

Phreaking: Past, Present and Future

Karachi 2004

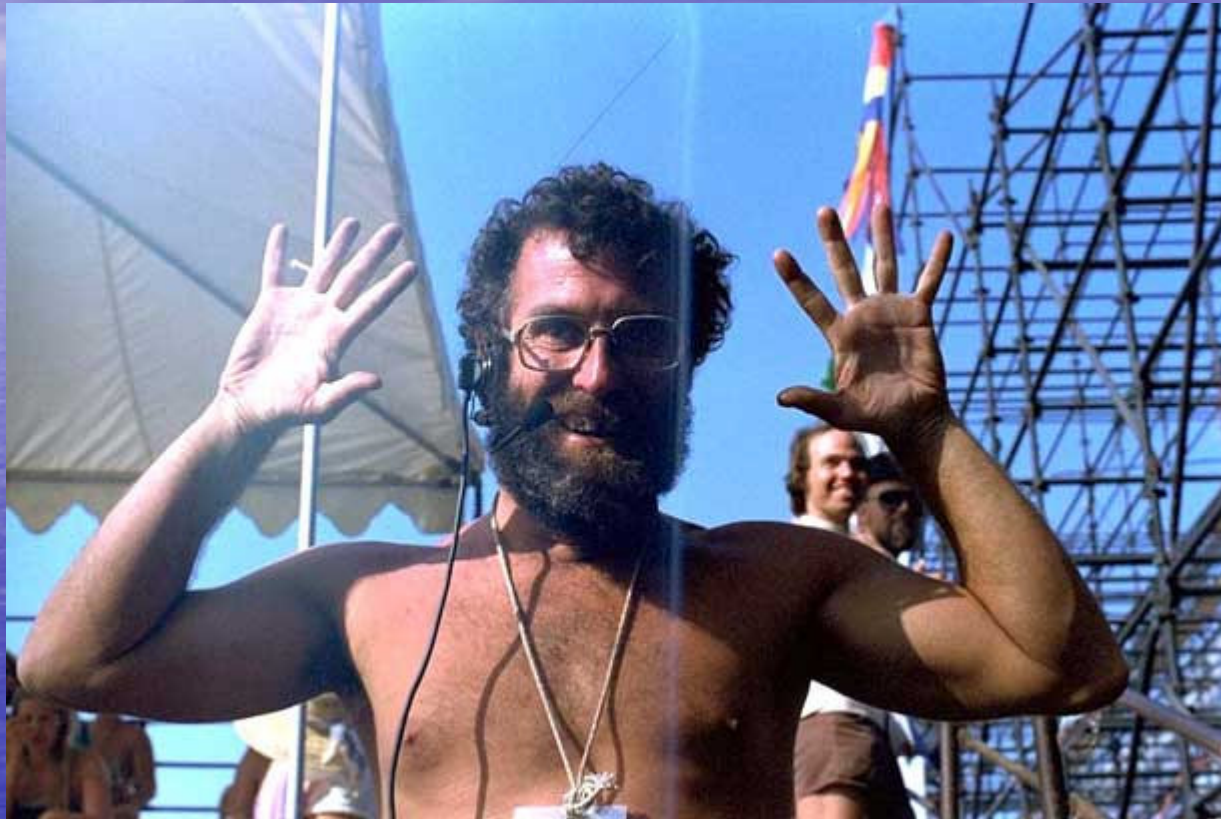
Disclaimer

- The speech is oriented towards the penetration testing methodology used while working with a telecommunications operator and its legal working framework.
- We do not recommend that you use this material for unauthorized access to 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 the laws of Pakistan.

Agenda

- Brief history of phreaking
- Review of digital telephony concepts
- Network Elements security
- Protocols security
- Future threats
- Conclusions / Q&A

Once upon a time...



John Draper aka **Captain Crunch** during the happy days of in-band signalling

Definition of phreaking

- ***Phreaking*** is a slang term for the action of making a telephone system do something that it normally should not allow.

But... what is it?

- **Discovery** and **exploration** of features of telecommunications systems
- **Controlling** Network Elements (NE) in a way that was not planned by its designers
- **Abusing weaknesses** of protocols, systems and applications in telephone networks

Why would anyone do this??



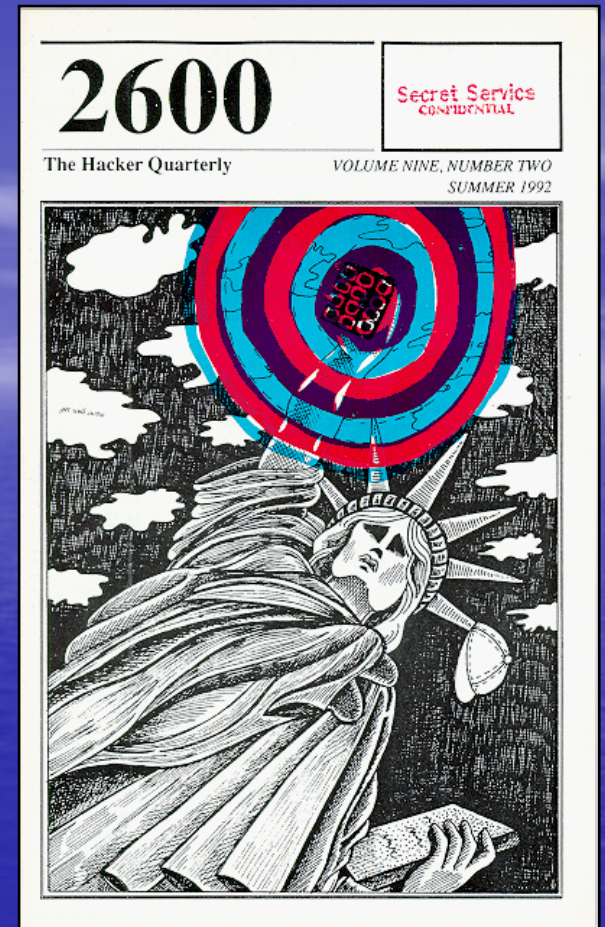
“ I do it for one reason and one reason only. I'm learning about a system. The phone company is a System. A computer is a System, do you understand? If I do what I do, it is only to explore a system. Computers, systems, that's my bag. **The phone company is nothing but a computer.** ”

Captain Crunch

From *Secrets of the Little Blue Box*
Esquire Magazine, October 1971

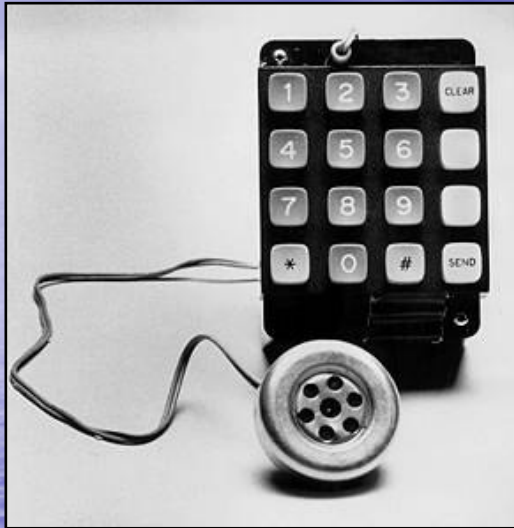
Beware!

Quote from 2600 magazine summer 1992
Phreaking in the nineties by **Billsf**



“ If you live in a currently repressed area, such as the United States, you should beware that even the things that you consider "harmless exploring" could get you into lots of trouble (confiscation of computer, fines, probation jail, loss of job, etc.) ”

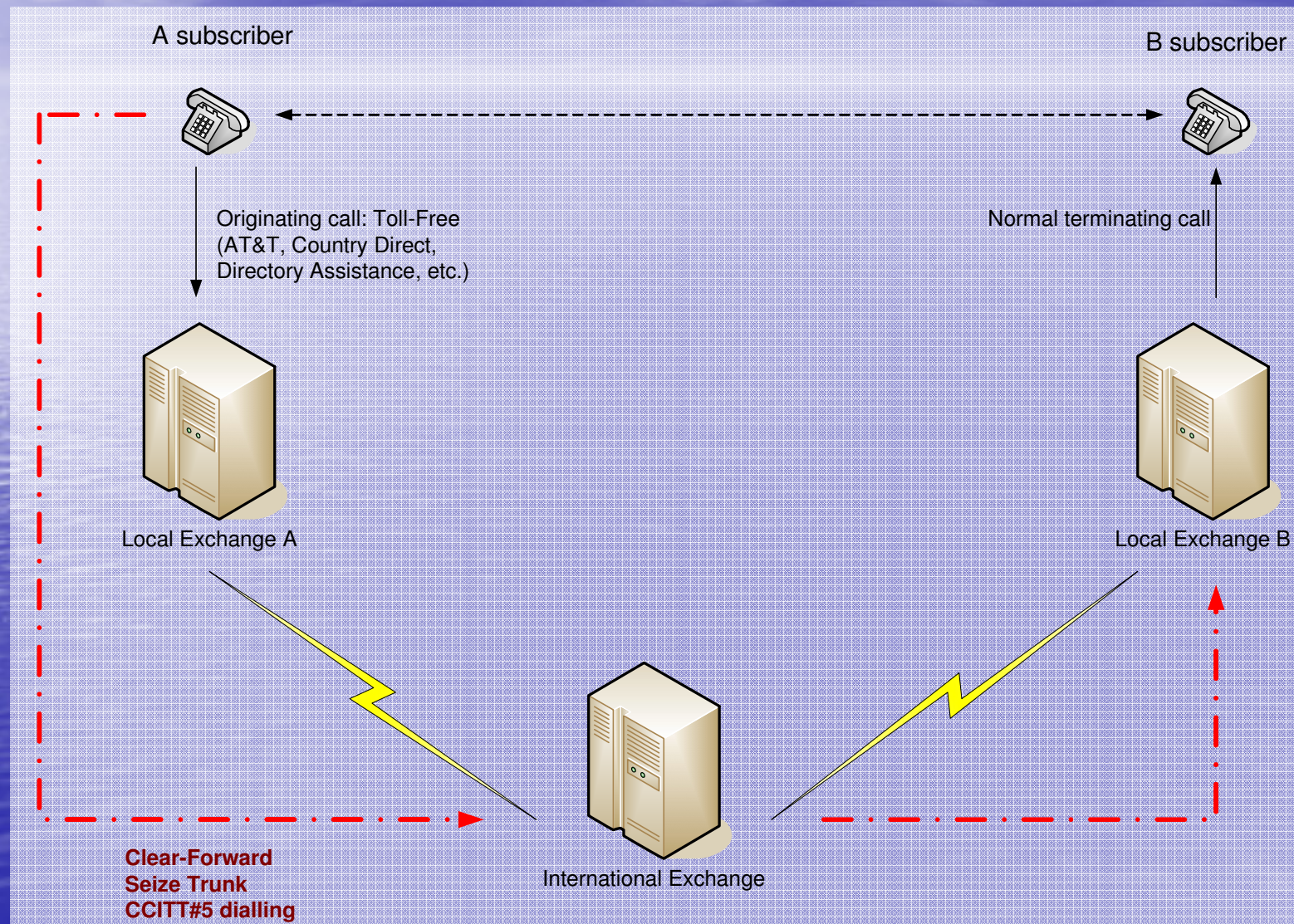
The Blue Box



Steve Jobs and Steve Wozniak in 1975 with a bluebox

- CCITT#5 in-band signalling sends control messages over the speech channel, allowing trunks to be controlled
- Seize trunk (2600) / KP1 or KP2 / destination / ST
- Started in mid-60's, became popular after Esquire 1971
- Sounds produced by whistles, electronics dialers, computer programs, recorded tones

Bluebox: in-band signalling



The end of the blueboxing era

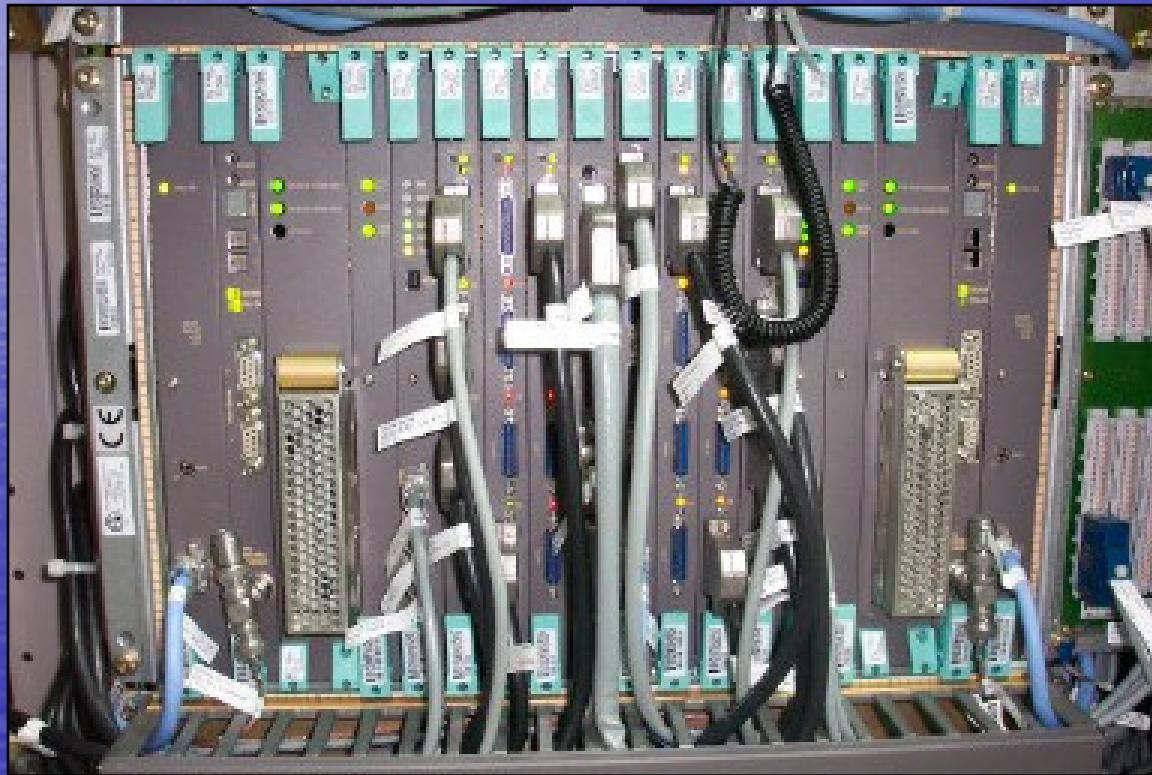


- Telcos installed filters, changed frequencies, analyzed patterns, sued fraudsters
- The new SS7 digital signalling protocol is out-of-band and defeats blueboxing
- In Europe, boxing was common until the early nineties and kept on until 1997-1998
- In Asia, boxing can still be done on some countries. There were blueboxers in Asia (at least in 1995-1996)

