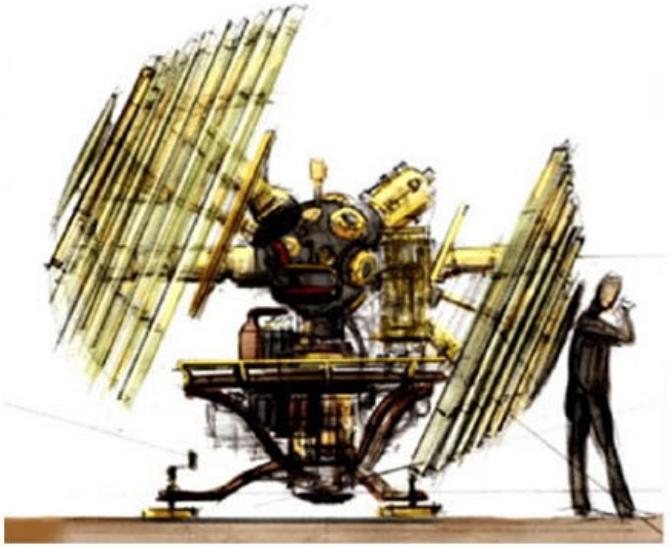
The Wayback Machine
Old School Hacking



Júlio César Fort
julio@rfdslabs.com.br

Agenda

Main Goals

War Dialing: The Search for Protovision

X.25: Playing Around With Packet Switched Networks

Dumpster Diving

Social Engineering and Password Guessing

Acknowledgements, References and Links

Conclusions

Questions

Main Goals

Main Goals

- Approach forgotten topics regarding computer security
- Satisfy nostalgic guys with old school tricks
- Make hackers and system administrators happy with real incident stories
- Show that so-called obsolete techniques still work nowadays with little or no modification
- Demonstrate the same weak links of 25 years ago still exist

War Dialing: The Search for Protovision

What is war dialing

- Automated process of calling blocks of phone numbers
- Dialing can be sequential or random
- Its main purpose is to find modems on the other end of the line
- Considered obsolete since early 1990's

Brief history

- Initially used to look for PABXs with default passwords
- Phone scanning became a phenomenom after the 1983 movie “War Games”
- The favourite game of ancient hackers
- “Hardcore” phreaking is a direct consequence of war dialing

Legal questions and more

- In some states of the USA this practice is considered crime
- Apparently in Brazil there is no law to forbid it

  Who the hell cares, anyway? :)
- War dialing itself cannot be considered disturbance or harassment

- Advanced phone switches are able to detect scanning

Famous incidents

- Slingshot for Yahoo! defacement in 1997

  Bring BoW and h4g1s back!

- Worcester County airport and nearby residences communications cut off in 1997
- Unauthorized access to high-voltage power management systems in Oakland, CA

