

Adventures in Open Source Lawful Intercept

openLI

Richard Nelson
RIPE 78



Telecommunications (Interception Capability and Security) Act 2013

Public Act 2013 No 91
Date of assent 11 November 2013

Telecommunications (Interception Capability and Security) Useable Format Notice 2017

Pursuant to section 42 of the Telecommunications (Interception Capability and Security) Act 2013 (“Act”) and having consulted in accordance with section 42(2) of the Act the Minister for Communications gives the following notice determining a useable format for the purposes of sections 10(5)(a) and 24(7)(a) of the Act.

Notice

1. Title—This notice is the Telecommunications (Interception Capability and Security) Useable Format Notice 2017.

2. Commencement—This notice commences on 17 August 2017.

3. Purpose—This notice determines a useable format for the purposes of sections 10(5)(a) and 24(7)(a) of the Telecommunications (Interception Capability and Security) Act 2013.

4. Application—This notice applies to any person who is subject to section 9 (Network operators must ensure public telecommunications networks and telecommunications services have full interception capability) and section 24 (Duty to assist) of the Act.

5. Useable format—For the purposes of sections 10(5)(a) and 24(7)(a) of the Act, call associated data and the content of a telecommunication is in a useable format if it complies with each of the ETSI standards specified in the table in clause 8 of this notice to the extent those standards are applicable to the activities of the network operator or the service provider, as the case may be.



Dave Mill dave@m...

Fri Aug 25 08:40:40 NZST 2017

- Previous message: [\[nznog\] SPF for Spark Business Mail](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)
-

Hi all

So, probably a bit a touchy subject this one but here goes..

If you are a network operator and you have more than 4000 customers in my understanding you need to have full interceptions capabilities. (I'm not a lawyer, etc, etc) This is more than just being 'interception ready'.

<http://www.police.govt.nz/advice/businesses-and-organisations/ticsa/interception-capability-and-compliance>

This will mean having a mediation system and being able to produce intercept data in the ETSI standard - again, as far as I know.

What are companies/organisations out there doing about this?

Is there a nice open source solution out there for this? (I haven't found one yet) Are people putting their heads in the sand and praying they never get served a warrant? Is everyone just shelling out hundreds of thousands of dollars on a vendor LI solutions?

What network kit are people integrating with LI in NZ?

And note, the last paragraph on the URL I linked above reads:

"Can I share interception capability resources?

Network operators may co-ordinate, share or contract for services (equipment or staff) in order to meet the interception capability requirements in the Act. However, it remains the responsibility of the network operator to ensure that any such arrangement does not affect any obligations that apply under the Act. Before entering into any such arrangement a network operator must notify the Director of the GCSB."

Replies on or off list welcomed.

Cheers
Dave

(AS17705)



NZNOG List - Response Summary

Most people I've talked to are a bit surprised at ETSI now being required and most people were just assuming they are compliant by being able to offer pcaps on demand.

NZNOG List - Key Questions

Is there a nice open source solution out there for this? (I haven't found one yet) Are people putting their heads in the sand and praying they never get served a warrant? Is everyone just shelling out hundreds of thousands of dollars on a vendor LI solutions?

NZNOG List - Eventual Theme

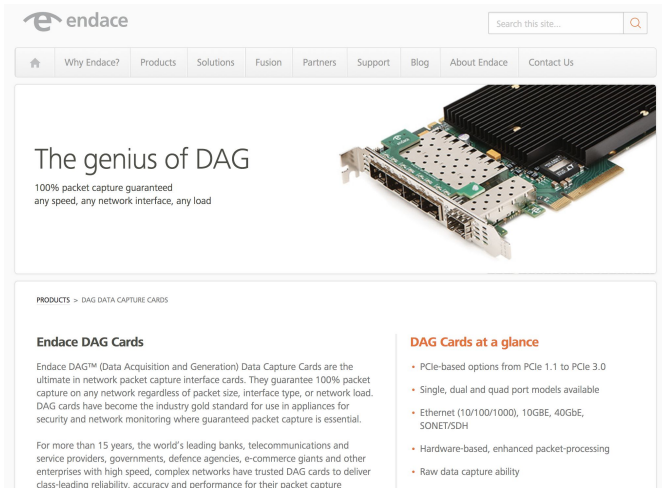
Perhaps some collaboration here would be useful, if others are looking at their own implementations of this stuff?

