ConfidEncE

Confidence 2007, CRACOW

X.25 (in)security in 2007: having phun with it

Real life and field-experiences on a really underestimated and still actual security issue

May 12th and 13th 2007 | Cracow, Poland

Raoul “Nobody” Chiesa

@ Mediaservice.net Srl
Founder,
Technical Director

TELECOM SECURITY TASK FORCE (TSTF)
Associated Partner,
Europe Manager

DISCLAIMER

- We **do not recommend** that you use this material for unauthorised access to telecommunications operators', private companies' or governments' infrastructures and/or systems.
- We cannot be held responsible if you decide nevertheless to explore such networks and systems, find them **fascinating**, start getting **sloppy** and leave **tracks** that finally gets you **busted**.
- The X.25 addresses used in the slides can be **sometimes real and sometimes fake**: in the first case they could be out-of-date, else they're still existing and they've been used for **clear example purposes**.
- In any case, the real X.25 addresses mentioned as evidences have been taken from **public or private (personal) sources** and their publication does not mean in any case an invitation to attack or test the connected systems.
- Quoted trademarks belongs to registered owners.
- 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 **known European laws**, including Poland ones**.**

AGENDA

- Intro
- Basic know-how
- Advanced know-how
- Highlights
- Funny tales
- X.25 Hacking
- Tools
- A look at the future
- End

INTRO

[The Speaker]

[The Company]

[TSTF]

[This Talk]

[Why are we talking about X.25 security in 2006 ?]

THE SPEAKER

- Raoul “Nobody” Chiesa
- Board of Director’s Member for CLUSIT (Italian Computer Security Association, ITALY), ISECOM (Institute for Security an Open Methodologies, USA/EU), OWASP Italian Chapter (Open Web Application Security Project, USA), TSTF (Telecom Security Task Force: Asia, EU, USA, Australia).
- OSSTMM Key Contributor (2.0, 2.1, 3.0)
- ISECOM international trainer
- HPP (Hacker’s Profiling Project) Manager @ ISECOM
- X.25 hacker, when it wasn’t “a crime”
- Working on X.25 networks since 1986 (20 years)
- Nowadays, Raoul is just a security professional, loving his job

The Company

- @ Mediaservice.net Srl
- A vendor-neutral, independent security consulting company, established in 1997
- Internal Tiger Team since 1999 (+15 ppl, fully ISECOM Certified)
- Penetration tests, Computer Forensics, customized consulting, telco specialized
- +800 pentests & +300 computer forensics projects carried out until today
- Active research and exploiting
- Offices and labs in Turin, Trento and Rome

The Key People

- Raoul “Nobody” Chiesa (International Aspects, “the next thing” ©)
- Andrea “Pila” Ghirardini (Computer Forensics, L.E.A. consulting)
- Daniele Poma (Strategic Alliances)
- Marco “Raptor” Ivaldi (R&D Director)
- Maurizio “Inode” Agazzini (Exploit Research)

TSTF: Who is Who

- 30 years combined GSM telecommunications experience.
- 50 years combined information security experience.
- A unique view on telco security.
- Active research (papers, tools, forums).
- Experienced in Europe, Asia, USA.
- Self-funded, no business cunts running it, no VCs.

TSTF: the Key People

- Emmanuel Gadaix (Thailand)
- Philippe Langlois (France)
- Fabrice Marie (Singapore)
- Raoul “Nobody” Chiesa (Italy)
- Stavroula “Venix” Ventouri (Greece)

THIS TALK

- This talk will introduce to X.25 and detail its hacking evolution in year 2007:

  - Alive & died operators
  - Interesting countries
  - Customer's users typology
  - X.25 exploiting
  - Field experiences
  - Funny tales
  - The next thing...

WHY ARE WE TALKING ABOUT X.25 SECURITY IN 2006 ?

- [We hang on X.25 since 1990.]
- This speech is oriented towards network security while **working in X.25 worldwide environments** and its legal working framework.
- The information contained is based on personal, company's and other international researchers/professionals' **penetration testing experiences** and field observations.
- During the 90's we encountered a **huge number** of breaches on tested infrastructures, usually getting access via the main X.25 link. More than 90% of them was insecure.
- We kept on finding **open doors** while pentesting companies with X.25 leased lines (1996->2007); these doors always brought the Tiger Team to the **core of the target network**.
- New connections and new services that lay on X.25 communications **still get launched**, also when if you don't know it or even think of.
- We are now in year **2007**, and hacking "news" are still upcoming.

BASIC KNOW-HOW

[What's this ? How it works]

[X.25 in ISO/OSI]

[User Facilities]

“ X.25 is used in a Packet Switched Network and in 1964 was designed by Paul Baran of the RAND Corporation for use with the Public Data Network (PDN) and unreliable analog telephone services.

The idea was to connect a dumb terminal to a packet-switched network.

In 1976 X.25 became a standard under the CCITT, now the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T).”

INTRODUCTION: WHAT'S THIS ?

- An International **P**acket **S**witched **D**ata **N**etwork (PSDN).
- A model **very similar** to Public Switched Telephone Networks (PSTN).
- 3 main packet type:
  - **Data**
  - **Control**
  - **Facilities**.
- **International standards** (X.25/X.29, X.28, X.75, X.121) created by ITU (International Telecommunications Union, Switzerland) in the 70's.
- **First commercial global data network.** Widely used 'cause it was the only applicable choice (Internet was only available for the academics and the government's employees) from 70's to 80's; in the '90 many commercial companies went to the Internet, **but they kept their X.25 access** and contracts (that, usually, are still active, even if they forgot about it!).
- X.25 networks owned both by national telcos (**mainly**) and private operators.
- Weird customers….

INTRODUCTION: HOW DOES IT WORK ?

- Each subscriber has an **international X.25 address** (N.U.A., Network User Address) assigned to a **leased line**, with one or more **logical channles**.
- Subscriber A can call Subscriber B in order to establish a **switched virtual circuit** (SVC) call or a **permanent virtual circuit** (PVC).

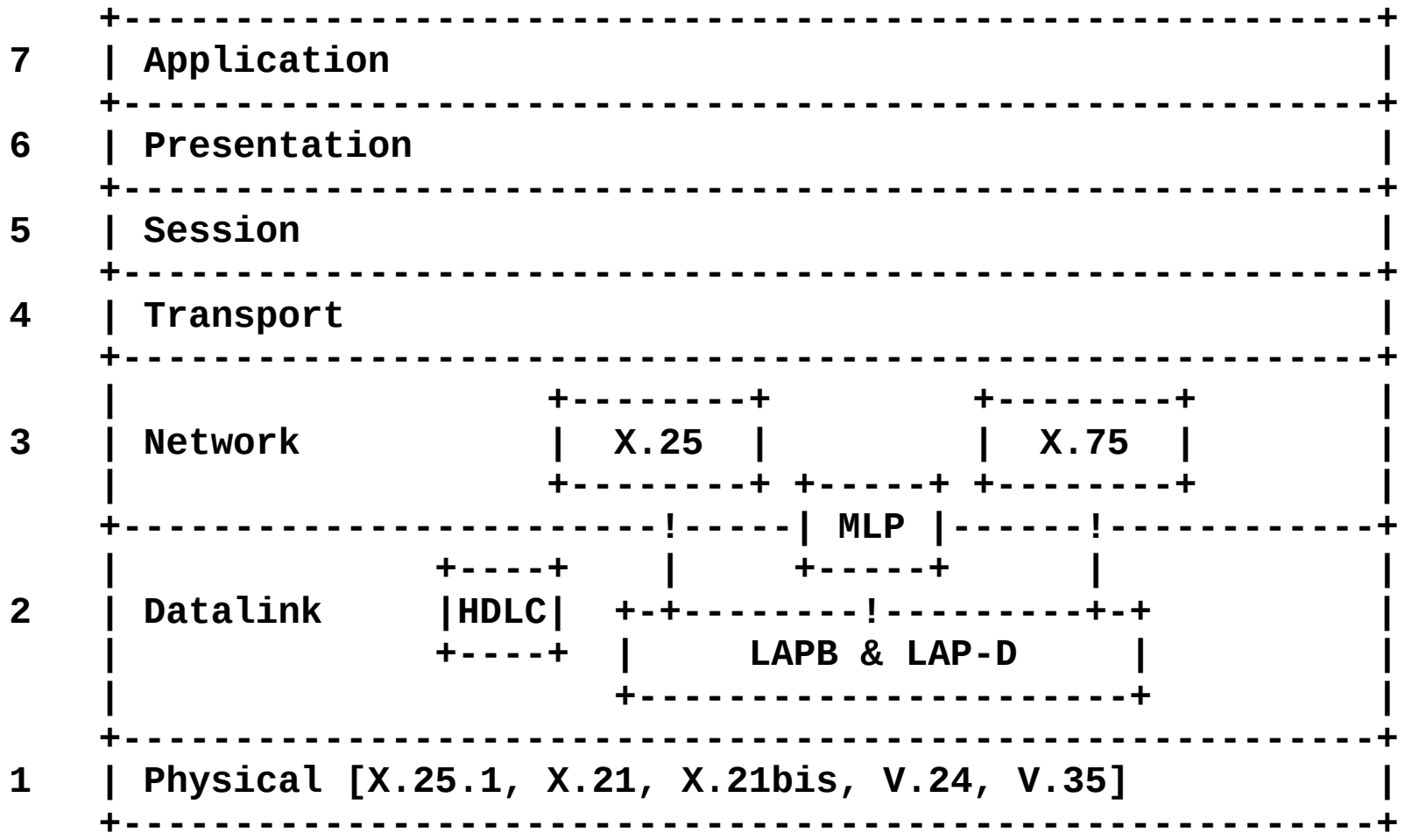
- **Only the traffic is billed**, and customers don't pay the "connection-time".

- Both on SVCs and PVCs links is possible to talk over **many different protocols** (TCP/IP, host-to-host, SNA, proprietary, voice, Kermit....).