Hackers vs. Phreakers

- In the nineties, the Internet started its phenomenal growth and overshadowed other networks
- Underground activities quickly shifted from BBS, X.25 and boxing to Internet hacking
- Many phreakers reconverted to hacking (or kept on working for the local telcos)
- Phreaking is not about using someone else's tools to automatically discover and exploit known bugs

Digital Telephony

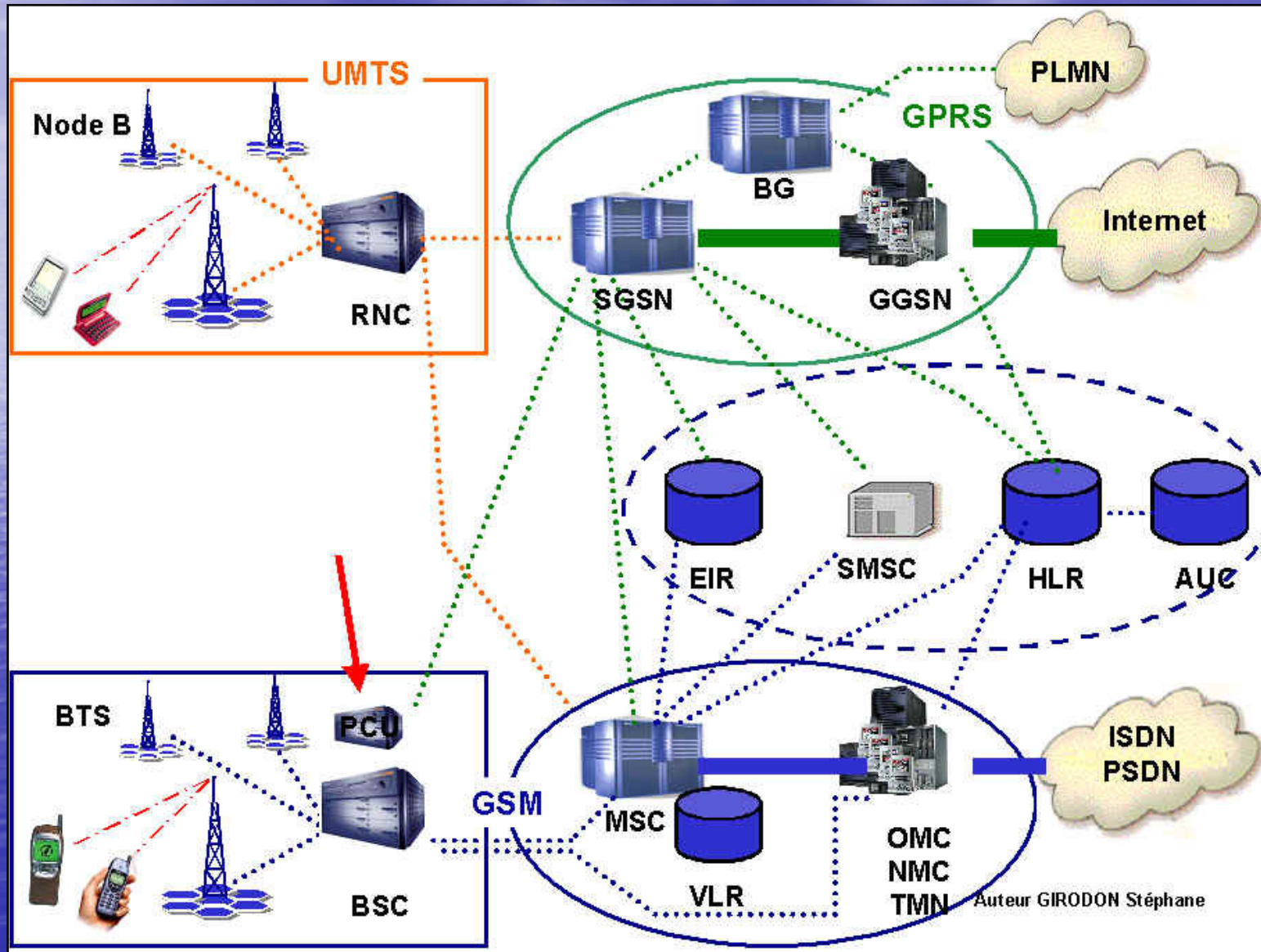


Telephony 101



- Fixed line (PSTN): analog, digital (ISDN)
- Mobile: analog (AMPS, NMT), digital (GSM, CDMA, 3G), private (PMR, Military)
- All switches now speak SS7 for signalling
- Speech and data convergence is increasing
- Services are growing (SMS, MMS, packet data, WLAN integration, etc.)

GSM/3G Mobile Telephony



Network Elements

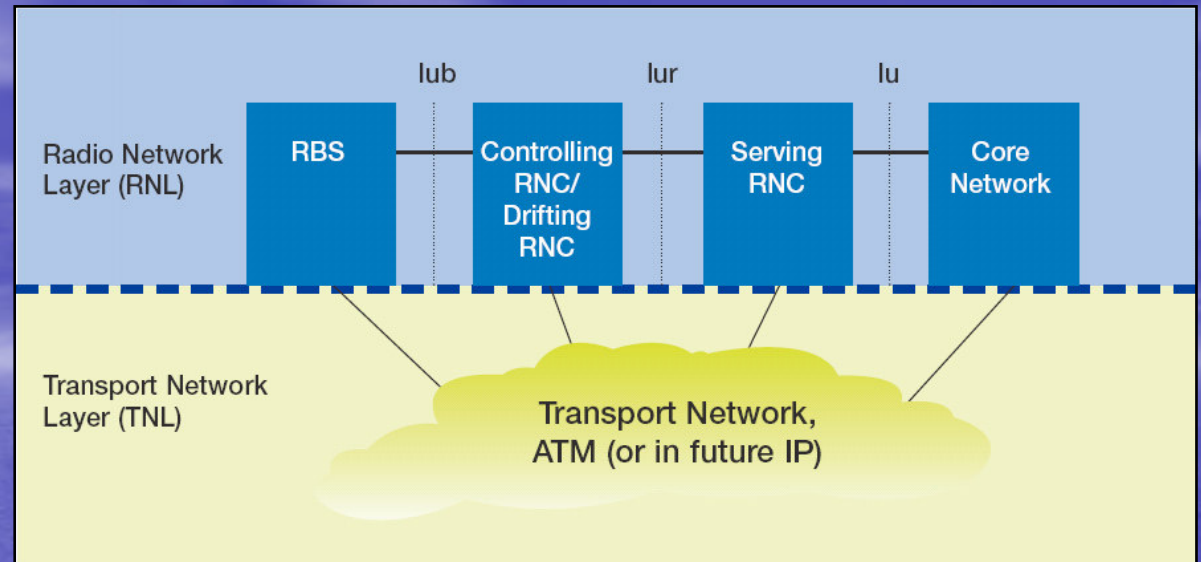
- Radio Access Network (BSS/RAN)
- Mobile Switching Center (MSC/NSS)
- Home Location Register (HLR/VLR)
- Intelligent Network (IN)
- Messaging (SMSC, MMSC, USSD, VMS)
- Packet data (GPRS, EDGE, 3G/UMTS)
- Network Management (NMS, OMC, OSS)
- Mediation, Billing, Customer Care, LIG

Radio Access Network

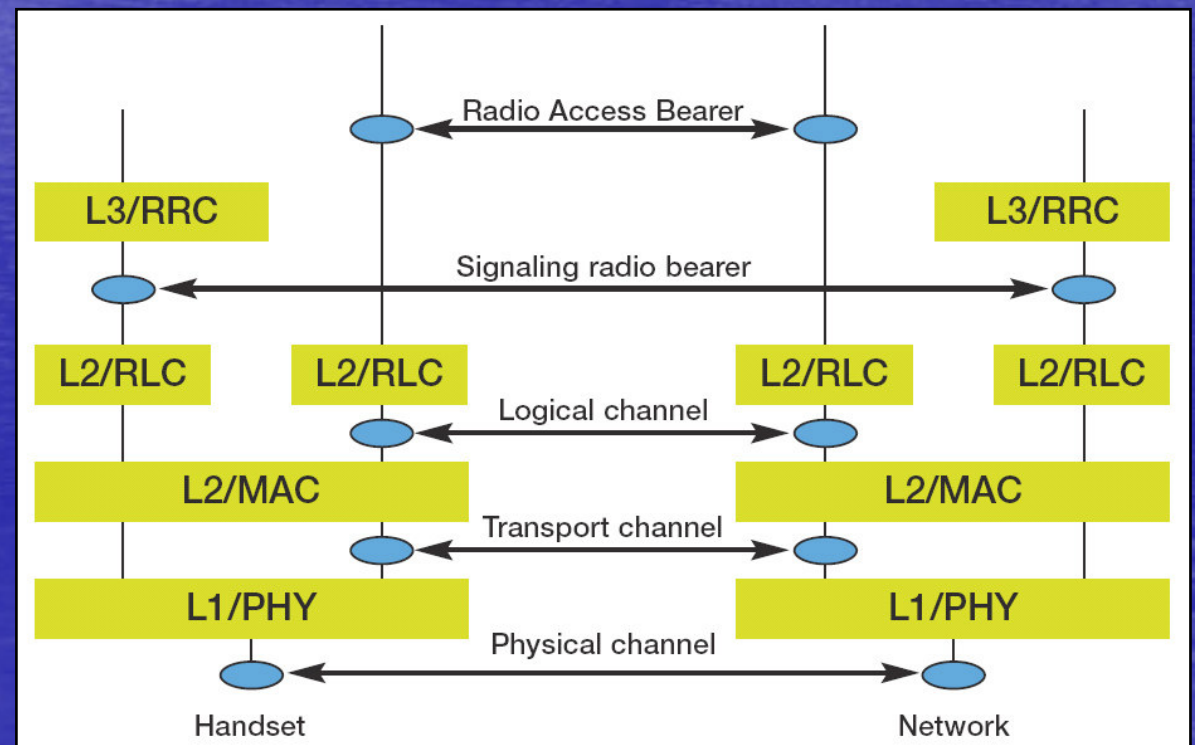


- In GSM and 3G, traffic is encrypted
 - Multiple channels (FDMA) and timeslots (TDMA)
 - Some signalling traffic in clear text
- *RAN Network Elements can be accessed over MML, Q.3, remote terminal and SS7*

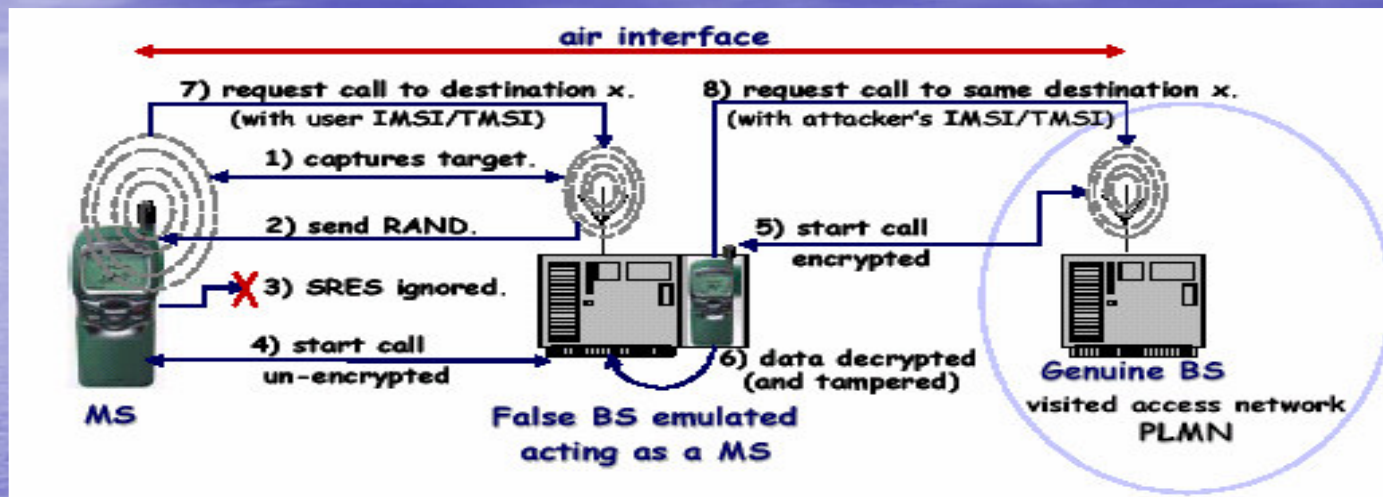
Transport Network



Radio Access Network



Examples of RAN attacks



- Fake BTS attacks (e.g. Man-in-the-Middle)
- Modified MS attacks
- Over-the-air SIM cloning
- DoS by MML configuration change



