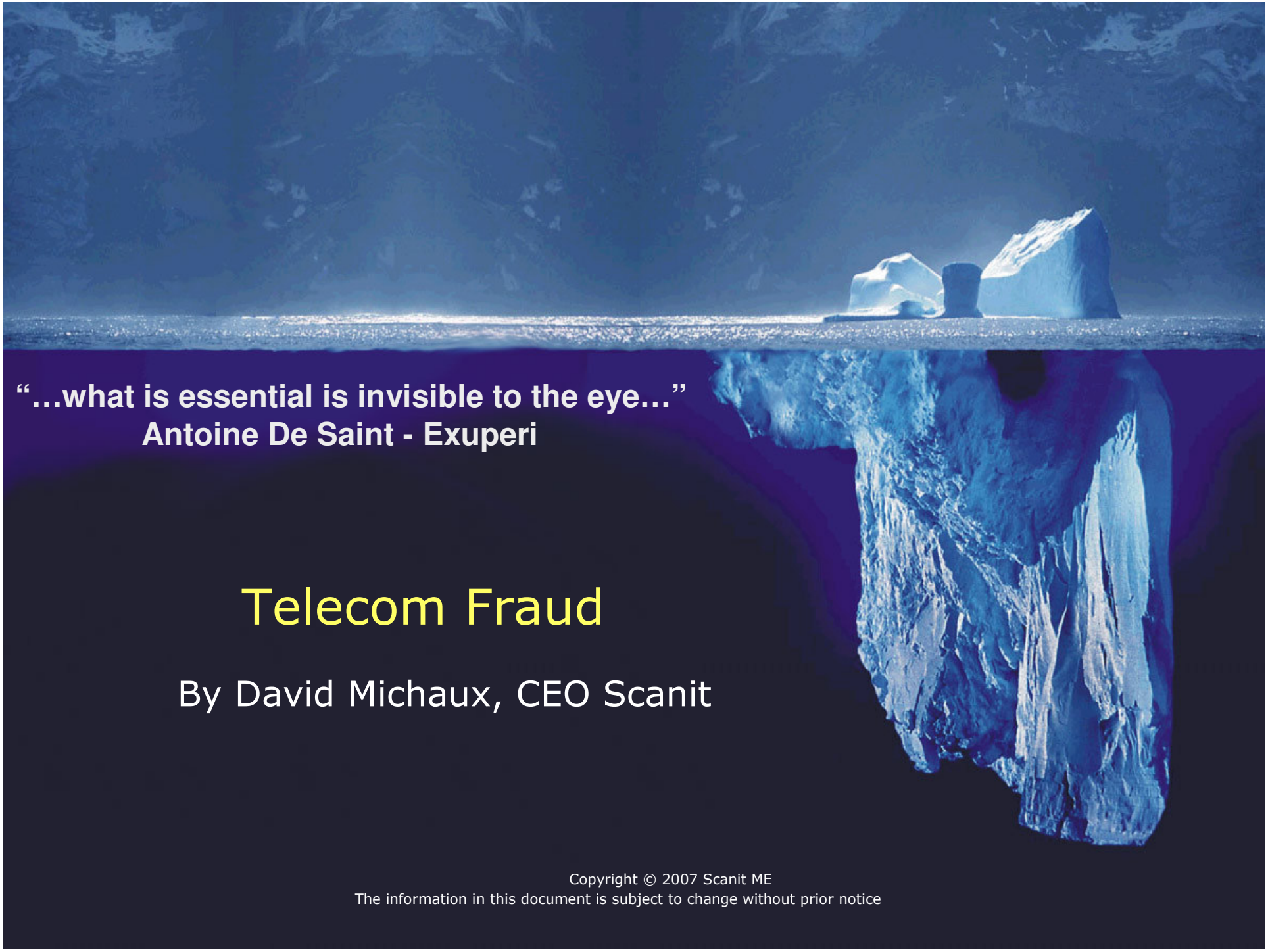


"…what is essential is invisible to the eye…"
Antoine De Saint - Exuperi

Telecom Fraud

By David Michaux, CEO Scanit

Agenda

- Introduction to Fraud
- Telecom Fraud Statistics
- Real time security breaches
- Types of telecom fraud
- Scenarios and examples
- SS7 and .. Vulnerabilities
- How easy it is .. (Live Demo)

Introduction to fraud

- Fraud Definitions

  “Intentional misrepresentation or concealment of information in order to deceive or mislead.”

  ”An intentional deception or misrepresentation that an individual knows to be false that results in some unauthorized benefit to himself or another person”

- Telecom Fraud

  Telecommunication fraud is the theft of telecommunication service (telephones, cell phones, computers etc.) or the use of telecommunication service to commit other forms of fraud. Victims include consumers, businesses and communication service providers.

Telecom Fraud Statistics

⇨ 1998 - A telecommunication company lost $700,000 in two days from PBX attacks

⇨ (PHOENIX,AZ) March 2003 – Phoenix-based Communications Fraud Control Association (CFCA) estimates the annual telecom fraud losses worldwide to be in the range of $35 - $40 billion U.S. dollars in contrast to the organization's previous (1999) estimate of $12 billion

Telecom Fraud Statistics

- A summary of the findings of the CFCA survey, 2005:

  80% of the telecom companies surveyed said that global fraud losses have increased

  45% of the respondents confirmed that telecom fraud has trended up within their own company

  Subscription fraud and Identity (ID) Theft continue to be the most common types of telecom fraud

  PBX/PABX/Voicemail fraud and Calling Card fraud are prevailing

Telecom Fraud Statistics

The Financial Impact

⇨ Average telecoms operator:

