White Paper

Cisco Lawful Intercept Security Best Practices

Cisco Systems, Inc.

Contents

Target Audience

This document provides enterprise network managers with Lawful Intercept feature monitoring and management best practices for Cisco products. It is meant to be a supplement to existing Lawful Intercept and product security configuration guides (see *Configuration Guides for Specific Product Families*).

Introduction

Lawful Intercept is the process by which law enforcement agencies (LEAs) conduct electronic surveillance as authorized by judicial or administrative order. Increasingly, legislation is being adopted and regulations are being enforced that require service providers and Internet service providers (ISPs) to design their networks to explicitly support authorized electronic surveillance. The types of service providers or ISPs that are subject to Lawful Intercept mandates vary greatly from country to country. For example, the Communications Assistance for Law Enforcement Act (CALEA) specifies Lawful Intercept compliance in the United States.

This document explains the Cisco® Lawful Intercept architecture, including the Cisco Service Independent Intercept Architecture and PacketCable™ Lawful Intercept Architecture. It also supplements existing product configuration guides with guidance for detecting and managing Lawful Intercept in your network.

Cisco supports two architectures for Lawful Intercept: PacketCable and Service Independent Intercept. The Lawful Intercept components by themselves do not ensure customer compliance with applicable regulations but, rather, provide tools that service providers and ISPs use to construct a Lawful Intercept–compliant network.

Cisco Service Independent Intercept Architecture

The **Cisco Service Independent Intercept Architecture Version 3.0** document describes implementation of Lawful Intercept for voice-over-IP (VoIP) networks using the Cisco BTS 10200 Softswitch call agent, Version 5.0, in a network that is not a PacketCable network. PacketCable Event Message specification Version 1.5-I01 is used to deliver the call identifying information along with Version 2.0 of the Cisco Tap MIB for call content. To view this document, please visit: http://www.cisco.com/en/US/technologies/tk583/tk799/technologies_design_guide09186a0080826773.pdf.

The **Cisco Service Independent Intercept Architecture Version 2.0** document describes implementation of Lawful Intercept for VoIP networks using the Cisco BTS 10200 Softswitch call agent, Versions 4.4 and 4.5, in a network that is not a PacketCable network. Although not a PacketCable network, PacketCable Event Messages Specification Version I08 is still used to deliver call identifying information, along with Version 1.0 or 2.0 of the Cisco Tap MIB for call content. The **Cisco Service Independent Intercept Architecture Version 2.0** document adds additional functions for conducting data intercepts by both IP address and session ID, which are both supported in Version 2.0 of the Cisco Tap MIB (CISCO-TAP2-MIB). To view this document, please visit: http://www.cisco.com/en/US/technologies/tk583/tk799/technologies_design_guide09186a008082682c.pdf.

The **Cisco Service Independent Intercept Architecture Version 1.0** document describes implementation of Lawful Intercept for VoIP networks that are using the Cisco BTS 10200 Softswitch call agent, Versions 3.5 and 4.1, in a network that is not a PacketCable network. Although not a PacketCable network, PacketCable Event Message Specification Version I03 is still used to deliver call identifying information, along with Version 1.0 of the Cisco Tap MIB (CISCO-TAP-MIB) for call content. Simple data intercepts by IP address are also discussed. To view this document, please visit: http://www.cisco.com/application/pdf/en/us/partner/tech/tk799/c1501/ccmigration_09186a0080826874.pdf.

PacketCable Lawful Intercept Architecture

The **PacketCable Lawful Intercept Architecture for BTS Version 5.0** document describes the implementation of Lawful Intercept for VoIP using Cisco BTS 10200 Softswitch call agent, Version 5.0, in a PacketCable network that conforms to PacketCable Event Messages Specification Version 1.5-I01. To view this document, please visit: http://www.cisco.com/application/pdf/en/us/partner/tech/tk799/c1501/ccmigration_09186a0080826582.pdf.

The **PacketCable Lawful Intercept Architecture for BTS Versions 4.4 and 4.5** document describes the implementation of Lawful Intercept for VoIP using Cisco BTS 10200 Softswitch call agent, Versions 4.4 and 4.5, in a PacketCable network that conforms to PacketCable Event Messages Specification Version I08. To view this document, please visit: http://www.cisco.com/application/pdf/en/us/partner/tech/tk799/c1501/ccmigration_09186a0080827768.pdf.

