

# Immersed Network Discovery and Attacks

Specifics of Telecom Core Network (CN) insider attacks

Philippe Langlois  
Telecom Security Task Force  
[Philippe.Langlois@tstf.net](mailto:Philippe.Langlois@tstf.net)  
<http://www.TSTF.net>

# Speaker Introduction

- [ 15 years in security
- [ Background as entrepreneur (Security consulting group, ISP, professional software, ASP)
- [ Founded Qualys, worldwide leader in vulnerability assessment ASP
- [ Founded Telecom Security Task Force 7 years ago, research forum.

# Agenda

— [ **Necessity is mother of invention, what about BIG PROBLEM?**

— [ New tool

— [ Actions

— [ Information access

— [ Demo

— [ CN Specifics

# Story of an SS7/SIGTRAN Pentest

- [ Asia, multi-perimeter (Internet, GPRS, WLAN, Internal)
- [ Root on the Internet segment
- [ Root on some MMS/SMS gw
- [ Shared usage of same passwords
- [ Guess it was going to be easy

# WRONG!

- [ Incredibly well segmented
- [ Excellent default firewall rules
- [ Not possible to get on CN
- [ Not the necessary tools
- [ Needed much more time to complete!

# Guess we needed something stronger

- [Multi-perimeter attacks
- [Permanent “on-watch” firewall monitoring
- [Pervasive & resilient way to communicate
- [Distributed attack stations

# Agenda

- [ Necessity is mother of invention, what about BIG PROBLEM?
- [ **New tool**
- [ Actions
- [ Information access
- [ Demo
- [ CN Specifics

# Introducing Barung



- [ Doesn't replace any tool

- Works on standard BackTrack ;-)

- Uses Metasploit

- Can use nmap / scanrand / ...

- [ Fast parallelization

- [ Easy to add attacks / behaviour

# New way to see / modelize

- [ Perspective-based scanning
- [ Inference-based expert system, module based
- [ Immersed behaviour
- [ Presence-based collaboration (Telepathy)
- [ Collaborative information database

# Technology

- [ Ruby command line tool (1500 lines of code)
- [ Interfaced to many external (C?) tools
- [ YAML datastore
- [ 1 file per module / information type
- [ dynamic loading i.e. `class_for_name()`

# Agenda

- [ Necessity is mother of invention, what about BIG PROBLEM?
- [ New tool
- [ **Actions**
- [ Information access
- [ Demo
- [ CN Specifics

# Perspective based

- [ Perimeters heterogeneity
  - Internet, VPN, WLAN, GPRS-HSCSD APNs, X25, SS7-SIGTRAN, VLANs, ...
- [ Firewall perspective
- [ Per participant GUID
- [ Anonymity of participant, changeability of GUID (TOR?)

# Inference scans

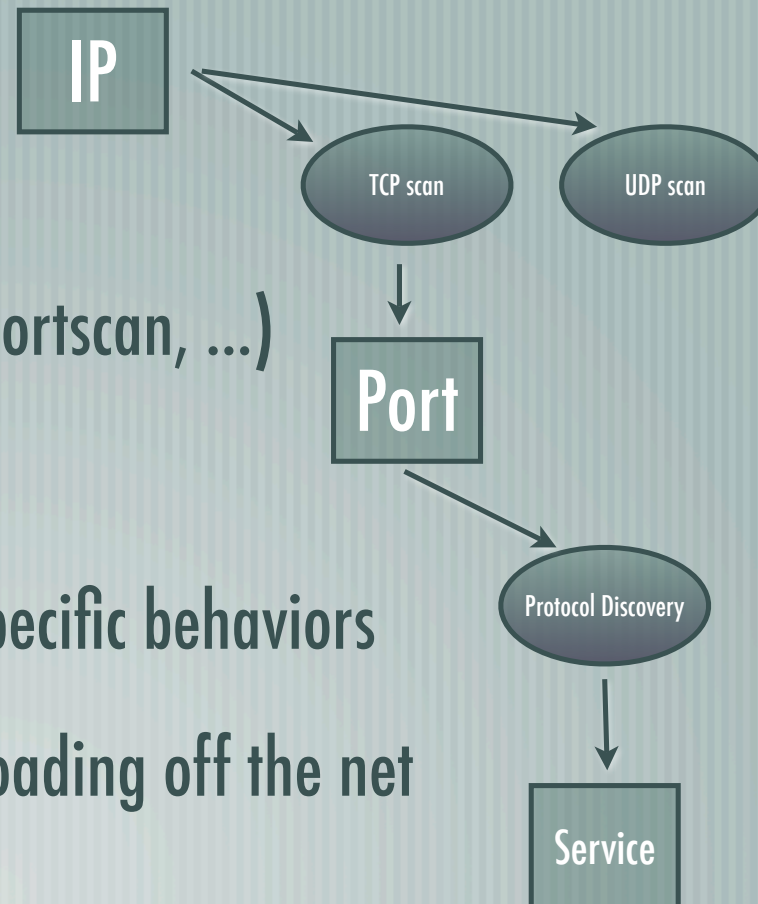
[ Informations (IP, Ports, ...)