....

if someone is or is thinking about writing some software or something then collaboration seems like a good idea.

WAND

The University of Waikato Network Research Group



The screenshot shows the Endace website. At the top is the Endace logo and a search bar. Below is a navigation menu with links: Home, Why Endace?, Products, Solutions, Fusion, Partners, Support, Blog, About Endace, and Contact Us. The main content area features a large image of a DAG Card with the headline "The genius of DAG" and the subtext "100% packet capture guaranteed any speed, any network interface, any load". Below this is a section titled "PRODUCTS > DAG DATA CAPTURE CARDS". Under "Endace DAG Cards", it states: "Endace DAG™ (Data Acquisition and Generation) Data Capture Cards are the ultimate in network packet capture interface cards. They guarantee 100% packet capture on any network regardless of packet size, interface type, or network load. DAG cards have become the industry gold standard for use in appliances for security and network monitoring where guaranteed packet capture is essential." It also mentions: "For more than 15 years, the world's leading banks, telecommunications and service providers, governments, defence agencies, e-commerce giants and other enterprises with high speed, complex networks have trusted DAG cards to deliver class-leading reliability, accuracy and performance for their packet capture". To the right, under "DAG Cards at a glance", there is a bulleted list of features.

The genius of DAG
100% packet capture guaranteed
any speed, any network interface, any load

PRODUCTS > DAG DATA CAPTURE CARDS

Endace DAG Cards

Endace DAG™ (Data Acquisition and Generation) Data Capture Cards are the ultimate in network packet capture interface cards. They guarantee 100% packet capture on any network regardless of packet size, interface type, or network load. DAG cards have become the industry gold standard for use in appliances for security and network monitoring where guaranteed packet capture is essential.

For more than 15 years, the world's leading banks, telecommunications and service providers, governments, defence agencies, e-commerce giants and other enterprises with high speed, complex networks have trusted DAG cards to deliver class-leading reliability, accuracy and performance for their packet capture

DAG Cards at a glance

- PCIe-based options from PCIe 1.1 to PCIe 3.0
- Single, dual and quad port models available
- Ethernet (10/100/1000), 10GbE, 40GbE, SONET/SDH
- Hardware-based, enhanced packet-processing
- Raw data capture ability

- Waikato Internet Traffic Storage (WITS)
 - Collection of network traffic header traces.
 - GPS synchronised
 - DAG statistics
 - Publicly available (WAND and RIPE Labs)
 - Uses WAND Developed software

Passive Measurement Research - Examples

“Sneaking Past the Firewall: Quantifying the Unexpected Traffic on Major TCP and UDP Ports”
ACM Internet Measurement Conference IMC 2016

“Measuring the Impact of the Copyright Amendment Act on New Zealand Residential DSL Users”
ACM Internet Measurement Conference IMC 2012

“Libtrace: a packet capture and analysis library” ACM Computer Communications Review,
Volume 42 Issue 2, April 2012

“Application Flow Control in YouTube Video Streams” ACM Computer Communications Review
(CCR) Vol 41 Number 2, April 2011

“Analysis of Long Duration Traces” ACM Computer Communication Review. Volume 35, Issue ,
January 2005

Current Work



Center for Applied Internet Data Analysis

[DONATE](#)[CONTACT US](#)[HOME](#)[RESEARCH](#)[DATA](#)[TOOLS](#)[INTERACTIVE](#)[PUBLICATIONS](#)[WORKSHOPS](#)[PROJECTS](#)[FUNDING](#)

www.caida.org > [projects](#) : [network_telescope](#)

The UCSD Network Telescope

The UCSD Network Telescope is a passive traffic monitoring system built on a globally routed, but lightly utilized /8 network. Under CAIDA stewardship, this unique resource provides valuable data for network security researchers.

Introduction

The UCSD network telescope (aka a black hole, an Internet sink, darkspace, or a darknet) is a globally routed /8 network

Sponsors



Local > Reliable > Fast > Broadband





The OpenLI Project.

