Case Study of SS7/SIGTRAN Assessment

Akib Sayyed

akibsayyed@matrixshell.com

About Me

- Work as Telecom security consultant
- Loves telecom
- Presented in conferences like nullcon ,c0c0n

Key problems in SS7

- Every network we are connecting to is trusted network
- Only operators will have access to SS7 network
- One cannot enter ss7 network easily
- So
  - While designing no security was defined other than filtering at point code level / STP level
  - No authentication

possible entry points to ss7

- VAS service provider
- SS7 Interconnection
- GSM phones
- Signalling Gateways, MGW
- Peer relationships between operators
- SIP encapsulation(ISUP)

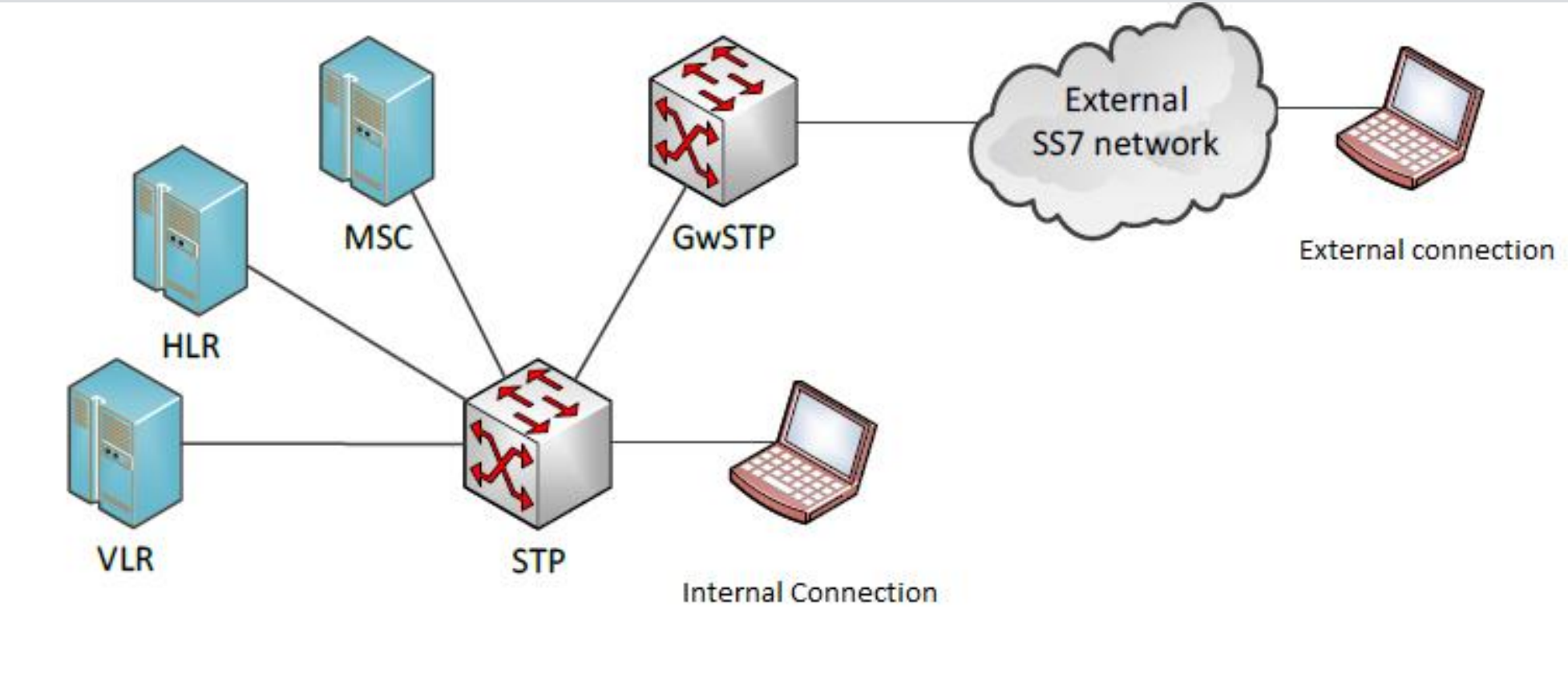
When we started penetration testing for operators

- Convincing operator that attacks exist was difficult
- Is it going to be destructive testing or just vulnerability assessment?
- If its destructive testing don’t touch my network you can test on testbed
- How it will affect my subscribers ?
- Don’t try DOS attacks

Our method for scanning ss7 - 1

- Interconnection from either perimeter
  - Internal
    - Connecting to operators network from his own network
  - External
    - Connecting via roaming partners network

