openli-support@waikato.ac.nz

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

University of Waikato
Network Research Group

openLI

Introduction to Lawful Intercept

OpenLI Training: Chapter One

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
  - Powers can vary between countries
- Severe penalties for failure to comply
  - Be prepared ahead of time!

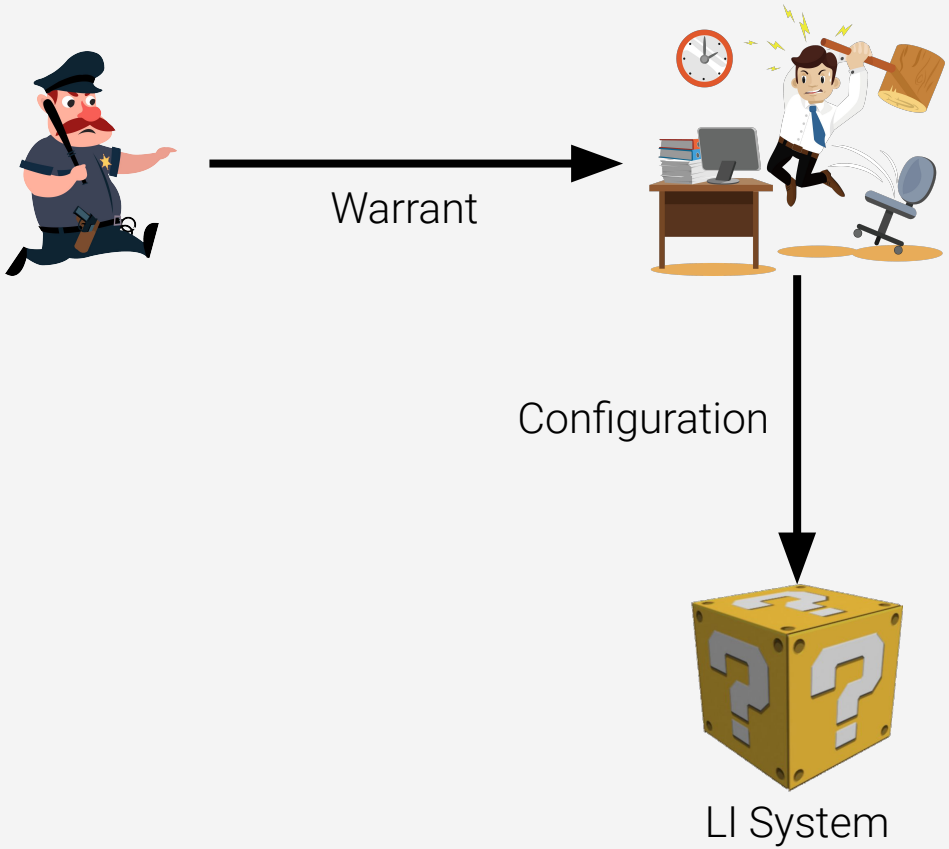
Lawful Intercept (LI)

