NGN Security

Next Generation Nightmare?

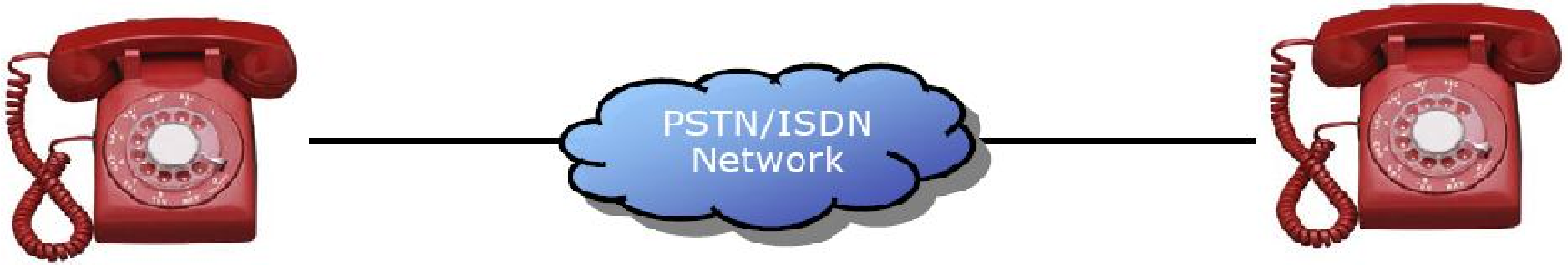
Emmanuel Gadaix
Telecom Security Task Force

Dubai, HITB 2007

Agenda

- Evolution of mobile security issues
- NGN, 3G, IMS, 4G: what is what?
- The NGN architecture
- NGN threats and security controls
- VoIP issues in the IMS model
- Decentralisation of telcos
- Conclusions

The Early Days

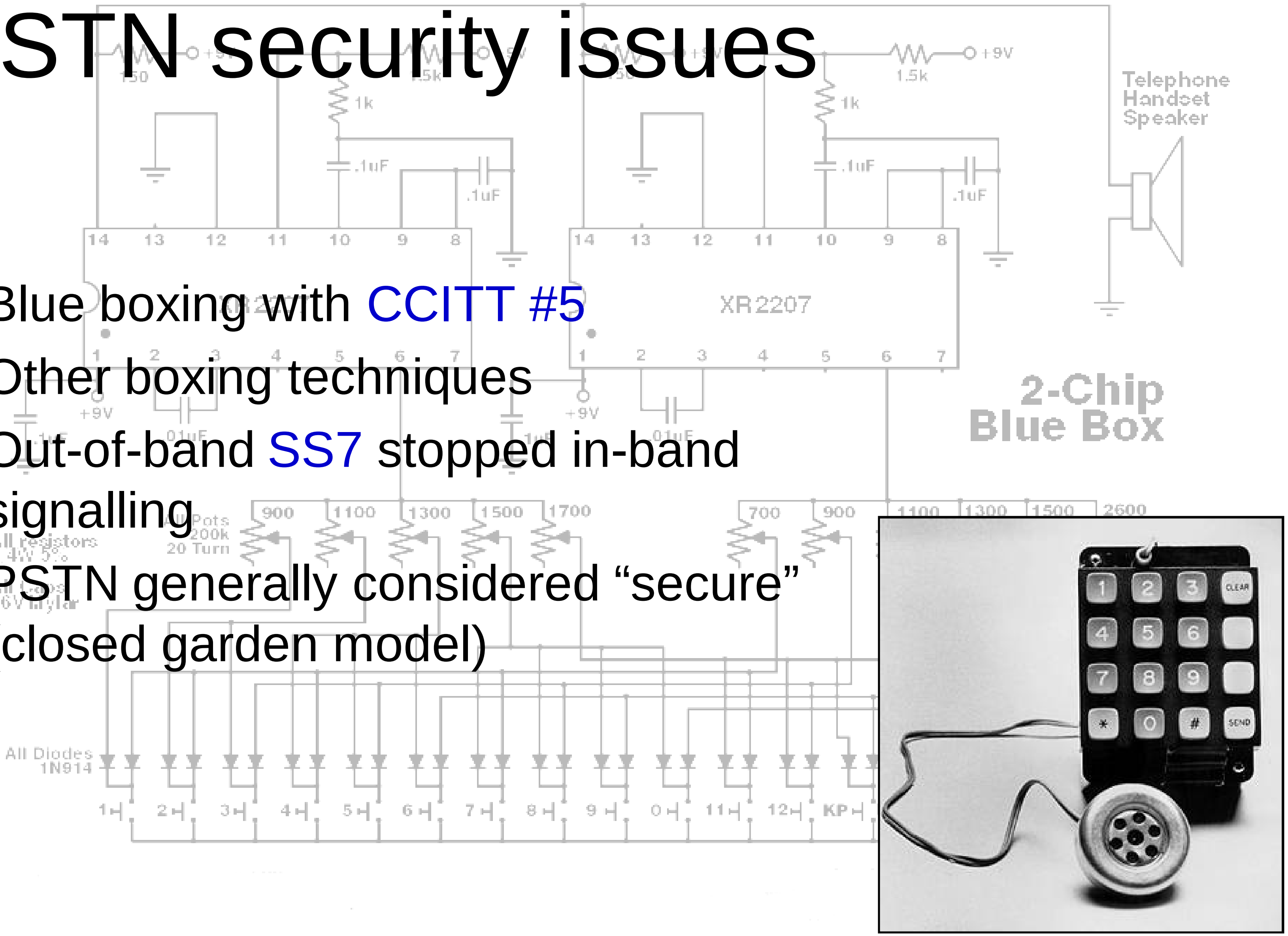


History of mobile networks

- Pre-mobile: the PSTN
- 1G: NMT, AMPS, RC2000
- 2G: GSM, CSD
- 2.5G: GPRS, EDGE
- 3G: UMTS, CDMA1x, CDMA-2000, WCDMA
- 4G: IMS, NGN
- 5G: no operator required?

PSTN security issues

- Blue boxing with CCITT #5
- Other boxing techniques
- Out-of-band SS7 stopped in-band signalling
- PSTN generally considered “secure” (closed garden model)



Early mobile systems

Copyright © 2000 Lucent Technologies.
http://www.bell-labs.com/history/75/gallery.html

First car mounted radio telephone (1921)

First cellular network

In 1978 Bahrain was the first country to operate a commercial cellular system…

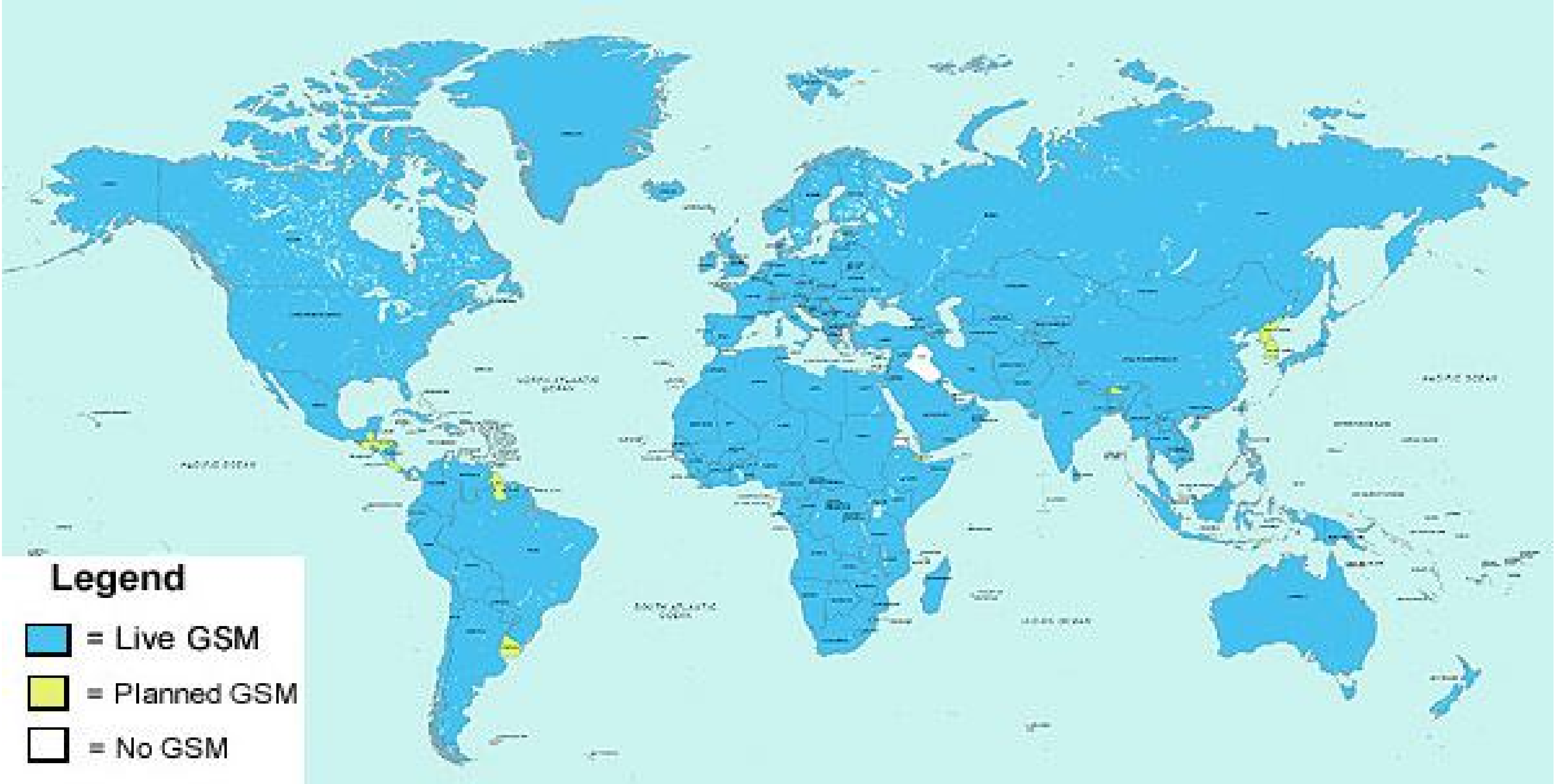
Security issues in 1G systems

- Eavesdropping (no over the air encryption, easy to listen in to frequencies with a simple radio scanner)
- Cloning of phones by intercepting the serial number (ESN)

