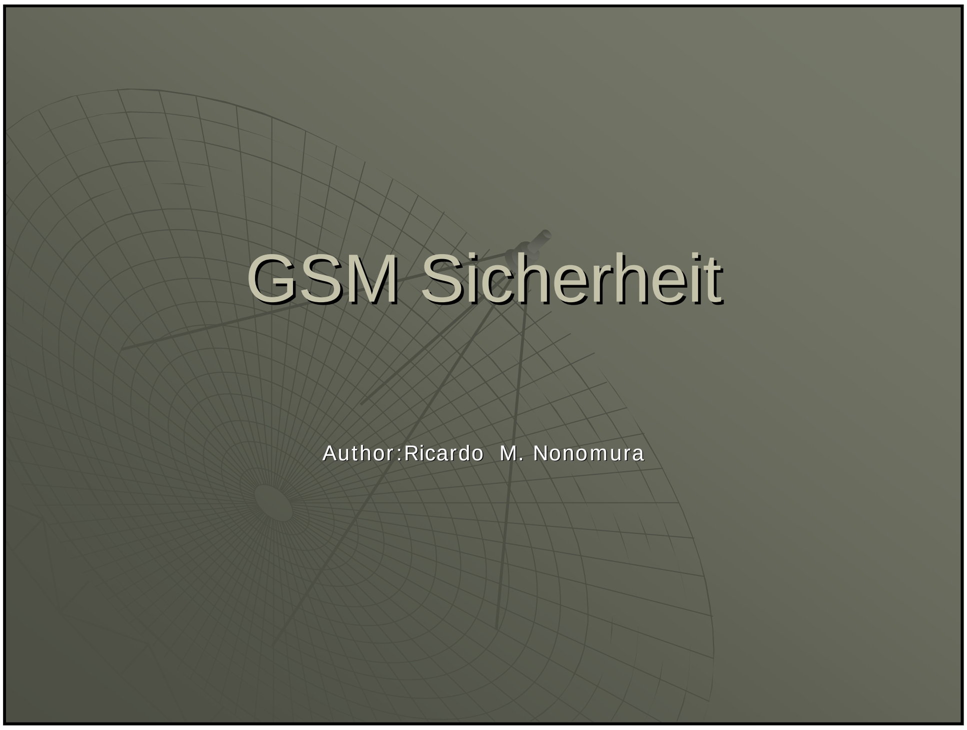
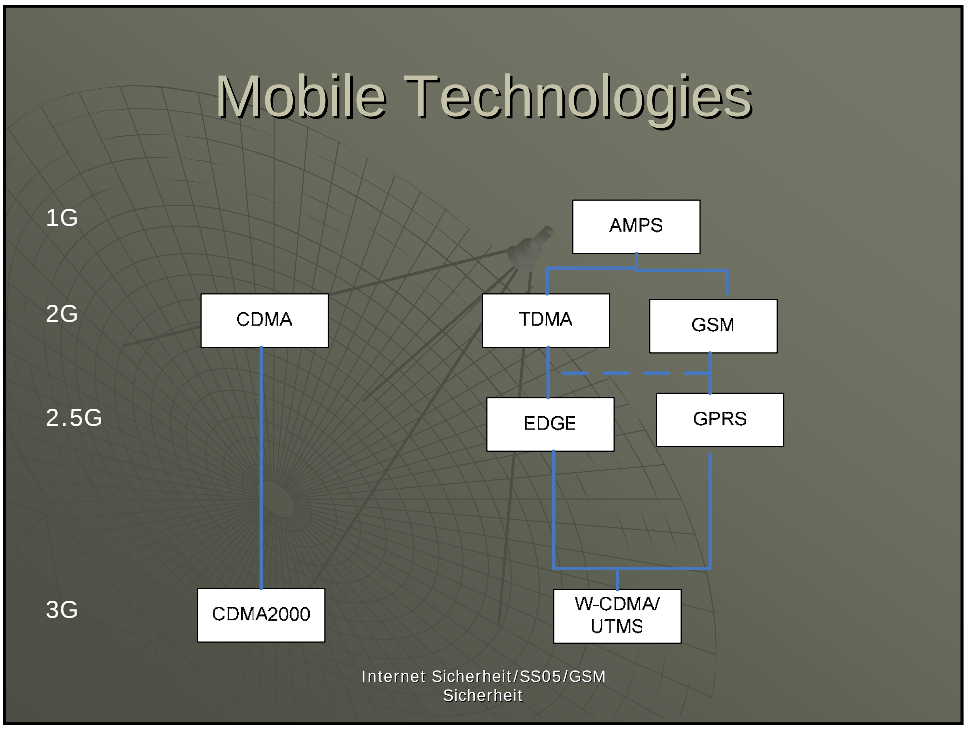


