Lawful Interception - Historical context and future challenges for Internet Service Providers

Dr. Philip Branch

Senior Lecturer (Telecommunications)

Outline

- Introduction to Lawful Interception (LI)
- Telecommunications Companies and LI
- Internet Service Providers and LI
- LI Research

What is Lawful Interception?

- Interception of communications between parties of 'interest' to the Law Enforcement Agencies
  - LEAs are police (state and federal), intelligence agencies, anti-corruption commissions
- LI is very tightly regulated
  - Need a warrant from a magistrate to use LI for investigating a crime
  - Attorney General authorises intercepts for intelligence gathering
  - Regular audits
- A condition for issuing a communications license
  - Governments will not allow communications companies to operate if they cannot provide interception facilities
- Any communications can be subject to interception
  - Not just voice. Can be emails, faxes, Internet chat rooms, file transfers, multi-player games…

Should Governments do interception?

- Why Intercept?
  - Crime investigation
  - Crime prevention
  - Intelligence gathering
  - Strong impetus following terrorist attacks in New York and Bali
- Why not?
  - Privacy
    - Abuse by Government
    - Blackmail
    - Identity theft
  - Security
    - Interception is about enabling eavesdropping on communications
    - By definition LI compromises network security

Should Governments do interception?

- Quote from Foundation for Information Policy Research (FIPR), an organisation concerned with protection of individual privacy (UK)

"Those who question the arrangements for oversight of interception are often supposed to be critical of the rights of the state to conduct secret surveillance. FIPR supports carefully targeted government surveillance of telecommunications in the fight against serious crime and for the collection of foreign intelligence.

"However public support for these activities has been very seriously eroded by the poor management of previous governments …

Australian Legislation

- Telecommunications (Interception) Act 1979
- Specifies obligation of “carriers” to provide LI
  - Carriers include ISPs!!
- Differentiates between interceptions for intelligence gathering and criminal investigations
- Specifies penalties for non-compliance
- Specifies penalties for unlawful interception
- Specifies interception must be identity based
  - Person or a subscriber number
  - Compare with some countries which allow device level interception

Outline

- Introduction to Lawful Interception (LI)
- Telecommunications Companies and LI
- Internet Service Providers and LI
- LI Research

Telecommunications Companies and LI

- Provide interception in the public access network
  - PSTN, GSM, GPRS, UMTS
  - Specific nodes that have LI capabilities: (MSC, SGSN)
- Have borne the main burden of interception
  - Until recently, telecommunications companies were either heavily regulated (US) or a government department (Australia and most of Europe)
  - Services other than voice are a relatively new
  - Access networks are an easy location in which to intercept
  - Telecommunications companies have the resources needed to provide interception
- Highly standards oriented
  - Lawful interception, like everything else related to telecommunications infrastructure is defined in great detail by international standards
  - There are LI standards for all public access network technologies

Telecommunications LI Standards

- European Telecommunications Standards Institute (ETSI)
  - Europe, Australia (soon) and much of Asia
- G-10
  - Germany
  - Forerunner to ETSI standards
- CALEA
  - Communications Assistance to Law Enforcement Agencies
  - North American standards
- SORM
  - Russian Federation and some former Eastern bloc countries
- Domestic ‘standards’
  - Australia

LI Procedures

- LEA prepares a warrant authorising and compelling interception of communications against a person
- Warrant is approved by a magistrate (or Attorney General)
- Warrant is then served on communications company
- Communications company initiates the warrant on their network
- When warranted party carries out communications, it and associated information are transmitted to LEA

LI Architecture (ETSI)

- How does this procedure get implemented according to the standards?
- ETSI defines three Handover Interfaces between the Network Operator and the LEA
  - HI1 Administrative Information
  - HI2 Intercept Related Information
  - HI3 Content of Communication
- Each interface provides separation of responsibilities and information

