ETSI & Lawful Interception of IP Traffic

Jaya Baloo RIPE 48

May 3 Amsterdam, The

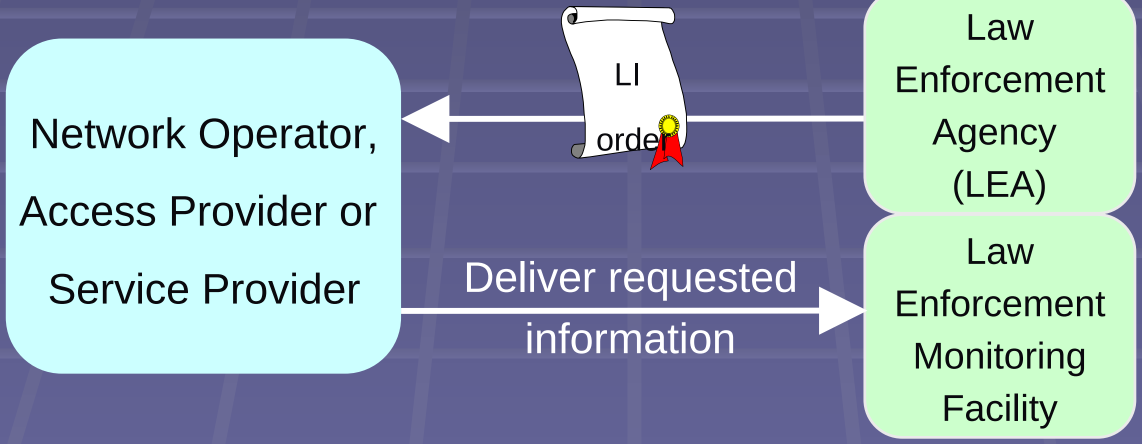
Netherlands

Contents

- **Introduction to Lawful Interception**
- **Interception of Internet services**
- **Origins in The European Community**
- **The European Interception Legislation in Brief**
- **ETSI Standards – 101 232, 101 233, 101 234**
- **Interception Suppliers & Discussion of Techniques**
- **Future Developments & Issues**

Introduction to Lawful Interception

- ETSI definition of (lawful) interception:
  - **interception:** action (based on the law), *performed* by an network operator/access provider/service provider (NWO/AP/SvP), of making available certain information and providing that information to a law enforcement monitoring facility.



LI’s Raison D’etre

- Why intercept?
  - Terrorism
  - Pedophilia rings
  - Cyber stalking
  - Data theft –Industrial espionage
  - Drug dealers on the internet
- Why not?
  - Privacy
  - Security

Legal Issues in LI

- Judge: "Am I not to hear the truth?"
  Objecting Counsel: "No, Your Lordship is to hear the evidence."

- Some characteristics of evidence- relevance to LI
  - Admissible – can evidence be considered in court– *differs per country
  - Authentic – explicitly link data to individuals
  - Accurate – reliability of surveillance process over content of intercept
  - Complete – tells a "complete" story of a particular circumstance
  - Convincing to juries – probative value, and subjective practical test of presentation

Admissibility of Surveillance Evidence

- Virtual Locus Delecti
- Hard to actually find criminals in delicto flagrante

- How to handle expert evidence? Juries are not composed of network specialists. Legal not scientific decision making.

- Case for treating Intercepted evidence as secondary and not primary evidence
  - **Primary** – is the best possible evidence – e.g. in the case of a document – its original.
  - **Secondary** – is clearly not the primary source – e.g. in the case of a document – a copy.

Interception of Internet services

Interception of Internet services

What are defined as Internet services?

- access to the Internet
- the services that go over the Internet, such as:
  - surfing the World Wide Web (e.g. html),
  - e-mail,
  - chat and icq,
  - VoIP, FoIP
  - ftp,
  - telnet