GSM Sicherheit

Author:Ricardo M. Nonomura



Mobile Technologies

1G

AMPS

2G

CDMA

TDMA

GSM

2.5G

EDGE

GPRS

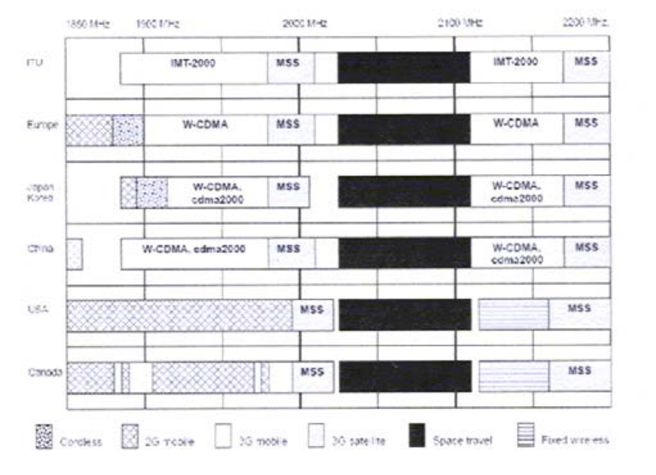
3G

CDMA2000

W-CDMA/
UTMS

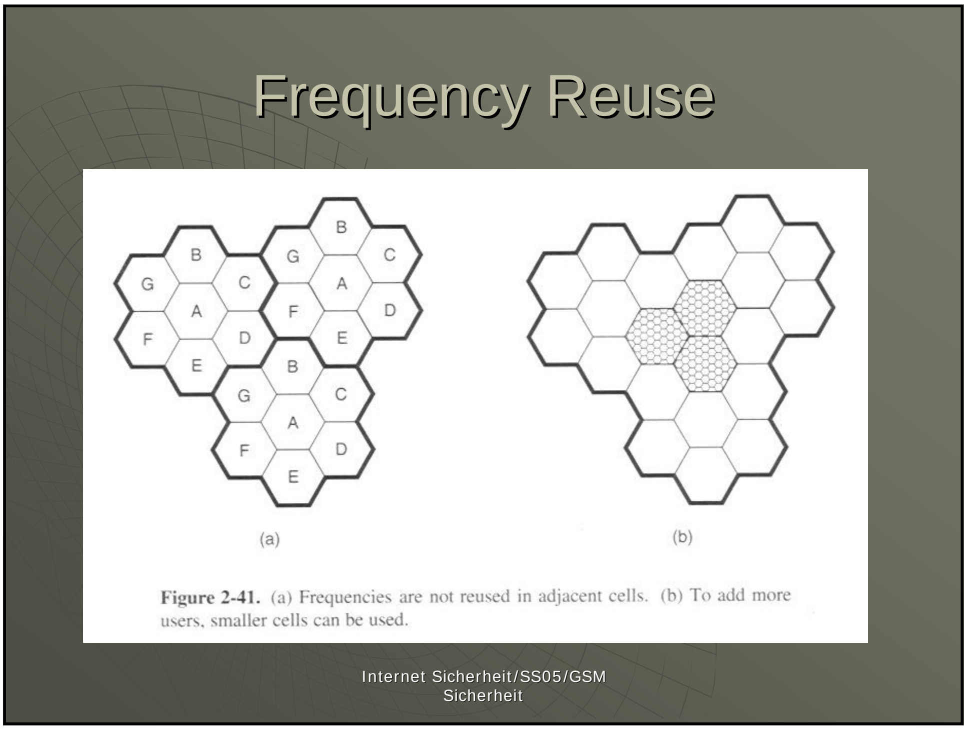
Internet Sicherheit/SS05/GSM
Sicherheit

Spektrum



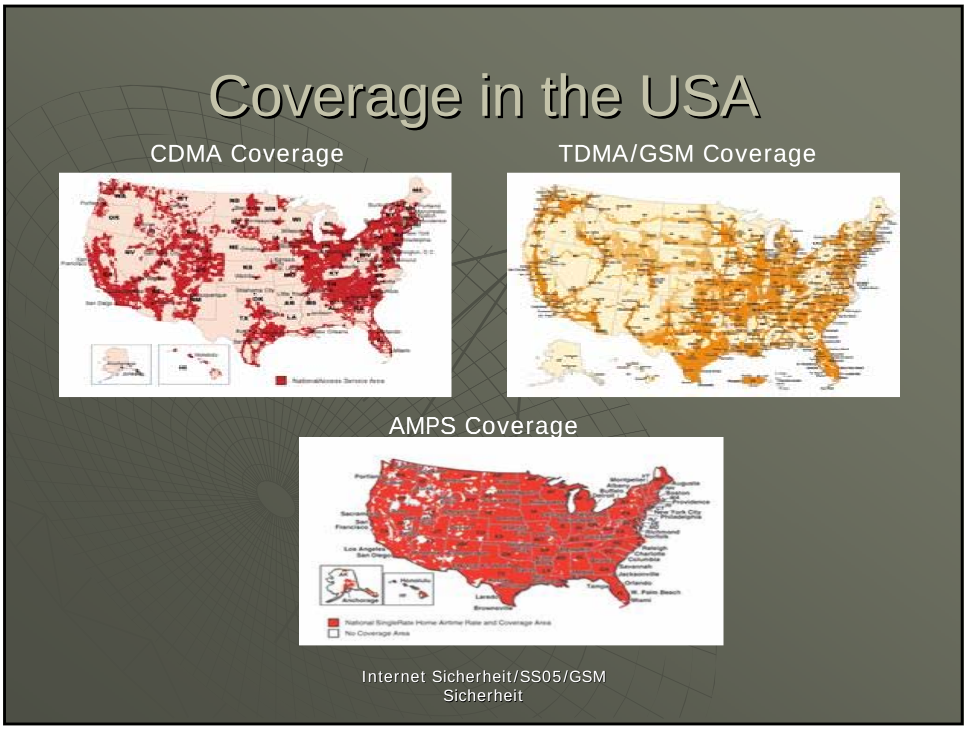
Band Usage

- AMPS (Advanced Mobile Phone System)
  - 832 duplex channels (practical 45 per BTS)
  - 824-849MHz (upload), 869-894MHz(download), 30KHz wide
- TDMA (Time Division Multiple Access)
  - 3-6 Users per channel
  - 1850-1910MHz (upload), 1930-1990MHz (download), 30KHz wide
- GSM (Global System for Mobile communications)
  - 8 Users per channel
  - 992 channels
  - 200KHz wide
- CDMA (Code Division Multiple Access)
  - 1.25MHz wide



Frequency Reuse

Figure 2-41. (a) Frequencies are not reused in adjacent cells. (b) To add more users, smaller cells can be used.

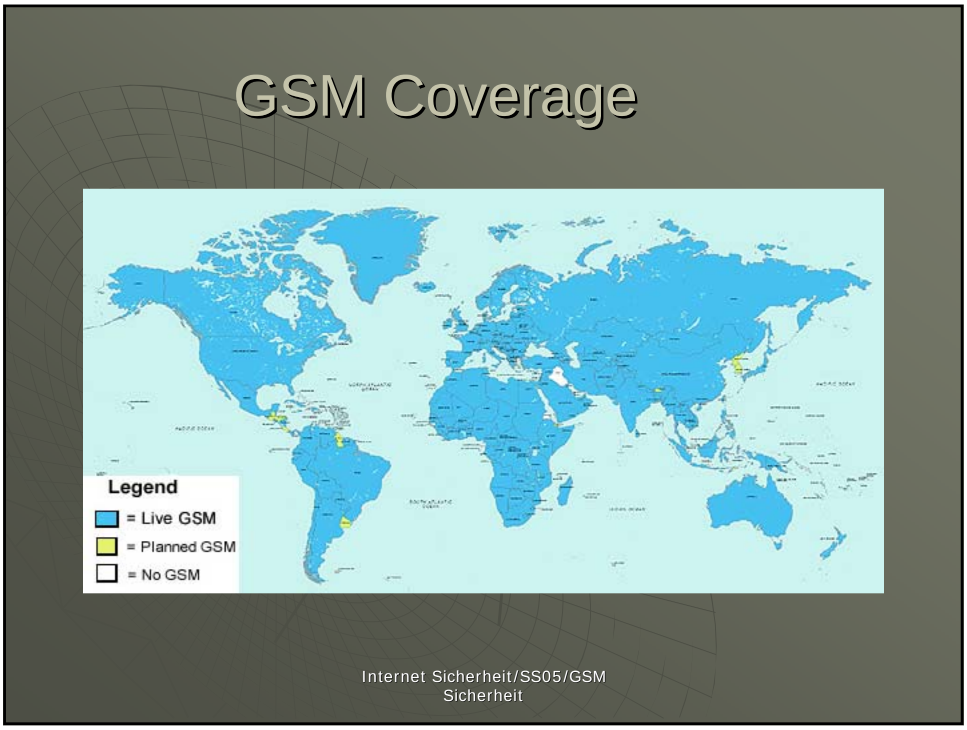


Coverage in the USA

CDMA Coverage

TDMA/GSM Coverage

AMPS Coverage



GSM Coverage

GSM Fakten

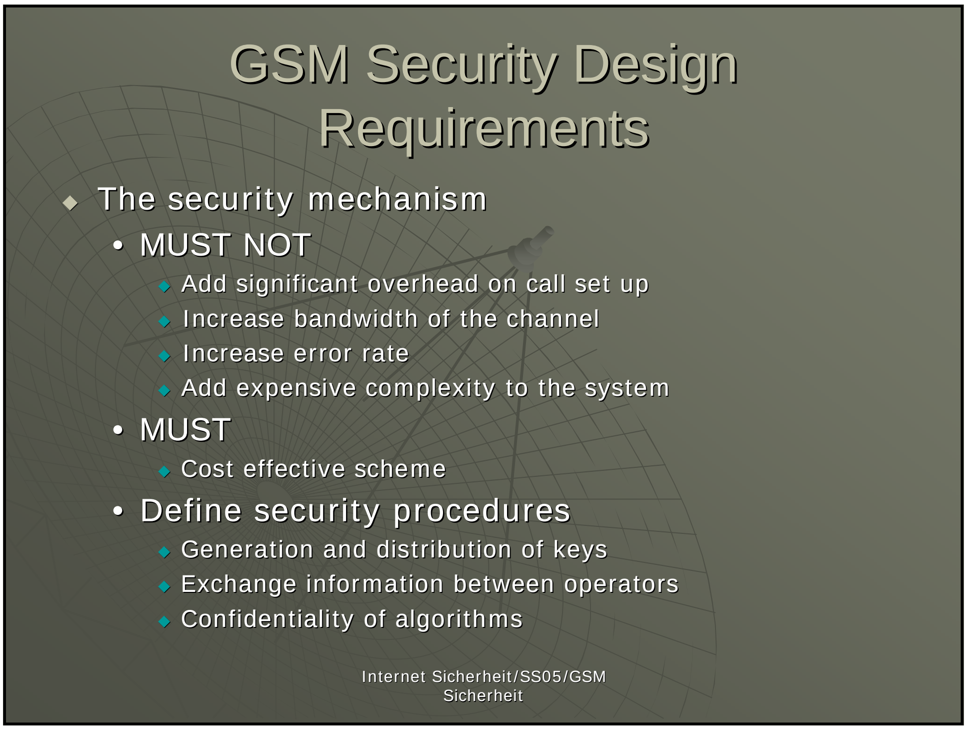
- Anfang: European Conference of Posts and Telecommunications Administrations (CEPT) – 1982;
- Groupe Spéciale Mobile -> Global System for Mobile Communications;
- 105 Länder;
- 32 Millionen Benutzern;
- 139 Netzwerken;
- 25% Handys Weltmarkt;