- X.3 PAD capabilities are implemented in **major OS**:

✓ all *NIX flavours
✓ Cisco IOS
✓ DEC VAX & HP AXP VMS/OpenVMS
✓ AS400 (OS400)
✓ old stuff, just Wargames (the movie) like
✓ strange or unknown systems (so many !!)

X.25 IN ISO/OSI



X.25 IN ISO/OSI (Datalink Layer and Network Layer)

⌘ **The Datalink Layer** (X25.1)

a) LAPB (Link Access Protocol Balanced)
b) LAP-D (Link Access Protocol for D-channel)
c) LAP-M (Link Access Protocol for Modems)
d) MLP (Multi-Link Procedure)
e) LLC (Logical Link Control)

⌘ **The Network Layer** (X25.2)

a) PLP (X.25 Packet Layer Protocol)
   - Multiplexing of VCs on PSDN
   - VCs Switching/Routing between WAN's nodes
b) PVC (Permanent Virtual Circuit) e SVC (Switched Virtual Circuit)
c) VCI (Virtual Channel Identifier)
d) Call Setup
e) X.121 and LCN
   X.121: ITU recommendations (international data links)
   LCN: Routing (basing on X.121 specs); **subaddressing** functions.

X.25 IN ISO/OSI: Higher Layers (Focus on X.25 Users Facilities)

- User Facilities are defined by **ITU recommendations**
- Each carrier implements **different, customized** User Facilities
- **X.25 User Facilities:**
  - **Network User Identification**

The NUI is never sent to remote node: it is verified on local PSDN switches (ACPs). NUI format **is different** from network to network.

- **ROA selection**

This function lets control the call routing: it recalls back the loose source routing in the IP world.

- **Call redirection**

As in PSTN world, it's possible to have **certain calls** redirect to other DTEs.

- **Hunt Group**

Again another analogy with PSTN and PBXs world: a load balancing is possible for incoming calls.

- **Mnemonic codes**

Some X.25 networks let the subscribers choose alphanumeric mnemonic codes, that are assigned to the real NUA. This makes easy the dialup connections via ACP (X.28 PAD).

ADVANCED KNOW-HOW

[Getting an X.25 access]

[NUA Addressing & DNICs]

[Scanning Examples]

[Penetration Testing Logical Flow]

HOW DO I ACCESS TO IT ? (1/2)

- TONS of X.25 assigned networks worldwide (all the countries of the globe).
- +100 of them are still active and in use.
- Worldwide: SprintNet/MCI (formerly aka Telenet), SITA (airports)
- The big ones: BT Tymnet, At&t/Accunet, Datex-P, C&W, ...
- The “pac” ones: Itapac, Transpac, Iberpac, Austpac, Datapac, PolPak...
- The “net” ones: Isranet, Pacnet, Rosnet, ...

- Outdials, CCs, PBXs or VoIP stuff are often used to call X.28 PADs.

→ **NOTE:** The backtracing investigation technique won’t so be easily applicable (or **nearly not applicable**);

→ **NOTE:** You can use NUIs **from other countries** (phreaking and social engineering can help definitely a lot here).

HOW DO I ACCESS TO IT ? (2/2)

Many ways to access to X.25 networks, legally and not:

- Direct connection to a X.25 network from an X.25 leased line;
- X.28 PAD via Dialup using a NUI;
- X.28 PAD via toll-free Dialup, with or w/o NUI (national's and international carrier's on 800 #s);
- "Official" Internet -> X.25 Gateways (PADs); (x25pad.ja.net, x25pad.autonet.net)
- (Hacked) Systems linked both to the Internet and to a X.25 network – directly and/or via LAN/WAN;
- X.25 over ISDN D Channel (X.25D; X.28D);
- X.25 over TCP – XoT (RFC1613).

X.25 ADDRESSING (1/2)

- X.25 hosts are **identified by**:
  - **NUA**s: one system can have multiple assigned NUAs or linked on more networks with same NUA and different DNIC (SprintNet->WW Partners)
  - ...but you may also find more systems linked to a single NUA (subaddressing)
  - **Mnemonics**: only on some public network – eg Tymnet, SprintNet, Autonet
  - ...think of 031069 Tymnet-gw - and of private X.25 networks.

→ **NOTE: X.25 addresses are reserved** and should not be disclosed

X.25 ADDRESSING (2/2)

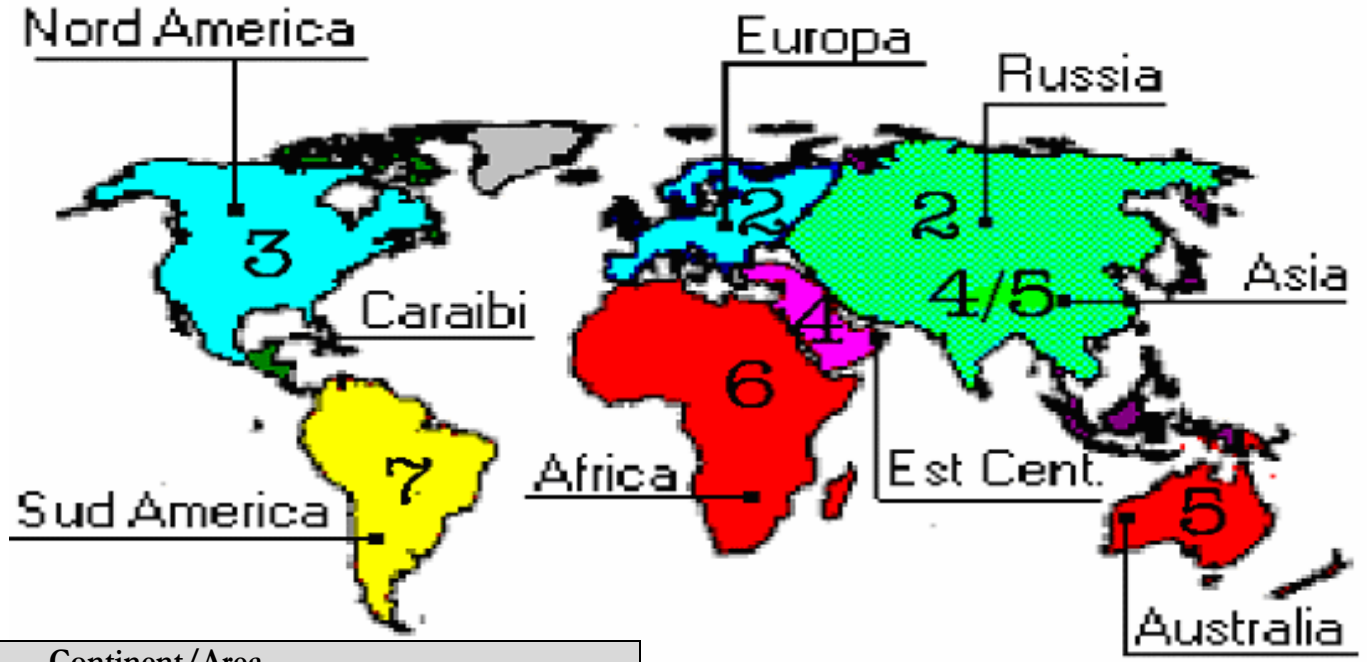
- X.121 address: **DNIC + NUA** = 15 digits max.
  - DNIC: **4 digits** international code: DCC + NCC
  - DNIC= DCC+NC
  - DCC assigned on a geographical basis by ITU (world's areas)
  - NC= Network Code (X.25 operators)

- NUA: **12 digits max** (typically 6->10). In many networks they have a structure derived from the PSTN numbering planning (area codes referred to towns/areas of the country)

- Example: DNIC (4) AC(3) NPA(5)

→	**3110**	**212**	**10126**	**(USA, Sprintnet, NYC)**
→	**2802**	**21**	**229**	**(Cyprus, Limassol)**
→	**2624**	**30**	**xxx-yyyy**	**(Datex-p, Germany, Berlin)**

DNIC WORLD AREAS



Zone	Continent/Area
1	Satellite connections for InmarSAT Voice/Dati(Atlantic, Pacific and Indian oceans)
2	Europe, Ex URSS
3	North America, Central America, some Carribean areas
4	Asia
5	Oceania
6	Africa
7	Part of Central America, Carribean and South America

Annex to ITU Operational Bulletin
No. 798 – 15.X.2003

INTERNATIONAL TELECOMMUNICATION UNION

TSB
TELECOMMUNICATION
STANDARDIZATION BUREAU
OF ITU

LIST OF DATA NETWORK IDENTIFICATION CODES (DNIC)
(According to ITU-T Recommendation X.121)

(POSITION ON 15 OCTOBER 2003)

Geneva, 2003

DNIC/1

INDONESIA
INDONESIA.Annex to ITU OB 714-E – 11 – 15.04.2000
INMARSAT (OCEANI)
INMARSAT 111 1 Atlantic Ocean-East
111 2 Pacific Ocean
111 3 Indian Ocean
111 4 Atlantic Ocean-West
IRAN
IRAN (REPUBLIQUE ISLAMIQUE D') 432 1 IranPac
IRLANDA
IRLANDE 272 1 International Packet Switched Service
IRELAND 272 3 EURONET
IRLANDA 272 4 EIRPAC (Packet Switched Data Networks)
272 8 PostNET (PostGEM Packet Switched Data Network)
ISLANDA/ICELAND
ISLANDE 274 0 ISPAK/ICEPAC
ISRAELE
ISRAEL 425 1 ISRANET
ITALIA
ITALIE 222 1 Rete Telex-Dati (Amministrazione P.T. / national)
ITALY 222 2 ITAPAC X.25
ITALIA 222 3 PAN (Packet Network)
222 6 ITAPAC - X.32 PSTN, X.28, D channel
222 7 ITAPAC International
223 3 ALBADATA X.25
223 4 Trasmissione dati a commutazione di pacchetto X.25 (UNISOURCE ITALIA S.p.A.)
223 5 Trasmissione dati a commutazione di pacchetto X.25 (INFOSTRADA S.p.A.)
223 6 Trasmissione dati a commutazione di pacchetto X.25 (WIND Telecomunicazioni S.p.A.)
JAPAN/GIAPPONE
JAPON 440 0 GLOBALNET (Network of the Global VAN Japan Incorporation)
JAPAN 440 1 DDX-P (NTT Communications Corporation)
JAPON 440 2 NEC-NET (NEC Corporation)
440 3 JENSNET (JENS Corporation)
440 4 JAIS-NET (Japan Research Institute Ltd.)
440 5 NCC-VAN (NRI Co., Ltd.)
440 6 TYMNET-JAPAN (JAPAN TELECOM COMMUNICATIONS SERVICES CO., LTD.)
440 7 International High Speed Switched Data Transmission Network (KDD)
440 8 International Packet Switched Data Transmission Network (KDD)
441 2 Sprintnet (Global One Communications, INC.)
441 3 KYODO NET (UNITED NET Corp)
441 5 FENICS (FUJITSU LIMITED)
441 6 HINET (HITACHI Information Network, Ltd.)
441 7 TIS-Net (TOYO Information Systems Co., Ltd.)
441 8 TG-VAN (TOSHIBA Corporation)
JAPON 442 0 Pana-Net (MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD.)
JAPAN 442 1 DDX-P (NTT Communications Corporation)
JAPON 442 2 CTC-P (CHUBU TELECOMMUNICATIONS CO., INC.)