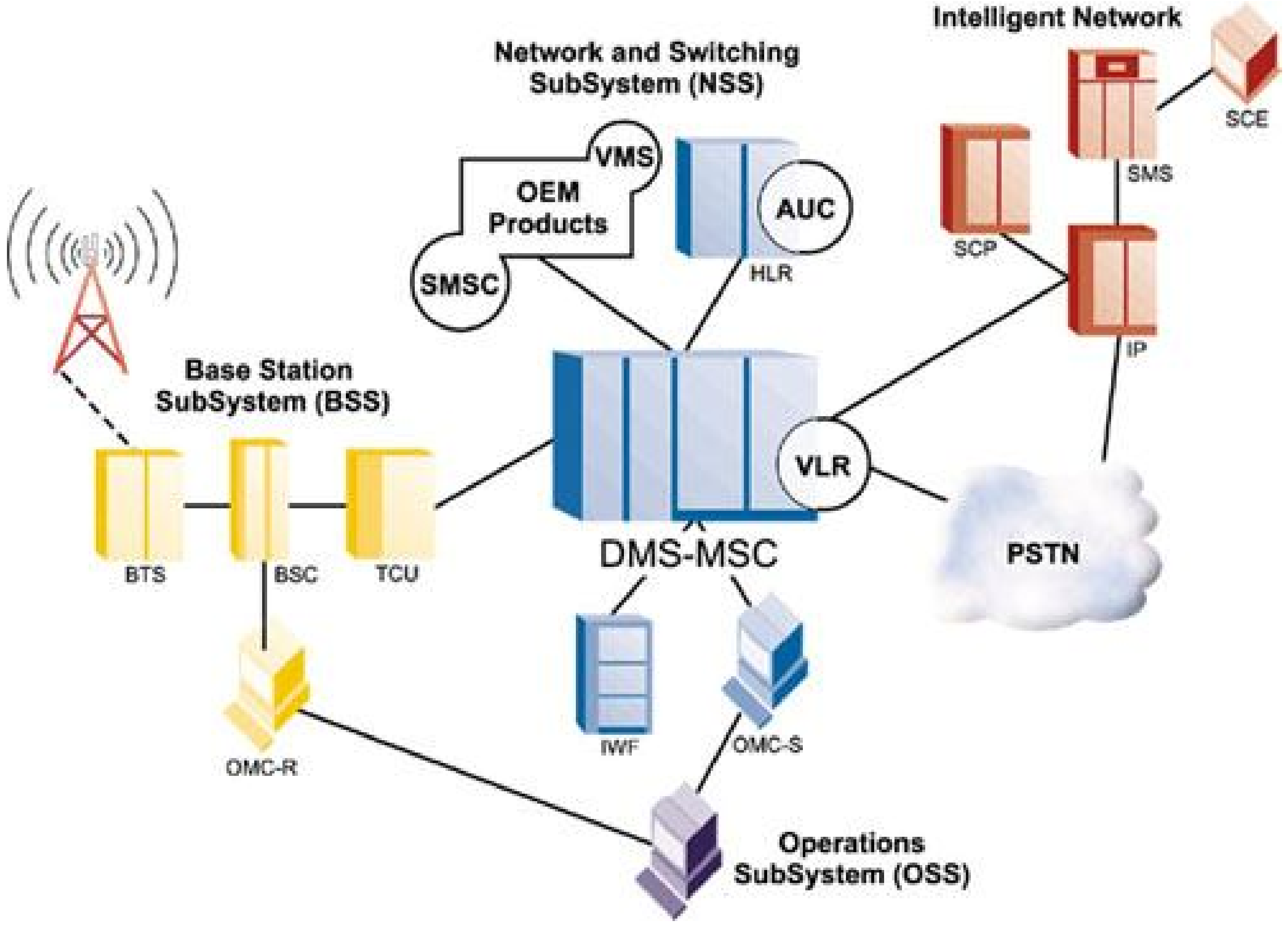
Lessons from 1G systems

- Designers of early telephony systems had no considerations for security – just for functionality.
- Phreakers were quick to learn how to abuse the system
- Countermeasures to limit the increasingly large fraud were only “band aid” that never really eradicated the problem

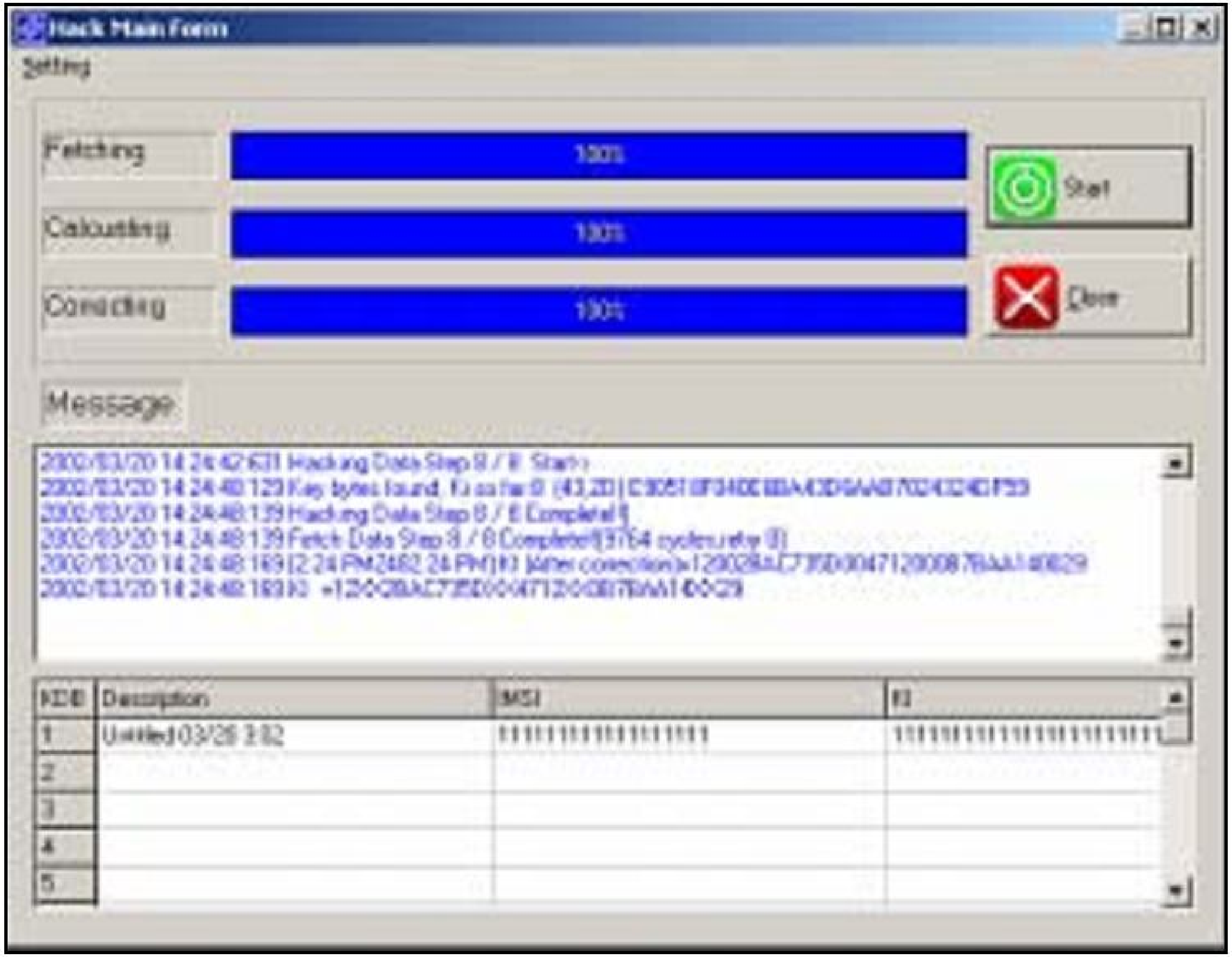
2G… the GSM world



2G: GSM “closed” garden


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

SIM Hacking tools



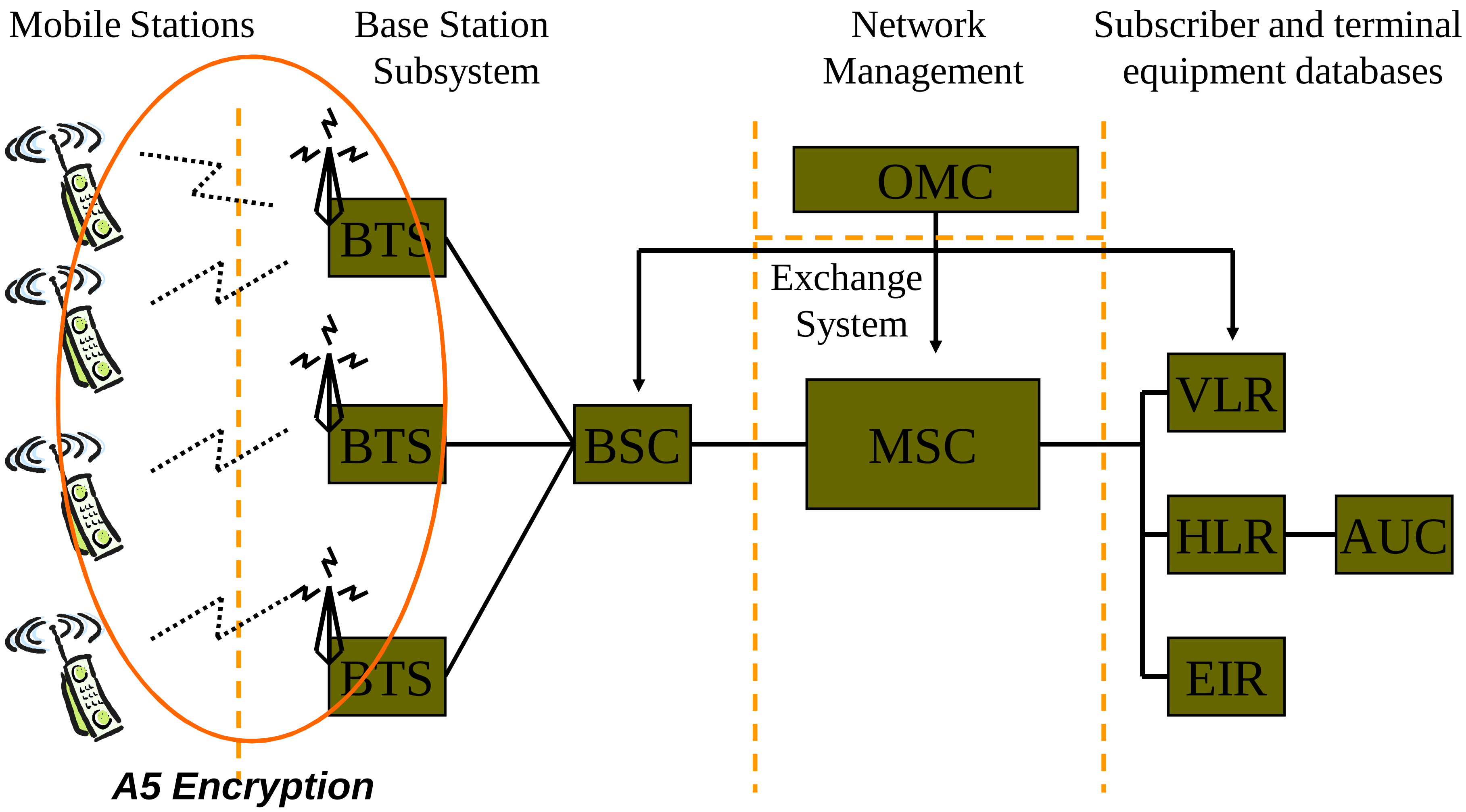
```
2002/03/20 14:24:42:631 Hacking Data Step 8 / 8 Start>
2002/03/20 14:24:48:129 Key bytes found. Ki so far 8 (43,20) [illegible]
2002/03/20 14:24:48:139 Hacking Data Step 8 / 8 Completed!
2002/03/20 14:24:48:139 Fetch Data Step 8 / 8 Completed!(3764 cycles,retry 0)
2002/03/20 14:24:48:169 [2:24 PM/2:48 2:24 PM] Ki (after correction)=129028AC73[illegible]
2002/03/20 14:24:48:169 Ki =1290[illegible]
```

KDB	Description	IMSI	Ki
1	Untitled 03/26 3:02	111111111111111111	1111111111111111111111
2			
3			
4			
5			

