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 Lampur (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- The X.25 addresses used in the slides can be sometimes real and sometimes fake: in the first case they are out-of-date, else they’ve been used for clear example purposes.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)
• Board of Directors Member:
  – 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 Packet Switched Data Network (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
(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 recomendations (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

- **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

<table>
<thead>
<tr>
<th>Zone</th>
<th>Continent/Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Satellite connections for InmarSAT Voice/Dati(Atlantic, Pacific and Indian oceans)</td>
</tr>
<tr>
<td>2</td>
<td>Europe, Ex URSS</td>
</tr>
<tr>
<td>3</td>
<td>North America, Central America, some Caribbean areas</td>
</tr>
<tr>
<td>4</td>
<td>Asia</td>
</tr>
<tr>
<td>5</td>
<td>Oceania</td>
</tr>
<tr>
<td>6</td>
<td>Africa</td>
</tr>
<tr>
<td>7</td>
<td>Part of Central America, Caribbean and South America</td>
</tr>
</tbody>
</table>
# List of Data Network Identification Codes (DNIC)

(According to ITU-T Recommendation X.121)

(Position on 15 October 2003)

---

<table>
<thead>
<tr>
<th>Data Network Identification Code (DNIC)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNIC 1</td>
<td>Example 1</td>
</tr>
<tr>
<td>DNIC 2</td>
<td>Example 2</td>
</tr>
<tr>
<td>DNIC 3</td>
<td>Example 3</td>
</tr>
</tbody>
</table>