Fake BTS

Transmissions Network



- It is the backbone of any digital network, links network elements together
- Can carry IP traffic but is not yet fully IP-based
- Mostly fiberoptics, SDH/PDH, ATM, dark fiber, microwaves, FSO

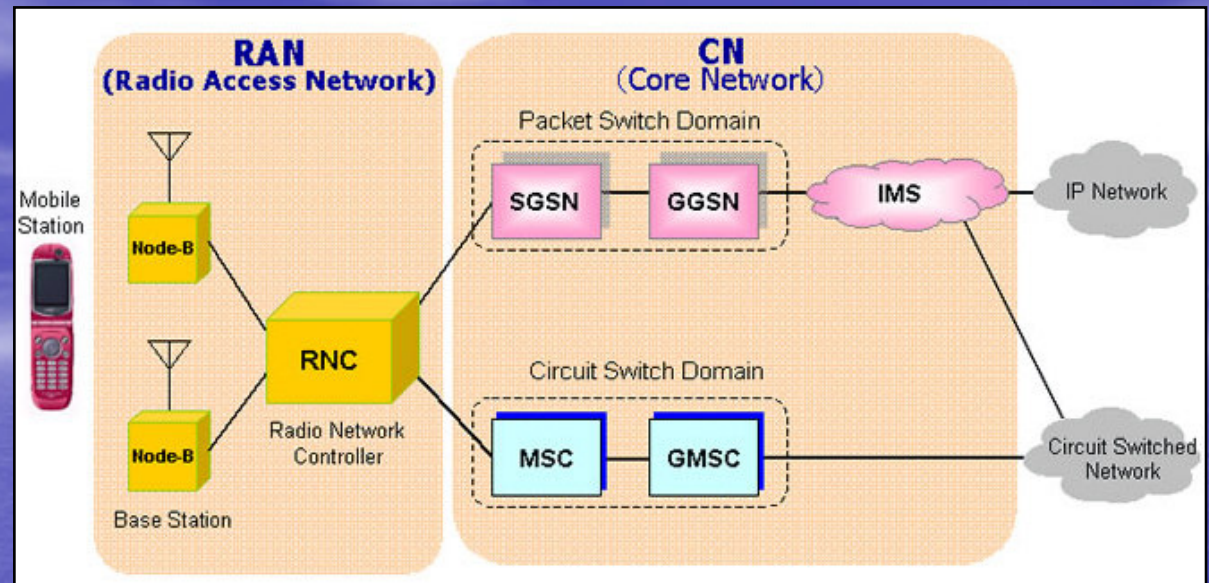
→ *NE accessed by MML, Q.3 and remote terminal*

Examples of TN attacks



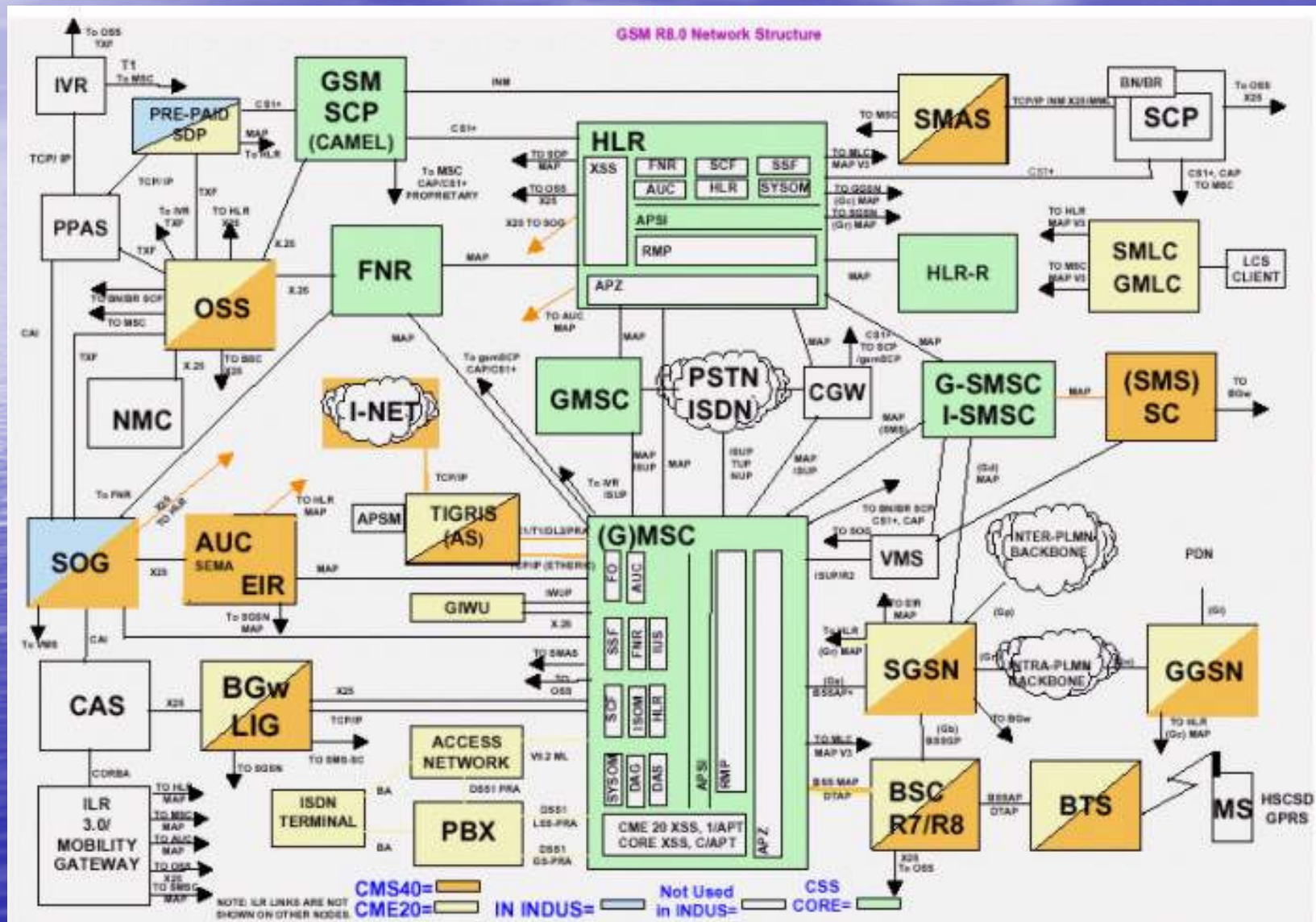
- Mostly vulnerable to physical attacks
- Fiber splicing
- Microwaves radiation leak
- DoS by MML reconfiguration of transmission ring

Switching Network



- Telephony is about circuit-switching
 - In GSM, the MSC works with HLR/VLR (subscribers DB) and with BSS/RAN (access network)
 - GSM uses TDMA (3G uses CDMA). The basic unit is E1 (2Mbps)
- ➔ *MSC can be accessed by MML (over X.25 or IP), FTAM, CMISE, SS7 protocols. HLR over MML, SS7 and remote terminal.*

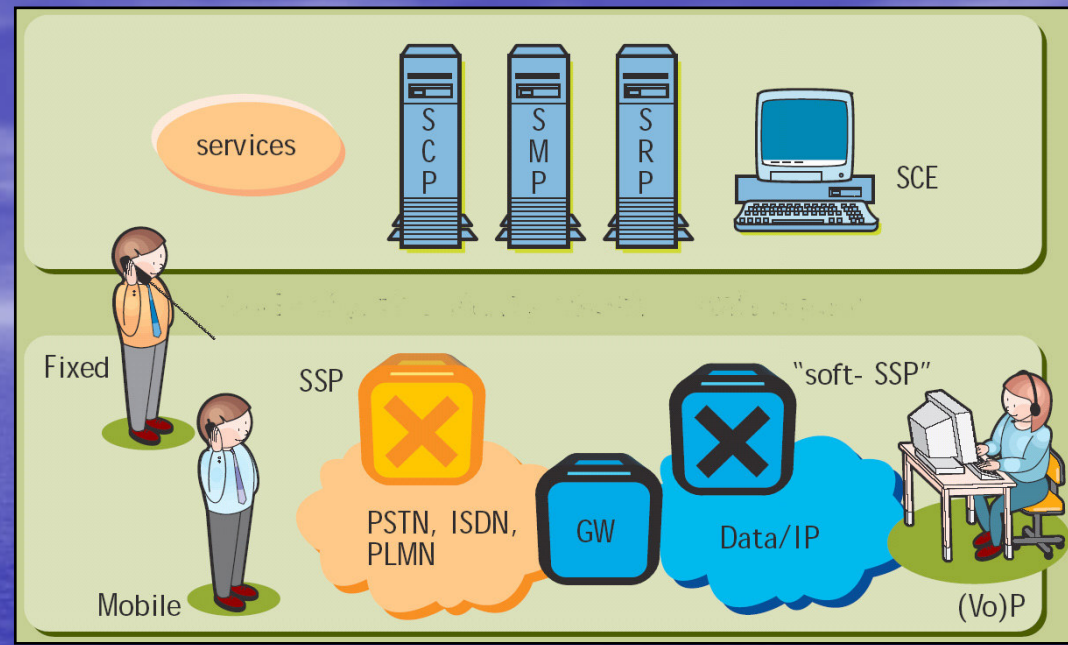
NSS – detailed view



Examples of NSS attacks

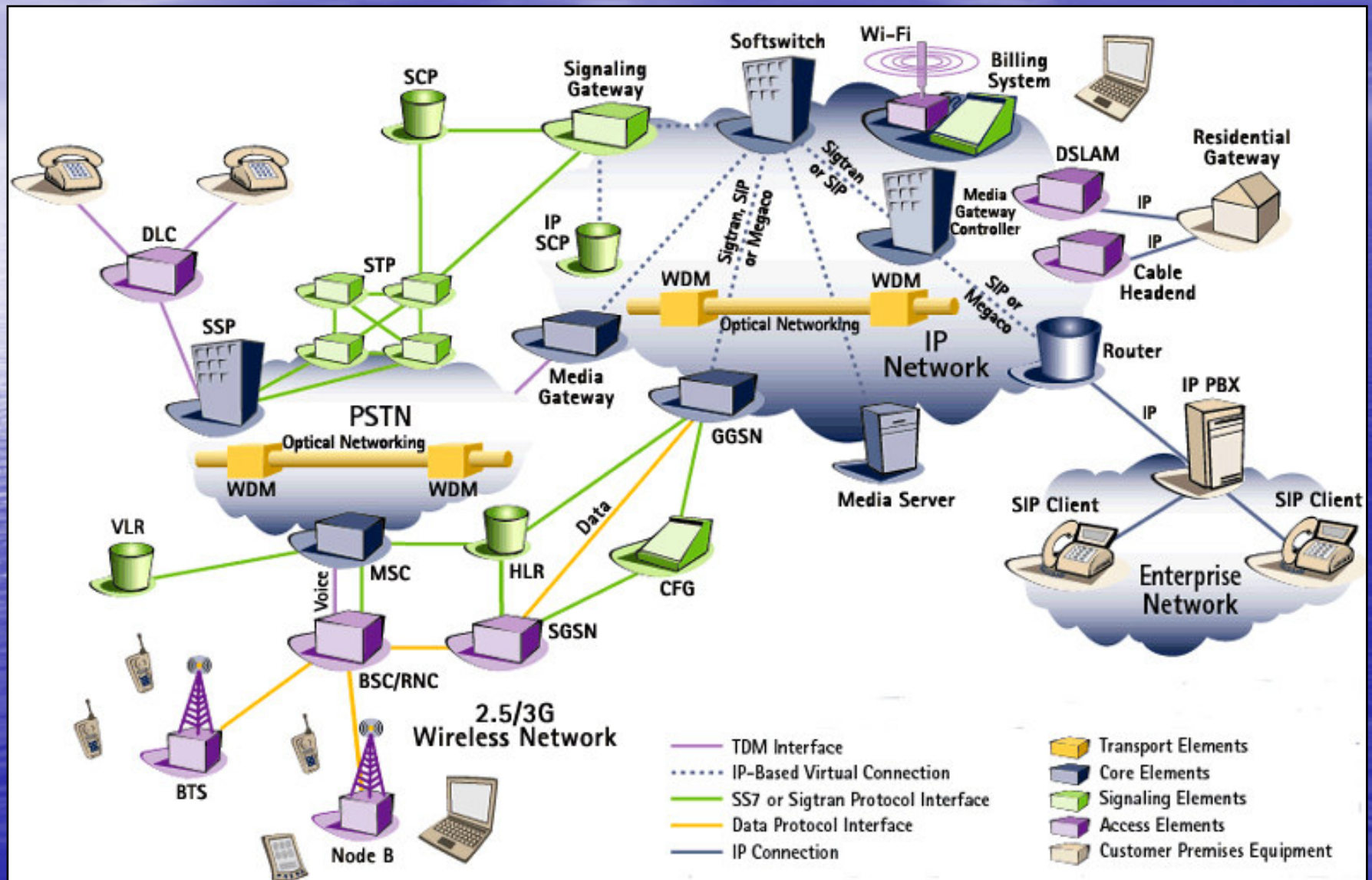
- Creation of **ghost numbering trees**
- **Forwarding** loops
- Modification of **roaming profiles**
- Creation of **ghosts subscriptions** on HLR
- Special **CDR** (Charging Data Record) generation rules
- DoS / harassment / pranks
- **Injected SS7** protocol messages

Intelligent Network



- UNIX high-available clusters outside of core network (SCP, SMP, SCE)
- Interrupt call-control, execute logic, resume control
- Toll-free (e.g. +800), prepaid (real-time credit control), VPN (PABX-like), etc.
- Based on SS7 INAP and CAMEL protocols