Each country has got at least one X.25 network... or more than one.

DNIC/2: THE AUSTRALIA CASE

Australian Network Identifiers:

Prefix	Allocation Date	Organisation
5052	30 June 1991	Telstra Corporation Ltd
5053	30 June 1991	Telstra Corporation Ltd
50541	6 September 1994	AAPT Ltd
50542	6 September 1994	AAPT Ltd
50543	6 September 1994	AAPT Ltd
50560	16 February 1994	SingCom (Australia) Pty Ltd
50568	16 February 1994	SingCom (Australia) Pty Ltd
50569	16 February 1994	SingCom (Australia) Pty Ltd
50573000	30 June 1991	Fujitsu Australia Ltd
50573500	19 February 1992	Department Of Defence
505790	17 November 1993	Department Of Defence
505791	17 November 1993	Department Of Defence
505799	23 February 1995	Telstra Corporation Ltd

Sub-carrier

Sub-carrier

Critical
(and shared !)

5052 = Austpac
5053 = Austpac International (formerly Midas / OTC Data Access)
5054 = Australian Teletex Network
5057 = Australian Private Networks

NB The allocation dates are official allocation dates, not necessarily actual dates. Austpac existed long before 1991.

313 1	RCAG Telex Network
313 2	Compuserve Network Services
313 3	RCAG XNET Service
313 4	AT+T/ACCUNET Packet Switched Capability
313 5	ALASCOM/ALASKANET Service
313 6	Geisco Data Network
313 7	International Information Network Services - INFONET Service
313 8	Fedex International Transmission Corporation - International Document Transmission Service
313 9	KDD America, Inc. – Public Data Network
314 0	Southern New England Telephone Company - Public Packet Network
314 1	Bell Atlantic Telephone Companies - Advance Service
314 2	Bellsouth Corporation - Pulselink Servie
314 3	Ameritech Operating Companies - Public Packet Data Networks
314 4	Nynex Telephone Companies - Nyex Infopath Service
314 5	Pacific Telesis Public Packet Switching Service
314 6	Southwestern Bell Telephone Co. - Microlink II Public Packet Switching Service
314 7	U.S. West, Inc. - Public Packet Switching Service
314 8	United States Telephone Association - to be shared by local exchange telephone companies
314 9	Cable & Wireless Communications, Inc. - Public Data Network
315 0	Globenet, Inc. - Globenet Network Packet Switching Service
315 1	Data America Corporation - Data America Network
315 2	GTE Hawaiian Telephone Company, Inc. - Public Data Network
315 3	JAIS USA-NET Public Packet Switching Service
315 4	Nomura Computer Systems America, Inc. - NCC-A VAN public packet switching service
315 5	Aeronautical Radio, Inc. - GLOBALINK
315 6	American Airlines, Inc. - AANET
315 7	COMSAT Mobile Communications - C-LINK
315 8	Schlumberger Information Network (SINET)
315 9	Westinghouse Communications - Westinghouse Packet Network
316 0	Network Users Group, Ltd. - WDI NET packet
316 1	United States Department of State, Diplomatic Telecommunications Service Black Packet Switched Data Network
316 2	Transaction Network Services, Inc. -- TNS Public Packet-switched Network
316 6	U.S. Department of Treasury Wide Area Data Network

The USA case

Data carriers & Telcos

Multinationals

Spy Game ? ;)

DNIC/4: THE ITALY CASE

ITALIE	222 1	Rete Telex-Dati (Amministrazione P.T. / national)
ITALY	222 2	ITAPAC X.25
ITALIA	222 3	PAN (Packet Network)
	222 6	ITAPAC - X.32 PSTN, X.28, D channel
	222 7	ITAPAC International
	223 3	ALBADATA X.25
	223 4	Trasmissione dati a commutazione di pacchetto X.25 (UNISOURCE ITALIA S.p.A.)
	223 5	Trasmissione dati a commutazione di pacchetto X.25 (INFOSTRADA S.p.A.)
	223 6	Trasmissione dati a commutazione di pacchetto X.25 (WIND Telecomunicazioni S.p.A.)
	223 7	Trasmissione dati a commutazione di pacchetto X.25 (Atlanet S.p.A.)

Picture source:
www.supertangas.com (ele)

DNIC/5: THE POLAND CASE

POLOGNE	260 1	POLPAK
POLAND	260 2	NASK
POLONIA	260 3	TELBANK
	260 4	POLPAK –T
	260 5	PKONET
	260 6	Shared by a number of data networks
	260 7	CUPAK

X.25 INTERNATIONAL ROUTING

- Since years x.25 routing by countries has never been reliable.

- **Not all countries can call all networks:**

  - France/Transpac is good for **scanning** Africa.
  - Italy/Itapac is good for scanning South America.
  - Germany/DatexP is good for asia-pacific scanning.

