X'CON 2003

GSM Operators Security *(or lack thereof)*

Author： Emmanuel Gadaix_

data： December 2003

Disclaimer

- **The speech is oriented towards the penetration testing methodology used while working with a GSM operator and its** legal **working framework.**
- **We do** not **recommend that you use this material for unauthorised access to telecommunications operators' infrastructure or systems.**
- **We** cannot **be held responsible if you decide nevertheless to explore such systems, find it fascinating, start getting sloppy and leave tracks that finally get you busted.**
- **The information contained within this presentation does** not **infringe on any intellectual property nor does it contain tools or recipe that could be in breach with Chinese laws.**

Contents

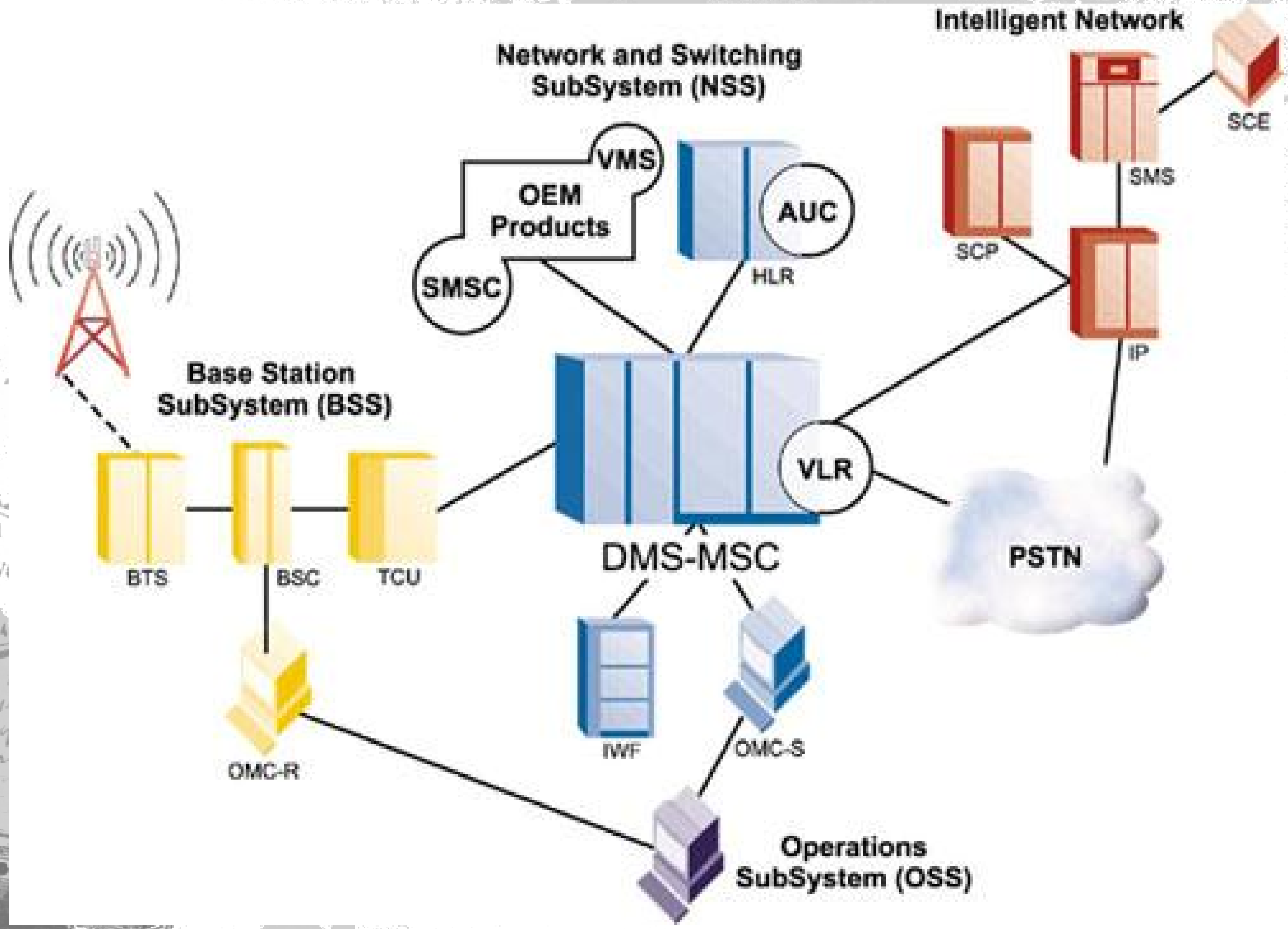
- GSM: a quick security overview
- Infrastructure of GSM operators
- Review of systems used
- Common fraud techniques
- Uncommon fraud techniques
- Future challenges
- Conclusions / Questions