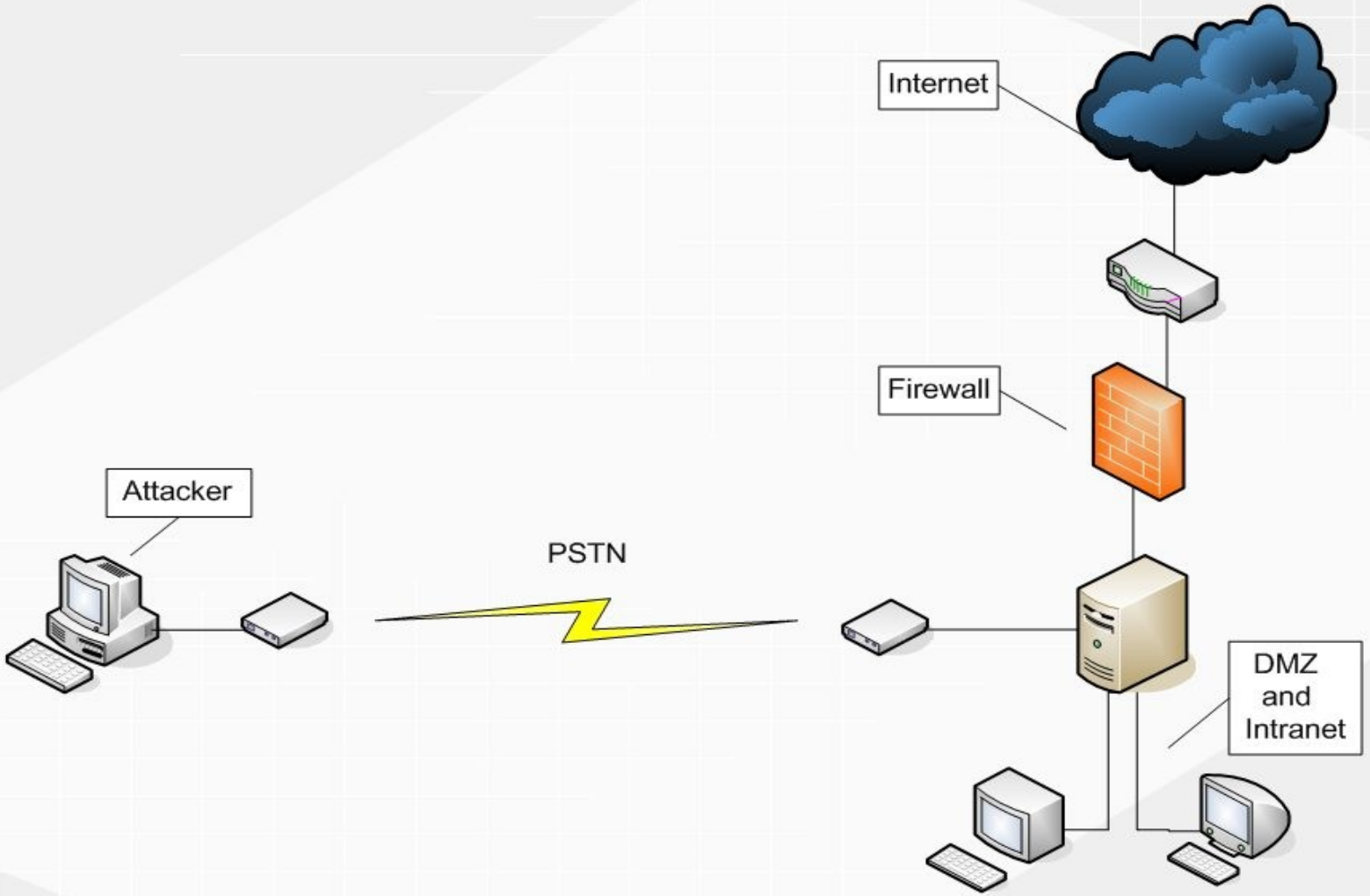
War dialing in Brazil – Tools and hardware

- Tools
  - ToneLoc 1.10 by Minor Threat and Mucho Maas
  - Telemate 4.21 by White River Software
- Hardware
  - Athlon XP 1700+ with Windows (XP)
    - But a 486 DX2 with MS-DOS could do the same task
  - Analog phone line
  - US Robotics Courier V.Everything 56k external

War dialing in Brazil - Methodology

- Service changed to minute-charged rate – provided free calls from 12 a.m. to 6 a.m.
- Common numbers had **20 seconds** timeout and 3 maximum rings
- Toll-free numbers had a timeout of **40 seconds** and 5 as ring out
- Maximum dialing speed was set for common numbers
  - Toll-free had dialing speed slowed down a bit