Eigenschaften:

- Verschlusselte Benutzerinformation;
- International Standard (einfachere Switching);
- Wenig Veränderung an existierende Festnetz;
- 2 Blockfrequenz in der 900MHz Bereich (890-915MHz und 935-960 MHz);
- Maximum Flexibilität für andere Dienste, wie ISDN;
- Möglichste geringe Kosten bei der Design von Handsets;

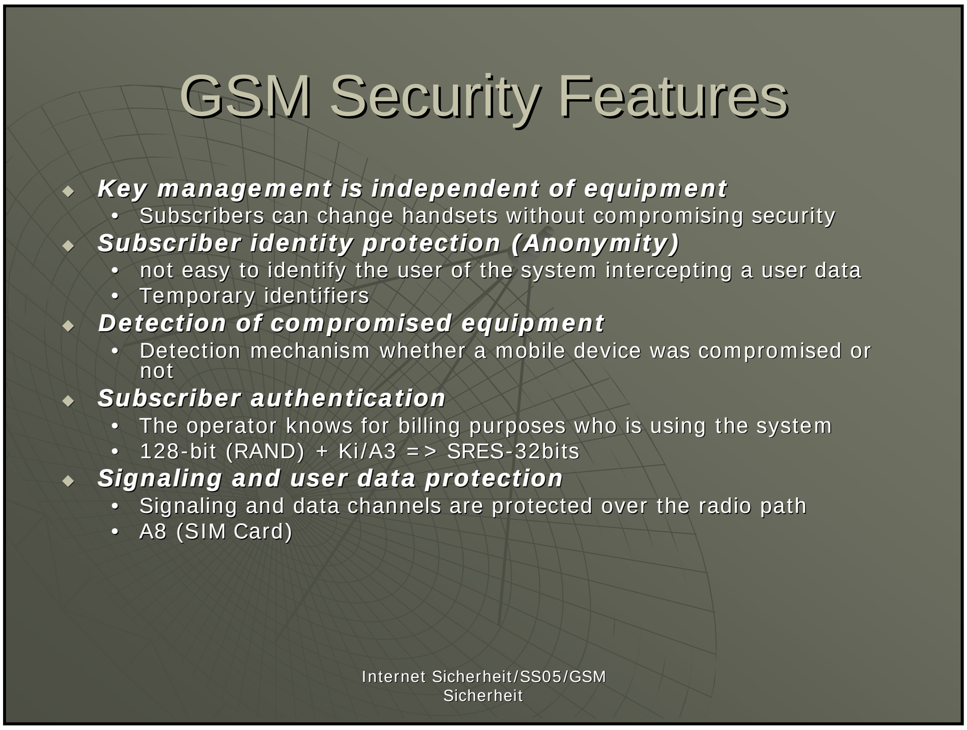
GSM Eigenschaften

- **Qualität:** digital: klar & deutliche Tone
- **Sicherheit:** Authentifizieren & Verschlusselt key distribution
- **Bequemlichkeit:** Batterie & Congestion
- **Roaming:** abhängig von Vertrag zwischen Operators