GSM Overview

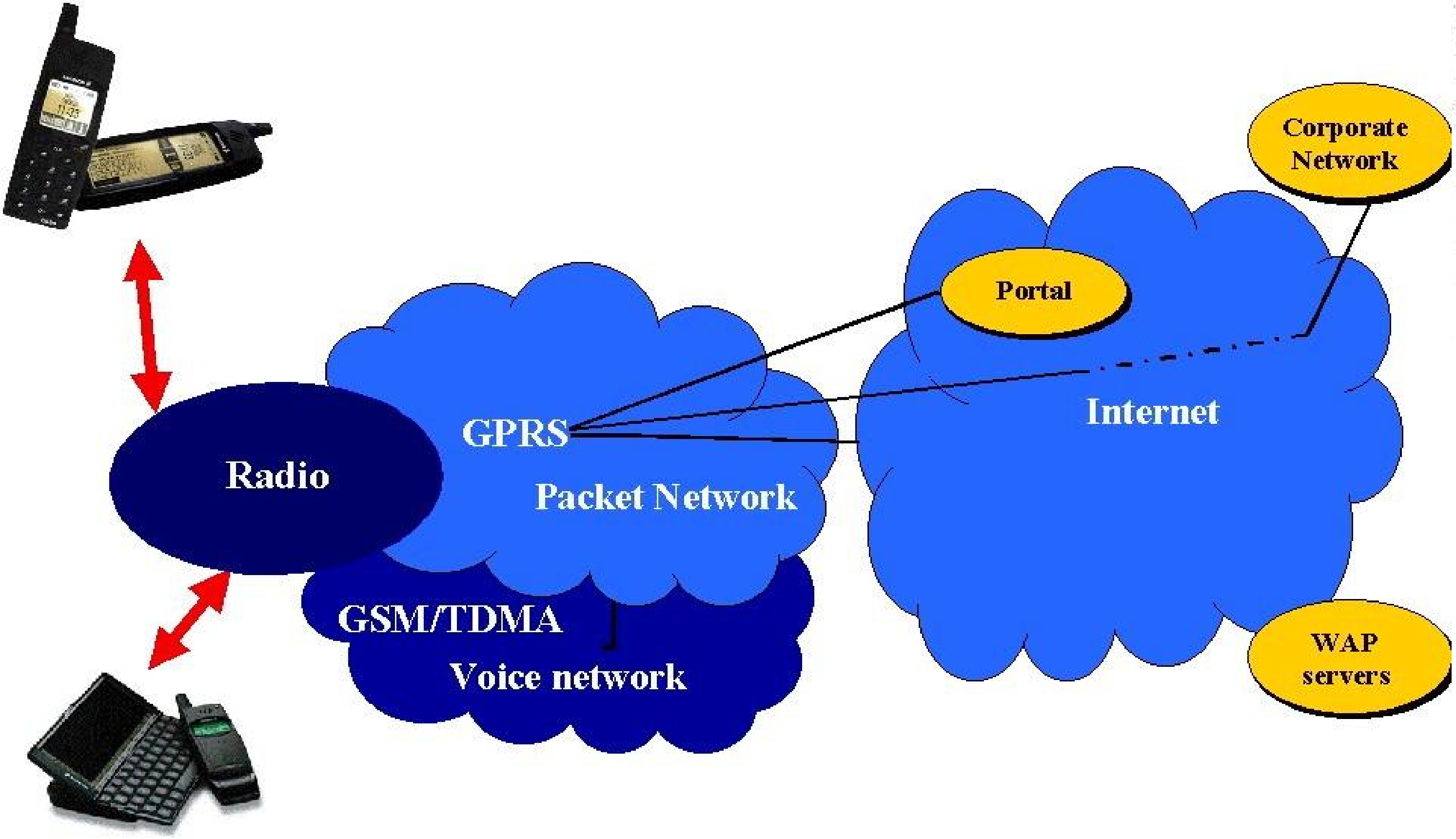
- GSM operators typically split their network between IT (the incompetent team running the mail, the domains, the printers and the proxy/firewall) and Engineering (the telco side).
- Usually there is distrust between the two entities, poor communications and certainly no common policy towards security.
- IT of course believe they are important, but in fact they just have a support role.

