Hacking, Phreaking, Carding & Social Engineering: back to the r00ts.

Workshop della
Commissione Calcolo e Reti dell'INFN
Hotel Ambasciatori
Rimini
11 - 15 giugno 2018

Speaker:
Raoul “Nobody” Chiesa

DISCLAIMER

- This presentation **aims to tell you**, throught examples and historical case studies which really happened, **a piece of history** of "telematics", with a special focus towards the **hacking**, **phreaking** and **carding scene**.

- DON'T TRY THIS AT HOME!!! We do not advise to use this material in order to **break into telecommunication operators or IT systems.**

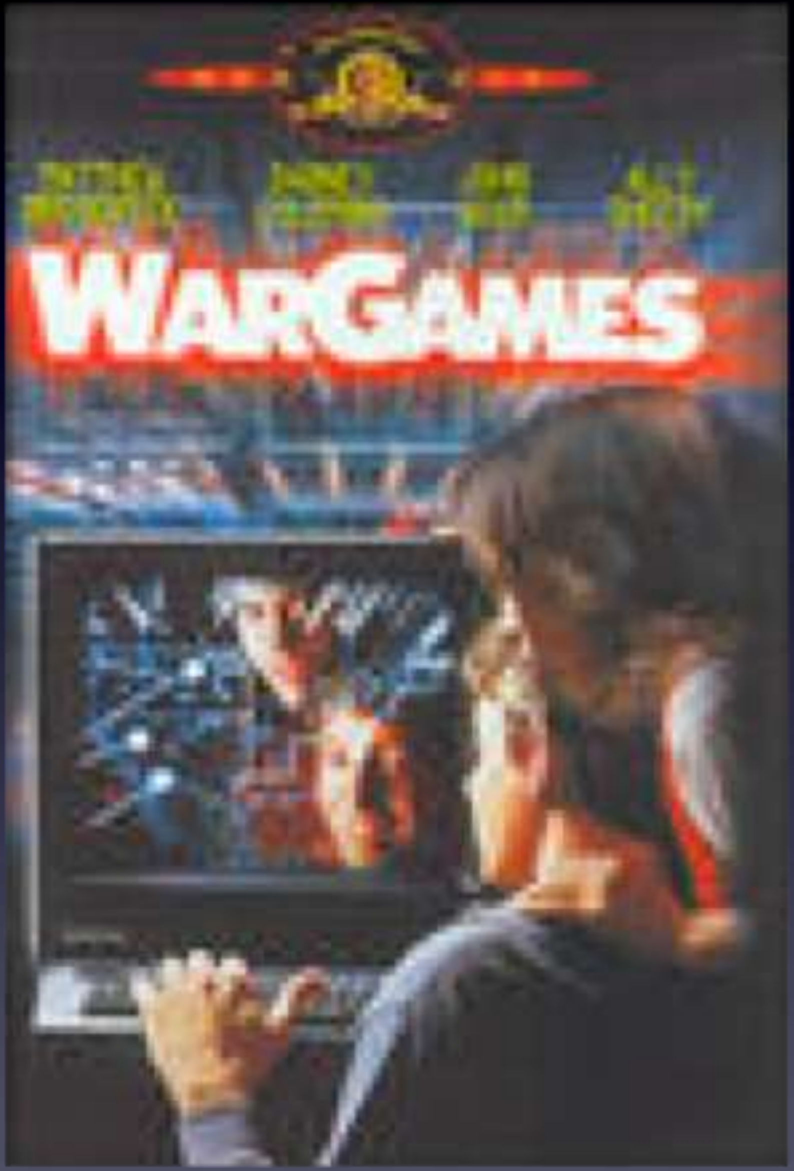
- Anyhow the author **cannot be held responsible** if you will decide, despite this disclaimer, to explore those systems, evaluating the whole thing as pretty sexy and fascinating, thus starting making mistakes, leaving tracks that would eventually allow the Law Enforcement to identify and bust you…

- As a last note, **whenever and wherever existing and applicable**, the **crimes committed and explained in this presentation** are from **more than 10 years ago**, so they are fallen into "prescription" ☺

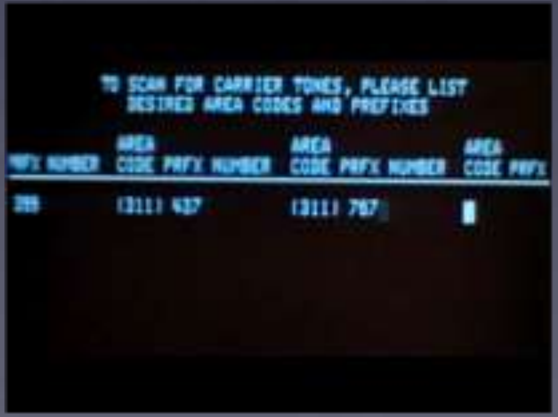
* 1983

At the very beginning..

- What generated more than 75M USD$ on that year?
- Well.. The very same thing that pushed most of us towards a deep interest on some topics…



WARGAMES



```
          TO SCAN FOR CARRIER TONES, PLEASE LIST
             DESIRED AREA CODES AND PREFIXES

           AREA                     AREA                     AREA
PRFX NUMBER CODE PRFX NUMBER        CODE PRFX NUMBER         CODE PRFX
--------------------------------------------------------------------------
399         (311) 437               (311) 767                █
```

* 1986

- Cellular phone network, 450 Mhz: the “car phones” or “portable” phones: today we may label them as a personal defense weapon ;)
- 300 BPS modem (Bits per Second!)
- Fidonet for “the mass” (very few people anyhow)
- A few “alternative” boards (BBS), designed for a few l33t users
- Family’s fights ‘cause of phone bills (300 BPS modem calls <u>PAID</u> towards USA)

«Portable» phones - LOL

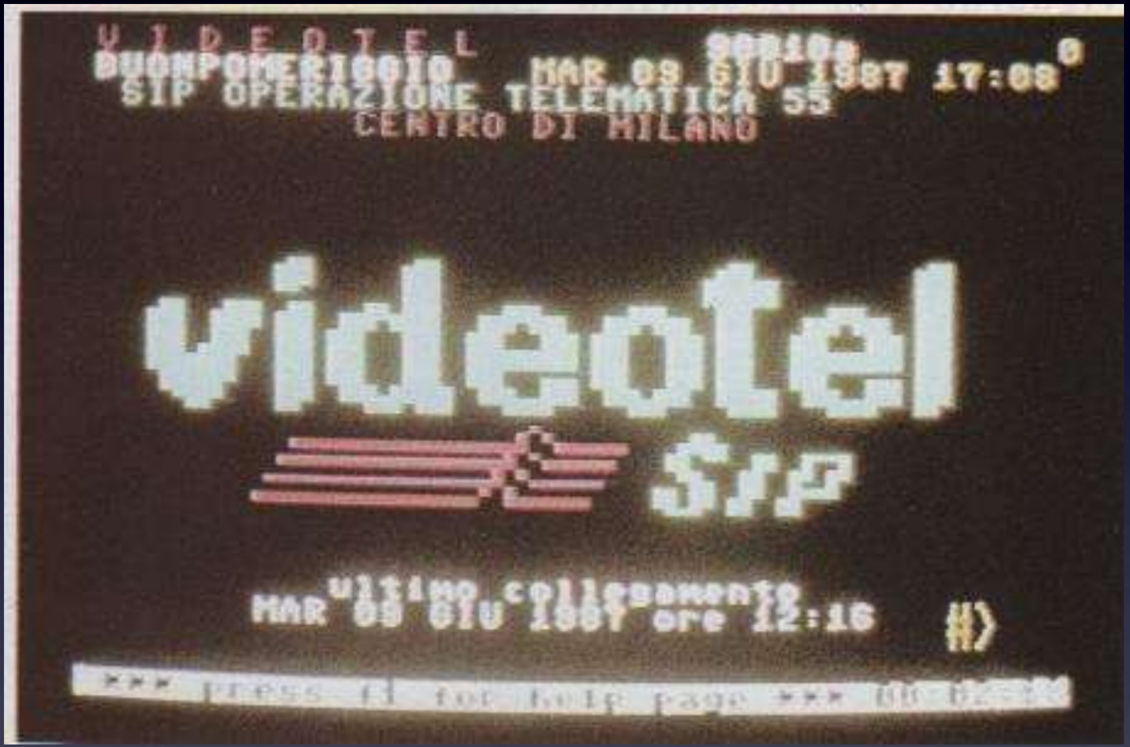
«Portable» phones - LOL

* 1988

- CEPT2/CEPT3 (1200/75 bps) in Italy, France, Germany, UK, etc. (Videotel, Minitel/Teletel, BTX, Prestel).

