Lawful Interception Basics

April 2018

Utimaco TS, Product Management
Lawful Interception

Definition

- Lawful Interception (LI) refers to the legally approved surveillance of public telecommunication services
- Important tool for law enforcement agencies (LEAs) around the world for investigating and prosecuting crime and terrorism
- National laws commonly oblige telecom operators to support LI for public communications services
- Telecom services under surveillance are defined by national laws, e.g.
  - Telephone calls, Fax, Voicemails
  - SMS, MMS
  - Internet data
  - E-mails
  - VoIP, VoLTE, ViLTE calls
  - other Internet services like Instant Messaging, file sharing, etc.
Lawful Interception

Regulatory Framework

- **National Legislation**
  - Constitution
  - Telecommunications Laws
  - Code of Criminal Procedure
  - Customs and Police Laws

- **International Technical Standards**
  - ETSI
  - ANSI, ATIS
  - CableLabs
  - 3GPP

- **Telecommunications**
  - National Regulations
    - Organization
    - Technology
    - Data Protection
Lawful Interception

General Requirements

Hard requirements
- Compliance with national laws
- Compliance with national technical regulations
- Compliance with international technical standards
- Transparent for users
- No negative impact on telecom services
- Highest security demands (privacy, integrity, unimpeachable results, protection against misuse, transparent to persons under surveillance)
- High reliability of service (24x7)

Soft requirements
- Cost-efficient solution (CAPEX, OPEX)
- Future-proof system
- Technical and legal expertise
- Quality
- Timely delivery
Lawful Interception
Requirements in Practice (example)

- The actual requirements for service providers and network operators are defined by national regulations

<table>
<thead>
<tr>
<th>Organisational Requirements</th>
<th>Technical Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>24x7 service for authorities to accept interception requests</td>
<td>Standard compliant handover (ETSI or national format/protocol)</td>
</tr>
<tr>
<td>Immediate activation of interception decisions</td>
<td>Real-time interception and delivery</td>
</tr>
<tr>
<td>Detailed reporting of all interception events</td>
<td>Transparent for subscribers (hidden intercept)</td>
</tr>
<tr>
<td>Trusted staff</td>
<td>Full intercept of all telecommunication (no data loss)</td>
</tr>
<tr>
<td>Physical access protection</td>
<td>Complete logging of all events</td>
</tr>
<tr>
<td>Internal and external security audits</td>
<td>Prevention of misuse, access control</td>
</tr>
<tr>
<td></td>
<td>Encrypted handover</td>
</tr>
<tr>
<td></td>
<td>99.99% availability</td>
</tr>
</tbody>
</table>
Lawful Interception
The Process from Court Order to Delivery of Intercepted Data

1. Receive warrant from LEA
2. Validation and confirmation
3. Activation of intercept in LIMS and on the network
4. Receipt, buffering, mediation, and delivery of intercept
5. Termination of intercept in LIMS and on the network
Lawful Interception

General Architecture (Functional Model)
Lawful Interception
Utimaco LIMS Overview
Lawful Interception

Access Methods

- **Active (aka on-switch)**
  - Signaling and media (respectively IRI and CC) are intercepted by internal interception functions of the serving network node (e.g. MSC, SGSN, PGW, SBC, S-CSCF)

- **Passive (aka off-switch)**
  - Signaling and media (respectively IRI and CC) are intercepted by probes which filter all data on one or more network links and extract all communication from and to selected targets.

