LAWFUL INTERCEPTION

Developed By Obrela Security Industries
George Daglas, MBA IT & Telecommunications
Senior Advisor
Index

1. INTRODUCTION ............................................................................................... 3
2. LEGAL ENVIRONMENT ................................................................................... 5
3. LI PROCEDURES ............................................................................................. 6
4. ARCHITECTURE OVERVIEW ......................................................................... 9
   4.1 Basic Elements of LI ................................................................................ 10
       4.1.1 Internal Intercept Function (IIF) .................................................... 10
       4.1.2 HI 1 Administration Function (ADMF) ........................................... 10
       4.1.3 Mediation Function (MF) ............................................................... 11
5. CONCLUSION ................................................................................................ 12
6. TERMINOLOGY ............................................................................................. 13
7. REFERENCES .................................................................................................. 14
1. Introduction

Information in the modern society is one of our most valuable assets. The need for protection of information has increased dramatically in the last decade since we are now living in an information society. The digital era has introduced new market sectors, electronic commerce, online transactions and has abolished several barriers to entry in the global market. Hand in hand with any technological and economical advancement appear new fraud and crime committing methods targeted at our valuable information assets. The confidentiality, integrity, and availability of information must be safeguarded by a mix of physical, organizational, technical, and legal controls. One of the key technologies for establishing information security is cryptography, systems which use mathematical algorithms and digital keys to encipher data in such a way that only authorized people can decrypt and read them. Cryptography is employed to protect telecommunications, personal data, electronic payment systems, intellectual property rights, sensitive government and business data. Cryptography however is being also used in order to cover criminal activities and evade wiretapping by Law Enforcement Authorities. Since the mid '90s, cryptography has spread widely along with the massive growth of the Internet primarily to facilitate electronic banking, and electronic transactions.

By the late '90s the mobile telecommunications market growth has made the use of cryptography (via GSM) a technology used by millions of people on a daily basis. The use of cryptography as a means of protection of privacy has created the need for establishing a Legal as well as technological framework in order to perform Lawful Interception (LI).

Lawful interception (LI) is the legally sanctioned official access to private communications, such as telephone calls or e-mail messages. In general, LI is a security process in which a network operator or service provider gives law enforcement officials access to the communications of private individuals or organizations. With small variations from country to country the LI system must provide transparent interception of specified traffic only and the subject must not be aware of the intercept. The service provided to other users must not be affected during interception.

The usage of Lawful Interception has been and still is one of the most controversial issues of modern society. The concerned segment of the public claim that use of LI abuses their human and privacy rights. Since the interception capabilities include any possible type of Voice Telecommunication –Cellular, Fixed and Voice over IP– Data
Exchange –Video, FAX, SMS, E-mail– and Internet access –Peer to Peer networks for chat or file sharing, Instant messaging like MSN and Yahoo Messenger, websites visited– a great feeling of insecurity is created.

The great controversy arises from the fact that governments worldwide state that the sole purpose of using LI is the national and individual security by preventing national and international crime, treason and break of public order, terrorist activities and by assisting in solving crimes such as murders, extortions, money laundering, drugs distribution, discovering criminal networks and terrorist associations.
2. Legal Environment

"Lawful interception plays a crucial role in helping law enforcement agencies to combat criminal activity. Lawful interception of public telecommunications systems in each country is based on national legislation in that country. The purpose of standardization of lawful interception in ETSI is to facilitate the economic realization of lawful interception that complies with the national and international conventions and legislation. The Technical Committee on Lawful Interception (TC LI) is the leading body for lawful interception standardization within ETSI. Lawful interception standards have also been developed by ETSI technical bodies AT, TISPAN (/SPAN and TIPHON™), TETRA, and by 3GPP™ (/SMG).” Source: ETSI

In several European Countries the Legal Framework for Lawful Interception has already been established for almost a decade. However it was not until after the terrorist hit in London in July 2005 that the European Union has published a directive for enforcing LI in all EU member countries. In Greece it was not until March 2005 that LI has become a National Law, however no national technical standards have been established yet.

![Figure 1 (Legal Framework for LI)](image-url)
3. LI Procedures

Lawful Interception is a system and, like every system its’ operation - involves Technology (Hardware, Software, Networks) People (Law Enforcement Agencies, Government and Legislation authorities, Network and Service provider employees) and Official Procedures that have to be followed in order for the interception to be legal, and in order for the evidence collected to be admissible for prosecution by the Judicial Authorities.