Loss of **3 to 6 % annual net revenues**

⇨ Other operators

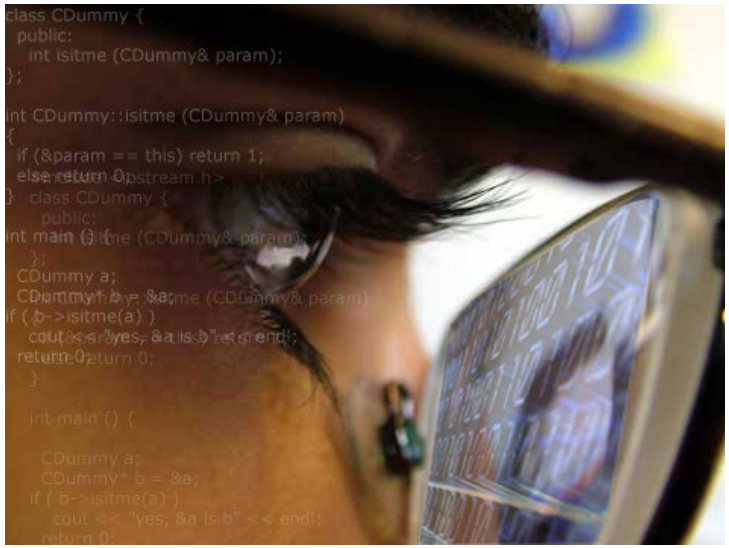
20 to 30 % Or more

⇨ Organized crime

$55 billion a year from illicit fraud schemes

Real time security breaches …

Real time security breaches and vulnerabilities in large enterprise organizations..



Set Target –> Telecom Industry

A Miami man was charged Wednesday with stealing more than 10 million minutes of VOIP (Voice over Internet Protocol) telephone service and then selling them to unsuspecting customers for as little as US$0.004 per minute.

Pena presented himself as a legitimate telecommunications wholesaler, while at the same time using hacking techniques to steal networking services valued at as much as $300,000 from each of the carriers.

With more than $1 million in profits from the scheme, Pena was able to buy real estate, a 40-foot motor boat and customized 2004 BMW M3 sports car, the U.S. Attorney said.

The whole story at:
http://www.infoworld.com/article/06/06/07/79053_HNvoiphack_1.html

Target – Telecom Industry (cont.)

An Indian woman has been arrested for allegedly leading a gang that hacked into the Philippines telecommunications system to make unauthorized long-distance calls, officials said Thursday.

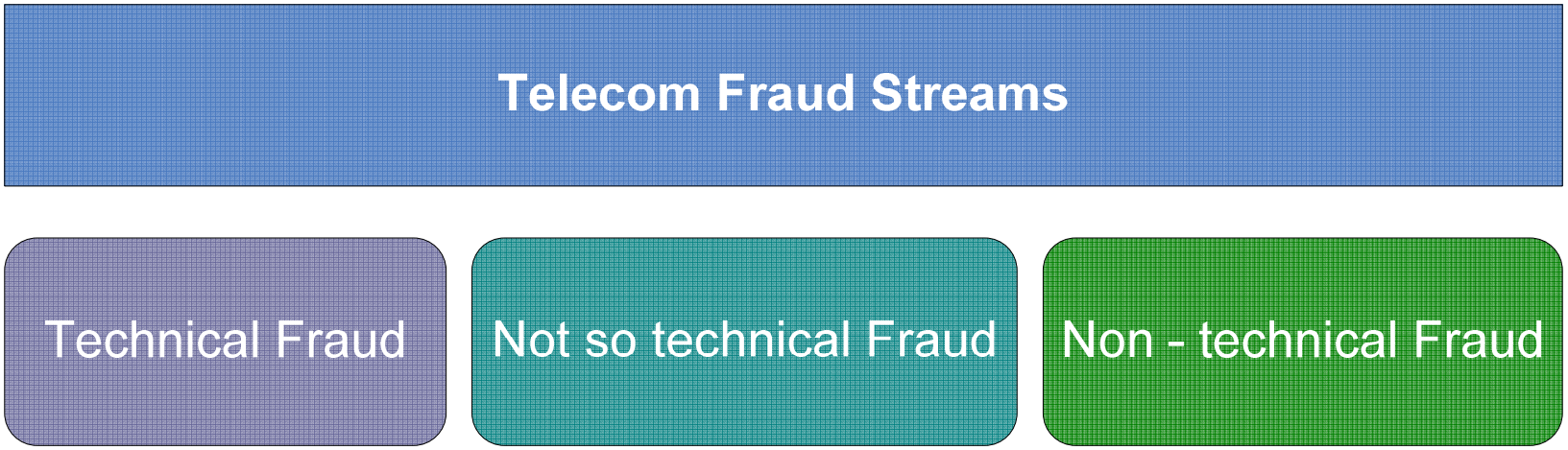
Khemlani allegedly financed a gang which tapped into the telephone systems of some 369 institutions, including private companies government agencies and foreign embassies to make unauthorized long-distance calls for which they charged a fee.

Their activities cost the Philippine Long Distance Telephone Co. some 197 million pesos (3.5 million dollars) in lost revenues, the bureau charged.