The GSM core network

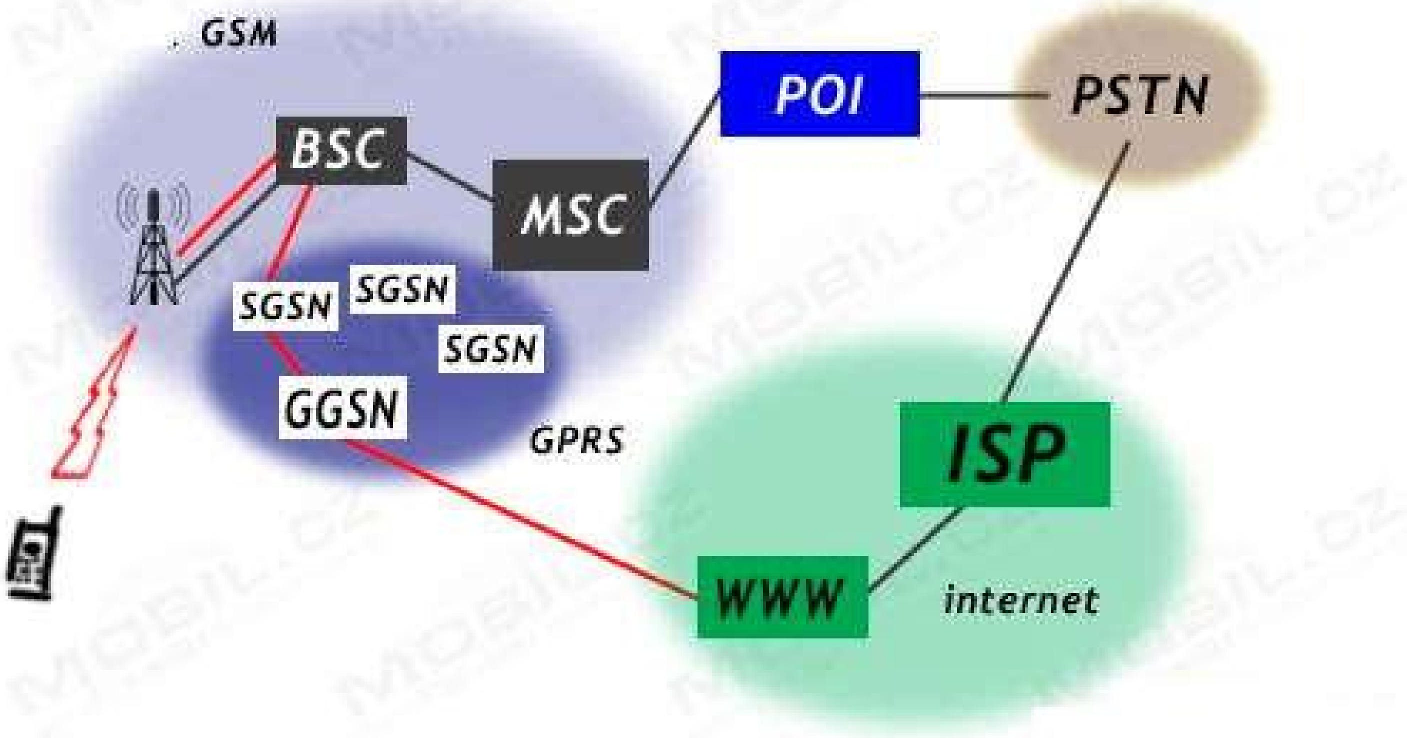
X'CON 2003


Intelligent Network
Network and Switching SubSystem (NSS)
SCE
VMS
OEM Products
AUC
SMS
SCP
SMSC
HLR
IP
Base Station SubSystem (BSS)
VLR
PSTN
BTS
BSC
TCU
DMS-MSC
IWF
OMC-S
OMC-R
Operations SubSystem (OSS)

GPRS network



GPRS details



GSM security

- Only provides *access security* – communications and signalling traffic in the fixed network are not protected.
- Does not address *active attacks*, whereby some network elements (e.g. BTS: Base Station) are faked
- Only as secure as the fixed networks to which they connect

- Lawful interception only considered as an after-thought
- Terminal identity cannot be trusted
- Difficult to upgrade the cryptographic mechanisms
- Lack of user visibility (e.g. doesn’t know if encrypted or not)

Attacks on GSM networks

- Eavesdropping. **This is the capability that the intruder** eavesdrops signalling and data **connections associated with other users. The required equipment is a modified MS.**

- Impersonation of a user. **This is the capability whereby the intruder** sends signalling and/or user data **to the network, in an attempt to make the network believe they originate from the target** user**. The required equipment is a modified MS.**

- Impersonation of the network. **This is the capability whereby the intruder** sends signalling and/or user data **to the target user, in an attempt to make the target user believe they originate from a genuine** network**. The required equipment is modified BTS.**

Attacks on GSM network

- Man-in-the-middle. **This is the capability whereby the intruder puts itself in between the target user and a genuine network and has the ability to** eavesdrop**,** modify**,** delete**,** re-order**,** replay**, and** spoof **signalling and user data messages exchanged between the two parties. The required equipment is modified BTS in conjunction with a modified MS**.

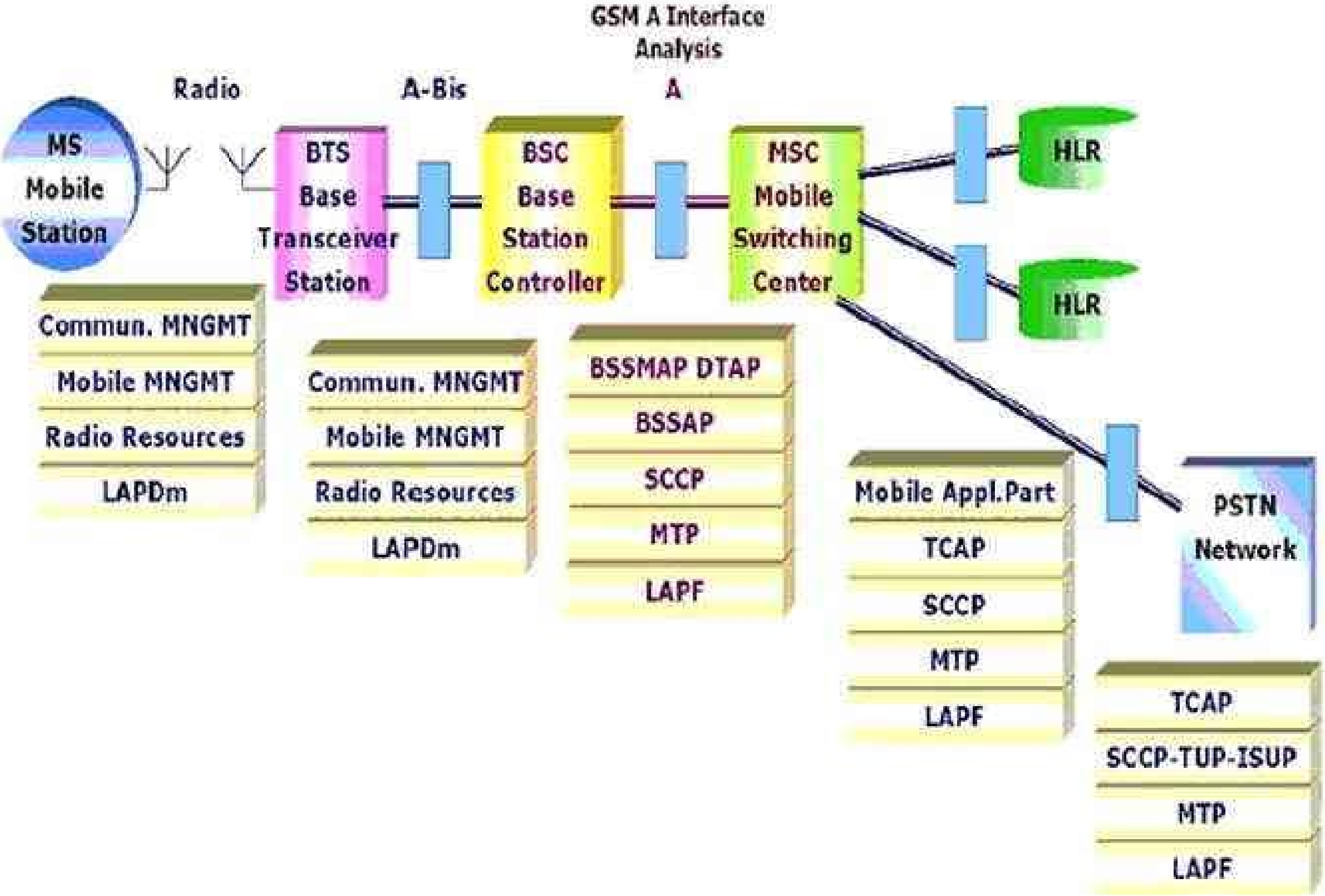
- Compromising authentication vectors in the network. **The intruder obtains a** compromised authentication vector**, which may include challenge/response pairs, cipher keys and integrity keys. This data may have been obtained by compromising network nodes or by intercepting signalling messages on network links.**

