

**X.25 (in)SECURITY in year 2005:
What, Why, When, Who, How
OR...
(not anymore) uncovered data
networks,
(yet) covered targets.**

[real life & field experiences on an underestimated
and still actual security issue]

**HITB 2005,
29th September
Kuala Lumpur (MY)**

**Raoul Chiesa, T.S.T.F.
Telecom Security Task
Force**

Disclaimer

- X.25 protocol's theories and specs have been **intentionally uncovered** in this document.
- 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 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 laws.
- The X.25 addresses used in the slides can be **sometimes real and sometimes fake**: in the first case they are out-of-date, else they've been used for clear example purposes.
- In any case, the real X.25 addresses mentioned as evidences have been taken from **public source** and their publication does not mean in any case an invitation to attack or test the connected systems.
- Quoted trademarks belongs to registered owners

Agenda

- Intros
- */your nightmare starts here/*
- (a brief) technical overview
- So, how does it work ?
- Understanding NUAs and DNICs
- The history always teach...
- Some (cool) evidences !
- Differences between X.25 and the Internet
- Attacker's typologies, preferred targets
- Conclusions
- Q&A
- */end of nightmare/*

TSTF: a short intro

- Founded by professionals and specialists.
- Located in Asia, Europe, USA.
- 30 years combined telecommunications experience.
- 50 years combined information security experience.
- A unique view on telco security – nobody else does it.
- Our field experience in worldwide networks makes the working difference, and let us know how to secure your infrastructures. For real.
- We know the slang, the terms, the devices and the techniques to use on X.25 networks as no one else does: we are the best on this topic and we know it.
- Active research (papers, tools, forums).
- Self-funded, no business cunts running it, no VCs.

The Speaker

- (direct) hacking experiences from 1986 to 1995
- Busted in the “Ice Trap” operation (13th December, 1995) managed by Criminalpol, Interpol and FBI
- Ethical hacker since that (well... I grow up ;)
- Professional Penetration tester (1996 -> today)
- Chief Technical Officer, @ Mediaservice.net Srl, a vendor-independent security consulting company based in Europe (Italy)
- OSSTMM (Open Source Security Testing Methodology Manual) Official Key Contributor (2002, 2003, 2004, 2005)
- Board of Directors Member:
 - T.S.T.F. (Telecom Security Task Force, www.tstf.net)
 - ISECOM (Institute for Security and Open Methodologies, www.isecom.org)
 - CLUSIT (Italian Computer Security Association, www.clusit.it)
 - OWASP – Italy Chapter (Open Web Applications Security Project, www.owasp.org)

“ 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).”

Why are we talking about X.25 security in 2005 ?

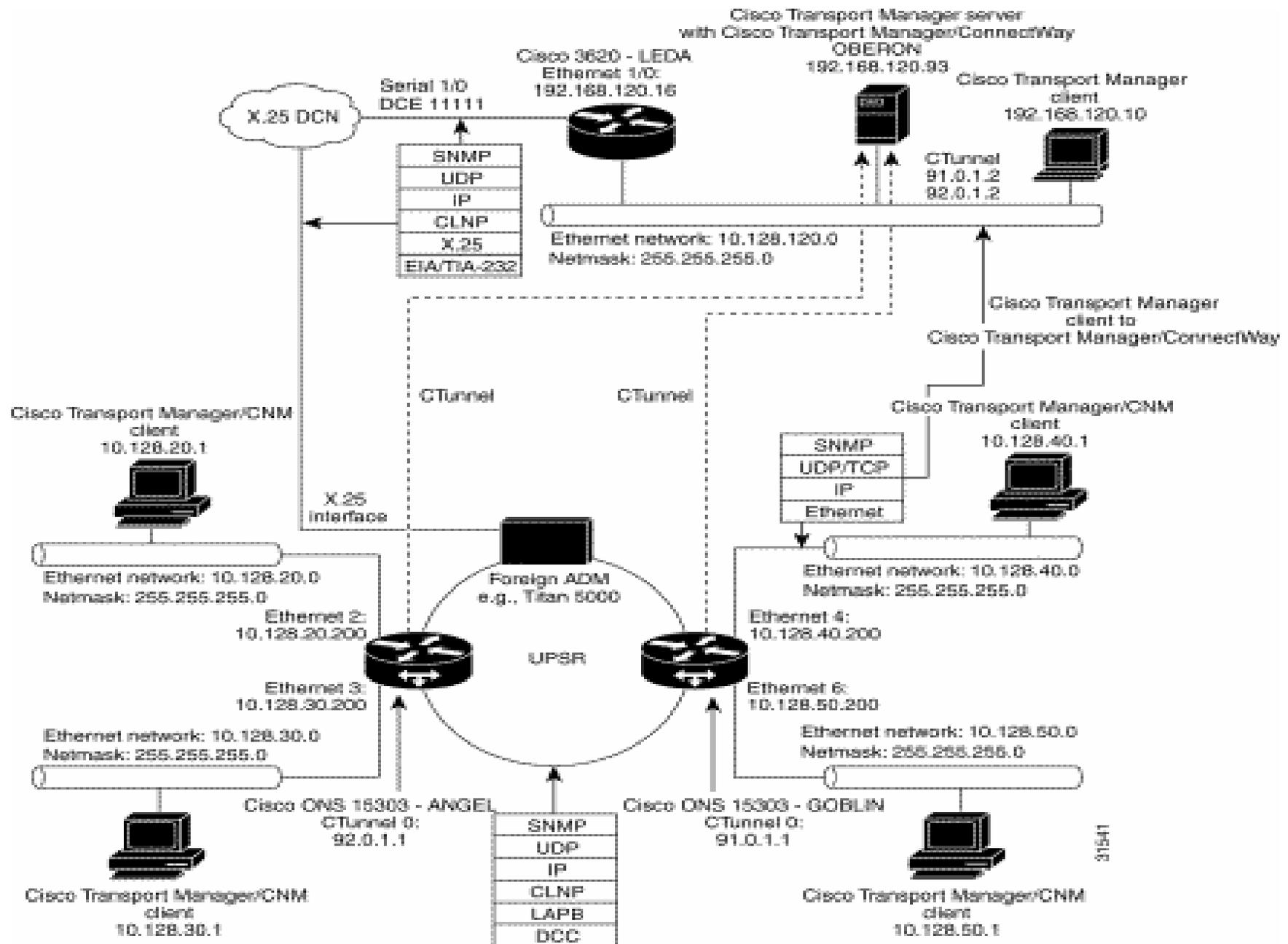
- This speech is oriented towards network security while **working in X.25 worldwide environments** and its legal working framework.
- The information contained is based on personal, company's and other international researchers' professional **penetration testing experiences** and field observations.
- 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 (1999->2003); 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 **2005**, and new breaches are still upcoming.