The whole story at:
http://www.long-distance-phone-cards.info/news/keys/hack+telecommunications+system

Types of telecom fraud

- Telecom Fraud can be divided in the following streams:



Technical Telecom Fraud

Technical Telecom Fraud:

Boxing

Clip -on fraud

Payphones

Telecard Fraud

Not so technical Telecom Fraud

Not so technical Fraud:

Calling Card Fraud

Premium Rate Service Fraud

Subscription Fraud

Non - technical Telecom Fraud

Non - technical Fraud:

Audio Text Scams

Comfort Services Abuse

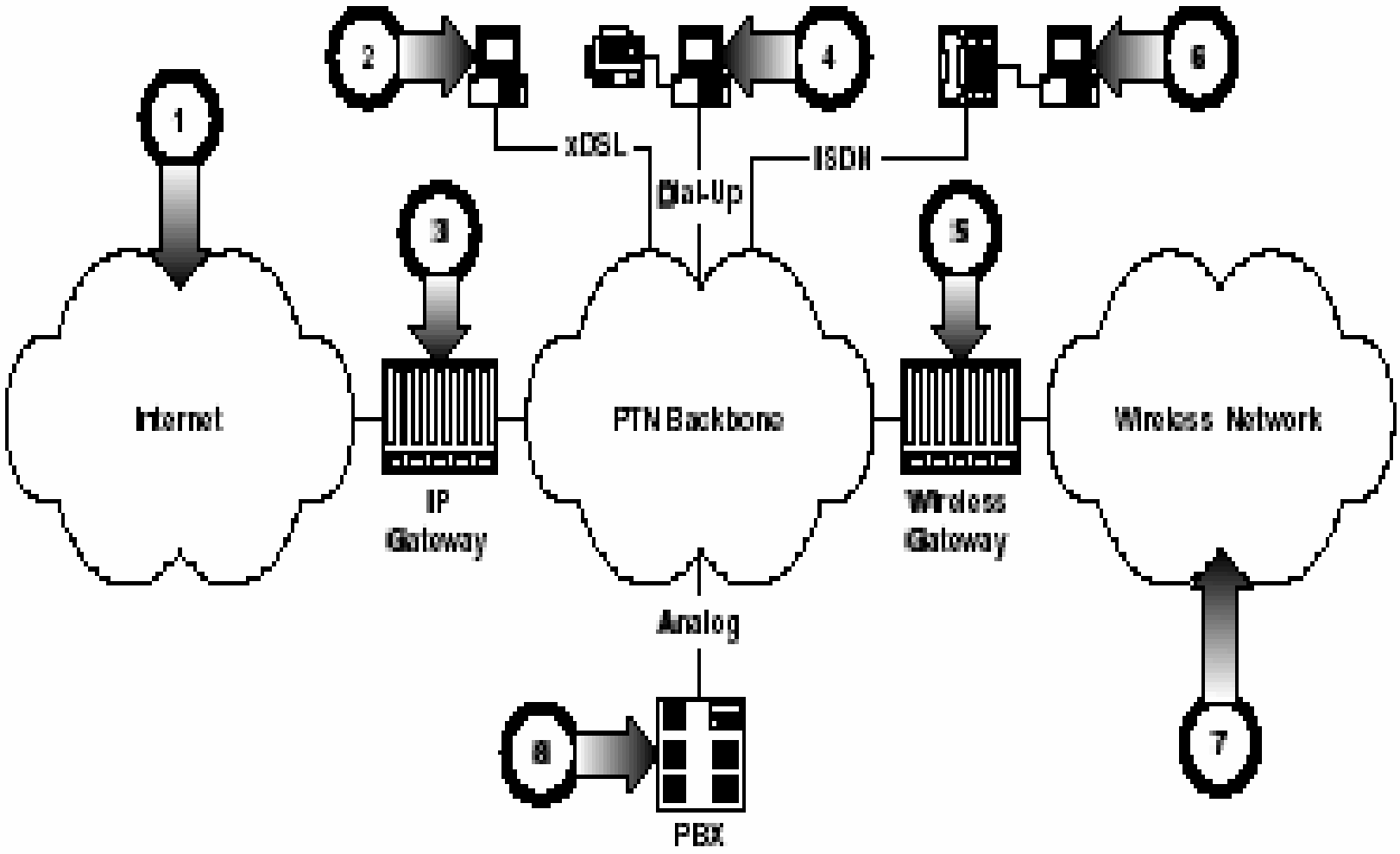
Cramming

PABX – hacking

Slamming

Social Engineering

PTN Attacks



PTN Attacks – cont.

- Point 1—Internet attack
- Points 2, 4 and 6—x-DSL, Dial-up and ISDN threats
- Points 3 & 5—PTN gateways
- Point 7—Wireless network vulnerabilities
- Point 8—PBX attacks

PTN Attack taxonomy

	MODIFICATION	INTERCEPTION	INTERRUPTION	FABRICATION
PTN IN-BAND	Toll Fraud (DTMF) * Chartreuse Box (Utility Theft) * Switch Tampering	Eavesdropping (Physical) * Wire Tapping Eavesdropping (DTMF) * Brown Box * Dayglo Box	Denial of Service (Physical) * Line Cutting Denial of Service (DTMF) * Copper Box * Blotto Box	Spoofing (Software) * Caller ID Subversion Toll Fraud (DTMF) * Red Box * Blue Box * Cap'n Crunch
PTN OUT-OF-BAND	Toll Fraud (Software) * OSS Attack * Billing DB Alteration * Toll Free DB Alteration * Credit Insertion * Advanced Service Fraud Eavesdropping * Speed Dialing DB Attack * Number Translation DB Attack * Routing DB Attack	Eavesdropping (Software) * SS7 Packet Sniffing * SS7 Authentication Attack * Voice Mail Snooping * Unauthorized SCP Browsing * Stealth Conference Calls	Denial of Service (Software) * OSS Component Destruction * Virus, Worm, Trojan Horse * Call Forwarding DB Deletion * SS7 Authentication Attack * Routing DB Deletion * Number Translation Deletion * Call Forwarding DB Deletion * Speed Dialing DB Deletion * Voice Mail DB Deletion	Spoofing (Software) * SS7 Authentication Attack Eavesdropping (Software) * Call Forwarding DB Insertion * STP Impersonation * SSP Impersonation * SCP Impersonation
WIRELESS	Toll Fraud (MIN/ESN) * Billing Database Alteration * Bogus HLR/VLR Data * EIR Record Deletion	Eavesdropping (Scanner) * MIN/ESS Code Theft * Confidential Information * Credit Card Numbers * Bank Account Numbers * Social Security Numbers	Denial of Service (Software) * Authentication Expoit (SS7) * Code Flaw Attack * Database Attack * SMS Exploits Denial of Service (Hardware) * Cellular Tower Flooding	Toll Fraud (MIN/ESN) * Cellular Cloning * Subscription Fraud * Roaming Fraud * Parallel Call Forwarding
INTERNET	Toll Fraud (Software) * VoIP Authentication Alteration * Subscription Fraud Eavesdropping * Rerouting VoIP Packets	Eavesdropping (Sniffer) * Username/Password Theft * Confidential Information * VoIP Packet Capture * Credit Card Numbers * Bank Account Number * Social Security Numbers	Denial of Service (Software) * Kiddy Scripts * Smurf, * Ping 'o Death * Authentication Attack (SS7) * Code Flaw Attack * SS7 Element Infiltration * Virus, Worm, Trojan Horse	Toll Fraud (Software) * Password Attack (SS7) * Code Flaw Attack * Virus, Worm, Trojan Horse Denial of Service (Software) * Cellular Tower Flooding