- **Hybrid**
  - Is a mixture of active and passive methods where either signaling is intercepted passively and the media is intercepted actively, or vice-versa.
Lawful Interception

Access Methods

- **Active**
  - Utimaco LIMS
    - X1 (target provisioning)
    - X2/X3 (IRI/CC delivery)
  - Network elements with IIF

- **Passive**
  - Utimaco LIMS
    - X1 (target provisioning)
    - X2/X3 (IRI/CC delivery)
  - Network with tap and probe
    - LIMS Access Point
## Lawful Interception

### Active Interception, Pro’s and Con’s

<table>
<thead>
<tr>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Cost-efficient, software only, commonly no additional hardware needed</td>
<td>▪ Vendor-specific LI interface (INI), requires mediation system</td>
</tr>
<tr>
<td>▪ Fast deployment, reuse of available network nodes</td>
<td>▪ Some vendors require a license on LI interfaces</td>
</tr>
<tr>
<td>▪ Highly available – same as communication service</td>
<td>▪ Limited capacity (number of targets, LI throughput)</td>
</tr>
<tr>
<td>▪ Works with encryption – if the encryption is terminated at the providers network</td>
<td>▪ Trust - some countries don’t trust the IIF of certain vendors.</td>
</tr>
<tr>
<td>▪ Standardized. Requirements and general functions covered in common ETSI, 3GPP standards</td>
<td></td>
</tr>
<tr>
<td>▪ Covers all communication of a target; incl. complex call scenarios, supplementary services</td>
<td></td>
</tr>
<tr>
<td>▪ Broad vendor support</td>
<td></td>
</tr>
<tr>
<td>▪ Secure - extra security profile on serving nodes</td>
<td></td>
</tr>
<tr>
<td>▪ Scalable - scales with the network</td>
<td></td>
</tr>
</tbody>
</table>
## Lawful Interception

### Passive Interception, Pro’s and Con’s

<table>
<thead>
<tr>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Independent of the serving network - no negative impact on performance or availability of the service</td>
<td>▪ High costs for additional hardware (probes and taps)</td>
</tr>
<tr>
<td>▪ Transparent - invisible for the subscriber and for the network</td>
<td>▪ Finite performance - the probe must fit to the network size and throughput. Growth leads to additional costs.</td>
</tr>
<tr>
<td>▪ High capacity - probes are (often) designed to capture large amounts of traffic and support mass monitoring</td>
<td>▪ Limited flexibility – (dynamic) changes within the network or services may require changes on the probes which lead to high maintenance costs and outages (e.g. protocols, call flows, new features, etc.)</td>
</tr>
<tr>
<td>▪ Multi-purpose - probes may be used for multiple purposes at the same time; e.g. LI, performance monitoring, fraud detection, CDR/IPDR generation.</td>
<td>▪ Limited capabilities – (sometimes) probes can not intercept all IRI&amp;CC due to lack of central call control of correlation issues.</td>
</tr>
<tr>
<td>▪ DPI – may be used to monitor and intercept various services/protocols at the same time.</td>
<td>▪ Unencrypted traffic only - probes do not function on encrypted links, but can process plain data only</td>
</tr>
<tr>
<td>▪ Secure - probes are segregated and protected from unauthorized access</td>
<td>▪ Deployment issues - deployment of probes (often) requires detailed knowledge about network links and data flows. Not eligible for software defined networks.</td>
</tr>
</tbody>
</table>
# Lawful Interception

## Hybrid Interception, Pro’s and Con’s

<table>
<thead>
<tr>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Best of both – in some cases a combination of both methods provides a cost-efficient and fast solution; e.g. dynamic Internet access monitoring: passive AAA interception (RADIUS) + active IP data intercept at a access router (BRAS).</td>
<td></td>
</tr>
<tr>
<td>▪ Suitable for split signaling and media links.</td>
<td>▪ Only useful in certain use cases</td>
</tr>
</tbody>
</table>
## Lawful Interception Standards