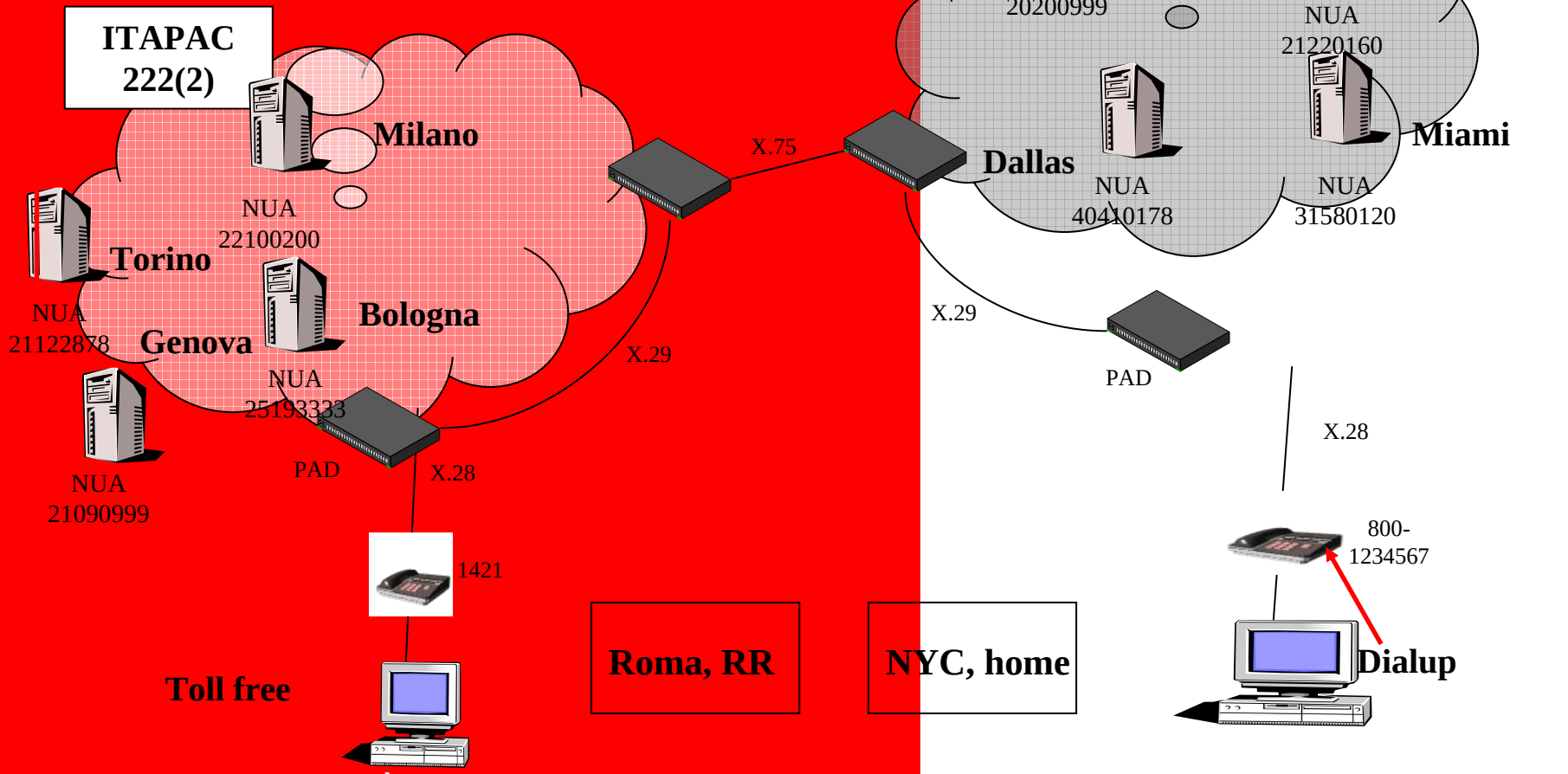
HOMEWORK

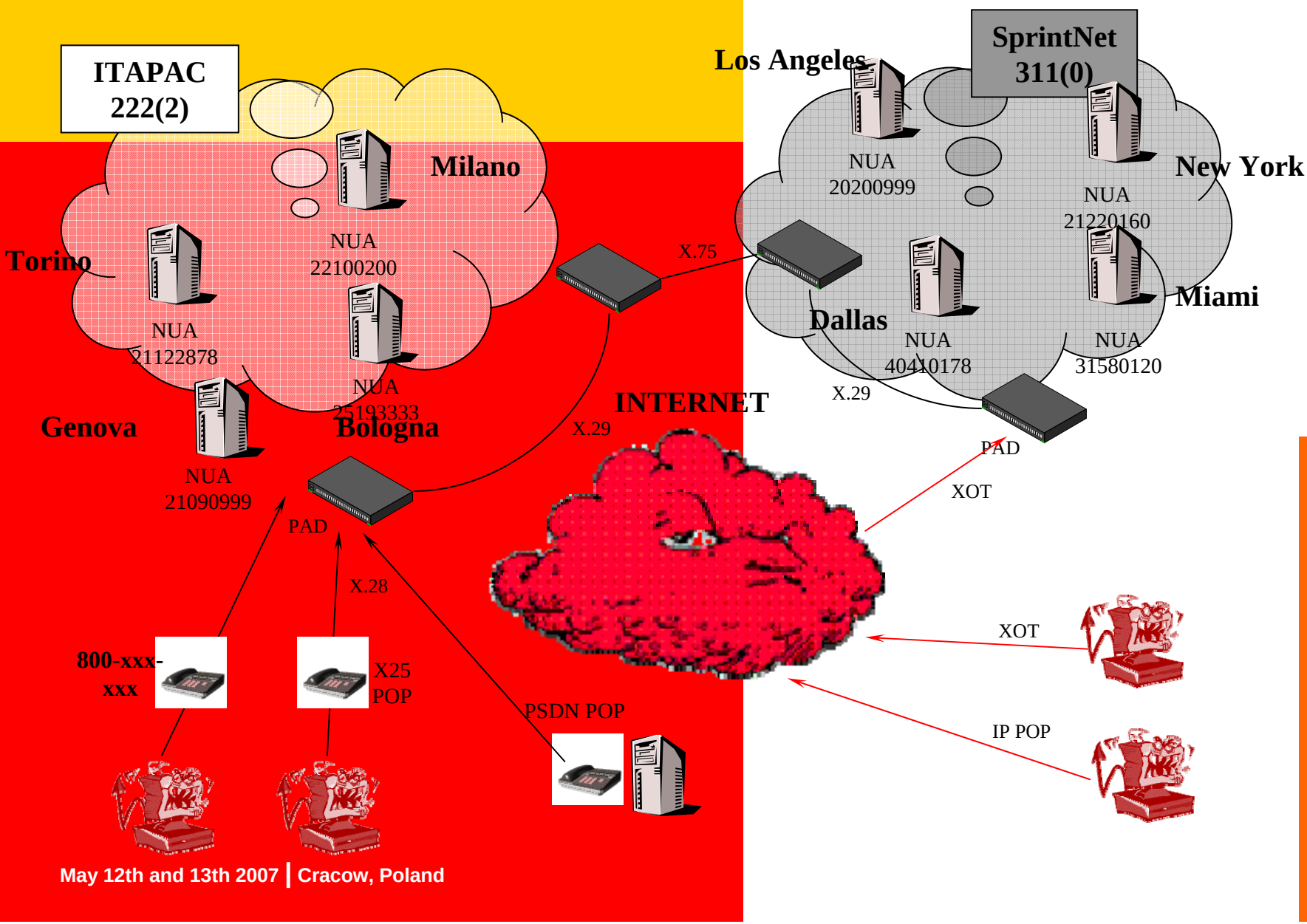
```
022221122878
|\ /|\_ _/|
| | | | | |____ 22878: Network Port Address (NPA)
| | | |_|_____  11: Area Code for Torino
| | |___________ 2: ITAPAC Network (more networks)
| |_____________ 222: DCC assigned to Italy by ITU
```

Reading it both externally and locally:

0 222 2 11 22 878 from other networks;

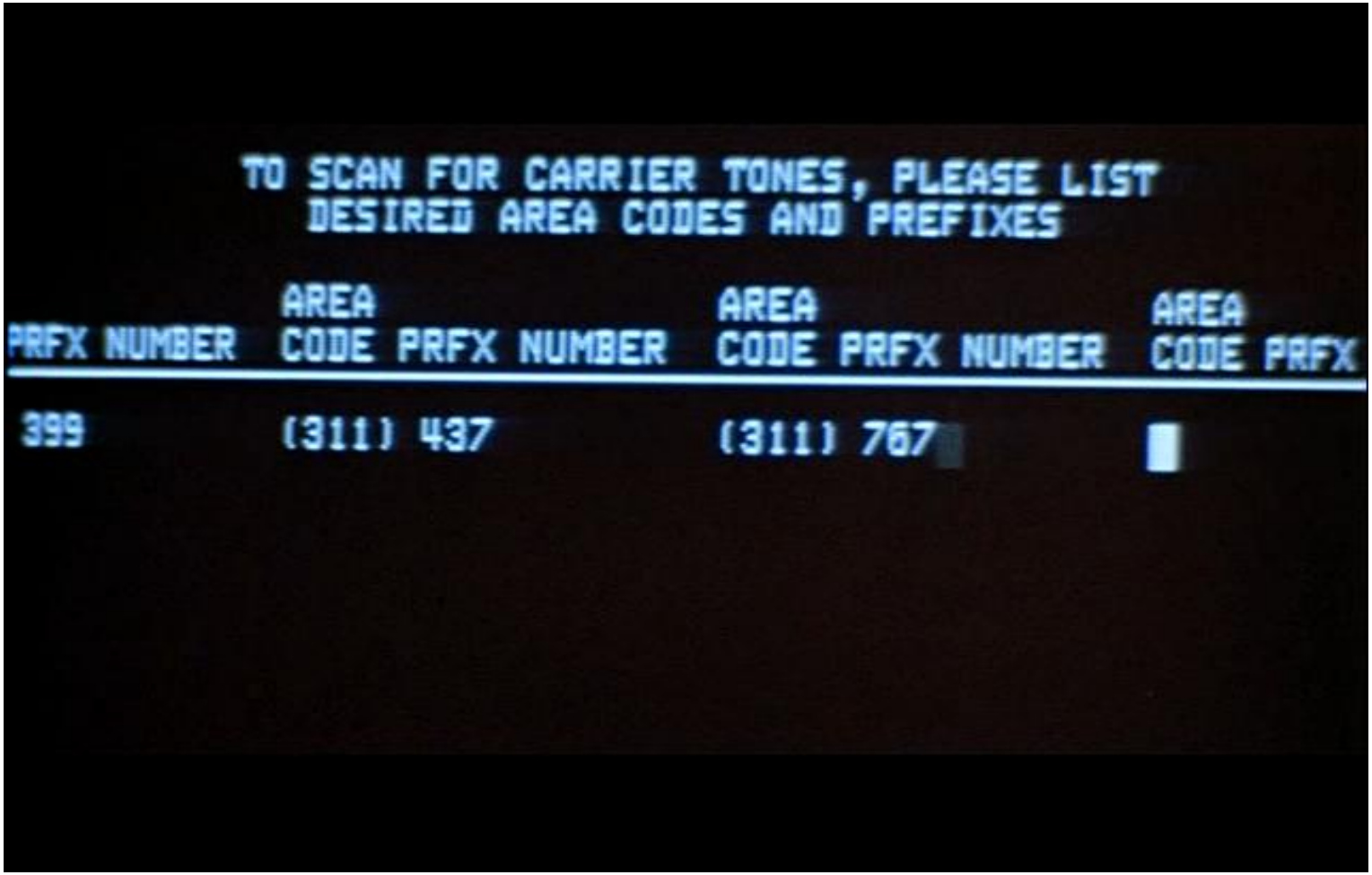
21122878 from Italy/ITAPAC.




ITAPAC
222(2)
Milano
NUA
22100200
Torino
NUA
21122878
NUA
25193333
Genova
Bologna
NUA
21090999
PAD
X.75
X.29
INTERNET
X.28
800-xxx-xxx
X25
POP
PSDN POP
Los Angeles
SprintNet
311(0)
NUA
20200999
New York
NUA
21220160
Miami
Dallas
NUA
40410178
NUA
31580120
X.29
PAD
XOT
XOT
IP POP

“WARGAMES” & SCANNING

WARDIALING…


TO SCAN FOR CARRIER TONES, PLEASE LIST
DESIRED AREA CODES AND PREFIXES
PRFX NUMBER
AREA CODE PRFX NUMBER
AREA CODE PRFX NUMBER
AREA CODE PRFX
399
(311) 437
(311) 767

X.25 WARDIALING: SCANNING FOR TARGETS 1/2 (Cyprus)

Scanning from NUA: 0280221000 started on 15-OCT-1994 15:29:30.75
0280221091 %COM **DROP STATION**
0280221092 %COM **ECHO STATION**
0280221093 %COM **TRAFFIC GENERATOR**
0280221101 %CLR_OCC
0280221102 %CLR_DTE
0280221106 %CLR_DTE
0280221107 %COM
0280221108 %CLR_DTE
0280221117 %CLR_OCC
0280221118 %CLR_DTE
0280221121 %COM **MINISTRY OF HEALT, VAX/VMS**
0280221122 %COM IBM AIX UNIX
0280221125 %CLR_DTE
0280221147 %CLR_RPE SUBADDRESS 48 CYTA Pager via x.25
0280221199 %COM CISCO
0280221206 %COM LOGON: ??
0280221225 %COM CISCO
0280221229 %COM CISCO **BYBLOS BANK S.A.L.** - LIMASSOL/CYPRUS ACS-CYPRUS LINE 6
0280221248 %COM COM/DTE
0280221273 %CLR_DTE
0280221274 %CLR_OCC
0280221276 %CLR
Scanning ended with NUA: 0280221396 on 15-OCT-2000 15:46:36.32