Boxing – the color doesn't matter..

- **Black box** : suppress billing
- **Blue box** : suppress billing & billing information
- **Beige box** : give a fraudster access to a customer's line via clip-on
- **Brown:** Creates a party line from two phone lines
- **Red box** : make free calls from coin operated telephones
- **Green:** Emulates the coin collect, coin return, and callback (DTMF) tones
- Silver: Generates tones for ABCD keys

Red Box

- Not applicable on every payphone
- Emits tones to inform telco that the right coins were deposited
- « Red box » produces the same tones
- Autorisation « bypassed »
- Free calls

PREMIUM RATE SERVICES

Principle

- **Marketing numbers**
  - PRS
  - TOLL FREE
    - Examples
      - 070
      - 077 erotic lines Internet
      - 078 shared cost, provider/customer
      - 0800 toll free numbers
      - 0900, 0901, 0902, 0903, 0909…
- **Service Provider & Operator**

PRS - FRAUD SCHEMES

- **Fraud by provider: trying to inflate traffic towards his own number (077 & 0900)**

  Example:

  – the “S”-case

Subscription fraud

- ⇨ The abuse of the identity of an individual or a company (or their information) to obtain goods or services:
- ⇨ Using pieces of personal and financial information
- ⇨ Identity verification: secondary to sales in most telecom companies: personnel evaluated on sales, fraud not part of equation

Subscription fraud

Where does it happen?

- 90 % of all subscription fraud is residential
  - "family fraud"
  - perpetrator & victim are related
  - 60 % are women
- However the remaining 10 % is responsible for the major loss

Residential Subscription fraud

- **COUNTERFEITED ID-CARD or PASSPORT**
- **STOLEN ID-card**
- **REAL ID - the dead or the living**
- **REAL ID - REAL ID-CARD based on stolen IDcard with forged identity**
- **FAKE ID**

Subscription Fraud - Business Segment

- ***Pretend you are in business:***

  From: MUKTHAR GILANI
  > [mailto:interactivemarketinggroup@yahoo.com]
  > Sent: 18 February 2004 20:35
  > To: call.and.conference@belgacom.be
  > Subject: sign up for self dail out conference>
  > Interactive Software Federation Of Europe
  > 38 Avenue des Arts / Kunstlaan
  > 1040 Bruxelles / Brussel
  > tel 02/5027462
  we like to reserve self dailout conference we need six subcription numbers
  for difereent department please email us six chairpersons code and
  particpant code starting from 19/2/2004 till 26/2/2004
  > Do you Yahoo!?

Business Segment – cont.

- **Send a letter on a company letterhead:**

  “Thanks for your email i have sent you approval letter so please sign up for self dail out conference and email me about pin numbers.

  Thankyou

  “

Call Sell Operation

Sell calls at considerably reduced rates by:

- **Using a combination of fraudulent techniques**
- **Operation "normally" targeted at ethnic communities who want to keep in contact with family and friends overseas**
- **Cost of the operation born by anybody else but the persons who set up the operation or NITP (no intention to pay)**

Call Sell Operation – cont.

How is it done ?

- **Fraudulent account**
- **Hacked PBX**
- **Fraudulent calling card platform**
- **Security hole in the network**

Sell Call – Scenario 1

- **Abuse of conference call facility**
- **Abuse of call-forwarding facility - *21*….#**
  – phone houses were set up by the dozens