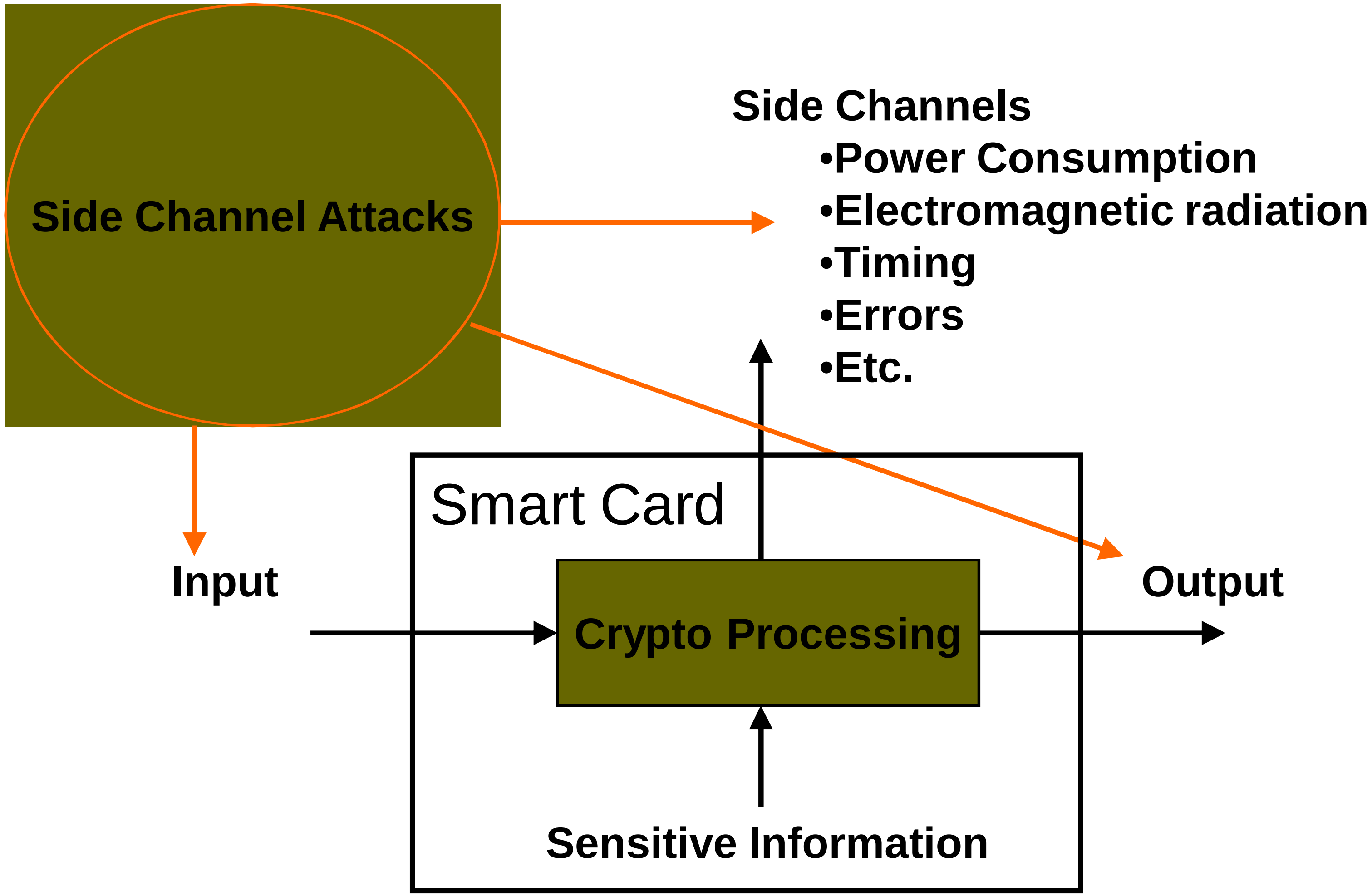
Bluetooth Security

- Bluejacking allows phone users to send business cards anonymously using Bluetooth.
- Bluesnarfing allows hackers to gain access to data stored on a Bluetooth enabled phone without alerting the phone's user of the connection made to the device: phonebook and associated images, calendar, and IMEI.
- Bluebugging allows access the mobile phone commands using Bluetooth without notifying or alerting the phone's user. This vulnerability allows the hacker to initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet.

Encryption in 2G



Mixed attacks on SIM crypto



Side Channel Attacks

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

Smart Card

Input

Crypto Processing

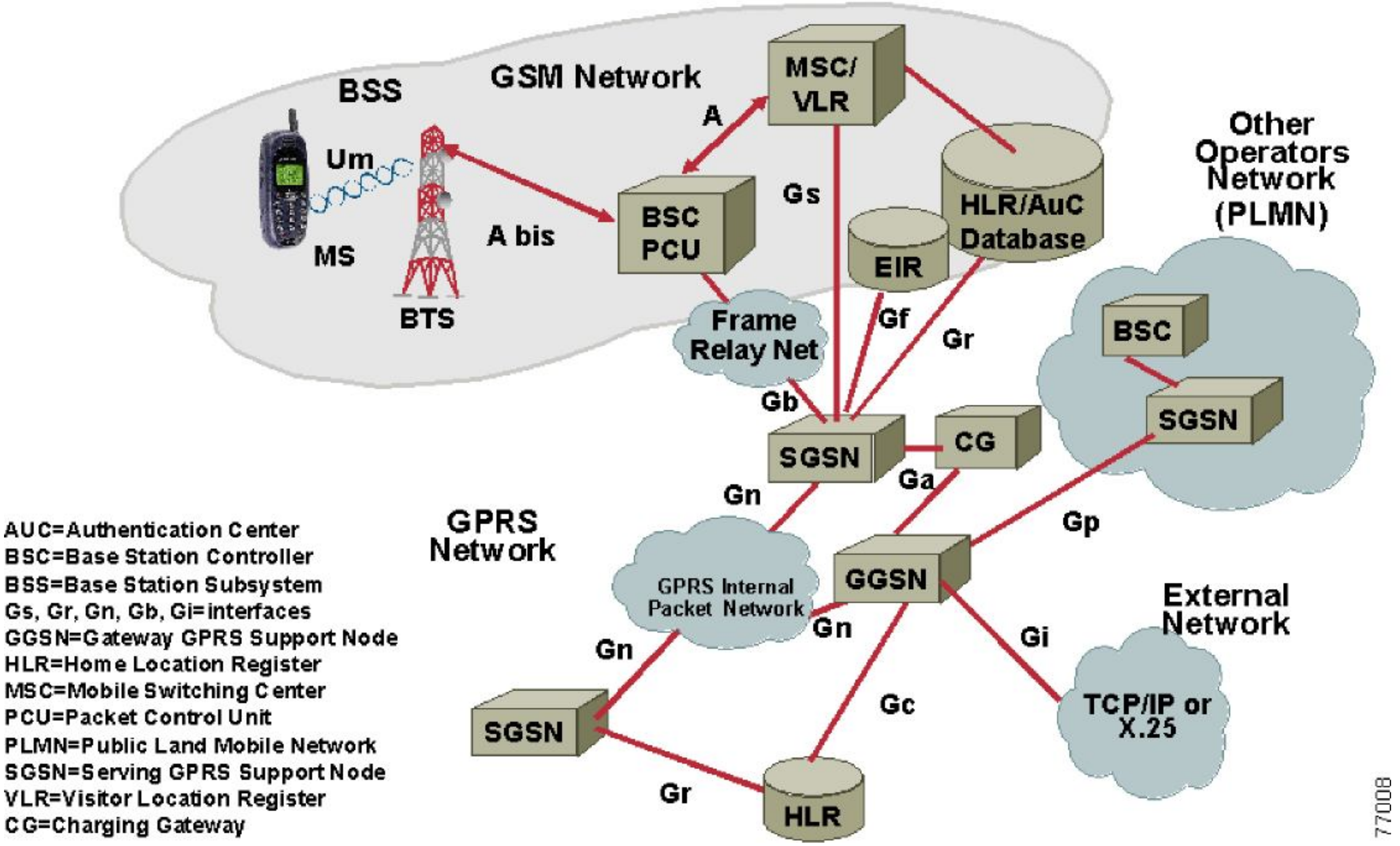
Output

Sensitive Information

Security issues in 2G

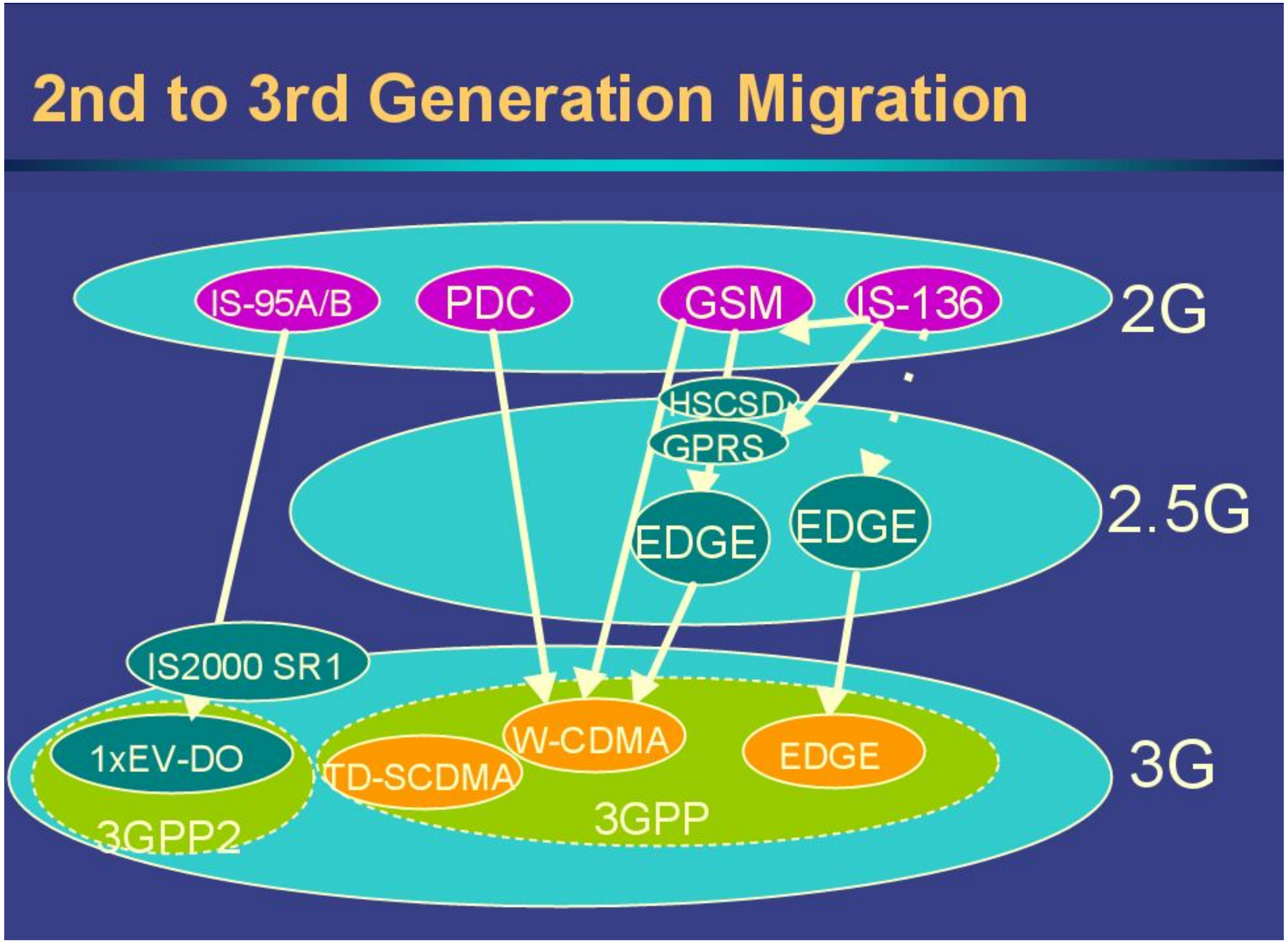
- Eavesdropping and cloning foiled by use of encryption (no more scanners) and authentication (no more cloning).
- SIM cloning demonstrated due to weaknesses in crypto algorithms. Attacks on COMP128, A5/1 A5/2, A5/3.
- Attackers can tap conversations and decrypt them either in real-time, or at any later time.
- Active attacks such as call hijacking, altering of data messages and call theft.
- Non-technical subscription fraud still a major issue, mitigated by the growth of Prepaid services and Fraud Management Systems.

