THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

University of Waikato
Network Research Group

openLI

The ETSI Standards for LI

OpenLI Training: Chapter Two

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

Motivation for Standards

- Interoperability
  - Common protocols, message formats, etc.
  - Output of the operator system must be understood by the LEA

Motivation for Standards

- Evidence Integrity
  - Intercepts are used as evidence in criminal trials
  - Must be able to withstand scrutiny
  - Precise and comprehensive labels
  - Account for any missing or corrupted evidence

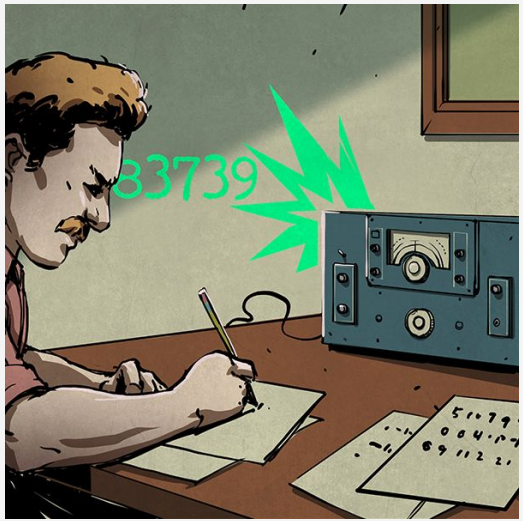
Downsides of Standards

- Complexity
  - Implementation requires significant expertise and time

- High costs for operators
  - Pay for a third-party solution
  - Invest in LI expertise in-house

ETSI Requirements

- Intercepted traffic must be streamed to LEAs in real time
  - Encrypted TCP sessions over public Internet
  - Closed physical connections for very sensitive intercepts



ETSI Requirements

- Two separate handovers
  - Separate encrypted TCP session for each handover
  - One handover for meta-data
  - One for intercepted communications / packets

ETSI Requirements

- Custom record format to label and sequence recorded data
  - Unique LIID provided by the LEA
  - Each session or call must also have a unique CIN
  - Sequence numbers per CIN to identify lost data

- Format is defined by many pages of ASN.1
  - IP, VOIP and Mobile IP intercepts are all slightly different

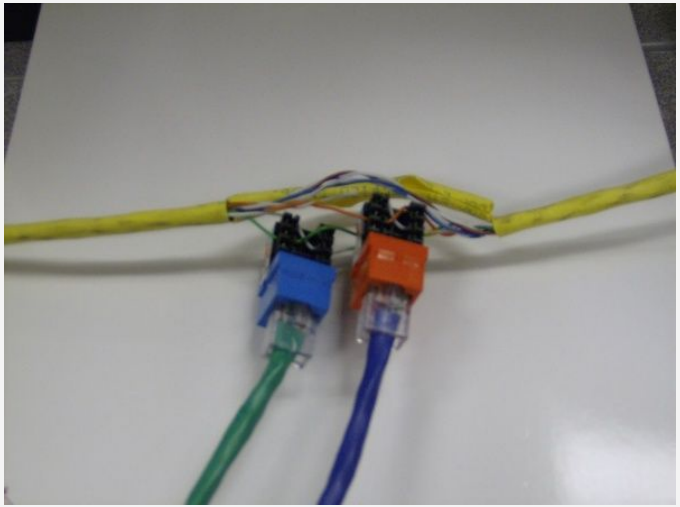
ETSI Requirements

- All communication by a target must be delivered to the LEA
  - No packet loss allowed

- Protect privacy of other network users
  - No interception of traffic for anyone other than the target

ETSI Requirements

- Target cannot detect that the intercept is taking place
  - Communication must continue uninterrupted
  - No noticeable changes in routing or latency



Summary

- Why do the ETSI standards exist?
- The problem of complexity and its related costs
- Specific requirements mandated by the standards

Next Time

- Packet capture for LI systems
  - Available methods and their limitations

- Stick around for some “bonus” material
  - Potentially useful for future OpenLI developers...

Standards Documents

- ETSI TS 101 671
  - Describes the basic communication model for an LI system
  - Handovers between LEA and operator
  - Overview rather than technically specific

Standards Documents

- ETSI TS 102 232-1
  - Delivery of intercept records to LEAs via the Internet
  - Header format and meaning of each field within
  - Session management
    - Keep alives
    - Option negotiation
    - Acknowledgements
  - TCP settings

Standards Documents

- ETSI TS 102 232-3
  - Interception of IP traffic
  - Formatting of IRIs and CCs for IP intercepts
  - Definition of target identity in an IP context
  - How to map AAA events to IRI records

Standards Documents

- ETSI TS 102 232-5
  - Interception of IP multimedia traffic
    - VOIP, video-conferencing
  - Formatting of IRIs and CCs for VOIP intercepts
  - Definition of target identity in a VOIP context
  - How to map SIP events to IRI records

Standards Documents

- ETSI TS 102 232-7
  - Interception of mobile IP traffic
    - 2G, 3G and 4G services
  - Formatting of IRIs and CCs for mobile IP intercepts
  - “Helpfully” defers to the equivalent 3GPP documents
    - Translation of 3GPP fields to ETSI header fields

Standards Documents

- Documents that I've left out
  - ETSI TS 102 232-2: Email
  - ETSI TS 102 232-4: Layer 2 services
  - ETSI TS 102 232-6: PSTN / ISDN legacy services

Next Time

- Packet capture for LI systems
  - Available methods and their limitations