- **Involved in the resale of reloaded telecards**

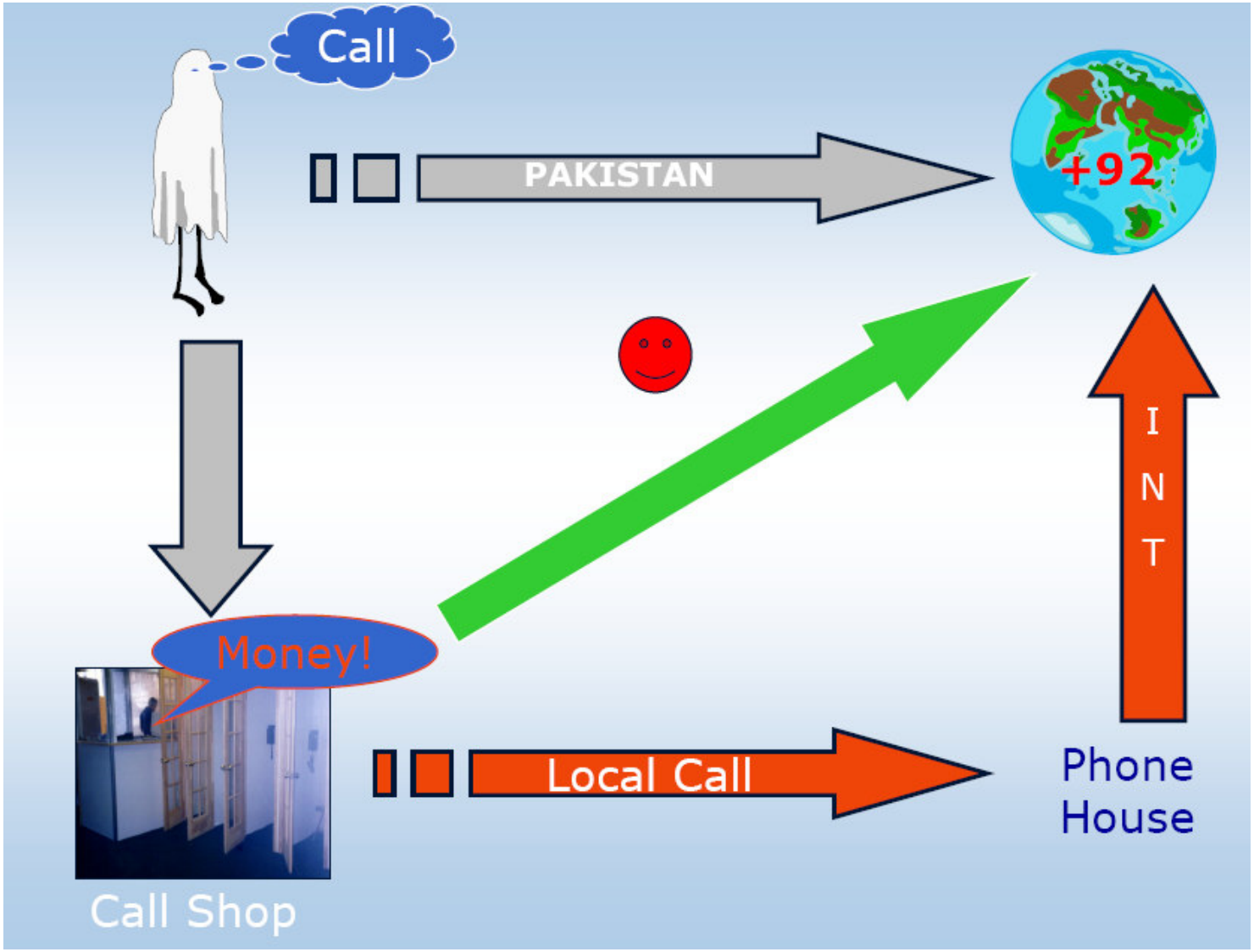
- **Involved in the sale of calling cards of fraudulent calling card platforms**

