Mobile Communication Security

Shahriar Bijani

Informatics School, Edinburgh University

Mar 2012

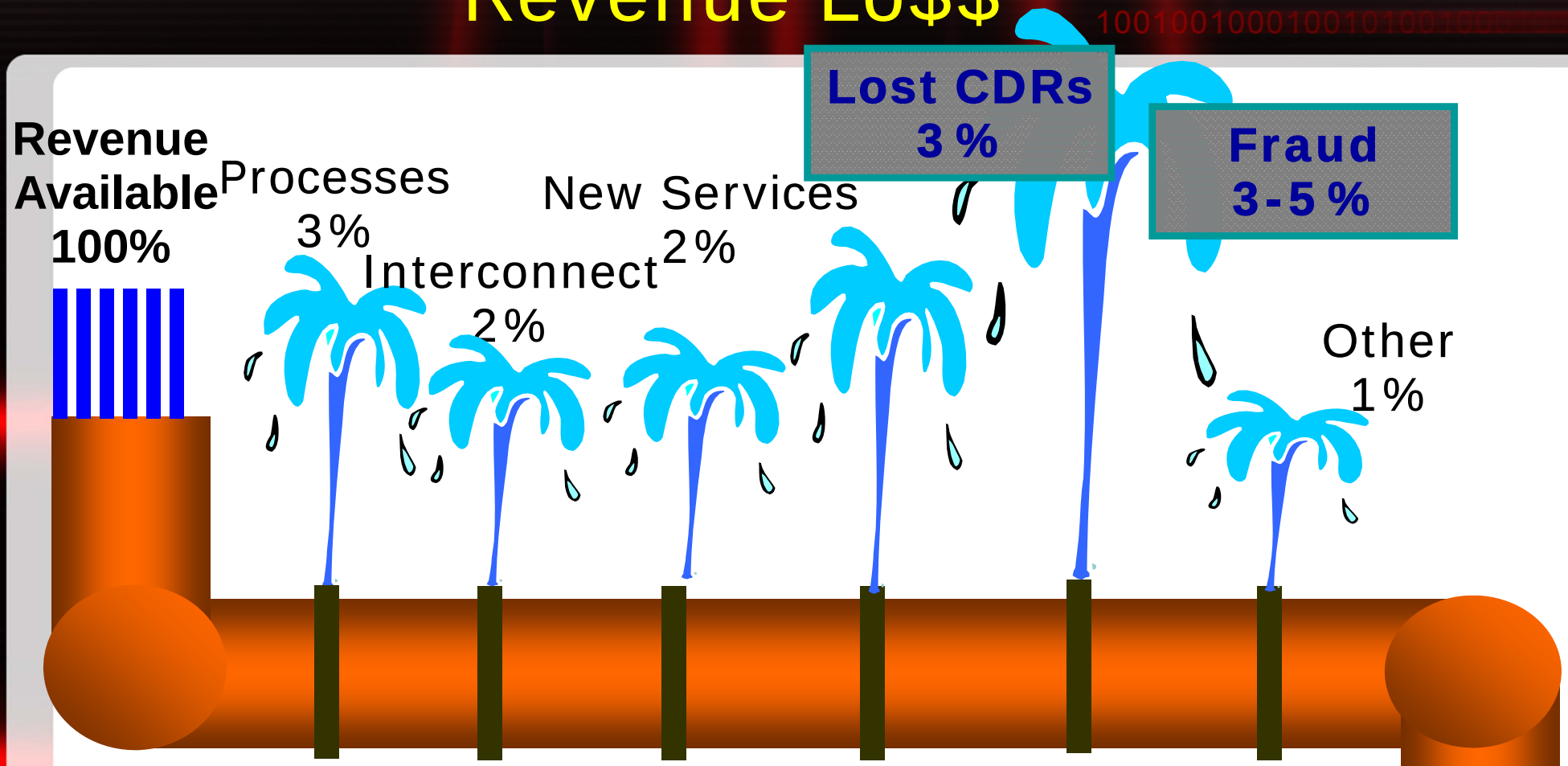
Outline

- **Why Security is Important?**
- Mobile Network Technologies
- Security Mechanisms in GSM
- GSM Security Vulnerabilities

Mobile Communication Fraud Stats

- Sources of the Stats
  - Governments
  - Mobile Operators
  - International Organisations (e.g. CTIA, CFCA, …)
- Estimated Communication Fraud Costs
  - 1997: %4-%6 of the operators' revenue
  - 2000: %5 of the operators' revenue ~ $13M
  - 2011: 40 Billion $
- **Communication fraud gives more income than drug trafficking!**

Revenue Lo$$



EXTRA!!! The Times EXTRA!!!