A word on GSM crypto

- GSM consortium decide to go "*security through obscurity*"
- A3/A5/A8 algorithms eventually leaked
- Cryptanalysis attacks against A5
- Attacks on COMP-128 algorithm
- Evolution of security model
- Key recovery allowing SIM cloning
- Over-the-air interception using fake BTS

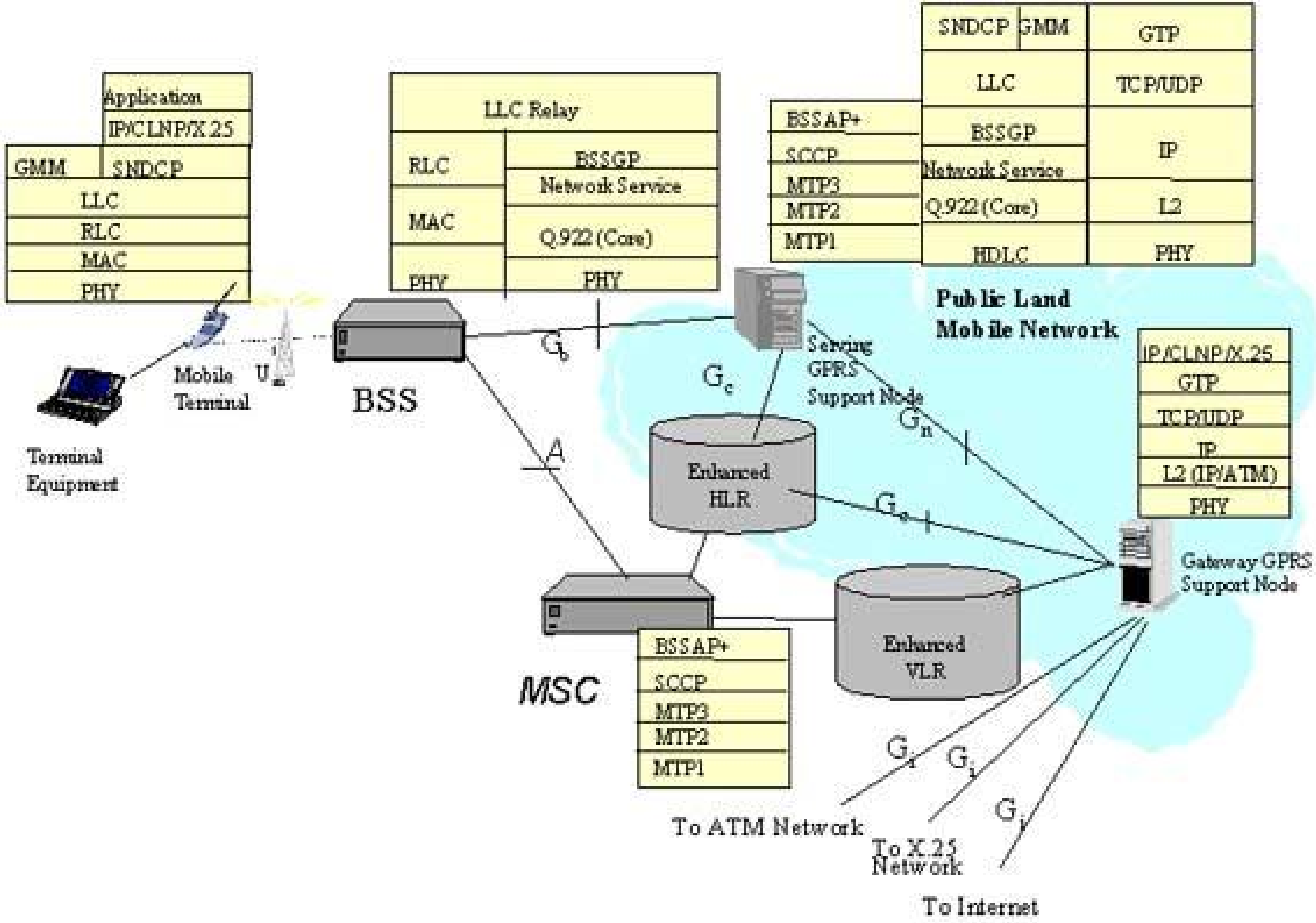
GSM protocols

X'CON 2003



GPRS protocols

X'CON 2003



GSM SS7 Signalling

- **GSM uses** SS7 signalling **for call control, mobility management, short messages and value-added services**
- MTP1-3**: Message Transfer Part**
- SCCP**: Signalling Connection Control Part**
- TCAP**: Transaction Capabilities Application Part**
- MAP**: Mobile Application Part**
- BSSAP**: Base Station Subsystem Application Part**
- INAP**: Intelligent Network Application Part**
- CAMEL**: Customized Application for Mobile Enhanced Logic**