Introduction – What's this ?

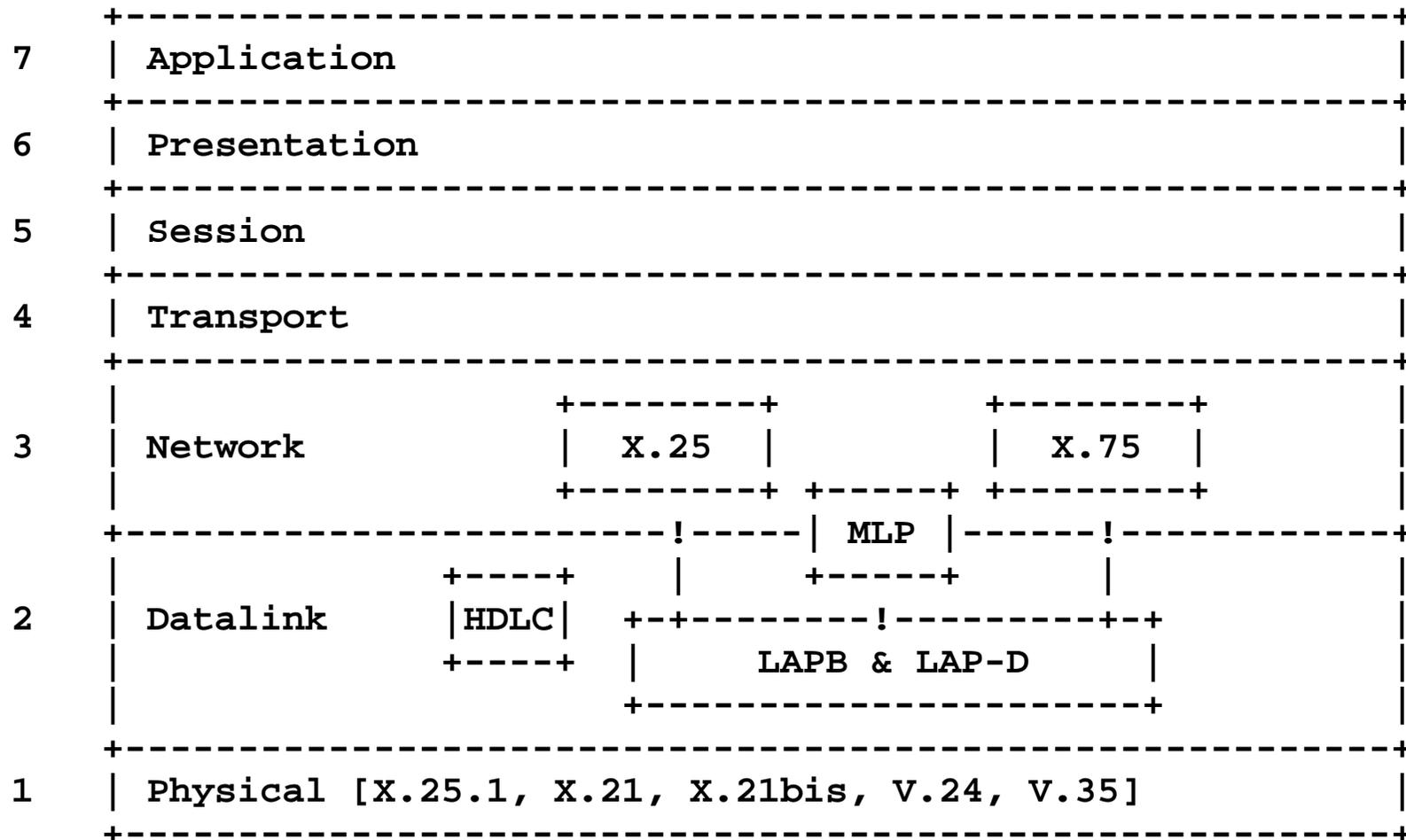
- An International **P**acket **S**witched **D**ata **N**etwork (PSDN).
- A model **very similar** to Public Switched Telephone Networks (PSTN).
- 3 main packet type: **Data, Control, Facilities**.
- **International standards** (X.25/X.29, X.28, X.75, X.121) created by ITU (International Telecommunications 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.
- **Multinationals, Governments** and **private SMEs** with worldwide or interregional quality data-connection needing, are the typical **key clients**.

