openLI

OpenLI Components

OpenLI Training: Chapter Four

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

Introducing OpenLI

- Open Source software for lawful intercept
  - Compliant with ETSI standards
  - Runs on x86 Linux
  - Runs on off-the-shelf computing hardware
  - GPLv3
  - Actively developed and maintained
  - Multiple successful deployments

The Components

- Provisioner
- Collectors
- Mediator

Provisioner

- Central controller for the entire system
  - Implements the “administration function”
- Used by authorised personnel to start/stop intercepts
  - Also configure other aspects of OpenLI system
- Provides a REST API for intercept configuration

Provisioner

- Low workload
  - Can easily be run in a small VM or container
- Must be able to talk to all other OpenLI components
- Should *not* be accessible from off-network
- Access should be strictly limited to approved persons only
  - REST API supports authentication via API keys and digest auth

Collectors

- Collectors do the bulk of the work in an OpenLI deployment
  - Listen for instructions from the provisioner
  - Capture packets
  - Track user sessions using AAA traffic
  - Decide which packets to intercept
  - Encode intercepted packets into ETSI IRIs and CCs
  - Forward IRIs and CCs to mediators

Collectors

- Packet Capture
  - Multiple capture interfaces are supported
  - Choose appropriate capture methods for your workload
    - See previous lesson for more info
  - Try to be smart about reducing packet rate
    - Use BPF filters for coarse filtering
    - Upstream filtering is better, but not always straightforward

Collectors

- Tracking user sessions -- RADIUS example
  - Operators pre-configure RADIUS servers via provisioner
  - RADIUS traffic is parsed separately by the collector
  - Maintains state table of all active users and their IP addresses
    - This is used to decide whether a packet should be intercepted
    - A collector must see all relevant RADIUS traffic

Collectors

- Deciding to intercept -- RADIUS example
  - IP addresses of captured packets are inspected
  - If match the address of an active intercept target: intercept
  - Otherwise: ignore

Collectors

- Encoding intercepted packets
  - ETSI standards specify formatting using ASN.1 / BER encoding
  - Encoding is computationally expensive (relatively)
  - Wrote our own encoding/decoding library (libwandder)

- Other requirements
  - Sequencing of ETSI records for each intercept
  - Consistency between IRIs and CCs for same intercept

Collectors

- Forwarding to mediators
  - Try to ensure records are sent in sequential order
  - Buffer records if mediator is unreachable
    - Support use of RabbitMQ for buffer management
    - Otherwise, simple in-memory buffering is used

Deploying Collectors

- Distribute collectors throughout your network
  - Suggest one per BNG / customer aggregation point
  - Ensure collector gets AAA feed for all those users
  - For VOIP, mirror both SIP and RTP traffic

Collectors -- Choosing Hardware

- Bare metal is best, but a VM will usually suffice

- More CPU cores is better
  - Packet capture: 10Gbps ⇒ 8+ CPU cores
  - Encoding: 10Gbps ⇒ 4+ CPU cores
  - Sequencing, forwarding, session tracking ⇒ 4 CPU cores

Collectors -- Choosing Hardware

- NICs and packet capture hardware
  - 1 high performance NIC supporting DPDK and/or XDP
    - Plus 1 standard 4-port NIC for management, AAA capture
- Memory: 16 GB recommended
- Disk
  - No special requirements, just enough for buffering
  - SSD optional

Collectors

- Security
  - Absolutely **NO** off-network access
  - Only permit login for administrative purposes

Mediators

- Mediators implement the handovers to the LEAs
  - Maintain mappings of active intercepts to their destination LEA
  - Establish and maintain HI2 and HI3 TCP sessions
  - Receive encoded ETSI records from collectors
  - Buffer, then forward ETSI records via handovers

Mediators

- Handover TCP sessions
  - Established over an encrypted tunnel, e.g. IPSec
  - Your LEA(s) will provide instructions on tunnel configuration
  - Sessions stay up even when no active intercepts
  - Your mediator will always initiate the TCP connection

