Adventures in Open Source Lawful Intercept

Richard Nelson

AusNOG 18, Sydney

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

WAND Network Research Group

TICSA

Telecommunications (Interception Capability and Security) Act 2013

Public Act 2013 No 91

Date of assent 11 November 2013

Gazette

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)

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?

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

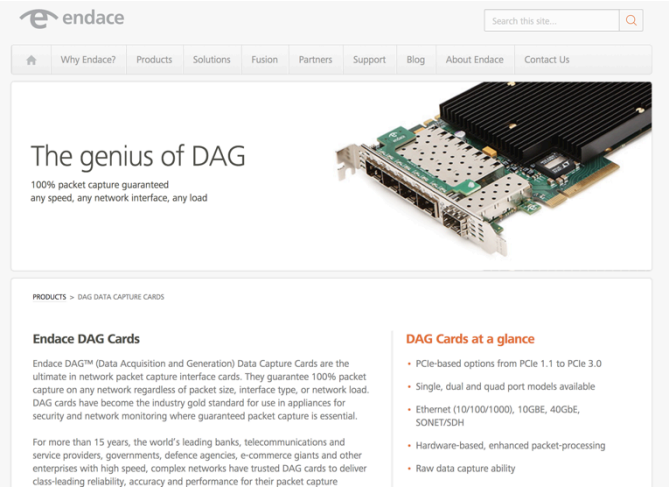
Perhaps some collaboration here would be useful, if others are looking at their own implementations of this stuff?

....

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

History

The University of Waikato
Network Research Group



- Waikato Internet Traffic Storage (WITS)
- Collection of network traffic header traces.
  - Anonymised
  - GPS synchronised
  - DAG statistics
  - Publicly available (WAND and RIPE NCC)
  - New Zealand Universities and ISPs
- Uses WAND Developed software
- Our best known research activity
  - “Waikato Network Traces” ~10k hits on Google Scholar

Passive Measurement Research - examples

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

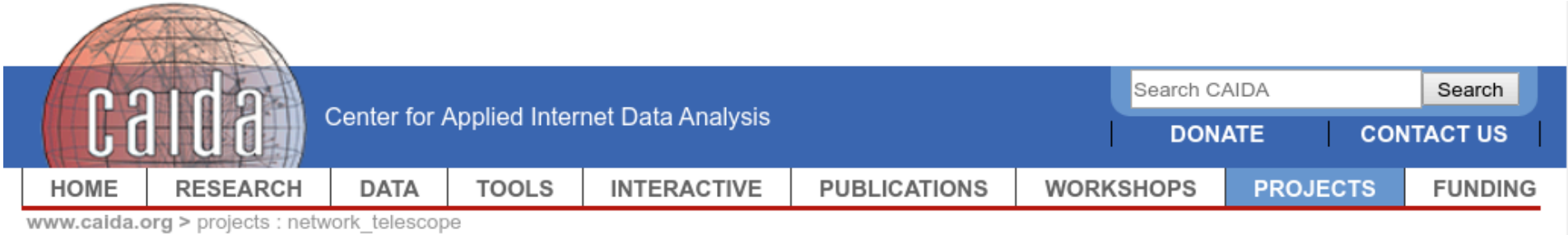
"Measuring the Impact of the Copyright Amendment Act on New Zealand Residential DSL Users" ACM Internet Measurement Conference IMC 2012