2.5G

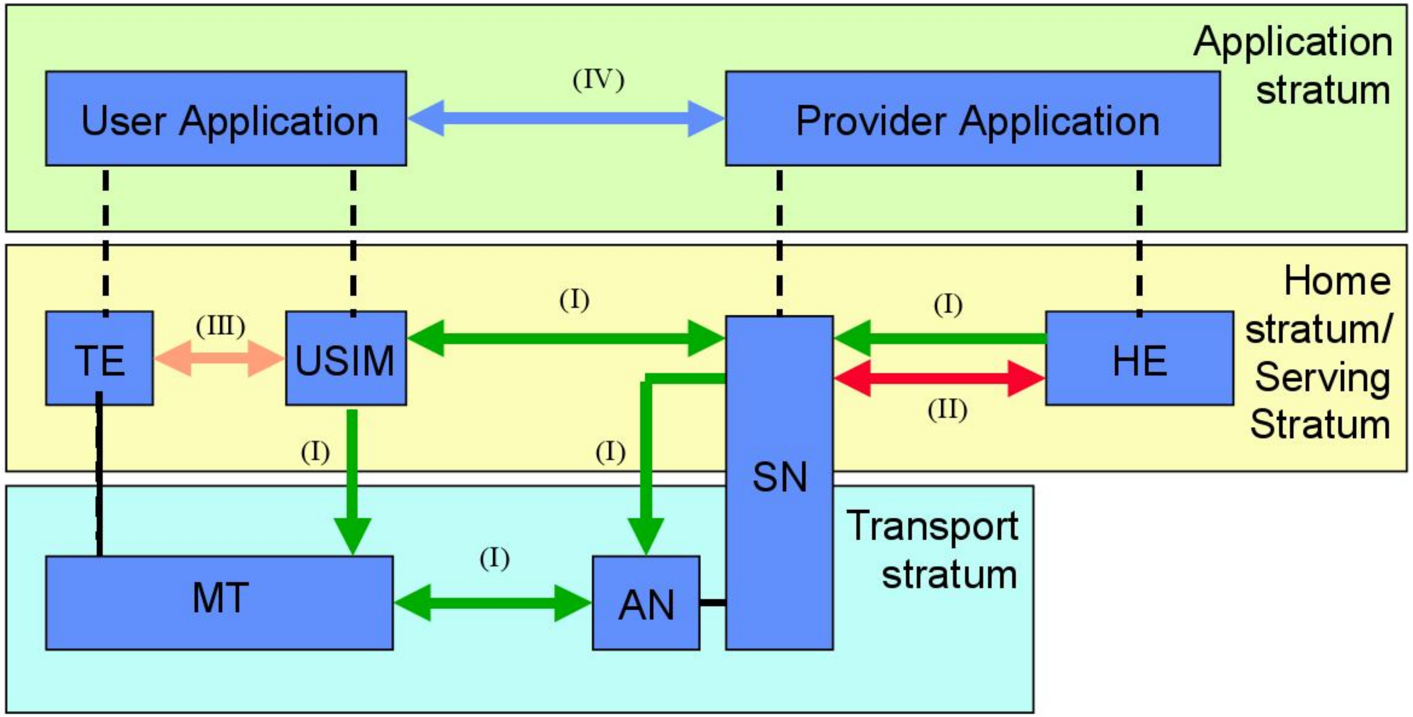


AUC=Authentication Center
BSC=Base Station Controller
BSS=Base Station Subsystem
Gs, Gr, Gn, Gb, Gi=interfaces
GGSN=Gateway GPRS Support Node
HLR=Home Location Register
MSC=Mobile Switching Center
PCU=Packet Control Unit
PLMN=Public Land Mobile Network
SGSN=Serving GPRS Support Node
VLR=Visitor Location Register
CG=Charging Gateway

The Evolution Continues



3G Security



Network access security (I)

Network domain security (II)

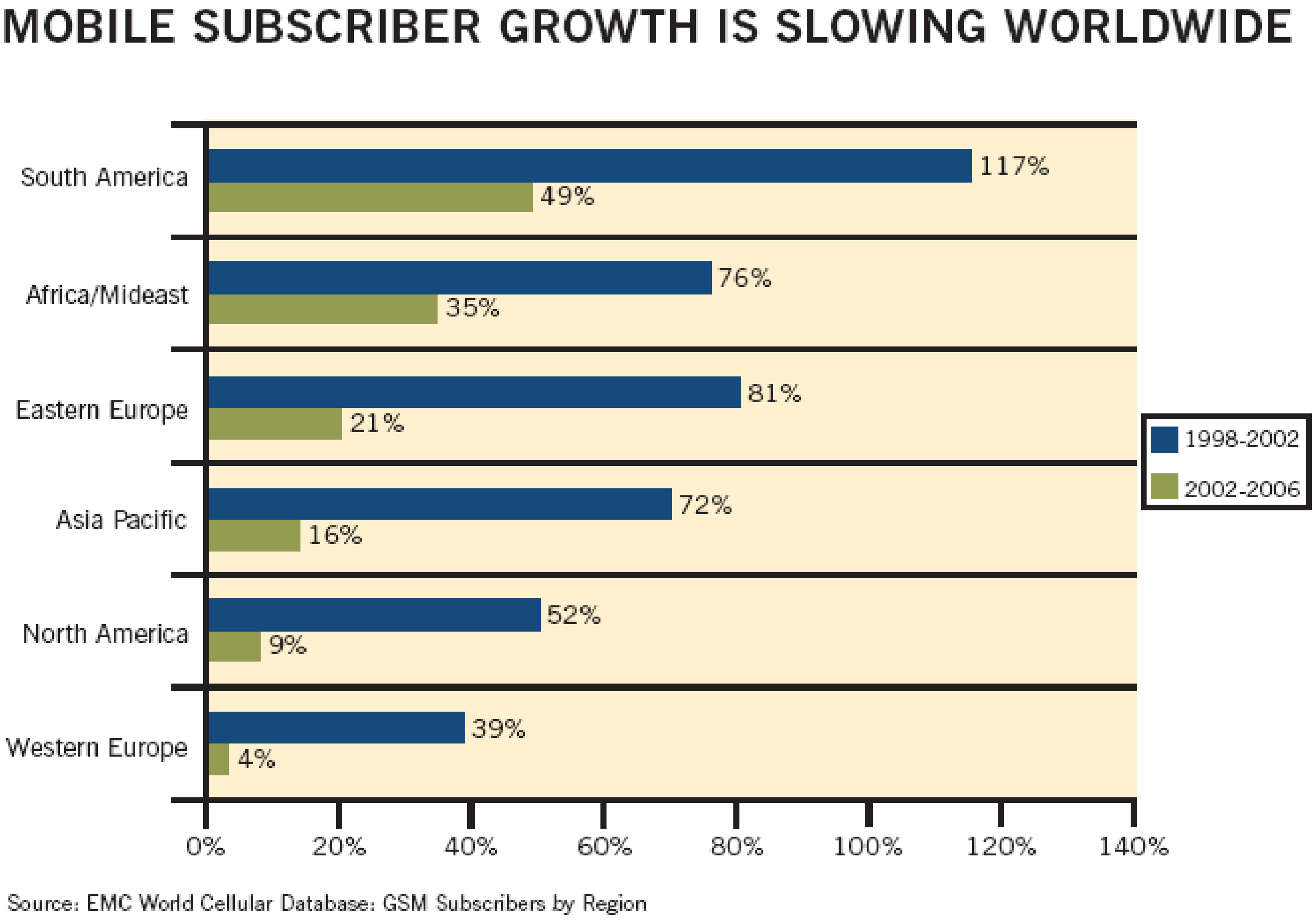
User domain security (III)

Application domain security (IV)

Visibility and configurability of security (V)

