OpenLI: An Open-Source Alternative for Lawful Intercept

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

Lawful Intercept (LI)

- Legal and authorised interception of telecommunications
  - Mandated by governments
  - Aim is to investigate or prevent criminal activity

- Requested by Law Enforcement Agencies (LEAs)
  - Police, Intelligence Services, National security agencies

- Actioned by network operators

Lawful Intercept (LI)

- Targeted at a specific user
- Supported by a lawfully issued warrant
- Severe penalties for failure to comply
  - Be prepared ahead of time!

Real Time Traffic Interception

- Increasingly common requirement
  - Fiji: Cybercrime Bill 2020
  - Vanuatu: Cybercrime Act 2020

- Allows agencies to react to ongoing events

- Much more challenging for operators to supply
  - tcpdump is not sufficient

Standards

- Two widely recognised standards for LI
  - CALEA / ATIS: used in USA
  - ETSI: used almost everywhere else

- Reasons for using standards
  - Standards ensure the intercept can withstand scrutiny in court
  - Interoperation with equipment bought by LEAs

Standards

- ETSI standards are complex and difficult to implement
  - Many pages of documents to read

- Expertise in high-performance packet capture required

Options

- Specialist LI vendors
  - Many companies offering LI solutions to choose from
  - Costs will be high and ongoing
  - Commercial-grade support
  - Provisioning and mediation included in the system
  - Good option for large carriers with money to spend

The New Zealand Story

- In 2017, ETSI was mandated as required for LI

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.

The New Zealand Story

- Onus was on operator to integrate LI into their network
  - No funding from government or the LEAs

- Vendor solutions for ETSI cost $$$$$$
  - Plus ongoing licensing costs

- Non-compliance would also cost $$$$$$

The New Zealand Story

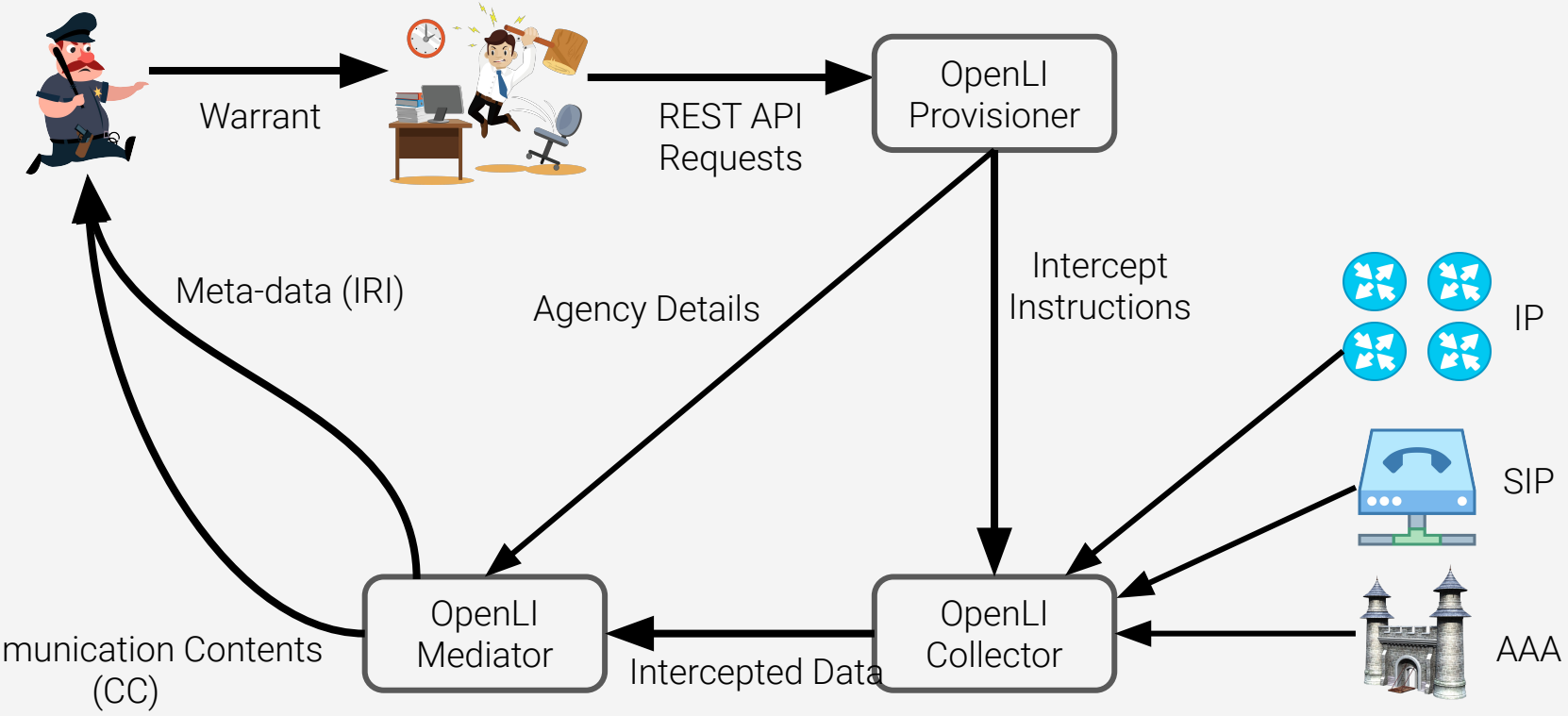
- Via NZNOG, operators began to discuss collaboration
  - Waikato offered to provide developer expertise
  - Operators agreed to pool funds to cover costs
  - Resulting solution must be open-source

The End Result

- OpenLI
  - Open source software for ETSI-compliant LI
  - Designed and maintained by me (mostly)
  - Runs of Linux + commodity server hardware
  - Target audience: smaller operators
  - Flexible, easy to integrate into existing networks (hopefully!)

https://openli.nz

Lawful Intercept with OpenLI



OpenLI

- Multiple collectors can be distributed throughout a network
  - One per BNG or customer aggregation point

- Collector uses AAA protocols to determine target IP
  - Only intercepts packets for that session
  - Tracks dynamic IP changes

- Mediator is the only external-facing component
  - Makes outbound connections to the LEAs

Success So Far

- Operators in NZ have now deployed OpenLI in production
  - Have had interest from operators in other countries

- Ongoing development and maintenance
  - Funding from grants and sponsorship
  - Income stream from support contracts
  - In NZ, consultants offer OpenLI deployment as a service

Looking Abroad

- ISIF Asia Grant
  - Expand OpenLI adoption in the APNIC region
  - Develop new features suggested by operators
  - Create better educational materials for new OpenLI users

Looking Abroad

- We want to engage with you!
  - Assist you with an OpenLI deployment
  - Get your feedback on what would make OpenLI better
  - Solve a pressing problem for smaller operators

Interested?

- Learn more:
  - https://openli.nz
  - https://github.com/wanduow/openli
  - Email: openli-support@waikato.ac.nz

Thank you!

- Questions?