OpenLI is being written by the [WAND Network Research Group](#) at the [University of Waikato](#). The primary aim is to meet the requirements of New Zealand's [TICSA](#) legislation. The work is being funded by a group of NZ services providers who came together in response to an [email](#) by Dave Mill to the [NZNOG mail list](#).

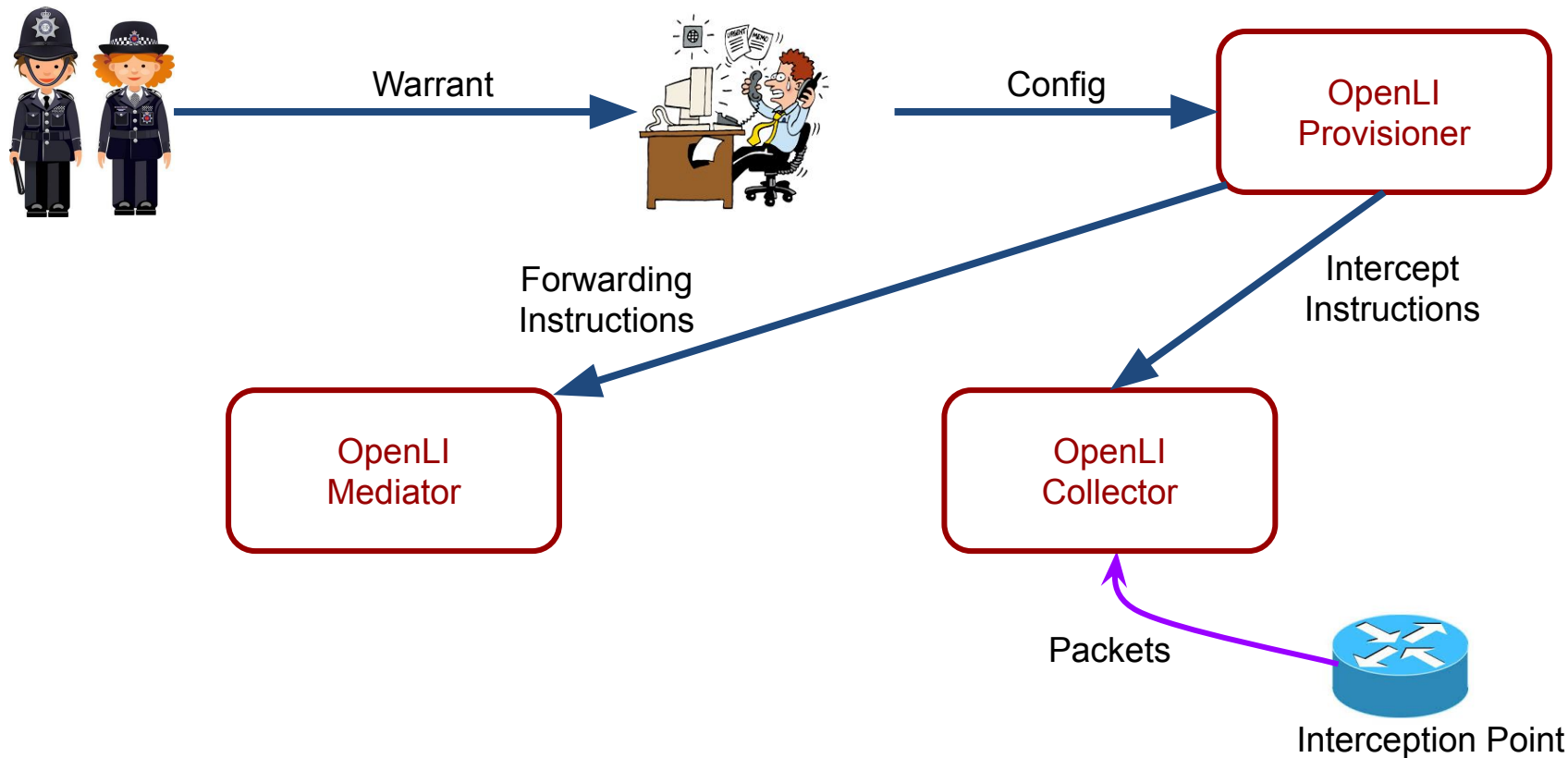
Standards

Column 1: Title of ETSI standard	Column 2: ETSI standard reference
Handover interface for the lawful interception of telecommunications traffic	ETSI TS 101 671 V3.12.1 (2013-10)
Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery	ETSI TS 102 232-1 V3.5.1 (2013-10)
Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services	ETSI TS 102 232-2 V3.6.1 (2013-10)
Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services	ETSI TS 102 232-3 V3.3.1 (2013-10)
Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services	ETSI TS 102 232-4 V3.1.1 (2012-02)
Handover Interface and Service-Specific (SSD) Details for IP delivery; Part 5: Service-specific details for IP Multimedia Services	ETSI TS 102 232-5 V3.2.1 (2012-06)

