Supporting Lawful Intercept in IP-based Networks

Matt Holdrege
Chair of the International Softswitch Consortium
Legal Intercept Working Group
Office of the CTO at Sonus Networks
Email: Matt@sonusnet.com.

IEEE Homeland Defense Series– March 2002
Agenda

- What is CALEA?
- Safe Harbor concept
- Internet Protocol
- Softswitch Architecture
- State of the art
- International Issues
- Remanded Punch List Items
- Summary of Concerns
- ISC and CALEA
CALEA

- Communications Assistance for Law Enforcement Act
- 1996 Act to update Law Enforcement tools for wiretapping
- Prompted by advances in Digital Telecommunications Services
Types of surveillance

- LEAs may be authorized to conduct any of three specific types of surveillance:
  - "pen register" which records call-identifying information for all calls originated by a subject
  - "trap and trace" which records call-identifying information for all calls received by a subject, and
  - "interception" which allows Law Enforcement to listen to the conversations of the subject, as well as access to call-identifying information.

- Approximately 90% of all surveillance orders are of the first two types; Federal law and laws of 42 states only allow the use of the third technique in the investigation of serious criminal offenses, and when other techniques have not worked, will not work, or are too dangerous.
Safe Harbor “Industry Standards”

• CALEA, § 107(a)
  → “shall be found to be in compliance”
  → “publicly available technical requirements or standards adopted by an industry association or standards-setting organization”

• CALEA, § 107(b)
  → “Government agency or any other person” may challenge a standard
  → FCC resolves the technical challenges
  → 107(b)(5): FCC establishes compliance schedule
“Reasonably Available”

• “call-identifying information is reasonably available to a carrier if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications” but

• what is “reasonably available” in a circuit-switched environment is not “reasonably available” in a Softswitch environment.
Concerns - “reasonably available”

• Providing Call Forwarding Information (easier in PSTN) - not always “reasonably available” in a Softswitch or SIP environment

• Dialed-Digit Extraction: “This service permits an LEA to receive, on the call data channel, digits dialed by a subject when a call is connected to another TSP’s service for processing and routing.” - not always “reasonably available” in a Softswitch or SIP environment.
Internet Protocol versus TDM

- TDM network is connection-oriented
- IP is connectionless
- TDM circuits follow fixed paths
- IP packets can traverse multiple independent paths to reach their endpoint
- TDM has guaranteed Quality of Service
- IP has no inherent QoS
Example Traditional Telecom Network Architecture

TDM Based Core Switching Module

Centralized Administrative and Control Processor on Fault Tolerant Platform

Proprietary Links Between Modules

Full Service Offering

Access and Remote Modules

Access and Features optimized for Voice Services

Source: www.lucent.com

IEEE Homeland Defense Series– March 2002
Distributed Switch Architecture

- IP Based Core Switching Network
- Centralized Administrative and Control Processor on Fault Tolerant Platform
- Standard Links Between Modules
- Seamless growth from legacy network infrastructure
- Full Service Offering
- Access and Remote Modules
- Access and Features for Voice, Data, and Video
- Seamless growth from legacy network infrastructure

Architecture Building Blocks:
- Softswitch
- OA&M
- Core IP Network
- IP App Server
- Trunking Gateway
- DSLAM or CMTS
- IP PBX
- MG
- Legacy

IEEE Homeland Defense Series– March 2002
Functional Architecture

Service Provider

Intercept Access Point (for Call Content)

Provisioning and Operation Support Systems

Intercept Access Point (for Call Data) SoftSwitch

Delivery Function

Law Enforcement Administration

Lawful Authorization

Collection

Law Enforcement Agency

Subscriber CPE

Interfaces in red - need to be standard for interoperability

Any Access Type, Any CCC format (IP, ATM)

Up to 5 LEA’s per Intercept (but the LEA’s can’t know about each-other)

Needs to be standard (save harbor spec)

Any Access Type, Any CCC format (IP, ATM)

Up to 5 LEA’s per Intercept (but the LEA’s can’t know about each-other)

Needs to be standard (save harbor spec)
Remanded Punch List Items

- Party-hold, party join, party drop
- In-band, and out of band signalling
- Dialed Digit Extraction
- Subject initiated dialing and signalling/feature info
What is happening in Europe and elsewhere?

- EU adopted IUR requirements in 1995 with support from the U.S. and other countries
- ETSI is studying LI for the purpose of standardization. It is a cooperative effort of government, operators and vendors.
- Certain individual countries have adopted strict rules for LI
Issues coming at us

- Identity? Host versus human
- Compensation
- Realistic capacity planning
- Roving wiretaps (mobility)
- More challenges
- More safe harbor specifications