[ Actions as Modules (enum, portscan, ...)

[ Inference process (Kernel)

[ Enable / Disable lists for specific behaviors

[ Barong online service, dyn loading off the net



# Informations & Modules

## — [ INFOs

— INFO\_defaultroute.rb INFO\_host.rb INFO\_immersed.rb INFO\_interface.rb  
INFO\_iprange.rb INFO\_iproute.rb INFO\_potentialiproute.rb  
INFO\_quietimmersion.rb INFO\_selector.rb ...

## — [ Modules

— MOD\_defaultroute.rb MOD\_internalrouting.rb MOD\_tcpscan.rb  
MOD\_dnsenum.rb MOD\_protocol\_discovery.rb ...

# Parallelization

- [ Thread based on modules runs

- Scan efficiency

- Duration

- Harshness?

- [ Number of thread organically set

- [ Dynamic adjustments on qualitative response measurements

# Pivoting

- [ Plenty of existing techniques
  - Syscall proxying? ala CORE IMPACT
  - Custom API? ala Random win32 backdoor
- [ Simpler Approach
  - Shell-based (telnet api / expect / ...)
  - SSH based

# Agenda

- [ Necessity is mother of invention, what about BIG PROBLEM?
- [ New tool
- [ Actions
- [ **Information access**
- [ Demo
- [ CN Specifics

# Information Storage

— [ Filesystem

— [ YAML

— [ Database

— [ > PersisterConverter

```
Terminal — bash — tty3 — %1
philippe-langlois-computer:~/Documents/work/barung philippelanglois$ head defau
---
85373eae2a99693e0469a91c110f15e0957989f3: |ruby/object:INFO_host
address: 18.2.1.3
data: {}

datefound: "2008-03-08T21:16:32+01:00"
hash: 85373eae2a99693e0469a91c110f15e0957989f3
perspectiveid: 1
8f33fe71918d2478860d015a85525505a5825327: |ruby/object:INFO_host
address: 17.1.8.4
philippe-langlois-computer:~/Documents/work/barung philippelanglois$
```

# Information sharing

— [ Email (s/mime)

— [ SVN

— [ Tor support / hidden services

— [ Telepathy / DRB

# Information access

- [ File-system
- Flat files
- [ Web-based Rails app?

# Reporting

- [ Raw results
- [ Remaining work
  - Statistical data
  - Graphical representation
  - Executive Presentation

# Analysis, Prioritization and Decision making

- [ Ignore list
- [ Comments
- [ Ranking / Ticket management interface

# Blah blah blah

- [ Didn't we start getting into fluffy markety things?
- [ Isn't it a tech conference?
- [ Ok, DEMO!

# Agenda

- [ Necessity is mother of invention, what about BIG PROBLEM?
- [ New tool
- [ Actions
- [ Information access
- [ Demo
- [ **CN Specifics**

# How does that mix with CN attacks?

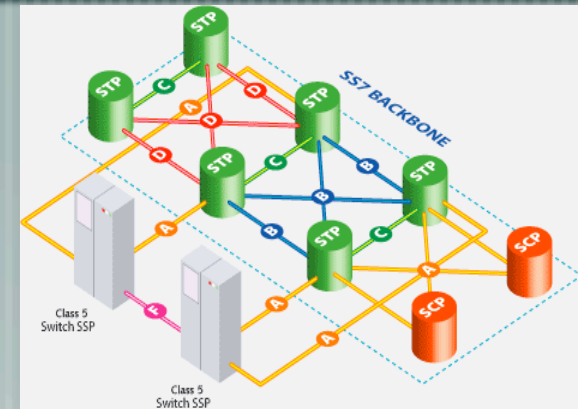
Immersed, exploded walled garden

Multi-perimeter, Multi-protocol

Internet, VPN, WLAN, GPRS-HSCSD APNs, X25, SS7-SIGTRAN, VLANs, ...

