THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

University of Waikato
Network Research Group

openLI

Emulating an LEA

OpenLI Training: Chapter Ten

Shane Alcock
University of Waikato
New Zealand
shane.alcock@waikato.ac.nz

Running a Mock LEA

- How do we know if OpenLI is working?
- Ideally, test with your real LEAs
  - Their time is limited
- Preliminary testing with a mock LEA
  - Resolve obvious issues before getting a real LEA involved

Libtrace and ETSI records

- Libtrace can receive and parse ETSI handover sessions
  - Any libtrace tool can emulate a receiving LEA
  - Nothing complex, just enough to assist with testing and validation

tracepktdump

- Tool that decodes and displays libtrace packet contents
  - Displays TCP/IP headers in a human readable format
  - Can also display ETSI header fields

- Perfect for validating records emitted by OpenLI mediators

The Agency

- Get a shell on your agency container

```
$ docker exec -i -t openli-agency /bin/bash

root@8f48ca8125bd:/home/openli-testagency#
```

The Agency

- Query the container's IP address on the openli-agency network

```
# ip addr list eth1

844: eth1@if2036: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP group default
    link/ether 02:42:ac:15:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.21.0.3/16 brd 172.21.255.255 scope global eth0
    valid_lft forever preferred_lft forever
```

The Agency

- Query the container's IP address on the openli-lab network

```
# ip addr list eth1

844: eth1@if2036: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP group default
    link/ether 02:42:ac:15:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.21.0.3/16 brd 172.21.255.255 scope global eth0
    valid_lft forever preferred_lft forever
```

Select Handover Ports

- Choose a port number for HI2 and HI3
  - HI2 is for receiving IRI records from the mediator
  - HI3 is for receiving CC records from the mediator

Start HI3 Handover

- Run tracepktdump as your HI3 handover

```
# tracepktdump etsilive:172.21.0.3:41003
```

- No output just yet
  - Waiting for the mediator to connect to it
  - Use Ctrl-C to halt the process

Start HI2 Handover

- Get a second shell on the openli-agency container
- Run another instance of tracepktdump on the HI2 port

```
# tracepktdump etsilive:172.21.0.3:41002
```

REST API for Agencies

- OpenLI REST API
  - Used to manage configuration of intercepts and agencies
  - We already configured the REST API socket on the provisioner
  - Use HTTP requests to add, modify, delete or fetch configuration

REST API for Agencies

- Adding an agency via REST
  - POST request
  - Content Type is a JSON object

http://<PROVIP>:<RESTAPIPORT>/agency

REST API for Agencies

- Example JSON Object for our mock agency

```
{
    “agencyid”: “mocklea”,
    “hi2address”: “172.21.0.3”,
    “hi3address”: “172.21.0.3”,
    “hi2port”: “41002”,
    “hi3port”: “41003”,
    “keepalivefreq”: 60,
    “keepalivewait”: 30
}
```

REST API for Agencies

- Example JSON Object for our mock agency

```
{
    “agencyid”: “mocklea”,
    “hi2address”: “172.21.0.3”,
    “hi3address”: “172.21.0.3”,
    “hi2port”: “41002”,
    “hi3port”: “41003”,
    “keepalivefreq”: 60,
    “keepalivewait”: 30
}
```

REST API for Agencies

- Example JSON Object for our mock agency

```
{
    “agencyid”: “mocklea”,
    “hi2address”: “172.21.0.3”,
    “hi3address”: “172.21.0.3”,
    “hi2port”: “41002”,
    “hi3port”: “41003”,
    “keepalivefreq”: 60,
    “keepalivewait”: 30
}
```

REST API for Agencies

- Example JSON Object for our mock agency

```
{
    “agencyid”: “mocklea”,
    “hi2address”: “172.21.0.3”,
    “hi3address”: “172.21.0.3”,
    “hi2port”: “41002”,
    “hi3port”: “41003”,
    “keepalivefreq”: 60,
    “keepalivewait”: 30
}
```

REST API for Agencies

- Example JSON Object for our mock agency

```
{
    “agencyid”: “mocklea”,
    “hi2address”: “172.21.0.3”,
    “hi3address”: “172.21.0.3”,
    “hi2port”: “41002”,
    “hi3port”: “41003”,
    “keepalivefreq”: 60,
    “keepalivewait”: 30
}
```