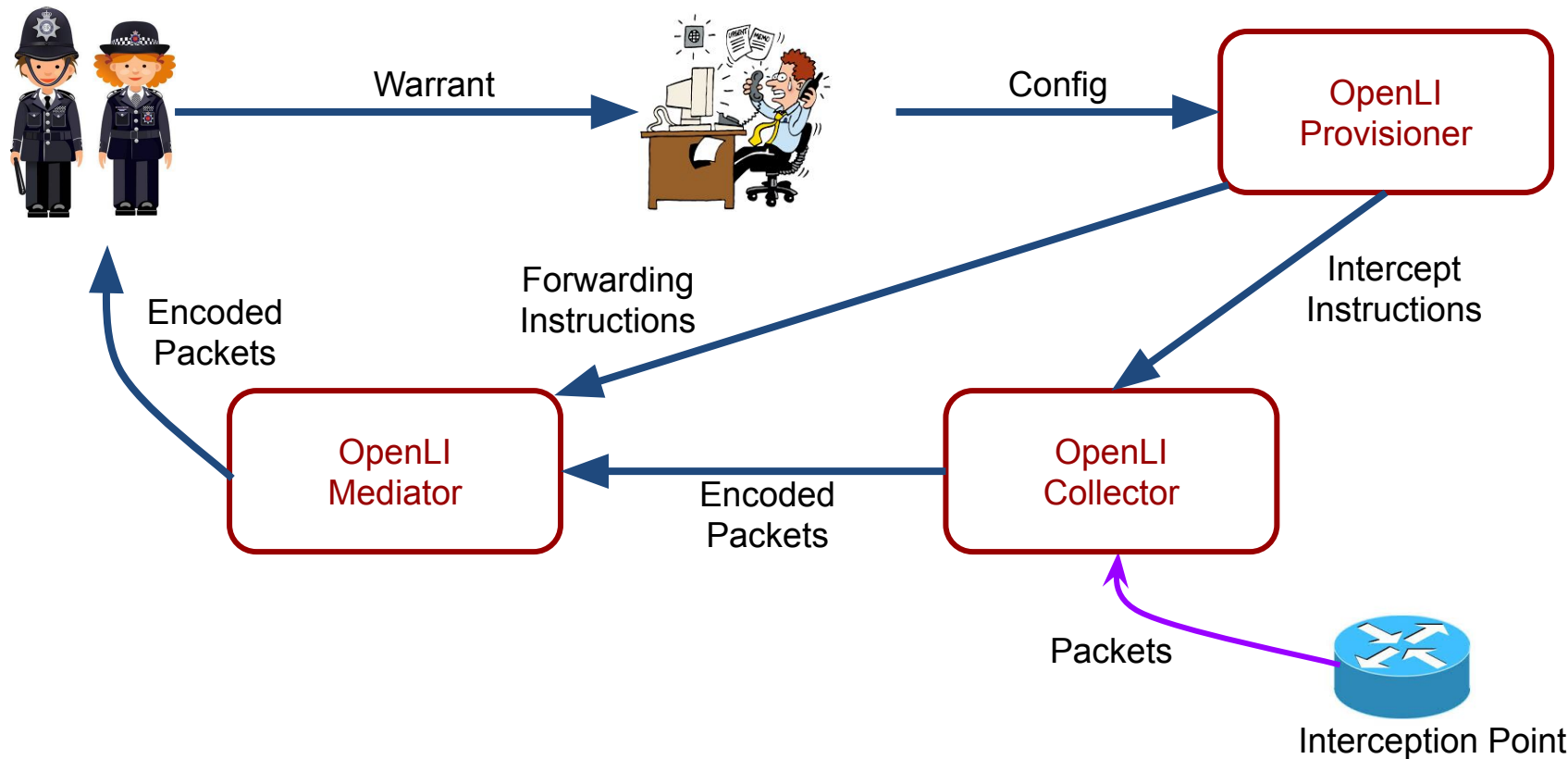
OpenLI Architecture



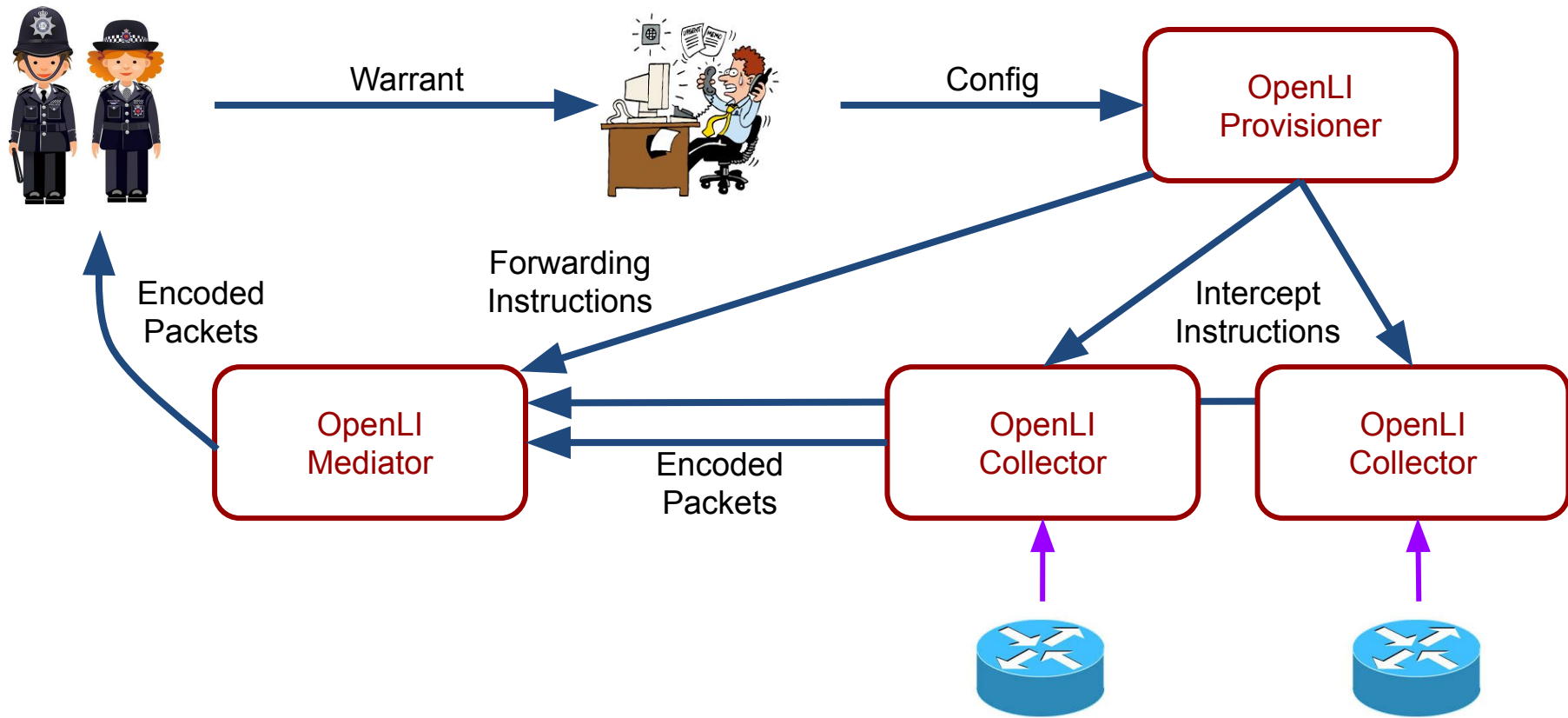
OpenLI Architecture



OpenLI Architecture



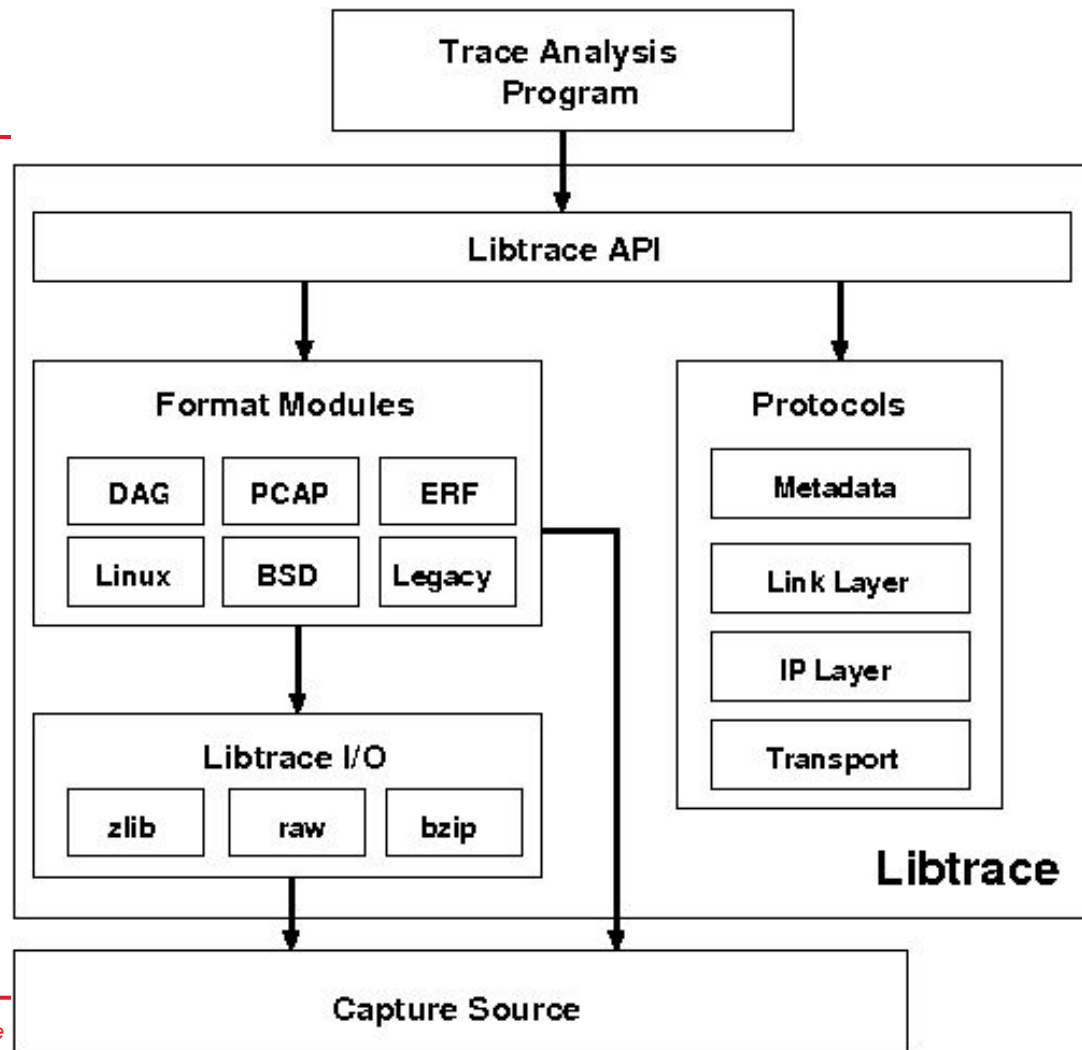
OpenLI Architecture



Implementation

- Target commodity server hardware
- Linux
- C
- Libtrace

Libtrace



Performance Targets

- A service provider *may* have to perform multiple simultaneous intercepts
 - Intercept targets may have 1Gbps service (today)
- Collector must not drop any packets
- Aim to support multiple Gbps of lossless packet capture