Introduction – How it works ?

- Each subscriber has an **international X.25 address** – N.U.A. Network User Address - assigned to a **leased line**, with one or more **logical channels**.
- Subscriber A can call Subscriber B in order to establish a **switched virtual circuit (SVC)** call or a **permanent virtual circuit (PVC)**.
- **Only traffic is billed**, customer doesn't pay the connection-time.
- Both on SVCs and PVCs links is possible to talk over **many different protocols** (host-to-host, SNA, proprietary, voice, Kermit....).
- X.3 PAD capabilities are implemented in **major OS**:
 - *NIX
 - linux
 - VMS/OpenVMS
 - AS400
 - old stuff
 - strange/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 User Facilities]

- **User Facilities are defined by ITU recommendations**
- **Each carrier implements different, customized U.F.**

- **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 let 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).

How do I access to it ?

- 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, **MAYPAC**...
 - the “net” ones: Isranet, Pacnet, Rosnet, ...
- 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) ;
 - (Hacked) Systems linked both to the Internet and to a X.25 network – directly and/or via LAN/WAN;
 - X.25 over TCP – XoT (RFC1613).
- Outdials, CCs or abused PBXs are often used to call X.28 PADs.
 - ...the backtracing investigation technique won’t so be easily applicable (or nearly impossible to do);
 - ...it’s possible to use NUIs from other countries (phreaking and social engineering can help definitely a lot here)