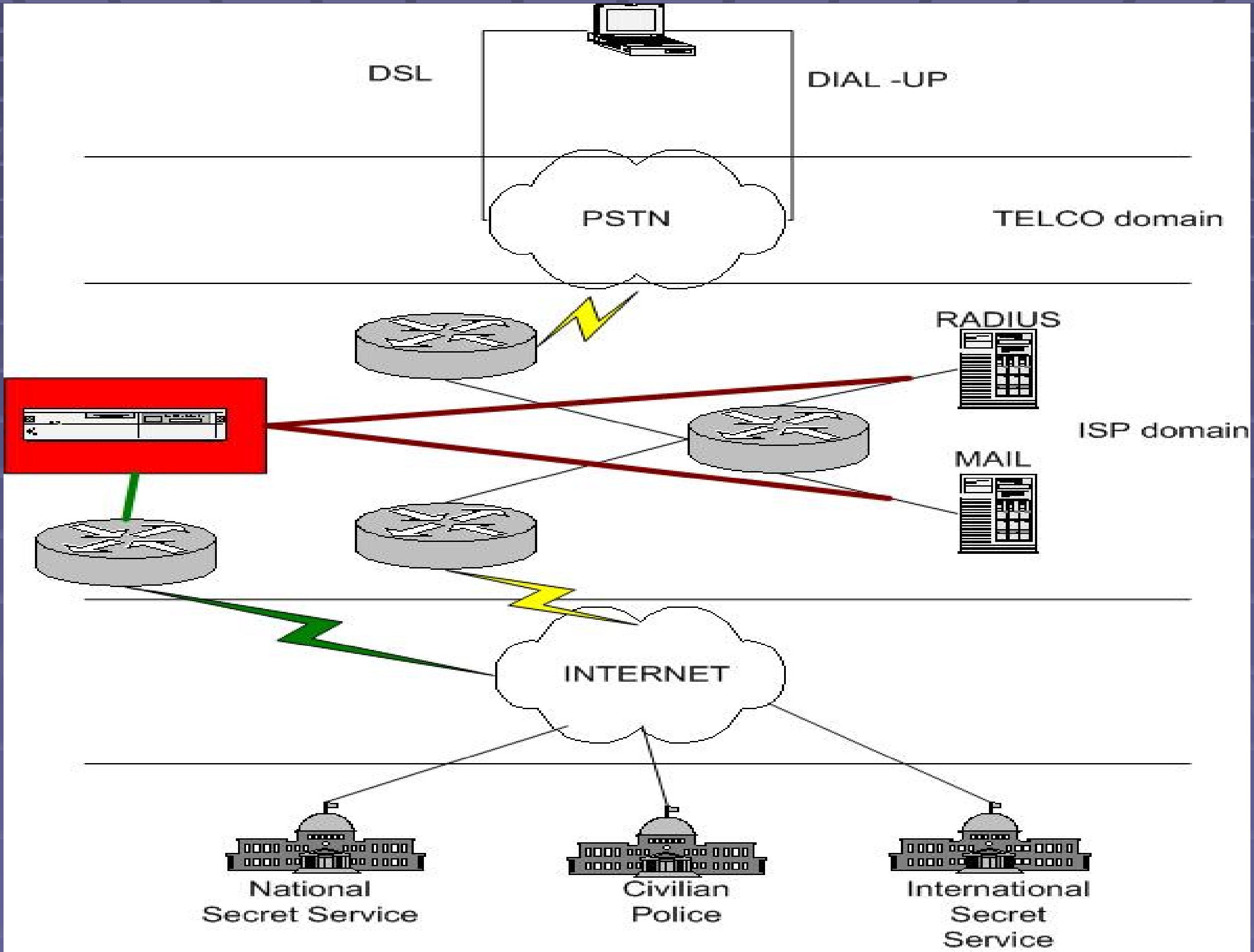
What about encrypted traffic?

  - Secure e-mail (e.g. PGP, S/MIME)
  - Secure surfing with HTTPS (e.g. SSL, TLS)
  - VPNs (e.g. IPSec)
  - Encrypted IP Telephony (e.g. pgp -phone and Nautilus)
  - etc.
- If applied by NWO/AP/SvP then
  - encryption should be stripped before sending to LEMF or
  - key(s) should be made available to LEA

else

  - *a challenge for the LEA*

Logical Overview



Technical Challenges

- Req. –Maintain Transparency & Standard of Communication
- Identify Target - Monitoring Radius – misses disconnect
- Capture Intercept information – Effective Filtering Switch
- Packet Reassembly
- Software complexity increases bugginess
- Peering with LEMF – monitoring multiple XDSL ccts.