SIP / IMS Evolution

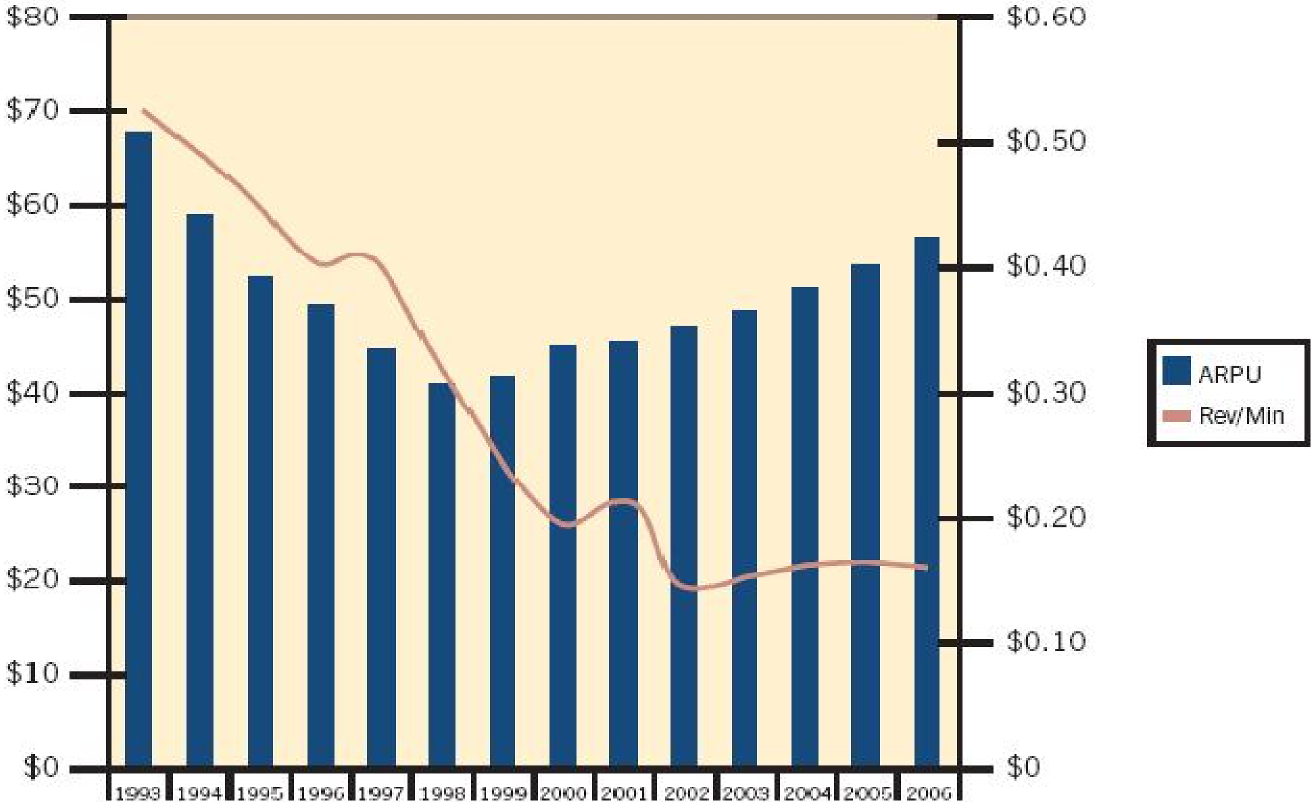
Still growing



Source: EMC World Cellular Database: GSM Subscribers by Region

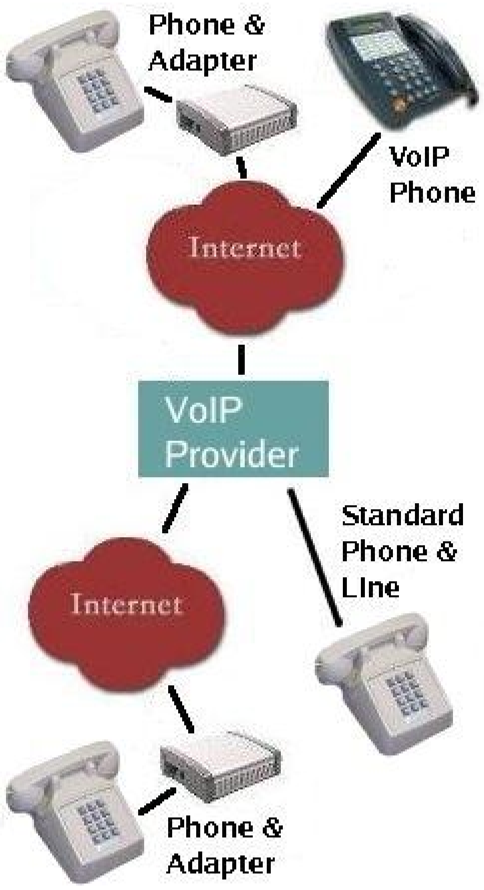
Price war

PRICE COMPETITION IS DRIVING DOWN REVENUE PER MINUTE



Source: CTIA, Merrill Lynch, TIA, Wilkovsky Gruen Assoc.