Average leakage of 1%
= $8 million/telco (PWC)

Lost Revenue

$$$$ £££

%%

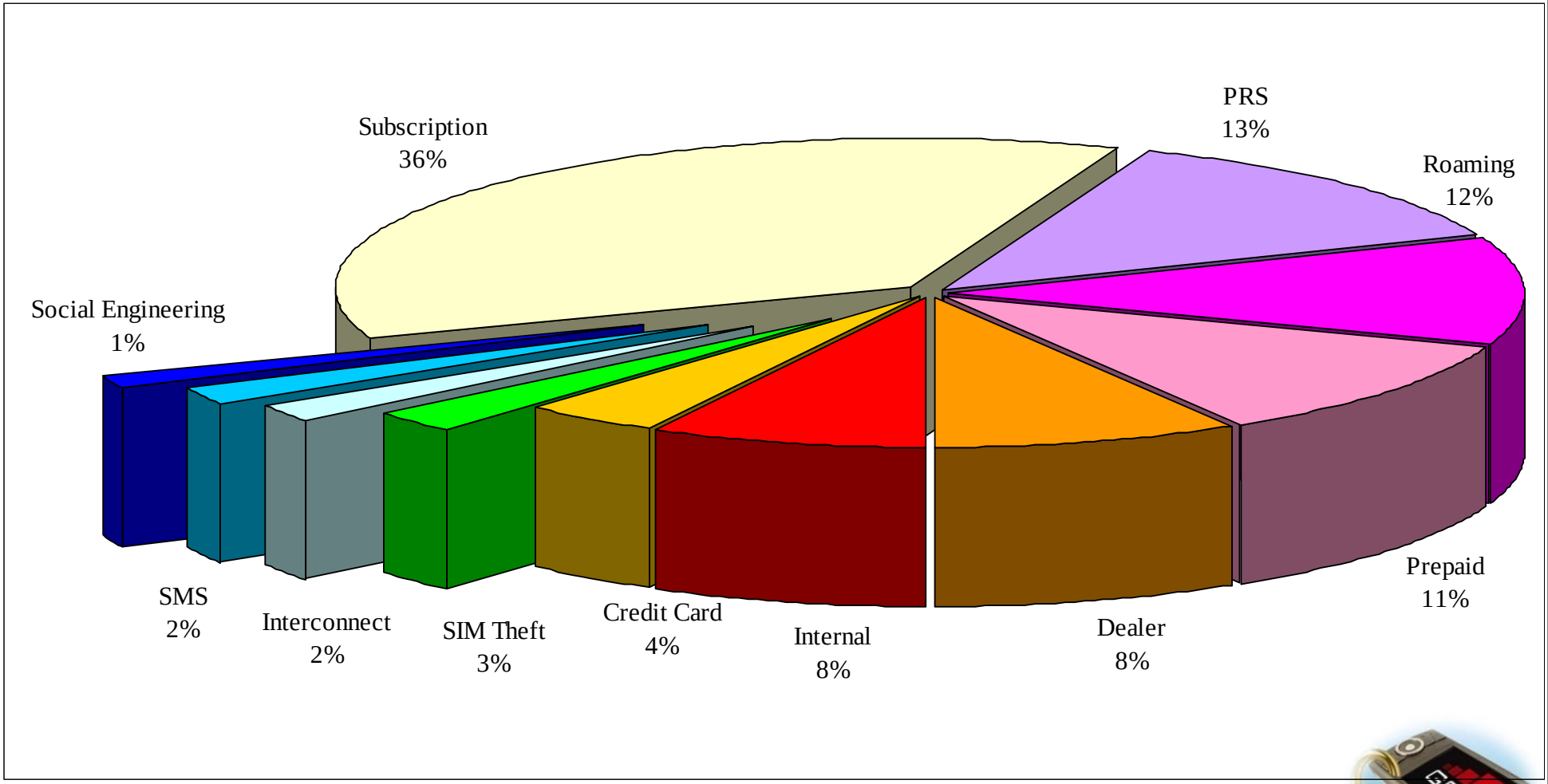
Revenue Realized <100%

Source: Analysis Survey for BT: representative sample of telecom providers around the world.