Handover Interface 1

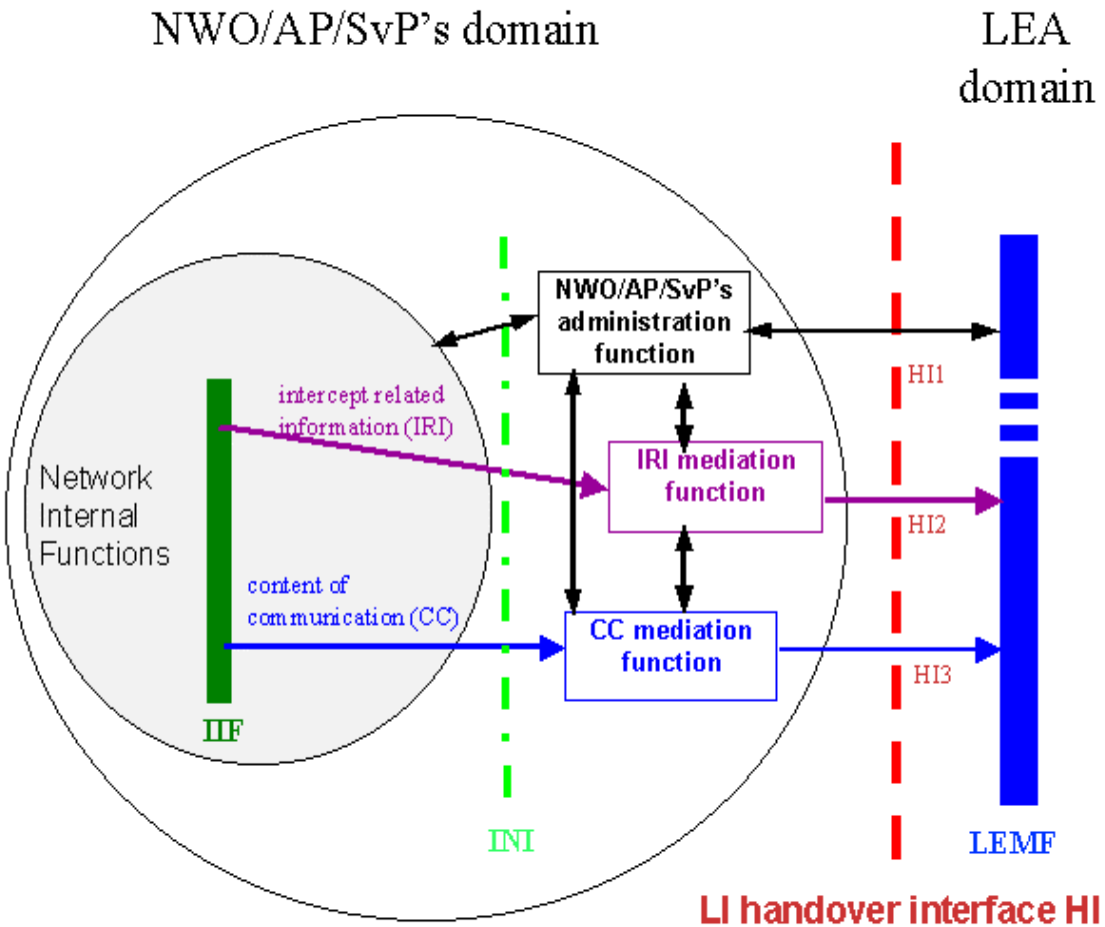
- Administrative Interface
- Concerned with the flow of warrant information
- A warrant specifies who the LEA wants intercepted
- Carrier loads the warrant on the LI administration system
  - LEA does NOT load the warrant
- The system reports significant events to the LEA
  - when the warrant was loaded, when it became active, when became inactive and when (if) it was deleted
- Reports delivered via FTP or FTAM

Handover Interface 2

- Intercept Related Information
- Information about the intercept
  - Who is calling whom and where from
  - Can contain lots of service information
- Often most important part of the intercept
  - LEAs usually more interested in who is talking to who rather than in what they are saying
  - 90% of warrants (in the US) are IRI only
- Can be cross-referenced to the warrant (HI1) and the Content of Communications (HI3)
- FTP or FTAM

Handover Interface 3

- Content of Communication
- Voice content, faxes, SMS, videoconferencing, modem dialup…
- Can be cross referenced to the warrant (Handover Interface 1) and any associated Intercept Related Information (Handover Interface 2)



IIF: internal interception function
INI: internal network interface

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

Other LI standards

- CALEA
  - Similar interfaces to ETSI
  - Poorly defined for mobile data (GPRS)
- SORM
  - Russian Federation
  - Much more centralised than ETSI or CALEA
  - Fewer checks and balances

Outline

- Introduction to Lawful Interception (LI)
- Telecommunications Companies and LI
- Internet Service Providers and LI
- LI Research

Problems of Access Network Interception

- LI has mainly been an Access Network function
  - LI obligations have mostly fallen on telecommunications companies
- ISP obligations have been modest
  - Usually limited to delivery of emails, http logs

BUT…

- IP Interception in access networks is easily subverted
  - Internet cafes, web mail, public libraries with Internet access, Universities, Large corporations
- Increased importance of interception by the ISP