SS7 Security

X'CON 2003

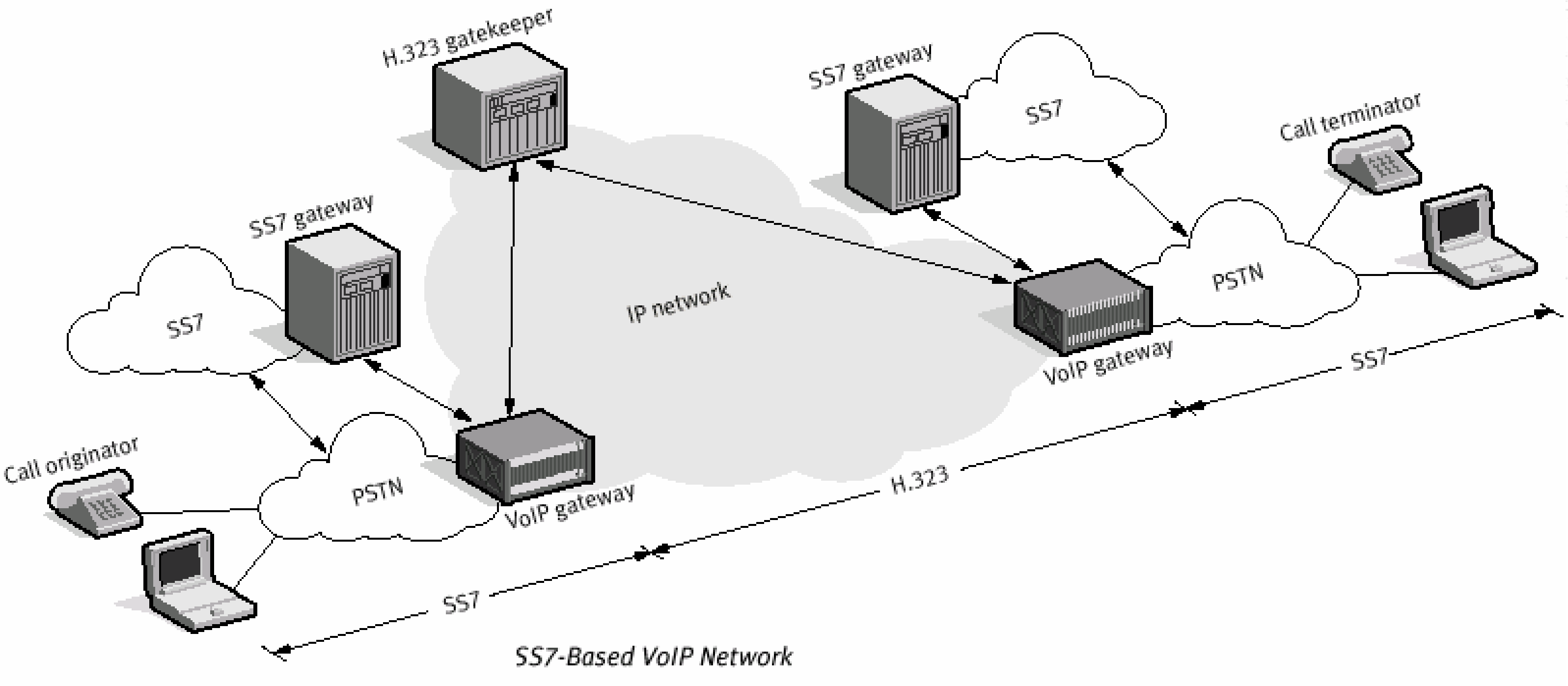
- Mobile networks primarily use signalling System no. 7 (SS7) for communication between networks for such activities as authentication, location update, and supplementary services and call control. The messages unique to mobile communications are MAP messages.
- The security of the global SS7 network as a transport system for signalling messages e.g. authentication and supplementary services such as call forwarding is open to major compromise.
- The problem with the current SS7 system is that messages can be altered, injected or deleted into the global SS7 networks in an uncontrolled manner.

SS7 Security

X'CON 2003

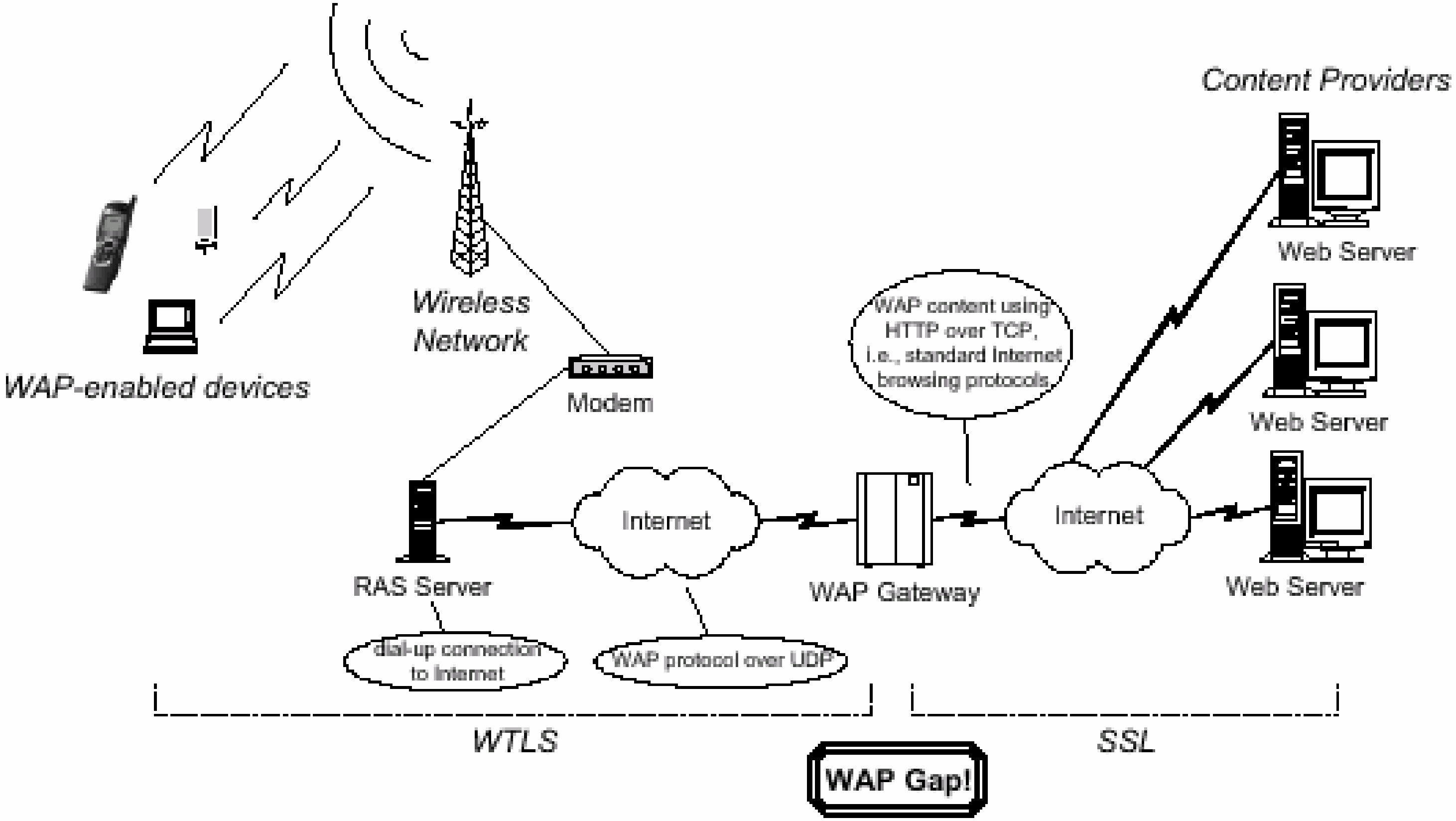
- There is also exponential growth in the use of *interconnection* between the telecommunication networks and the Internet .
- The IT community now has many protocol converters for conversion of SS7 data to IP, primarily for the transportation of voice and data over the IP networks. In addition new services such as those based on IN will lead to a growing use of the SS7 network for general data transfers.
- There have been a number of incidents from accidental action, which have damaged a network. To date, there have been very few deliberate actions.