- Marketing made our job easy: “forced” selling of subscriptions to every town, region, province, and Public Administration entities

- The “telematic adapter” C-6499 (to be used with Commodore 64/128) and the Epson CX-21 for PCs



V I D E O T E L [illegible]

BUONPOMERIGGIO MAR 09 GIU 1987 17:08

SIP OPERAZIONE TELEMATICA 55

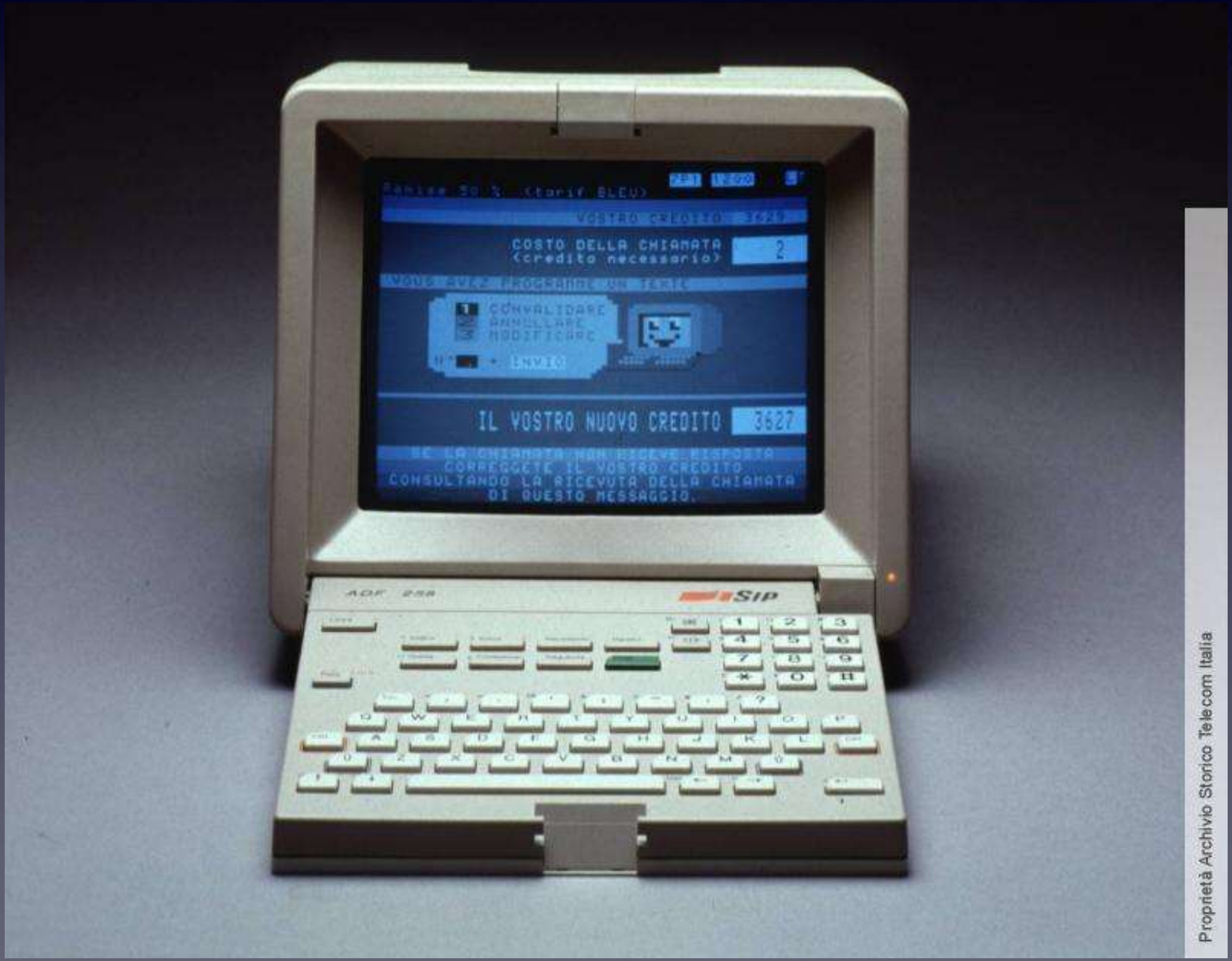
CENTRO DI MILANO

ultimo collegamento

MAR 09 GIU 1987 ore 12:16

#>

*** press f1 for help page *** [illegible]



Remise 50 % (tarif BLEU)