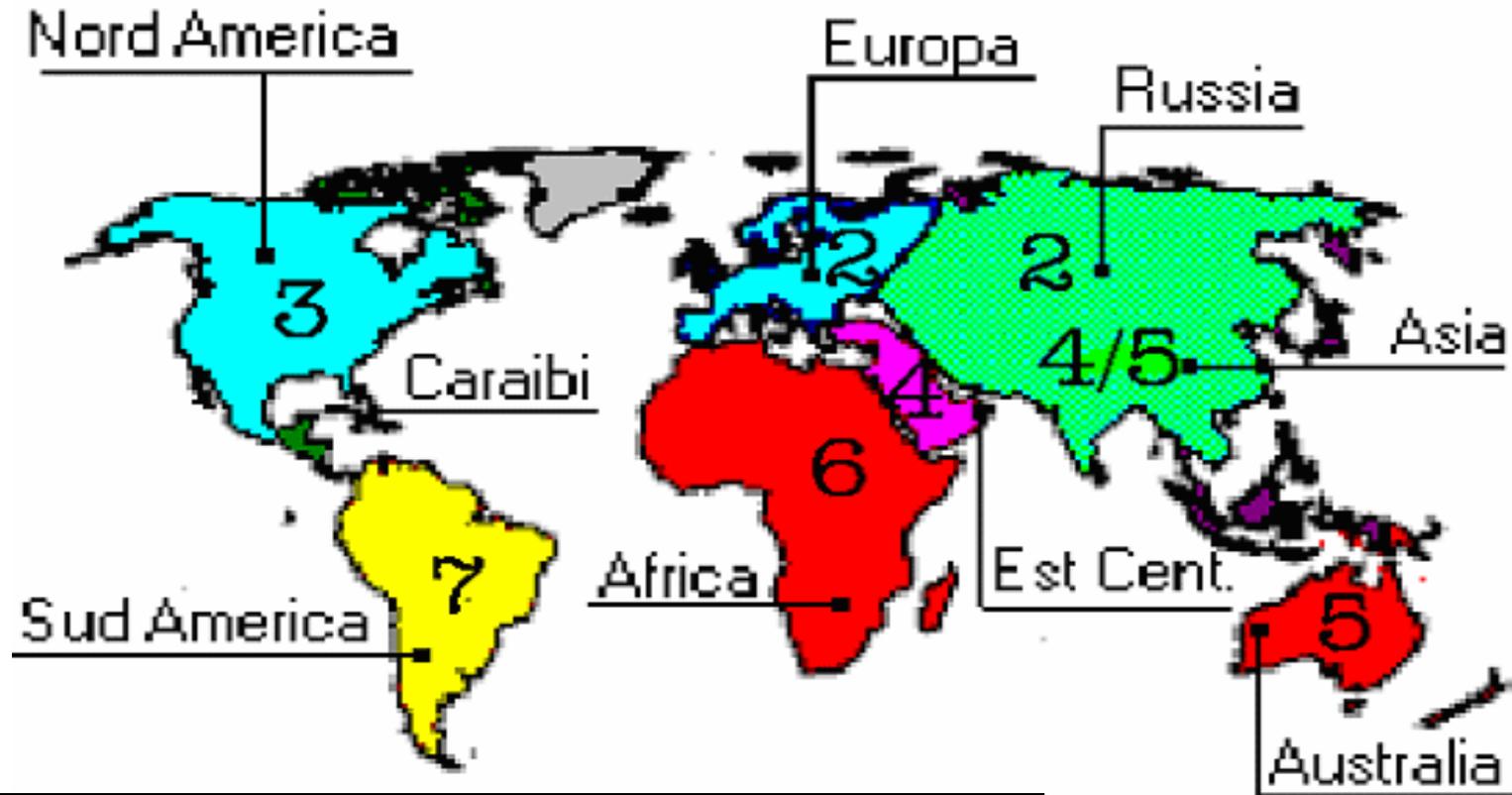
X.25 Addressing

- Hosts are identified by:
 - **NUAs**: 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.
- **X.25 addresses are reserved** and should not be disclosed
- X.121 address: DNIC + NUA = 15 digits max.
 - DNIC: 4 digits international code: DCC + NCC
 - DCC assigned on a geographical basis by ITU (world's areas)
- 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)

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 Caribbean areas
4	Asia
5	Oceania
6	Africa
7	Part of Central America, Caribbean 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

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.)

DNICs -

1

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

The Australia case

DNICs - 2

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	← Sub-carrier
50542	6 September 1994	AAPT Ltd	
50543	6 September 1994	AAPT Ltd	
50560	16 February 1994	SingCom (Australia) Pty Ltd	← Sub-carrier
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	← Critical (and shared !)
505790	17 November 1993	Department Of Defence	
505791	17 November 1993	Department Of Defence	
505799	23 February 1995	Telstra Corporation Ltd	

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.

DNICs -3

The U.S.A. case

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 Service
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

← Data carriers

← Multinationals

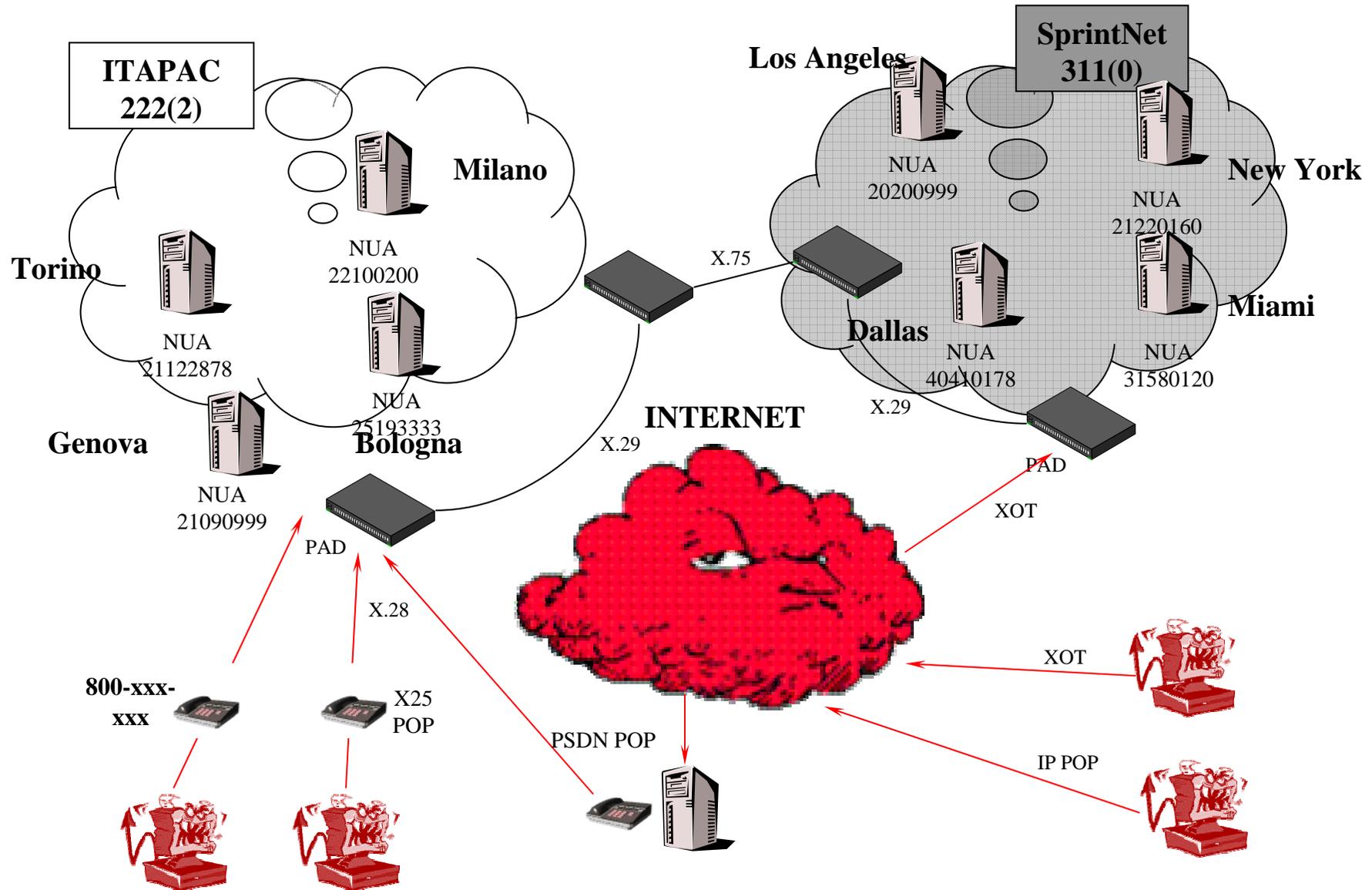
← Spy Game ? ;)