- **Premium rate fraud**

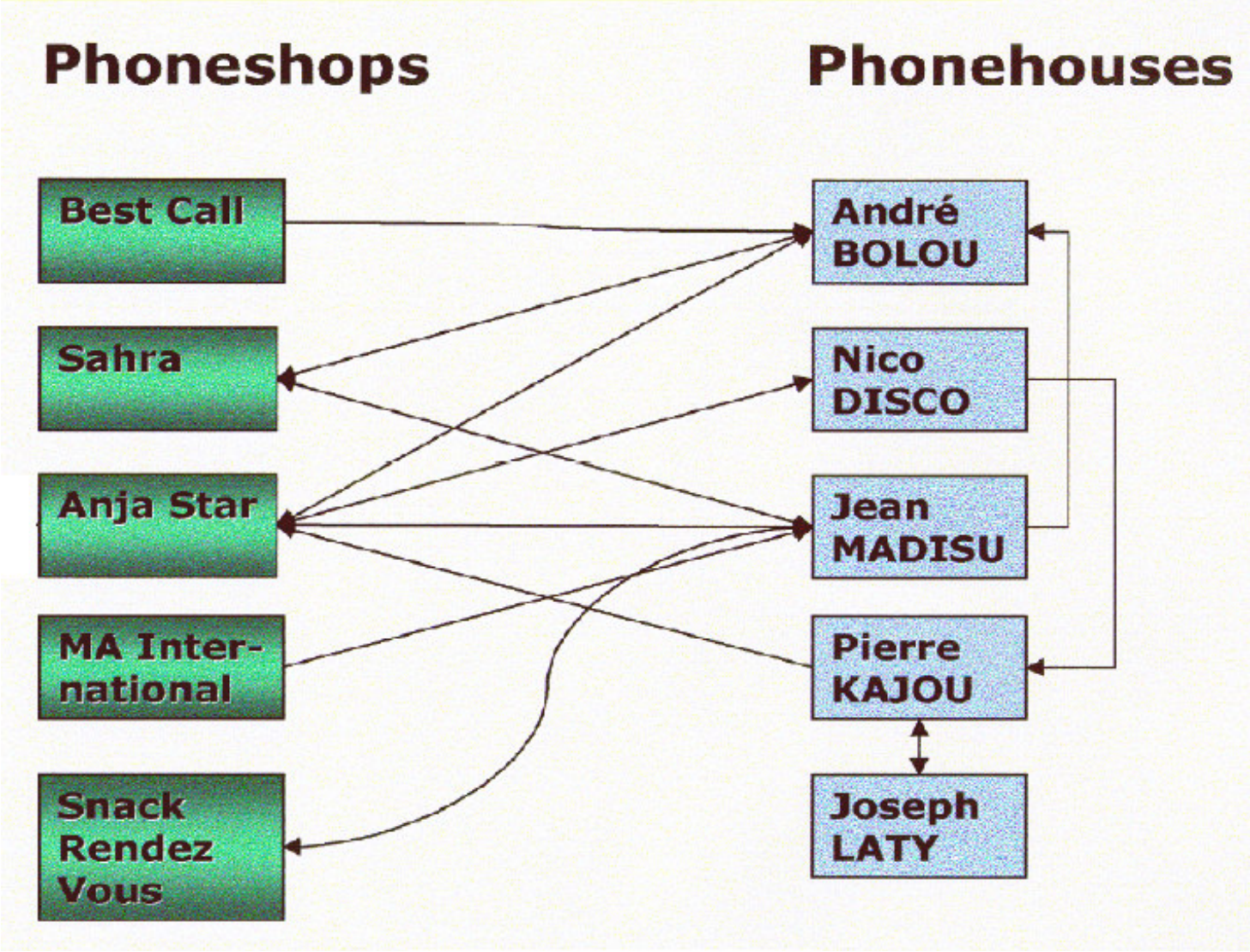
Sell Call – Scenario 2

- **Abuse of hacked PBX's**
  - **– hiring hackers to intrude PBX's & get hold of DISA codes**
- **With a little help from the "friends":**
  - **•manipulating CLI to mask the fraudulent traffic**
- **Exploiting security holes eg. in the software of a voice-mail system (2002)**
- **Moving to retail market segment (calling cards)**

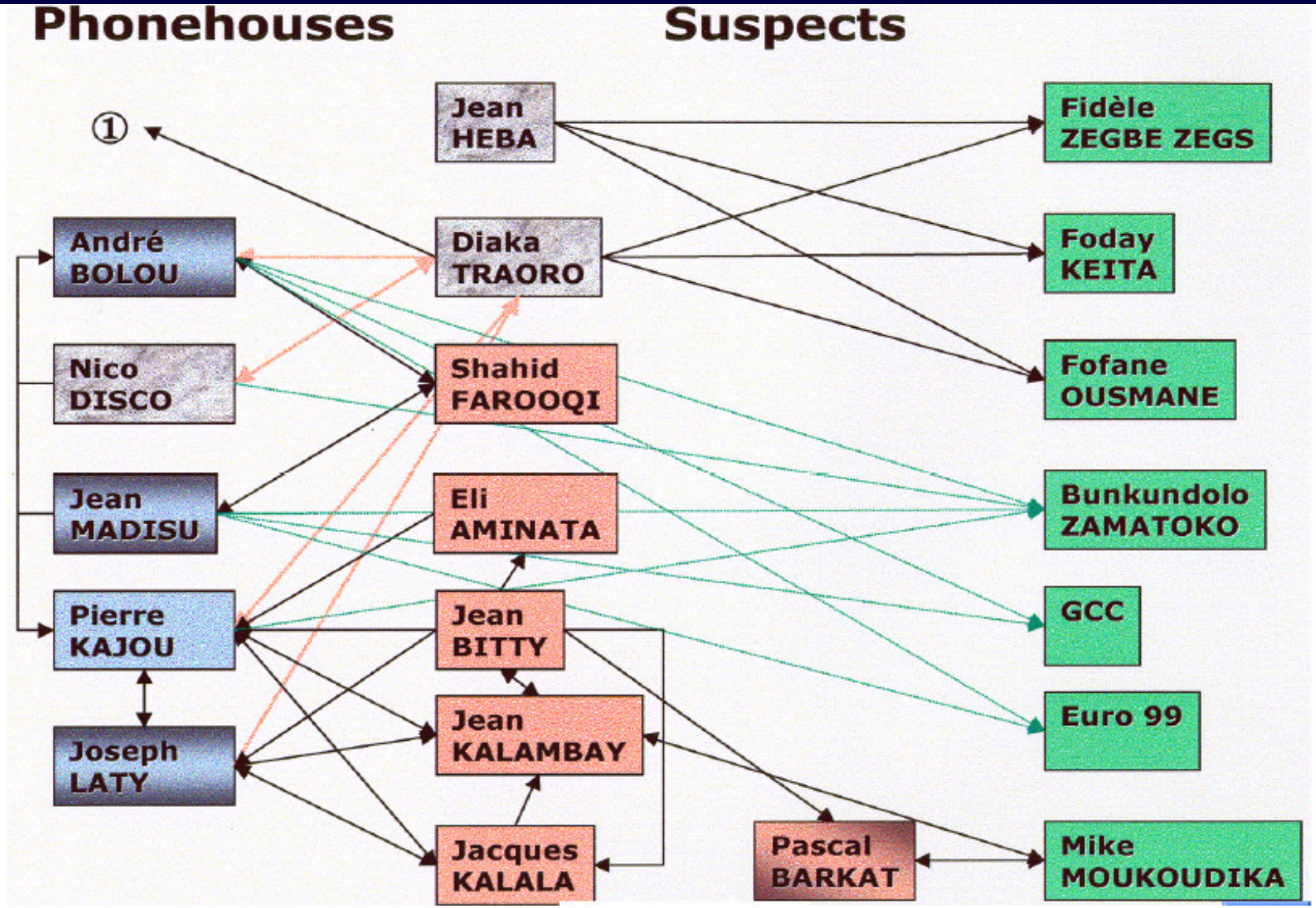
Scenario 2 - Visualized..



Scenario 2 - Visualized..



Scenario 2 - Visualized..



PBX Threats

Private Branch Exchange (PBX) is a computer based switch that can the thought of as a small in-house telephone company

The following threats affect a PBX:--

- **Theft of service**
- **Data modification**
- **Unauthorized access**
- **Disclosure of Information**
- **Denial of service**
- **Traffic analysis**

PBX Threats result in..