LEA

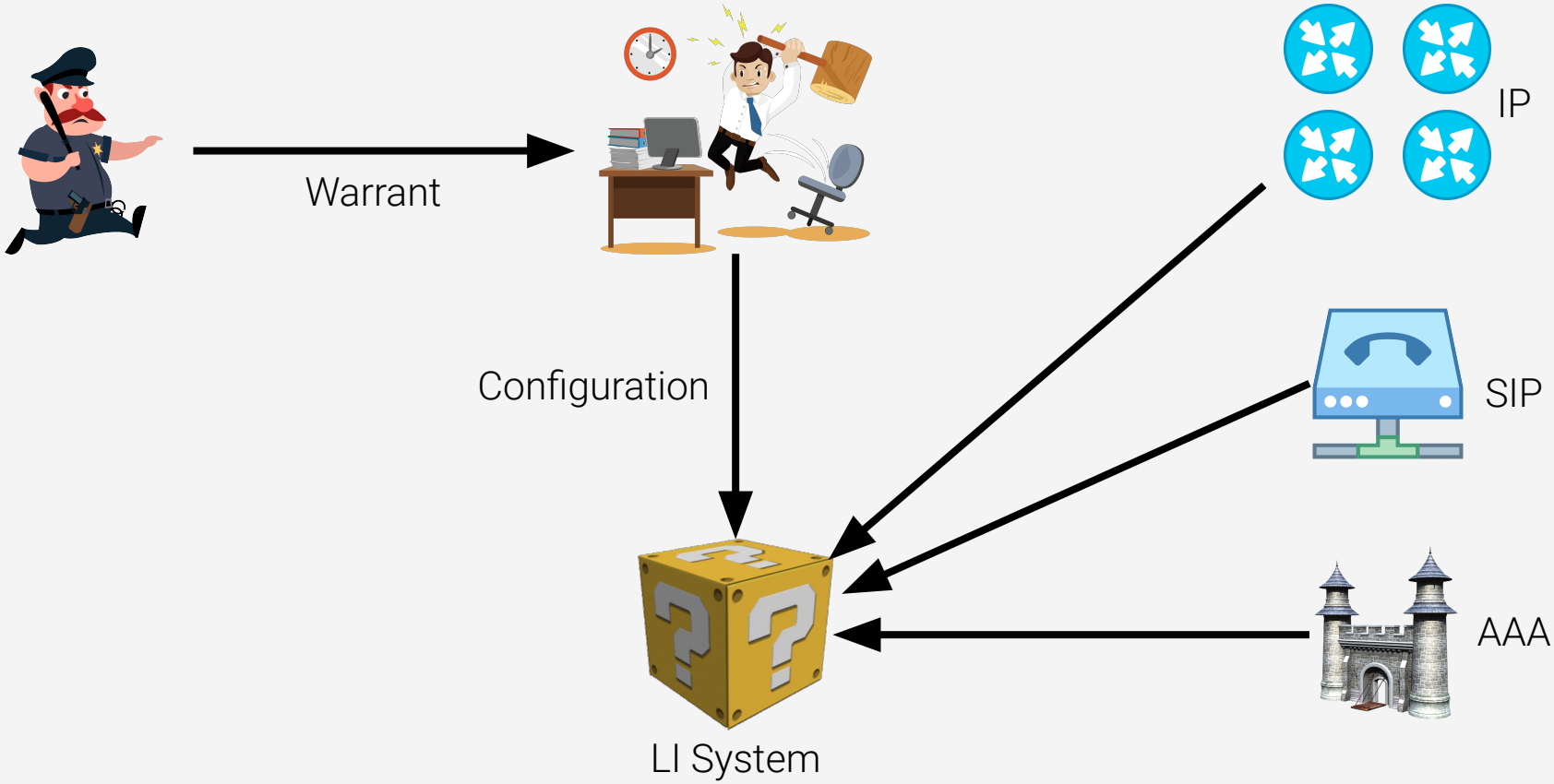
Warrant

Network Operator