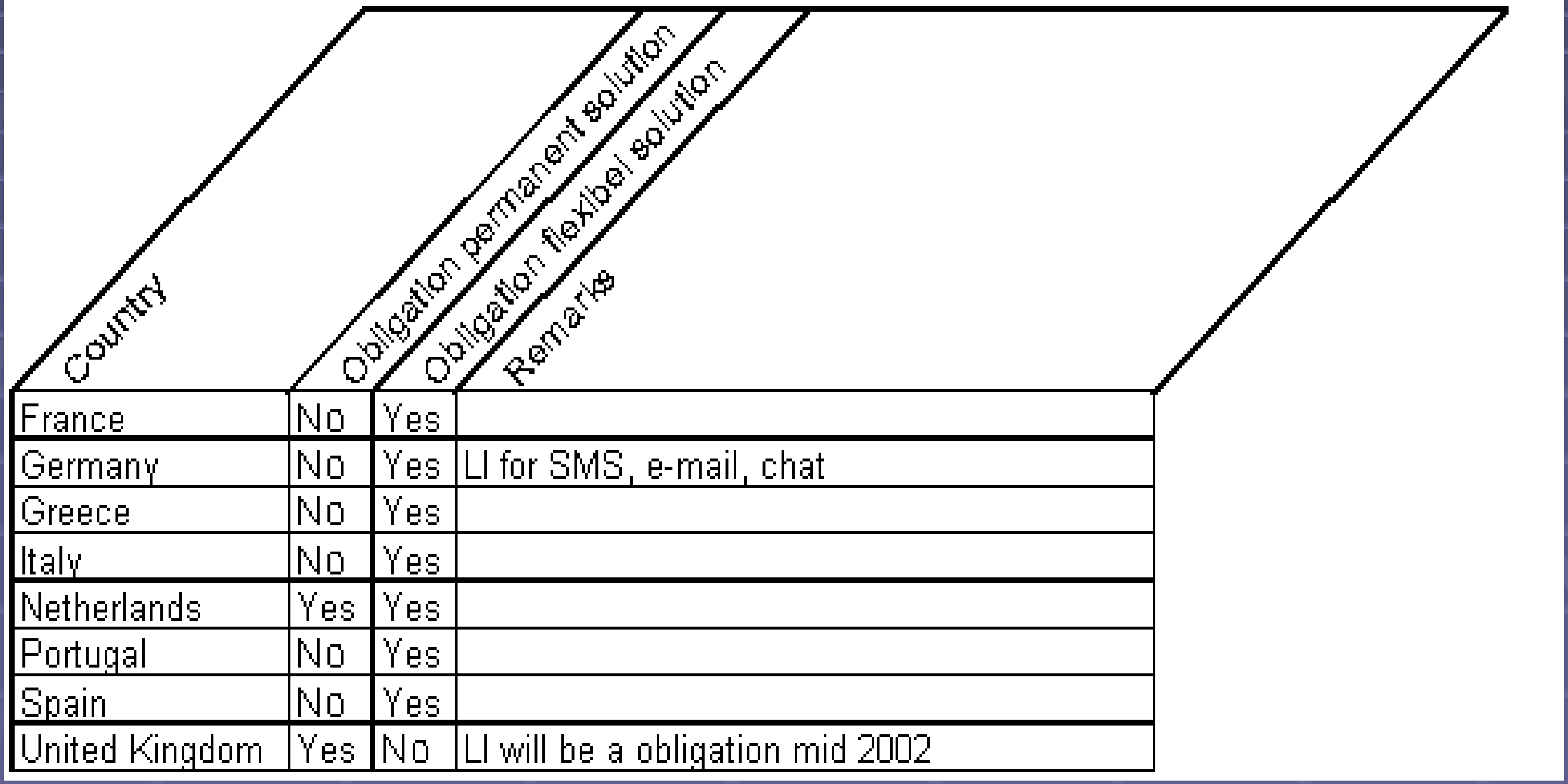
Origins in The European Community

What is LI based on in the EU?