Mobile Communication Fraud Stats

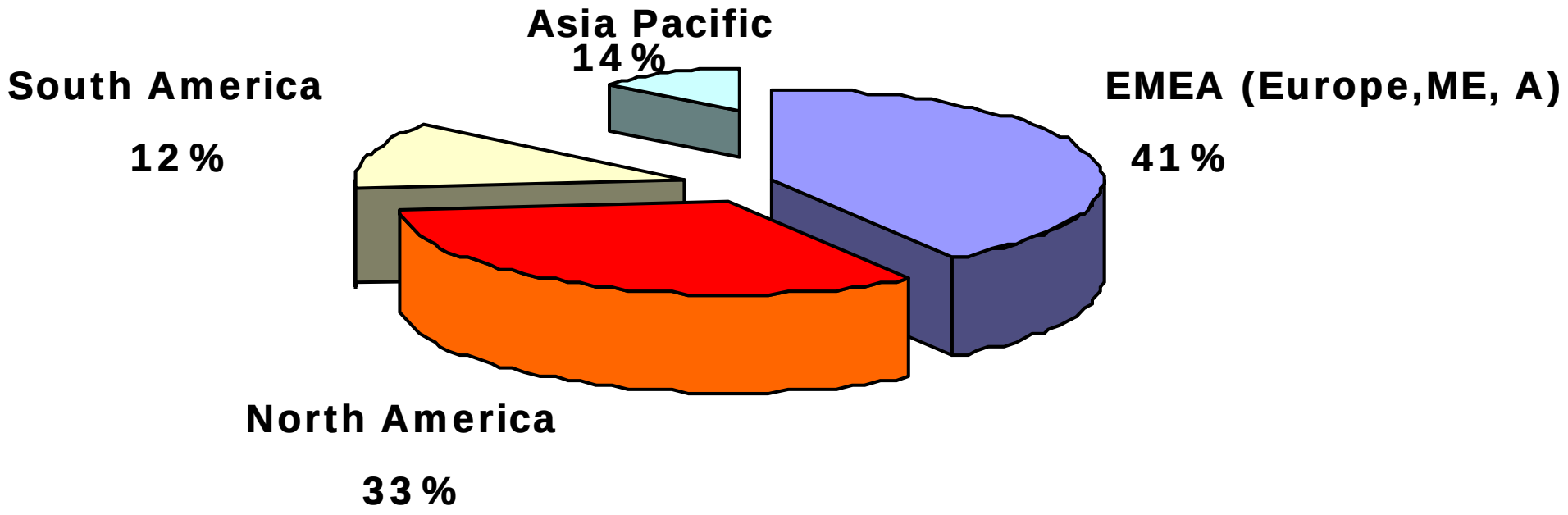
GSM Mobile Network Fraud

Source: Communications Fraud Control Association, www.cfca.org



Mobile Communication Fraud Stats

Geographical Distribution of the Mobile Networks Fraud



Source: Chorleywood Consulting

Outline

- Why Security is Important?
- **Mobile Network Technologies**
- Security Mechanisms in GSM
- GSM Security Vulnerabilities