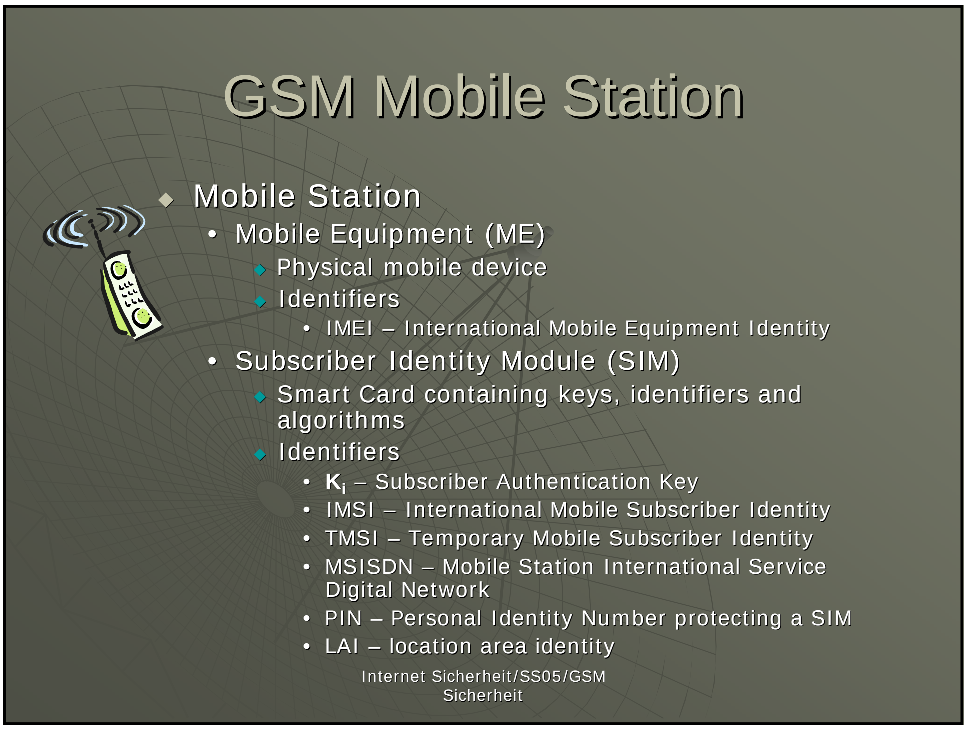
GSM Security Design Requirements

- 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



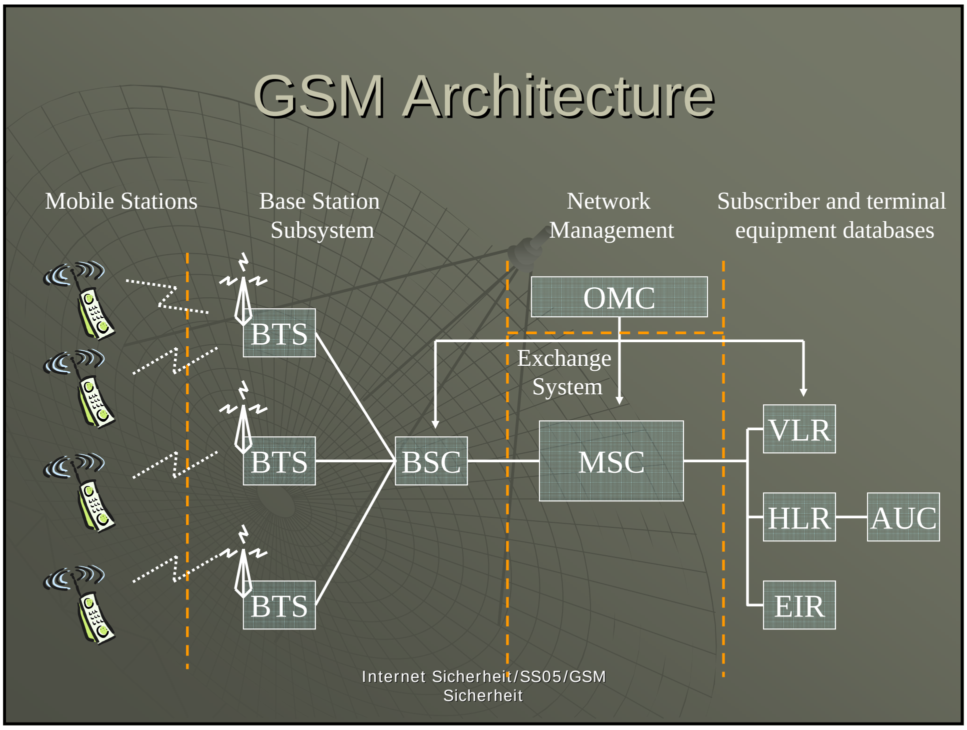
GSM Security Features

- ***Key management is independent of equipment***
  - Subscribers can change handsets without compromising security
- ***Subscriber identity protection (Anonymity)***
  - not easy to identify the user of the system intercepting a user data
  - Temporary identifiers
- ***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
  - 128-bit (RAND) + Ki/A3 => SRES-32bits
- ***Signaling and user data protection***
  - Signaling and data channels are protected over the radio path
  - A8 (SIM Card)



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

OMC

Exchange System

BTS

BTS

BTS

BSC

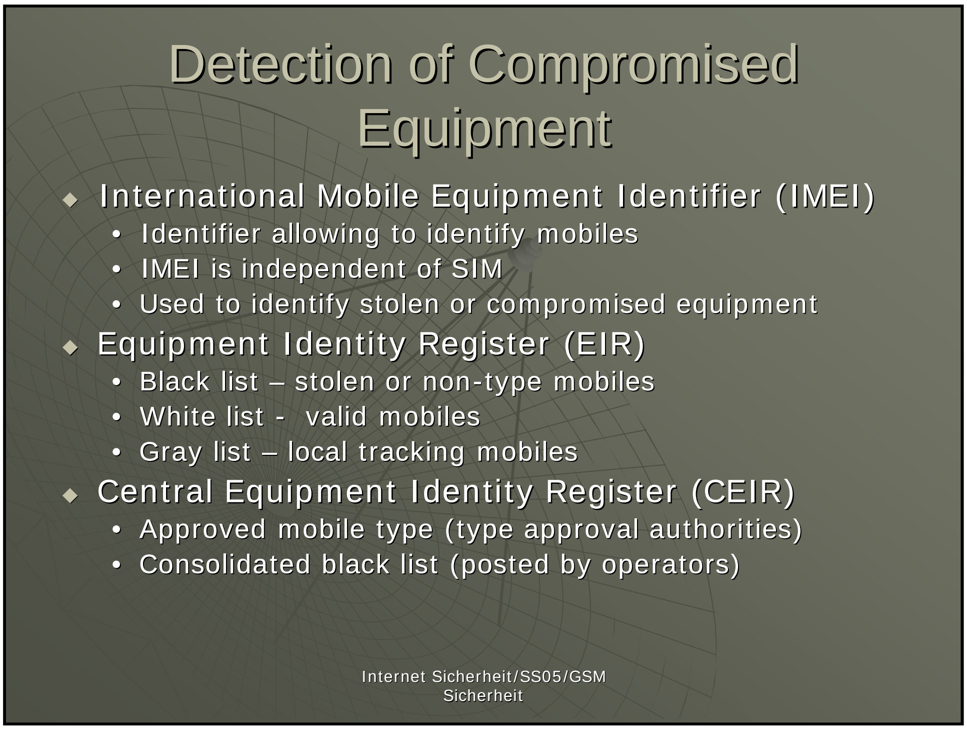
MSC

VLR

HLR

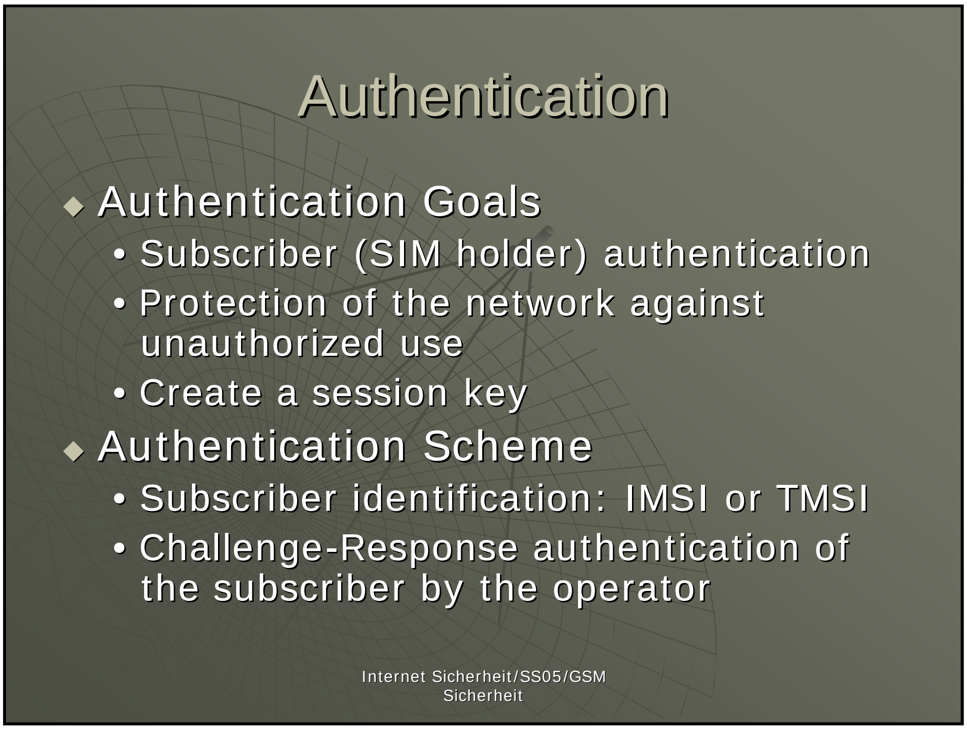
AUC

EIR



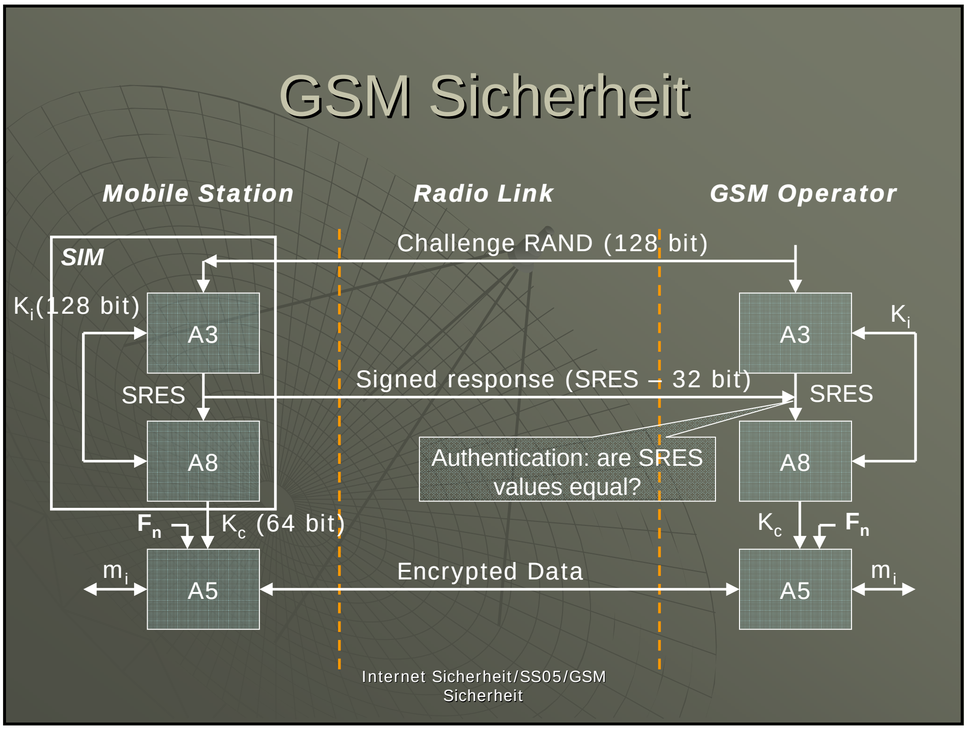
Detection of Compromised Equipment

- 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



GSM Sicherheit

Mobile Station

Radio Link

GSM Operator

SIM

Challenge RAND (128 bit)

K_i(128 bit)

A3

K_i

SRES

Signed response (SRES – 32 bit)

SRES

A8

Authentication: are SRES values equal?