LI is regulated and procedures exist worldwide for its enforcement. Variations may exist from country to country but the following concept is a common practice:

1. The Law Enforcement Agency prepares a warrant authorizing interception of communications against a person
2. The Warrant is approved by the responsible Judicial Authority
3. The Warrant is then served on communications company(ies)
4. Communications company(ies) initiates the warrant on their network
5. When warranted party carries out communications, it and associated information are transmitted to the Law Enforcement Monitoring Facility (LEMF) of the Law Enforcement Agencies (LEA)

The above mentioned procedures, which are schematically depicted in figures 2 and 3, are in place in order to safeguard that the individual parties involved can not take advantage of the LI capabilities for unlawful and unjustified purposes. The transmission of the information intercepted is transmitted via the “handover interfaces” which are further described in chapter 4.

According to ETSI standards, safeguarding the integrity and confidentiality of the information transmitted via the handover interfaces is an obligation of the Service Provider/Network Operator. In this regard basic measures that must be followed include restricting to a minimum the interception involved personnel, ensuring that the interception takes place and is contained in specific rooms/locations which restricted access, ensuring that the product of the interception is transmitted/delivered only to the authorized Law Enforcement Monitoring Facility (LEMF) following manual and electronic (if available) authentication procedures, strictly monitoring and enforcing access control and non repudiation measures for enabling and disabling of the LI capabilities.

Asymmetric Encryption via Public Key Infrastructure is a technology that fulfills most of the above mentioned security requirements, thus Lawful Interception Solutions are usually PKI enabled.
Figure 2 Basic Interception Process – Request
Figure 3 Basic Interception Process - Delivery
4. Architecture Overview

Although the detail of LI may vary from country to country we can look at the general logical and physical requirements and also explain much of the common terminology used.

The primary purpose of the service provider network is to enable private communications between individuals while any LI functionality built into the network must not affect the normal service to those individuals. According to ETSI “The generic Handover Interface adopts a three-port structure such that administrative information (HI1), Intercept Related Information (HI2) and the Content of Communication (HI3) are logically separated.”

![Diagram of Communication network, Lawful Interception Solution, and LEA](image)

*Figure 4*
4.1 Basic Elements of LI

The basic elements required in order to perform Lawful Interception are the “Internal Intercept Function (IIF)” in the network nodes of the Carrier/Service Provider (Figure 4 – Switches – Servers – Network Elements), the Mediation Function (MF) between the Carrier/Service Provider and Law Enforcement Monitoring Facility (Figure 4 – HI2 and HI3) and the Administration Function (ADMF) to manage orders for interception in the Carrier/Service Provider (Figure 4 – HI1).

4.1.1 Internal Intercept Function (IIF)

These functions are located in the network nodes where information passes through (Switches, Servers, Network Elements). IIF serves the purpose of “filtering” “capturing” “forwarding” information - Intercept Related Information (IRI) and Contents of Communications (CC)- intercepted from the target and forwarding it to the Mediation Function (MF) Handover Interfaces (HI2 and HI3).

In the majority of the implementations IIF is a hardware based solution since it performs a processing intensive task. If this task is left to be performed by the network nodes, delays may occur resulting in the detection of the interception.

4.1.2 HI 1 Administration Function (ADMF)

Handover Interface 1 (HI 1) is concerned with the flow of the warrant specific information. A warrant specifies the target which the LEA wants to be intercepted. Consequently the Carrier/Network Operator (NOT the LEA) loads the warrant on the LI administration system which reports significant events to the LEA such as when the warrant was loaded, when it was activated and deactivated. In the case of the electronic LI each target requires a Warrant ID and Case ID assigned by the LEA. Each case may require IRI or CC or both to be intercepted. Each task is assigned a start date and an end date, upon which the case will expire. The ADMF is typically responsible for auditing the IIFs to ensure that the target lists match and that there are no differences or discrepancies.

In the majority of the implementations LI Administration Function (ADMF) is based on a security hardened management system and provides a secure method of targeting and routing intercept traffic via a secure connection with one or more IIFs and Mediation Function (MF) units. The ADMF must be accessed only by authorized users as it manages...
the deployment of tasks to all the other LI elements. The Administration Function (ADMF) makes the requests for the interception, the IIF collects Intercept Related Information (IRI) and Contents of Communication (CC) and the Mediation Function (MF) converts them to a generic format and sends them to the Law Enforcement Monitoring Facility (LEMF).

4.1.3 Mediation Function (MF)

The Mediation Function (MF) serves the purpose of communicating with the IIFs and performing the mediation and delivery functions from the IIFs to the (LEMF). Specifically, the MF receives IRI and CC data from the IIFs in a generic format and translates them to a specific format required by the LEA.

The MF uses the Handover Interface 2 for transmitting Intercept Related Information (IRI) such as who is calling whom and where from, service information such as, in the case of a cellular interception, the nearby antennas and their relevant signal, which can determine the location of the subject intercepted with very high accuracy usually within a range of 2 to 50 meters. The accuracy is dependent on various parameters such as the number of antennas in the region, the type of network used (GSM or 3G), the signal strength etc.