Mobile Network technologies

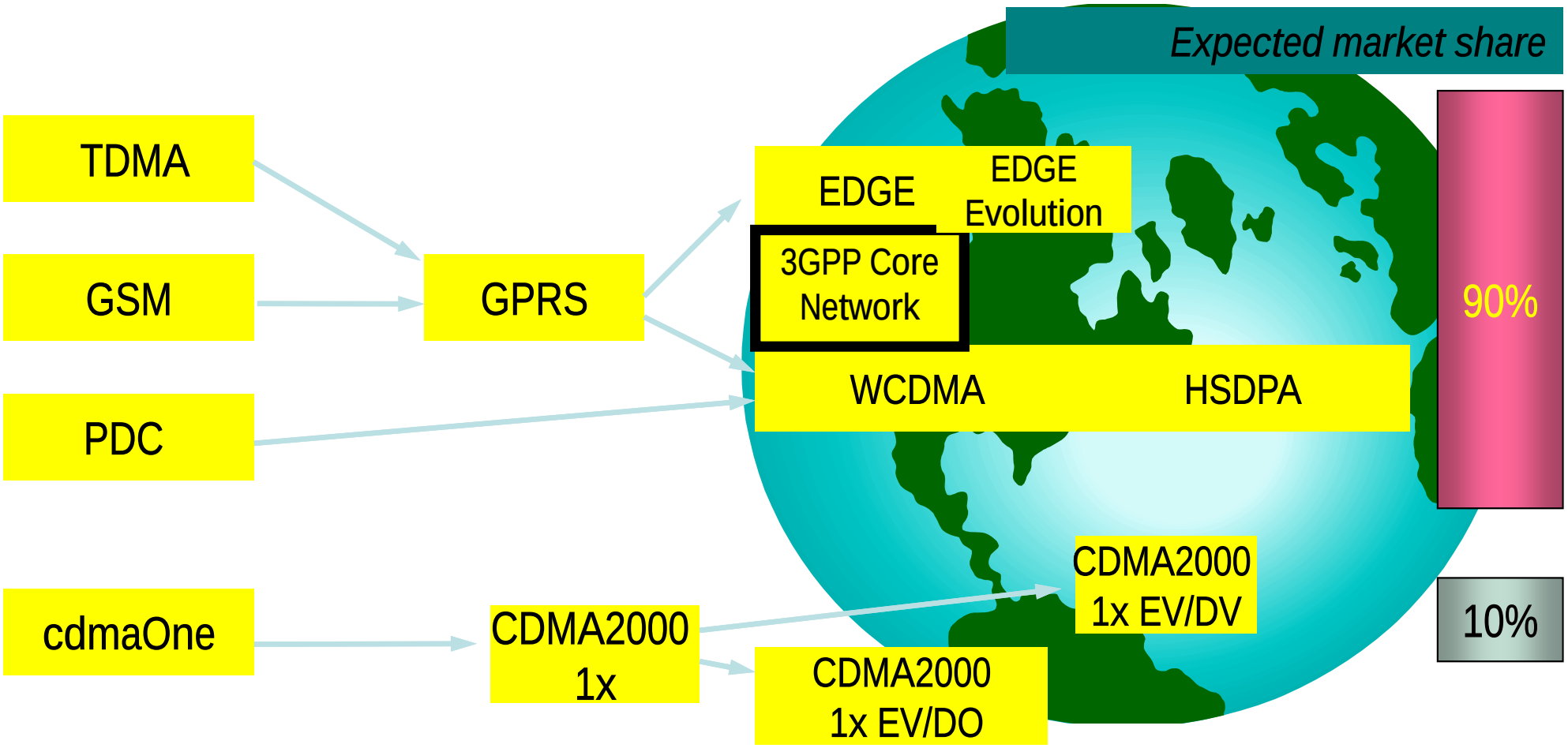
- **2G:** GSM (1990-1)

  (2010: *GSM Association* estimates that technologies defined in the GSM standard serve 80% of the global mobile market, encompassing more than 5 billion people)
- **2.5 G:** GPRS, …
- **3G**: UMTS (2001)

  (+ %15)
- **4G:** LTE Advanced (2011)
  - Services will roll out in 2013 in the UK