A8

F_n

K_c (64 bit)

K_c

F_n

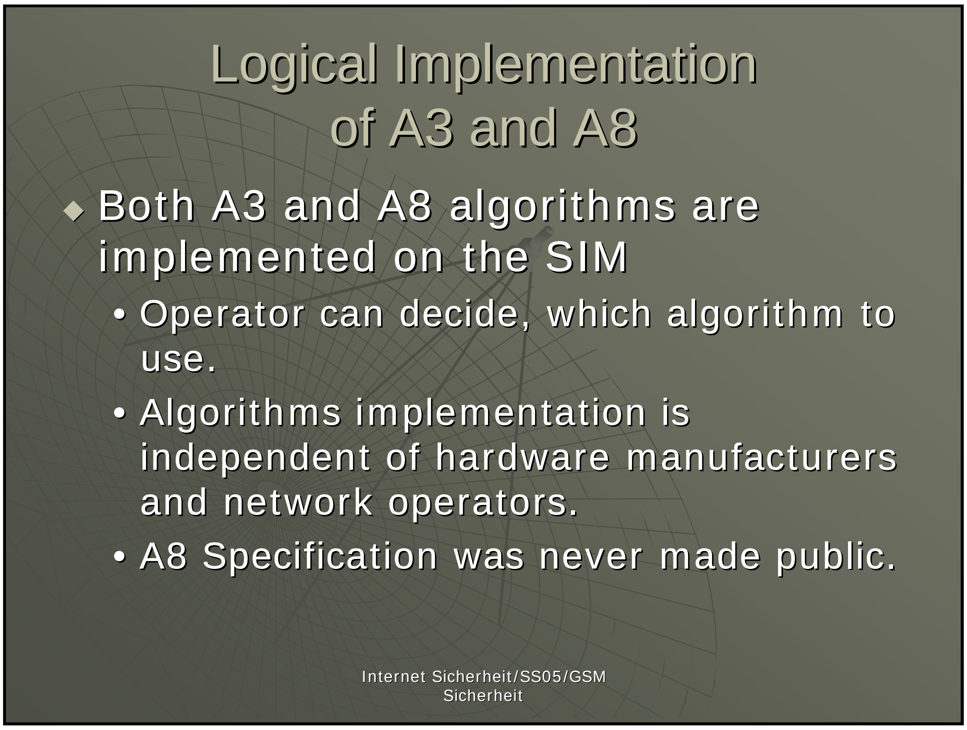
m_i

A5

Encrypted Data

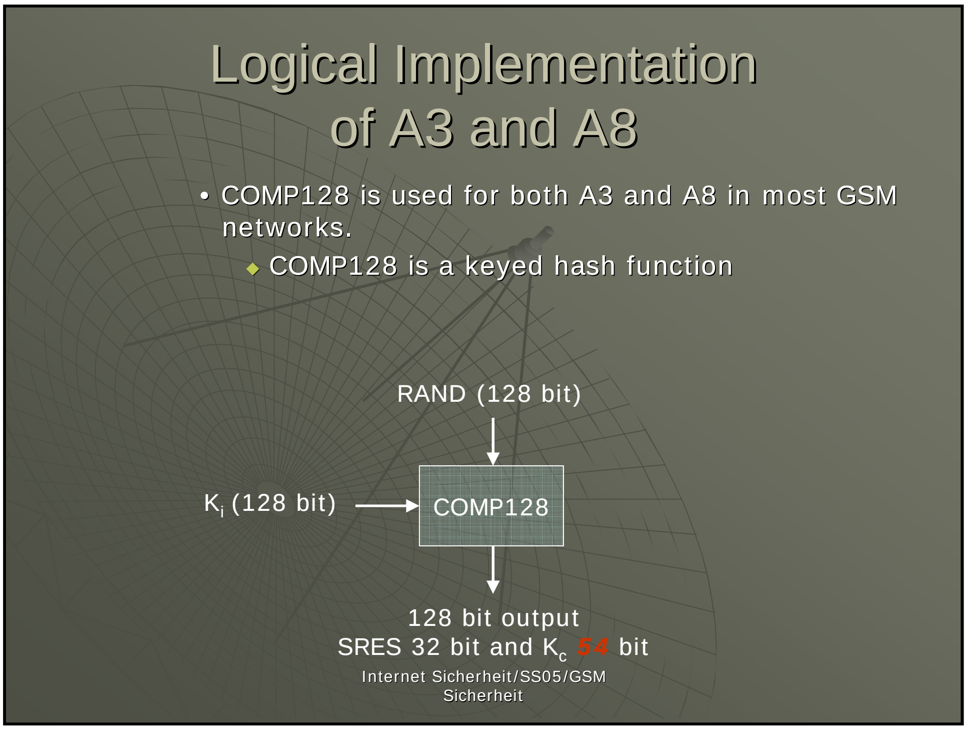
A5

m_i



Logical Implementation of A3 and A8

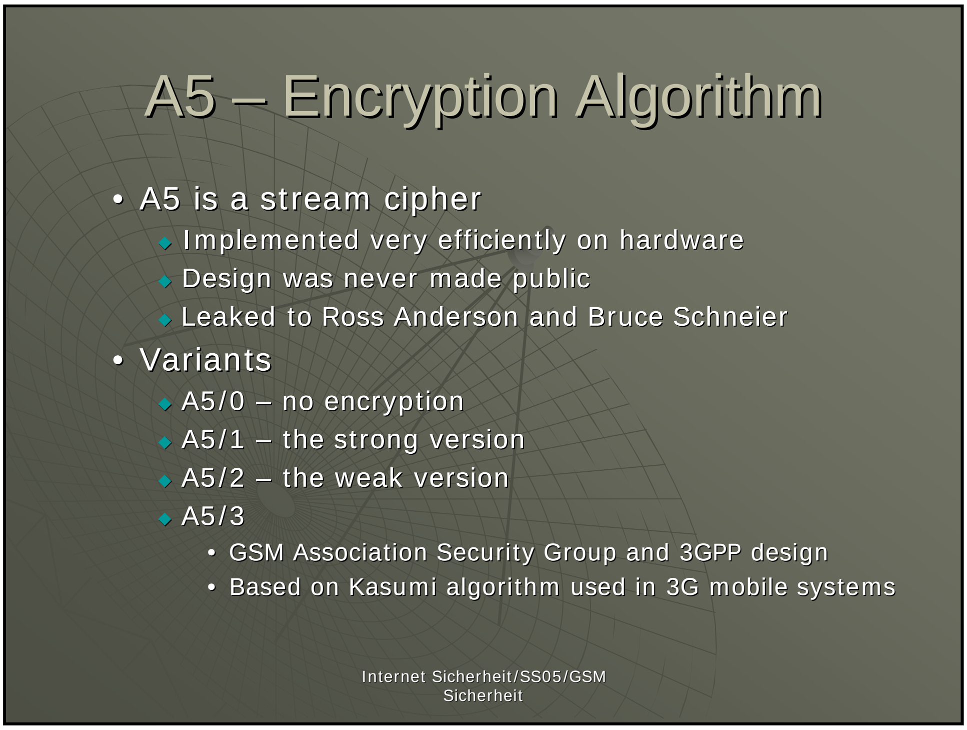
- Both A3 and A8 algorithms are implemented on the SIM
  - Operator can decide, which algorithm to use.
  - Algorithms implementation is independent of hardware manufacturers and network operators.
  - A8 Specification was never made public.