The VoIP Threat



Anyone can become a VoIP provider

Thousands of VoIP companies

Low investment

Flexible

Fast Time-to-Market

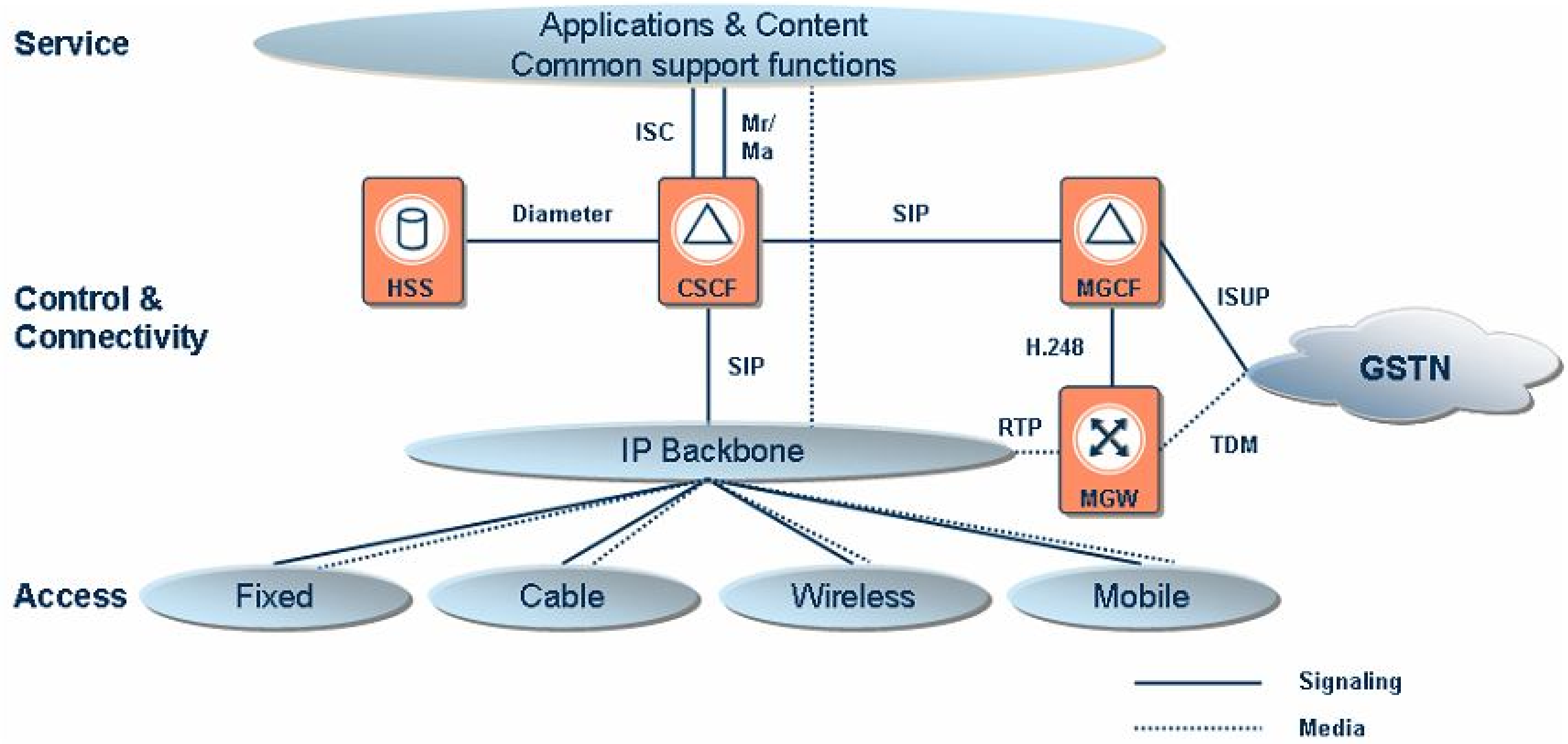
Easy to introduce new services

Low cost international calls

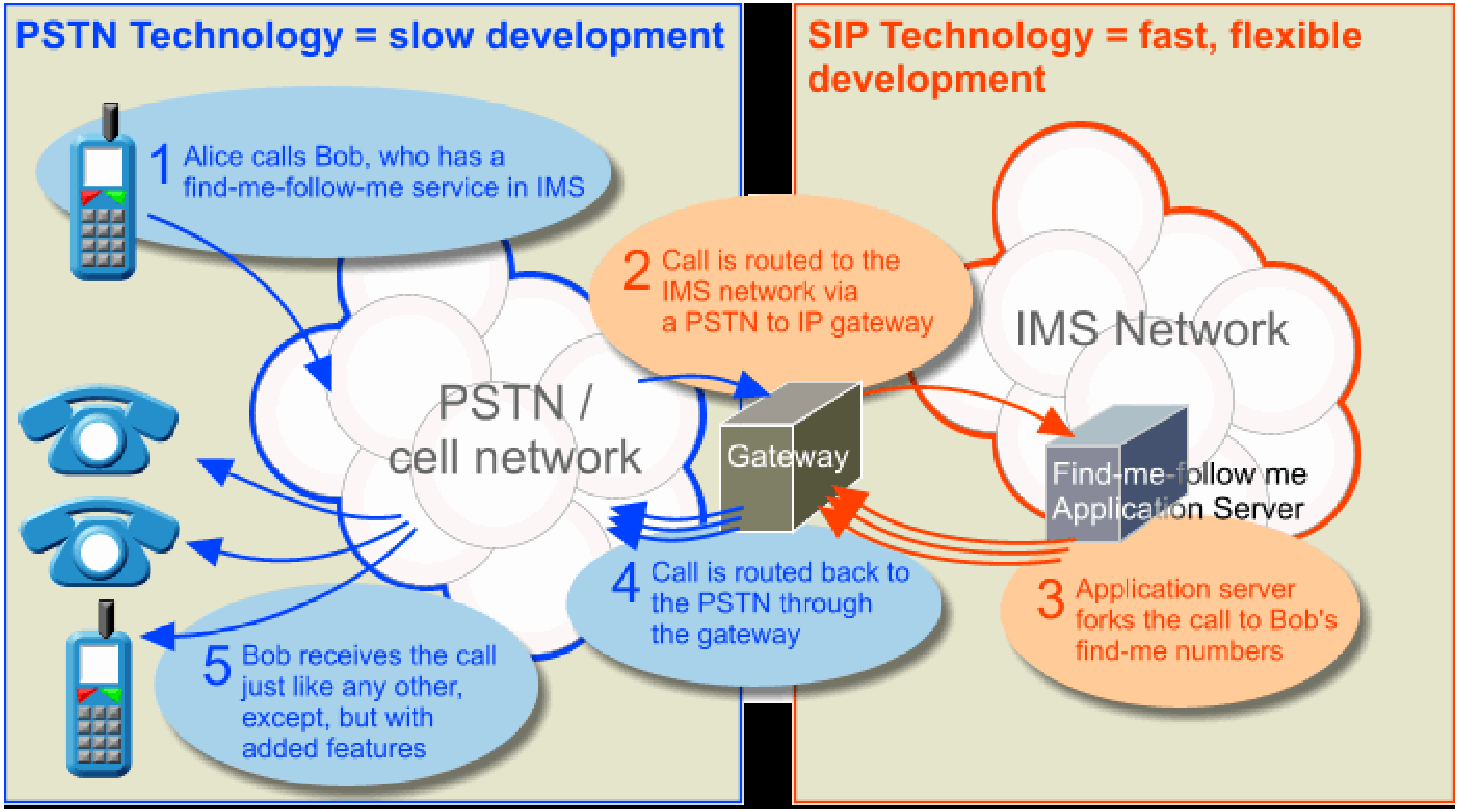
Flat rate plans

VoIP business growing very fast

IMS overview

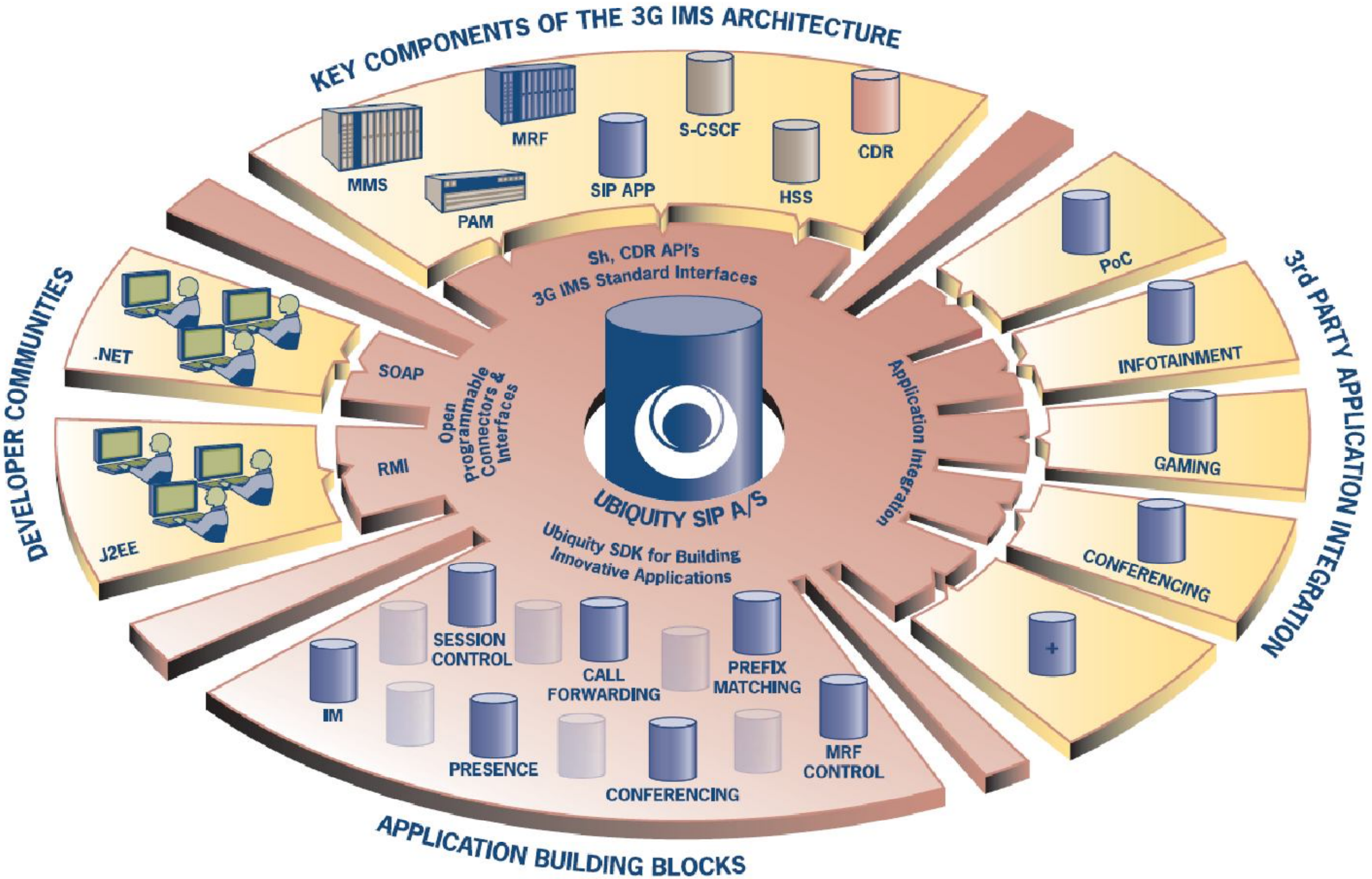


IMS Model



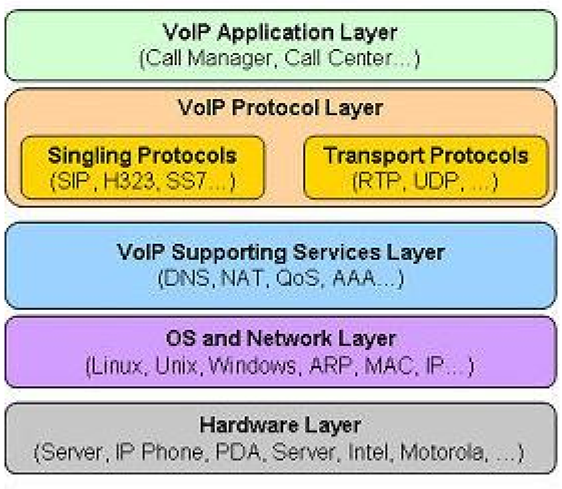
PSTN Technology = slow development
SIP Technology = fast, flexible development
1 Alice calls Bob, who has a find-me-follow-me service in IMS
2 Call is routed to the IMS network via a PSTN to IP gateway
IMS Network
PSTN / cell network
Gateway
Find-me-follow me Application Server
3 Application server forks the call to Bob's find-me numbers
4 Call is routed back to the PSTN through the gateway
5 Bob receives the call just like any other, except, but with added features

IMS: “Open Garden”



Security in IMS networks

IMS: Inherit VoIP problems



VoIP Application Layer
(Call Manager, Call Center…)

VoIP Protocol Layer

Singling Protocols
(SIP, H323, SS7…)

Transport Protocols
(RTP, UDP, …)

VoIP Supporting Services Layer
(DNS, NAT, QoS, AAA…)

OS and Network Layer
(Linux, Unix, Windows, ARP, MAC, IP…)

Hardware Layer
(Server, IP Phone, PDA, Server, Intel, Motorola, …)

Security assessment concerns several layers, from the terminal (mobile phones) to the SIP application servers

Protocol Attacks

- SIP attacks: interception, impersonation, denial or degradation of service, toll bypass, voice phishing
- Access Network: localized denial of service, interception
- SS7 Network: SIGTRAN-based attacks could compromise the signaling infrastructure
- IP Backbone: routing protocols could compromise operator’s network integrity, cause overload
- Perimeter: morphing DMZ with numerous vendors, service providers, content providers, API

IMS-related Attack Tools

Scanning

SCTPscan
SIPping
fping
Nessus
nmap
snmpwalk
SNSscan
VLANping
SuperScan

Enumeration

netcat
SiVuS
sipsak
SIPSCAN
smap
TFTP BruteForcer
SS7auditor

Denial of Service

DNS Auditing tool
Internetwork Routing Protocol Attack Suite
UDP Flooder
Wireshark
TCAPflood
MTPsequencer
INVITE Flooder
RTP Flooder

Eavesdropping

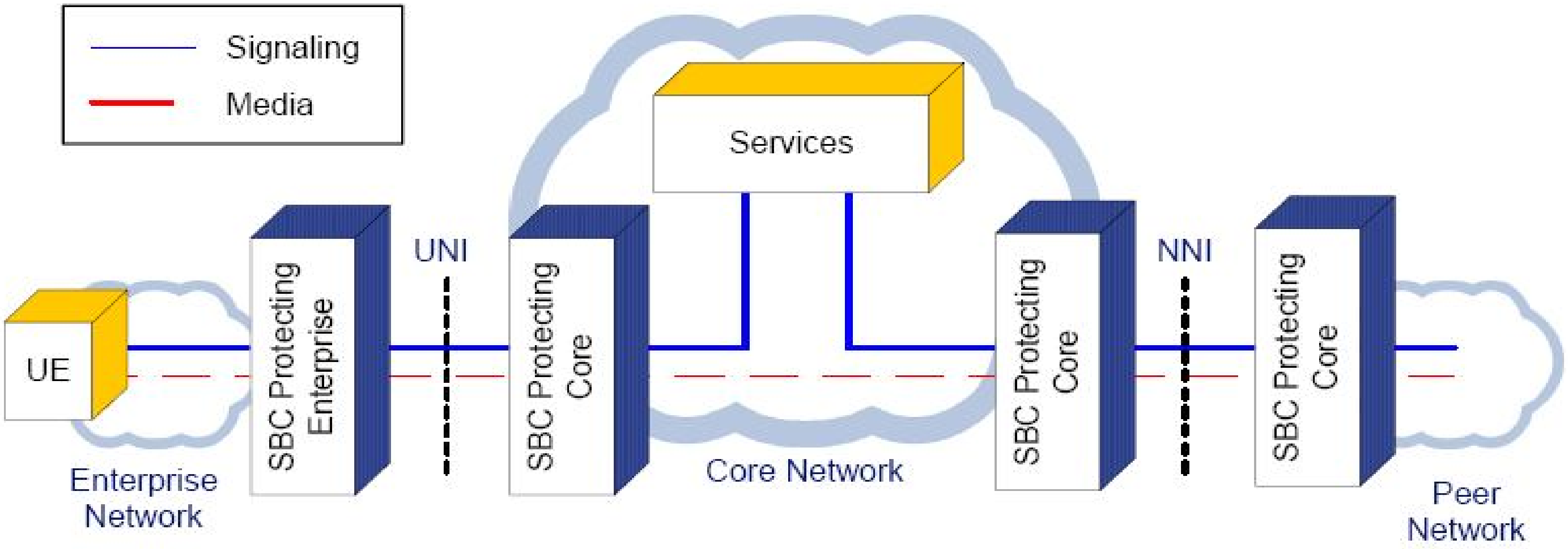
Angst
Cain and Abel
DTMF Decoder
dsniff
NetStumbler
Oreka
VoIPong
vomit

Others

RedirectPoison
Sipproxy
MTPflood
Registration Hijacker
siprogue
Ravage
ohrwurm RTP fuzzer

Session Border Controller

The “SIP Firewall” concept



Insider Attacks

- NMS: Controls the whole network and every single Network Element
- OSS: Customer data, billing records
- IN: Prepaid database, Vouchers, CDR
- Core: IB backbone, SS7 network
- VAS: Services data, billing data

SS7

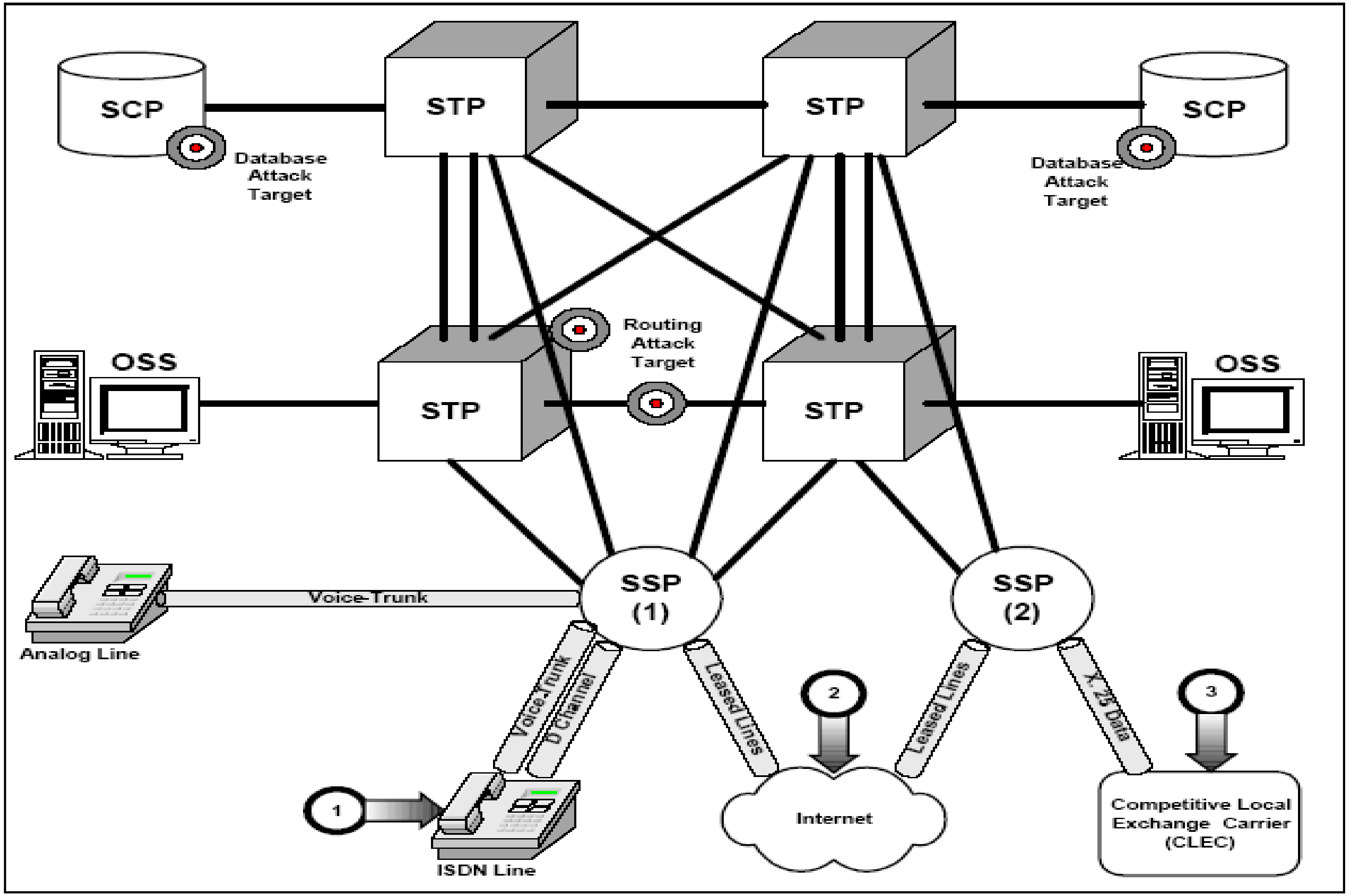
- Mobile networks use Signalling System no. 7 (SS7) for communication between networks for such activities as authentication, location update, and supplementary services and call control.