Mediators

- Security
  - Needs to be able to make outbound connections to the LEAs
    - via public Internet
  - No inbound connections from external parties, though
    - Firewall any connection attempts from outside
  - As usual, login should only be required for administration

Mediators -- Choosing Hardware

- Memory
  - To buffer intercepts if handovers fail
  - Minimum 16GB, 32GB+ recommended

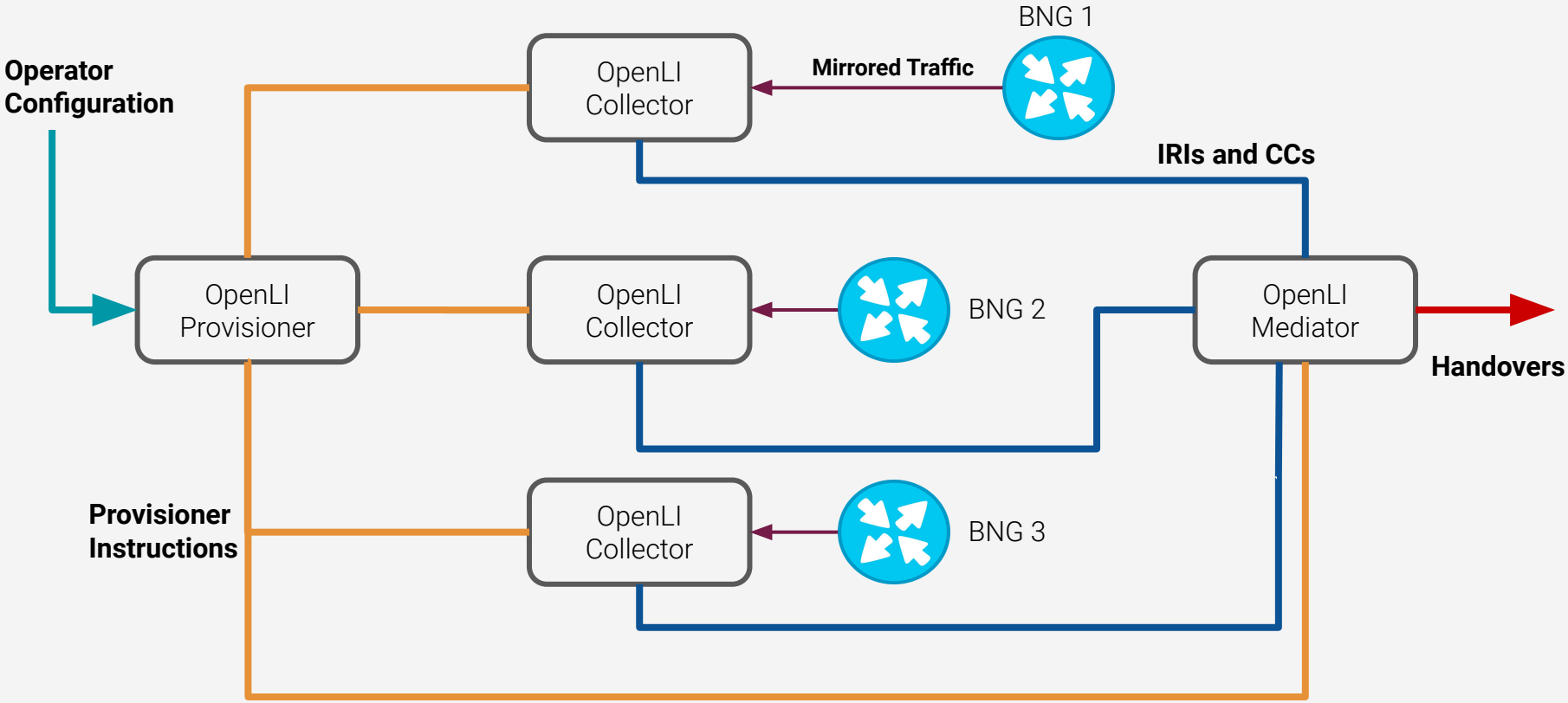
- Networking
  - Capacity to receive peak concurrent intercept traffic
  - Capacity to forward peak concurrent intercept traffic
  - Example, 2 10Gb interfaces + a management interface

