             Cisco Architecture for Lawful Intercept in IP Networks

IESG Note

   This RFC is not a candidate for any level of Internet Standard. The
   IETF disclaims any knowledge of the fitness of this RFC for any
   purpose, and in particular notes that the decision to publish is not
   based on IETF review for such things as security, congestion control
   or inappropriate interaction with deployed protocols. The RFC Editor
   has chosen to publish this document at its discretion. Readers of
   this document should exercise caution in evaluating its value for
   implementation and deployment.

Abstract

   For the purposes of this document, lawful intercept is the lawfully
   authorized interception and monitoring of communications. Service
   providers are being asked to meet legal and regulatory requirements
   for the interception of voice as well as data communications in IP
   networks in a variety of countries worldwide. Although requirements
   vary from country to country, some requirements remain common even
   though details such as delivery formats may differ. This document
   describes Cisco's Architecture for supporting lawful intercept in IP
   networks. It provides a general solution that has a minimum set of
   common interfaces. This document does not attempt to address any of
   the specific legal requirements or obligations that may exist in a
   particular country.

Table of Contents

1. Introduction

   For the purposes of this document, lawful intercept is the lawfully
   authorized interception and monitoring of communications of an
   intercept subject. The term "intercept subject", "subject", "target
   subscriber" or "target" in this document refers to the subscriber of
   a telecommunications service whose communications and/or intercept
   related information (IRI) has been lawfully authorized to be
   intercepted and delivered to some agency. Note that although the
   term "Law Enforcement Agency" (LEA) is used throughout this document,
   this may refer to any agency that is able to request lawfully
   authorized interception.

   By intercept related information (IRI) we mean information related to
   the IP traffic of interest. There is currently no standardized
   definition for IRI for IP traffic. IRI has been defined for a few
   services that might run over IP (e.g., Voice over IP) or that IP runs
   on top of (e.g., GPRS). For example, IRI for voice over IP could be
   the called and calling phone numbers. The definition of IRI from
   [14] is shown below:

         Intercept Related Information: collection of
         information or data associated with
         telecommunication services involving the target
         identity, specifically communication associated
         information or data (e.g., unsuccessful
         communication attempts), service associated
         information or data and location
         information.

   Service providers are being asked to meet legal and regulatory
   requirements for the interception of voice as well as data
   communications in IP networks in a variety of countries worldwide.
   Although requirements vary from country to country, some requirements
   remain common even though details such as delivery formats may
   differ. This document describes Cisco's Architecture for supporting
   lawful intercept in IP networks. It provides a general solution that
   has a minimum set of common interfaces. This document does not deal
   with legal requirements or obligations.

   This document describes one method for supporting lawful intercept.
   Other methods may be available.

   The IESG wishes to draw the reader's attention to RFC 2804 [15] for a
   description of why architectures such as these are vendor-specific,
   rather than a topic of standardization for the IETF.

1.1. Requirements Motivating the Architecture

   The purpose of the following list of requirements is to provide an
   understanding of the motivation behind the architecture and some of
   the requirements imposed on components and interfaces that are
   described in the later sections of the document. This does not imply
   any legal requirements on service providers or equipment vendors
   although such requirements may coincide.

   Note that there are a variety of requirements that have been defined
   for lawfully authorized intercept throughout the world. Some of
   these have been defined by standards bodies (e.g., [13]), while
   others are country specific. The following itemized list is a
   distillation of some of these, although a given item may or may not
   apply to a specific country:

   * Lawful Intercept (LI) should be undetectable by the intercept
      subject.

   * Mechanisms should be in place to limit unauthorized personnel from
      performing or knowing about lawfully authorized intercepts.

   * There is often a requirement (especially for telecommunications
      services) to provide intercept related information (IRI)
      separately from the actual Internet Protocol (IP) traffic (or
      content) of interest (Note: some authorizations may be restricted
      to IRI).

   * If IRI is delivered separately from content, there should be some
      means to correlate the IRI and the content with each other.

   * If the information being intercepted is encrypted by the service
      provider and the service provider has access to the keys, then the
      information should be decrypted before delivery to the Law
      Enforcement Agency (LEA) or the encryption keys should be passed
      to the Law Enforcement Agency to allow them to decrypt the
      information.