X.25 WARDIALING: SCANNING FOR TARGETS 2/2 (Canada)

```
- 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
```

X.25 WARDIALING: SCANNING FOR TARGETS IN POLAND ! /1

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

X.25 WARDIALING: SCANNING FOR TARGETS IN POLAND ! /2

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

X.25 WARDIALING: SCANNING FOR TARGETS IN POLAND ! /3

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

X.25 WARDIALING: SCANNING FOR TARGETS IN POLAND ! /4

CENSORED

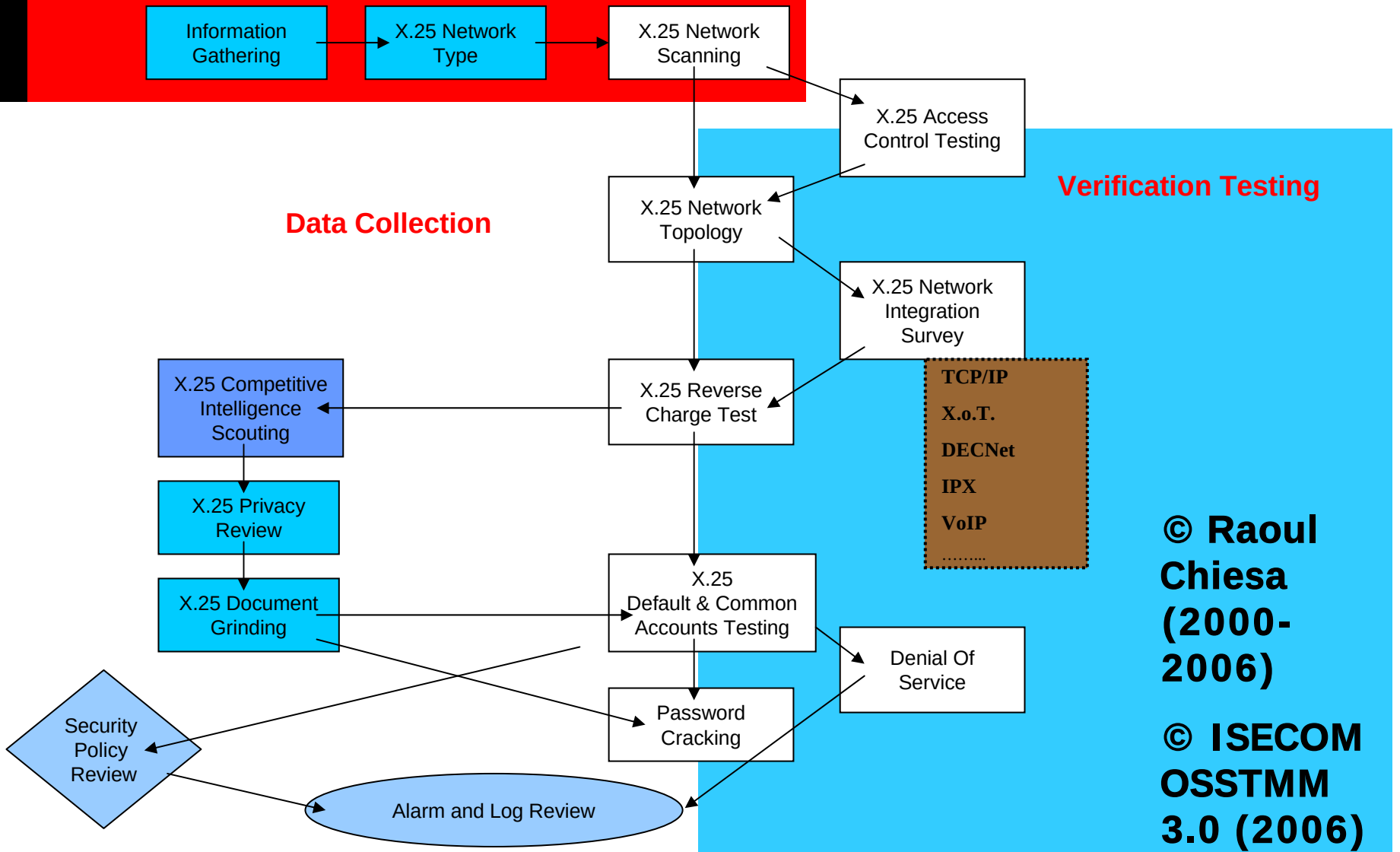
You should have joined Confidence 2007 …If you really wanted to see this slide ☺

X.25 WARDIALING: SCANNING FOR TARGETS IN POLAND ! /5

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

X.25 PENETRATION TESTING LOGICAL FLOW



HIGHLIGHTS

[Old Tales]

[Recent Tales]

[Banners & Logs]

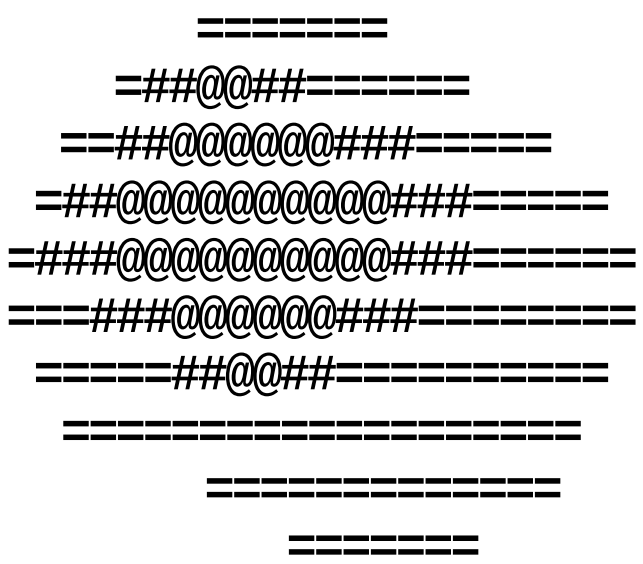
OLD TALES AND HISTORICAL (HUGE) PROBZ

- **80's**: CCC members Pengo and Hagbard breaked into US Military, Government and Gov. Contractors computer systems, calling from Datex-P and using a TymNet gateway to access LBNL Laboratories.
- **1989**: the CITIBANK's CitiSaudi scandal and the Melbourne connection.
- **15 jan 1990**: MOD & LOD hacking groups crashed the AT&T interregional and international phone system. They did (also) use X.25 links to get the final access.
- **90's**: The Aussie scene: Electron, The Force, Phoenix and the Primos scanner.
- **90's**: Kevin Mitnick got the SAS and eavesdropped on the FBI (the Russia and China NYC embassies tale).

PAST AND RECENT TALES

- **90's**: NUA scanners available for PRIMOS, VMS, *NIX, DOS, Windows.
- **90's**: Kevin Poulsen used to play with COs via X.25.
- **1994-95**: AT&T, GTE and others major US telcos got hacked via X.25 (.....)
- **Recent years**: worldwide famous group released their own scanner (**ADMx25**).
- Recent years: **Multithread** and **Multichannel** Unix X.25 scanner available in the wild: it's able to scan a whole country in a few hours.
- **2003-07**: Russian crackers perform **mass huge scans** over SprintNet international networks and dialups (intl' reverse charge scans).

BANNER'S GALLERY



```
Welcome to At&T node attmail Unix System V/386 Release 3.2B

attmail login:
```

[TLC carriers have always been targets]
(and will always be)

BANNER'S GALLERY

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

[Land Earth Station]

BANNER'S GALLERY

```
$ pad 05057998210xxxx
Connected
Trying xxx.xx.xxx.xx ... Open
    ************************************************************************
    * Access to this computer system is limited to authorised users only. *
    * Unauthorised users may be subject to prosecution under the Crimes   *
    *                        Act or State legislation                     *
    *                                                                     *
    *   Please note, ALL CUSTOMER DETAILS are confidential and must       *
    *                            not be disclosed.                        *
    ************************************************************************

User Access Verification
Username:
```

[TLC carriers have always been targets/2]

BANNER'S GALLERY

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

Satellites from Brazil

BANNER'S GALLERY

```
$ pad 0311077200704
Break-in sequence is '^Pa'

Connecting...
Connected

                                        ########
                                      ##############
                                    ##################
 ####  ##       ##           ##    ##   ###############
#    #  #        #            #    # ### ##############
#       #   ###  ####   ###   #    # ### #    ###   ###
#   ##  #  #   # #   # #   #  #    # ### # ### # ##  ##
 ##### ### ###  ####   #### ###   ##  ## ### ##  ###
 ....................................###############.......................
                                        ########
    +++                         ####                        =#\
  ...|.  Deutsche             #### France Telecom       -==#### Sprint
     |   Telecom             ####                          -#/

#=========================================================================#
#                                WARNING!!                                #
# ACCESS TO AND USE OF THIS SYSTEM IS RESTRICTED TO AUTHORIZED INDIVIDUALS! #
#         Now we are start sending your addresses to the FBI / KGB!       #
#=========================================================================#

User Access Verification

Username:
```

[TLC carriers have always been targets/3]

BANNER'S GALLERY

```
-----------------------------------------------------------------
 |ATTENTION: You have accessed a confidential and proprietary |
 |computing network.  Access  beyond this  point is  unlawful |
 |without  previous authorization from  BP and  MCI Security. |
 |TACACS+ account is required for access                      |
  ----------------------------------------------------------
 |WARNING: All  transactions  on this  router are logged 7x24 |
  ----------------------------------------------------------

ROUTER ID - BPAVMELR15C36


User Access Verification (Domain 10 - PDC)

The GNOC is in the process of cleaning up TACACS accounts. If your
account is disabled, you will require re-approval from the GNOC and
PSO WAN Service Line Leader.  Please send e-mail to
bpgnoc_tacacs_request@lists.wcom.com.

TACACS Username:
```

[TLC carriers have always been targets/4]