Logical Implementation of A3 and A8

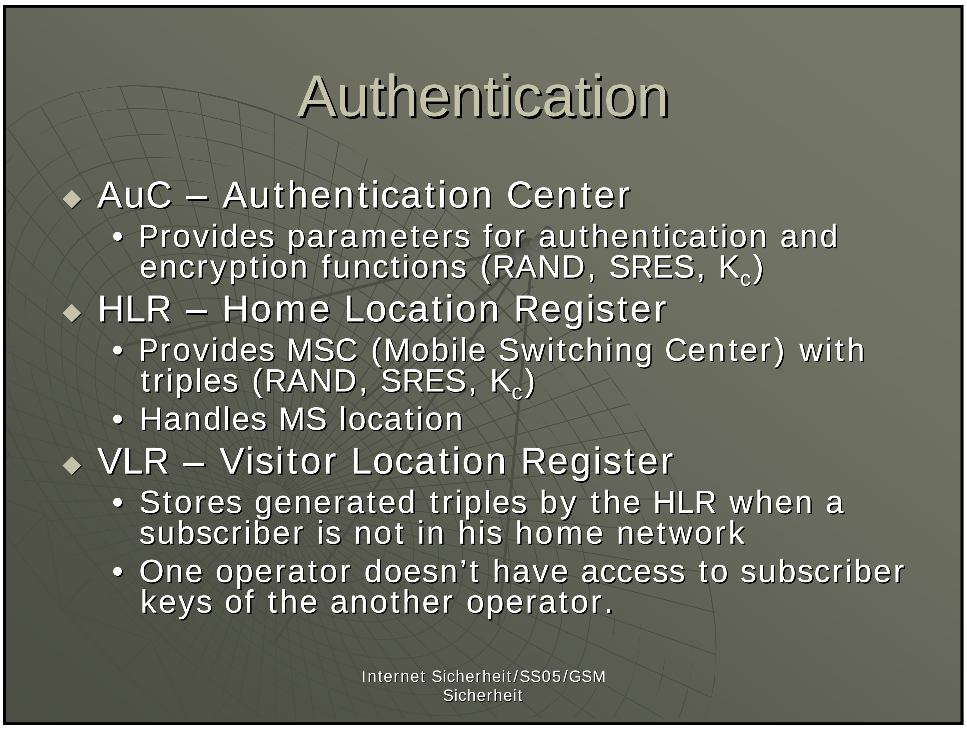
- COMP128 is used for both A3 and A8 in most GSM networks.
  - COMP128 is a keyed hash function

128 bit output
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
  - A5/0 – no encryption
  - 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



Authentication

- AuC – Authentication Center
  - Provides parameters for authentication and encryption functions (RAND, SRES, K_c)
- HLR – Home Location Register
  - Provides MSC (Mobile Switching Center) with triples (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.

SIM Anatomy

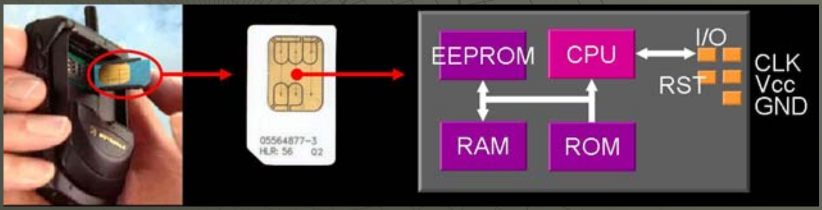
Subscriber Identification Module (SIM)

Smart Card – a single chip computer containing OS, File System, Applications

Protected by PIN

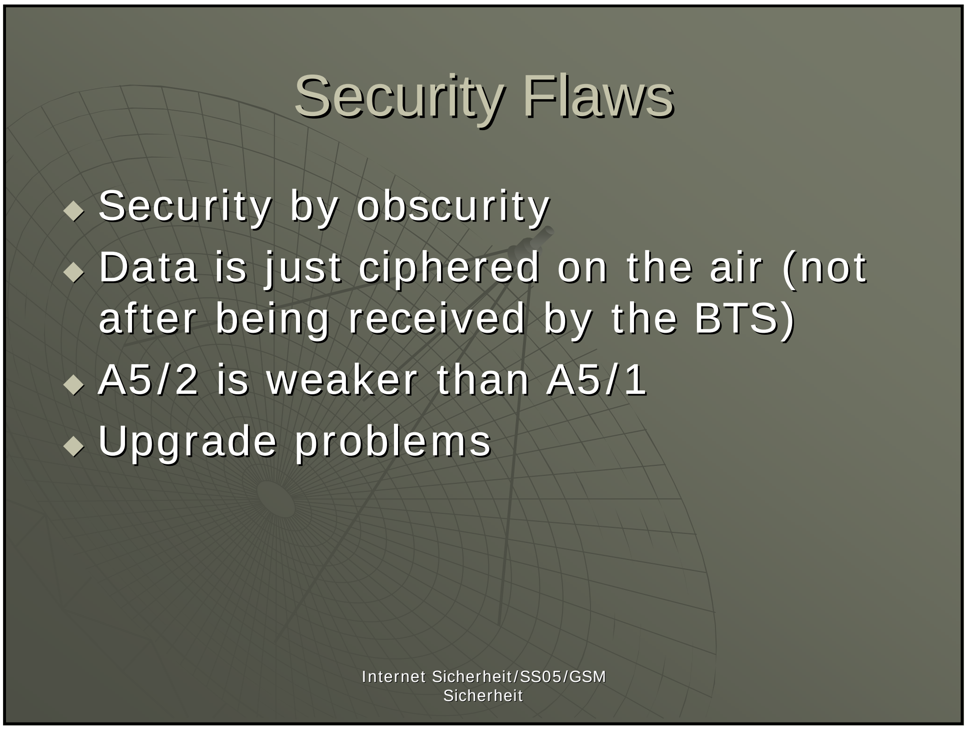
Owned by operator (i.e. trusted)