   * If the information being intercepted is encrypted by the intercept
      subject and its associate and the service provider has access to
      the keys, then the service provider may deliver the keys to the
      LEA.

   * There is often a requirement for a service provider to be able to
      do multiple simultaneous intercepts on a single subject. The fact
      that there are multiple intercepts should be transparent to the
      LEAs.

   * There is often a requirement that the service provider should not
      deliver any unauthorized information to the LEA.

   The architecture and interfaces described in this document attempts
   to address these requirements.

1.2. Document Organization

   Section 1 of this document lists requirements motivating the
   architecture. Section 2 of this document describes a reference model
   along with some operation considerations. Section 3 provides more
   detailed requirements on the interfaces related to content
   interception. Section 4 applies the reference model to voice over IP
   and data intercepts and Section 5 examines security considerations.

2. Reference Model

   This section describes a generic reference model (Figure 1) for
   lawful intercept.

```
                       +--------------------+          +-----+
                       | LI Administration  |  HI1(a)  |     |
                       |      Function      |<-------------|  |
                       +--------------------+          |     |
                                |                       |     |
                                | MD Provisioning       |     |
                                | Interface(b)          | LEA |
                                v                       |     |
   +-----------+       +--------------------+           |     |
   |           |<---(c)----|                |           |     |
   |  IRI IAP  |--IRI(e)-->|   Mediation    |----HI2(g)--->|  |
   |           |       |   Device (MD)      |           |     |
   +-----------+       |                    |----HI3(h)--->|  |
                       +--------------------+          +-----+
                         |            ^
              Intercept  |            |  Intercepted
              Request(d) |            |  Content(f)
                         |            |
                         v            |
                    +--------------------+
            User    |      Content       |  User
            ------->|       IAP          |-------->
            Content +--------------------+  Content
```
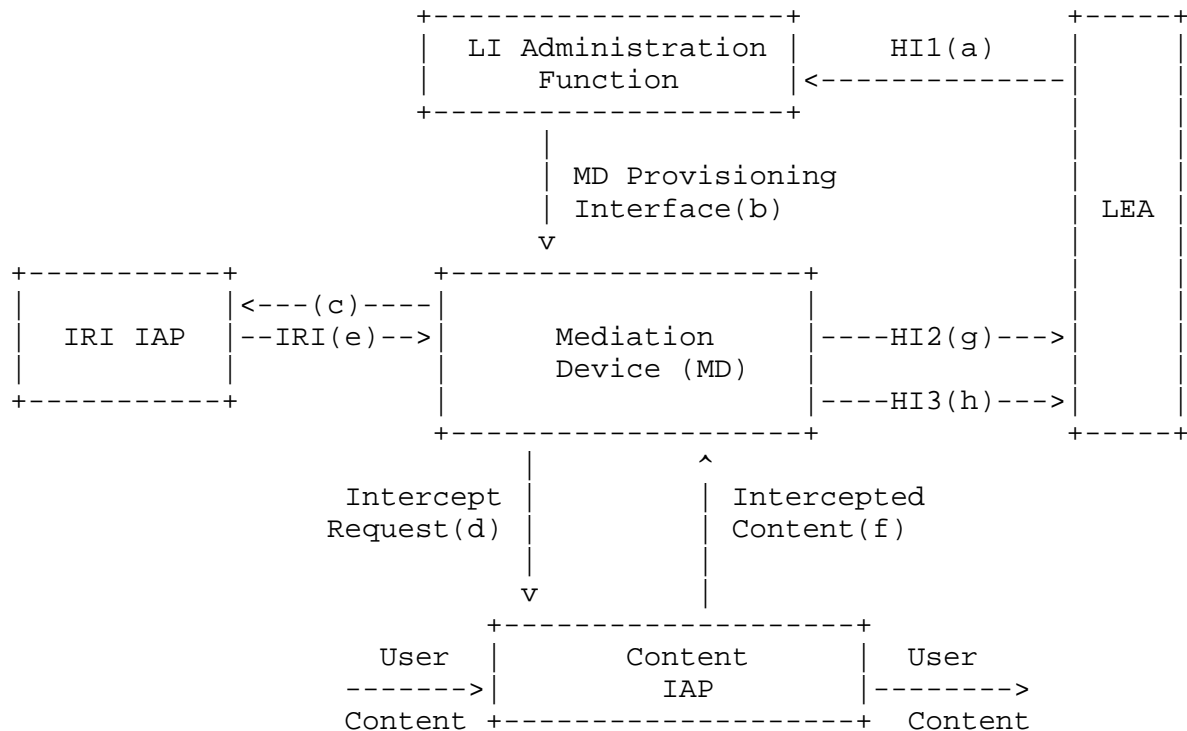
       Figure 1: Intercept Architecture

   A brief description of the interfaces is included in table 1 below.
   For a more detailed description of the interfaces refer to section 3.
   For a description of the components refer to section 2.1.