BANNER'S GALLERY

```
bash-2.02# pad 0250177200867
Break-in sequence is '^Pa'

Connecting...
Connected

                ##
               #  #                                          #
              #  #          ###    ###   #   #   ####   ####   #####
              #     #     #   #  #   #  #   #  #   #   #   #     #
               #   #      #####  #   #  #   #  #   #   #   #     #
             #  # #       #      #   #  #   #  #   #   #   #     #
            #    #        #   #  #  ##  #   #  #   #   #   #     #  #
             #  # #         ###    ## #   ###    ### #  #   #      ##
              ##   #                  #
                                      #

#====================================================================#
#                                WARNING!!                           #
# ACCESS TO AND USE OF THIS SYSTEM IS RESTRICTED TO AUTHORIZED INDIVIDUALS! #
#         Now we are start sending your addresses to the FBI / KGB!  #
#====================================================================#

User Access Verification

Username:
```

BANNER'S GALLERY

```
0505232650010

     ***
  *********   ************
   *******       ***************
   *** ***           ************************************
  **      **               ********************************************************


  WW      WW      WW                    ll        dd
  WW     Www     WW                    ll        dd
  WW    WWWW    WW   oooooo    rr rr    ll    dddddd   ccccc   oooooo    mmmm   mmmmm
  WW   WW WW   WW   oo    oo   rrrrrr   ll   dd    dd  cc      oo    oo   mm  mmm  mm
  WW WW  WW WW   oo    oo    rr       ll   dd    dd  cc      oo    oo   mm   mm  mm
  WWWW    WWWW    oooooo    rr      ll   ddddddd   ccccc    oooooo   mm        mm

  ------------------------------------------------------------------------------
 |ATTENTION: You have accessed a confidential and proprietary computing         |
 |network. Access beyond this point is unlawful without previous authorization|
 |from BP Amoco and Worldcom Security. TACACS+ account is required for access |
  ------------------------------------------------------------------------------
 |WARNING: All transactions on this router are logged 24 hours a day.           |
  ------------------------------------------------------------------------------

User Access Verification

Username:
```

BANNER'S GALLERY

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

BANNER'S GALLERY

pad 0487321873

```
      ____  ____   ____                /\  /^\
     o |  ____! |  __ \  / __ \       o  _     ,'  /' /\`\
    /\/| !__    | !__) || !__! |     /|\/    ___/  /' /'  `\`\
   /   |  __!   |  ___/ |  __  | o  ,  / |     ____/' /' /^\  `\`\_
  /\   | !____  | |     | |  | | |\/    / \     -----'_/'   `\__`-
 /_/_  !______! !_!     !_!  !_! |/\_  _/___\_     ___________
```

BUREAU OF ENVIRONMENTAL MONITORING & DATA PROCRSSING __________

ENVIRONMENTAL PROTECTION ADMINISTRATION

GOVERNMENT OF THE REPUBLIC OF CHINA

Username:

FUNNY TALES

[The Sky and the Sea]

[Banks & NA]

[DoSsing intl X.25 links]

[Mixed stuff]

THE SKY AND THE SEA

- Years ago, we've learnt a couple of nice things about **Airplanes** and **Ships** data connections.
- They've used the X.25 standard for over a decade, laying on **InmarSat** satellite network
- **SITA** plays an important role relating to **ground-connections**
- **AMSS** plays an important role relating to **air** and **sea connections**...

The addressing plan for AMSS is treated in [3]. The scope and impact of the AMSS addressing plan is limited to the AMSS subnetwork. Systems not directly attached to the AMSS network are not affected by the AMSS addressing plan.

The two principal types of ATN systems which use the AMSS subnetwork are airborne routers and air/ground routers. The AMSS address of an airborne router is formatted using BCD-encoded digits as follows:

<AMSS airborne address> :: <DNIC> '5' <AES> > <D>

<DNIC> :: '1111' (AOR-E satellite) or '1112' (POR satellite) or '1113' (IOR satellite) or '1114' (AOR-W satellite)

<AES> :: 8-digit BCD-encoded 24-bit address of aircraft

<D> :: Optional subaddress digit

The digit '5' following the DNIC is a discriminator indicating that the address refers to an airborne system. A example AMSS address of an airborne router flying over the Atlantic Ocean may be `1111.5.46721005`.

The AMSS address of an air/ground router is formatted using BCD-encoded digits as follows:

<AMSS ground address> :: '26' <DNIC> <NTN>

<DNIC> :: 4-digit DNIC of the ground network as registered in [X.121] or by international convention (e.g. SITA's DNIC is '1116').

<NTN> :: Up to 9-digit network terminating number (DTE network address) of the air/ground router on the provider's network identified by the ASNID.

The digits '26' comprise a prefix indicating that the address is used to access an internetwork router within the AMSS addressing plan. As an example, a SITA air/ground router AMSS address may be `26.1116.2331123`.

EXCESSIVE COUNTERMEASURES/1: THE ANDORRA CASE

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

BANKS AND NA (BEFORE)

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

BANKS AND NA (AFTER)

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

THE FRANCE CASE

- France Transpac seems to be the last "security-active" network.
- During 2004, russian hackers tried a couple of mass-scanning on 2080 DNIC...
- ...Any attempt to mass scan Transpac leaded to the **at once death** of the host used to scan.

DOSsing X.25 INTERNATIONAL LINKS

- Intl links depend on agreements among countries.
- The # of lines is limited (usually << 1000).
- Some little countries are routed only by one country (San Marino via Italy/ITAPAC, Andorra via Spain/IBERPAC, ...
- It might be theoretically possible to flood a whole country (with domino effect).

X.25 HACKING

[X.25 VS Internet]

[Attackers, Targets & Goals]

[What can I find ?]

[Evidences]

DIFFERENCES WITH THE INTERNET

- **X.25 Addressing is reserved**: scanning is the mostly used way to find targets.
- WAN concept: a NUA can **open a whole new world** to the attacker.
- No TCP/IP stack, **no "exploiting" concept** (well, until 2006...).
- Primarily **brute force attacks** on login (always works!).
- Old school hacking, social engineering and smartness **may help a lot**.
- There are a few X.25 walkers all over the world: **no kiddies, no noise, no game's playing**.
- If he isn't a walker, he's an attacker: probably with a **very high skill level**.
- There are also just **a few X.25 security experts** all over the world.

ZOOMING THE DIFFERENCES: X.25 HACKING

- Mostly done via scanning and bruteforcing
- There are not “bugs” but “features”
  - ✓ PSI mail
  - ✓ CUD and FACILITY
  - ✓ XoT (x.25 over TCP)
  - ✓ IP over x.25
  - ✓ PPP

ATTACKERS, TARGETS AND GOALS

- “X.25 Newbies” (Russia & South America scene)
- Lonely attackers, old school hackers
- Security researchers / Elite hackers (la crème)

- Criminal organizations (w/insiders on target)
- Industrial spies
- Intelligence Agencies’ agents
- (cyber) Terrorists (?)

ATTACKERS, TARGETS AND GOALS

- **Subscribers**
  - X.25 subscribers did **always** run **huge data networks**.
  - It's like having an **open door to the world**, that directly brings up strangers into our bedroom.
  - Monitoring **isn't easy at all**, requires specific skills and the knowledge of high-level attackers' habits.
  - Attackers abuse of X.25 resources to **scan for new targets**: this means **money** that will be billed to you as well as **legal problems (**if someone will ever realize what happened).
- **Services**
  - Telco Management Network (NMC, NE, Billing, etc..)
  - GSM and 3G SMSCs
  - Bank to Bank transfers (SWIFT); E-payments (POS)
  - Local PTs offices WAN
  - Worldwide Logistics & Transports
  - Heavy Industry
  - Travelling and Hotels agencies/environments (airports and flight companies as well)
  - Chemical and Pharmaceutical
  - SAP, ORACLE and similars (let's say "the big software houses")
  - WHQ -> HQ -> Branches World Wide
  - Government institutions and Agencies

TARGETS: WHO'S USING X.25 AND WHY ? (1/2)

- Finance
  - Banks
  - Credit card supplier and issuer
  - EDI
  - Swift (still?!)
  - Payment gateway (igfs, mtfs)
  - Local PTs offices (via X.25 or X.25D [ISDN D Channel])
- Aerocontrol (sita, rapnet)

TARGETS: WHO'S USING X.25 AND WHY ? (2/2)

- Big companies/multinationals
- System integrators (SAP's friends and more...)
- Governments
- Telcos (traditional and mobile)

ATTACKERS, TARGETS AND GOALS
(The honey prize: OS for prime time)

- AOS/VS
- *BBS Systems*
- Bull PAD (Bull DPX/2)
- CICS/VTAM
- Cisco IOS
- CDC NOS – Control Data Corporation
- DEC VAX/VMS and AXP/OpenVMS
- DEC Ultrix
- DEC Terminal Decserver
- DG/UX Aviion General
- DOS
- DRS/NX
- GS/1
- HP 3000
- HP/UX 9000
- IBM Aix
- IBM OS/400 (AS/400)
- IRIX SGI
- IRIS Operating System (PDP and others)
- Linux
- Motorola XMUX (Gandalf)
- Northern Telecom PBXs
- PACX/Starmaster (Starmaster Gandalf)
- **Pick Systems**
- PRIMOS Prime Computer
- RSTS
- SCO
- Shiva LAN Router
- Sun Solaris
- TOPS 10/20
- Unknown systems (you will find many of them)
- VCX Pad
- VM/CMS
- VM/370
- XENIX
- WANG Systems
- ……

WHAT CAN I FIND HERE ? (1/3)

⌘ X.25 hacking is **still** a very attractive target.

- **TELCOS**. Bypassing toll, getting services without fees, setting up premium numbers, amusing CDRs, getting fun with calls details&logs.
- **MOBILE OPERATORS**. As above, plus everytime you send an SMS :)
- **MULTINATIONALS**. Privacy invasions, industrial espionage, exciting hacking playground.
- **FINANCE**. The easiest way to get into legacy production systems. Also, POS heavily use X.25.
- **GOVERNMENT**. Many countries still hang up on their national X.25 network for their official gov' stuff.
- **NATIONAL CRITICAL INFRASTRUCTURES**. Many countries (East Europe, Africa) still manage their national N.C.I. via X.25 management links.