"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 Passive Capture



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

Project

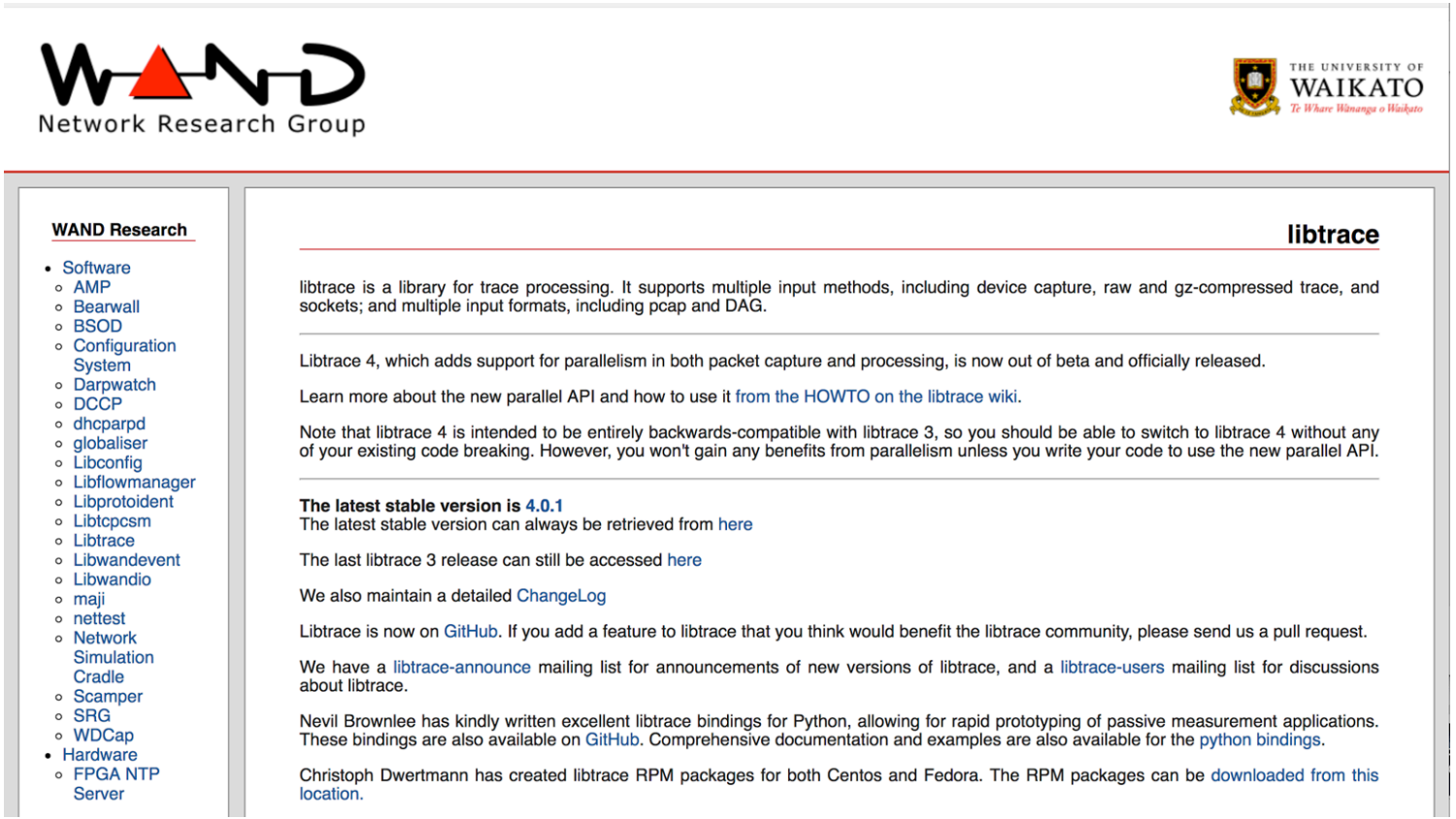
The OpenLI Project.

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.