   Table 1 LI Interfaces

      Interface   Description
   ---------------------   --
   (a) HI1   Handover Interface 1 - Administration
                            Interface: The LEA provides intercept
                            information to the service provider
                            administration function.

   (b) MD Provisioning   Mediation Device provisioning interface.
                            Parameters include: target identifier,
                            duration of intercept, type of intercept,
                            etc.

       (c) IRI IAP Provisioning Specifies Target identifier, duration,
                                 etc. for provisioning of delivery of
                                 Intercept Related Information (IRI).

       (d) Content Intercept   Provisioning of the Content IAP.
           Provisioning

       (e) IRI to MD   Internal interface between IRI Intercept
                                 Access Point (IAP) and Mediation device
                                 (MD) for delivery of IRI.

       (f) Content to MD   Internal interface between content
                                 IAP and MD for delivery of Content.

       (g) HI2   Handover Interface 2: Interface between
                                 the MD and LEA for delivering IRI. This
                                 interface may vary from country to
                                 country.

       (h) HI3   Handover Interface 3: Interface between
                                 the MD and LEA for delivering Content.
                                 This interface may vary from country to
                                 country.

2.1. Reference Model Components

   A brief description of the key components in the reference model is
   as follows:

   Lawful Intercept (LI) Administration Function:
      This function provides the (typically manual) provisioning
      interface for the intercept as a result of a court order or
      warrant delivered by the Law Enforcement Agency (LEA). It could
      involve separate provisioning interfaces for several components,
      but more typically is a single interface to the Mediation Device
      (MD), which then takes care of provisioning of other components in
      the network. Because of the requirement in some laws to limit
      accessibility to authorized personnel, the provisioning interface
      has to be strictly controlled. In many cases, the identity of the
      subject received from the LEA has to be translated into an
      identity that can be used by the network to enable the intercept.

   Intercept Access Point (IAP):
      An IAP is a device within the network that is used for
      intercepting lawfully authorized intercept information. It may be
      an existing device that has intercept capability or it could be a

special device that is provided for that purpose. Two types of
IAP's are discussed here: IAP's that provide content; and IAP's
that provide intercept related information (IRI).

Content IAP:
   A content IAP is an IAP that is used to intercept the IP traffic
   of interest.

IRI IAP: This is an IAP that is used to provide intercept related
   information (IRI).

Law Enforcement Agency (LEA):
   This is the agency that has requested the intercept and to which
   the service provider delivers the information.

Mediation Device (MD):
   The MD requests intercepts from IAPs through interfaces (c) and
   (d) in Figure 1. The Mediation Device receives the data from the
   IAP, packages it in the correct format (which may vary from
   country to country) and delivers it to the LEA. In the case where
   multiple law enforcement agencies are intercepting the same
   subject, the mediation device may replicate the information
   multiple times. The assumption is that the service provider
   operates the MD (via specially authorized personnel) and that the
   LEA only has access to interfaces (a), (g) and (h) in Figure 1.

2.2. Operational Considerations

   In a typical operation, a lawfully authorized surveillance request
   arrives for a specified intercept subject. Authorized personnel
   provision the intercept using interface (b) in Figure 1, which may be
   for content only, IRI only or both. Once the intercept is
   provisioned, the IAP's send the IRI and/or content to the MD, which
   formats the information into the appropriate format for delivery to
   the LEA. Some operational issues that need to be considered:

   * Location and Address Information for Content Intercepts: In some
      cases where the location and/or addressing information for the
      intercept is not known until the subject registers (or makes a
      call in the case of voice), the IRI may provide needed information
      in order to do the content tap (e.g., the IP address and port for
      the content streams).