An attack scenario

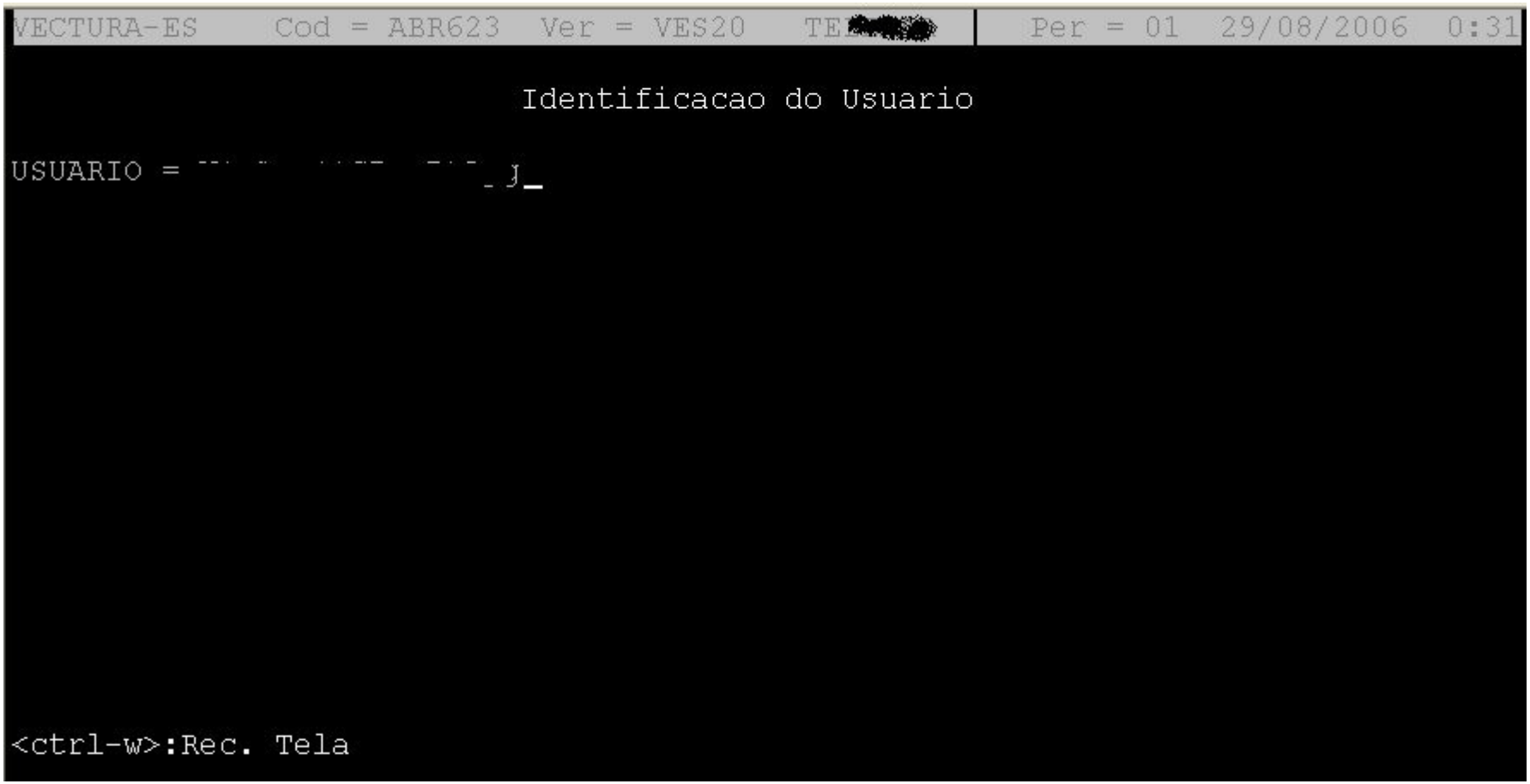


Some results

- Wide open routers and PPP connections
  - Most of them did not require authentication
    - Some of them led **straightforward to internal networks**
- Phone switches, faxes and other telephony goodies
- Login prompts
  - One was particulary very interesting: a state-runned lottery
- Even a BBS!

A picture is worth a thousand words

- Toll-free line controller telephone switch



No intrusion techniques were performed on this system

Why it is still a threat

In many cases is possible to find:

- Telnet-like prompts
- Telephone switches
- Dial-up servers with weak passwords
- Voicemail boxes
- Unattended legacy systems
- Misconfigured routers
- Faxes, PABXs and ISDN modems
- Internal computers not reachable from the Internet
- Confidential internal numbers

Future trends

- VoIP-based war dialing tools
  - iWar, by Beave
  - SkypeDiver, by legi0n
- Scanning digital lines with ISDN devices
  - tmap, by Immutec GmbH
  - PAWS, by wyae.de