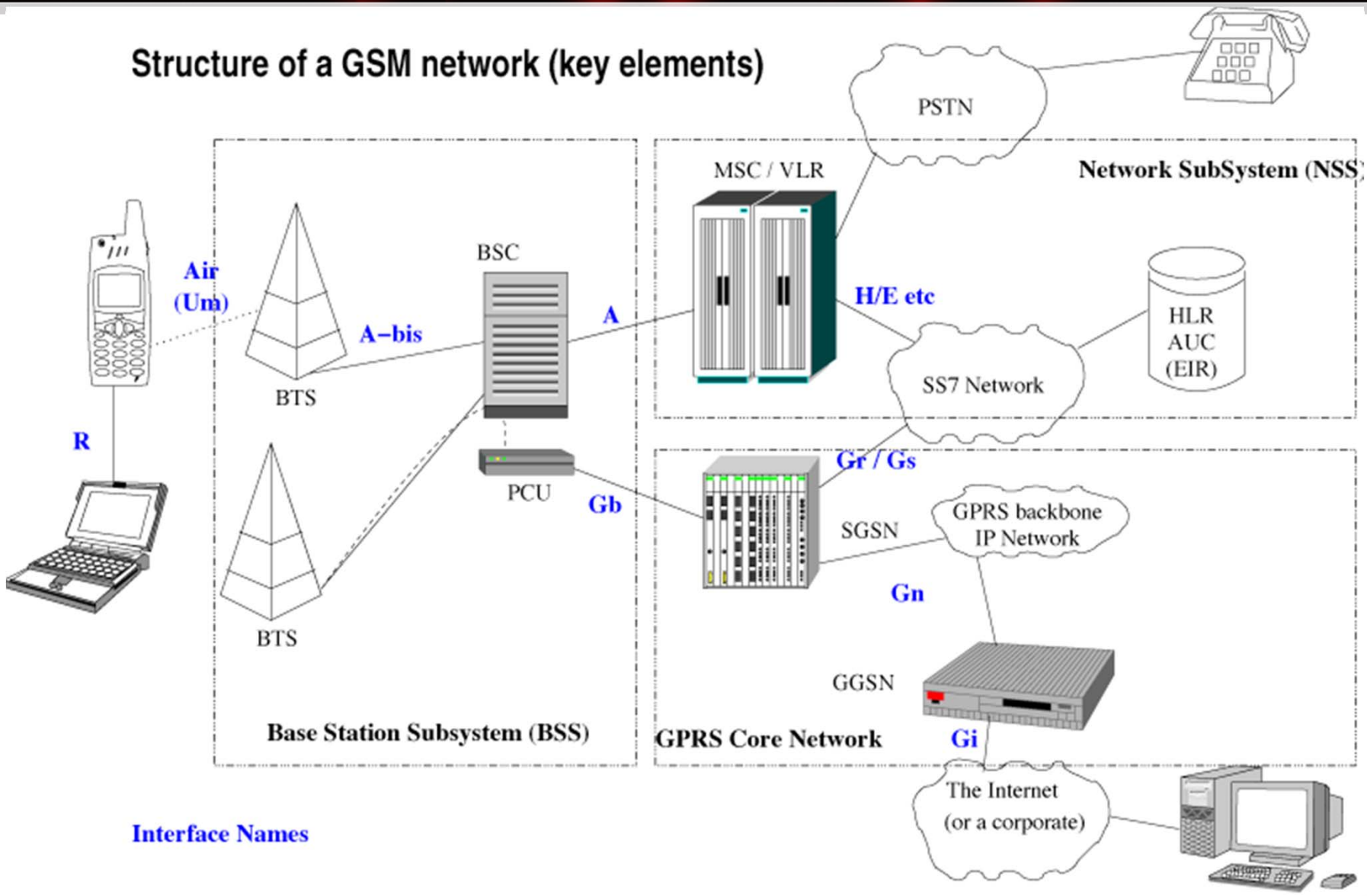
Evolution of Mobile Systems to 3G

- drivers are capacity, data speeds, lower cost of delivery for revenue growth



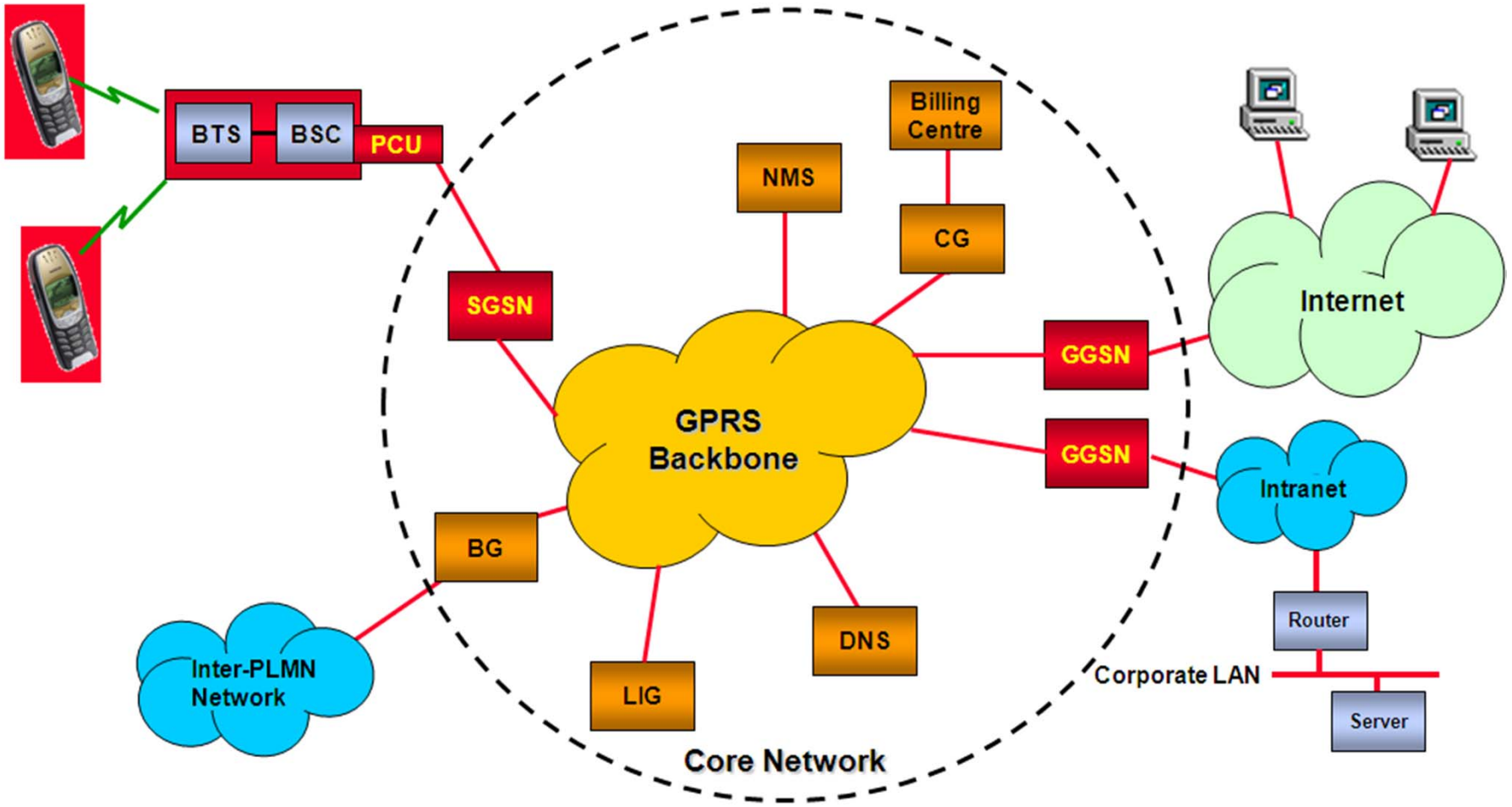
Source: ICIL

GSM and GPRS Architecture

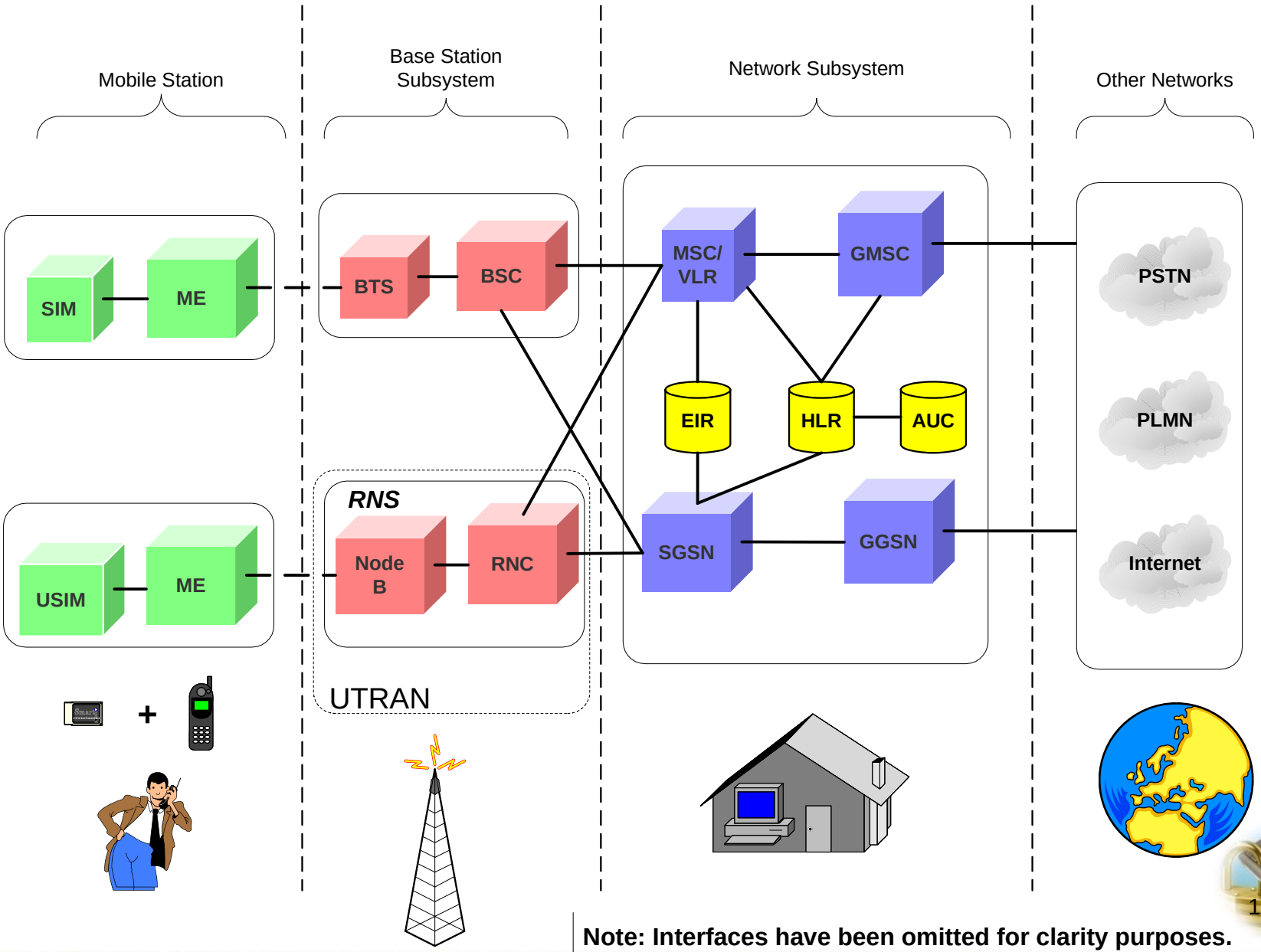


SIM: Subscriber Identity Module | MSC: Mobile services Switching Center
BSC: Base Station Controller | HLR: Home Location Register | EIR: Equipment Identity Register
BTS: Base Transceiver Station | VLR: Visitor Location Register | AuC: Authentication Center

GPRS Architecture



3G (UMTS) Network Architecture



Note: Interfaces have been omitted for clarity purposes.

Outline

- Why Security is Important?
- Mobile Network Technologies
- **Security Mechanisms in GSM**
- GSM Security Vulnerabilities

Security Mechanisms in GSM

- **Anonymity of the subscriber**
- **Authentication**
- **Confidentiality**

Identity in GSM

- **IMSI** (International Mobile Subscriber Identify) :
  - For unique identification of a subscriber
- **IMEI** (International Mobile Equipment Identity):
  - A mobile equipment is uniquely identified by the manufacturer provided IMEI
- **Ki**: 128bit shared authentication key
  - Stores in AuC (Authentication Centre) and the subscriber's SIM card.
  - The foundation of GSM security
- **Kc**: The cipher key for encryption between mobile phone and BTS