   * Content Encryption: If the intercept content is encrypted and the
      service provider has access to the encryption keys (e.g., receives
      keys in Session Description Protocol for Voice over IP), then the
      keys can be sent via IRI. It is, however, possible for end-users
      to exchange keys by some other means without any knowledge of the

service provider in which case the service provider will not be
able to provide the keys. Content transformations could make
decryption at the LEA impossible. This is why the original
packets are provided on interface (f) rather than attempting to
convert them to some other format.

* Detection by the Intercept Subject: One requirement is to ensure
  that the intercept subject is unable to detect that they are being
  intercepted. This document assumes a sophisticated subject:

  - Able to check IP addresses, use traceroute, etc.

  - Able to check if any unusual signaling is occurring on their
    customer premises equipment (CPE).

  - Able to detect degradation or interruptions in service.

  This is why the intercept mechanism described here does not
  involve special requests to the CPE, re-routing of packets or
  end-to-end changes in IP addresses. Instead, content intercept is
  done on a device along the normal content path (i.e., no re-
  routing has occurred) that is within the service provider's
  network. A convenient content IAP is a router or switch at the
  edge of the service provider's network to which the intercept
  subject connects. This is illustrated in Figure 2.

```
                        |
      Customer Premises  |  Service Provider's Network
                        |
                                +-------+
        +-----+                 |       |
        | CPE |-------------|  Router|----------
        +-----+                 | (IAP) |
                                |       |
                                +-------+
```
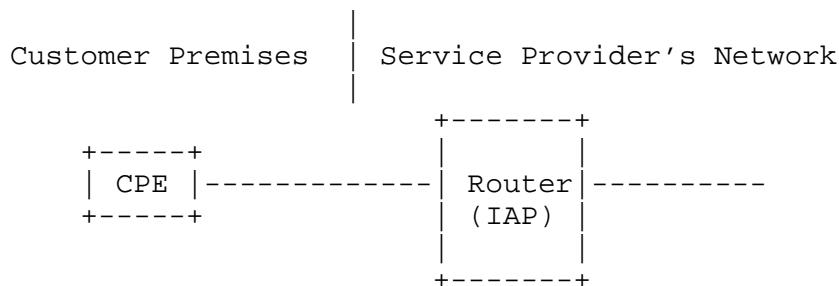
                Figure 2 Content IAP - Router

Another possibility of course is to provide a special device along
the path to provide the content IAP capabilities.

Note that in the case where there is multi-homing (two or more
routers connected to provide access for the CPE), intercept taps
may have to be installed on more than one access router. If the
CPE is multi-homed to multiple service providers, then the
intercept will have to be installed on each service provider
separately and the LEA will have to correlate the data.

   * Unauthorized Creation and Detection: Another concern is the
      prevention of unauthorized creation and detection of intercepts.
      This is particularly important when a network element such as a
      router is used as a content IAP. Those routers that have the
      capability should be carefully controlled with access to intercept
      capability and information only via authorized personnel. In one
      approach using the reference model in Figure 1, the MD is in a
      controlled environment and the MD does the intercept request to
      the content IAP over an encrypted link. Logging and auditing are
      used to detect unauthorized attempts to access the intercept
      capability.

   * Capacity: Support for lawful intercept on a network element
      supporting customers consumes resources on that equipment.
      Therefore, support for lawful intercept requires capacity planning
      and engineering to ensure that revenue-producing services are not
      adversely affected.

3. Interfaces

   This section provides a brief description of the interfaces in the
   reference model (Figure 1). A list of these interfaces is included
   in Table 1 in Section 2.

   One of the objectives in defining these interfaces is to keep the
   internal interfaces (b to f) the same regardless of country-specific
   requirements. The MD then formats the IRI and the content to meet
   the country specific requirements for interfaces (g) and (h).

3.1. Content Intercept Request Interface

   This section describes some of the requirements for the content
   intercept request interface (d) in Figure 1. It makes use of a
   common request protocol (SNMPv3) regardless of the type of
   application (e.g., voice, data) and suggests the usage of a TAP-MIB,
   which is defined in a separate document [1]. Some of the
   considerations that lead to the use of SNMPv3 and to the definition
   of the specific Management Information Base (MIB) defined in [1] are
   provided here.

   In order to provide a generic interface for intercepting,
   replicating, encapsulating and transporting content packets to the
   MD, the content intercept interface ((d) in Figure 1) should specify:

   * A Filter specification for classifying the packets to be
      intercepted.