IN Overview



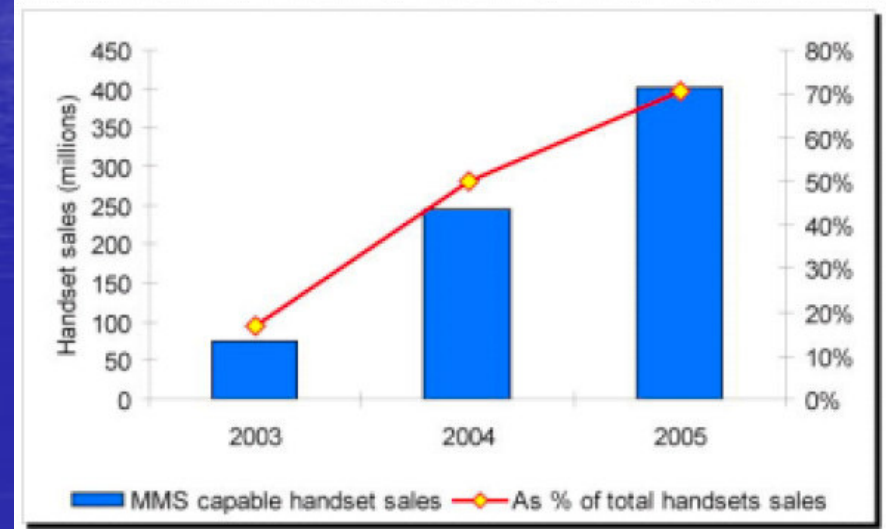
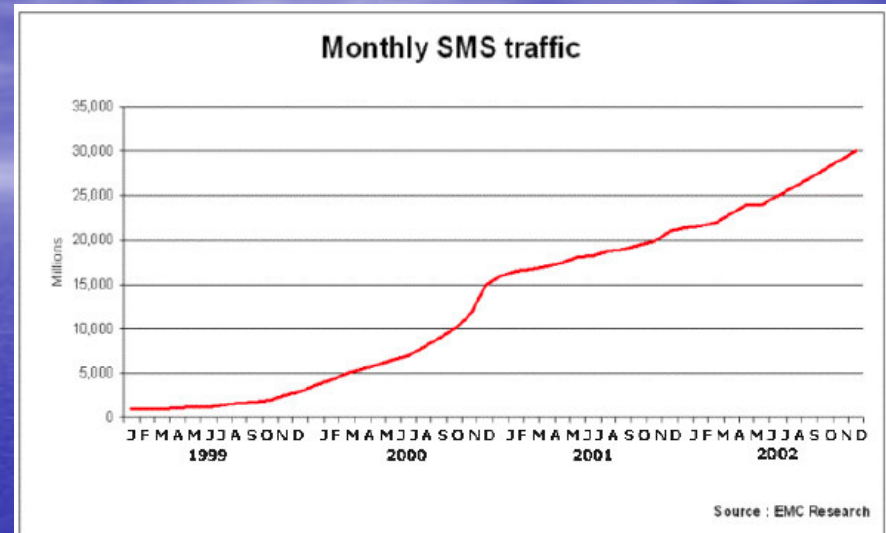
Examples of IN attacks



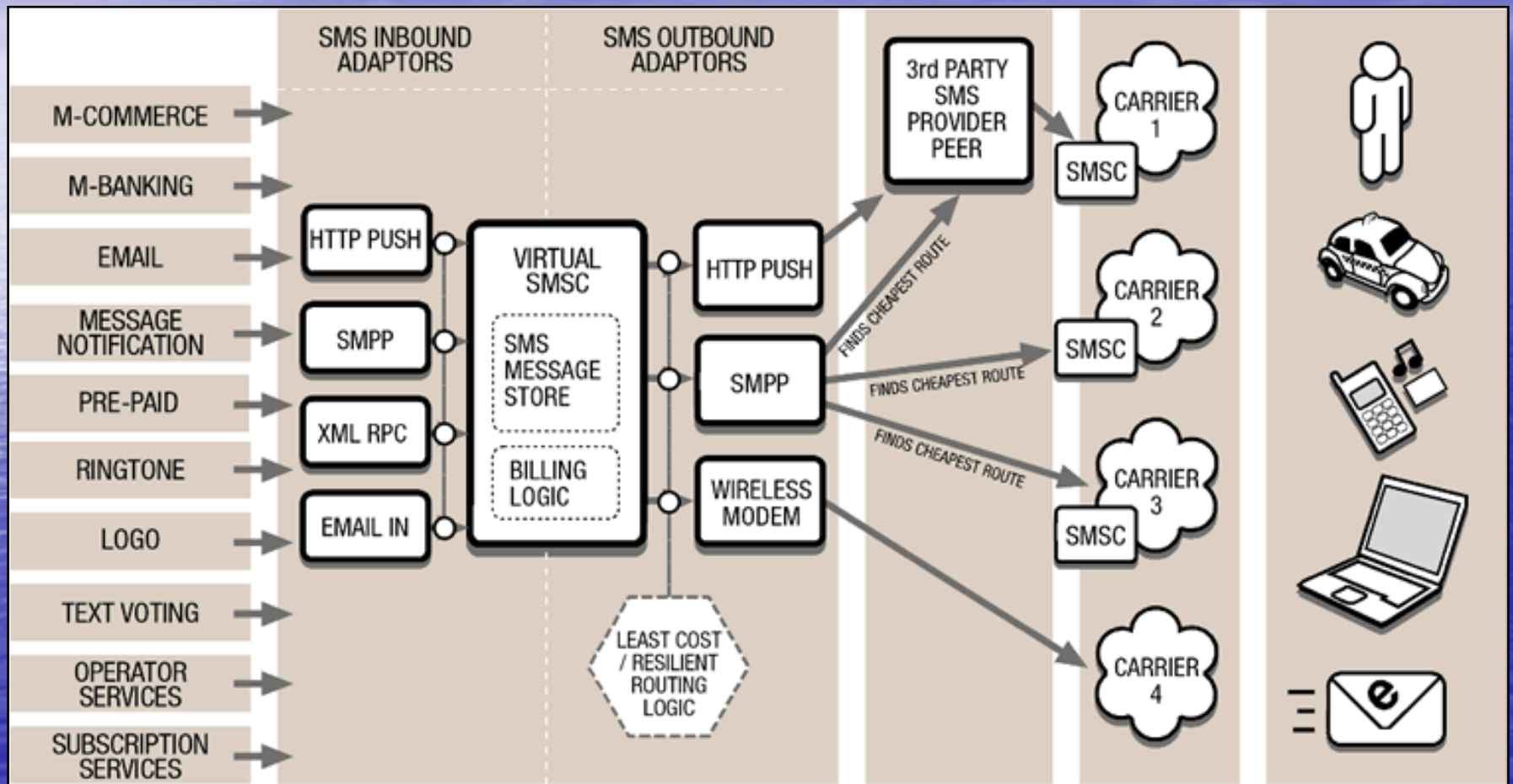
- Modification of Prepaid account DB
- Creation of ghost 800 numbers
- Tracing of subscriber activity
- Fake trigger in SSP + fake service in SCP
- CDR generation special rules
- Modification of charging tables
- Unauthorized forwarding
- Unauthorized supplementary services

Messaging

- SMS “after-thought” in GSM design, uses SS7 transport, involves MSC/HLR/VLR
- Messages are handled with “store and forward” mechanism on an SMSC
- MMS extends the concept with multimedia capabilities and uses MMSC for delivery
- USSD messages
- Voice Mail (VMS)



SMS growth

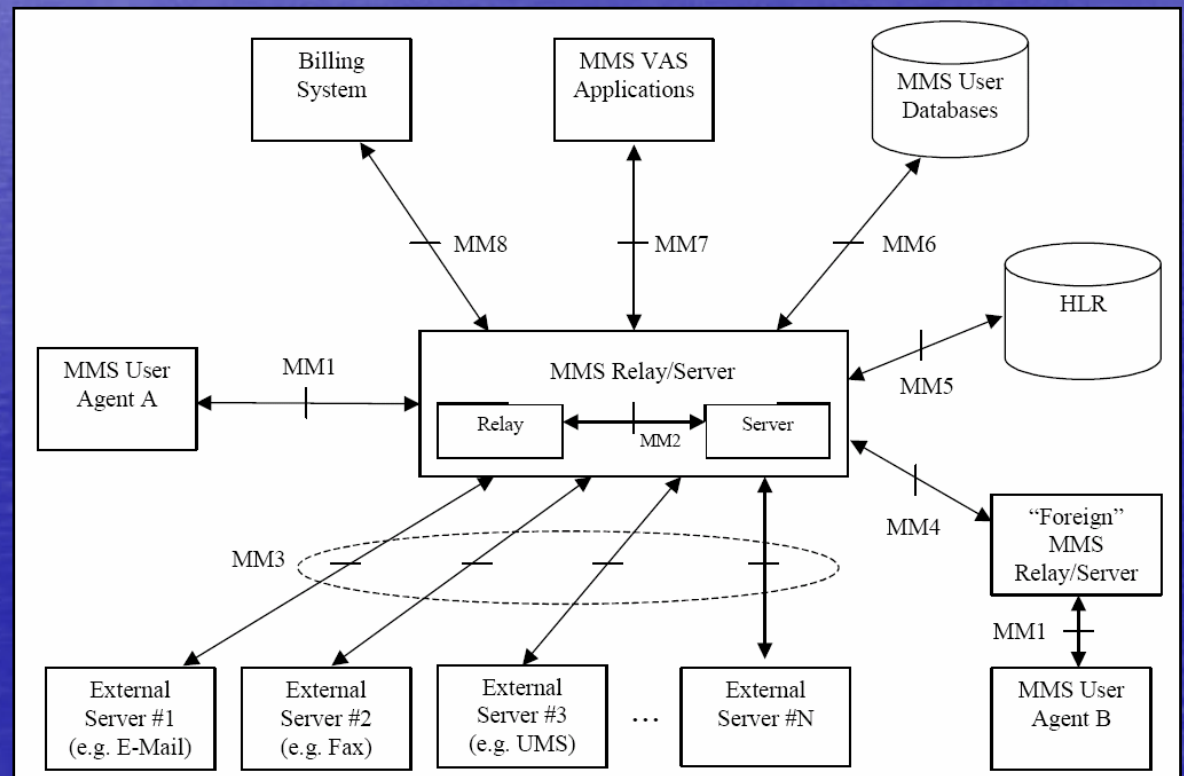


Examples of Messaging attacks

- **Interception** of messages on SMSC
- **Injection** of messages (spam...)
- Modified MS can craft **evil messages**
- SS7 and IP **connectivity**
- VMS hacks (e.g. **callout**)
- Special **USSD** sequences

MMS Architecture Model

- MMS brings the IP world one step closer to the GSM/3G network core
- The MMSC connects to the HLR using SS7 and to the IP network for transport, billing and management
- MMSE can be deployed outside of network operators' infrastructures



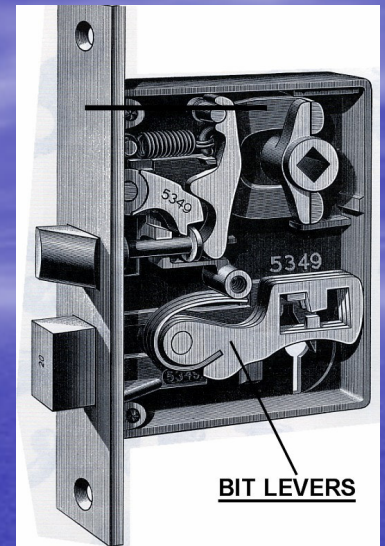
MMS Security (from 3gpp)



- The user shall be able to use and access MM in a secure manner. It shall be possible for the contents of MM to be read only by the intended recipient.
- A Recipient shall be informed of the reliability of the sender in case the sender has authorized his identity to be transmitted.
- The integrity of MM during transit shall be assured to the extent of the network capabilities.
- The MMS shall be intrinsically resistant to attempts of malicious or fraudulent use.
- The MMS shall have the ability to authenticate the user regardless of access technology.
- The MMS shall support data transport in a secure manner between the user and MMS The MMS authentication scheme shall use access specific information.

MMS security in practice

- Not all communications encrypted and authenticated
- Vulnerabilities in GRX protocol
- MAP security not fully implemented
- DNS security not implemented
- WAP gap in WTLS sessions with UA
- Service Initiation Request can force another gateway
- SMS traffic not encrypted
- TLS/SSL on SMTP not always implemented
- No IPsec between MMSC and MMS brokers or VAS
- No proper certificates and keys management
- SOAP security not fully implemented
- Hostile UA and VAS can induce DoS, virus, faulty charging, spam
- SMIL and XHTML presentation and synchronization vulnerabilities



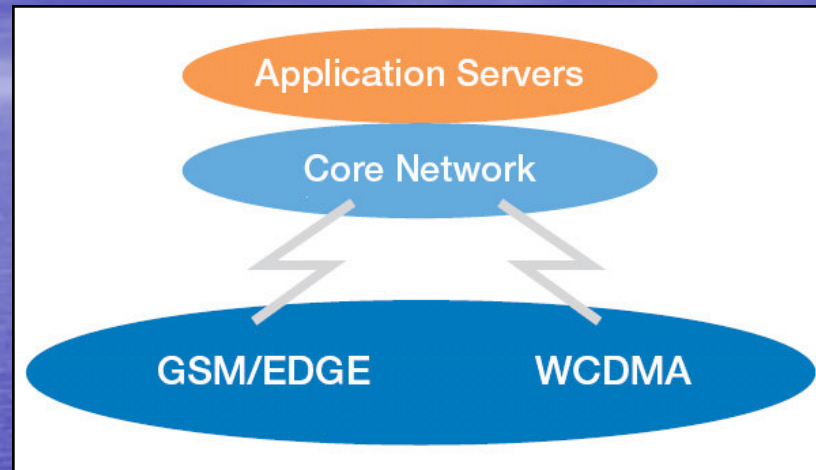
MMS as a viral vector

Quote from "MMS Security Consideration"

- " Currently the majority of handsets are based on **closed OS systems** built on more or less proprietary hardware. To some extent **this act as protection against buffer overflow** attacks that try to execute a malicious application. "

Yeah, right !!