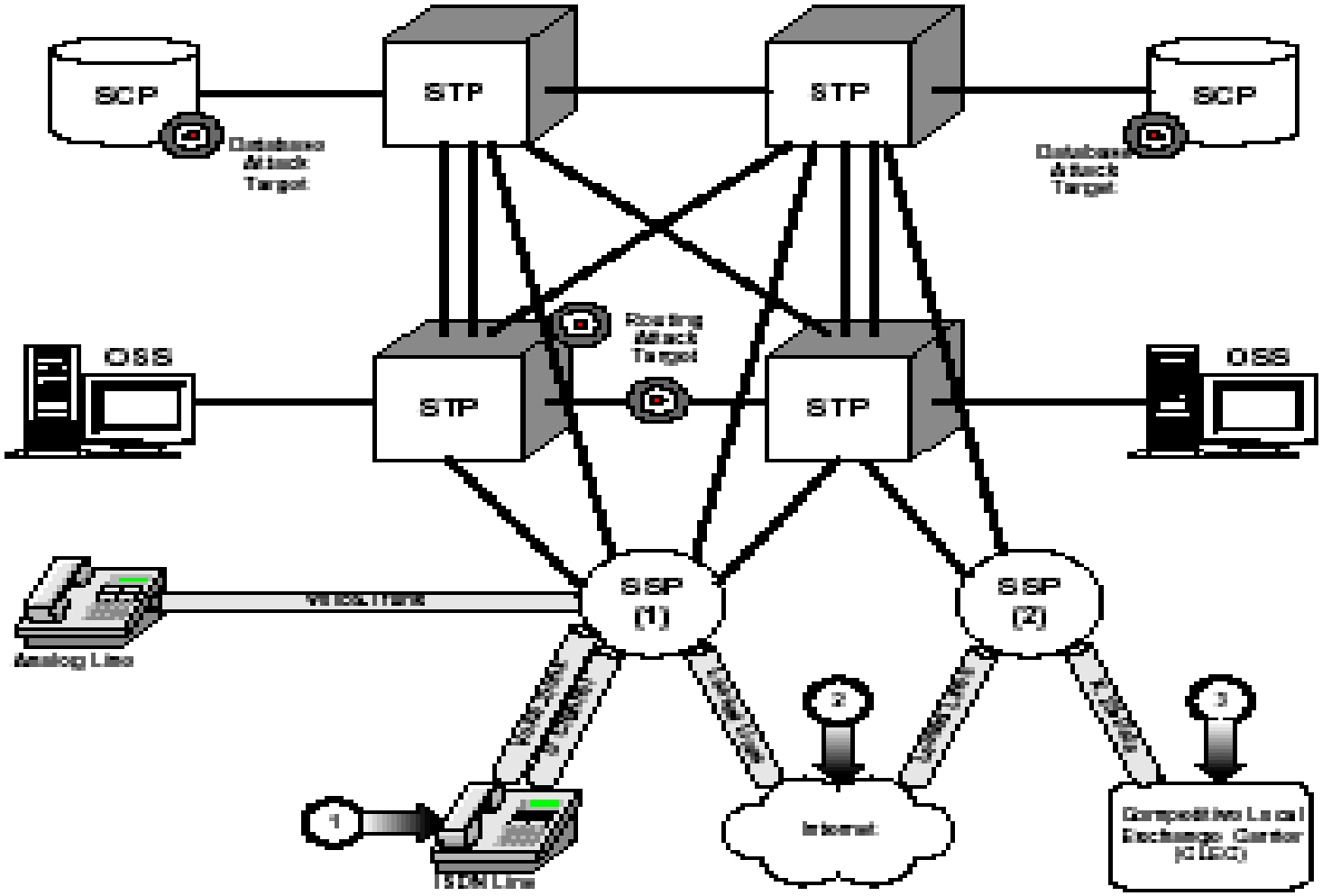
- Loss of confidential information from voice mail
- Toll fraud
- Monitoring of calls
- Data modification
- Denial of service
- Rerouting of calls and impersonation
- Monitoring of room audio
- Use of Voice mailboxes which are not assigned

Cont..

SS7 ..and vulnerabilities

SS7 ..and vulnerabilities

SS7 Architecture



SS7 ..and vulnerabilities (cont.)

Major SS7 network vulnerabilities arise from:

•The number and complexity of interfaces between distinct SS7 entities

•Advanced services like call forwarding have intrinsic vulnerabilities (attackers can create havoc by modifying SCPs containing forwarding destinations).