SS7 and VoIP



SS7-Based VoIP Network

The WAP gap


Content Providers
Web Server
Web Server
Web Server
Wireless Network
WAP-enabled devices
Modem
WAP content using HTTP over TCP, i.e., standard Internet browsing protocols
Internet
Internet
RAS Server
WAP Gateway
dial-up connection to Internet
WAP protocol over UDP
WTLS
SSL
WAP Gap!

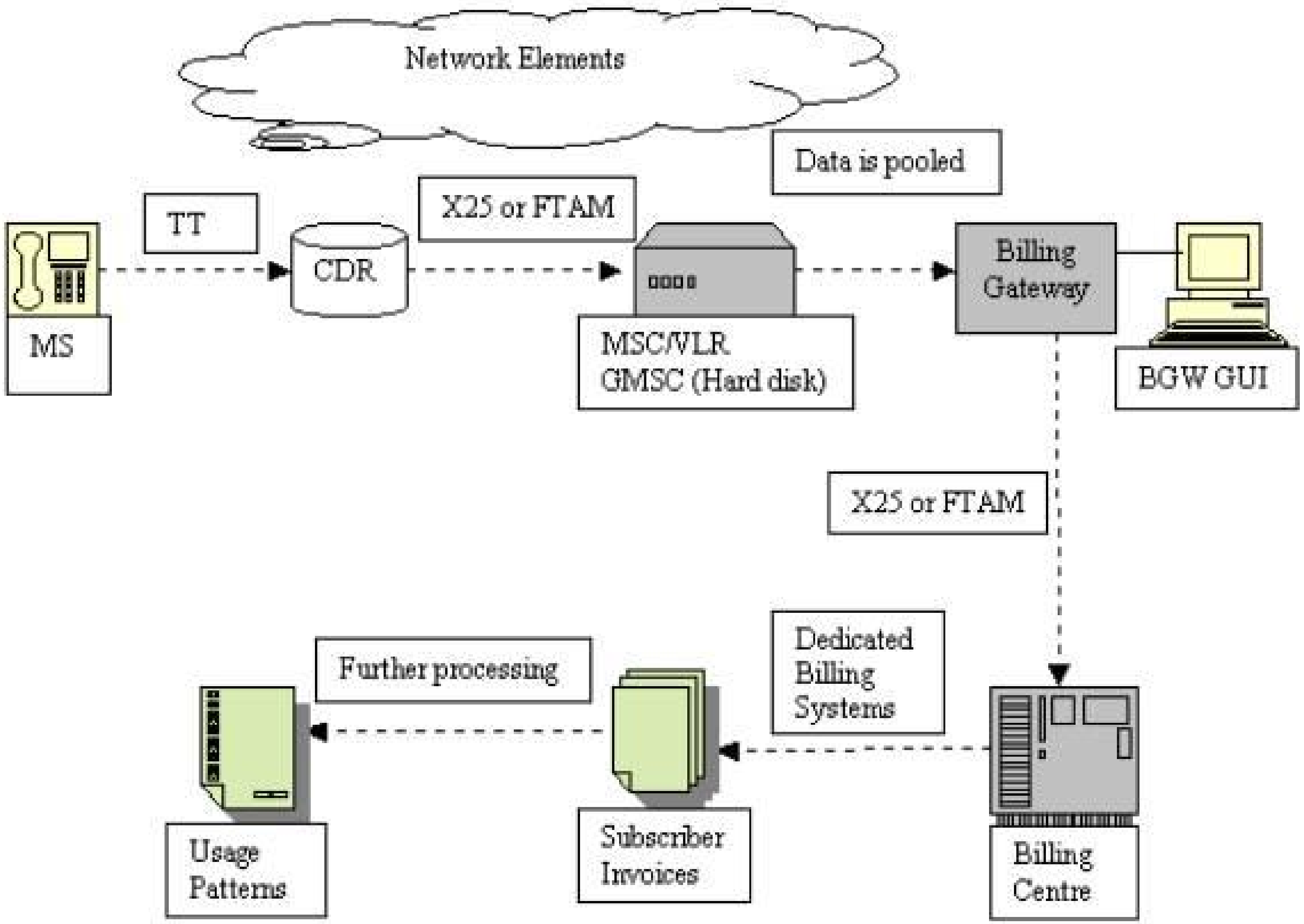
Legal Interception

- CDR **data always available to authorities, kept forever in operators' data warehouses**
- **GSM monitoring facilities designed as an "after thought".**
- **System plugs onto MSC special interface and allows** interception **of signalling and speech traffic.**
- **Monitoring and interception can be** delocalized **from the MSC**
- **3G has done a much better job for big brother.**
- **Any event can be intercepted in a very user-friendly way, including packet data.**
- **Billing data can be intercepted in real-time.**