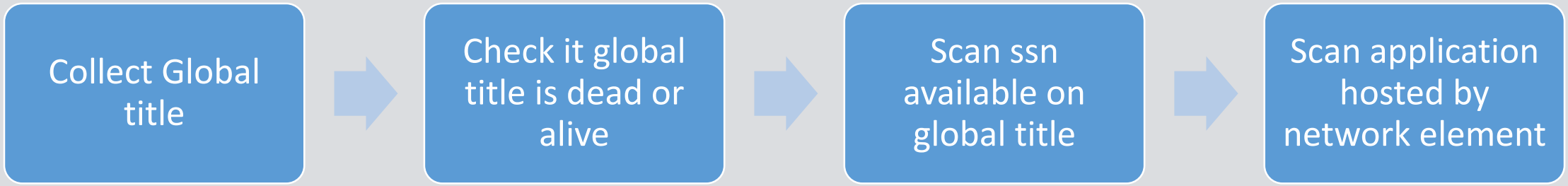
External & internal connectivity



Our method for scanning ss7 - 2

- Scanning process was very similar to IP Scanning
  - Get list of Global titles from operator
  - Check if global title is alive or dead
  - Scan for SSNs available on Global title
  - Scan serving Applications on that Global title's ssn such as
    - MAP –HLR
    - MAP – MSC/VLR
    - MAP – USSD

Scanning method



How easy it was to get connection (external scan)

- Getting access to live ss7 network was very difficult
- Operator was charging approx. few thousand $ for interconnection as deposit
- Per message charges was separately charged
- Need permission for every different type of message we sent
- Written permission from target operator to interconnection provider for permission of test
- Connectivity was provided from SIGTRAN- M3UA

How easy it was to get connection (internal scan)

- Easy as compare to external connection
- Most of the time direct connectivity to STP from data centre
- Some time access was provided from operators corporate network
- Most of time it was SIGTRAN –M3UA peering

Connectivity issues of internal connection

- Most of times only m3ua provisioning no map routing
- Map messages looping due to improper routing in STP
- Most of time while doing internal connectivity
  - Operator just gives IP of STP asking to do ss7/sigtran audit
  - Reason - you are doing ss7 hacking so get create your own path

Scanning from external perimeter

- Multiple global titles to scan
- Using Empty TCAP message to scan Global title (port scanning like approach)
- Found global titles are responding to various messages in MAP category
- Filtering level was not good
  - if its from roaming partner then its good message

Scanning internal perimeter

- Local peering with Operator STP reveals some info such as
  - Vendor of STP
  - DAVA DUNA messages give live point codes
- Scanning Global titles from internal perimeter gives more results
- Point code scanning gives visibility of internal network

Apart from our pentest we found – 1

- We asked operator some information from STP,MSC/VLR,HLR to study further
- These info include
  - Type of message tried
  - Originating global title and destination global title
- We have found
  - DOS attempt (subscriber specific)
  - Info leakage message (location of subscriber, imsi disclosure, MSC leckage)
  - Incomplete procedures

Apart from our pentest we found – 2

- DOS Attempts
  - Cancel Location
  - PurgeMS
  - Delete subscriber DATA
- Information leakage
  - Cryptographic keys (current and future)
  - Location leaks
  - IMSI disclosure
  - VMSC leaks

Why incomplete/unauthorized procedures

- Most of them are
  - Send Routing Info for SM
  - Send Routing info (from external perimeter)
  - Any time interrogation
  - SendIMSI
- Aim could be
  - Privacy leakage
  - Location tracking

Major reason

- Improper implementation of IR 21 document
- Operator often add range of global title to be allowed to query or request. Eg
  - Allow 1234567890-900
- This creates loophole in security

what we suggested

- As first aid
  - Implement IR 21 document strictly
- Allow query only if subscriber is owned by roaming partner
- Perform filtering on STP for global title which are not network element as per IR21 document
- Raise complaint for Global title which are from roaming partner but are not valid network element as per IR21

Existing tools for ss7

- SS7 Mapper
  - Based on Osmocom Stack
  - Does SMSC,MSC,HLR tests as per readme
  - Uses erlang

Tool we are releasing

- Safe-seven
- Based on Mobicents ss7 stack
- Uses M3UA over SCTP to connect to STP
- Does all tests for HLR,VLR ,SGSN,MSC
- Easy to use menu based approach (command line)

SS7 simulator

- Have HLR and MSC functionality
- Based on mobicents stack
- Allows you to simulate ss7 network in realtime
- Support MAP protocol

Where to download tools

- Now you can download tool from https://github.com/akibsayyed/safeseven
- We will be doing demo of this tool in blackhat asia arsenal 2017 so meet us there

Questions