DNICs - 4

The Malaysia case

MALAISIE	502 0	COINS Global Frame Relay
MALAYSIA	502 1	Malaysian Public Packet Switched Public Data Network (MAYPAC)
MALASIA	502 3	Corporate Information Networks
	502 4	ACASIA-ASEAN Managed Overlay Network
	502 6	Mutiara Frame Relay Network
	502 7	Mobile Public Data Network (WAVENET)
	502 8	Global Management Data Services (GMDS)

Hackwork





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

```
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

- 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

Historical (big) problems

- **80's**: CCC members Pengo and Hagbard broke 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 also used 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).
- **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 ADM group released their own scanner (ADMx25 by Antilove).
- **Recent years**: **Multithread** and **multichannel** Sun Solaris X.25 scanner available in the wild: it's able to scan a whole country in a few hours.
- **2003-05**: Russian crackers perform mass huge scannings over SprintNet international networks and dialups (intl' reverse charge scans).

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

```
=====  
=##@##=====  
==#####  
=#####  
=#####  
==#####  
=====
```

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

attmail login:

Connected to 0420160014025

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

WELCOME TO INMARSAT C LES JEDDAH KINGDOM OF SAUDI ARABIA

Enter ?<CR> to get help information,

C<CR> to cancel input.

TLC carriers have always been targets (2)

\$ 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:

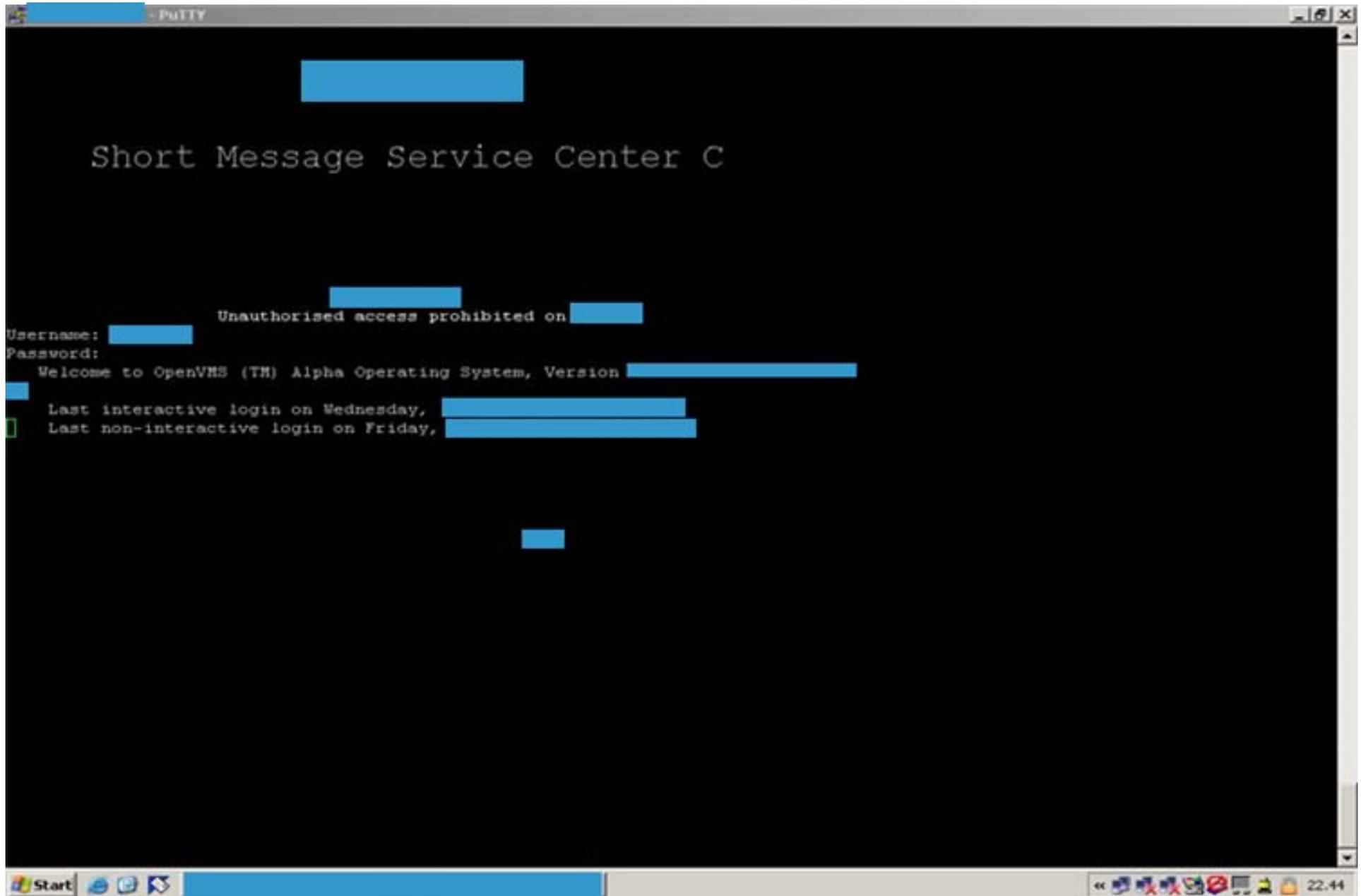
Differences with the Internet

- **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** (a kind of...).
- 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 the **highest skill level** you’ve ever encountered with.
- There are also just **a few X.25 security experts** all over the world.

Major Target Areas

- Subscribers
 - X.25 subscribers **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 (Central Offices, Switches, etc..)
 - GSM and 3G **SMSCs**
 - Bank to Bank transfers (SWIFT); E-payments (POS)
 - Worldwide Logistics & Transports
 - Heavy Industry
 - Travelling and Hotels agencies/environments (airports and flight companies as well)
 - Chemical and Pharmaceutical
 - SAP and similars
 - WHQ -> HQ -> Branches World Wide

Uh, is this an SMSC ???



Processed SMSs: “FROM”, “TO”

NITT	TENT	DEST	STATUS	SUBNTI	DELIVERY	TIPO	IDE	SIZE
[REDACTED]8122978	[REDACTED]	[REDACTED]01100005	4	2003-02-04 10:50:44	2003-02-04 11:22:19	98	0	125
1								
[REDACTED]8122978	[REDACTED]	[REDACTED]00900013	4	2003-02-04 12:53:04	2003-02-04 12:53:11	98	0	125
1								
[REDACTED]8122978	[REDACTED]	[REDACTED]00000001	4	2003-02-04 13:42:03	2003-02-04 13:42:13	98	0	125
1								
[REDACTED]8122978	[REDACTED]	[REDACTED]6334481	4	2003-02-04 16:43:19	2003-02-04 16:43:27	97	98	36
1								
[REDACTED]8122978	[REDACTED]	[REDACTED]92400042	4	2003-02-04 20:42:46	2003-02-04 20:43:48	98	0	94
1								

Press RETURN to continue

SMS Processing que (!)