Mediation in GSM

- Mediation **is the process that converts and transports raw** CDR **data**
- **It can also be used to translate** provisioning **commands to the NE**
- **It is a critical part of the provisioning and billing cycles.**
- **Most convenient place to commit fraud**

Charging Overview


Network Elements

Data is pooled

TT

X25 or FTAM

MS

CDR

MSC/VLR
GMSC (Hard disk)

Billing Gateway

BGW GUI

X25 or FTAM

Dedicated Billing Systems

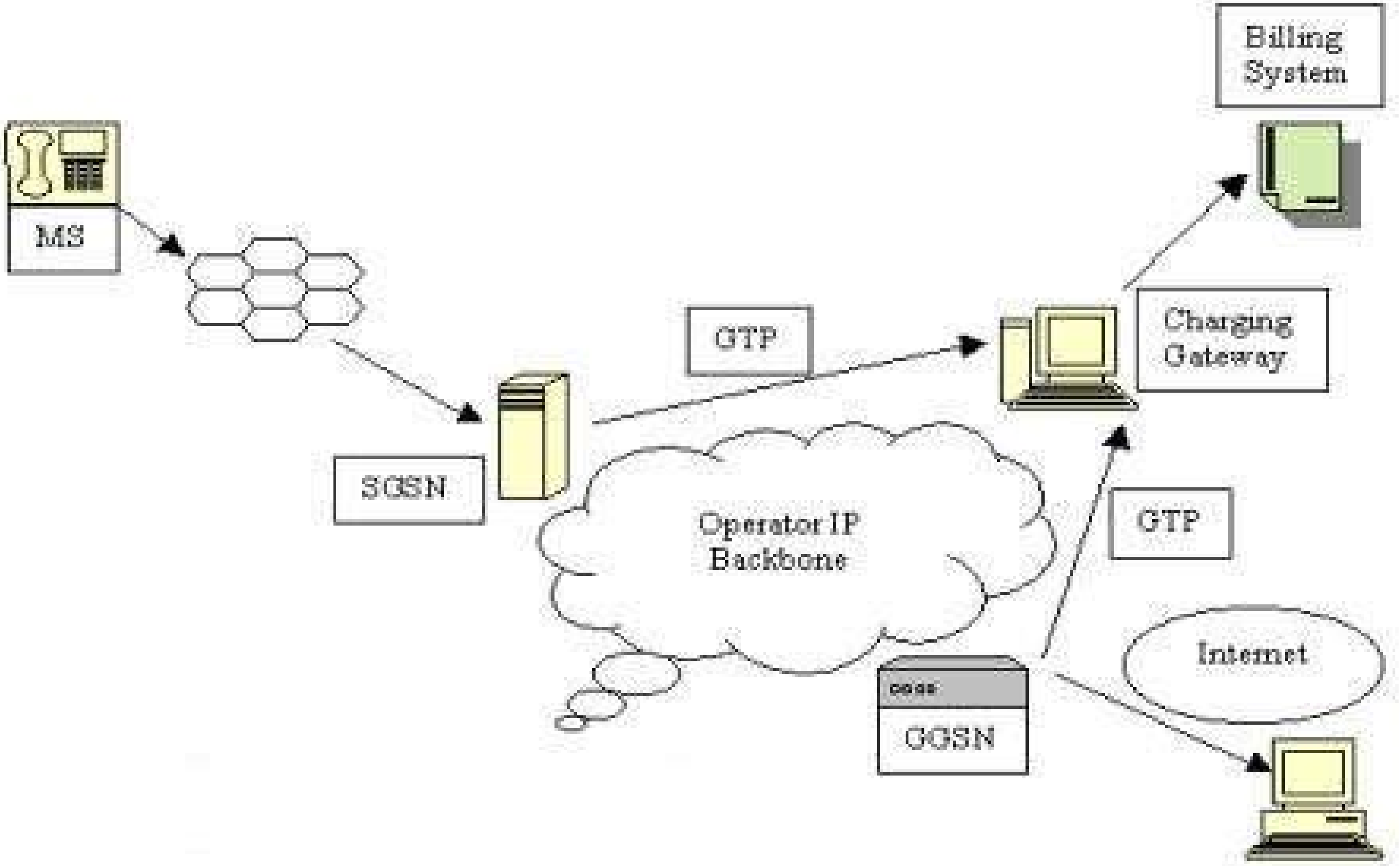
Further processing

Usage Patterns

Subscriber Invoices

Billing Centre

GPRS charging



Messing with Mediation

- Modification of CDR processing rules
- Modification of “test numbers” list
- Live patching of CDR data
- Patching of mediation application
- GPRS packet aggregation rules modification

Mediation (Charging Gateway)