VOSTRO CREDITO 3629

COSTO DELLA CHIAMATA (credito necessario) 2

VOUS AVEZ PROGRAMME UN TEXTE

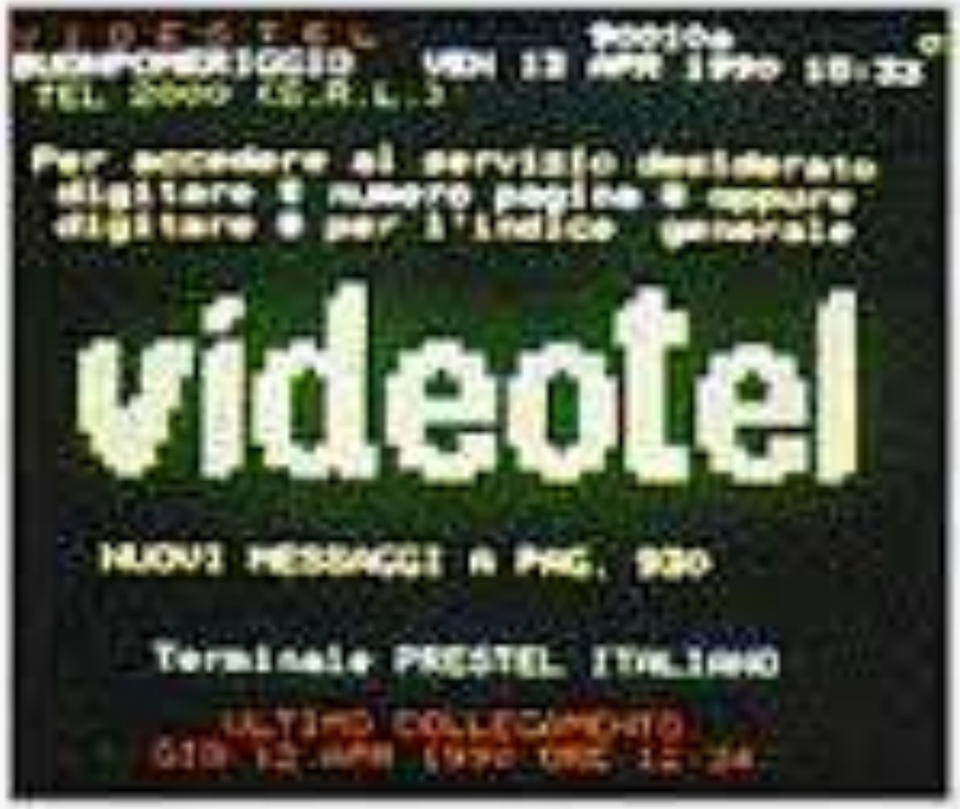
1 CONVALIDARE
ANNULLARE
MODIFICARE

N° + INVIO

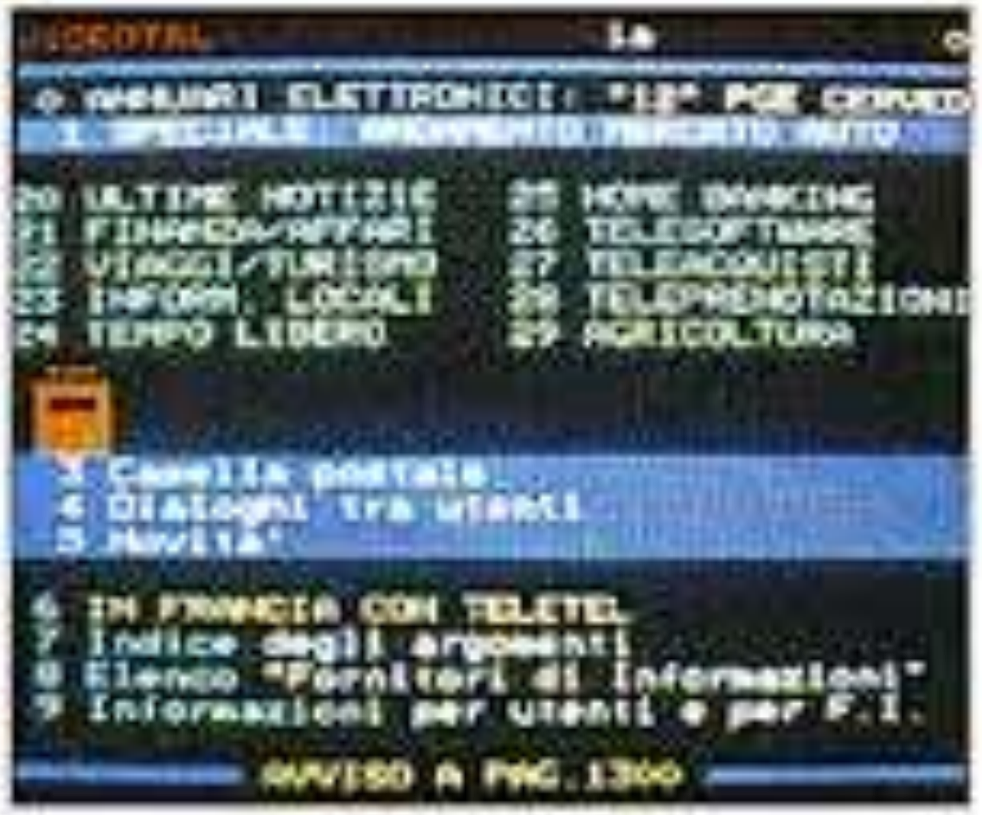
IL VOSTRO NUOVO CREDITO 3627

SE LA CHIAMATA NON RICEVE RISPOSTA
CORREGGETE IL VOSTRO CREDITO
CONSULTANDO LA RICEVUTA DELLA CHIAMATA
DI QUESTO MESSAGGIO.

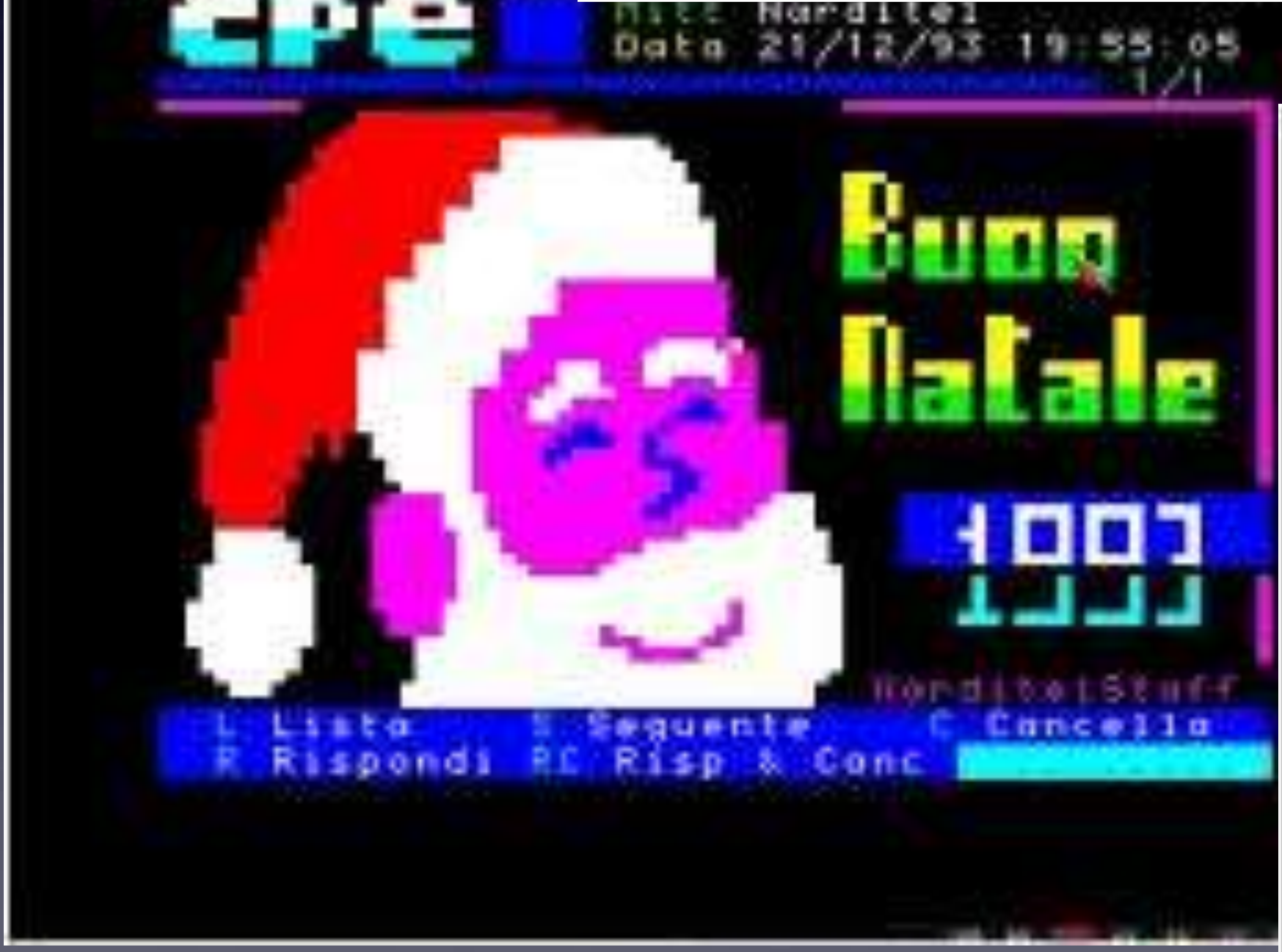
Proprietà Archivio Storico Telecom Italia