---

*Geneva, 2003*
INDONESIA
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
IRLANDE 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 (INFOISTRADA S.p.A.)
223 6 Trasmissione dati a commutazione di pacchetto X.25 (WIND Telecommunicazioni S.p.A.)
JAPAN/GIAPPONE
JAPON 440 0 GLOBALNET (Network of the Global VAN Japan Incorporation)
JAPON 440 1 DDX-P (NTT Communications Corporation)
JAPON 440 2 NEC-NET (NEC Corporation)
440 3 JENSNET (JENS Corporation)
440 4 JAIS-NET (Japanese 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.)
JAPON 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
### Australian Network Identifiers:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Allocation Date</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>5052</td>
<td>30 June 1991</td>
<td>Telstra Corporation Ltd</td>
</tr>
<tr>
<td>5053</td>
<td>30 June 1991</td>
<td>Telstra Corporation Ltd</td>
</tr>
<tr>
<td>5054</td>
<td>6 September 1994</td>
<td>AAPT Ltd</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>5054</td>
<td>6 September 1994</td>
<td>AAPT Ltd</td>
</tr>
<tr>
<td>5056</td>
<td>16 February 1994</td>
<td>SingCom (Australia) Pty Ltd</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>5056</td>
<td>16 February 1994</td>
<td>SingCom (Australia) Pty Ltd</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>5057</td>
<td>30 June 1991</td>
<td>Fujitsu Australia Ltd</td>
</tr>
<tr>
<td>5057</td>
<td>19 February 1992</td>
<td>Department Of Defence</td>
</tr>
<tr>
<td>5057</td>
<td>17 November 1993</td>
<td>Department Of Defence</td>
</tr>
<tr>
<td>5057</td>
<td>17 November 1993</td>
<td>Department Of Defence</td>
</tr>
<tr>
<td>5057</td>
<td>23 February 1995</td>
<td>Telstra Corporation Ltd</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>313.1</th>
<th>RCAG Telex Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>313.2</td>
<td>Compuserve Network Services</td>
</tr>
<tr>
<td>313.3</td>
<td>RCAG XNET Service</td>
</tr>
<tr>
<td>313.4</td>
<td>AT&amp;T/ACCUNET Packet Switched Capability</td>
</tr>
<tr>
<td>313.5</td>
<td>ALASCOM/ALASKANET Service</td>
</tr>
<tr>
<td>313.6</td>
<td>Geisco Data Network</td>
</tr>
<tr>
<td>313.7</td>
<td>International Information Network Services - INFONET Service</td>
</tr>
<tr>
<td>313.8</td>
<td>FedEx International Transmission Corporation - International Document Transmission Service</td>
</tr>
<tr>
<td>313.9</td>
<td>KDD America, Inc. - Public Data Network</td>
</tr>
<tr>
<td>314.0</td>
<td>Southern New England Telephone Company - Public Packet Network</td>
</tr>
<tr>
<td>314.1</td>
<td>Bell Atlantic Telephone Companies - Advance Service</td>
</tr>
<tr>
<td>314.2</td>
<td>Bellsouth Corporation - Puiselink Service</td>
</tr>
<tr>
<td>314.3</td>
<td>Ameritech Operating Companies - Public Packet Data Networks</td>
</tr>
<tr>
<td>314.4</td>
<td>Nynex Telephone Companies - Nynex Infopath Service</td>
</tr>
<tr>
<td>314.5</td>
<td>Pacific Telesis Public Packet Switching Service</td>
</tr>
<tr>
<td>314.6</td>
<td>Southwestern Bell Telephone Co. - Microlink II Public Packet Switching Service</td>
</tr>
<tr>
<td>314.7</td>
<td>U.S. West, Inc. - Public Packet Switching Service</td>
</tr>
<tr>
<td>314.8</td>
<td>United States Telephone Association - to be shared by local exchange telephone companies</td>
</tr>
<tr>
<td>314.9</td>
<td>Cable &amp; Wireless Communications, Inc. - Public Data Network</td>
</tr>
<tr>
<td>315.0</td>
<td>Globenet, Inc. - Globenet Network Packet Switching Service</td>
</tr>
<tr>
<td>315.1</td>
<td>Data America Corporation - Data America Network</td>
</tr>
<tr>
<td>315.2</td>
<td>GTE Hawaiian Telephone Company, Inc. - Public Data Network</td>
</tr>
<tr>
<td>315.3</td>
<td>JAWS USA-NET Public Packet Switching Service</td>
</tr>
<tr>
<td>315.4</td>
<td>Nomura Computer Systems America, Inc. - NCC-A VAN public packet switching service</td>
</tr>
<tr>
<td>315.5</td>
<td>Aeronautical Radio, Inc. - GLOBALINK</td>
</tr>
<tr>
<td>315.6</td>
<td>American Airlines, Inc. - AANET</td>
</tr>
<tr>
<td>315.7</td>
<td>COMSAT Mobile Communications - C-LINK</td>
</tr>
<tr>
<td>315.8</td>
<td>Schlumberger Information Network (SINET)</td>
</tr>
<tr>
<td>315.9</td>
<td>Westinghouse Communications - Westinghouse Packet Network</td>
</tr>
<tr>
<td>316.0</td>
<td>Network Users Group, Ltd. - VIDI NET packet</td>
</tr>
<tr>
<td>316.1</td>
<td>United States Department of State, Diplomatic Telecommunications Service - Black Packet Switched Data Network</td>
</tr>
<tr>
<td>316.2</td>
<td>Transaction Network Services, Inc. - TNS Public Packet-switched Network</td>
</tr>
<tr>
<td>316.3</td>
<td>U.S. Department of Treasury Wide Area Data Network</td>
</tr>
</tbody>
</table>

**DNICs -3**

Data carriers

Multinationals

Spy Game ? ;)

The U.S.A. case
## DNICs - 4

The Malaysia case

<table>
<thead>
<tr>
<th>Country</th>
<th>Code</th>
<th>Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MALAISIE</td>
<td>502 0</td>
<td>COINS Global Frame Relay</td>
</tr>
<tr>
<td>MALAYSIA</td>
<td>502 1</td>
<td><strong>Malaysian Public Packet Switched Public Data Network (MYPAC)</strong></td>
</tr>
<tr>
<td>MALASIA</td>
<td>502 3</td>
<td>Corporate Information Networks</td>
</tr>
<tr>
<td></td>
<td>502 4</td>
<td>ACASIA-ASEAN Managed Overlay Network</td>
</tr>
<tr>
<td></td>
<td>502 5</td>
<td>Mutiara Frame Relay Network</td>
</tr>
<tr>
<td></td>
<td>502 7</td>
<td>Mobile Public Data Network (WAVENET)</td>
</tr>
<tr>
<td></td>
<td>502 8</td>
<td>Global Management Data Services (GMDS)</td>
</tr>
</tbody>
</table>
022221122878
\1 /\ |_/ \ 22878: Network Port Address (NPA)
\1 | | | | | 11: Area Code for Torino
\1 | | | | | | 2: ITAPAC Network (more networks)
\1 | | | | | | | 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.