- Legal Basis
  - EU directive
  - Convention on Cybercrime – Council of Europe-
    - Article 20- Real time collection of traffic data
    - Article 21- Interception of content data
  - National laws & regulations
- Technically
  - Not Carnivore
  - Not Calea
- Standards, Best Practices based approach
  - IETF’s standpoint (RFC 2804 IETF Policy on Wiretapping)

The European Interception Legislation in Brief

Solution Requirements



Country	Obligation permanent solution	Obligation flexibel solution	Remarks
France	No	Yes	
Germany	No	Yes	LI for SMS, e-mail, chat
Greece	No	Yes	
Italy	No	Yes	
Netherlands	Yes	Yes	
Portugal	No	Yes	
Spain	No	Yes	
United Kingdom	Yes	No	LI will be a obligation mid 2002

European Interception Legislation

- France
  - Commission Nationale de Contrôle des Interceptions de Sécurité -- La loi 91-636
  - Loi sur la Securite Quotidienne – November 2001
- Germany
  - G-10 – 2001- ”Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses”
  - The Counter terrorism Act – January 2002

UK Interception Legislation

- UK
  - Regulation of Investigatory Powers Act 2000
  - Anti-terrorism, Crime and Security Act 2001

- “The tragic events in the United States on 11 September 2001 underline the importance of the Service’s work on national security and, in particular, counter-terrorism. Those terrible events significantly raised the stakes in what was a prime area of the Service’s work. It is of the utmost importance that our Security Service is able to maintain its capability against this very real threat, both in terms of staff and in terms of other resources. Part of that falls to legislation and since this website was last updated we have seen the advent of the Regulation of Investigatory Powers Act 2000, Terrorism Act 2000 and the Anti-Terrorism Crime and Security Act 2001. Taken together these Acts provide the Security Service, amongst others, with preventative and investigative capabilities, relevant to the technology of today and matched to the threat from those who would seek to harm or undermine our society. “ – The UK Home Secretary’s Foreword on MI5

The Case in Holland

- At the forefront of LI : both legally & technically

- The Dutch Telecommunications Act 1998– Operator Responsibilities
- The Dutch Code of Criminal Proceedings – Initiation and handling of interception request
- The Special Investigation Powers Act -streamlines criminal investigation methods
- WETVOORSTEL 20859 – backdoor decree to start fishing expeditions for NAW info – Provider to supply info not normally available

TIIT STANDARD – predecessor to current ETSI standards

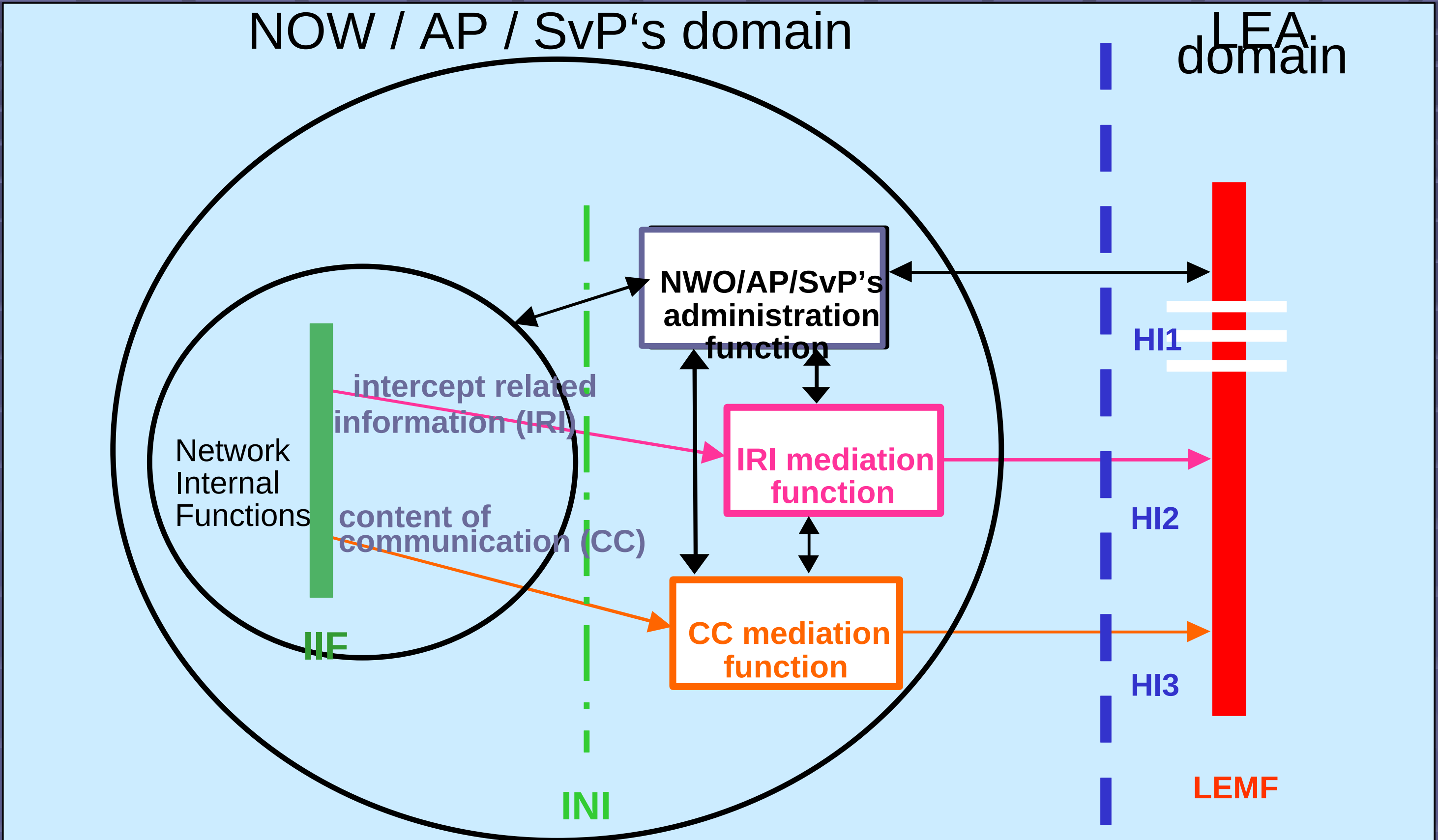
- LIO – National Interception Office – in operation since end of 2002