Countermeasures

- Do not allow unknown numbers dial into your modems
- Record all incoming connections
- Turn on dial-back feature on modems that support it
- Some features in PABXs can detect scanning
- Use the most mysterious banners or remove them
- If there is really the need to leave modems available to everyone, make sure your passwords are strong

X.25: Playing Around With Packet Switched Networks

What is X.25

- X.25 is a set of protocols developed in 1964 by Rand Co. for packet switched networks
- Similar to the model used in PSTNs
- Was the first kind of network to reach global scale
  - Lost popularity when Internet went mainstream
- Still in use by large corporations and governments

Basic information

- Communication based on circuits
  - They can be permanent or switched
- Protocol is connection-oriented
- Each subscriber is assigned to a NUA (network user address), unique or with logic channels
- NUI is equivalent to user/password pair on dial-up connections on X.28 PADs

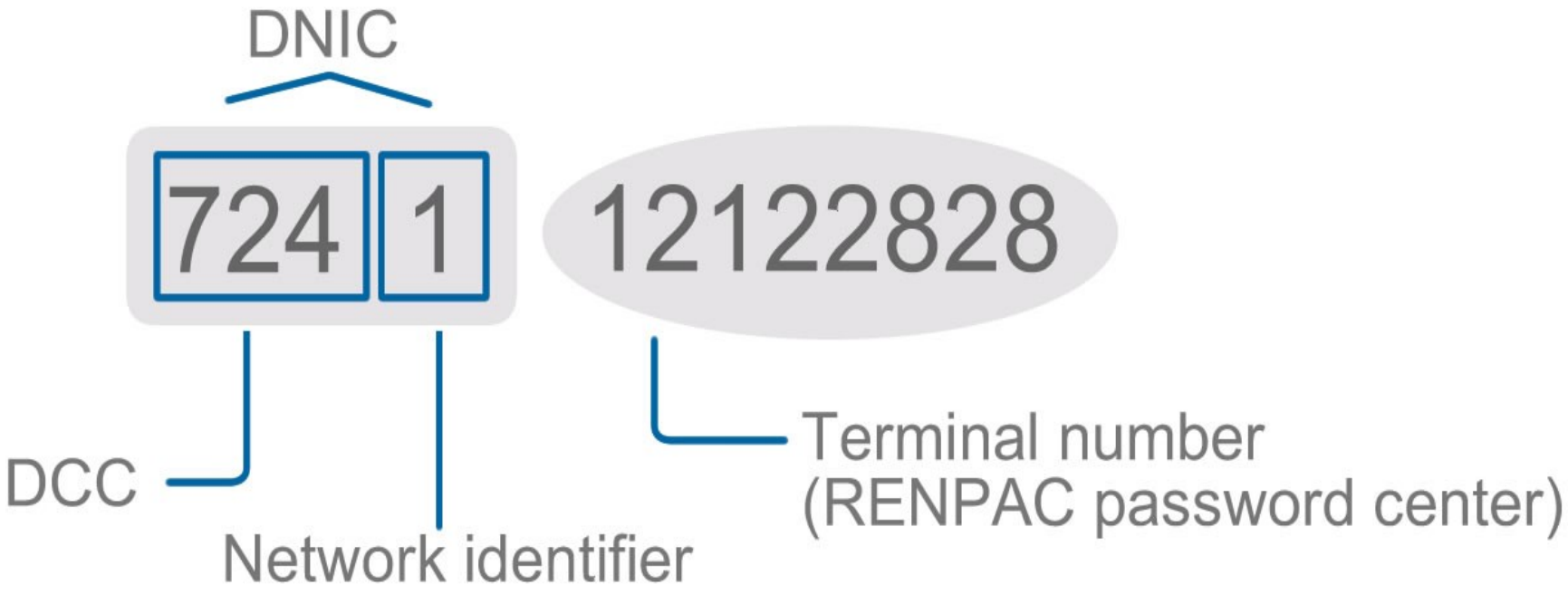
Basic information

- Billing is based on the amount of traffic transfered
  - Reverse-charge is allowed under some circumstances
- Maximum transmission speed is 64kbps
- Maximum frame length is 128 bytes
- To dial into nodes belonging to other networks, one must prepend a “0” or “9” before entering the NUA
- User facilities provide reverse charging, mnemonics, etc.