Total unknown, very often proprietary systems

Lots of specific network setups



# Specific answers to telco pentest

- [ First: Easy to develop new modules, needed onsite
- [ Fast grasp of net / situation
- [ Interface with SCTPscan and other TSTF tools for SS7 & SIGTRAN
- [ SSH based pivoting
- [ Pivot-based tools

# Easy development

- [ Weird VoIP extension to SIP sniffed?
- [ Need for SIP-embedded SS7 data scanning / fuzzing?
- [ SIGTRAN stack on HPUX or Solaris?
- [ MMS software suite on dedicated hardware?
- [ IMS equipment on open unix platform?

# Fast Grasp

Huge networks

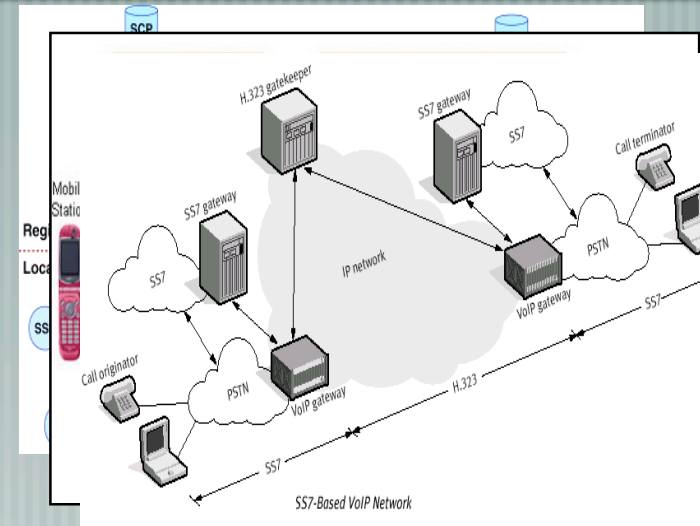
Redundant RFC1918 address spaces

Heavily segmented into N planes

equal N times the same mapping / scanning

Make some pentest undoable by hand

Use of automated scanner?



# Interface with SCTPscan

- [ First Protocol layer for SS7 adaptation over IP
- [ Tool released earlier
- [ Command line based
- [ Act as nmap for ASPs on SIGTRAN

# SCTP Association: 4-way handshake, not stealth

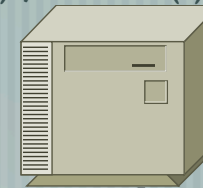
**Client**

`socket(), connect()`



**Server**

`socket(), bind(), listen(), accept()`



INIT

INIT-ACK

COOKIE-ECHO

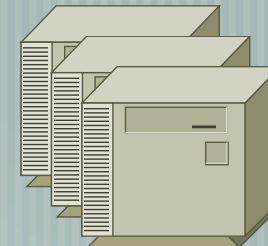
COOKIE-ACK

# Scanning vs. Stealth Scanning

Attacker



Servers



INIT

INIT

INIT

INIT-ACK

~~Port 100~~

~~Port 101~~

Port 102

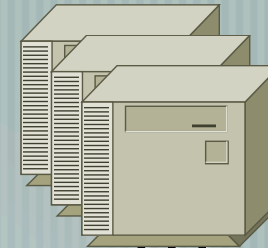
Closed? Packet loss? Delay? Re-xmit?