IP Interception is difficult

- IP is a connectionless protocol
  - The route taken by traffic may change from packet to packet
- Intercepting IP traffic means examining every packet to see if it is of interest
  - Needs lots of computing power
- How do you tell if a packet is ‘of interest’?
  - IP addresses are (often) allocated dynamically
  - Warrants (in Australia and US) are expressed in terms of the identities of people to intercept
  - How do you link identity to an IP address?
- IP protocols are complex to examine
  - Tunnelling of IP packets within IP packets

There are no international LI standards for IP

- Something of a vacuum in IP interception
  - Many ad-hoc and potentially dangerous solutions
- Some work by ETSI on identifying issues of service level and access level interception
- Standards for delivery of IP packets as part of other technologies
  - Eg. ETSI specifies standards for delivery of IP packets as part of GPRS and UMTS
- Some national standards
  - Netherlands most advanced (TIIT)
  - Most other countries (including Australia) just specify TCPDUMP output as their national ‘standard’

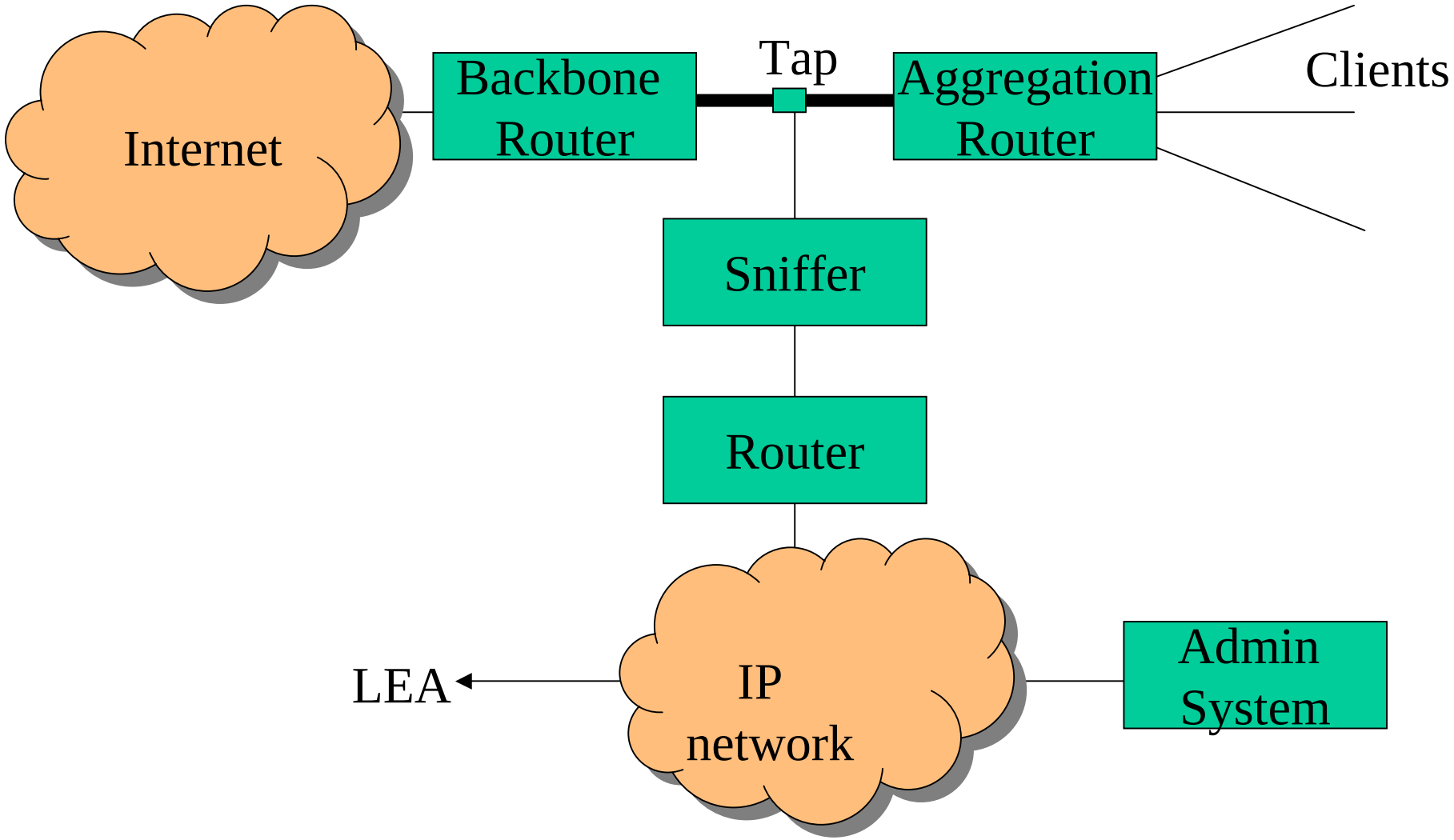
IETF's policy on wiretapping doesn't help