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

<table>
<thead>
<tr>
<th>PRFX NUMBER</th>
<th>AREA CODE</th>
<th>PRFX NUMBER</th>
<th>AREA CODE</th>
<th>PRFX NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>399</td>
<td>(311) 437</td>
<td>(311) 767</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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**: 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 if 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”

<table>
<thead>
<tr>
<th>SEND</th>
<th>DEST</th>
<th>STATUS</th>
<th>SUBJECT</th>
<th>DELIVERY</th>
<th>TIPO</th>
<th>IDE</th>
<th>SIZE</th>
</tr>
</thead>
</table>
SMS Processing que (!)
SMS sniffing (in real time !)
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

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

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% ONLY.**
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

<table>
<thead>
<tr>
<th>NETWORK #</th>
<th>NAME / ORGANISATION</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>404100000162</td>
<td>A C C</td>
<td>WADI</td>
</tr>
<tr>
<td>404100010681</td>
<td>A C C</td>
<td>BILASPUR</td>
</tr>
<tr>
<td>404100000589</td>
<td>A C C</td>
<td>BOMBAY</td>
</tr>
<tr>
<td>404100000381</td>
<td>A C C</td>
<td>CHAIKASA</td>
</tr>
<tr>
<td>404100000555</td>
<td>A C C</td>
<td>JAMUL</td>
</tr>
<tr>
<td>404100000420</td>
<td>A C C</td>
<td>KYMORE</td>
</tr>
<tr>
<td>404100010162</td>
<td>A C C</td>
<td>WADI</td>
</tr>
<tr>
<td>404100010589</td>
<td>A C C</td>
<td>BOMBAY</td>
</tr>
<tr>
<td>404100010626</td>
<td>A P RAYONS</td>
<td>KAMALAPURA</td>
</tr>
<tr>
<td>404100010625</td>
<td>A P RAYONS</td>
<td>HYDERABAD</td>
</tr>
<tr>
<td>404100000172</td>
<td>ANAND BAZAR PATRIKA</td>
<td>BOMBAY</td>
</tr>
<tr>
<td>404100010882</td>
<td>ANAND BAZAR PATRIKA</td>
<td>CALCUTTA</td>
</tr>
<tr>
<td>404100000362</td>
<td>ANAND BAZAR PATRIKA</td>
<td>NEW DELHI</td>
</tr>
<tr>
<td>404100010172</td>
<td>ANAND BAZAR PATRIKA</td>
<td>BOMBAY</td>
</tr>
<tr>
<td>404100000821</td>
<td>B A R C</td>
<td>BOMBAY</td>
</tr>
</tbody>
</table>
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:

\[
\text{<AMSS airborne address>} :: \text{<DNIC>} \text{‘}5\text{’} \text{<AES>} > \text{<D>}
\]

\[
\text{<DNIC>} :: \text{‘}1111\text{’} (\text{AOR-E satellite}) \text{ or ‘}1112\text{’} (\text{POR satellite}) \text{ or ‘}1113\text{’} (\text{IOR satellite}) \text{ or ‘}1114\text{’} (\text{AOR-W satellite})
\]

\[
\text{<AES>} :: 8\text{-digit BCD-encoded 24-bit address of aircraft}
\]

\[
\text{<D>} :: \text{Optional subaddress digit}
\]

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:

\[
\text{<AMSS ground address>} :: \text{‘}26\text{’} \text{<DNIC>} \text{<NTN>}
\]

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

\[
\text{<NTN>} :: \text{Up to 9\text{-digit network terminating number \textbf{(DTE network address)} of the air/ground router on the provider’s network identified by the ASNID.}
\]

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.

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..VHGH.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'LS+*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
  - 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 ?