European Telecommunications Standards Institute

ETSI TR 101 944

- Responsibility- Lawful Interception requirements must be addressed separately to Access Provider and Service Provider.
- 5 layer model - Network Level & Service Level division
- Implementation Architecture –
  - Telephone cct. (PSTN/ISDN)
  - Digital Subscriber Line (xDSL)
  - Local Area Network (LAN)
    - Permanent IP Address
- Security Aspects
- HI3 Delivery

The ETSI model


NOW / AP / SvP‘s domain
LEA domain
NWO/AP/SvP’s administration function
intercept related information (IRI)
Network Internal Functions
content of communication (CC)
IRI mediation function
CC mediation function
IIF
INI
HI1
HI2
HI3
LEMF

LI handover interface HI

HI1: administrative information

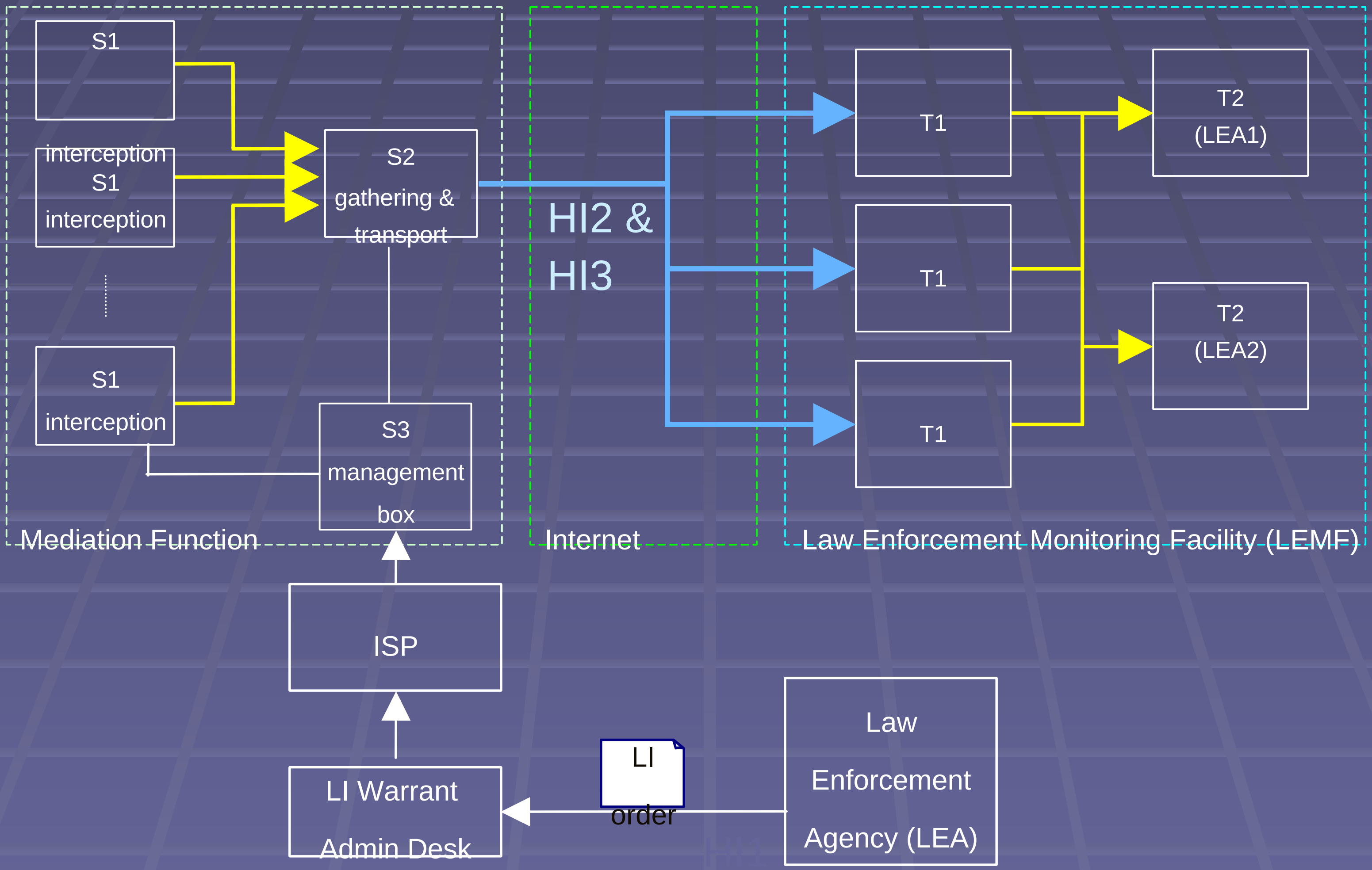
HI2: intercept related information

HI3: content of communication

IIF: internal interception function

INI: internal network interface

Sample Architecture for HI2 and HI3



ETSI 101 232 – IP Delivery

- Specifies:
  - modular approach used for specifying IP based handover interfaces
  - header(s) to be added to IRI & CC sent over HI2 & HI3
    - (R4 LIID)   (R5 & R7 Communication Identifier)
    - (R37 & R38 Timestamp)
    - (R15 & R19 Sequence Number)
    - (R10 Direction)
    - (R9 Payload Type) (R8 Interception Type)
  - protocols for the transfer of IRI & CC
  - protocol profiles for the handover interface