WHAT CAN I FIND HERE ? (2/3)

- As stated before, X.25 hacking will bring you to discover **unattended computer systems**, generally belonging to **huge institutions** and companies.
- In the next slides, we'll give out some examples, using some evidences gathered from **real-life experiences**.

WHAT CAN I FIND HERE ? (3/3)

We could name this slide as “strange things and possible problems that did **already happened**” so, pay attention folks!

- The security problem here is **really underestimated**.
- Everybody “**forgot**” about their X.25 direct links.
- **Closed countries** didn’t open to the Internet if not recently, but since more than a decade they’re opened to X.25 (unauthorized) access. (IRAN, CHINA)
- Some network **kindly gives** out X.25 addresses’ lists. (INDIA)
- As we said, while calling a NUA, you could also **reach an airplane** flying over the Atlantic Ocean. (INMARSAT)

UNCOMMENTED…

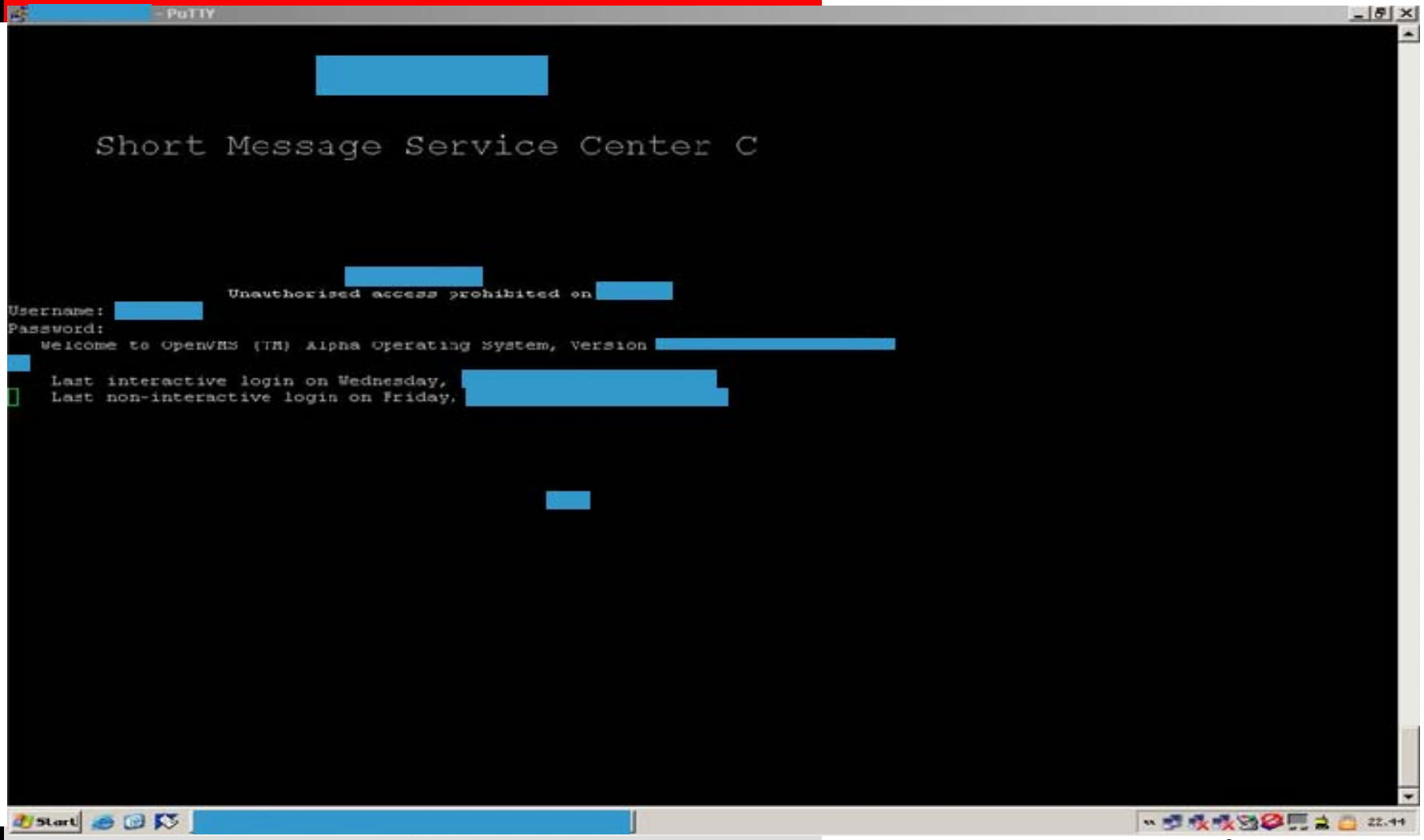
CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

UH, IS THIS AN SMSC ?!?



PROCESSED SMSs: “FROM”, “TO”

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

SMS PROCESSING QUE (!)

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

SMS SNIFFING (IN REAL-TIME…)

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

X.25 INTERCEPTION AND REAL-TIME INVESTIGATION

```
================================================================

10:15:16:56    10  A   outgoing       RcvR     3 octets    8       136
           LGN=0   LCN=10   LCI=10    P(R)=4
10 0a 81

Command line:  x25decode
Trace protocol: /dev/x25
Trace date: Tue Apr  7 10:14:54 BST 1998

Timestamp      VC  Snid  Direction   Pkt Type      Size     Mod  PacketId
================================================================

10:15:16:98    10  A   outgoing       Data   126 octets    8       137
      D=0  LGN=0   LCN=10   LCI=10    P(S)=3    P(R)=4    M=0  Q=0
10 0a 86 56 2e 0d 56 48    48 47 2e 57 41 2f 45 31    * ...V..VHHG.WA/E1 *
42 54 55 4b 2f 49 31 31    47 49 41 2f 50 a0 25 d9    * BTUK/I11GIA/P.%. *
0d 56 47 59 41 0d 55 4e    42 2b 49 41 54 41 3a 31    * .VGYA.UNB+IATA:1 *
2b 31 47 2b 46 53 2b 39    38 30 34 30 37 3a 31 30    * +1G+FS+980407:10 *
31 35 2b 54 32 27 55 4e    48 2b 31 2b 48 53 46 52    * 15+T2'UNH+1+HSFR *
45 51 3a 39 34 3a 31 3a    49 41 27 4f 52 47 2b 46    * EQ:94:1:IA'ORG+F *
53 3a 4c 4f 4e 27 4c 54    53 2b 2a 52 27 55 4e 54    * S:LON'LTS+*R'UNT *
2b 34 2b 31 27 55 4e 5a    2b 31 2b 54 32 27          * +4+1'UNZ+1+T2'   *

================================================================
```

TOOLS

[Old times]

[Today]

OLD TIMES

- Telix SALT scripts (DOS)
- NComm scripts (Amiga)
- Home-made “dumb” scanning code (+ blue-boxing/calling cards modem-call to SprintNet or other ACPs/POPs)
- Prime PRIMOS Scanner (The Force)
- VMS X.25 Scanner (Nobody & Zibri)
- Unix X.25 shell script Scanner (Escom)

TODAY

- ADMx25.
- Unix multithread & multichannel X.25 scanner.
- Perl multithread & multichannel XoT scanner.
- Unix multithread x.25 brute forcer http://wayreth.eu.org/x25bru.c

A SCAN FROM 2005

CENSORED

You should have joined Confidence 2007 …If you really wanted to see this slide ☺

A LOOK AT THE FUTURE

[Mass Scanning]

[CUD Fuzzying]

[Abusing XoT]

MASS SCANNING

- **With multithreaded software scanning is really faaaast!**
- Depending on the number of available channels and on the network used to scan (some countries networks are faster than others).
- 32 available physical channels are enough to scan **10.000** x.25 NUAs in less than **3 minutes**.

Solaris example:

bash-2.02# grep "two_range" /etc/opt/SUNWconn/x25/config/link_config_0000.cfg
*two_range 1-**128***

bash-2.02#

XOT

- x.25 over IP (RFC **1613**)
- Because the legacy world **still needs** x.25
- It's easy to add systems to the network without installing the x.25 stack

USING XOT: AN EXAMPLE

⌘ In order to (ab)use XoT, you don’t need to have an X.25 link on your machine: you can simply configure your own Cisco IOS to use another Router’s XoT facilities.

```
service pad to-xot
x25 routing
x25 route .* xot 196.xxx.xxx.7
```

PRIVATE X.25 NETWORKS VIA XOT

- A new world opens to you:
  - Not-routed networks, just local and “private”.
  - Mostly used by finance and telcos.
  - Needed by legacy applications.

```
root@darkstar:~# telnet 154.85.233.xxx
Trying 154.85.233.xxx...
Connected to 154.85.233.xxx.
Escape character is '^]'.
Trying 1234555500...Open

PIN:
```

JUMPING FROM X.25 TO IP

```
bash-2.02# pad 025017722029600
Break-in sequence is '^Pa'

Connecting...
Connected
Trying 195.82.10.10, 2001 ...Connect

Login:
```

NOTE: You can shell to the Cisco, with the correct escape sequence.

- See:
  http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080174a34.shtml

ABUSING XOT

- Auth is **not needed**

- Easy to manipulate: (RFC **1613**)
  - NUA spoofing
  - ACL bypassying
  - CUD fuzzying

PRIVATE X.25 NETWORKS VIA XOT

- A lot of company use PPP over x.25 to carry IP (where there is no Internet).
  - There is no Interactive Login, only PPP.
  - With XoT you can connect to the NUA and start PPPD (just some conversion problem, ie. 7E2 or 7E1 to 8N1).