### LI Standards

<table>
<thead>
<tr>
<th>Organisation/Region</th>
<th>No.</th>
<th>Title/Topic</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ETSI EU, World</strong></td>
<td>TS 101 331</td>
<td>Requirements of Law Enforcement Agencies</td>
<td>Generic</td>
</tr>
<tr>
<td></td>
<td>ES 201 158</td>
<td>Requirements for Network Functions</td>
<td>Generic</td>
</tr>
<tr>
<td></td>
<td>TS 101 671 (ES 201 671)</td>
<td>Handover Interface for the Lawful Interception of Telecommunications Traffic</td>
<td>PSTN, GSM, GPRS</td>
</tr>
<tr>
<td></td>
<td>TS 102 232-1</td>
<td>Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery</td>
<td>IP-generic</td>
</tr>
<tr>
<td></td>
<td>TS 102 232-2</td>
<td>Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for E-mail services</td>
<td>E-Mail</td>
</tr>
<tr>
<td></td>
<td>TS 102 232-3</td>
<td>Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services</td>
<td>Internet Access</td>
</tr>
<tr>
<td></td>
<td>TS 102 232-4</td>
<td>Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services</td>
<td>Internet Access, Layer 2 services</td>
</tr>
<tr>
<td></td>
<td>TS 102 232-5</td>
<td>Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; VoIP and other SIP/RTP based services</td>
<td>VoIP, multimedia services</td>
</tr>
<tr>
<td></td>
<td>TS 102 232-6</td>
<td>Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services</td>
<td>PSTN/ISDN, emulated services</td>
</tr>
<tr>
<td></td>
<td>TS 102 232-7</td>
<td>Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services</td>
<td>Mobile services</td>
</tr>
<tr>
<td></td>
<td>TS 133 106, TS 133 107, TS 133 108</td>
<td>Universal Mobile Telecommunications System (UMTS); LTE; Lawful interception requirements, Lawful interception architecture and functions, Handover interface</td>
<td>GSM, UMTS, LTE</td>
</tr>
<tr>
<td><strong>ATIS/TIA US, CAN</strong></td>
<td>ATIS-1000678v2</td>
<td>LAES for Voice over Packet Technologies in Wireline Telecommunications Networks, also: ATIS-1000678.a.2007, ATIS-1000678.b.2010 (ATIS-1000678v3 on demand)</td>
<td>VoIP</td>
</tr>
<tr>
<td></td>
<td>ATIS-1000013</td>
<td>Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access</td>
<td>IP</td>
</tr>
<tr>
<td></td>
<td>ATIS-0700005</td>
<td>LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE (LAES) FOR 3GPP IMS-BASED VOIP AND OTHER MULTIMEDIA SERVICES (ATIS-0700005.v2 on demand)</td>
<td>IMS-VoIP</td>
</tr>
<tr>
<td><strong>CableLabs, US, World</strong></td>
<td>PacketCable 1.5</td>
<td>Electronic Surveillance Specification</td>
<td>Voice over Cable (telephony)</td>
</tr>
<tr>
<td><strong>3GPP World</strong></td>
<td>TS 33.106, TS 33.107</td>
<td>Lawful interception requirements, architecture and functions, Handover Interface</td>
<td>PacketData, CS Multimedia Services</td>
</tr>
<tr>
<td></td>
<td>TS 33.108</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Abbreviations

- CAPEX  Capital Expenditure
- CC     Content of Communication
- DF2    Delivery Function 2
- DF3P   Delivery Function 3 for Packet Data
- DF3CC  Delivery Function 3 for Circuit-Switched Call
- GSN    GPRS Support Node
- GGSN   Gateway GPRS Support Node
- GPRS   General Packet Radio Service
- HA     High Availability
- HI.1/2/3 Handover Interface 1/2/3
- HSAP   High Speed Access Point
- ICD    Interception Decision
- IDP    Intercept Data Product
- IMS    IP Multimedia Subsystem
- INI    Internal Network Interface
- IP     Internet Protocol
- IRI    Intercept Related Information
- LEA    Law Enforcement Agency
- LI     Lawful Interception
- LIMS   LI Management System
- MC     Monitoring Center
- NE     Network Element
- OMA    Open Mobile Alliance
- OPEX   Operational Expenditure
- PoC    PTT over Cellular
- PTT    Push-To-Talk
- RAI    Remote Administration Interface
- RM     Rack-Mount
- RPU    Remote Provisioning Unit
- RTP    RealTime Protocol
- SBC    Session Border Controller
- SGSN   Serving GPRS Support Node
- SIP    Session Initiated Protocol
- SSL    Secure Socket Layer
- VoIP   Voice-over-IP
Thank you for your attention!