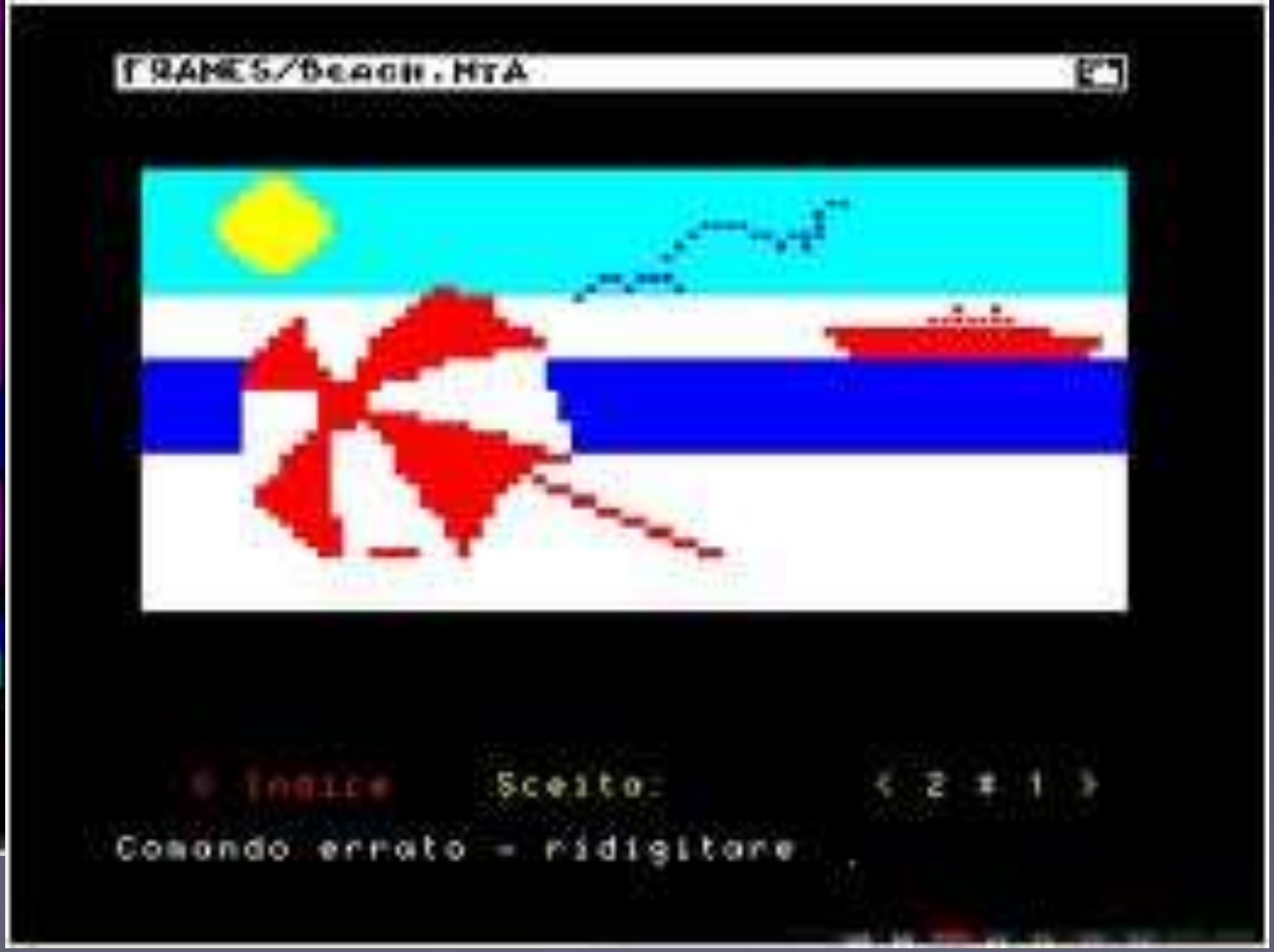
```
VIDEOTEL              900106a
BUONPOMERIGGIO    VEN 13 APR 1990 10:33
 TEL 2000 (S.R.L.)

Per accedere al servizio desiderato
 digitare # numero pagina # oppure
 digitare # per l'indice  generale

videotel

  NUOVI MESSAGGI A PAG. 930

    Terminale PRESTEL ITALIANO

       ULTIMO COLLEGAMENTO
    GIO 12 APR 1990 ORE 12:24
```



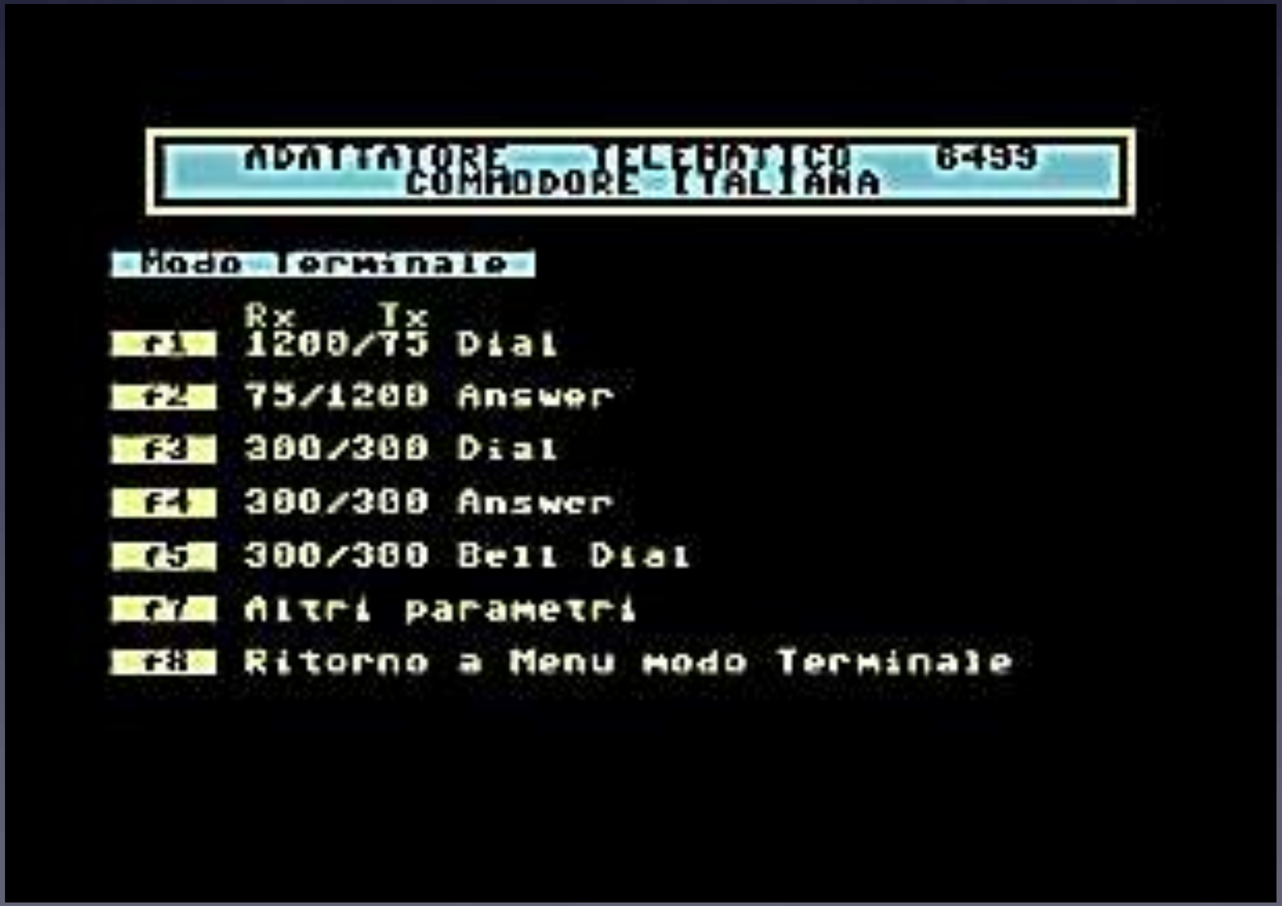
```
VIDEOTEL              1a
 0 ANNUARI ELETTRONICI: "12" PGE CERVED
  1 SPECIALE: ANDAMENTO MERCATO AUTO

20 ULTIME NOTIZIE        25 HOME BANKING
21 FINANZA/AFFARI        26 TELESOFTWARE
22 VIAGGI/TURISMO        27 TELEACQUISTI
23 INFORM. LOCALI        28 TELEPRENOTAZIONI
24 TEMPO LIBERO          29 AGRICOLTURA

  3 Casella postale
  4 Dialoghi tra utenti
  5 Novita'

 6 IN FRANCIA CON TELETEL
 7 Indice degli argomenti
 8 Elenco "Fornitori di Informazioni"
 9 Informazioni per utenti e per F.I.

          AVVISO A PAG.1300
```



```
FRAMES/BuonNatal
cpe     Mitt  Norditel
        Data  21/12/93 19:55:05
                                  1/1
                Buon
                Natale
                1993
               NorditelStaff
  L Lista     S Sequente    C Cancella
  R Rispondi  RC Risp & Conc
```



```
FRAMES/Beach.MTA

   0 Indice     Scelta:          < 2 # 1 >
Comando errato - ridigitare
```



```
ADATTATORE   TELEMATICO   6499
  COMMODORE ITALIANA

Modo Terminale

       Rx     Tx
 f1   1200/75 Dial
 f2   75/1200 Answer
 f3   300/300 Dial
 f4   300/300 Answer
 f5   300/300 Bell Dial
 f7   Altri parametri
 f8   Ritorno a Menu modo Terminale
```

* 1988

- **Videotel/Minitel/BTX services = chat systems (uh, really?? ;)**
- **The very first IRL meetings**
  - **Goal: to have sex with ppl u met in chat (things didn’t change so much since that… ☺**
- Videotel passwords were **reversed** and could be calculated (the Algorythm’s “myth”)
- Videotel’s “Content Providers” (CPs) begin **self-billing themselves**, so that their revenues rise up… Of course the money was billed to (regular) subscribers. Which, basically, didn’t even know what a “chat” was. LOL
- “SIP” pays (amazing amounts of money) to CPs.