   * The destination address of the MD (where to send the packets).

   * Encapsulation and Transport parameters.

   In addition, a timeout value for the intercept should also be
   specified. This defines a limited lifetime for the intercept so that
   failures will not result in intercepts remaining beyond their
   authorized lifetime. If a failure of the MD occurs such that it is
   not able to supply the refresh to the timeout, then the intercept
   will cease to exist after the timeout expires. Similarly, if the IAP
   re-boots, then the intercept will not survive the re-boot unless the
   IAP is capable of ascertaining that the intercept lifetime
   requirements will continue to be met.

   In order for this to work, it must be possible for the mediation
   device to realize that there is a failure in the IAP such that it
   must re-establish the intercept. This may be in the form of an audit
   (from the MD to the IAP), or in the form of a heartbeat mechanism in
   the content stream, or both.

3.2. Intercept Content Interface (f)

   The encapsulation method should retain all of the information in the
   original packets (source and destination addresses as well as
   payload) and provide an identifier for correlating the packets with
   the IRI. One encapsulation that meets those requirements is
   described in Section 4 of [2]. For non-voice intercepts, the
   "Intercepted Information" field in Table 1 of [2] contains the
   original intercepted IP packet.

   Note, however, that the interface defined in [2] is based on UDP
   which is an unreliable and unordered transport protocol (i.e.,
   provides neither retransmission on detection of errors nor ordering
   of data). If this transport is used, the underlying network (Layers
   1 -   - 3) should be engineered to meet the overall reliability
   requirements for delivery of content.

   If a more reliable transport protocol is required, then a mechanism
   that provides timely delivery as well as limits the burden (both
   processing and buffering) on the Content IAP should be used. One
   mechanism that meets these requirements is a NACK-oriented
   retransmission scheme based on [12].

   If [12] is used, the call content channel identifier may be placed in
   the SSRC field of the encapsulating RTP packet. The payload type may
   be used to identify the type of packet encapsulated in RTP (e.g., IP,
   PPP, Ethernet MAC). Note that usage of [12] is still under
   investigation and may need further specification. Usage of [12] in
   the content IAP places more processing burden on the content IAP than
   a UDP-based intercept and can affect the capacity of the content IAP.

4. Applying the Reference Model

    This section applies the reference model to some example
    applications.

4.1. Voice over IP networks

    This section will look at some of the issues surrounding interception
    of voice over IP calls, taking local voice services as a specific
    service example. The reference model from Figure 1 will be applied
    with the use of a common set of interfaces that are independent of
    the call signaling protocols in use.

4.1.1. Interception of Voice over IP Services

    There are a variety of architectures in use for voice over IP (e.g.,
    centralized versus distributed) as well as various protocols (SIP
    [6], H.323 [9], MGCP [7], H.248 [8]). There are also a variety of
    services that may be offered:

    * Local Voice Services (i.e., service to a user that has an IP phone
       or a phone connected to a gateway)

    * Transit services

    * Long distance access services (e.g., calling/debit card).

    This document does not address any obligations that a service
    provider might or might not have to support intercepts. It simply
    describes how intercept might be done using the reference model in
    Figure 1.

    Note that in the case of services where the intercept subject
    accesses the network via a non-IP endpoint (e.g., TDM), the
    detectability issue is less acute (e.g., re-routing of packets to
    intercept them in a special device is a possible option), since the
    intercept subject does not have access to the IP addresses or to
    traceroute.

    However, in the case of local services, this is a much more difficult
    problem. The intercept for a call originating and terminating on-net
    (i.e., a call that is voice over IP end-to-end) has to be intercepted
    along its normal route in order to be undetectable. In addition, the
    call-forwarding feature that is often provided as a local service
    feature makes interception even more difficult: If call forwarding is
    invoked, a call that was intended to terminate on the intercept
    subject may be forwarded anywhere in the network resulting in the
    media stream bypassing the original content IAP (since in voice over

IP, the media stream goes directly from end-to-end). Also, since
call forwarding can often be set up on a call-by-call basis, the
location of the content IAP will often not be known until the call is
set up.