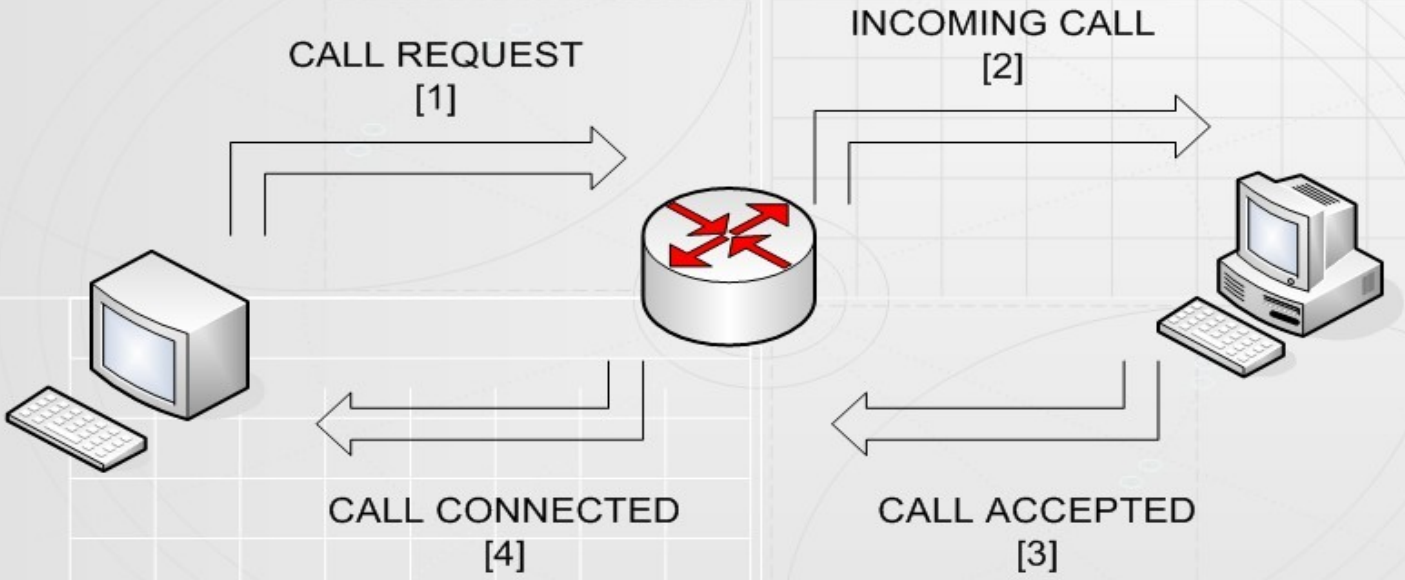
Network elements

- Data Terminal Equipment (DTE)
  - The end-point of the network
- Data Circuit-terminal Equipment (DCE)
  - Equipment used in the actual communication
- Packet Assembler/Disassembler (PAD)
  - A full-featured protocol converter