SIM applications can be written with SIM Toolkit



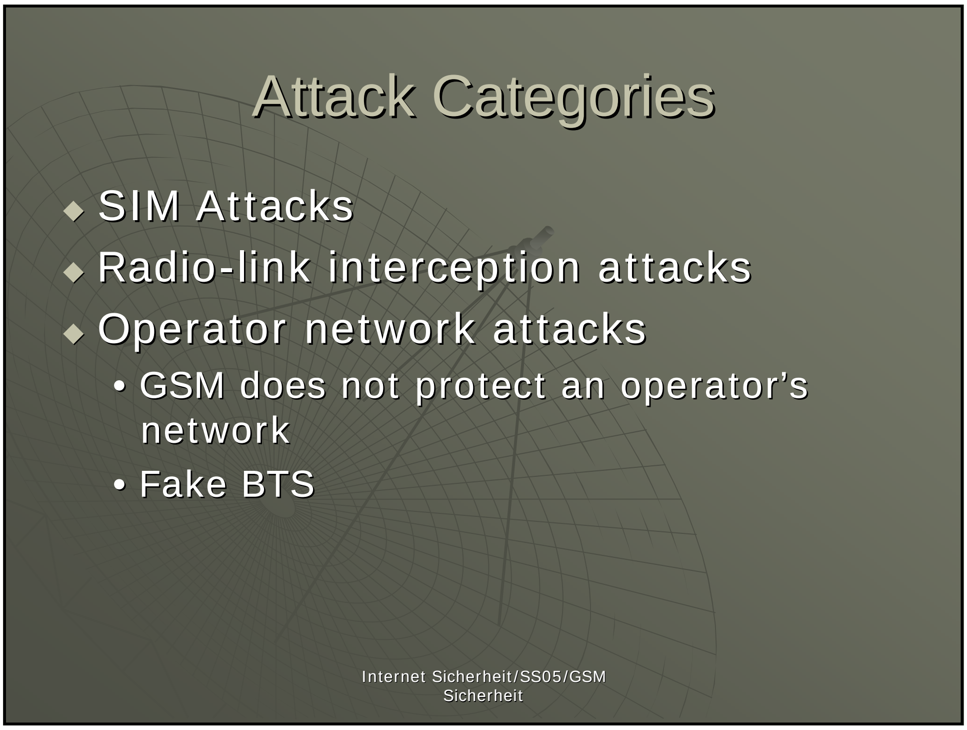
Microprocessor Cards

- 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



Security Flaws

- Security by obscurity
- Data is just ciphered on the air (not after being received by the BTS)
- A5/2 is weaker than A5/1
- Upgrade problems



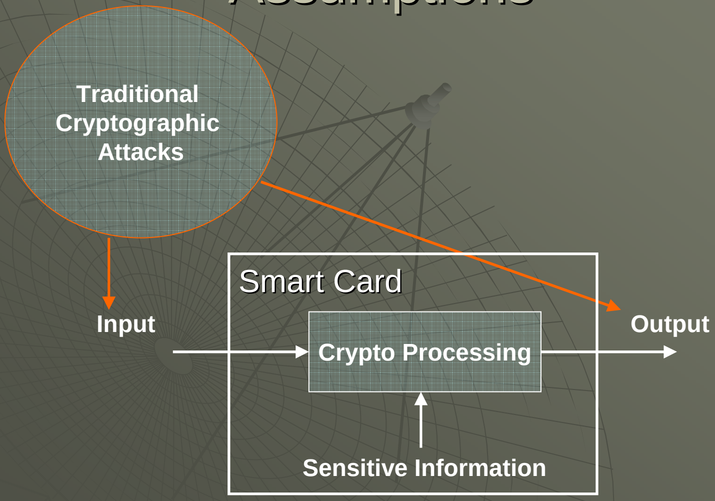
Attack Categories

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

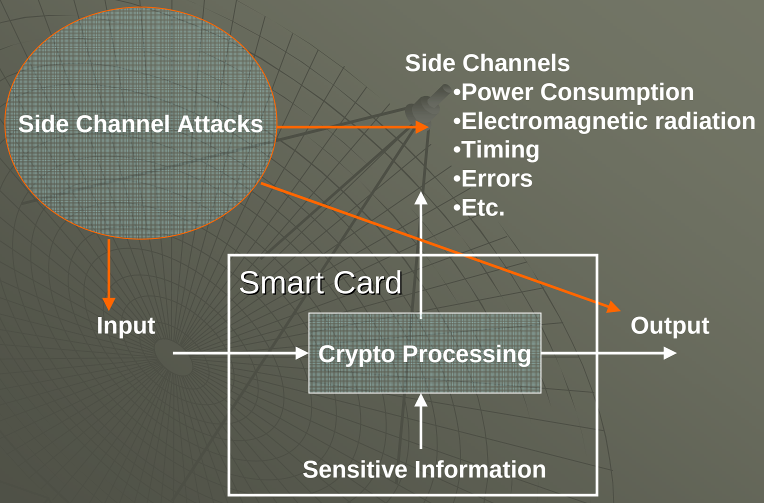
Attack History

- 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 Kc uses only 54 bits.
- August 1999
  - The weak 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.

Traditional Cryptographic Assumptions



Actual Information Available



Side Channel Attacks

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

Smart Card

Input

Crypto Processing

Output

Sensitive Information

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

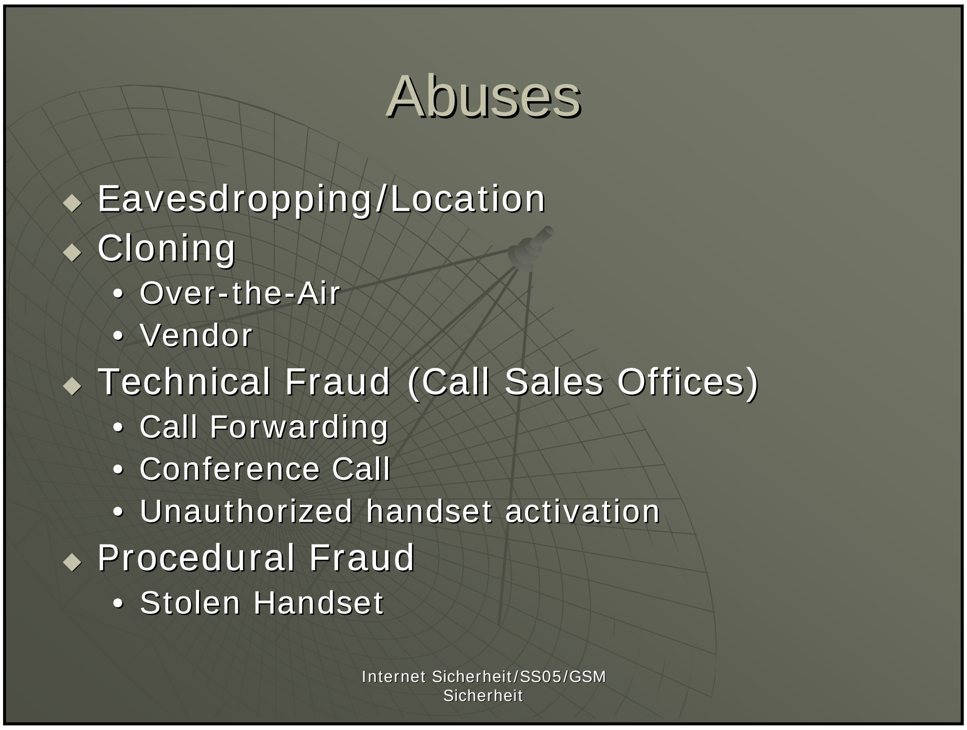
GSM Interceptor Pro System

Features:

8 channels 900/1800 MHz,
(System with 1900 MHz is also available).
The system can target specific numbers or
randomly screen GSM mobile
Communication.
Conversations are monitored and logged
simultaneously to voice and data logger for
storage and retrieval..
Housed in industrial PC 19” rack mounted
portable cabinet with attached keyboard and
LCD monitor. Weight:12 Kg about 23 Lb.
Decodes voice codes LPT, RPE and EFR.
Works with identificators IMSI, TMSI, IMEI,
and MSISDN.
Can receive BCCH, CCCH, SACCH, SDCCH,
FACCH, and TCH.
Find incoming call number when call ID is
available.
Intercept 1 voice duplex Channel.
Possibility to receive SMS Messages.
Working range: Forward Channel 25 KM or
15.6 Miles, Reverse Channel depends on
conditions - varies from 300 to 800 meters,
or up to half a mile.
If unidirectional antennas are used, the
range can be increased.