* 1989

- Products were sold on Videotel: watches, wine, computers and flowers, **free for everybody**.. But, CPs do not always deliver the goods
- Car Plates real-time queries throught National Registry (abused by Private Investigators)
- How to rise up the money using “the Assistant” (today we name this “bot”)
  - Finally, the “black market” business gets started, and Italian coders are having phun

* 1989

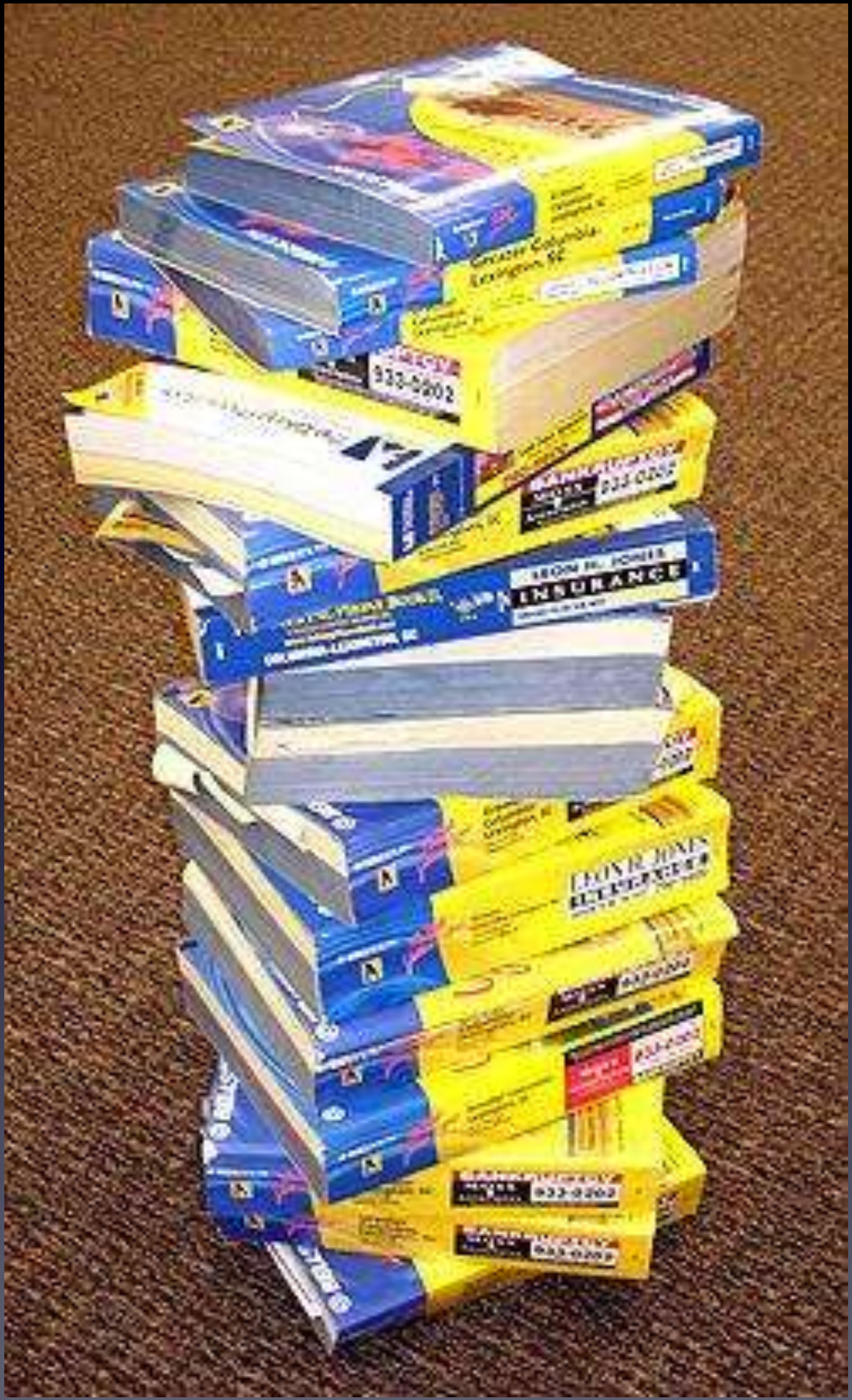
- The market releases the very first E-TACS (900 MHz)
  - Motorola MicroTAC, fu**ing expansive! i.e. as I’d cost 1.500 EUR today
- 0337 becomes 31337 ;)
  - People were stunned watching you at the traffic light, sit in the car and speaking at the phone!

* 1989

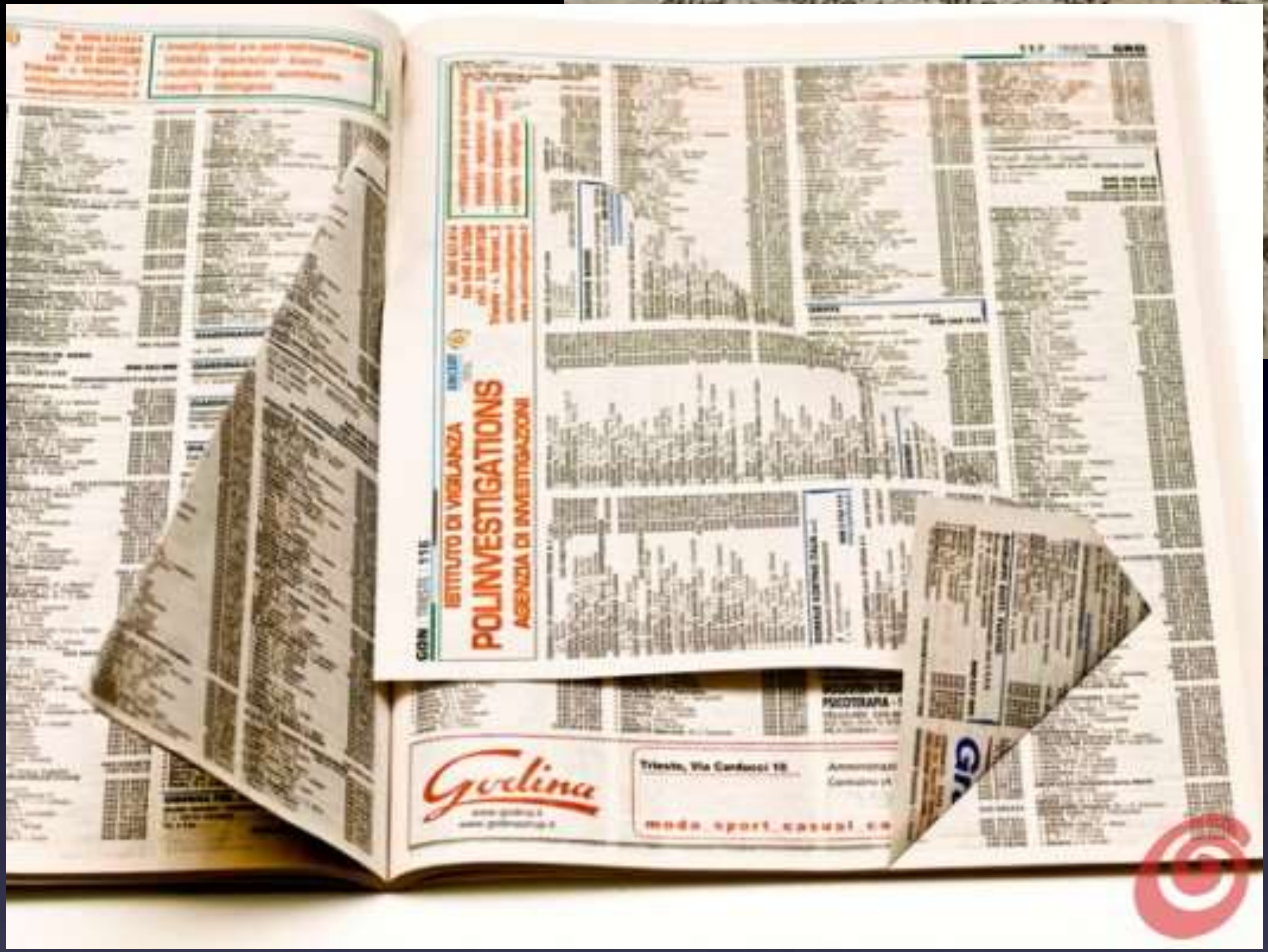
- Excessive use (aka “**hyper-fraud**”) brings to the end-of-life of those passwords generated throught easy algorythms; here SIP then generates new passwords, produced by new algos
- PS (Panic & Scare ™): Videotel CPs go “on crisis”; passwords become “goods”, with a price list.
    - A black market quickly emerges here (avg: 150/300 EUR for each sold password)
    - Recalls the 0day market thing, isn’it? ☺