ETSI – 101 232 – Protocol Stack

LAYER NAME	OSI Layer	Clause	Responsibilities
Handover	6 & 7	6.2	Create & maintain one or more delivery functions. Error Reporting. Aggregate PDUs; Associate header info; Create padding PDUs; Assign PDUs to delivery functions
Session	5	6.3	Create & maintain a single transport connection and monitor its status. Run keepalive mech.; Encode/ decode PDU elements; integrity mech, Buffer data
Transport	4	6.4	Create & maintain a network cct.
Network	3	6.5	Network Protocol

ETSI 101 233 – EMAIL

- “Stage 1”description of interception info. in process of sending & receiving email
- “Stage 2” description of when IRI & CC shall be sent and what info it shall contain

- Email Send Event
- Email Recieve Event
- Email download event – distinction – client
    - Content intercept or complete session
    - Webmail

ETSI 101 234- Internet Access Services

- “Stage 1” description of the interception information in relation to the process of binding a “target identity” to an IP address when providing IAS
- “Stage 2” description of when IRI & CC shall be sent and what info. it shall contain

  - LI Requirements -administrative as well as capturing of traffic
  - Preventing over and under collection of intercept data
  - Reference Topologies & Scenarios
  - Further Radius & DHCP
  - IP IRI intercepts & TCP,UDP IRI intercepts