GPRS / EDGE / 3G



- Data rates evolution (CSD kb/s, 3G mb/s)
- Architecture evolution (Wideband CDMA)
- Internet integration (TCP/IP)
- New services (email, web, push/pull, etc.)

Examples of GPRS/3G attacks

- See Ollie Whitehouse: the best authority on the topic!



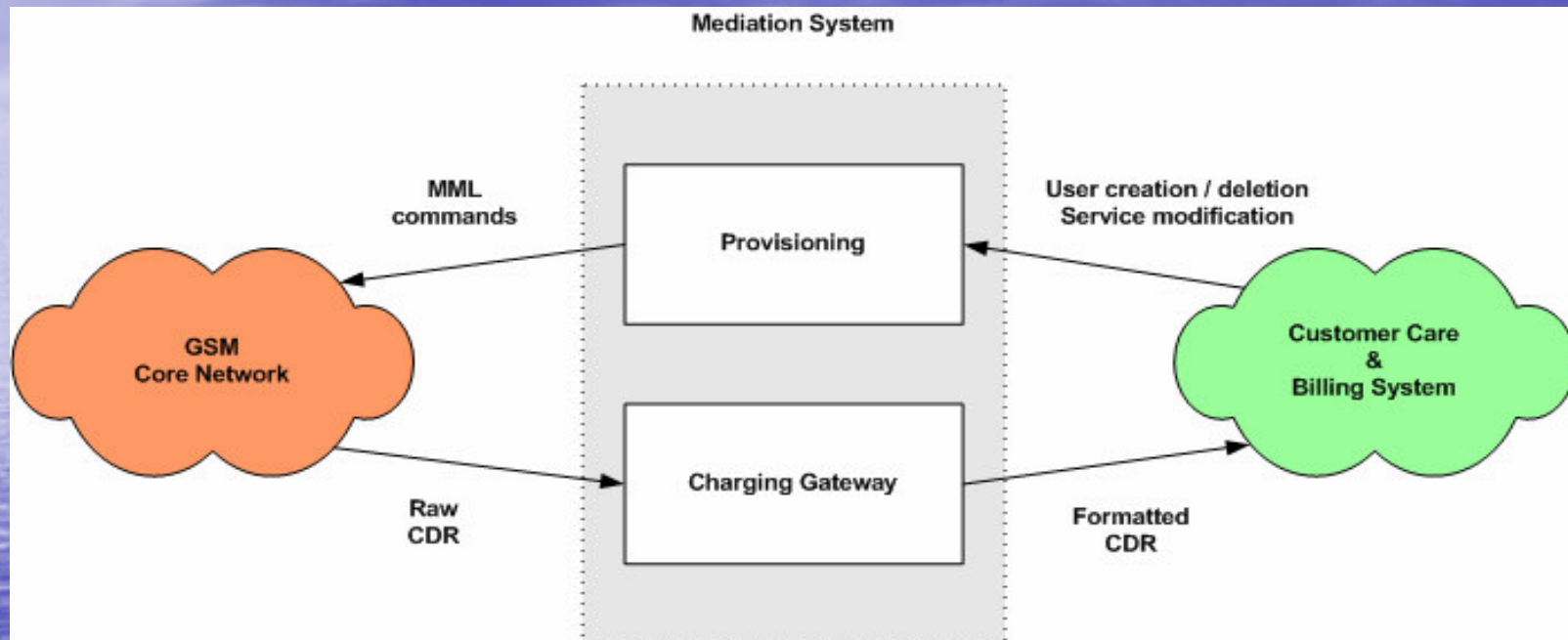
Network Management

- UNIX clusters (comms, DB, applications)
 - Events, Alarms, Measurements
 - Software upload, configuration, integration, remote diagnostics
 - Access to every single NE, parameter, option, frequency, power level, etc.
- *NMS/OSS systems can be access over IP, X.25 and remote access dialups*

Example of NMS/OSS attacks

- DoS on any Network Element
- Confidential information leak (e.g. design)
- Easy access to all NE (cleartext password, config files, scripts, DB connections, etc.)
- Access to private X.25 and IP sensitive areas such as VAS clusters, IN, etc.
- User-friendly subscriber tracing

Mediation and Billing



- 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

Billing Processes

The diagram illustrates the Billing Processes, centered around the **Billing System & Golden Database**, which manages customer and service administration, personalisation, content management, tariffing, SIM and number management, provisioning requests, call data collection, rating and billing (roaming, retail and interconnect), and payment collection.

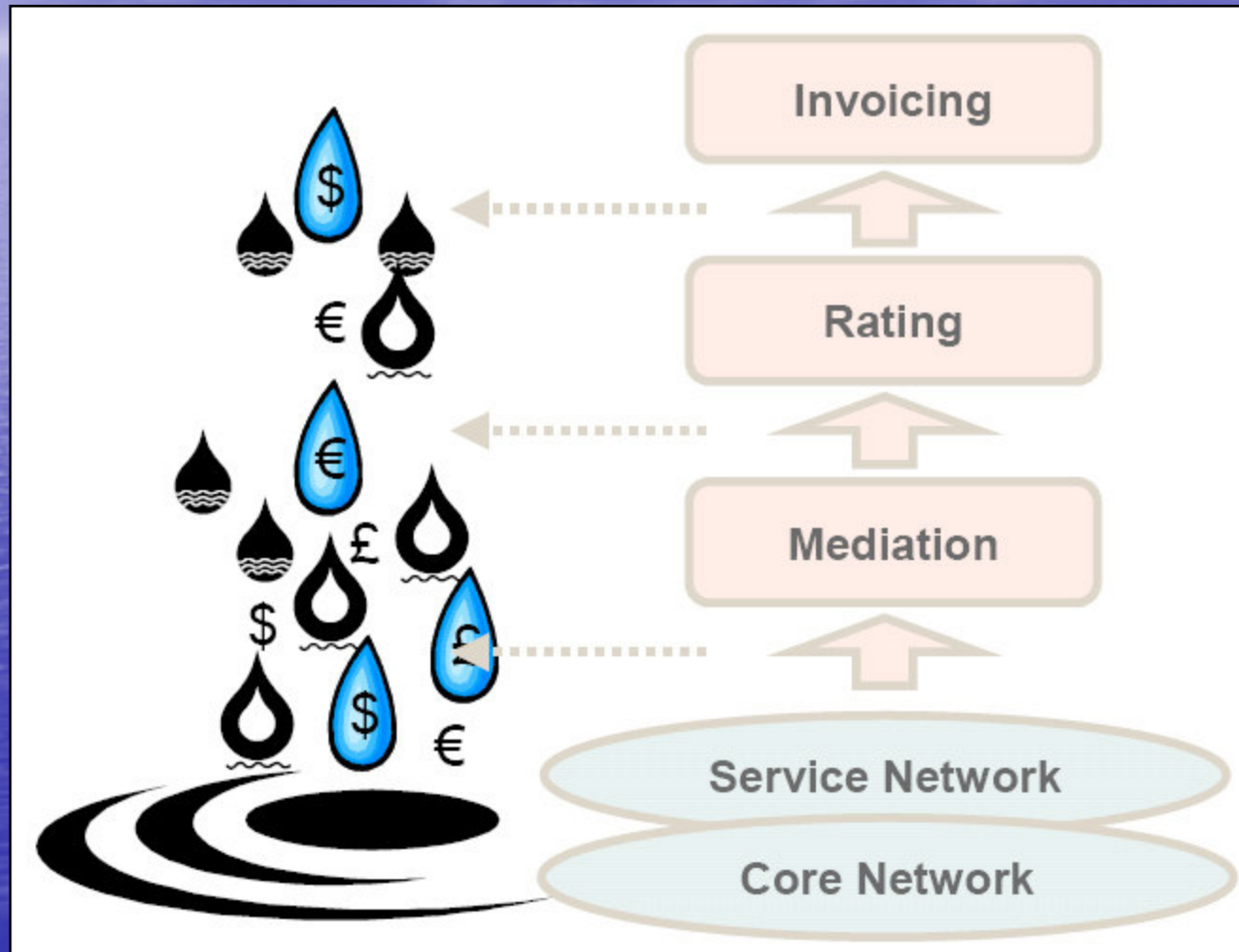
Key Components and Interactions:

- Payment Systems:** Includes **BANK** (DD payments, DD Returns), **CARD AUTHORISATION** (Card payments & authorisation), **CARD PAYMENTS (EFT)** (Card payments), **BANK I/F** (DD payments, DD Returns), **E-Wallet** (Small Purchases, Roaming call data), and **TAP CLEARING HOUSE** (Customer and subscription data).
- Reporting and Data:** **Reporting** feeds into the Billing System. **Mediation System** handles service requests and responses, normalised call data, and call data transfer to the **BGW Billing gateway**.
- Service and Network:** **SOG Service activation gateway** and **ISCP** (Interconnect Service Control Point) are linked to the Billing System. **SGSN**, **GGSN**, **WAP**, **VMS**, **SMC**, **AuC**, **HLR**, and **MSC** are connected to the **IN Platform** and **IVR**.
- Internal Tools and Data:** **CRM Tool** (Manage customer tasks to completion) is a central hub for **Customer details**, **Normalised address**, **CREDIT CHECK**, **BLACKLIST ?**, **POS Activation**, **Document Imaging**, **FRAUD**, **Ernie**, **PRINTING**, **SAP** (Sales support, logistics and finance processing, Human Resource, and Materials Management), **WCS Shops**, **Retail Outlets**, **Logistics Company**, **GIS** (Geographical Information System), **Radio planning tool**, **IMS** (Sites administration, BTS build provision and transmission, operations and network faults logging), **Site rental Assets**, **Bad Debt Database**, **Subscriber data** (Rated CDRs, Pre-pay CDRs, Unrated CDRs), **Ernie**, **PRINTING**, **SIM Manufacturer**, **Commissions** (Sales and Dealer), **BANK I/F**, **Data Warehouse**, **Electronic Queue Manager** (Service Centre Queue measurement tool), **Multi Media**, **Customer call**, **IVR** (Identify customer, preference and satisfy simple queries), **Predictive Dialler**, **O/S** (Operator services Directory inquiries), **Scholar** (Knowledge System On-line call centre reference), **Isaac** (Case Based Reasoning Tool Diagnose problems and recommend solutions), **Screen navigation**, **Query type**, **Recommendation**, **Screen navigation**, **Signal strength and coverage**, **Sites, faults & Links**, **Shops & Dealers**, **Financial/Inventory Material master**, **Outbound** (Goods invt inbound, Picking conf. inbound, Change serial# kits, Physical inv. inbound), **Dispatch SIM** (SIM orders, dispatched SIMS, Dealer codes, activation information, money back deactivations, general ledger updates), **Dispatch SIM** (SIM orders, dealers codes GL updates & Roaming), **Service requests and responses**, **Normalised call data**, **Call data**, **Service requests, and responses**, **Customer details, Credit score result**, **Customer details**, **Customer and subscription data, and real time billing**, **External Billing for content supply**, **Security. Certification and encryption**, **Multiple Fulfillment Vendors.** (Information access, supply for Internet information (APIs) and Interactive TV), **Portal.** (Information access device for Internet information (APIs)), **To WAP, SMSC, IN etc.**, **www**, **ID & Address Validation**, **CREDIT CHECK**, **BLACKLIST ?**, **Electronic Queue Manager** (Service Centre Queue measurement tool), **Multi Media**, **Customer call**, **IVR** (Identify customer, preference and satisfy simple queries), **Predictive Dialler**, **O/S** (Operator services Directory inquiries), **Scholar** (Knowledge System On-line call centre reference), **Isaac** (Case Based Reasoning Tool Diagnose problems and recommend solutions), **Screen navigation**, **Query type**, **Recommendation**, **Screen navigation**, **Signal strength and coverage**, **Sites, faults & Links**, **Shops & Dealers**, **Financial/Inventory Material master**, **Outbound** (Goods invt inbound, Picking conf. inbound, Change serial# kits, Physical inv. inbound), **Dispatch SIM** (SIM orders, dispatched SIMS, Dealer codes, activation information, money back deactivations, general ledger updates), **Dispatch SIM** (SIM orders, dealers codes GL updates & Roaming), **Service requests and responses**, **Normalised call data**, **Call data**, **Service requests, and responses**, **Customer details, Credit score result**, **Customer details**, **Customer and subscription data, and real time billing**, **External Billing for content supply**, **Security. Certification and encryption**, **Multiple Fulfillment Vendors.** (Information access, supply for Internet information (APIs) and Interactive TV), **Portal.** (Information access device for Internet information (APIs)), **To WAP, SMSC, IN etc.**, **www**, **ID & Address Validation**, **CREDIT CHECK**, **BLACKLIST ?**, **Electronic Queue Manager** (Service Centre Queue measurement tool), **Multi Media**, **Customer call**, **IVR** (Identify customer, preference and satisfy simple queries), **Predictive Dialler**, **O/S** (Operator services Directory inquiries), **Scholar** (Knowledge System On-line call centre reference), **Isaac** (Case Based Reasoning Tool Diagnose problems and recommend solutions), **Screen navigation**, **Query type**, **Recommendation**, **Screen navigation**, **Signal strength and coverage**, **Sites, faults & Links**, **Shops & Dealers**, **Financial/Inventory Material master**, **Outbound** (Goods invt inbound, Picking conf. inbound, Change serial# kits, Physical inv. inbound), **Dispatch SIM** (SIM orders, dispatched SIMS, Dealer codes, activation information, money back deactivations, general ledger updates), **Dispatch SIM** (SIM orders, dealers codes GL updates & Roaming), **Service requests and responses**, **Normalised call data**, **Call data**, **Service requests, and responses**, **Customer details, Credit score result**, **Customer details**, **Customer and subscription data, and real time billing**, **External Billing for content supply**, **Security. Certification and encryption**, **Multiple Fulfillment Vendors.** (Information access, supply for Internet information (APIs) and Interactive TV), **Portal.** (Information access device for Internet information (APIs)), **To WAP, SMSC, IN etc.**, **www**, **ID & Address Validation**, **CREDIT CHECK**, **BLACKLIST ?**, **Electronic Queue Manager** (Service Centre Queue measurement tool), **Multi Media**, **Customer call**, **IVR** (Identify customer, preference and satisfy simple queries), **Predictive Dialler**, **O/S** (Operator services Directory inquiries), **Scholar** (Knowledge System On-line call centre reference), **Isaac** (Case Based Reasoning Tool Diagnose problems and recommend solutions), **Screen navigation**, **Query type**, **Recommendation**, **Screen navigation**, **Signal strength and coverage**, **Sites, faults & Links**, **Shops & Dealers**, **Financial/Inventory Material master**, **Outbound** (Goods invt inbound, Picking conf. inbound, Change serial# kits, Physical inv. inbound), **Dispatch SIM** (SIM orders, dispatched SIMS, Dealer codes, activation information, money back deactivations, general ledger updates), **Dispatch SIM** (SIM orders, dealers codes GL updates & Roaming), **Service requests and responses**, **Normalised call data**, **Call data**, **Service requests, and responses**, **Customer details, Credit score result**, **Customer details**, **Customer and subscription data, and real time billing**, **External Billing for content supply**, **Security. Certification and encryption**, **Multiple Fulfillment Vendors.** (Information access, supply for Internet information (APIs) and Interactive TV), **Portal.** (Information access device for Internet information (APIs)), **To WAP, SMSC, IN etc.**, **www**, **ID & Address Validation**, **CREDIT CHECK**, **BLACKLIST ?**, **Electronic Queue Manager** (Service Centre Queue measurement tool), **Multi Media**, **Customer call**, **IVR** (Identify customer, preference and satisfy simple queries), **Predictive Dialler**, **O/S** (Operator services Directory inquiries), **Scholar** (Knowledge System On-line call centre reference), **Isaac** (Case Based Reasoning Tool Diagnose problems and recommend solutions), **Screen navigation**, **Query type**, **Recommendation**, **Screen navigation**, **Signal strength and coverage**, **Sites, faults & Links**, **Shops & Dealers**, **Financial/Inventory Material master**, **Outbound** (Goods invt inbound, Picking conf. inbound, Change serial# kits, Physical inv. inbound), **Dispatch SIM** (SIM orders, dispatched SIMS, Dealer codes, activation information, money back deactivations, general ledger updates), **Dispatch SIM** (SIM orders, dealers codes GL updates & Roaming), **Service requests and responses**, **Normalised call data**, **Call data**, **Service requests, and responses**, **Customer details, Credit score result**, **Customer details**, **Customer and subscription data, and real time billing**, **External Billing for content supply**, **Security. Certification and encryption**, **Multiple Fulfillment Vendors.** (Information access, supply for Internet information (APIs) and Interactive TV), **Portal.** (Information access device for Internet information (APIs)), **To WAP, SMSC, IN etc.**, **www**, **ID & Address Validation**, **CREDIT CHECK**, **BLACKLIST ?**, **Electronic Queue Manager** (Service Centre Queue measurement tool), **Multi Media**, **Customer call**, **IVR** (Identify customer, preference and satisfy simple queries), **Predictive Dialler**, **O/S** (Operator services Directory inquiries), **Scholar** (Knowledge System On-line call centre reference), **Isaac** (Case Based Reasoning Tool Diagnose problems and recommend solutions), **Screen navigation**, **Query type**, **Recommendation**, **Screen navigation**, **Signal strength and coverage**, **Sites, faults & Links**, **Shops & Dealers**, **Financial/Inventory Material master**, **Outbound** (Goods invt inbound, Picking conf. inbound, Change serial# kits, Physical inv. inbound), **Dispatch SIM** (SIM orders, dispatched SIMS, Dealer codes, activation information, money back deactivations, general ledger updates), **Dispatch SIM** (SIM orders, dealers codes GL updates & Roaming), **Service requests and responses**, **Normalised call data**, **Call data**, **Service requests, and responses**, **Customer details, Credit score result**, **Customer details**, **Customer and subscription data, and real time billing**, **External Billing for content supply**, **Security. Certification and encryption**, **Multiple Fulfillment Vendors.** (Information access, supply for Internet information (APIs) and Interactive TV), **Portal.** (Information access device for Internet information (APIs)), **To WAP, SMSC, IN etc.**, **www**, **ID & Address Validation**, **CREDIT CHECK**, **BLACKLIST ?**, **Electronic Queue Manager** (Service Centre Queue measurement tool), **Multi Media**, **Customer call**, **IVR** (Identify customer, preference and satisfy simple queries), **Predictive Dialler**, **O/S** (Operator services Directory inquiries), **Scholar** (Knowledge System On-line call centre reference), **Isaac** (Case Based Reasoning Tool Diagnose problems and recommend solutions), **Screen navigation**, **Query type**, **Recommendation**, **Screen navigation**, **Signal strength and coverage**, **Sites, faults & Links**, **Shops & Dealers**, **Financial/Inventory Material master**, **Outbound** (Goods invt inbound, Picking conf. inbound, Change serial# kits, Physical inv. inbound), **Dispatch SIM** (SIM orders, dispatched SIMS, Dealer codes, activation information, money back deactivations, general ledger updates), **Dispatch SIM** (SIM orders, dealers codes GL updates & Roaming), **Service requests and responses**, **Normalised call data**, **Call data**, **Service requests, and responses**, **Customer details, Credit score result**, **Customer details**, **Customer and subscription data, and real time billing**, **External Billing for content supply**, **Security. Certification and encryption**, **Multiple Fulfillment Vendors.** (Information access, supply for Internet information (APIs) and Interactive TV), **Portal.** (Information access device for Internet information (APIs)), **To WAP, SMSC, IN etc.**, **www**, **ID & Address Validation**, **CREDIT CHECK**, **BLACKLIST ?**, **Electronic Queue Manager** (Service Centre Queue measurement tool), **Multi Media**, **Customer call**, **IVR** (Identify customer, preference and satisfy simple queries), **Predictive Dialler**, **O/S** (Operator services Directory inquiries), **Scholar** (Knowledge System On-line call centre reference

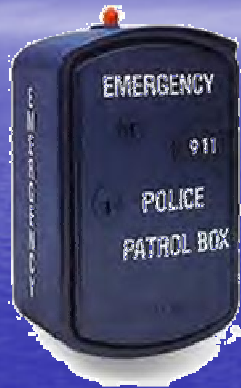
Attacks on Mediation / Billing

- Raw **database edit**. Conveniently deletes selected records containing billing data.
- Modification of the **charging tables** in the billing system
- Patching of the rater application to **eliminate certain CDR** e.g. belonging to a given MSISDN
- Backdoors in mediation gateways to **remove CDR data**
- Confidential **information leak** on subscribers activities (numbers called, received, SMS, data, etc.)
- Modification of **CDR processing** rules
- Modification of "**test numbers**" whitelist
- **Live patching** of CDR data while in mediation queue
- Patching of **mediation application** (e.g. loading scripts)
- GPRS packet aggregation **rules modification**

Revenue Leakage



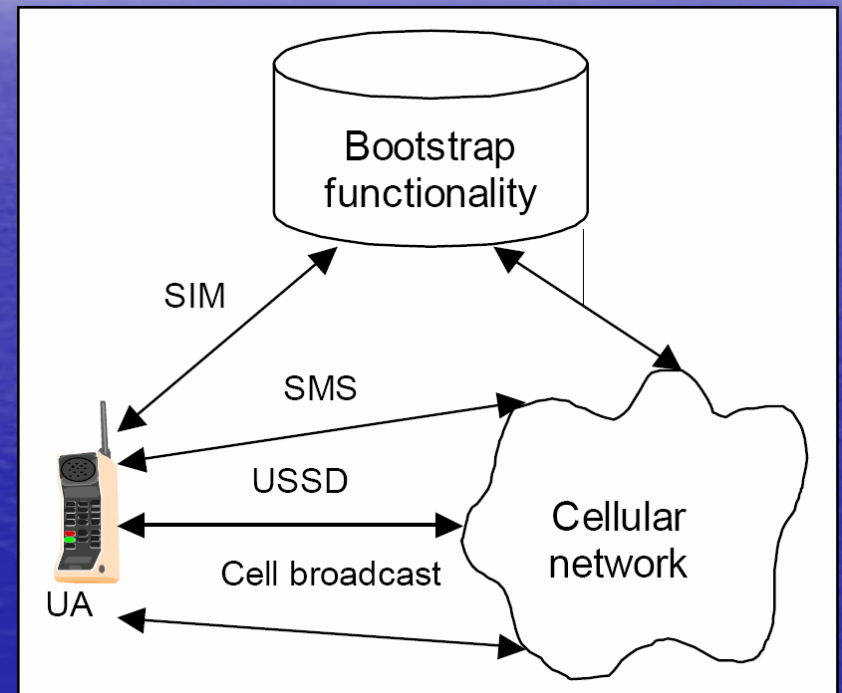
Legal Interception Gateway



- Legal Interception Gateway is used by **police** and **intelligence agencies**.
- Connected to **MSC** through 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 – a phreaker's dream!
- Could **compromise the agencies'** own facilities.

OTA and SIM applications

- Over-The-Air methods allow **provisioning of new applications** or modification of parameters
- Example: **SIM Toolkit** (STK) applications can be uploaded, new services numbers updated, email servers modified
- **OTA server** is a UNIX cluster located in VAS area. Reachable over IP.



Authentication Vectors



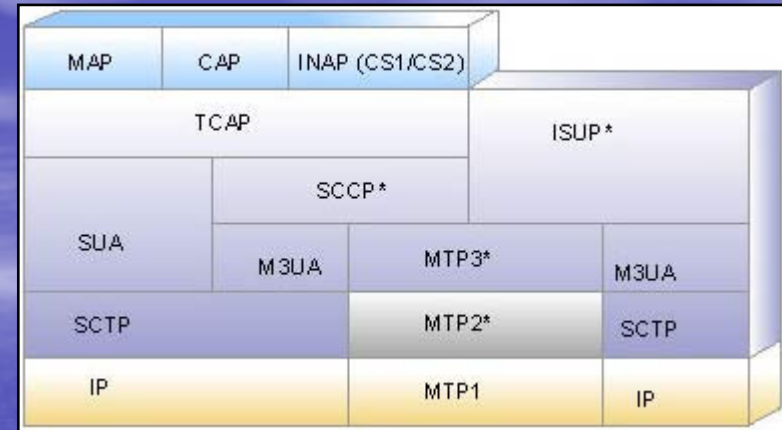
- GSM started with questionably **weak crypto** (weaknesses found in COMP-128 and A5 algorithm)
- **Cloning** of SIM cards is possible (first in hours, then minutes, now over-the-air)
- **New algorithms** e.g. A5/3 fixes vulnerabilities. 3G/UMTS security models introduce stronger cryptography
- However **cryptographic secrets are stored in the AuC** where they can generally easily be retrieved using MML commands or raw DB edit.
- The provisioning cycle of the SIM (e.g. loading Ki into the AuC) uses **insecure** methods (clear files, FTP transfers, multiple copies of files, etc.)



