SIP Call Analysis

SANOG12 VoIP Workshop
Kathmandu, August 2008

Jonny Martin - jonny@jonnynet.net
Vicky Shrestha - vicky@pch.net

What to do when It Doesn’t Work ???

- Need a solid trouble shooting and debug approach
    - Back to basics
- Debug SIP endpoint if you have access
    - is the SIP endpoint registered with the SIP server? (sip show peers)
- tcpdump / debug SIP packets hitting SIP server
    - tcpdump -n -v -s0 port 5060 <-- capture entire SIP packets on port 5060
    - tcpdump -n -A -s0 port 53 <-- check DNS queiries, for ENUM lookups
    - ‘man tcpdump’ is your friend!

What to do when It Doesn’t Work ???

- Check the SIP server console for error messages
    - On asterisk, ‘set verbose 10’ and watch for messages
- If the call seems to be good up to this point, check the outgoing call leg (SIP or telephony interface)
    - Exact same techniques as previously

sip_scenario

- http://www.iptel.org/~sipsc/
- A bunch of scripts that:
    - Reads in a tcpdump file
    - Analyses it for SIP calls
    - Builds friendly html files to graphically display the call flow
- Very handy for debugging calls

Install sip_scenario

- cd /home/voip/
- mkdir callflow
- cd callflow
- wget http://www.iptel.org/~sipsc/index/sip_scenario.v1.2.7.zip
- unzip sip_scenario.v1.2.7.zip
- edit sip_scenario.pl and change:
  - #!/usr/local/bin/perl -w --to--
  - #!/usr/bin/perl -w

Capture SIP traffic

- To capture all traffic (there might be lots!):
    - tcpdump -s0 -w capture_filename
- To capture just sip traffic:
    - tcpdump -s0 -w capture_filename2 port 5060
- Make a SIP call through your Asterisk box...
- ./sip_scenario.pl capture_filename
- Then drop the html files in a webserver directory, or open them with your file browser on your linux box.

Using in a production system

- In real networks, not everything is running through one box
- Need to either:
    - Mirror a switch/router port in a useful part of your network
        - Will need tcpdump filters so as to only capture traffic of interest
    - Capture traffic on multiple different boxes and move them back to a central place
        - Script of GUI front end to make it easy