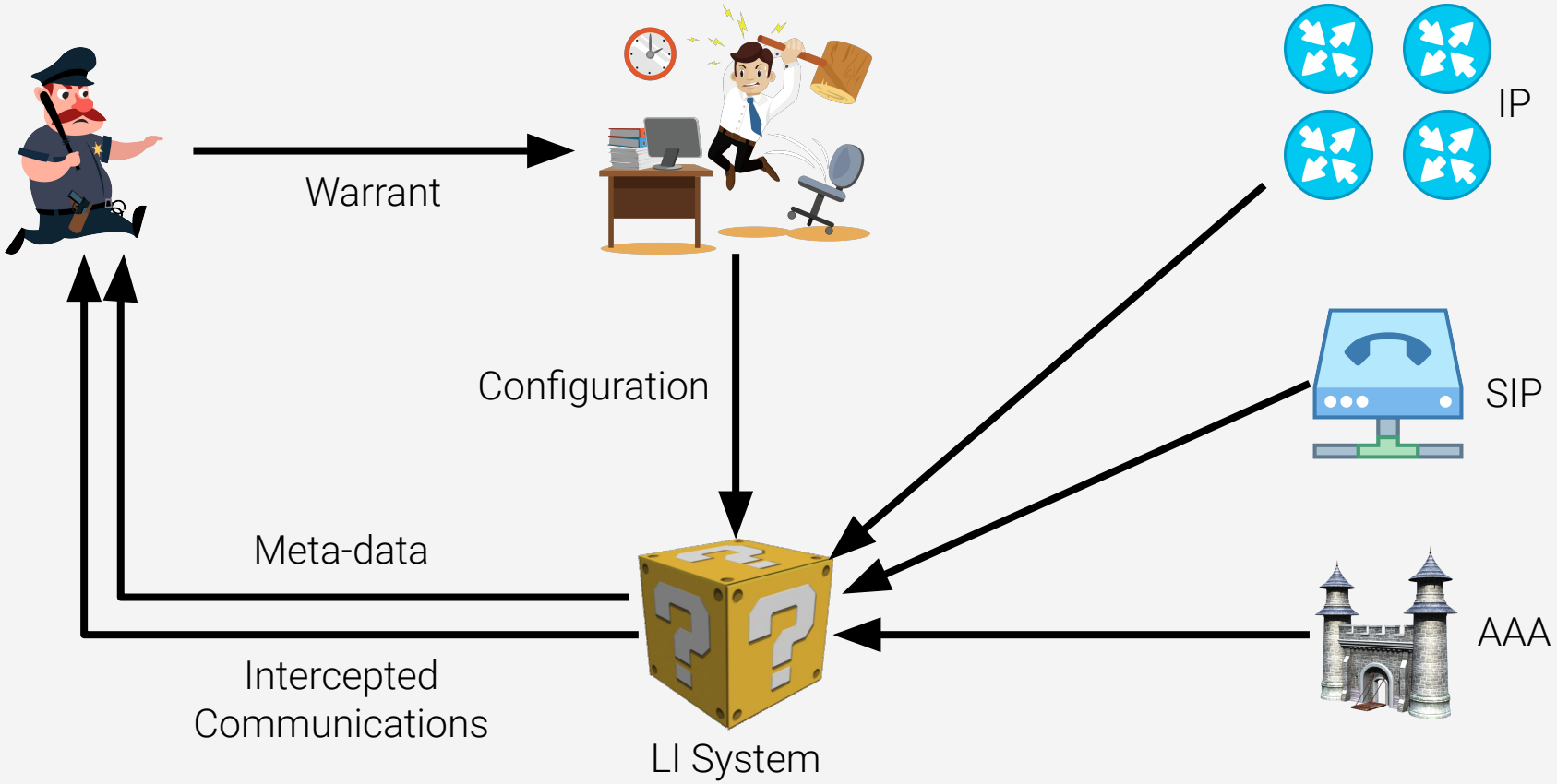
Lawful Intercept (LI)