```
000C91 9180988FFFFFFF 00000000000000000000000000000000 FFFFFFF 9 5690500000000000 000000 0000000000000000000000
00000000000000000000
15:55:02.18|04400403|MSISDN not found in cache
15:55:02.18|04400403|ISID inserted in cache
15:55:02.18|04400403|MSISDN inserted in cache
15:55:02.18|04400403|Context new 823
15:55:02.18|04400403|IOS received
15:55:02.18|04400403|SAD_DECODE_ADDR: Encoded address 000C91 185900FFFFFFF -> address 0039 819500
15:55:02.18|04400403|SAD_DECODE_ADDR: Decoded address 819500 TELEPHONE NATIONAL
15:55:02.18|04400403|TP-MTI -----01 SMS-SUBMIT (in the direction MS to SC)
15:55:02.18|04400403|TP-RD -----0-- Accept duplicate message
15:55:02.18|04400403|TP-VPF ---10--- TP-VP field present and integer represented (relative)
15:55:02.18|04400403|TP-SRR --0----- A status report is not requested
15:55:02.18|04400403|TP-UDHI -1----- The beginning of the TP-UD field contains a header in addition to the short message
15:55:02.18|04400403|TP-RP 0----- TP-Reply-Path parameter is not set in this SMS-SUBMIT/DELIVER
15:55:02.18|04400403|TP-MR 11100111 Message reference number 231
15:55:02.18|04400403|TP-DA 00001010 Address length 10
15:55:02.18|04400403|TP-DA -00----- TON -> Unknown
15:55:02.18|04400403|TP-DA ----0001 NPI -> ISDN/telephone numbering plan (E.164/E.163)
15:55:02.18|04400403|TP-DA 00110011
15:55:02.18|04400403|TP-DA 00100011
15:55:02.18|04400403|TP-DA 01100011 36
15:55:02.18|04400403|TP-DA 01111001 97
15:55:02.18|04400403|TP-DA 00010110 61
15:55:02.18|04400403|TP-DA Address: 369761
15:55:02.18|04400403|TP-PID 00----- Protocol or Telematic interworking
15:55:02.18|04400403|TP-PID --0----- SME to SME protocol
15:55:02.18|04400403|TP-PID ---00000 SM-AL protocol
15:55:02.18|04400403|TP-DCS 0000---- General Data Coding indication
15:55:02.18|04400403|TP-DCS --0----- Uncompressed
15:55:02.18|04400403|TP-DCS ---0---- No message class meaning
15:55:02.18|04400403|TP-DCS ----00-- Default alphabet
15:55:02.18|04400403|TP-VP 11111111 Validity period : 63 week(s)
15:55:02.18|04400403|TP-UDL 00110010 50
15:55:02.18|04400403|TP-UDHL 00000101 5
15:55:02.18|04400403|..IEI 00000000 Concatenated short messages, 8-bit reference number
15:55:02.18|04400403|..IEIDL 00000011 3
15:55:02.18|04400403|..IEDa 00110110 54 reference number
15:55:02.18|04400403|..IEDb 00000010 2 maximum number of short messages
15:55:02.18|04400403|..IEDc 00000010 2 sequence number
15:55:02.18|04400403|Event: 00, State: 00, Action: 01
15:55:02.18|04400403|Save DATIND data
