Lawful Interception of IP Traffic: The European Context

Jaya Baloo
July 30, 2003

BLACKHAT
Las Vegas, Nevada
Contents

- Introduction to Lawful Interception
- Interception of Internet services
- Origins in The European Community
- The European Interception Legislation in Brief
- ETSI
- The Dutch TIIT specifications
- 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
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

<table>
<thead>
<tr>
<th>Country</th>
<th>Obligation permanent solution</th>
<th>Obligation flexible solution</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>No</td>
<td>Yes</td>
<td>LI for SMS, e-mail, chat</td>
</tr>
<tr>
<td>Greece</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Yes</td>
<td>No</td>
<td>LI will be a obligation mid 2002</td>
</tr>
</tbody>
</table>
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**
  - 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 www.MI5.gov
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
- LIO – National Interception Office – in operation since end of 2002
- CIOT – central bureau for interception for telecom
European Telecommunications Standards Institute
Technical Specs. of Lawful Interception The ETSI model

NOW / AP / SvP’s domain

LEA domain

Network Internal Functions

IIF: internal interception function
INI: internal network interface

HI1: administrative information
HI2: intercept related information
HI3: content of communication

intercept related information (IRI)
content of communication (CC)

NWO/AP/SvP’s administration function

IRI mediation function

CC mediation function

HI1
HI2
HI3
LEMF

IIF
INI

LI handover interface HI
ETSI

- Purpose of ETSI LI standardization – “to facilitate the economic realization of lawful interception that complies with the national and international conventions and legislation”
- Enable Interoperability – Focuses on Handover Protocol
- Formerly ETSI TC SEC LI – working group
- Now ETSI TC LI – separate committee standards docs.
- DTS/LI-00005 – Service specific details for internet access – RADIUS DHCP – etc. how to intercept internet access services – payload
- DTS/LI-00004 – Email specific
- Extras VOIP PPP tunneling – proposals
- IPV6 - integrate in 0005 ?
- Current Status : still in progress
- Comprised primarily of operators and vendors - WG LI
- ETSI TR 101 944 – The Issues
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 Dutch TIIT specifications
The TIIT

- WGLI
- The Players
- The End Result V.1.0
- The deadlines – Full IP & Email –2002
- NLIP
- Costs
- ISP Challenge
TIIT

- User (LEA) Requirements for transport

- Description of Handover Interface
  - HI1: method depends on LEA, but also contains crypto keys
  - HI2: events like login, logout, access e-mailbox, etc.
  - HI3: Content of Communication and additional generated information (hash results and NULL packets)

- Description of General Architecture for HI2 and HI3

- Handover Interface specification
  - Global data structures
  - S1 – T2 Traffic Definition
  - Data structures and message flows for HI2 and HI3
  - Use of cryptography
TIIT

General Architecture for HI2 and HI3
TIIT

General Architecture for HI2 and HI3

**S1:**
- Intercept target traffic
- Time stamp target packets
- Generate SHA hash over 64 target packets
- Encrypt with key specific for this interception
- Send to S2

**S2:**
- Collect target packets from authenticated S1s
- Distribute target packet randomly over the T1s over a TLS or IPsec channel
- Use X.509 certificates for mutual authentication
TIIT - General Architecture for H12 and H13

- S3 is not really TIIT
- Management system for
  - Starting & stopping interceptions
  - Collect billing data
  - Etc.

Mediation Function

Internet

Law Enforcement Monitoring Facility (LEMF)

H12 & H13
TIIT - General Architecture for HI2 and HI3

- **T1s:**
  - End TLS or IPsec channel(s)
  - Forward data to T2(s) of the LEA that ordered the interception

- **T2:**
  - Decrypt packets from S1s
  - Check integrity

Diagram:

- S1 interception
- S2 gathering & transport
- S3 management box
- Mediation Function
- HI2 & HI3
- Internet
- Law Enforcement Monitoring Facility (LEMF)
- T1
- T2 (LEA1)
- T2 (LEA2)
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
NICEL

- 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