SS7

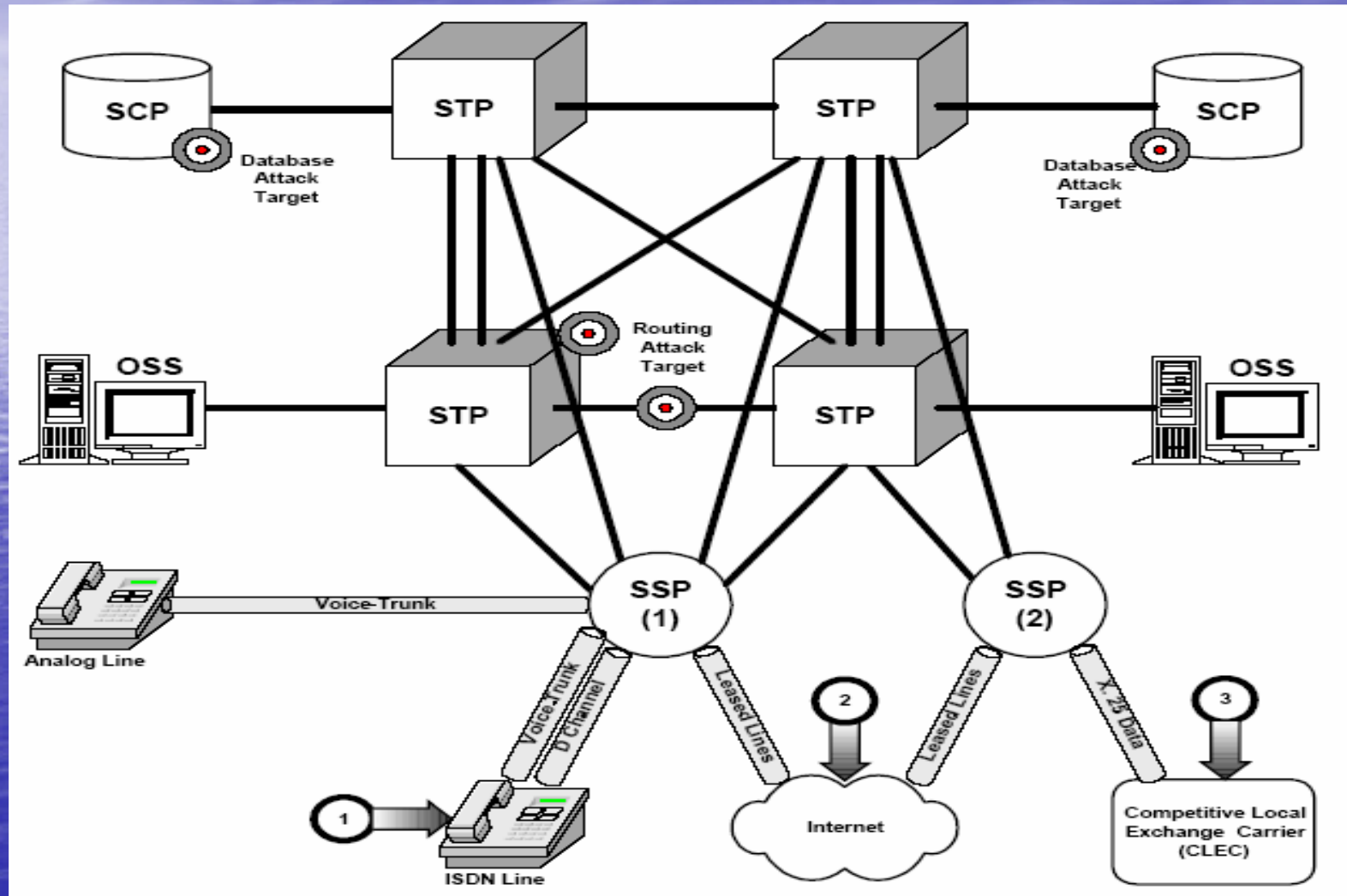
Digital Signalling Standard

SS7 Signalling



- 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 entry points



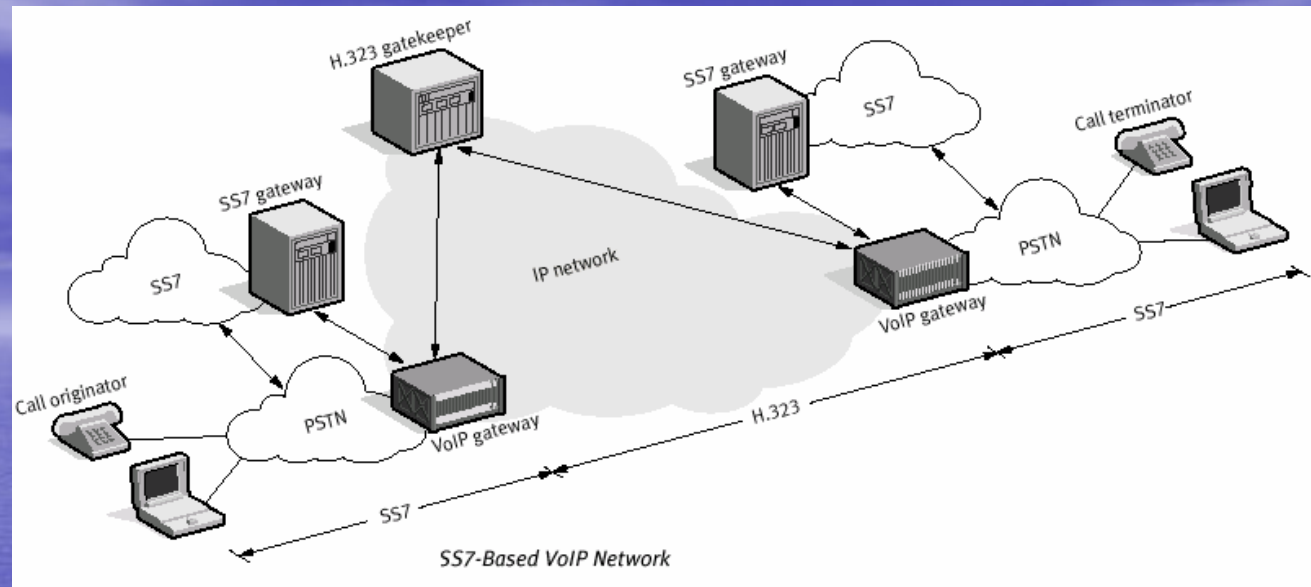
Examples of SS7 attacks

- Theft of service, interception of calling cards numbers, privacy concerns
- Introduce harmful packets into the national and global SS7 networks
- Get control of call processing, get control of accounting reports
- Obtain credit card numbers, non-listed numbers, etc.
- Messages can be read, altered, injected or deleted
- Denial of service, security triplet replay to compromise authentication
- Annoyance calls, free calls, disruption of emergency services
- Capture of gateways, rerouting of call traffic
- Disruption of service to large parts of the network
- Call processing exposed through Signaling Control Protocol
- Announcement service exposed to IP through RTP
- Disclosure of bearer channel traffic

SS7 attacks taxonomy

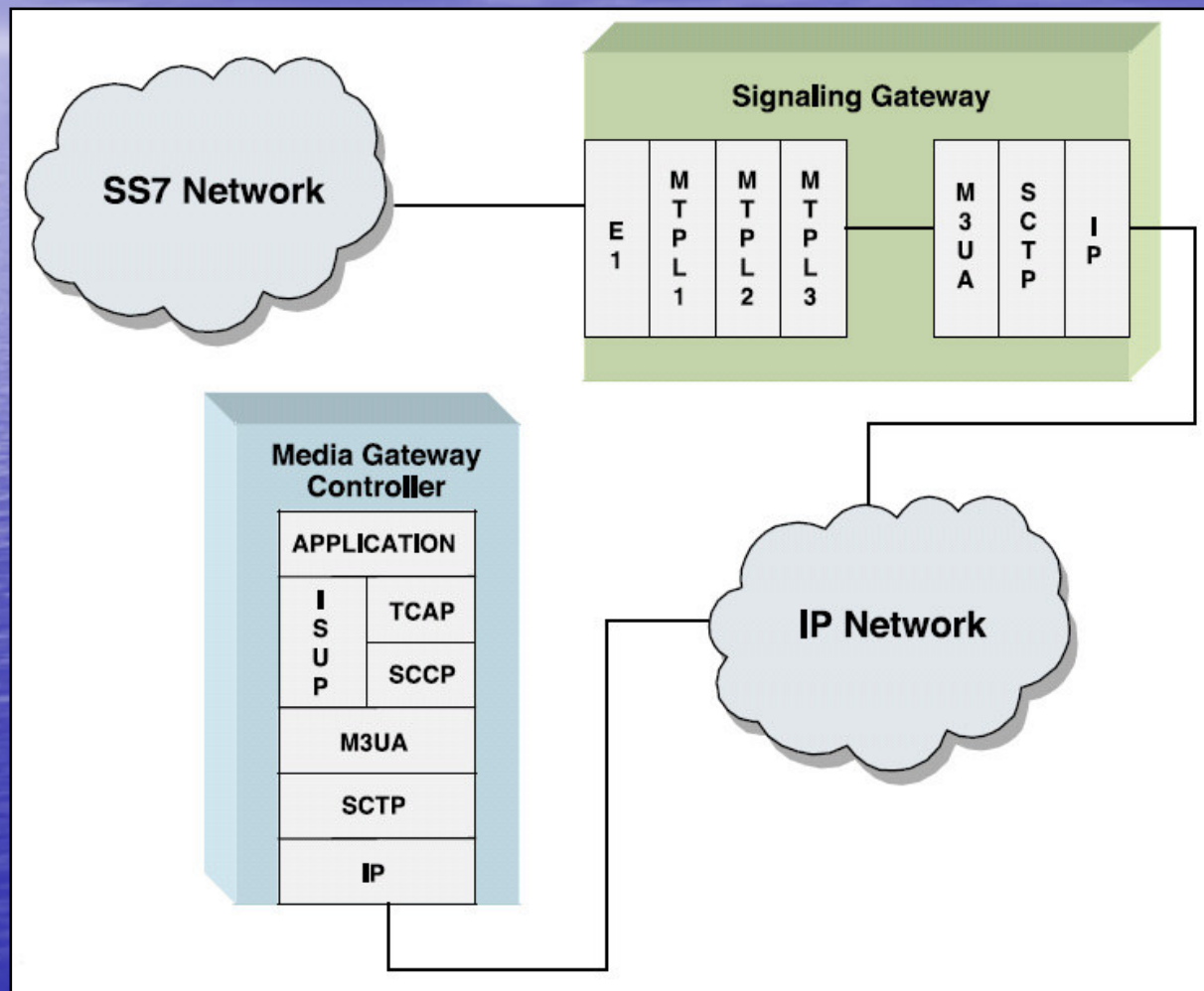
	MODIFICATION	INTERCEPTION	INTERRUPTION	FABRICATION
SSP	Physical Modification * Hardware Configuration ISDN End User * ISUP Msg. Modification	Eavesdropping (Software) * SS7 Packet Sniffing * SS7 Authentication Attack * Stealth Conference Calls	Denial of Service (Software) * SS7 Authentication Attack * Routing DB Attack * MTP Link Management Attack	Spoofing (Software) * SS7 Authentication Attack * ISUP, ANI Spoof Eavesdropping (Software) * SSP Impersonation * ISUP Msg. Generation
STP	Toll Fraud (Software) * OSS Attack Eavesdropping * Routing DB Attack * SCCP Msg. Rerouting Attack	Eavesdropping (Software) * SS7 Packet Sniffing * SCCP / Global Title Translation Attack	Denial of Service (Software) * OSS Component Destruction * Virus, Worm, Trojan Horse * Routing DB Deletion * LNP DB Attack * SCCP Msg. Alteration * MTP Link Management Attack	Eavesdropping (Software) * STP Impersonation * SCCP Msg. Generation
SCP	Toll Fraud (Software) * LIDB (Billing) Alteration * CMSDB (Toll Free) Alteration * Credit Insertion * Advanced Service Fraud * TCAP Msg. Modification Eavesdropping * Speed Dialing DB Attack * Number Translation DB Attack	Eavesdropping (Software) * SS7 Packet Sniffing * Voice Mail Snooping * Unauthorized SCP Browsing * TCAP Modification * Stealth Conference Calls	Denial of Service (Software) * Call Forwarding DB Deletion * Number Translation Deletion * Call Forwarding DB Deletion * Speed Dialing DB Deletion * Voice Mail DB Deletion * LNP DB Attack * TCAP Msg. Alteration * MTP Link Management Attack	Eavesdropping (Software) * Call Forwarding DB Insertion * SCP Impersonation * SCCP, TCAP Msg. Generation * TCAP DB Query Fabrication

VoIP Evolution



- There is also exponential growth in the use of interconnection between the telecommunication networks and the Internet, for example with VoIP protocols (e.g. SIP, SCTP, M3UA, etc.)
- 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 security exposure increases

- Increased number of access points and networking
- Increased number of interconnected inexperienced systems administrators and processes
- Embedded Operations Channels of Signaling and Transport Protocols (e.g., SONET DCC, ATM OAM Cells, SS7 Network Management Messages) gives virtually unlimited access to everything to them
- Internet and Intranet Exploitable technology used for access to Network Operations and Signaling Systems
- Added complexity, dependencies and single points of failure

Based on the success with which hackers and other (admittedly small-time) intruders have invaded or subverted parts of the network, it is not unreasonable to expect that a malicious assault upon the PSTN by a serious team of aggressors attacking multiple targets has a realistic chance of forcing an outage of large scale and broad geographic range.

The expertise required to pull off such an attack is not extreme, and is in fact within the capabilities of many technically competent, computer-literate people around the world. Because the service providers have no experience with this kind of forced outage, they may be unprepared to recover from it as promptly and successfully as they recover from natural disasters or equipment failures.

SS7 Security Solutions

- SS7 firewalls are introduced to become 'packet cops' like early IP firewalls
- Access Control modules on network elements ensure only authorized users can access
- SS7 scanners can help in identifying weaknesses in an operators' infrastructure

After all, implementing IP firewalls was enough to stop all the IP hackers on the Internet, right??