# Scan against current implementation

Attacker



Servers



INIT

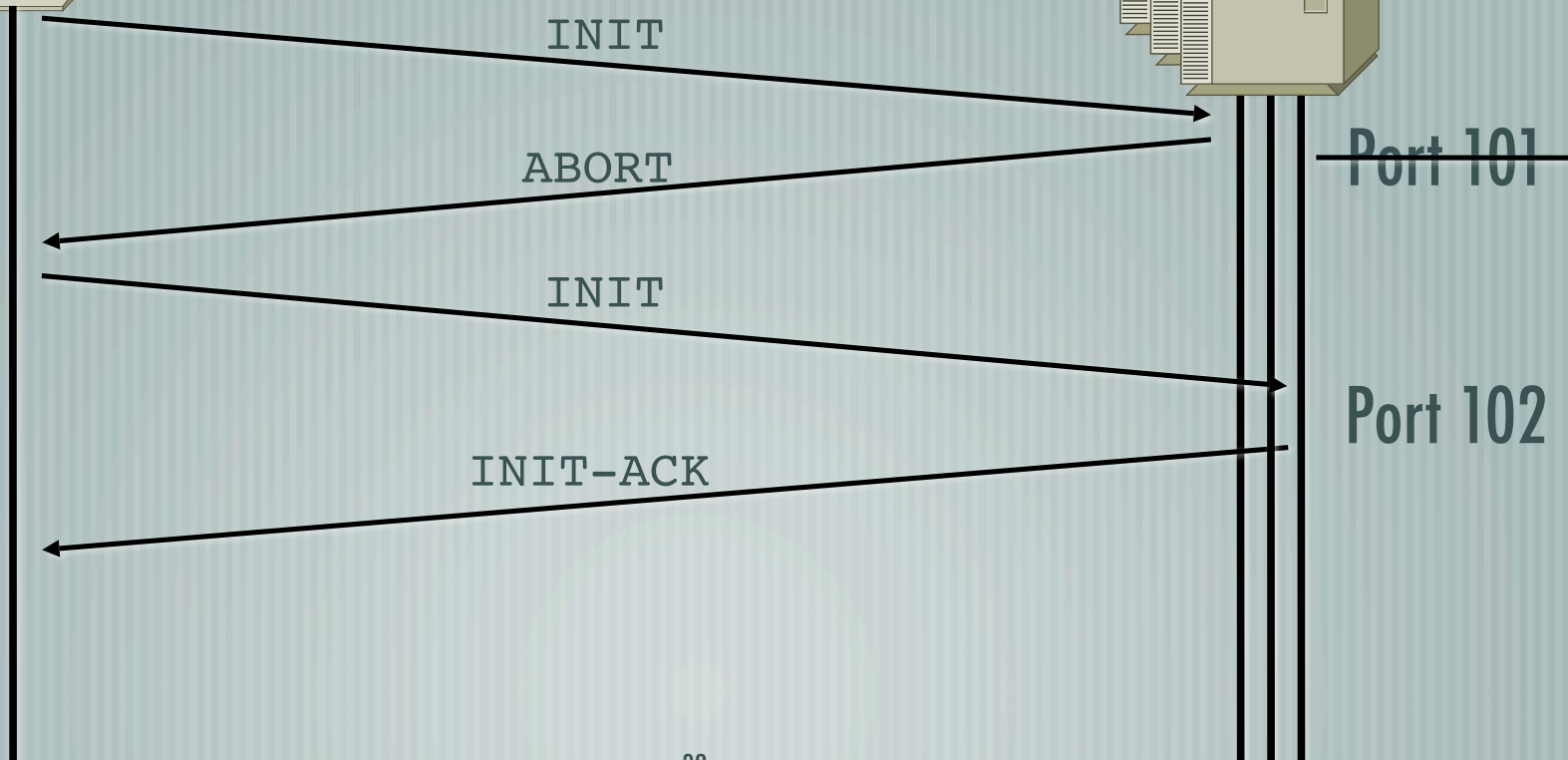
ABORT

INIT

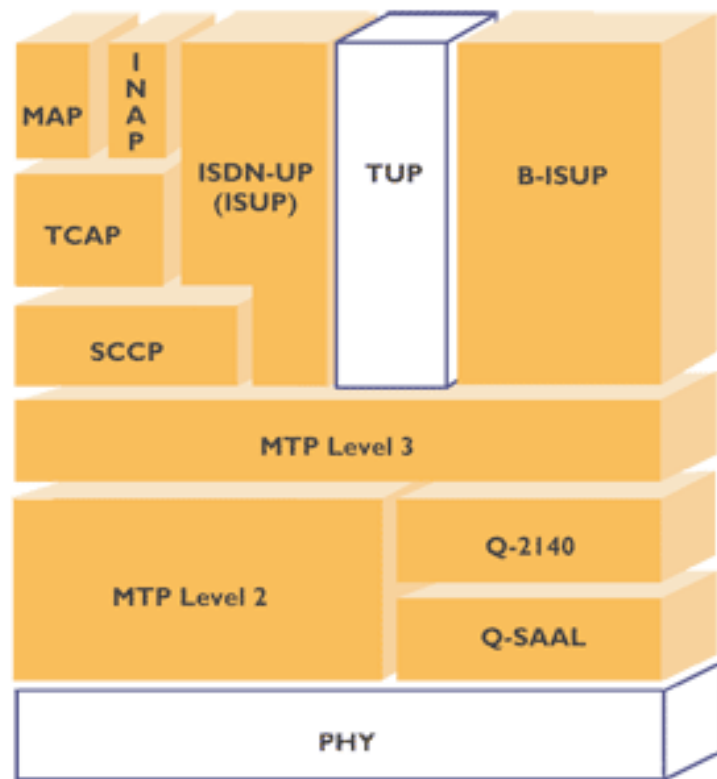
INIT-ACK

Port 101

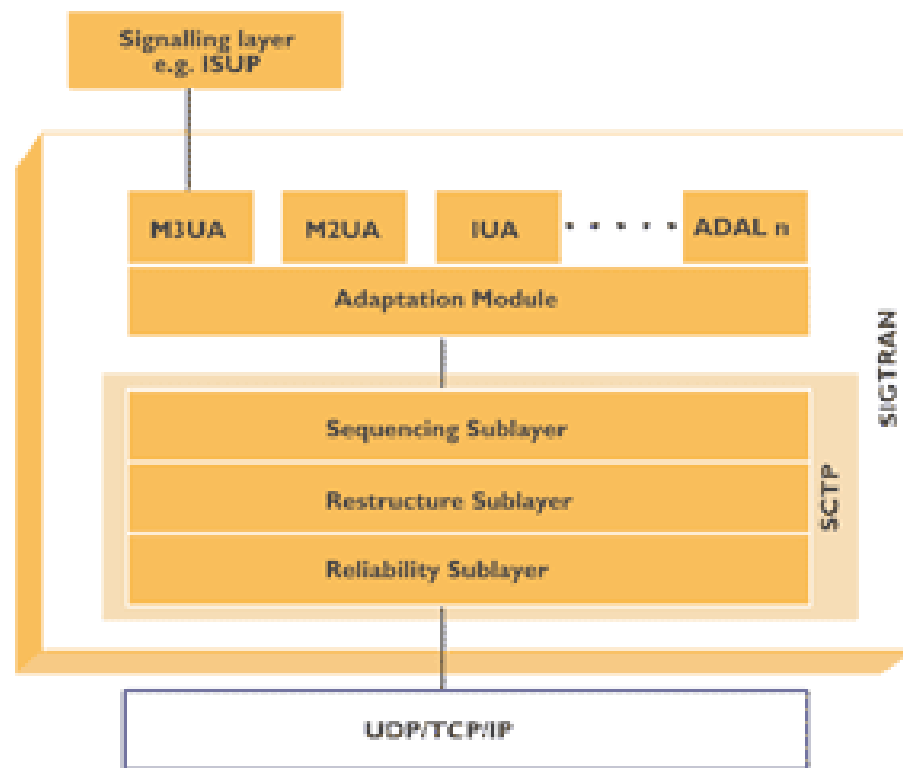
Port 102



# Other SIGTRAN Layers, other tools



SS7



SIGTRAN

# Barung CN modules coding

- [ Proprietary command-line tools
- [ Proprietary binaries
- [ Proprietary protocols
- [ Downtime unacceptable

# Entry point specificities

- [ SIGTRAN ASPs
  - Defined Peers
  - Abusing “Authorized” peers
  
- [ SIP & H323
  - Signalling information injection
  - Not direct SIGTRAN attacks
  
- [ Other weirdness
  - MML injection
  - Internet Messaging to SMSC / MMSC
  - OTA signalling attacks

# CN == unknown environment all the time

- [ Need for a way to generically find SS7 / SIGTRAN entry points

- [ Echelon lesson

- Let the dictionary be the key (M2PA, M3UA, DPC, OPC, MML, TCAP, ISUP, LINKSET, ...)

- [ Module

- Host based key-word search for SS7 / SIGTRAN related terms

- SSH pivoting, dev time, adjustment time

# Status & Conclusion

- [ alpha alpha alpha
- [ Very useful in CN pentests now! In other environments?
- [ Capitalize on every mission
- [ Need to test in multitude of environment
- [ If you want to participate, come after the conference.

# Q & As

— [ Go ahead...

# Thanks

— [ [Philippe.Langlois@tstf.net](mailto:Philippe.Langlois@tstf.net)

— [ See you at Hacker Space Fest in Paris, 16 to 22 June 2008,  
<http://www.hackerspace.net>