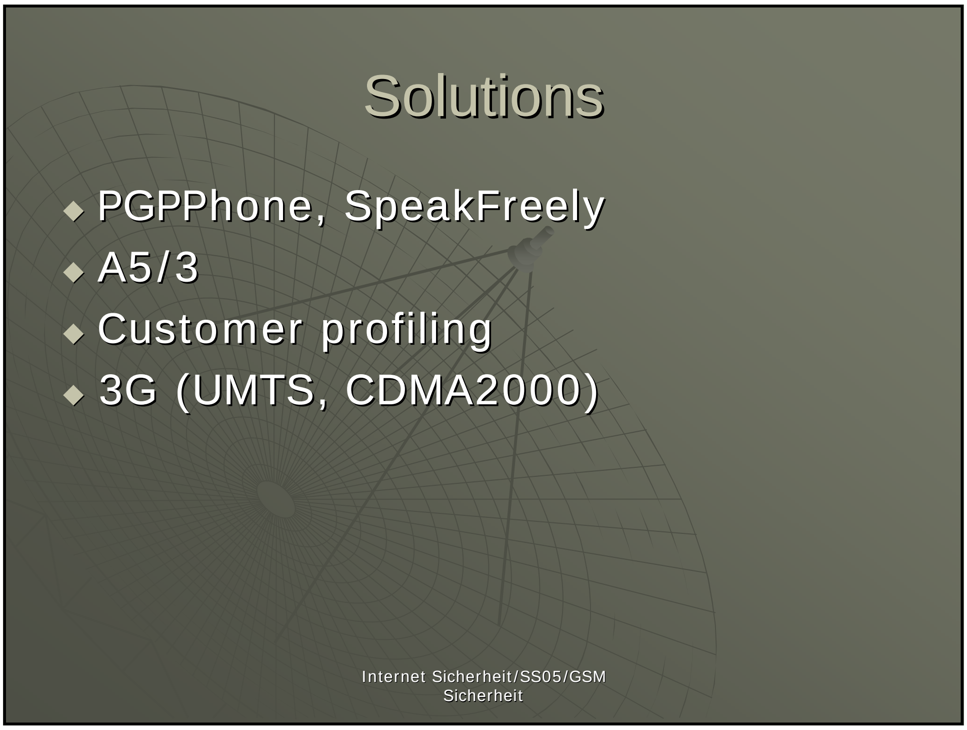
GSM Interceptor Pro System

- **Encryption Modes:**
  A5.2 cooperation with network operator is not needed, the system works in real time.
  A5.1 If cooperation with network operator is possible, the system works in real time.
  If cooperation with network operator is not possible but there is an access to mobile phone, information can be extracted directly from SIM card, Extraction time – 15 Min., SIM card scanner should be added to the system.
  With special hardware and software module A5.1 Decoder the interceptor works without cooperation with network operator.
- **Off The Air GSM Cellular Monitoring System - GENERAL DESCRIPTION:**
  The GSM Cellular Monitoring System is an advanced OFF AIR monitoring system designed to intercept and track all cellular traffic, within a city or region operating according to GSM standards. The system tracks up to 1000 simultaneous conversations and provides voice monitoring and call information display, at a central monitoring station. This unit is the latest addition to our complete line of monitoring systems.
- **SYSTEM FEATURES:**
  * Real time, off air interception of the regional GSM Mobile Telephone network, including data and fax transmissions.
  * Intercept up to 1000 lines of traffic simultaneously.
  * System can randomly screen GSM Mobile communication, with the ability to monitor and record traffic.
  * System can Target specific Numbers Of Interest on the GSM network.
  * Conversations can be monitored and logged simultaneously to a high capacity digital voice and data logger for storage and retrieval.
  * GSM mobile telephone calls can be tracked and followed from a central control station.
  * Central Command and control center can be located in your facility or headquarters.
  * Base system is compact and housed in a 24" rack mounted portable cabinet.
  * System is user friendly, operates with windows platform, and a powerful graphical user interface, enabling the user to master the system after just a few hours of training.
- **GSM Interceptor Pro System**
  Item: 4001-D ------------------------------------
  $420,000.00 (depends on configuration)



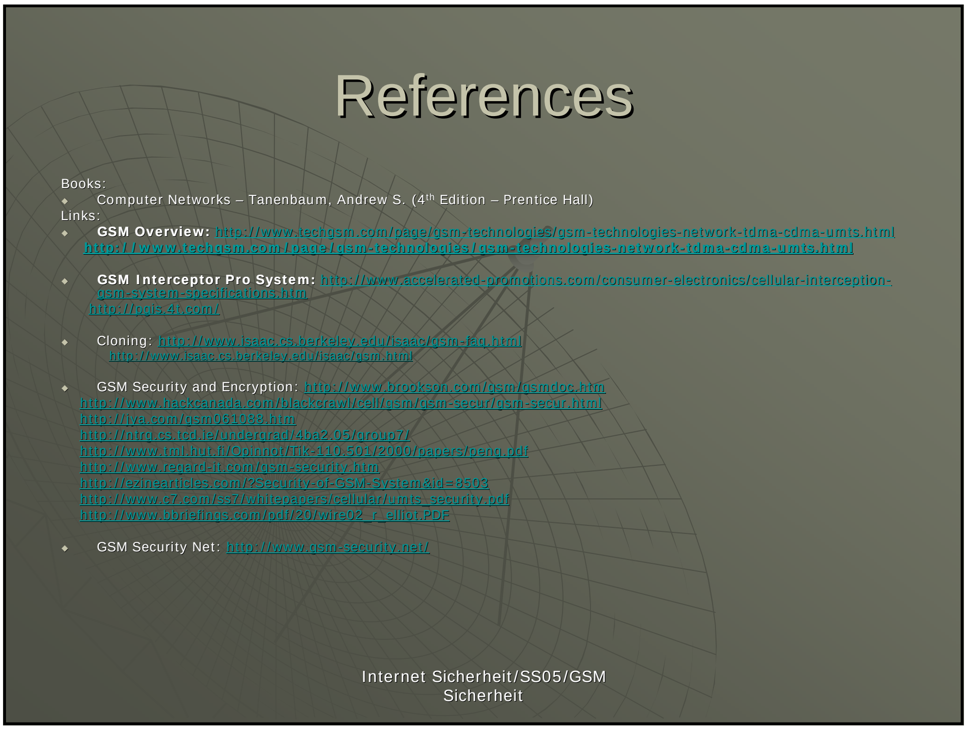
Abuses

- Eavesdropping/Location
- Cloning
  - Over-the-Air
  - Vendor
- Technical Fraud (Call Sales Offices)
  - Call Forwarding
  - Conference Call
  - Unauthorized handset activation
- Procedural Fraud
  - Stolen Handset



Solutions

- PGPPhone, SpeakFreely
- A5/3
- Customer profiling
- 3G (UMTS, CDMA2000)



References

Books:

- Computer Networks – Tanenbaum, Andrew S. (4th Edition – Prentice Hall)

Links:

- **GSM Overview:** http://www.techgsm.com/page/gsm-technologies/gsm-technologies-network-tdma-cdma-umts.html
  http://www.techgsm.com/page/gsm-technologies/gsm-technologies-network-tdma-cdma-umts.html
- **GSM Interceptor Pro System:** http://www.accelerated-promotions.com/consumer-electronics/cellular-interception-gsm-system-specifications.htm
  http://pgis.4t.com/
- Cloning: http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html
  http://www.isaac.cs.berkeley.edu/isaac/gsm.html
- GSM Security and Encryption: http://www.brookson.com/gsm/gsmdoc.htm
  http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html
  http://jya.com/gsm061088.htm
  http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/
  http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers/peng.pdf
  http://www.regard-it.com/gsm-security.htm
  http://ezinearticles.com/?Security-of-GSM-System&id=8503
  http://www.c7.com/ss7/whitepapers/cellular/umts_security.pdf
  http://www.bbriefings.com/pdf/20/wire02_r_elliot.PDF
- GSM Security Net: http://www.gsm-security.net/