4.1.2. Local Voice Services

This sub-section will look at the specific case in which the
intercept subject under surveillance is being provided with a local
voice service by the same provider that also provides the network
access (e.g., controls the edge router or switch). This is an
important assumption, since in VoIP the entity providing call control
(e.g., SIP server) can be totally separate from the entity providing
network access (e.g., operates edge routers).

Suppose that a subscriber that subscribes to a local (e.g.,
residential) voice service is a target for a lawfully authorized
surveillance. Part of the system providing these services is a
subscriber database that includes addressing information about the
subscriber as well information on what features are in effect (e.g.,
call forwarding). Some call control entity (CCE) accesses that
database in order to provide local services. For example, if the
subject has call forwarding invoked, that fact (and where to forward
the call) is indicated in the subscriber database. A call arriving
at the CCE that "owns" that subscriber can then take the appropriate
action (e.g., forward the call).

The CCE that "owns" the target subscriber (which could be an H.323
gatekeeper, a SIP proxy or a Media Gateway Controller) is provisioned
with the intercept parameters (e.g., subject identification
information such as the telephone number and where to deliver the
IRI). The provisioning of this CCE could be through interface (c) in
Figure 1. The CCE in question is the IRI IAP and once provisioned,
it passes the IRI to the MD. In the scenario being discussed, the
CCE typically remains in the signaling path throughout the call, even
in the call-forwarding case. Part of the IRI it passes to the MD is
the media signaling information (i.e., SDP [11] or H.245 [10]), which
includes endpoint IP address and port information for the media
(content) streams. Armed with this media address information, the MD
can determine the content IAP (e.g., [5]) and make the request via
interface (d). The request identifies the voice stream to be
intercepted based on information received in the call signaling
(i.e., IP addresses and UDP port numbers).

Note that the content IAP in the case of voice over IP could be an
edge router or a PSTN gateway (e.g., a call from the PSTN forwarded
to the PSTN). SIP, H.323, MGCP or H.248 call signaling protocols
could be used. However, the protocol (SNMPv3 [1]) used for interface

(d), is not dependent on the type of call signaling protocol used;
nor is the encapsulation format and transport protocol (interface
"f"). The same reference model (Figure 1) with the same interfaces
can be used for lawfully authorized surveillance, regardless of the
signaling protocol and regardless of the type of service being
provided (Note: even though a local voice service was used in this
example, other voice services could use the same model and
interfaces).

4.2. Data Services

The same model (Figure 1) can also be used for data services. In
this case the IRI IAP could be a server that acts as registration,
authentication and authorization point for the data service (e.g., a
RADIUS server). If a potential IRI IAP does not have the available
interfaces (c) and (e), the MD may have to do a content tap on
registration signaling in order to obtain the IRI.

The IRI in the case of a data service could include:

* The time that the user registered or de-registered for the
   service.
* Addressing information (i.e., given the user identity, what IP
   address or other information is available that could be used in
   interface (d) to do the content tap).

Once suitable addressing information is available in order to do
content tapping the MD can invoke the tap via interface (d).

Clearly the IRI interfaces (c, e, g) are different for data than they
are for voice services. However, the content IAP is typically the
same (an edge router). Interfaces (d, f, and h) may also be the
same.

5. Security Considerations

Given the sensitive nature of lawful intercept (LI) -- both from the
standpoint of the need to protect sensitive data, as well as conceal
the identities of the intercept subjects, the LI solution should have
the ability to provide stringent security measures to combat threats
such as impersonation of MD's, privacy and confidentiality breaches,
as well as message forgery and replay attacks.

While this document doesn't discuss issues of physical security,
operating system, or application hardening within the principals of
the LI solution, they are clearly important. In particular, the MD
server would be considered a prime target for attacks.

In general, all interfaces should have the capability of providing
strong cryptographic authentication to establish the identity of the
principals, and be able to correlate the identity of the principal
with the action they are attempting to perform. All interfaces
should be capable of performing some sort of cryptographic message
integrity checking such as, for example, HMAC-MD5. Message integrity
checking can also be used to counter replay attacks. Privacy and
confidentiality considerations, may also require the use of
encryption.

The content and IRI IAPs also should also provide protection of the
identity of the intercept subject and the existence of an intercept.

