ \xrightarrow{XOR} \]

- Ciphertext (114 bit)

**BTS**

- \( F_n \) (22 bit)
- \( K_c \) (64 bit)

\[ \xrightarrow{A5} \]

- 114 bit

\[ \xrightarrow{XOR} \]

- Data (114 bit)

Real A5 output is 228 bit for both directions
A5 Encryption

Mobile Stations

Base Station Subsystem

Network Management

Subscriber and terminal equipment databases

OMC

Exchange System

BTS

BSC

MSC

VLR

HLR

AUC

EIR

A5 Encryption
SIM Anatomy

- Subscriber Identification Module (SIM)
  - Smart Card – a single chip computer containing OS, File System, Applications
  - Protected by PIN
  - Owned by operator (i.e. trusted)
  - SIM applications can be written with SIM Toolkit
Smart Card Anatomy

SIM Plug-In Size

- Printed Circuit
- Microcontroller
- Glue
- Plastic Support

15 mm (.59“)
20.8 mm (.82“)
Microprocessor Cards

• Typical specification
  – 8 bit CPU
  – 16 K ROM
  – 256 bytes RAM
  – 4K EEPROM
  – Cost: $5-50

• Smart Card Technology
  – Based on ISO 7816 defining
    • Card size, contact layout, electrical characteristics
    • I/O Protocols: byte/block based
    • File Structure
Algorithm Implementations and Attacks
Attack Categories

- SIM Attacks
- Radio-link interception attacks
- Operator network attacks
  - GSM does not protect an operator’s network
Attack History

• 1991
  – First GSM implementation.
• April 1998
  – The Smartcard Developer Association (SDA) together with U.C. Berkeley researches cracked the COMP128 algorithm stored in SIM and succeeded to get $K_i$ within several hours. They discovered that $K_c$ uses only 54 bits.
• August 1999
  – The week A5/2 was cracked using a single PC within seconds.
• December 1999
  – Alex Biryukov, Adi Shamir and David Wagner have published the scheme breaking the strong A5/1 algorithm. Within two minutes of intercepted call the attack time was only 1 second.
• May 2002
  – The IBM Research group discovered a new way to quickly extract the COMP128 keys using side channels.
COMP128

Keyed hash function
Pseudo-code of the compression in COMP128 algorithm

```
Level 0  for j = 0 to 4 do {
  for k = 0 to 2^j-1 do {
    for i = 0 to 2^{(4-j)}-1 do {
      m = l + k*2^{(5-j)};
      n = m + 2^{(4-j)};
      y = (X[m] + 2*X[n]) mod 2^{(9-j)};
      z = (2*X[m] + X[n]) mod 2^{(9-j)};
      X[m] = Tj[y];
      X[n] = Tj[z];
    }
  }
}
```
Actual Information Available

Side Channel Attacks

Side Channels
- Power Consumption
- Electromagnetic radiation
- Timing
- Errors
- Etc.

Smart Card

Input → Crypto Processing → Output

Sensitive Information
Simple Power DES Analysis

SPA of DES operation performed by a typical Smart Card
- Above: initial permutation, 16 DES rounds, final permutation
- Below: detailed view of the second and third rounds
Partitioning Attack on COMP128

- **Attack Goal**
  - $K_i$ stored on SIM card
  - Knowing $K_i$ it’s possible to clone SIM

- **Cardinal Principle**
  - *Relevant bits of all intermediate cycles and their values should be statistically independent of the inputs, outputs, and sensitive information.*

- **Attack Idea**
  - Find a violation of the *Cardinal Principle*, i.e. side channels with signals does depend on input, outputs and sensitive information
  - Try to exploit the *statistical dependency* in signals to extract a sensitive information
Partitioning Attack on COMP128

- How to implement 512 element $T_0$ table on 8 bit Smart Card (i.e. index is 0..255)?
  - Split 512 element table into two 256 element tables

- It’s possible to detect access of different tables via side channels!
  - Power Consumption
  - Electromagnetic radiation
Partitioning Attack on COMP128

Pseudo-code of the compression in COMP128 algorithm

\[
\text{for } j = 0 \text{ to } 4 \text{ do } \{
    \text{for } k = 0 \text{ to } 2^j - 1 \text{ do } \{
        \text{for } l = 0 \text{ to } 2^{(4-j)} - 1 \text{ do } \{
            m = l + k \cdot 2^{(5-j)};
            n = m + 2^{(4-j)};
            y = (X[m] + 2 \cdot X[n]) \mod 2^{(9-j)};
            z = (2 \cdot X[m] + X[n]) \mod 2^{(9-j)};
            X[n] = T_j[y];
            X[m] = T_j[z];
        \}
    \}
\}
Partitioning Attack on COMP128

Values of $y$ and $z$ depend on the first bytes of $K$ and $R$.

It’s possible to detect via side channels whether values of $y$ and $z$ are within $[0..255]$ or $[256..511]$. 

$y = K[0] + 2R[0]$  
$z = 2K[0] + R[0]$
Partitioning Attack on COMP128

- All we need is...
  - A) Find $R[0]$ such that
    
    \[
    K[0] + 2R[0] \pmod{512} < 256
    \]
    
    \[
    K[0] + 2(R[0]+1) \pmod{512} \geq 256
    \]
    
    (There are only two options)
  - B) Find $R'[0]$ such that
    
    \[
    2K[0] + R'[0] \pmod{512} < 256
    \]
    
    \[
    2K[0] + R'[0] + 1 \pmod{512} \geq 256
    \]
  - C) One of $K[0]$ from A) will match B)

- The key byte is always uniquely determined from partitioning information.

- Computation of the others bytes of $K$ is similar.
Summary

• GSM Security Objectives
  – Concerns, Goals, Requirements
• GSM Security Mechanisms
• SIM Anatomy
• Algorithms and Attacks
  – COMP128
  – Partitioning Attack on COMP128