Mediators -- Choosing Hardware

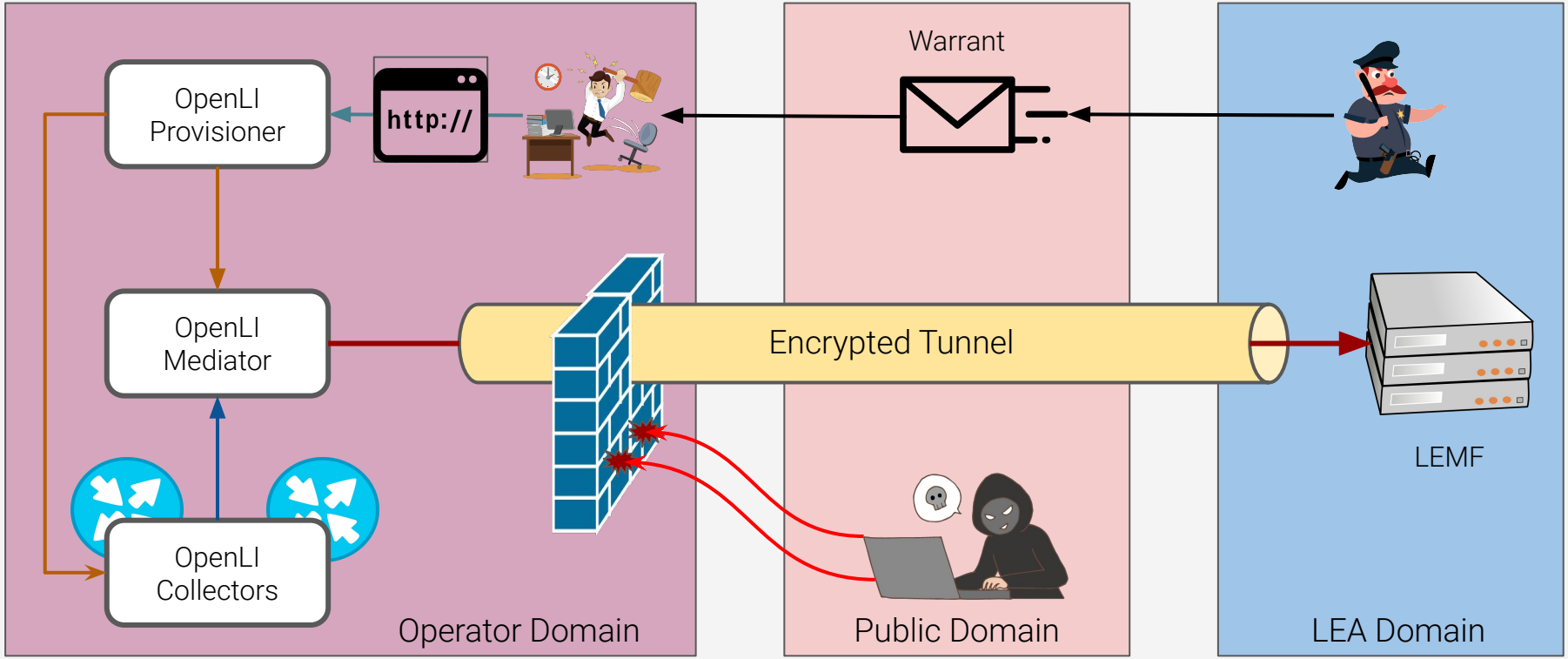
- CPU is unlikely to be a significant bottleneck
  - Allow 8+ cores just to be safe
  - Should be fine to run inside a VM or container

- You can run multiple mediators if required
  - Confirm with your LEAs that they are happy to support this

A Typical Deployment -- High Level



Security Domain Perspective



Next Time

- Installing and maintaining OpenLI