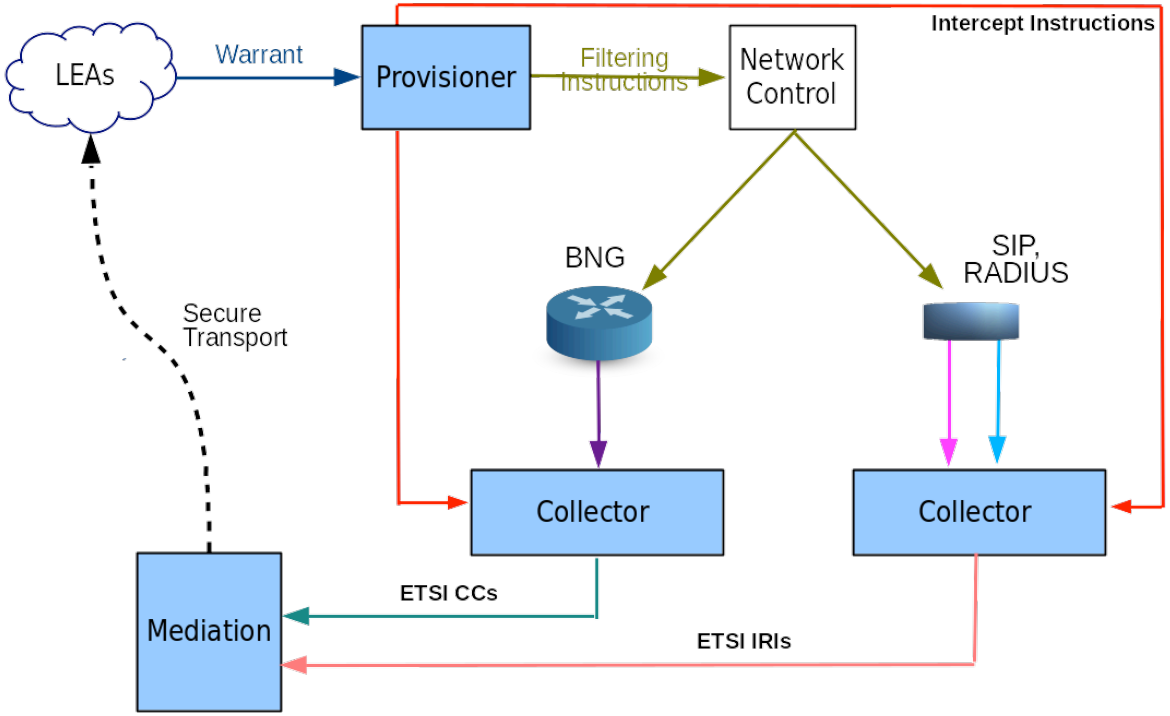
Standards

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)

Libtrace


Network Research Group
THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato
WAND Research
Software
AMP
Bearwall
BSOD
Configuration System
Darpwatch
DCCP
dhcparpd
globaliser
Libconfig
Libflowmanager
Libprotoident
Libtcpcsm
Libtrace
Libwandevent
Libwandio
maji
nettest
Network Simulation Cradle
Scamper
SRG
WDCap
Hardware
FPGA NTP Server
libtrace
libtrace is a library for trace processing. It supports multiple input methods, including device capture, raw and gz-compressed trace, and sockets; and multiple input formats, including pcap and DAG.
Libtrace 4, which adds support for parallelism in both packet capture and processing, is now out of beta and officially released.
Learn more about the new parallel API and how to use it from the HOWTO on the libtrace wiki.
Note that libtrace 4 is intended to be entirely backwards-compatible with libtrace 3, so you should be able to switch to libtrace 4 without any of your existing code breaking. However, you won't gain any benefits from parallelism unless you write your code to use the new parallel API.
The latest stable version is 4.0.1
The latest stable version can always be retrieved from here
The last libtrace 3 release can still be accessed here
We also maintain a detailed ChangeLog
Libtrace is now on GitHub. If you add a feature to libtrace that you think would benefit the libtrace community, please send us a pull request.
We have a libtrace-announce mailing list for announcements of new versions of libtrace, and a libtrace-users mailing list for discussions about libtrace.
Nevil Brownlee has kindly written excellent libtrace bindings for Python, allowing for rapid prototyping of passive measurement applications. These bindings are also available on GitHub. Comprehensive documentation and examples are also available for the python bindings.
Christoph Dwertmann has created libtrace RPM packages for both Centos and Fedora. The RPM packages can be downloaded from this location.

OpenLI - Architecture



OpenLI Status

- Feature complete to initial spec
- Tested with NZ Police
- In “production” with at least two ISPs

- Current work
  - Performance testing
  - Bug fixing
  - Documentation
  - Release - GPL

- WAND
  - https://wand.net.nz
- Libtrace
  - https://research.wand.net.nz/software/libtrace.php
- OpenLI
  - https://openli.nz