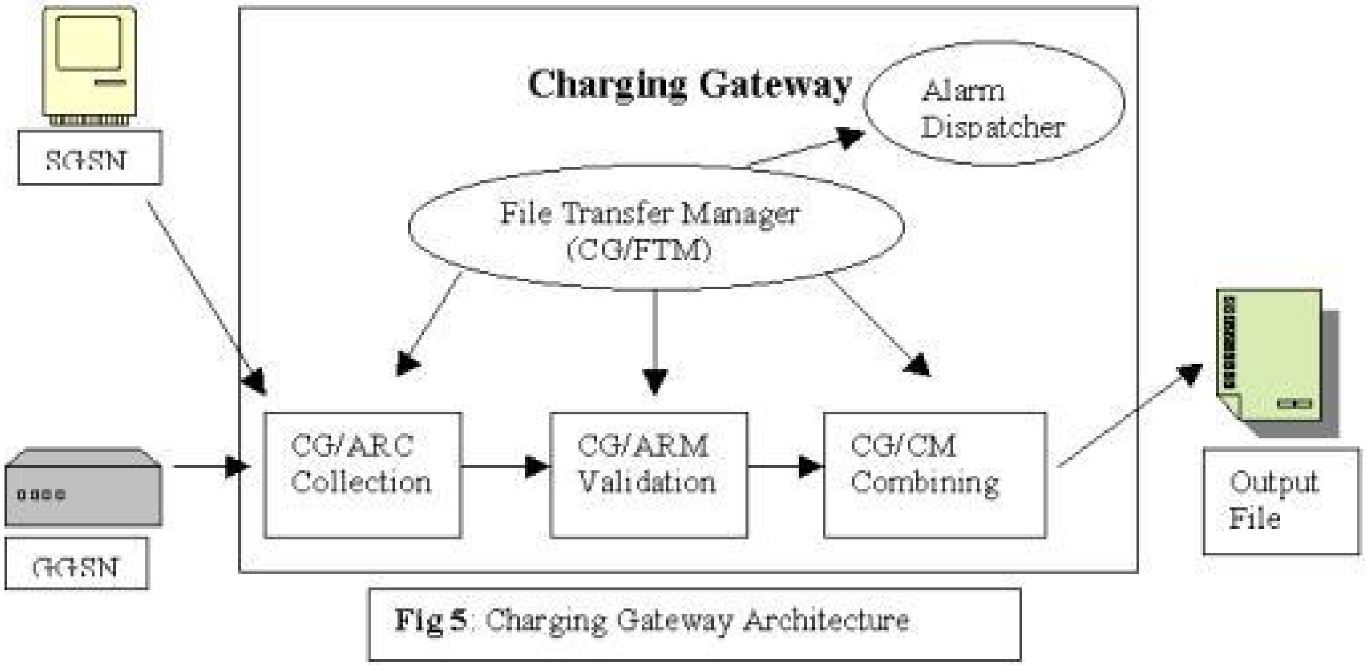


Fig 5: Charging Gateway Architecture

GSM Fraud

- **Subscription fraud.** Most common due to the lag between calls and corresponding bill.
- **Roaming fraud.** Also common due to lag between inter-operators bill reconciliation.
- **Call forwarding schemes.** Popular “sell call” vector.
- **Prepaid fraud.** Vouchers and balance can be modified.
- **M-commerce payment fraud.** Compromise of credit cards or fraudulent transactions.
- **Internal fraud.** Perpetrated by staff at the operator or any of its subcontractors.

GPRS threats

- **Unsolicited malicious content**
- **Spamming information with associated charging**
- **Virus and trojans imported by Content Downloading**
- **Username and IP harvesting**
- **Attacks from MS to operator's IP backbone**

Internal Fraud

- **Requires access to the LAN.**
- **Knowledge of GSM network elements.**
- **Knowledge of Mediation.**
- **Knowledge of Billing.**
- **Very difficult to detect and eradicate.**

Modification of NE

- **Modification of supplementary services on prepaid subscriptions**
- **Setup of ghost subscriptions**
- **Modification of roaming profile**
- **Setup of call forwarding bouncers**
- **Modification of charging rules**
- **Electronic harassment**

Billing System

- Raw **database edit**. Conveniently deletes selected records containing billing data.
- **Modification** of charging tables.
- Creation of **special rules** for unrateable CDRs
- **Patching** of the rater application

NMS attacks

- **Network Management System. Controls the entire network.**
- **Can be used to reconfigure any element, e.g. power level on a cell.**
- **Contains extremely valuable network design information.**
- **Stores the entire network database (faults, events, measurements, etc.)**

LIG attacks

- **Legal Interception Gateway is used by police and intelligence agencies.**
- **Connected to MSC though special interface. Very user-friendly.**
- **Based on standard UNIX and TCP/IP so potentially open to common attacks**
- **Compromise of a LIG would allow real-time interception and call eavesdropping.**
- **Could compromise the agencies' own facilities.**

Other concerns

- **Financial systems co-located, e.g SAP, Oracle Financials.**
- **Data Warehouse hosts.**
- **Vouchers provisioning cycle.**
- **AuC Ki management.**
- **SIM locking.**
- **OTA uploading malicious SIM applications.**

Typical Weaknesses

- **Dialup remote access. Installed by vendors, then forgotten.**
- **Traditional hacking through Internet links.**
- **X.25 PSPDN hacking.**
- **Inter-operators links.**
- **No co-ordination between IT and Engineering.**
- **No IDS understands GSM protocols.**
- **Infrastructure too complex to be understood by a single entity.**

Field Observations

X'CON 2003

- No **operator is secure. Not even close.**
- **Internal systems** widely open**.**
- **Telco vendors use** unpatched **and** unsecured **operating systems.**
- No **hardening procedure.**
- No **proper segmentation of various LANs.**
- No **end-to-end security, e.g. with vouchers.**
- **Critical platforms (IN, CCBS, WAP, Payment Gateway)** seldom **protected.**
- No **audit procedures.**

Conclusions

- **Operators' infrastructure an** exciting playground **for sophisticated hackers.**
- **Hackers could seek** phreaking thrills **using SS7, VoIP.**
- Increasing complexity **with GPRS, 3G and VAS applications leads to many further opportunities for attackers.**
- Serious lag **between telcos and IP-centric companies**

THANK YOU

Emmanuel Gadaix

eg@tstf.net

X'CON 2003