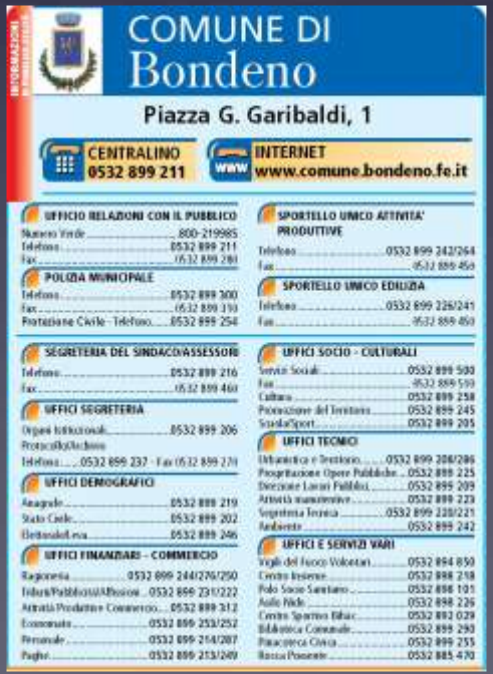
* 1989

- Now, people need **a way to find out passwords**: algos can’t be cracked anymore ☹
- **Social engineering** is the answer! Very first organized groups then setup, backed by the money coming from the passwords selling
    - Phone calls-based, and physically-based, **SE attacks**
- Target’s hunting runs by dialing possible subscribers from the phone book
- Social Engineering **side actions**: some “gifted” hardware can help out;)



Arnhild Bue, Røssv. 40 μ 4640
– Arvid, Løvsangerv. 9 μ 4626
– Arvid, disp. Tverrv. 19 μ 4620
– Asbjørn, Gunhildsv 149 μ 4620
– Aslaug, Haumyrv. 40
– Astrid





COMUNE DI Bondeno

Piazza G. Garibaldi, 1

CENTRALINO 0532 899 211

INTERNET www.comune.bondeno.fe.it

UFFICIO RELAZIONI CON IL PUBBLICO	
Numero Verde	800-219985
Telefono	0532 899 211
Fax	0532 899 280
POLIZIA MUNICIPALE	
Telefono	0532 899 300
Fax	0532 899 330
Protezione Civile - Telefono	0532 899 254
SEGRETERIA DEL SINDACO/ASSESSORI	
Telefono	0532 899 216
Fax	0532 899 460
UFFICI SEGRETERIA	
Organi Istituzionali	0532 899 206
Protocollo/Archivio	
Telefono	0532 899 237 - Fax 0532 899 270
UFFICI DEMOGRAFICI	
Anagrafe	0532 899 219
Stato Civile	0532 899 202
Elettorale/Leva	0532 899 246
UFFICI FINANZIARI - COMMERCIO	
Ragioneria	0532 899 244/276/250
Tributi/Pubblicità/Affissioni	0532 899 231/222
Attività Produttive Commercio	0532 899 312
Economato	0532 899 253/252
Personale	0532 899 214/207
Paghe	0532 899 213/249

SPORTELLO UNICO ATTIVITA' PRODUTTIVE	
Telefono	0532 899 242/264
Fax	0532 899 450
SPORTELLO UNICO EDILIZIA	
Telefono	0532 899 226/241
Fax	0532 899 450
UFFICI SOCIO - CULTURALI	
Servizi Sociali	0532 899 500
Fax	0532 899 559
Cultura	0532 899 258
Promozione del Territorio	0532 899 245
Scuola/Sport	0532 899 205
UFFICI TECNICI	
Urbanistica e Territorio	0532 899 208/286
Progettazione Opere Pubbliche	0532 899 225
Direzione Lavori Pubblici	0532 899 209
Attività manutentive	0532 899 223
Segreteria Tecnica	0532 899 220/221
Ambiente	0532 899 242
UFFICI E SERVIZI VARI	
Vigili del Fuoco Volontari	0532 894 850
Centro Insieme	0532 898 218
Polo Socio Sanitario	0532 898 101
Asilo Nido	0532 898 226
Centro Sportivo Bihac	0532 892 029
Biblioteca Comunale	0532 899 290
Pinacoteca Civica	0532 899 255
Rocca Possente	0532 885 470

* 1989

- The amount of Videotel CPs grows up: easy money is sexy to many guys.
- “unethical” empreneurs, organized crime (Mafia, Camorra) lacking of technical know-how, acquires it “on the market”
    - ...just like it happened decades later with ISPs, and today within IT Security...
    - And with Cybercrime.
- Not such a cool memory to think about ☹

* 1989

- “Someone” discovers a gateway between Italian Videotel and French Minitel
  - The French market is less interesting, tough: the billing is per use and not per time
- First, slow, shy contacts among Videotel and Minitel CPs

* 1989

- Remember those 450 Mhz “light” phones?
- They get cracked this year!
  - No Authentication, no Encryption
  - A “security-free” technology
  - Everything you need is a clip (!)
  - Free National calls, while walking (coooolll!)
  - Crazy ppl started wardialing the WHOLE country, hunting for modem handshakes (LOL)

* 1990

- SIP starts selling “phone credit cards”, just like AT&T, MCI, Sprint and GTE they sell in the USA
- A new, cool resource for a lot of phone frauds
- Telcos used to create weak algorythms for these calling cards: was this done intentionally?
- Do they still do it? Is this intentional?
- Think about Premium Numbers-based frauds…still today within GSM and 3G (oh well…PSTN as well!)
- I’d like a small debate in the room…. But no time! ☹

* 1991

- Blue Boxes spread around:
  - Amiga environment (Agnus, Denise and Paula ruled :)
  - PC environment (the lame Creative Sound Blaster)
- (ab)Use of different “service numbers” as “diverters”
  - Hint: **read the book** “Exploding the Phone”, 2013

* 1991

- Procedural “bugs” from our national telco = Fake phone lines
  - How to obtain a phone line and calling cards at your own place, while not paying for that + risk-free ☺

* 1991

- Mr. White needs a modem (the GREAT Us Robotics Courier): ahead of “creative financing”, “creative carding” popped up
- “Fake address” management (aka “the dropping place”)

* 1991

- A full year of carding towards the very first Italian Pay TV (Tele+, then acquired by SKY)
  - NOTE: a few years later, I hacked Tele+ via a PSTN dialup (02/xxxxxxxxx) which brought you in directly into the Pay TV LAN (!)
  - I become a “VIP” customer ☺

* 1991

- The excessive abuse of Videotel’s passwords leads to a full degeneration of the whole system
- The phone company realizes huge financial losses, and stop paying the CPs
- CPs sue in tribunal the Phone Company (LOL)
- It’s time for a new fraud playground… hmmmm??

* 1992

- The E-TACS network is now a National one.
- Its own “security” relays on two factors: the subscriber’s phone number and the serial number of the mobile device (WOW)
- E-TACS network starts giving out satisfactiosn to phreakers: mobile phones can be cloned and eavesdropped
  - Once again, Private Investigators do appreciate the nice mix between technologies and digital underground (ops… “analog” underground ;)

* 1992

- How to obtain the “Serial # / Phone #” match?
- Good eye spotting, social engineering or…. Your own E-TACS tower cell!
  - Highway Milan-Venice: 2 yrs of collection
- Motorola-based phone calls eavesdropping
- NEC P3 keypad-programmable + remote bug (“who do you want to listen to, today?”)
  - NOTE: that’s why Kevin Mitnick was hacking into OKI and Motorola: in order to get the source code, modify it, and being able to reprogram & clone mobile phones

SND
END
PWR
STO
CLR
RCL
FCN
NEC

TELECOM
NEC

* 1993

- Videotel is not anymore a revenue source, the phone company is not paying CPs and wins court trials

- Many CPs do not get their own money (even the lawful ones!), get into debts with the banking system, and shutdown

* 1993

- In the meanwhile, many phone companies are limiting the damages caused by blue-boxing
- It’s not possible anymore to call internationally, but only local calls
  - i.e. inside USA, Brazil, Taiwan, Uruguay, etc..
  - NOTE: btw, blue-boxing still works: try to call from a PSTN line a phone number i.e. in Africa, and send the 2600Hz break….it works! ☺

* 1993

- Because of this, the (ab)use of calling cards gets a rise:90% USA cards, then Italian Calling Cards
- Very often, US phone companies were using as the Card number:
    - Subscriber’s PSTN number (home/office phone line #) + a security PIN (4 to 10 digits)

* 1993

- Many “Social Engineering operators” make agreeme nts with French Minitel CPs, running “service reselling” contracts
- Abuse of the Videotel-Minitel gateway

* 1993

- The Videotel-Minitel gateway closes up, ‘cause of issues with payments between Italy and France (guess why??)
- A workaround is needed, in order to keep the illegal business alive: how?