HI2 is often the most important part of the intercept since LEAs are usually more interested in who is talking to who rather than in what they are actually saying.

Handover Interface 3 is used by the MF for transmitting Content of Communication such as the actual Voice content, Faxes, SMS, Videoconferencing, E-mail, Internet IP packets, etc.

The Mediation Function (MF) receives target details from the Administration Function (ADMF) and validates the received IRI and CC data to ensure that only the warranted data is passed to the Law Enforcement Monitoring Facility. The Mediation Function (MF) may support forwarding of the intercepted traffic to multiple Law Enforcement Monitoring Facility interfaces.
5. Conclusion

There is a very fine line between Lawful and Un-Lawful Interception which is dependent primarily on the legal and regulatory framework, followed by the policies and procedures involved in its utilization monitoring and inspection and finally on the technology involved. In most EU countries the Legal and Regulatory Framework for LI already exists, and where it does not exist it will be developed according with the EU Directive of December 2005. In addition, the technology involved is very well standardized and documented worldwide since interoperability is a major requirement for LI solutions. In other words almost every LI solution is similar to every other LI solution. This leaves us with the weakest link in ensuring that LI solutions are utilized only by authorized people for lawful purposes, which is policies, procedures and common practices in the utilization of the LI system.

In this regard, the only way to ensure that such systems will not be used against the human and privacy rights of individuals, for industrial espionage or for counterintelligence is establishing a strict policies and procedures framework such as minimizing the involved individuals from all parties, performing background checks on them, consistently training them in the appropriate use of the system, continuously monitoring and auditing the use of the LI systems -preferably by independent authorities- enforcing four eyes policies for every task involved on an operational level and utilizing authentication solutions that guarantee accountability and non-repudiation. The above mentioned policies may be considered the minimum baseline security policies for the secure operation of LI.

LI is very well standardized, regulated and documented worldwide. It is however of imperative importance that when LI solutions are deployed and utilized, conformity with the standards is ensured both from a procedural and from a technological / architectural standpoint due to the immense potential impact when misused or abused.
6. Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMF</td>
<td>Administration Function</td>
</tr>
<tr>
<td>CALEA</td>
<td>Communications Assistance for Law Enforcement Act</td>
</tr>
<tr>
<td>CC</td>
<td>Contents of Communication</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>HI</td>
<td>Handover Interface</td>
</tr>
<tr>
<td>IIF</td>
<td>Internal Intercept Function</td>
</tr>
<tr>
<td>INI</td>
<td>Internal Networks Interface</td>
</tr>
<tr>
<td>IRI</td>
<td>Intercept Related Information</td>
</tr>
<tr>
<td>LEA</td>
<td>Law Enforcement Agency</td>
</tr>
<tr>
<td>LEMF</td>
<td>Law Enforcement Monitoring Facility</td>
</tr>
<tr>
<td>LI</td>
<td>Lawful Interception</td>
</tr>
<tr>
<td>MF</td>
<td>Mediation Function</td>
</tr>
</tbody>
</table>
7. References

<table>
<thead>
<tr>
<th>Organization</th>
<th>Standard ID</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETSI</td>
<td>TS 102 232</td>
<td>V1.1.1 (2004-02)</td>
<td>Telecommunications security; Lawful interception; Handover specification for IP delivery</td>
</tr>
<tr>
<td>ETSI</td>
<td>TS 102 233</td>
<td>V1.1.1 (2004-02)</td>
<td>Telecommunications security; Lawful interception; Service specific details for E-Mail delivery</td>
</tr>
<tr>
<td>ETSI</td>
<td>TS 102 234</td>
<td>V1.1.1 (2004-11)</td>
<td>Telecommunications security; Lawful interception; Service specific details for Internet Access Services</td>
</tr>
<tr>
<td>ETSI</td>
<td>TS 101 671</td>
<td>V2.8.1 (2003-11)</td>
<td>Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic</td>
</tr>
<tr>
<td>ETSI</td>
<td>TS 101 331</td>
<td>V1.1.1 (2001-08)</td>
<td>Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies</td>
</tr>
<tr>
<td>ETSI</td>
<td>TS 133 106</td>
<td>V5.1.0 (2002-09)</td>
<td>Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful interception Requirements</td>
</tr>
<tr>
<td>ETSI</td>
<td>TS 133 107</td>
<td>V5.6.0 (2003-09)</td>
<td>Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful interception Architecture and Functions</td>
</tr>
<tr>
<td>ETSI</td>
<td>TS 133 108</td>
<td>V5.6.0 (2003-12)</td>
<td>Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI)</td>
</tr>
</tbody>
</table>