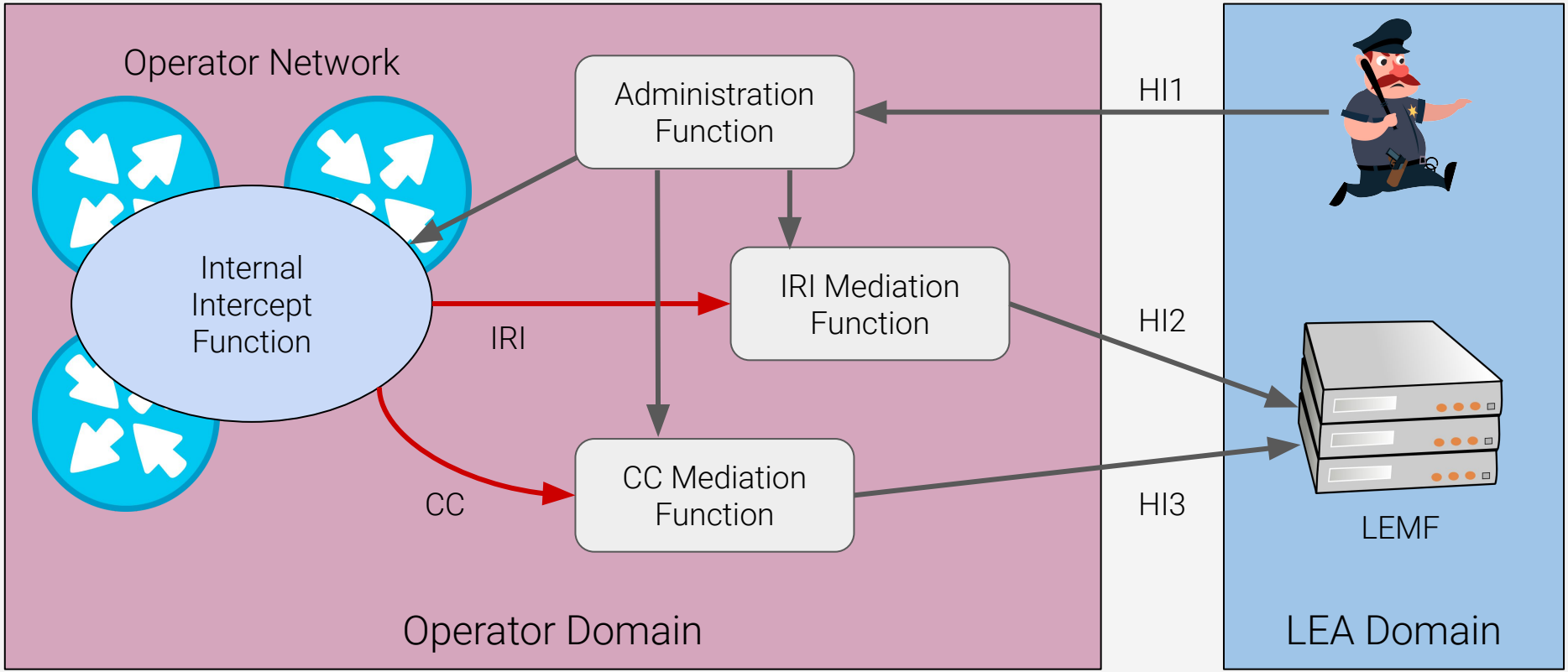
Lawful Intercept (LI)



Lawful Intercept (LI)



Lawful Intercept (LI)



Terminology

- Content of Communication (CC)
  - The data packets that were intercepted for a given target

- Intercept Related Information (IRI)
  - Meta-data describing the session/call that has been intercepted
  - Start time, end time
  - For IP sessions: username, assigned IP, bytes transmitted
  - For VOIP calls: caller, callee, media type

Terminology

- Mediation Function (MF)
  - Aggregates and sends intercepted data to the LEAs
  - Communication protocol is standardised

- Law Enforcement Monitoring Facility (LEMF)
  - The system used by the LEA to receive and process your intercept

Terminology

- Internal Intercept Function (IIF)
  - Generates intercept records from captured network packets
  - These will run on or alongside your networking equipment

Terminology

- Administration Function (AF)
  - Processes interception orders from the LEAs
  - Sends instructions to the IIFs and MF

- Handover
  - A communication channel between the operator and the LEA

Terminology

- HI1
  - Used by the AF receive interception orders from the LEA
- HI2
  - Used by the MF to deliver IRI records to the LEMF
- HI3
  - Used by the MF to deliver CC records to the LEMF

Standards

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

- Not as simple as just sending a pcap to the LEA!
  - Standards ensure the intercept can withstand scrutiny in court
  - LEA systems must be able to decode your LI output
  - Require operators to be able to deliver intercepts in real time

Standards

- Standards are complex and onerous
  - Implementation in-house requires significant resources

- Most operators will want to deploy an existing solution
  - Budget, long-term support, required standards all play a role

Possible Solutions

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

Possible Solutions

- LI licenses for networking hardware
  - Cisco, Juniper, Nokia, etc.
  - Can be used as an IIF
  - Still require a third-party mediator
    - Output is not standards compliant

Image credit: Jim Bryson

OpenLI

- Open source software for ETSI-compliant LI
  - Designed and maintained by WAND group
  - Low cost alternative to buying solutions from an LI vendor
  - Runs on Linux + commodity server hardware
  - Target audience: smaller operators
    - Deployed in production by operators in NZ
  - Can convert some network vendor LI formats into ETSI

https://openli.nz

Summary

- What is Lawful Intercept (LI)?
- How does LI work in practice?
- Terminology
- Standards for LI
- Existing LI solutions, including OpenLI

Next Time

- Delve a bit deeper into the ETSI standards
  - Key requirements for a compliant LI system