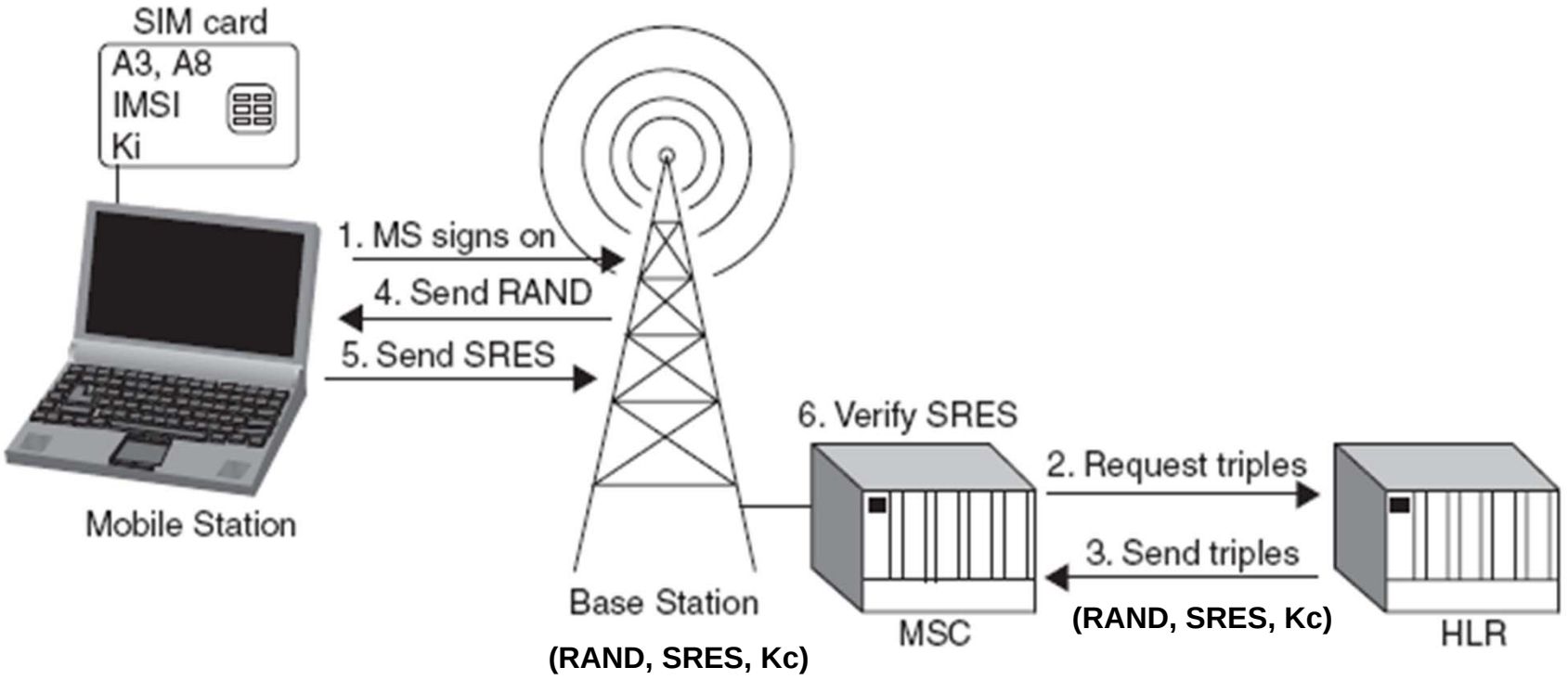
Anonymity

Location Management:

- **TMSI** (Temporary Mobile Subscriber Identity) is used for anonymity.
  - A 4-byte number for local subscriber identification
  - Only valid within the location area of the VLR temporarily
  - TMSI minimize the number of times IMSI is needed to be sent.

Authentication

- Ki never leaves the SIM
- The A3 (authentication) and A8 (key management) algorithms
  - key- dependent one-way hash functions. (similar in functionality)
  - commonly implemented as a single algorithm called COMP128.



Confidentiality

- A5 encryption algorithm (between Phone and BTS)
- A5 has three types: A5/1, A5/2, A5/3 (for 3G)

Outline

- Why Security is Important?
- Mobile Network Technologies
- Security Mechanisms in GSM
- **GSM Security Vulnerabilities**

Security Vulnerabilities

Security properties in GSM

- Access control
- Authentication
- Non-repudiation
- Confidentiality
- Communication security
- Data integrity
- Privacy
- Availability

Security Vulnerabilities

Security properties in GSM

- Access control
- Authentication
- ~~Non-~~repudiation
- Confidentiality
- Communication security
- ~~Data~~ integrity
- Privacy
- Availability

Security Vulnerabilities

- **The main security shortcoming: Integrity** is not considered in the GSM design and implementation
- No end to end security: limited encryption
- In GSM encryption algorithms obscurity is used for security!
- A3/A5/A8 algorithms eventually leaked
- A5/2 breakable in real-time and A5/1 also breakable in practice.
- One way authentication is not enough
- A3/A8 key management algorithms have been broken!

GSM Security Threats

- Identity theft using IMEI
  - e.g. stealing of mobile phone
- Fake subscription
  - by subscribers' Identity theft : e.g. SIM cloning
- DoS/ DDoS attacks
  - Cellular Phone Jamming
  - De-registration
- Interception of voice and data of subscribers
  - Over-the-air interception using fake BTS
  - Cryptanalysis attacks against A5
  - Hijacking incoming calls
  - Hijacking outgoing calls
- Tracking of the subscribers

GSM Security Threats

Commercial Interception devices!

Some specifications:

- Fake BTS
- Fake mobile phone/SIM
- Braking A5 algorithm
- Direction finder (DF)
- Jammer
- …

GSM Interceptor Pro System
$420,000.00

GSS-ProA

A GSM Security Threat Analysis

An threat analysis method for the GSM network

- **DREAD**:
  - Damage potential: **D**
  - Reproducibility: **R**
  - Exploitability: **E**
  - Affect Users: **A**
  - Discoverability: **D**

A GSM Security Threat Analysis

Threat	Discoverability	Affect Users	Exploitability	Reproducibility	Damage Potential	Risk
Denial of Service	10	9	8	10	5	8.4
Hijacking outgoing calls	10	1	5	10	4	6
Hijacking incoming calls	10	1	5	10	4	6
Fake BTS	10	1	4	10	3	5.6
Passive Identity Caching	10	1	5	8	2	5.2
De-registration	10	1	5	10	3	5.8
Location Update	10	1	5	10	3	5.8

Any Question?