* 1993

- Someone discovers a second gateway, between the Finnish Videotel and the French Minitel!
- But… how to reach that gateway?

* 1993

The solution

- Blueboxing towards USA, calling a Calling Cards responder (PBX)
- (ab)use of a CC in order to call Finland via USA
- Jumping from Finland to France throught the gateway

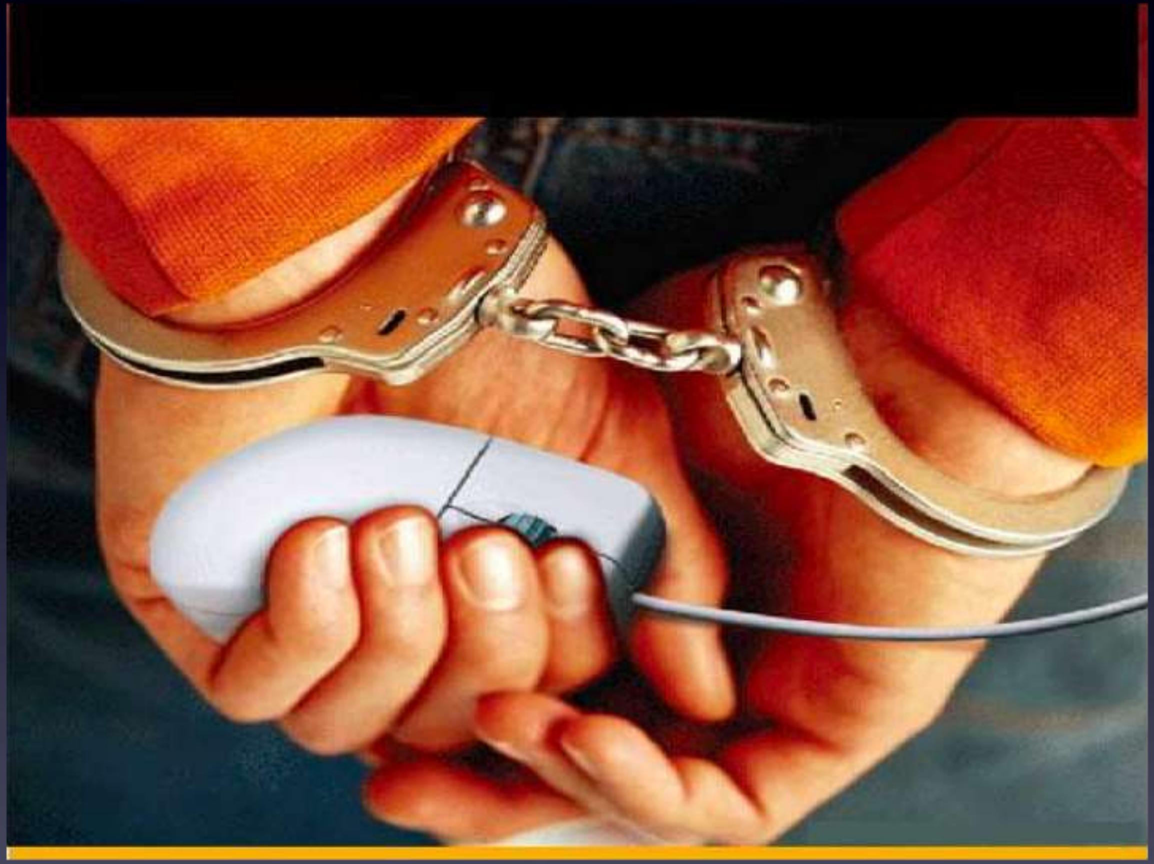
* 1993

The result

- Return of investement from the French CPs, proportionally to the use time of the services VS their cost per minute
- In the meanwhile, in Italy…

* 1993

- The very first Italian Crackdown (a good mix of X.25 hackers + Videotel abusers)
- Wargames makes its 10th birthday :)



* 1994

The Game goes Over....

- Videotel is vanishing: now it’s a ghost network
- Automatic blocking of international calls from cellulars
- Automatic blocking of international calls from CCs towards “weird countries”

* 1994

- Mass-internet appears with “Video On Line” (VOL)
- A real, true generational change!!
- I had *root* on vol.it ;)

* 1994

- The FBI highlights high-level break-ins on private companies and telcos
- The SCO (Central Operative Section) of Italian Police Special Corps gets involved
  - They are the guys who arrested the Capo dei Capi Mr. Totò Riina (Chief of the Sicilian Mafia)

* 1995

- SCO investigations
- “ICE TRAP”, the very first anti-hackers operation in Italy
- I was the key actor in this ☺
- Because of this, Italian policy-makers they wrote the laws against hacking, which didn’t exist earlier (615, 617, 618 etc CPP)

* 1995/12

- From here on, we’re not specifically updated (well..a kind of ;)
  - Next time, we’de loike to bring you the Rel 2.0: 1996->2008
  - That’s all folks !

* 1995/12

YOU GUYS will tell the rest of the story…. ;)

21th Century Phreaking

(a short intro)

Raoul “Nobody” Chiesa

Yesterday: attacks & frauds

- PSTN old school
- Wardialing, National and International Toll-free numbers
- Blue-Boxing
- Public phones
- Calling Cards Carte telefoniche (Social) *
- PBXs
- 450 Mhz
- E-TACS/AMPS

Yesterday: phreaking & IT

- **ISDN-trace** on Linux: how to find the real PSTN phone number instead of the IN (Intelligence Network) alias
- **SMSC Data Call** (flood, spoofing)
- **GSM A1/A5** Cracking
- The ***Passion for Telcos*** ™ aka "*phreaking loves hacking*"