- RFC 2804 "IETF Policy on Wiretapping ",
- Decided IETF would not support LI
  - LI a national standards issue
  - Risk of compromising security of the multiple users of the Internet
  - Interception can be done effectively in the network without changes to existing protocols
  - Strong cryptography makes the likely future viability of LI questionable
  - Any approach to interception should be open
- All good points, but has left a vacuum in IP LI

IP Interception Techniques

- Sniffer based
  - Special purpose protocol sniffers are placed in the network at suitable points
  - They contain a list of target's login usernames (maintained by system administrator)
  - Monitor all RADIUS accounting messages
    - Contain temporary IP address assigned by Network Access Server
  - Listen for any traffic to or from temporary IP address
  - Transmit to LEA
- Require access to traffic stream
  - Splitter taps or broadcast hub

Sniffer based interception system



Weaknesses of sniffer systems

- Complex
  - Need to introduce much new hardware into the network.
- Expensive
  - Sniffer systems start from $Aus 100,000 and go on up
  - Sniffers need to be located at key points throughout the network. So a typical ISP may need to purchase a sniffer for each point of presence
- Difficult to manage
  - RADIUS server disconnects
  - Installing a warrant

CISCO's approach to LI

- A very recent development
- CISCO have released two internet drafts describing their approach to LI
- Integrates LI into the router
- Has an architecture similar to ETSI
- Controversial!
  - Routers are commodity items. Should private employers have routers with interception facilities?

Outline

- Introduction to Lawful Interception (LI)
- Telecommunications Companies and LI
- Internet Service Providers and LI
- LI Research

Lawful Interception Research Related to IP

- IP interception
  - Generic IP interception
  - Identity in IP interception
  - Providing IRI in IP
  - Auditing mechanisms ensuring only requested information
- LI for Mobile IP
  - Interception of IP tunnels
  - Reconstructing a message intercepted at multiple points
- Mobile ad-hoc networks
  - How to intercept when routers and hosts constantly shifting??!!
- Pervasive applications
  - Machine to machine communications
  - What to intercept? Can application interfaces be standardised for LI?
- Security and LI
  - How do we ensure that LI facilities are only used for authorised purposes?
  - How do we reduce the risk of a hack attack on LI functions?
- LI Policy
  - ‘Good’ ways of interception
  - Designing systems to minimize risk of abuse of LI

Research elsewhere in the world

- Standards
  - KPN (Netherlands) – TIIT (Transport of Intercepted IP Traffic)
  - ETSI – Identifying responsibilities for IP interception
  - CALEA – Limited packet network interception specifications
- Commentary / Policy
  - Bellovin, S.M., “Wiretapping the Net”, ATT Research, 2000
  - IETF, “IETF Policy on Wiretapping”, RFC 2804, 1999
  - FIPR, “Interception of Communications in the UK”, 1999
- Nothing on IP mobility, pervasive applications, IPv6, ad-hoc networks...

Should we be involved in LI?

- Poorly designed LI systems are dangerous
  - Can compromise network reliability, network security and user privacy
- Consequences of IETF RFC 2804
  - Created a vacuum in IP LI
  - Mostly sniffer based interception solutions
  - Difficult to audit and manage
  - Expensive
- If LI is going to be done it needs to be done properly
  - Audit mechanisms
  - Mechanisms for providing agencies with only the information authorised
  - Designed for reliability
  - Secure

Quote from Fred Baker (CISCO and one of the authors of RFC 2804)

"I have some moral and ethical issues (about Lawful Interception), but I think quite frankly that the place to argue this is in Congress and in the courtroom, not a service provider's machine room when he's staring down the barrel of a subpoena…"

Summary

- LI Background
  - LI is an obligatory capability for telcos and ISPs
- Telco Interception
  - Well defined standards for telco LI
  - ETSI and CALEA most important
  - Auditable separation of functions
- ISP Interception
  - ISPs are experiencing increasing LI obligations
  - No international standards for IP interception
  - Current IP interception solutions quite primitive
- LI Research
  - IP interception
  - Pervasive applications
  - Policy

References

- Telecommunications Interception Act
  - http://scaleplus.law.gov.au/html/pasteact/0/464/pdf/TeleInt79.pdf
- ETSI standard for interception
  - http://cryptome.sabotage.org/espy/2001040Meeting27G1.html
- RFC 2804
  - http://www.ietf.org/rfc/rfc2804.txt