Parallelism

- Libtrace supports hardware assisted capture and streaming
 - DPDK, Endace DAG
- Extremely parallel capture
 - Multiple simultaneous capture interfaces
 - Multiple streams per capture interface
 - Use multiple CPU cores to increase performance
- Packets spread across threads.
 - Control vs Data, Hashing.
- Session state synchronisation
- Consistent sequence numbering.

Parallelism - Solution

- More threads
 - Synchronisation thread for VoIP calls
 - Synchronisation thread for IP sessions
 - Sequence tracking thread for sequence numbers
 - Worker thread pool for ASN.1 encoding
 - Forwarding thread to export to the mediator
- Use ZeroMQ to handle inter-thread communication
- Performance tested to 500kpps with DPDK in our test environment
 - Further optimisation possible

OpenLI 1.0 Dec 2018

- Feature complete to initial spec
 - IP Intercepts
 - RADIUS parsing to map IP sessions to users
 - VOIP Intercepts
 - Static IP ranges for IPv4 and IPv6
 - ETSI encoding of both IRIs and CCs
 - Custom encoding Library : LibDER
 - Mediation of encoded ETSI records to LEAs
 - Centralised provisioning
 - Distributed collection, including multiple interfaces per collector

Released

<https://github.com/wanduow/openli>

The screenshot shows the GitHub repository page for `wanduow / openli`. At the top, there are buttons for `Unwatch` (4), `Star` (3), and `Fork` (0). Below these are tabs for `Code`, `Issues` (8), `Pull requests` (0), `Projects` (0), `Wiki`, `Insights`, and `Settings`. The repository description is "Open Source ETSI compliant Lawful Intercept software" with an `Edit` button. Below the description is a "Manage topics" link. A summary bar shows `446` commits, `2` branches, `1` release, `1` contributor, and `GPL-3.0` license. Below the summary bar are buttons for `Branch: master`, `New pull request`, `Create new file`, `Upload files`, `Find file`, and `Clone or download`. At the bottom, there is a commit by `salcock` with the message "Force gzip compression for all debian packages" and a link to the commit details. The latest commit is `a6a27b2` from 5 days ago.

wanduow / openli

Unwatch 4 Star 3 Fork 0

Code Issues 8 Pull requests 0 Projects 0 Wiki Insights Settings

Open Source ETSI compliant Lawful Intercept software Edit

Manage topics

446 commits 2 branches 1 release 1 contributor GPL-3.0

Branch: master New pull request Create new file Upload files Find file Clone or download

salcock Force gzip compression for all debian packages Latest commit a6a27b2 5 days ago

Packaged

<https://bintray.com/wand/OpenLI/>



wand / OpenLI



<https://dl.bintray.com/wand/OpenLI>

Owned by [WAND Network ...](#)

 [Report](#)

 **debian**



Packages for the components of OpenLI, an open-source ETSI-compliant Lawful Intercept software suite.

Note that you may need to also add <https://dl.bintray.com/wand/libtrace/> and <https://dl.bintray.com/wand/general/> to your apt sources to install all of the dependencies for the OpenLI packages.

SET ME UP!



Deployed

- Inspire
 - TICS A Part 3 Approval
 - Police Testing
- Others??

Police reaction



Further Development

- Bug Fixes
- Testing
- Internal security and Auditability improvements
- Disk backed buffering
 - Memory-backed for now, but limited capacity
 - Fall back to disk before memory gets full
 - Clear backlog when situation is resolved
- Further Performance improvements
 - BER
- APIs
 - Entering warrant/customer details
 - Controlling network devices
- Support vendor formats

-
- WAND
 - <https://wand.net.nz>
 - Libtrace
 - <https://research.wand.net.nz/software/libtrace.php>
 - OpenLI
 - <https://openli.nz>
 - Code:
 - <https://github.com/wanduow/openli>