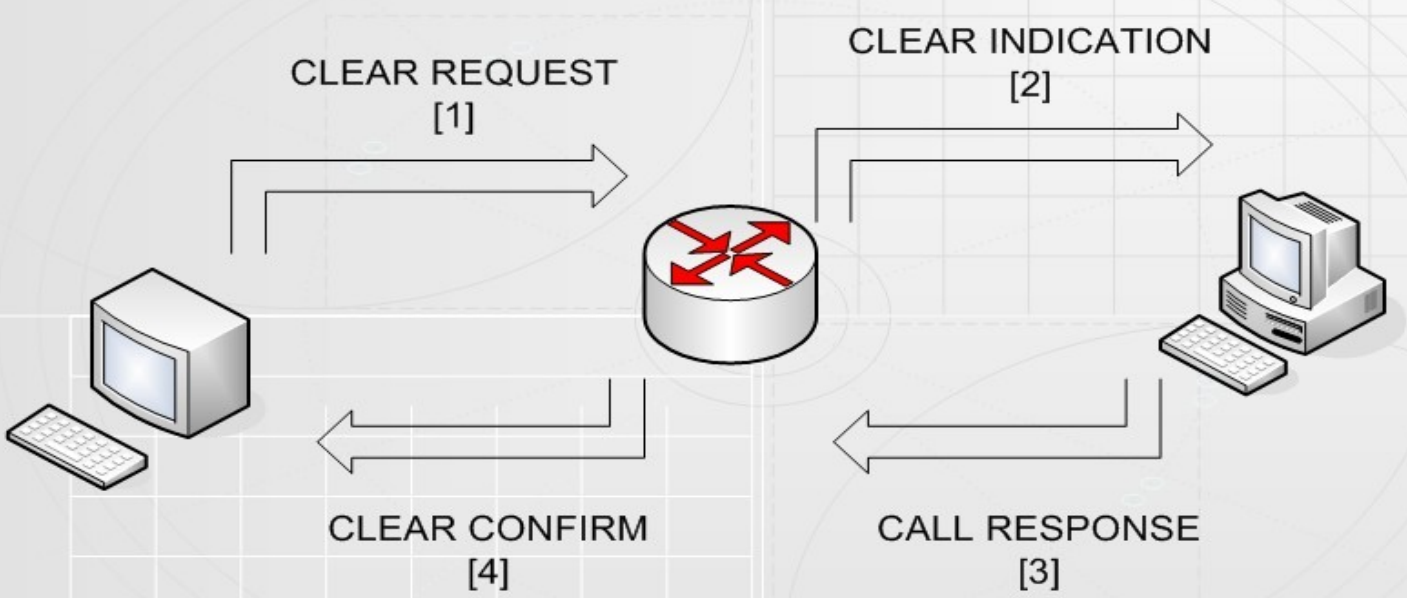
X.121 addressing format



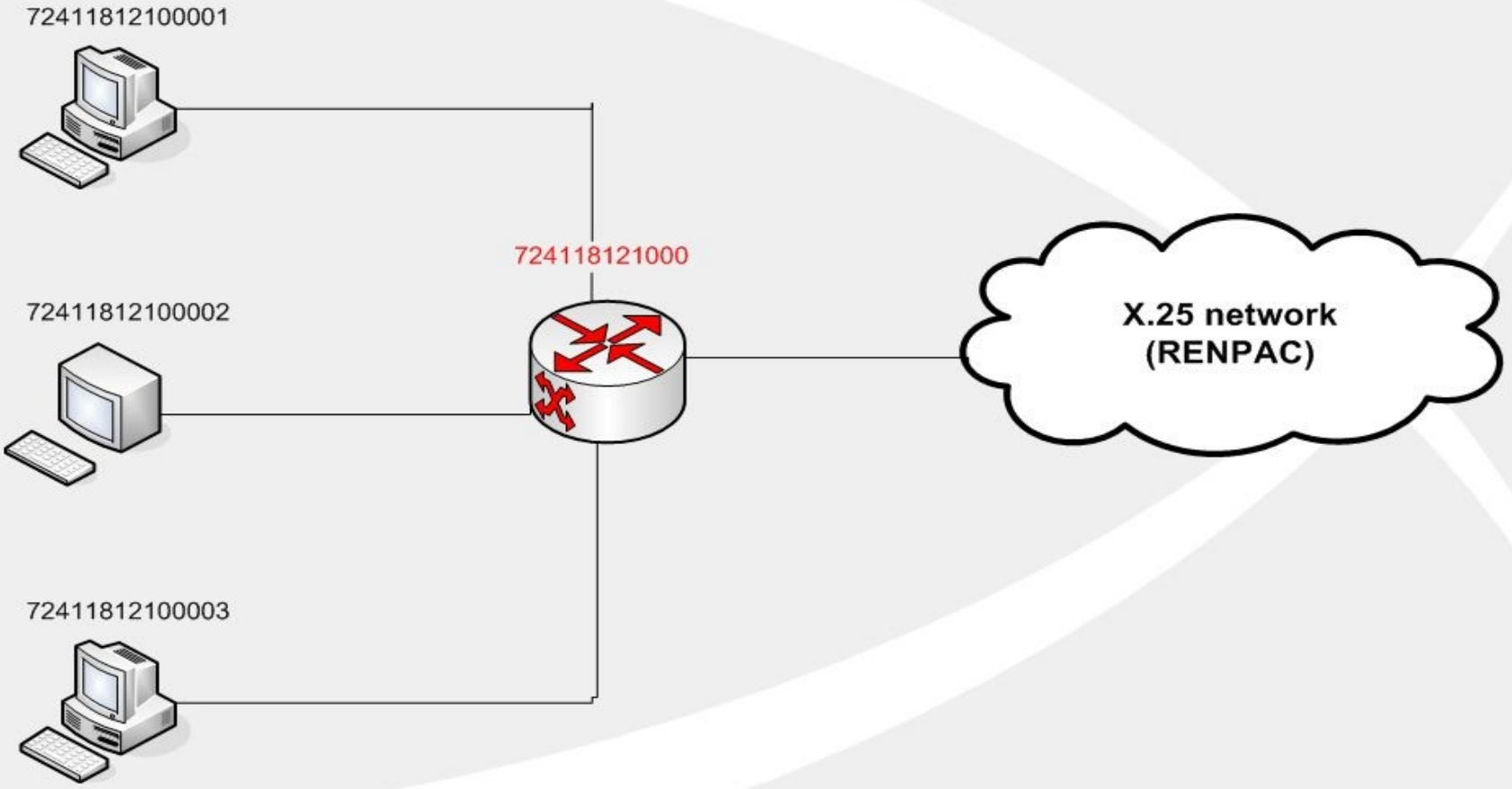
Call setup


CALL REQUEST
[1]
INCOMING CALL
[2]
CALL CONNECTED
[4]
CALL ACCEPTED
[3]

Call clearing



Subnetting


72411812100001
72411812100002
72411812100003
724118121000
X.25 network
(RENPAC)

X.28 PAD messages

CODE	DESCRIPTION
CLR OCC	Busy
CLR INV	Invalid request facility
CLR RNA	Does not accept reverse charge
CLR NC	No circuits
CLR NA	Access baried
CLR NP	No port
CLR RPE	Remote procedure error
CLR ERR	Local error
CLR DTE	Disconnected by the other end

How to access PSNs

- Leased lines
  - Direct connection to an X.25 PAD
  - Always identified with a NUI
- Public dial-up access
  - Dial into an X.28 PAD
  - Can be identified or not
- X.25 over IP (XoT – RFC 1613)
  - In theory router's XoT capabilities are reached from the Internet
  - Security is lax: no authentication required

Security considerations on X.25 networks

- Threats to PSNs have been neglected for years
- Security aspects were not evolved in the days of its peak of popularity

Network tapping

- Information traversing networks are subject to many types of attacks
- Data eavesdropping and forgery can be applied to nearly every network medium
- There are tools to perform sniffing on X.25 networks

NUI brute-forcing

- To travel through all the networks, including international ones, an attacker must have an identified access
- Brute-force attacks are noisy, yet the most reasonable manner to 'hack' NUIs

- NUI crackers
  - THC's LoginHacker
  - x25bru.c by in0de