15:55:02.18|04400403|NRT: recognised address as type EMPTY
15:55:02.18|04400403|SAD_RAW_ENCODE: Encoding 369761 as an TELEPHONE UNKNOWN address
15:55:02.18|04400403|SAD_RAW_ENCODE: Encoded address 000A81 637916FFFFFFF
Press RETURN to continue
```


Attackers' typology

- “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 (?)

The honey prizes: OS for prime time

- OS that you may find on X.25 networks

- 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 Aviiion 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

NOTE: This list is an extract from the upcoming white paper “The (un)official Systems Catalogue”, by Raoul Chiesa

The nightmares of the past

- Based on a TSTF 5-years study, encompassing 21 network operators:

100% could be hacked from the Internet

90% could be hacked through PSTN, X.25 or ISDN

72% had a security incident in the last 2 years

23% had appropriate perimeter security control

0% had all their mission-critical hosts secured

0% had comprehensive database security in place

0% had integrity measures protecting billing data

- Based on a 15 years personal background and knowledge:

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

YES, 1% O N L Y.

The nightmares of today

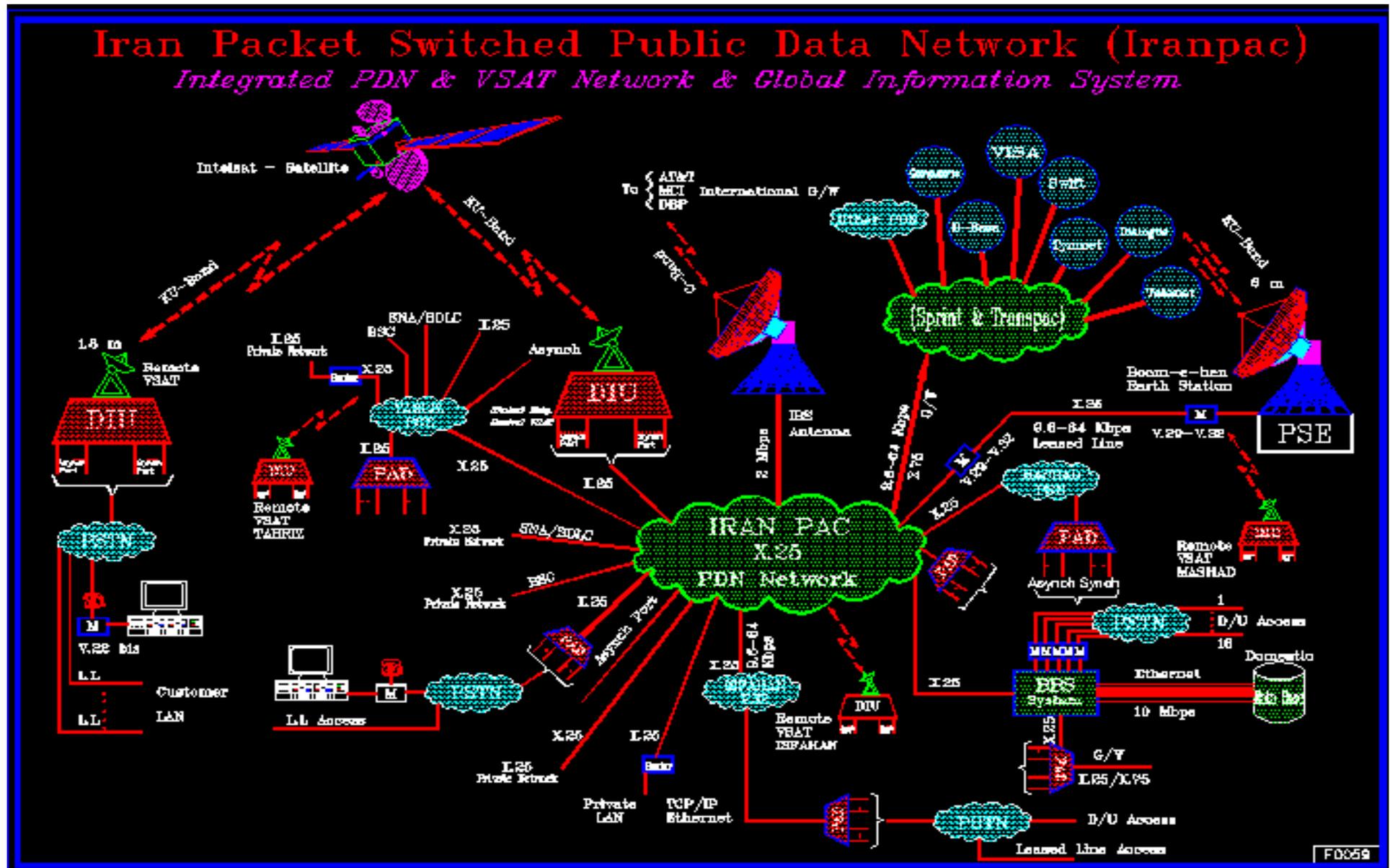
X.25 hacking is **still** a very attractive target.

- 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.

Hot Points: strange things and possible problems that had already happened

- 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)
- When calling a NUA, you could also **reach an airplane** flying over the Atlantic Ocean. (INMARSAT)

Let's make an X.25 hacker happy



How to help an X.25 hacker

Inet DIRECTORY ENQUIRY SERVICE

DIRECTORY ENQUIRY SERVICE ___NMC VER 2 ___ NETWORK : RABMN, INDIA PAGE
0

NETWORK #	NAME / ORGANISATION	LOCATION
404100000162	A C C	WADI
404100010681	A C C	BILASPUR
404100000589	A C C	BOMBAY
404100000381	A C C	CHAIBASA
404100000055	A C C	JAMUL
404100000420	A C C	KYMORE
404100010162	A C C	WADI
404100010589	A C C	BOMBAY
404100010626	A P RAYONS	KAMALAPURA
404100010625	A P RAYONS	HYDERABAD
404100000172	ANAND BAZAR PATRIKA	BOMBAY
404100010882	ANAND BAZAR PATRIKA	CALCUTTA
404100000362	ANAND BAZAR PATRIKA	NEW DELHI
404100010172	ANAND BAZAR PATRIKA	BOMBAY
404100000821	B A R C	BOMBAY

How to excite an X.25 hacker

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.

X.25 Interception & real-time Investigation

- Getting the datas and the evidences from an X.25 incident...

...it's not impossible.