- The messages unique to mobile communications are MAP messages. Other protocols inclue MTP, ISUP, SCCP, TCAP, INAP, CAP.

- The security of the global SS7 network is based on trust relationships between operators and is assuming a closed network architecture.

- One of 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 attacks

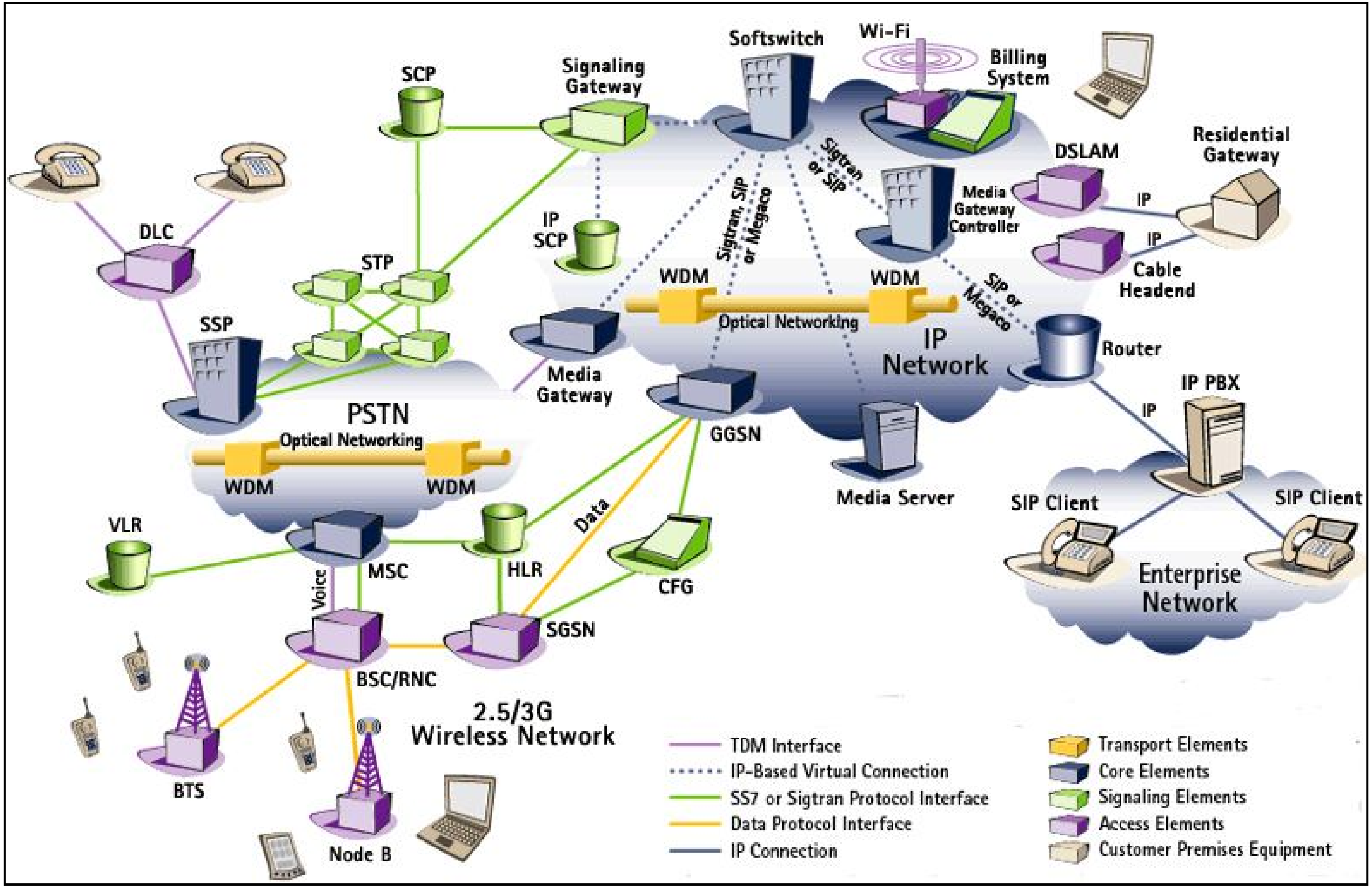

SCP
STP
STP
SCP
Database Attack Target
Database Attack Target
Routing Attack Target
OSS
STP
STP
OSS
Voice-Trunk
SSP (1)
SSP (2)
Analog Line
Voice-Trunk
D Channel
Leased Lines
Leased Lines
X.25 Data
1
2
3
ISDN Line
Internet
Competitive Local Exchange Carrier (CLEC)

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

NGN Security

NGN: Not a garden any more…



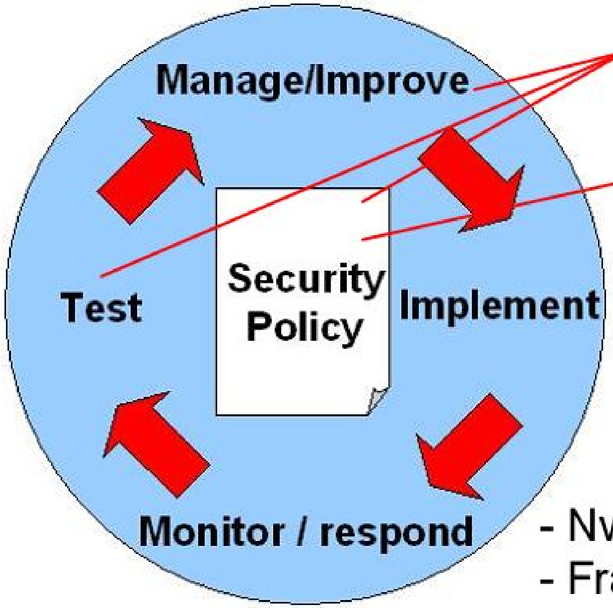
Managing Security

- To be able to make sound security judgments, both the particular business context and the networking environment must be fully understood.
- To support the whole telecom system life cycle, from end-to-end, the following operations have to be undertaken:
  - Business Continuity Management
  - Network Security Design
  - Network Configuration / Integration
  - Network Security Audits
  - Network Security Implementation
  - Fraud Management

Security Operations

- Risk Management: all network operation implies a certain risk that must be accepted, avoided, reduced or transferred.
- Business Continuity: the operator’s critical processes and information should be protected from disclosure and/or disruption.
- Lowering operator costs: well thought-out security solutions provide a payback in terms of
  - Reduced operating costs
  - Reduced risk of fraud
  - Reduced risk of critical security-related network outages and potentially less churn

Security Wheel



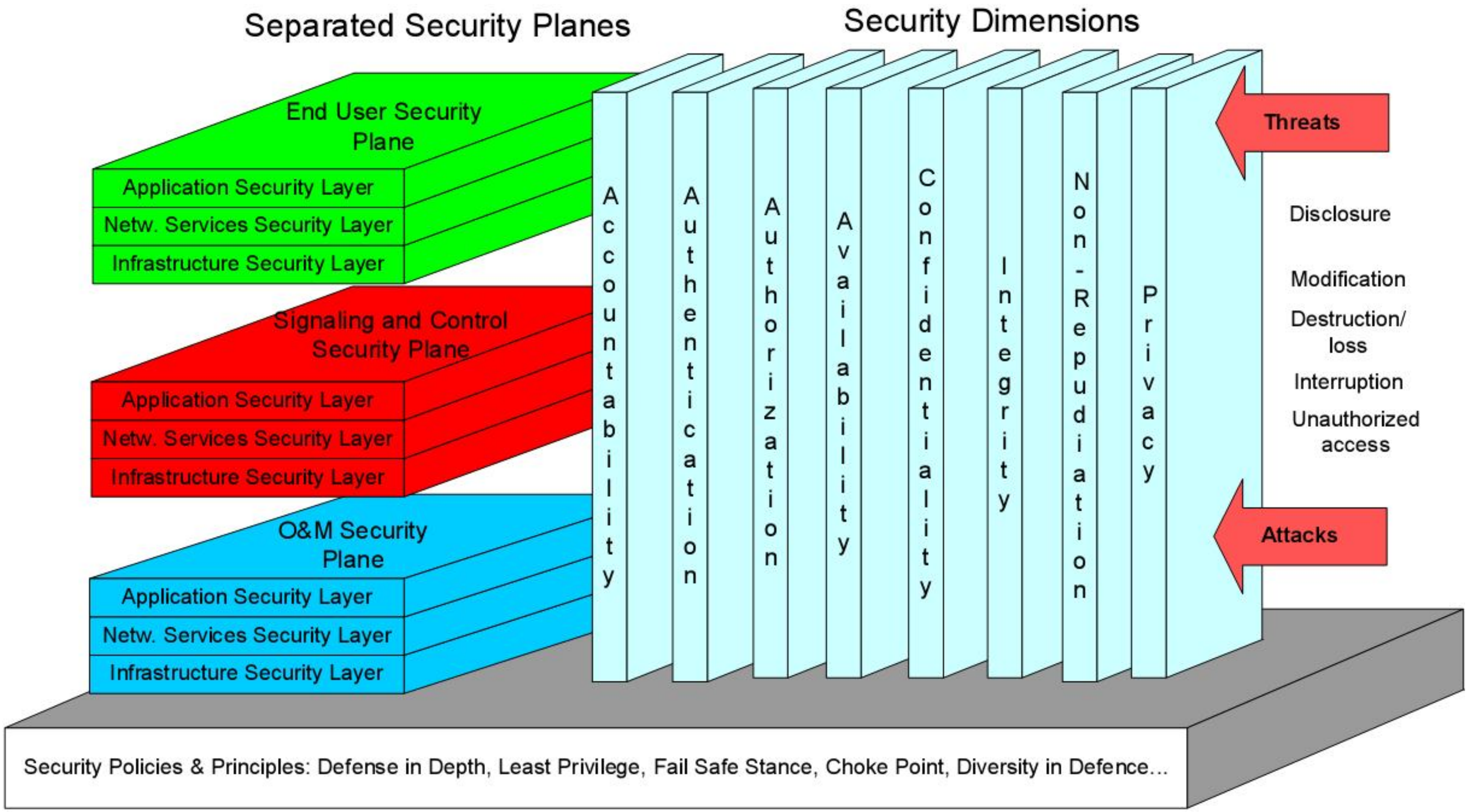
- Business Continuity Management
- Nw Security Assessment

- Nw Security Analysis (incl. penetration tests)

- Nw Security Design
- Nw Configuration/Integration

- Nw Management
- Fraud Management
- Nw Security Assessment/Analysis

Security Architecture Model


Separated Security Planes
Security Dimensions
End User Security Plane
Application Security Layer
Netw. Services Security Layer
Infrastructure Security Layer
Signaling and Control Security Plane
Application Security Layer
Netw. Services Security Layer
Infrastructure Security Layer
O&M Security Plane
Application Security Layer
Netw. Services Security Layer
Infrastructure Security Layer
Accountability
Authentication
Authorization
Availability
Confidentiality
Integrity
Non-Repudiation
Privacy
Threats
Disclosure
Modification
Destruction/ loss
Interruption
Unauthorized access
Attacks
Security Policies & Principles: Defense in Depth, Least Privilege, Fail Safe Stance, Choke Point, Diversity in Defence…