  - ... or act like a punk and do it yourself!

X.25 hacking

- Scanning for valid NUAs is the most popular way of finding potential targets
  - Tools
    - ADMx25, by antilove
    - Vudu, by Marco “raptor” Ivaldi
    - dscan, by Beave and jfalcoon (for Datapac and Sprintnet)
- Guessing mnemonics names are quite popular as well
- Exploitation concepts are different, but things seems to be changing...

Countermeasures

- Disable reverse-charging; it can slow down some attackers, but not all of them
- Encrypt your X.25 connection
- Enable Closed User Group on your network
- Remove banners or use a very mysterious one
- And the omnipresent recommendation: Make sure your passwords are not weak

Future trends

- It is possible to perform NUA spoofing through XoT
- Exploitation concepts supposedly not to work on X.25 networks became reality now (i.e. Solaris /bin/login buffer overflow)
  - Both shown by Raoul Chiesa on his latest presentation

Why it is still a threat

- Due to its lack of popularity security is often neglected
- Some critical infrastructure coordination systems are accessible through X.25
- Most of attackers playing around these networks are not ordinary script kiddies

Dumpster Diving

Dumpster diving (trashing)

- The art of rummage through trash cans looking for valuable information
- It is possible to find internal memos, documents, manuals, etc.
- Although forgotten, has been used by hackers and urban explorators

  > "revolviendo basura juntando lo que este sistema dejo para mi (...) y a ver si se bancan vivir mi vida de cartonero."