```
=====
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
```

**If you
know
HOW
to do it.**

```
=====
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' *
=====
```

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, and they'll suggest you to migrate everything you have onto the IP world.
- **Your 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 us).
- **In-house resources:** Very dangerous. Internal fraud overlooked. Interdepartmental ego problems. Good security and bad security looks the same.

Conclusions

Doing Nothing...

- ... with your PSDN infrastructure today is like doing nothing with your Internet hosts in the 90's and with your Wi-Fi networks in 2000: **how many hackers** played with your datas ?
- ...in critical environments, the above is simply **an invitation for disaster.**

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

Bibliography

- Online material
 - **I network X.25: Comprensione della struttura di rete, Tecniche di intrusione ed Identificazione degli attacchi**, by Raoul Chiesa and Marco 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/>).
 - X25US (<http://www.x25us.net/>).
 - **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
 - The Alt.2600 Hack FAQ - 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 - Written By Blade Runner

Greetings

X.25 gurus

machine

Emmanuel Gadaix

Philippe Langlois

Vanja

Raist

Synack

Raptor

The Force (and the aussie scene)

Friends

Venix

d0

xant

dialtone

naif

rpunk and people at #x.25 (efnet)

Fyodor

The Xfocus team

Jim Geovedi

Anthony Zboralski

Fabrice Marie

Telcos

...just for being there :)

All of the HITB staff

For this great security event.

TSTF Contacts

- **Asia/Far East**

Emmanuel Gadaix

eg@TSTF.net

- **Northern Europe**

Philippe Langlois

pl@TSTF.net

- **Southern Europe**

Raoul Chiesa

rc@TSTF.net

- **North America**

Tony Bannister

tb@TSTF.net

I hope you enjoyed this “nightmare”

Thanks :)

QUESTIONS ?