ETSI 101 234- Internet Access Services contd. 2

- Target Identity-
  - Username or Network Access Identifier
  - IP address (Ipv4 or Ipv6)
  - Ethernet address
  - Dial-in Number calling line identity
  - Cable Modem Identifier
  - Other unique identifier agreed beteween AP & LEA

Result of interception- provided when

  - Attempt to access the access network
  - When access to access network permitted /not
  - On change of status/ location

ETSI 101 234- Internet Access Services contd. 3

- IRI contains-
  - Identities used by or associated with the target identity (dial in calling line number and called line number, access server identity, ethernet addresses, access device identifier
  - Details of services used and their associated parameters
  - Info. relating to status
  - Timestamps

CC shall be provided for every IP datagram that:

  - Has the target's IP address as the IP source address
  - Has the target's IP address as the IP destination address

CC shall contain a stream of octets for every

Interception Suppliers & Discussion of Techniques

LI Implementations

- Verint formerly known as Comverse Infosys
- ADC formerly known as SS8
- Accuris
- Pine
- Nice
- Aqsacom
- Digivox

- Telco/ ISP hardware vendors
  - Siemens
  - Alcatel
  - Cisco
  - Nortel

Implementation techniques

- Active- direct local interception – i.e. Bcc:
- Semi-Active- interaction with Radius to capture and filter traffic per IP address
- Passive- no interaction with ISP required only interception point for LEA device

- Most of the following are active or a combination of active and semi-active implementations

Verint = Comverse - Infosys

- Based in Israel – Re : Phrack 58-13
- Used by Dutch LEMF
- Used extensively internationally – supports CALEA & ETSI
- Use of Top Layer switch

- Response

NICE

- Used in BE as t1
- Proprietary – implemented for ETSI
- Feat., topic extraction, Keyword Spotting, Remote Send of CC
- Auto Lang. detection and translation
- Runs on Windows NT &2000 Svr.
- Stand alone internet/ telephony solution

ADC = SS8

- Use of proprietary hardware
- Used for large bandwidth ccts.
- Known to be used in Satellite Traffic centers
- Supports CALEA – ETSI
- Use of Top Layer switch

Accuris

- Max. of 50 concurrent taps
- Solution not dependant on switch type
- Can use single s2 as concentrator
- Offer Gigabit Solution – but depends on selected switch capability and integration with filter setting
- Supports Calea & ETSI

It’s all about the M$ney

- Solutions can cost anywhere from 100,000 Euro to 700,000 Euro for the ISP
- UK Govt. expected to spend 46 billion over the next 5 years- subsequently reduced to 27 billion
- Division of costs
  - Cap Ex = ISP
  - Op Ex = Govt.
- Penalties for non-compliance
  - Fines – up to 250,000 euros
  - Civil Charges
  - House Arrest of CEO of ISP
- Cooperation between ISPs to choose single LI tool

Conclusions for Law Enforcement

- “If you’re going to do it … do it right”
  - Disclosure of tools and methods
  - Adherence to warrant submission requirements
  - Completeness of logs and supporting info.
  - Proof of non- contamination of target data
  - Maintaining relationship with the private sector
- Law Enforcement personnel
  - Training
  - Defining role of police investigators
  - Defining role of civilian technicians
  - Handling Multi – Focal investigations

Future Developments & Issues

- EU Expansion – Europol stipulations
- Data Retention Decisions
- ENFOPOL organization
- Borderless LI
- ISP Role
- EU wide agreements on Intercept Initiation
- Quantum Cryptography
- WLAN challenges
- The Future of Privacy Legislation ?

Web Sites

- www.opentap.org
- http://www.quintessenz.at/cgi-bin/index?funktion=doquments
- www.phrack.com
- www.cryptome.org
- www.statewatch.org
- www.privacy.org
- www.iwar.org.uk
- www.cipherwar.com
- www.cyber-rights.org/interception

Q&A / Discussion

- Does LI deliver added value to Law Enforcement’s ability to protect the public?
- What about open source Interception tools?
- Will there be a return of the Clipper Chip?
- Should there be mandated Key Escrow of ISP’s encryption keys?
- What types of oversight need to be built into the system to prevent abuse?

Thank You.

Jaya Baloo
jaya@baloos.org
+31-6-51569107