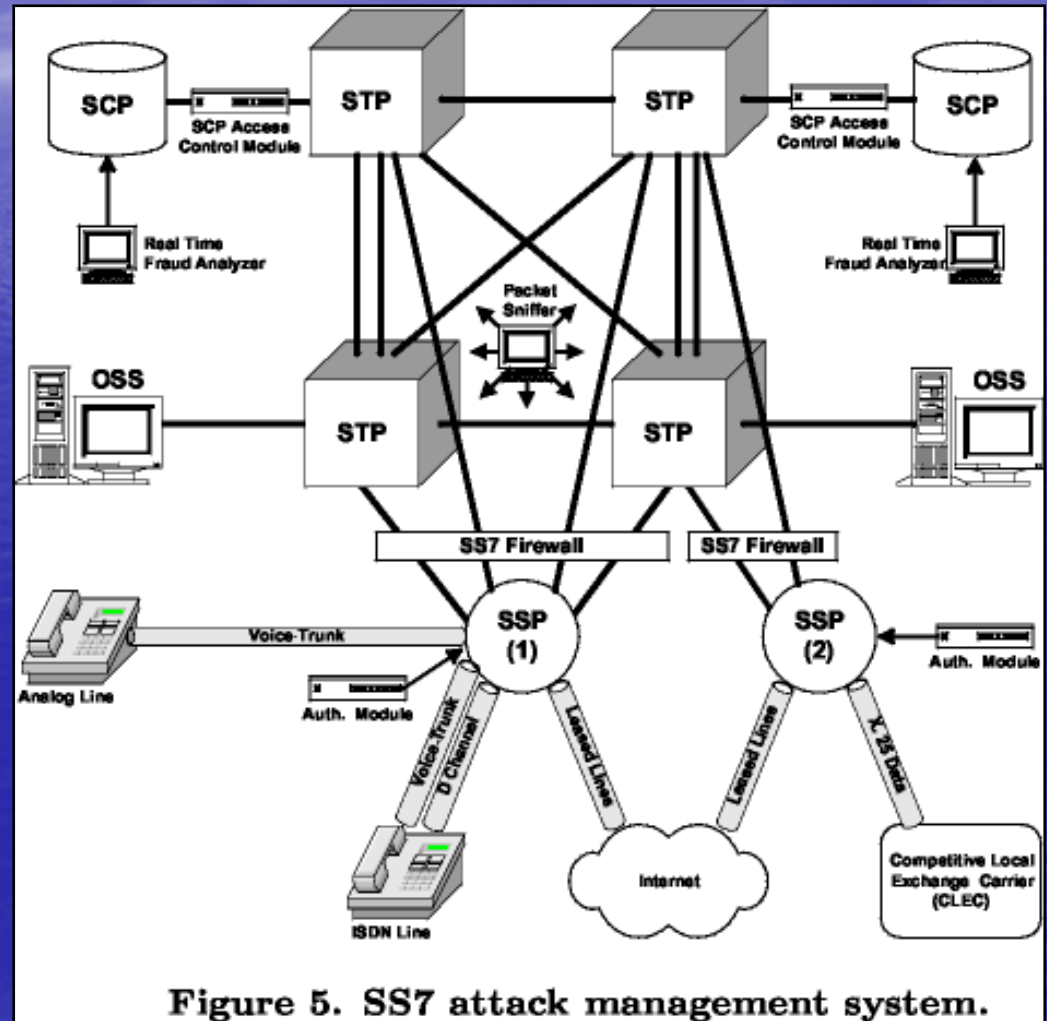
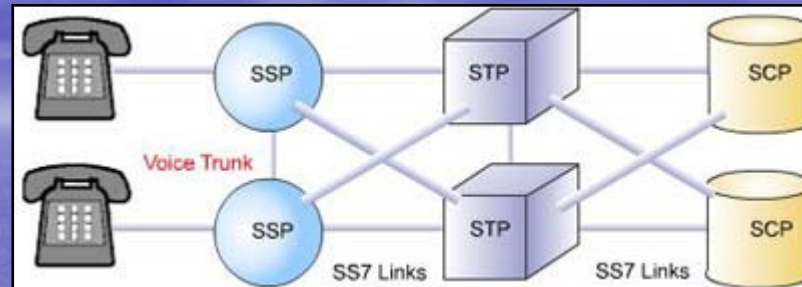


Figure 5. SS7 attack management system.

SS7: a closed network



- With a limited number of carriers and limited points of interconnection, the operators could assume with fair certainty that all of the elements passing data were trusted sources.
- Unlike IP protocols, security features like authentication and encryption were not built into the SS7 protocol. Rather, the focus has been placed on creating secure physical environments for the network equipment rather than secure protocols.
- STPs, the routers of the SS7 network, perform gateway screening to prohibit inbound and outbound messages from unauthorized nodes. The addresses of individual nodes within a network are isolated.
- Global title translation (GTT) enables a network to receive messages from other networks without disclosing the unique addresses, called point codes, of its own nodes.

SS7: the landscape changes

- The increasing number and complexity of **interfaces between SS7 and other networks** increases its vulnerability to attack.
- Every point of interconnection is a potential point of access. The developing **interdependence between SS7 and IP networks** is increasing that vulnerability.
- If there is an IP network anywhere in the chain of interconnection, all the **connected networks are vulnerable** to some extent.
- There is **no encryption or authentication in the signaling network** to ensure the validity of sending nodes outside the network boundary. A rogue server in the IP network sending damaging management messages could seriously impair the signaling network.
- Anyone capable of generating SS7 messages and introducing them to the network could **cripple the PSTN** service.
- Each element in the SS7 network is engineered to handle a certain amount of traffic. A node could be flooded and call processing in that section of the **network could come to a halt**.



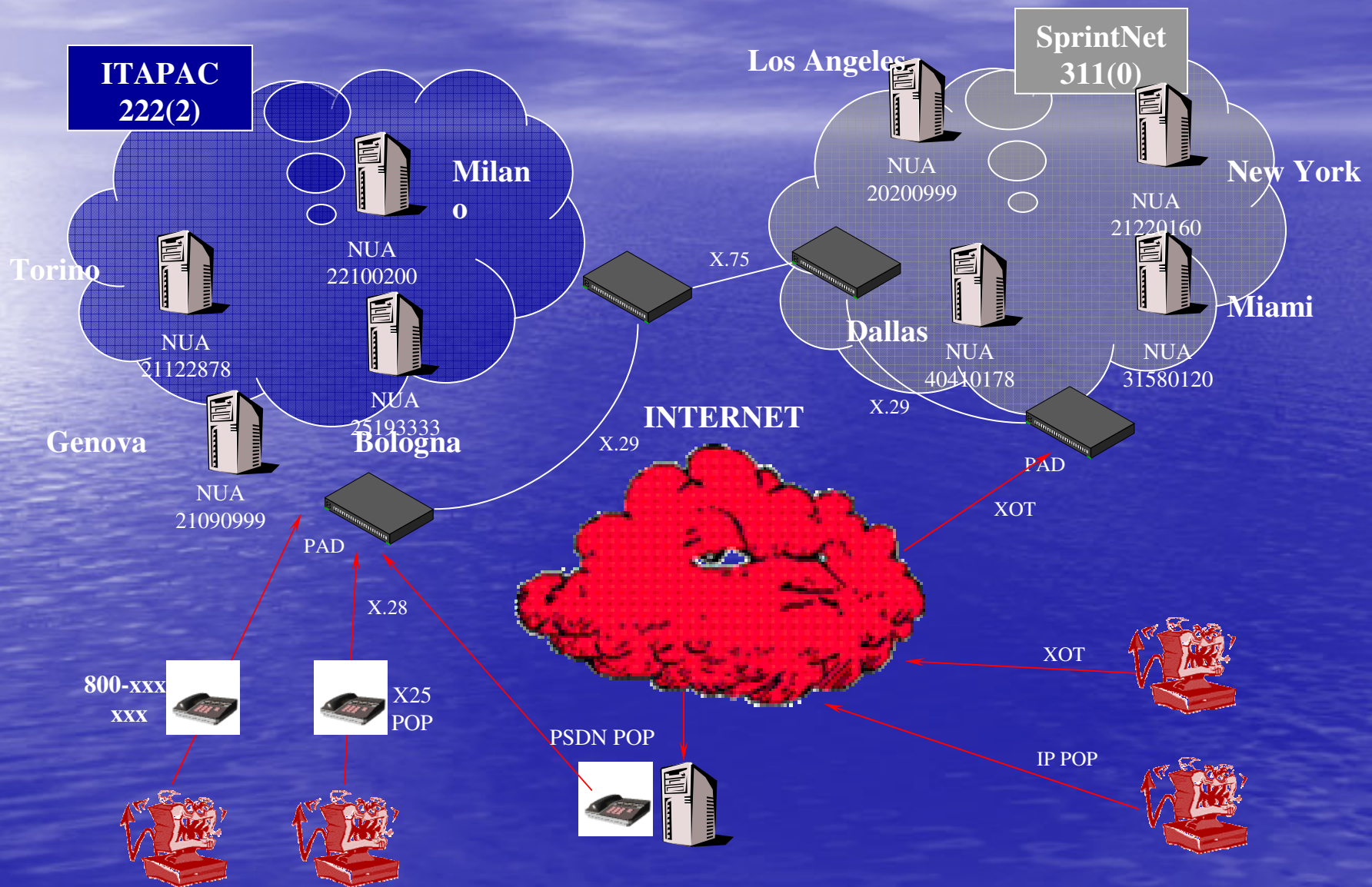
X.25 networks

The Forgotten Link

Origins of X.25

- First worldwide packet-switching technology
- Deployed before the Internet
- Used by banks, governments, telcos, private companies, universities
- Interconnected using X.75 protocol, also uses X.3, X.121, X.28 and X.29 protocols
- 64kbps links, virtual circuit technology
- Gateways from PSTN (PAD dialups) and Internet

X.25 "out of band" transport



X.25 wardialing

```
- 202 - ONTARIO - Up to 700
20200115      VAX/VMS
20200116      VAX/VMS
20200156      Diand Information System
20200214      $ UNIX    (gtagmhs2)
20200230      METS Dial-In Server  Enter your login:
2020024098    Control Port on Node Ottawa 6505 PAD
20200286      $ VAX/VMS
2020032099    MPX.25102: PASSWORD
20200321      SunOS    Rel 4.1.3 (X25)
20200322      SunOS    ""
20200330      INETCO    Magicbank
20200342      ::
20200497      VAX/VMS
202005421     $ VAX/VMS
20200548      SunOS    Rel 4.1.3 (TMS470)
20200582      $ VAX/VMS  Production System
```

Connected to 0420160014025

INMARSAT-C Land Earth Station at INMARSAT C LES JEDDAH KSA

WELCOME TO INMARSAT C LES JEDDAH KINGDOM OF SAUDI ARABIA

Enter ?<CR> to get help information,

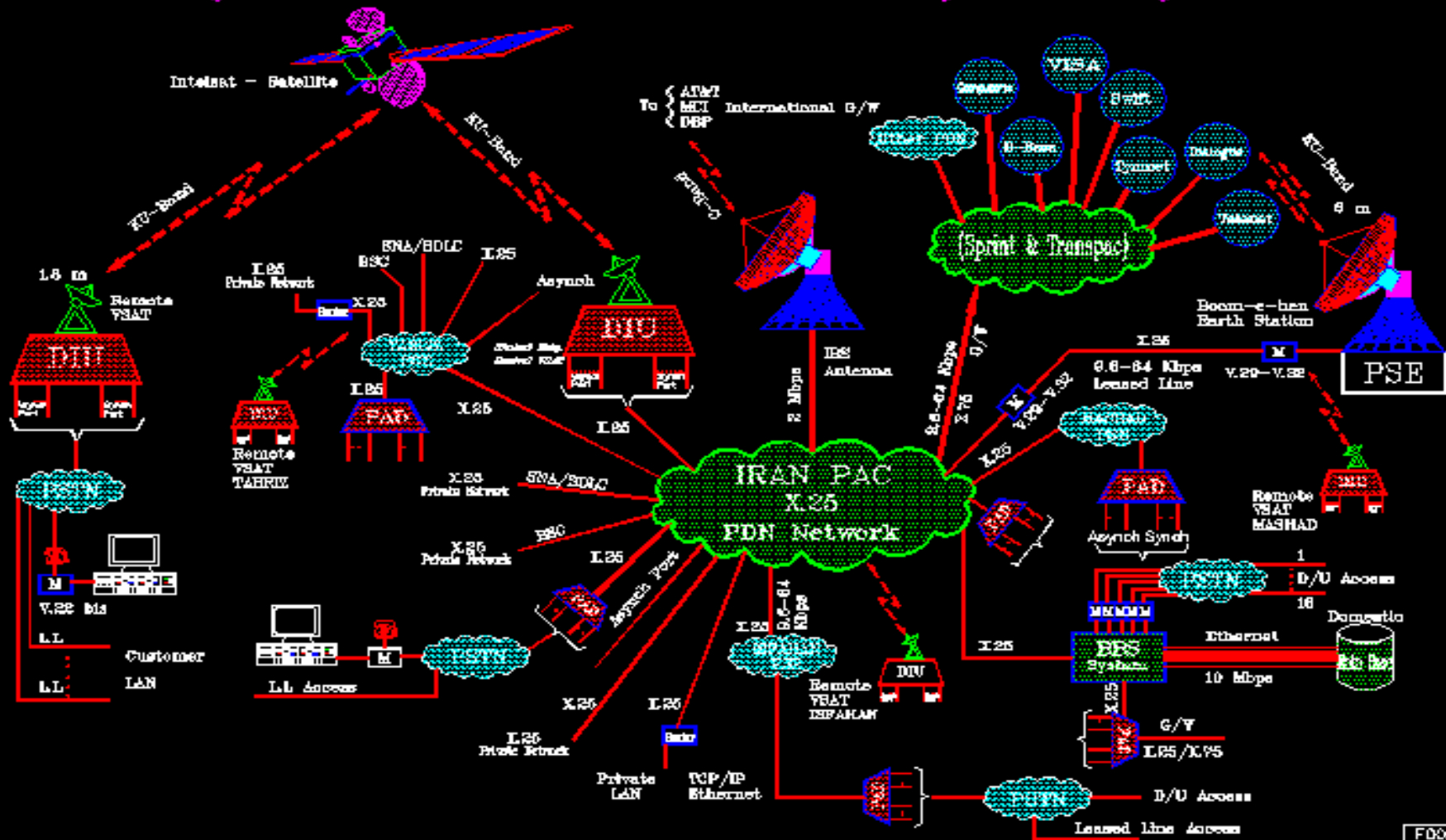
C<CR> to cancel input.

X.25 landscape

- Lots of hosts found by scanning
- PR1MOS, VM/CMS, VAX/VMS, UNIX, terminal servers, routers, XENIX
- Usually not firewalled
- Some hosts accept “reverse charging”
- X.25 calls usually connect to login service
- No “port scanning” like on Internet

X.25 reaches everywhere!

Iran Packet Switched Public Data Network (Iranpac) *Integrated PDN & VSAT Network & Global Information System*



X.25 – the forgotten frontier?

- Quote from Raoul Chiesa, one of Europe's leading X.25 security experts, after 15 years of exploration:

1% of the Top 1.000 companies and nation's critical infrastructures with X.25 links worldwide are somehow "not penetrable"

Conclusions

- The systems, protocols and networks found in mobile telephony could become an **exciting playground** for sophisticated hackers
- Increasing complexity with GPRS, 3G and VAS applications leads to many **further opportunities for attackers**
- The threat of **hostile user agents** hasn't really started yet, but it is looming
- Telcos are traditionally "closed environment" and rely upon this **obscurity to ensure their security**



THANK YOU

Emmanuel Gadaix

eg@tstf.net