- Paper shredding is the best countermeasure against it
- "Sometimes, the greatest treasures are found beneath piles of trash"

Social Engineering and Password Guessing

Old tricks for a new dog

- Social engineering is nothing but tricking someone to do something in your favor
- Human factor plays a key role on computer security as well
- Widely used by hackers but also by fraudsters and ordinary criminals
  - Social engineering was fundamental on most of Mitnick's and Poulsen's hacks, for instance

Conclusions

Conclusions

- Forgotten hacking techniques may look outdated and inefficient...
- ... however, after thousands of telephonic pulses, this presentation showed it is not true
- There are still many mission-critical systems lying around on “obscure” networks
  - And most of them are legacy systems left unattended for years and supposed to be secure because of its “isolation”
- Old school hacking is still not only **simple** but amazingly **effective**
- Dust off your modem and go hack, kid!

And listen to Michael Jackson while watching The Goonies with a Dip 'N Lik lolypop

Acknowledgements, References and Links

Acknowledgements

- Saludos a los hermanos en Ekoparty staff
- **Attaque 77** for being the inspirational soundtrack

  Vamos, vamos, mira cuanta cerveza que hay allí
- Marvin Madson (mmadson.com) for designing the slides
- Rodrigo Branco, Domingo Montanaro, Filipe Balestra and H2HC guys
- Lazy bastards of The Bug! Magazine staff and former members of rfdslabs and gotfault
- Mark “Phiber Optik” Abene
- Iruatã Souza and Paolo Oliveira for **keeping the old school alive**
- Blubbers: Robert Connolly, Júlio Auto and Tiago Assumpção
- Raoul Chiesa for sharing some ideas with me and his great paper and presentations on X.25 security

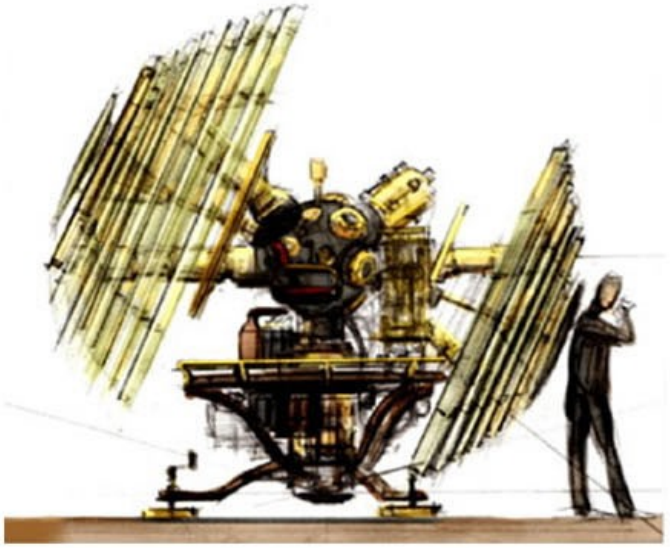
Special thanks to you for your patience. Muchas gracias!

References and links

- Shipley, P. and Garfinkel, S. (2001) “An Analysis of Dial-Up Modems and Vulnerabilities”
- Powell, D., Schuster, S. and Amoroso, E. “Local Area Detection of Incoming War Dialing Activity”
- Chiesa, R., Ivaldi M. (2002) “I Network X.25 – Comprensione della struttura di rete, Tecniche di attaco ed Identificazione delle intrusioni”
- Clark, A. (1988) “Data Security in X.25 Networks”
- Esko (2004) “Austpac X.25 Network Guide”
- Cyb0rg, Asm, (1999) “Complete Guide to AGNPAC v2.0”
- oldskoolphreak.com
- binrev.com/forums

Questions?

The Wayback Machine
Old School Hacking



Júlio César Fort
julio@rfdslabs.com.br