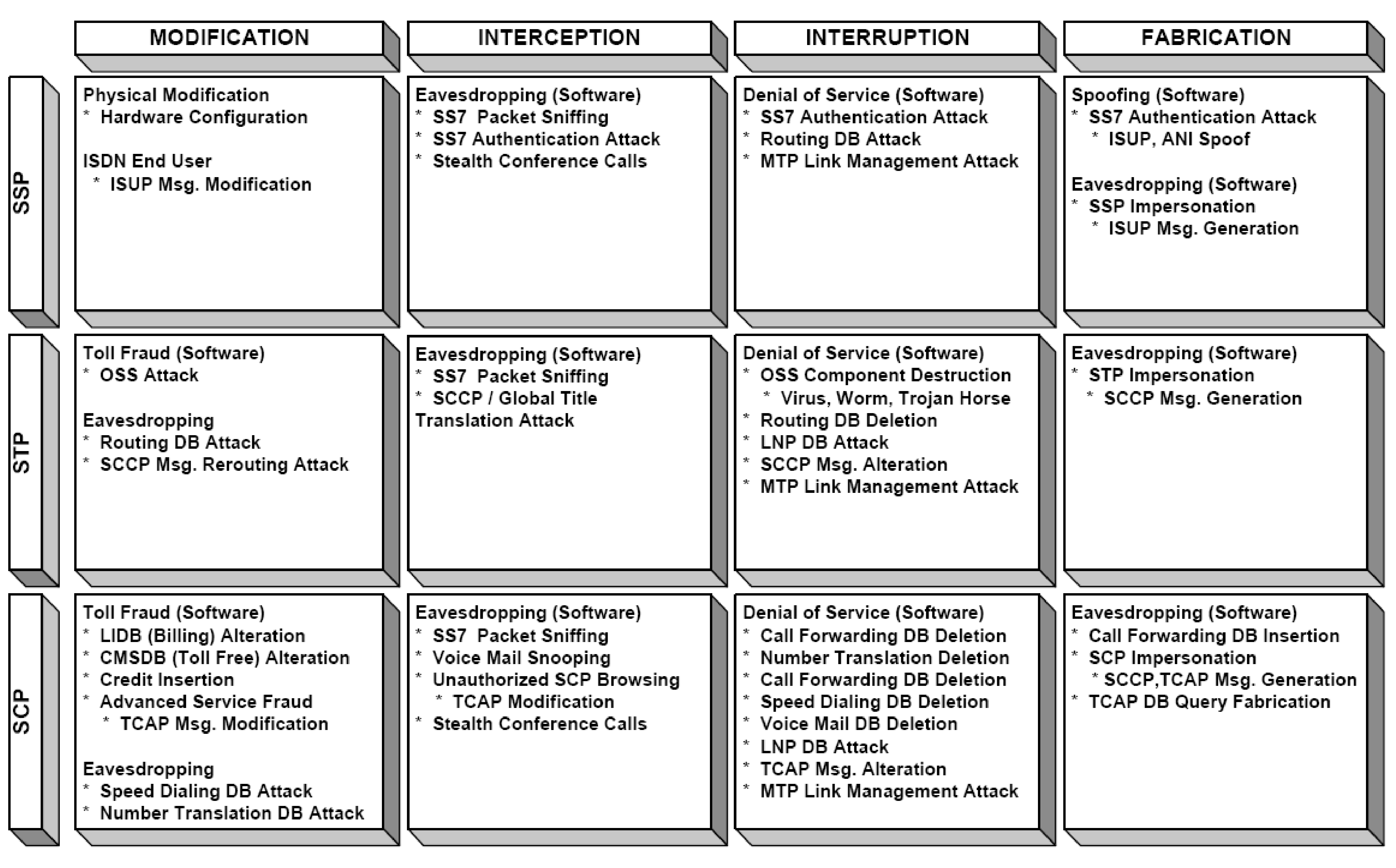
TODAY:
the malicious vision

- The phone network as a **network for malicious economical transactions**
- A different approach:
  - Highly-complex ecosystem, and open (messy, abusable, funny because of its “complex chaos”)
  - Complexity of phone technologies: closed & open
  - Communicatyion media’s pervasivity + crossing
  - Rise up of risk’s exposure
- Different actors (and motivations)
  - Telephone phreaking: phreakers in the 21st century
  - Phone fraud: not anymore a low-level crime, while «we» are still there.
  - Exponential rise up of speculative activities, cross-border with legality

Attacks & Frauds

- VoIP
  - End-users (VoIP subscribers)
  - Router Attacks
  - WISPs
  - Fuzzying
- Mobile Hacking
  - 3G phones
  - SS7 (see next)
  - GSM standard abuse (i.e. PDU), SMS Scam

SS7 – Attack 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

From traffic to cash-out

- premium numbers
- SMS frauds (mobile decade #4)
- «Complex» fraud frameworks (see next)

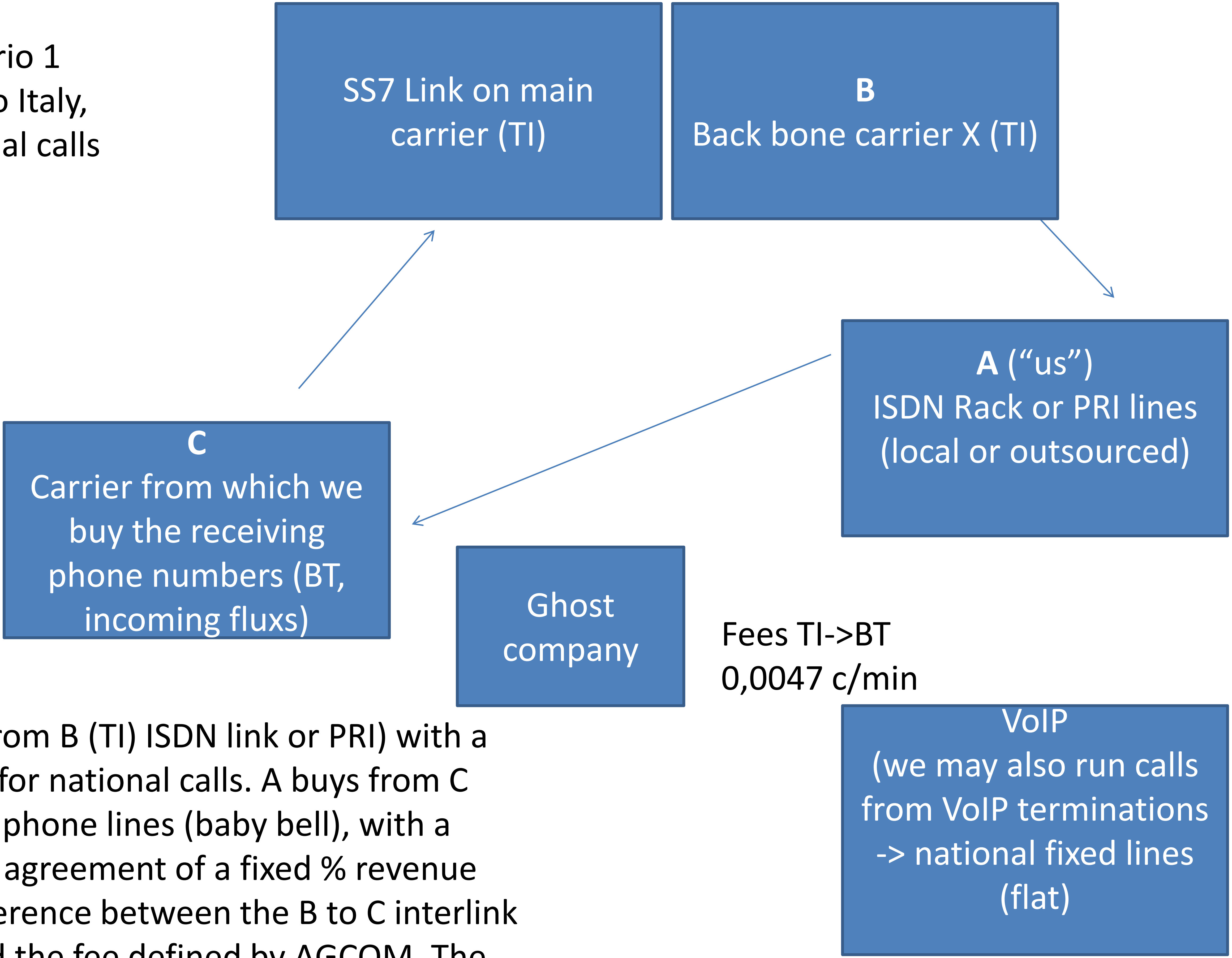
Phone termination fees

(being an operator brings you advantages)

- Speculative’s operators (MVMO)
- International Premium Numbers
- Dirty SMS and MMS termination fee provider
- Traffic generation
- Phone fees «holes»
- Dialers

“Reverse calls” business: a basic layout

Scenario 1
Italy to Italy,
national calls



SS7 Link on main carrier (TI)

B
Back bone carrier X (TI)

A (“us”)
ISDN Rack or PRI lines (local or outsourced)

C
Carrier from which we buy the receiving phone numbers (BT, incoming fluxs)

Ghost company

Fees TI->BT
0,0047 c/min

VoIP
(we may also run calls from VoIP terminations -> national fixed lines (flat)

A buys from B (TI) ISDN link or PRI) with a flat rate for national calls. A buys from C national phone lines (baby bell), with a contract agreement of a fixed % revenue (the difference between the B to C interlink cost, and the fee defined by AGCOM. The result is our business.

MOBILE HACKING

Mobile Hacking

- Marriage between hacking and phreaking ? :)
- OTA attacks towards handset’s DNS (mseclab public research)
- SMS Fuzzying

- Operating Systems and Mobile Environments
- OTA attacks (Job De Haas)
- SMS Fuzzying on Android/iPhone

FRAUDs

Frauding, today

- Premium numbers frauds & co:
  - Telecom Box at the corner (old skool)
  - SIM pre-paid frauds
  - Company’s PBXs (ISP; VMBs Attack)
  - Malware on browser
- WISP Frauds:
  - Hacking Linux Exposed, ISECOM Edition (chap. VoIP by Raptor)

CIAO!