ITU-T X.800 Threat Model

1 - Destruction (an attack on availability):

- Destruction of information and/or network resources

2 - Corruption (an attack on integrity):

- Unauthorized tampering with an asset

3 - Removal (an attack on availability):

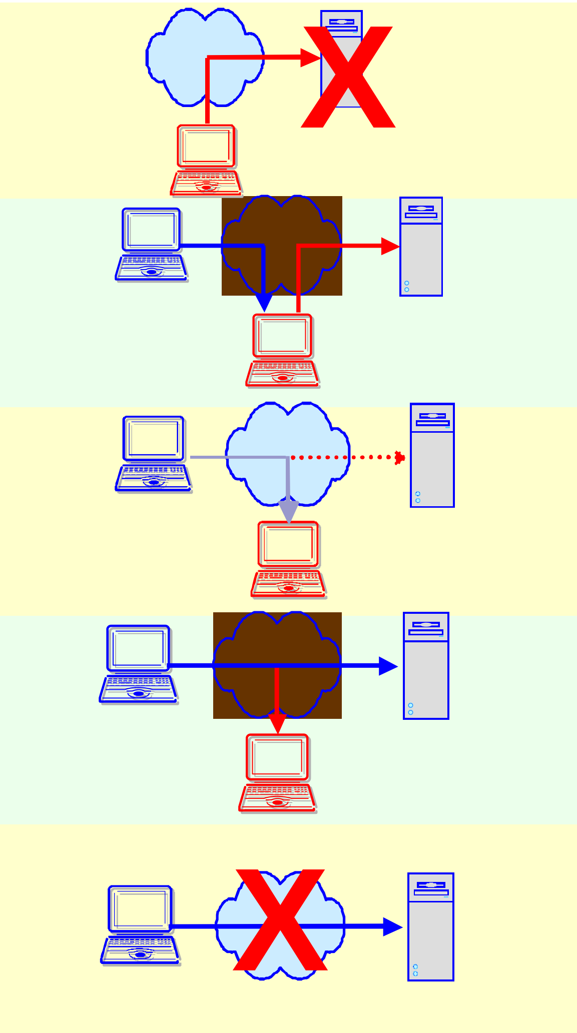
- Theft, removal or loss of information and/or other resources

4 - Disclosure (an attack on confidentiality):

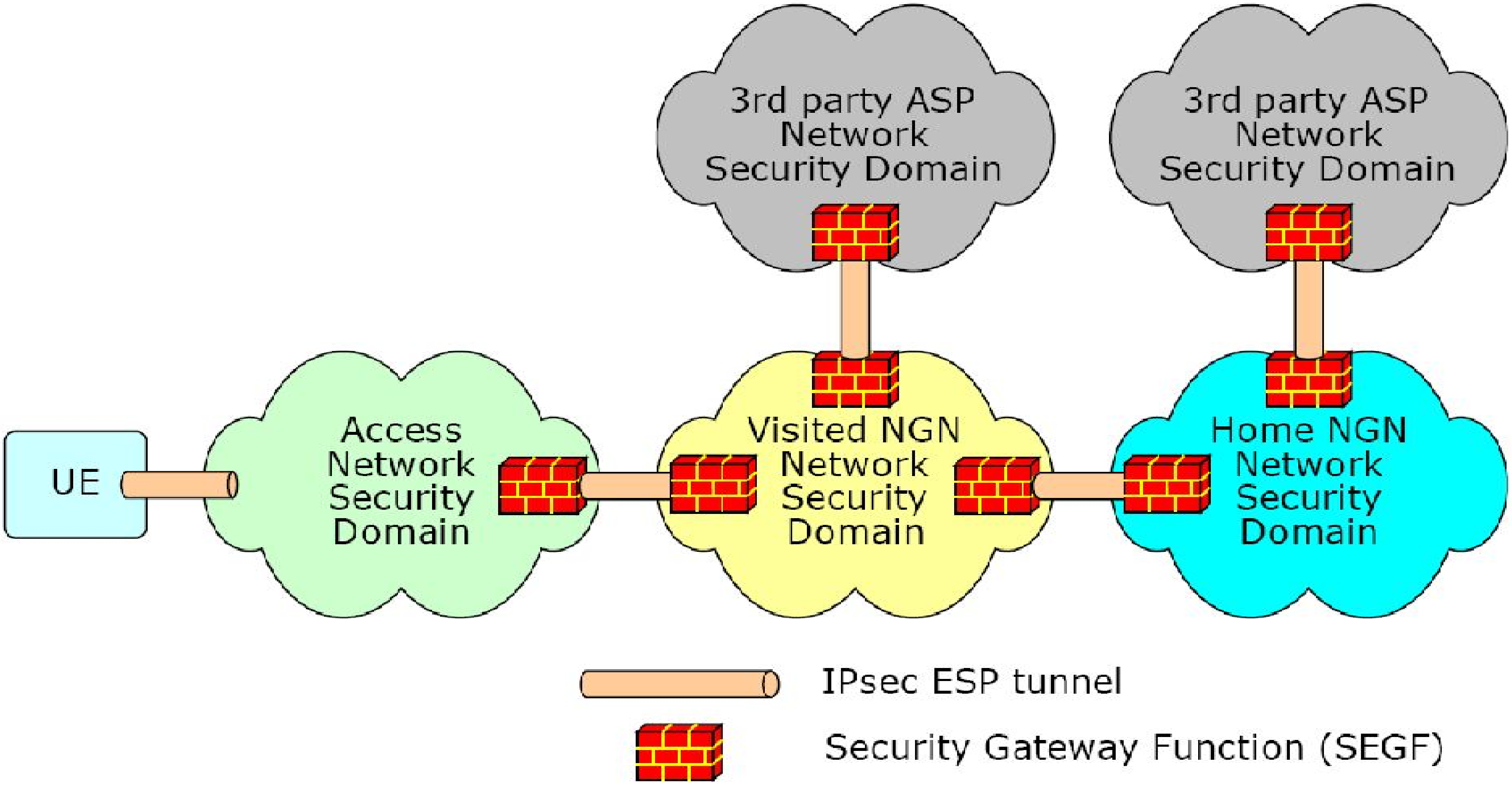
- Unauthorized access to an asset

5 - Interruption (an attack on availability):

- Interruption of services. Network becomes unavailable or unusable

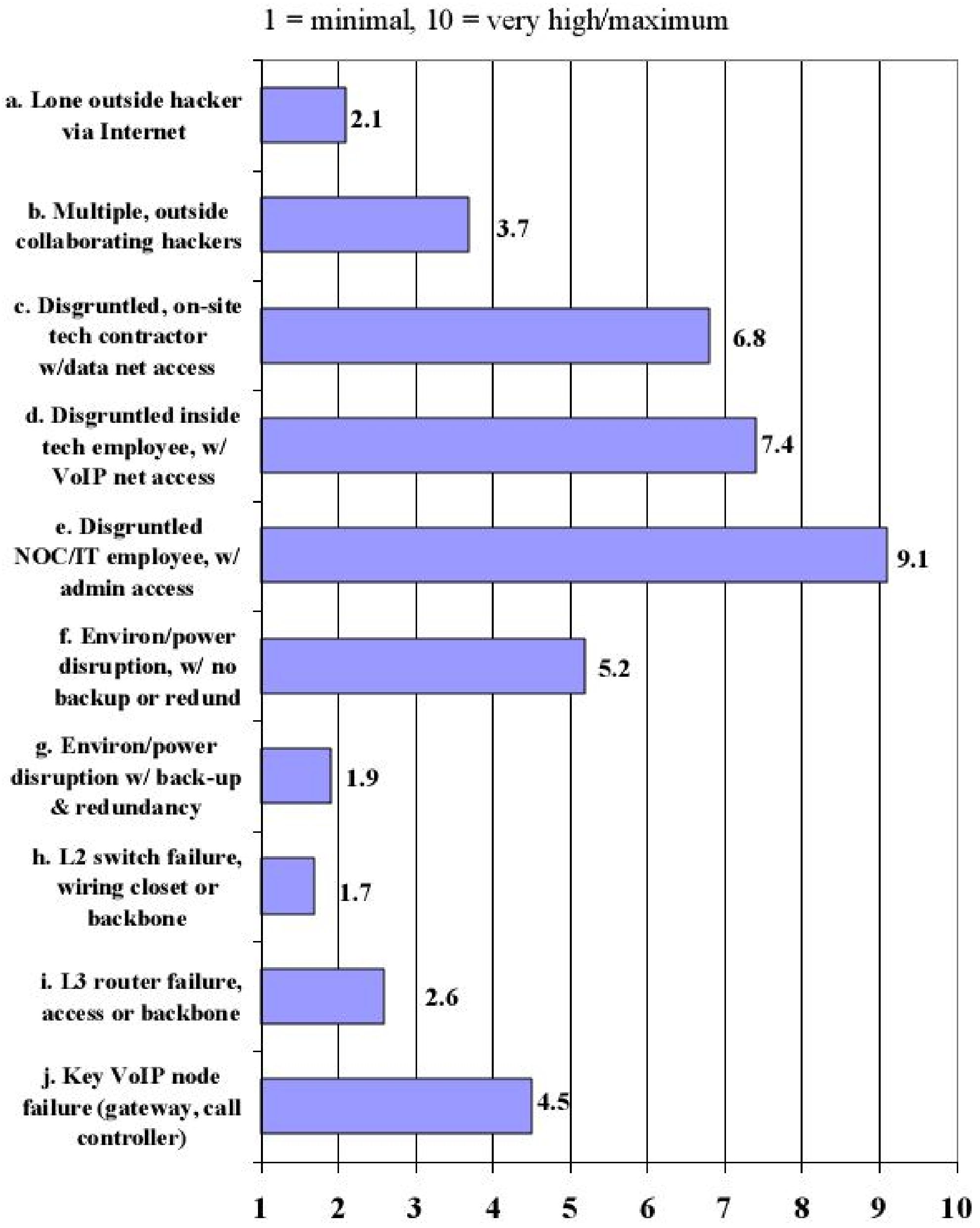


X.805 Security Domains


3rd party ASP Network Security Domain
3rd party ASP Network Security Domain
UE
Access Network Security Domain
Visited NGN Network Security Domain
Home NGN Network Security Domain
IPsec ESP tunnel
Security Gateway Function (SEGF)

Threats

Relative threats of NGN networks: insiders still #1 problem



NGN Security Summary

- Divided into Security domains
- Authentication is performed on service and transport layer
- Authentication for NGN IMS is based on identity and keys stored on smart card (UICC)
- The S-CSCF authenticates users during registration
- Full IMS security as defined by 3GPP is the preferred solution
- Domains are considered to be trusted
- Inter-domain security is provided by IPsec
- Media data security relies on transport network

Conclusions

- The IMS paradigm introduces several new attack vectors
- Critical Infrastructure such as SS7 is more exposed and will be targeted
- NGN Security is well defined and properly documented – at least in theory
- NGN implementations will likely suffer from interoperability problems leading to security exposure
- The complexity of emergent network architectures will present a serious challenge to their security
- Operators and Regulatory Bodies must embrace security as part of the design process of their networks

Questions?

Contact: eg@tstf.net

Thanks

- H.E. Mr. Mohamed Nasser Al Ghanim
- The HITB Crew
- The TSTF OOB Research Group

Some illustrations on slides copyright from RCS Labs, Data Connection Limited, Aqsacom, 3GPP, Ericsson, ETSI, EMC, ITU, Merrill Lynch, Newport Networks