PRIVATE X.25 NETWORKS VIA XOT

```
bash-2.02# /opt//SUNWconn/x25/bin/pad 025017725200468
Break-in sequence is '^Pa'

Connecting...
Connected
Entering PPP mode.
Virtual-Access2 interface address is unnumbered (Loopback0)
MTU is 1500 bytes
Header compression is on.

~ÿ}#À!}!}!} }8}"}&} }*} } }#}$À#}%}&ò}%uã}'}"}(}"EÄ~~ÿ}#À!}!}"}
}8}"}&} }*} } }#}$À#}%}&ò}%uã}'}"}(}"}/V~~ÿ}#À!}!}#} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"Æß~~ÿ}#À!}!}$} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"z~~ÿ}#À!}!}%} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"Có~~ÿ}#À!}!}&} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"})a~~ÿ}#À!}!}'} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"Àè~~ÿ}#À!}!}(} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"#~
```

XOT MANIPULATION

- X.25 spoofing
  - Make calls “nearly untraceable”
  - Fool system’s ACLs (not the telco’s ones)

- CUD
  - Used to ask for application

X.25 EXPLOITING

- Really hard to perform
- Only few and not-standard services
- But IT IS still possible... ☺
- Actually, we've developped the porting of the Solaris remote telnet exploit to X.25 environments. **It works**.

X.25 EXPLOITING

- Looking for services and applications
  - Check for subaddresses
  - Check for CUD
  - Es. Sunlink smnpx25d (http://www.securityfocus.com/bid/8882)
  - E.g.: customized applications.
  - Solaris login exploit: http://wayreth.eu.org/padxploit.c

CUD

- **CUD is the Call User Data**
- It can be 16 bytes long till 128.
- You can configure you x.25 daemon to accept only calls with a known CUD (like a password) (**or like a backdoor**! Defining /bin/sh as a service).
- It's often used to specify an application.
- Default CUD is "01/00/00/00" and it means "interactive login" (solaris sunlink exec /bin/login).

CUD MANIPULATION

- Interactive login relocation
  - An application answer on the default CUD
  - The interactive login may answer on another CUD
  - CUD guessing and brute-forcing
- Application scanning
  - There are few known CUD and application
    - PPP (RFC1598)
    - VMS and Open VMS PSI (Packet Switched Interface) mail

CUD EXAMPLES

- CUD starting with “01” is the default (interactive login).
- CUD starting with “CC” point to IP over x.25 (RFC877).
- VMS examples (with cisco regular expr):
  - ^\$COPY$ for remote copy.
  - ^\$DECNET$ for DECNET connections.
  - ^\$MAIL$ for PSI mail.
  - ^\ITS who knows?
  - ^\$PRBLM$ who knows?
  - ^\REG who knows?

CUD FUZZYING

- Just to try to discover applications and interactive login relocations.
- Stress tests against systems.
- XoT is useful to automate and speed-up the process.
- Maybe something can be overflowed?

END

[Getting Help: take care]

[Conclusions]

[References]

[Bibliography]

[Greetings]

[Contacts]

TAKE CARE WHEN ASKING FOR HELP

- **Traditional security shops**: zero knowledge of X.25 security problems, telcos, poor understanding of global WANs logicals & procedures.
- **Traditional telcos consultants**: very poor knowledge of security issues.
- **X.25 carriers**: they'll try to sell you IP connections instead of fixing your X.25 and Frame Relay links security holes, and they'll suggest you to migrate everything you have onto the IP world.
- Customers' **loved and trusted security consultant**: in this case he probably doesn't even know what you are talking about.
- The **"Big 5" audit firms**: focused on policies, no real expertise (they outsource their jobs to companies like us).
- **In-house resources**: Very dangerous. Internal fraud overlooked. Interdepartmental ego problems. Good security and bad security looks the same.

@ MEDIASERVICE.NET CONSULTING NETWORK

- Networked structure
  - Structure similar to the Global Business Network (http://www.gbn.org/)
  - 3 **Operating Central Offices** (Torino, Trento, Rome)
  - +10 years experienced professional consultants network
- Leverage on **each individual's skills** and services
- Leverage on **network effect**

OUR X.25 PROFESSIONAL SERVICES

- **Penetration Testing**
- **Ethical Hacking**
- **Security Audit**
  - over PSDN, PSTN/ISDN networks (and others)

- **ISECOM's OSSTMM Certified Security Testing** (YES, including X.25! :)

- **X.25 Security Consulting**
  - Short term (Incident investigation, Security review)
  - Long term (Fraud Management, SOC 24x7x365)
  - Emergency services (Red Team/Blue Team)

BENEFITS FOR PARTNERS

- Consulting Partners
  - Develop common offer
  - Co-branding
- Professional Service Resellers
  - High-end service with high-revenue generation
- Premium
  - Research capability of @ Mediaservice.net focused on your needs
  - Low fee

CONCLUSIONS

Doing Nothing…

- … with your PSDN infrastructure today is like doing nothing with your Internet hosts in the 90's: how many hackers played with your datas ?
- …in critical environments, this is an invitation for disaster.

REFERENCES

- RFCs
- RFC 874 - A Critique Of X.25
- RFC 877 - Standard For Transmission Of IP Datagrams Over Public Data Networks
- RFC 1356 - Multiprotocol Interconnect On X.25 And ISDN In The Packet Mode
- RFC 1090 - SMTP On X.25
- RFC 1381 - SNMP MIB Extension For X.25 LAPB
- RFC 1382 - SNMP MIB Extension For The X.25 Packet Layer
- RFC 1461 - SNMP MIB Extensions For Multiprotocol Interconnect Over X.25

- Tutorials
- RIM Remote System - Neurocactus Ezine
- Hacking UNIX Tutorial - By Sir Hackalot
- Advanced Hacking VAX's VMS - By Lex Luthor
- Guide to Gandalf XMUXs - By Deicide
- B4B0 Ezine #7 : Hacking The Shiva LAN-Rover - By Hybrid
- The Complete Hewlett Packard 3000 Hacker's Guide - By AXIS
- X.25 And LAPB Commands For Cisco Routers
- A Novice's Guide To Hacking - By The Mentor
- The Beginner's Guide To Hacking On Datapac - By The Lost Avenger and UPI
- NEOPHYTE'S GUIDE TO HACKING (1993 Edition) - By Deicide

BIBLIOGRAPHY

- **Online material**
  - **I network X.25:Comprensione della struttura di rete, Tecniche di intrusione ed Identificazione degli attacchi**, by Raoul “Nobody” Chiesa and Marco “Raptor” Ivaldi, Italian Black Hats Technical Paper #1 (Italian only, 95 pages). http://www.blakhats.it/papers/x25.pdf/
  - **Libnet-X.25**: The Preamble
  - **Protocol Vulnerabilities within the X.25 Networking suite**.
  - X.25 Standards and ITU Recommendations (http://www.itu.int/)
  - X25zine (http://www.x25zine.org/)
  - **X25 Trace: X.25 network tracing for Internet users**, by Dennis Jackson, JANET-CERT Coordinator, U.K.
  - **A novice Guide to X.25 Hacking**, by Anonymous
  - **Desktop Guide to X.25 Hacking in Australia**, by Epic Target
  - **Accessing Telecom Australia's AUSTPAC service** - By Softbeard
  - **The Force Files** - By The Force
  - **Austpac.notes** - by Vorper VII
  - **Globetrotter Ezine** - By The Force
  - **Alt.2600 Hack** (90’s posts) - By Simple Nomad
- **Literature**
  - **Underground** - By Suelette Dreyfuss (Australia)
  - **The Cuckoo’s Egg**, Clifford Stoll, Pocket Books, 1989 (USA)
  - **Cyberpunks: Outlaws and hackers on the Computer Frontier**, Katie Hafner & John Markoff, Touchstone Books 1991 USA
  - **Out Of The Inner Circle** - By Bill Landreth, McGraw Hill Internetworking Handbook
  - **An Introduction To Packet Switched Networks Parts I and II**, Telecom Security Bulletin File by Blade Runner

BIBLIOGRAPHY

RFCs

- RFC 874 - A Critique Of X.25
- RFC 877 - Standard For Transmission Of IP Datagrams Over Public Data Networks
- RFC 1356 - Multiprotocol Interconnect On X.25 And ISDN In The Packet Mode
- RFC 1090 - SMTP On X.25
- RFC 1381 - SNMP MIB Extension For X.25 LAPB
- RFC 1382 - SNMP MIB Extension For The X.25 Packet Layer
- RFC 1461 - SNMP MIB Extensions For Multiprotocol Interconnect Over X.25

Tutorials

- RIM Remote System - Neurocactus Ezine
- Hacking UNIX Tutorial - By Sir Hackalot
- Advanced Hacking VAX's VMS - By Lex Luthor
- Guide to Gandalf XMUXs - By Deicide
- B4B0 Ezine #7 : Hacking The Shiva LAN-Rover - By Hybrid
- The Complete Hewlett Packard 3000 Hacker's Guide - By AXIS
- **X.25 And LAPB Commands For Cisco Routers**
- A Novice's Guide To Hacking - By The Mentor
- The Beginner's Guide To Hacking On Datapac - By The Lost Avenger and UPI
- **NEOPHYTE'S GUIDE TO HACKING** (1993 Edition) - By Deicide

GREETINGS

/X.25 gurus/

Machine
b
Vaxer
Id0
Pengo
V2
Freehunt from x25zine.org
Emmanuel Gadaix
Vanja
Raptor
The Force (and the aussie scene)

/Friends/

Venix
Philippe Langlois
D0
FX from Phenoelit
Andrea Barisani
Asbesto
dialtone
rpunk and people at #x.25 (efnet)
Fyodor Yarochkin
The Xfocus team
Jim Geovedi
Anthony Zboralski
Fabrice Marie

/Telcos/

...just for being there :)

...And all of the Confidence 2007 folks for this nice meeting !

QUESTIONS ?

Raoul “Nobody” Chiesa

TELECOM SECURITY TASK FORCE: rc@TSTF.net

@ Mediaservice.net Srl: raoul@mediaservice.net