REST API for Agencies

- Get a shell on the provisioner
- Use curl to POST the agency JSON object
  - Longer term, you want proper HTTP integration

```
curl -X POST -H "Content-Type: application/json"
  -d '{
        "agencyid": "mocklea",
        "hi2address": "172.21.0.3",
        "hi3address": "172.21.0.3",
        "hi2port": "41002",
        "hi3port": "41003",
        "keepalivefreq": 60,
        "keepalivewait": 30
      }'
  http://172.19.0.3:8080/agency
```

REST API for Agencies

- Expected response to the curl command

```
<html><body>OpenLI provisioner configuration was successfully
updated.</body></html>
```

Handovers

- Each handover running on openli-agency should now say:

```
Thread 0 is now handling 1 sources.
```

Mediator Log

- Examine the logs on your mediator container

```
openlimediator[2799]: OpenLI Mediator: received LEA announcement for
mocklea.
openlimediator[2799]: OpenLI Mediator: HI2 = 172.21.0.3:41002   HI3 =
172.21.0.3:41003
openlimediator[2799]: OpenLI Mediator: Connected to agency mocklea on HI2
172.21.0.3:41002.
openlimediator[2799]: OpenLI Mediator: Connected to agency mocklea on HI3
172.21.0.3:41003.
```

Provisioner Log

- Examine the logs on your provisioner container

```
openliprovisioner[2715]: OpenLI: added new agency 'mocklea' via update
socket.
```

Troubleshooting

- Check that you can ping eth1 on openli-agency
  - Ping from the openli-mediator

- Check for typos or errors in your curl JSON object
  - IP addresses must match your tracepktdump instances
  - Port numbers must also match

- Deleting a bad agency -- see next slide

REST API for Agencies

- Removing a configured agency
  - DELETE method

```
curl -X DELETE http://172.19.0.3:8080/agency/mocklea

<html><body>OpenLI provisioner configuration was successfully
updated.</body></html>
```

REST API for Agencies

- Query the details for a particular agency
  - GET method

```
curl -X GET http://172.19.0.3:8080/agency/mocklea

{ "agencyid": "mocklea", "hi3address": "172.21.0.3", "hi2address":
"172.21.0.3", "hi3port": "41003", "hi2port": "41002", "keepalivefreq": 60,
"keepalivewait": 30 }
```

REST API for Agencies

- Query the details for all agencies
  - GET method

```
curl -X GET http://172.19.0.3:8080/agency

[ { "agencyid": "mocklea", "hi3address": "172.21.0.3", "hi2address":
"172.21.0.3", "hi3port": "41003", "hi2port": "41002", "keepalivefreq": 60,
"keepalivewait": 30 }, { "agencyid": "secondlea", "hi3address":
"10.100.0.3", "hi2address": "10.100.0.3", "hi3port": "33003", "hi2port":
"33002", "keepalivefreq": 30, "keepalivewait": 0 } ]
```

REST API for Agencies

- Modifying a configured agency
  - PUT method with JSON data
  - Must include modified fields and “agencyid”

```
curl -X PUT -H "Content-Type: application/json" -d '{"hi2port": "11002",
"hi3port": "11003", "agencyid": "mocklea"}' http://172.19.0.3:8080/agency

<html><body>OpenLI provisioner configuration was successfully
updated.</body></html>
```

More tracepktdump tips

- Use the -c option to halt tracepktdump after N packets

```
# tracepktdump -c 10 etsilive:172.21.0.3:41003
```

- Pipe tracepktdump into the less tool to scroll output

```
# tracepktdump etsilive:172.21.0.3:41003 | less
```

https://github.com/LibtraceTeam/libtrace/wiki/User-Documentation

Other Libtrace Tools

- tracertstats
  - Print regular packet and byte counts for a live capture
  - Useful for observing data rates and general monitoring

```
# tracertstats -i 1 -d etsilive:172.21.0.3:41003
```

https://github.com/LibtraceTeam/libtrace/wiki/User-Documentation

Next Time

- Configuring our first VOIP Intercept