5.1. Content Request Interface (d) - SNMPv3 Control

For interface (d,) native SNMPv3 security module mechanism is used.
The additional requirement is that the IAP should support the ability
to protect the TAP MIB's [1] from disclosure or control by
unauthorized USM [3] users. VACM [4] provides the necessary tools to
limit the views to particular USM users, but there are also special
considerations:

*   The ability to limit access to the appropriate TAP MIB's by only
    those SNMPv3 USM users which have keys established and the proper
    VACM views defined.

*   Segregation of the TAP MIB such that only operators of sufficient
    privilege level can create VACM views that include the TAP MIB
    [1].

6. Informative References

[1]   Baker, F., "Cisco Lawful Intercept Control MIB", Work in
      Progress, April 2004.

[2]   PacketCable(TM) Electronic Surveillance Specification, PKT-SP-
      ESP-I04-040723, http://www.packetcable.com/specifications/

[3]   Blumenthal, U. and B. Wijnen, "User-based Security Model (USM)
      for version 3 of the Simple Network Management Protocol
      (SNMPv3)", STD 62, RFC 3414, December 2002.

[4]   Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access
      Control Model (VACM) for the Simple Network Management Protocol
      (SNMP)", STD 62, RFC 3415, December 2002.

   [5]   Warnicke, E., "A Suggested Scheme for DNS Resolution of Networks
         and Gateways", Work in Progress.

   [6]   Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A.,
         Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP:
         Session Initiation Protocol", RFC 3261, June 2002.

   [7]   Andreasen, F. and B. Foster, "Media Gateway Control Protocol
         (MGCP) Version 1.0", RFC 3435, January 2003.

   [8]   ITU-T Recommendation H.248.1, Gateway Control Protocol: Version
         2, May 2002.

   [9]   ITU-T Recommendation H.323, Packet-based Multimedia
         Communications Systems, July 2003.

   [10] ITU-T Recommendation H.245, Control Protocol for Multimedia
         Communications, July 2003.

   [11] Handley, M. and V. Jacobson, "SDP: Session Description
         Protocol", RFC 2327, April 1998.

   [12] Rey, J., Leon, D., Miyazaki, A., Varsa, V., and R. Hakenber,
         "RTP Retransmission Payload Format", Work in Progress.

   [13] ETSI TS 101 331, Telecommunications security; Lawful
         Interception (LI); Requirements of law enforcement agencies.

   [14] ETSI TS 33.108 v6.7.0, 3rd Generation Partnership Project;
         Technical Specification Group Services and System Aspects; 3G
         Security; Handover Interface for Lawful Interception (Release
         6).

   [15] IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, May 2000.

7. Acronyms

    CCE   Call Control Entity
    CMTS   Cable Modem Termination System
    CPE   Customer Premises Equipment
    ETSI   European Telecommunications Standards Institute
    GPRS   Generalized Packet Radio Service
    HMAC-MD5   Hash-based Message Authentication Code -
                    Message Digest 5
    IAP   Intercept Access Point
    IETF   Internet Engineering Task Force
    IRI   Intercept Related Information
    ITU-T   International Telecommunications Union -
                    Telecommunications Sector
    LEA   Law Enforcement Agency
    LI   Lawful Intercept
    MGCP   Media Gateway Control Protocol
    MD   Mediation Device
    MIB   Management Information Base
    NACK   Negative Acknowledgement
    PSTN   Public Switched Telecommunications Network
    RFC   Request for Comment
    RTP   Real-time Transport Protocol
    SDP   Session Description Protocol
    SIP   Session Initiation Protocol
    SSRC   Synchronization Source
    TDM   Time Division Multiplex
    UDP   User Datagram Protocol
    USM   User Service Model
    VACM   View-based Access Control Model
    VoIP   Voice over IP

8. Authors' Addresses

   Fred Baker
   Cisco Systems
   1121 Via Del Rey
   Santa Barbara, CA 93117
   US

   Phone: +1-408-526-4257
   Fax: +1-413-473-2403
   EMail: fred@cisco.com

   Bill Foster
   Cisco Systems
   Suite 2150
   1050 West Pender St.
   Vancouver, BC, V6E 3S7
   Canada

   Phone: +1-604-647-2315
   EMail: bfoster@cisco.com

   Chip Sharp
   Cisco Systems
   7025 Kit Creek Road
   RTP, NC 27709 USA

   Tel:+1.919.392.3121
   EMail: chsharp@cisco.com

9. Full Copyright Statement

Acknowledgement