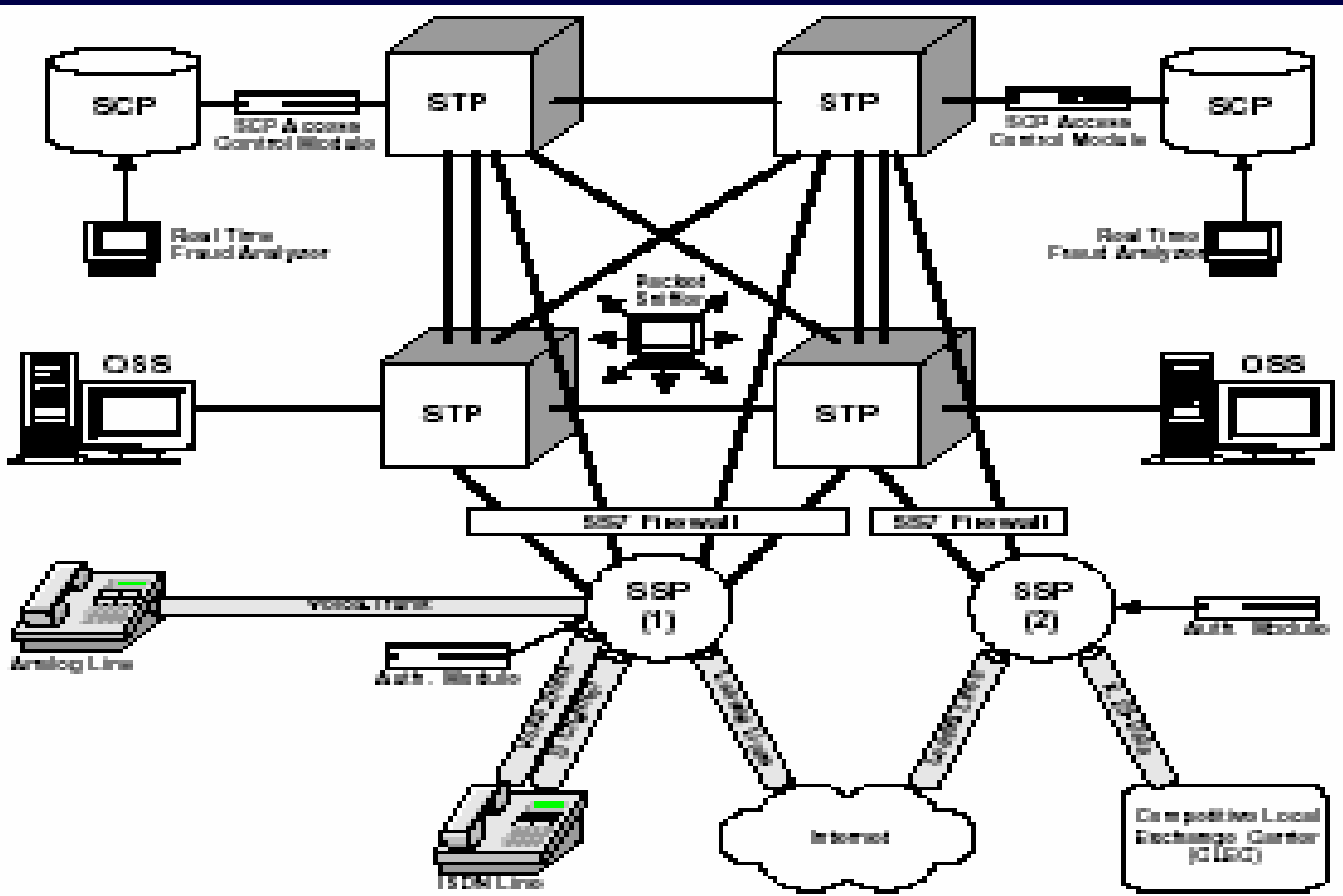
•The increasing interdependence and interconnectivity between SS7 networks and the Internet.

• SS7 incorporates limited authentication procedures (because it was originally designed for a closed telecommunications community). Anyone capable of generating SS7 messages and introducing them into a network can disrupt PTN services.

SS7 Attack Taxonomy

	Modification	Interception	Interruption	Fabrication
SSP	Physical modification • Hardware configuration ISDN End User • ISUP Msg. modification	Eavesdropping • SS7 Packet sniffing • SS7 Authentication attack • Stealth Conference calls	Denial of service attack • SS7 Authentication attack • Routing DB attack • MTP link mgmt. attack	Spoofing • SS7 Authentication attack oISUP, ANI spoof Eavesdropping • SSP impersonation oISUP msg. generation
STP	Toll Fraud(Software) • OSS attack Eavesdropping • Routing DB attack • SCCP Msg. Rerouting attack	Eavesdropping (Software) • SS7 Packet Filtering • SCCP/Global title translation attack	Denial of service (Software) • OSS Component destruction (Virus, Worms, Trojan horses) • Routing DB attack • LNP DB Attack • SCCP Msg. alteration • MTP link mgmt. attack	Eavesdropping (Software) • STP Impersonation o SCCP Msg. generation
SCP	Toll Fraud(Software) • LIDB (Billing) Alteration • CMSDB(toll free) Alteration • Credit insertion • Advanced service Fraud o TCAP Msg. modification Eavesdropping • Speed Dialling • Number translation DB attack	Eavesdropping (Software) • SS7 Packet Filtering •Voice mail Snooping • Unauthorized SCP browsing oTCAP modification • Stealth Conference calls	Denial of service (Software) • Call forwarding DB deletion • Number translation deletion • Speed DiallingDB deletion • Voice mail DB deletion • LNP DB attack • TCAP Msg. alteration • MTP link mgmt. attack	Eavesdropping (Software) • Call forwarding DB Insertion • SCP impersonation • SCCP,TCAP Msg. Generation • TCAP DB query fabrication

SS7 Attack Management system



SS7 Attack Management System (cont.)

- Since SSPs represent the SS7 network perimeter, authentication modules are positioned at each SSP to certify all entries. The modules detect attempts at spoofing and identity subversion by comparing SS7 messages with signatures of spoofing attacks.
- SS7 packet sniffers, specially designed to read and interpret SS7 messages, are the primary information gatherers of the attack management system. These are positioned to passively monitor all signaling channels.
- SS7 firewalls are designed to actively filter SS7 messages. They are positioned between SSPs and STPs to control traffic at all switching points. The firewalls screen traffic for attack signatures that are maintained in a special database.
- A real time fraud analyzer is located at each SCP as they interfaces with databases supporting PTN services. The analyzers examine SCP queries (TCAP messages) for suspicious patterns.
- SCP access control modules work in conjunction with fraud analyzers. They are positioned in front of SCPs to regulate entrance.

How easy is it?

LIVE DEMO

Questions