The **PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1** document describes the implementation of Lawful Intercept for VoIP using Cisco BTS 10200 Softswitch call agent, Versions 3.5 and 4.1, in a PacketCable network that conforms to PacketCable Event Message Specification Version I03. To view this document, please visit: http://www.cisco.com/application/pdf/en/us/partner/tech/tk799/c1501/ccmigration_09186a0080827794.pdf.

How to Determine if a Product Supports Lawful Intercept

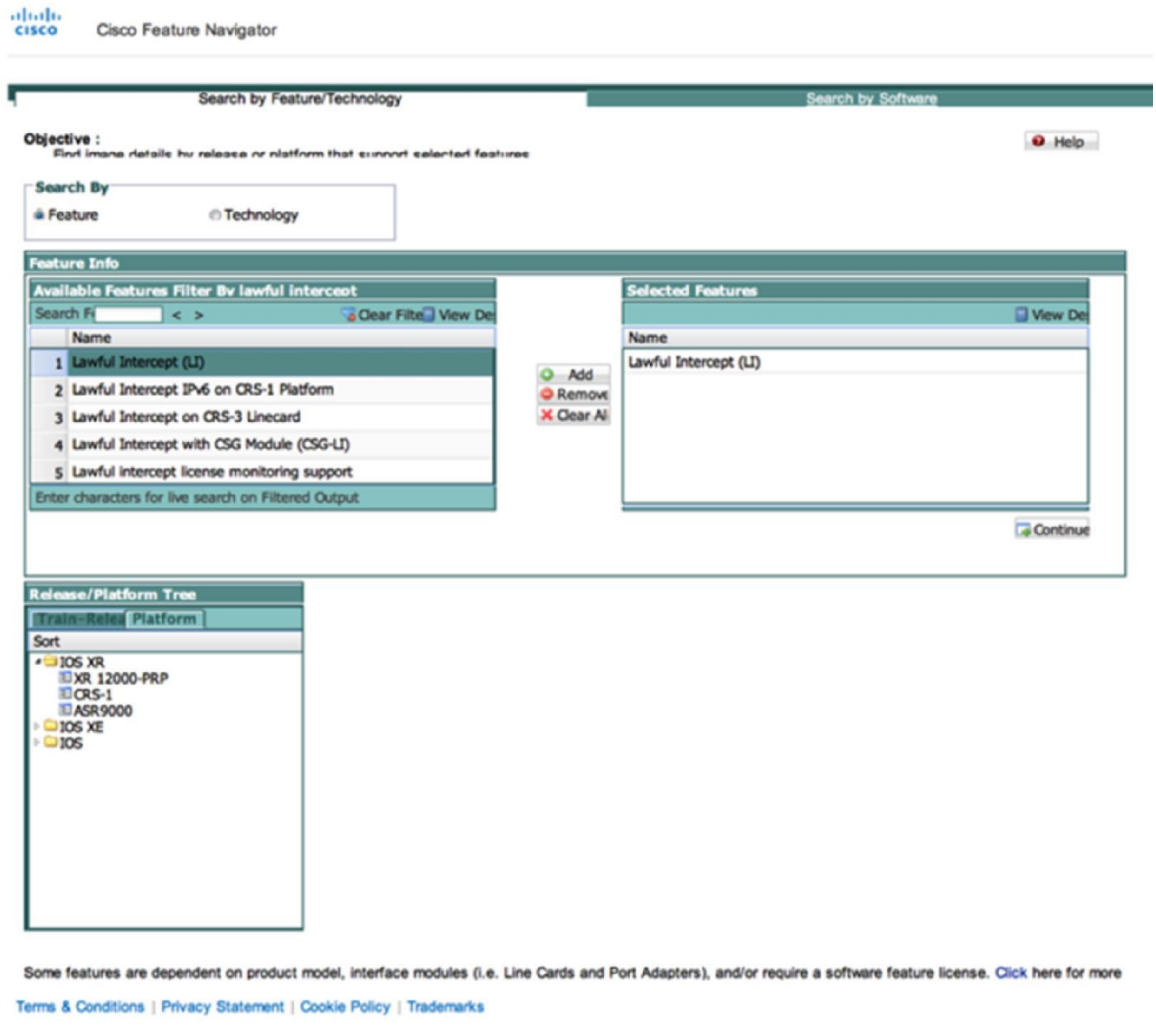
By using the Feature Navigator on Cisco.com, you can view the platforms and versions of software that support Lawful Intercept. Do the following to use the Feature Navigator:

1. Click the following link to access the Feature Navigator (see Figure http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp.

Figure 1. Cisco Feature Navigator Homepage

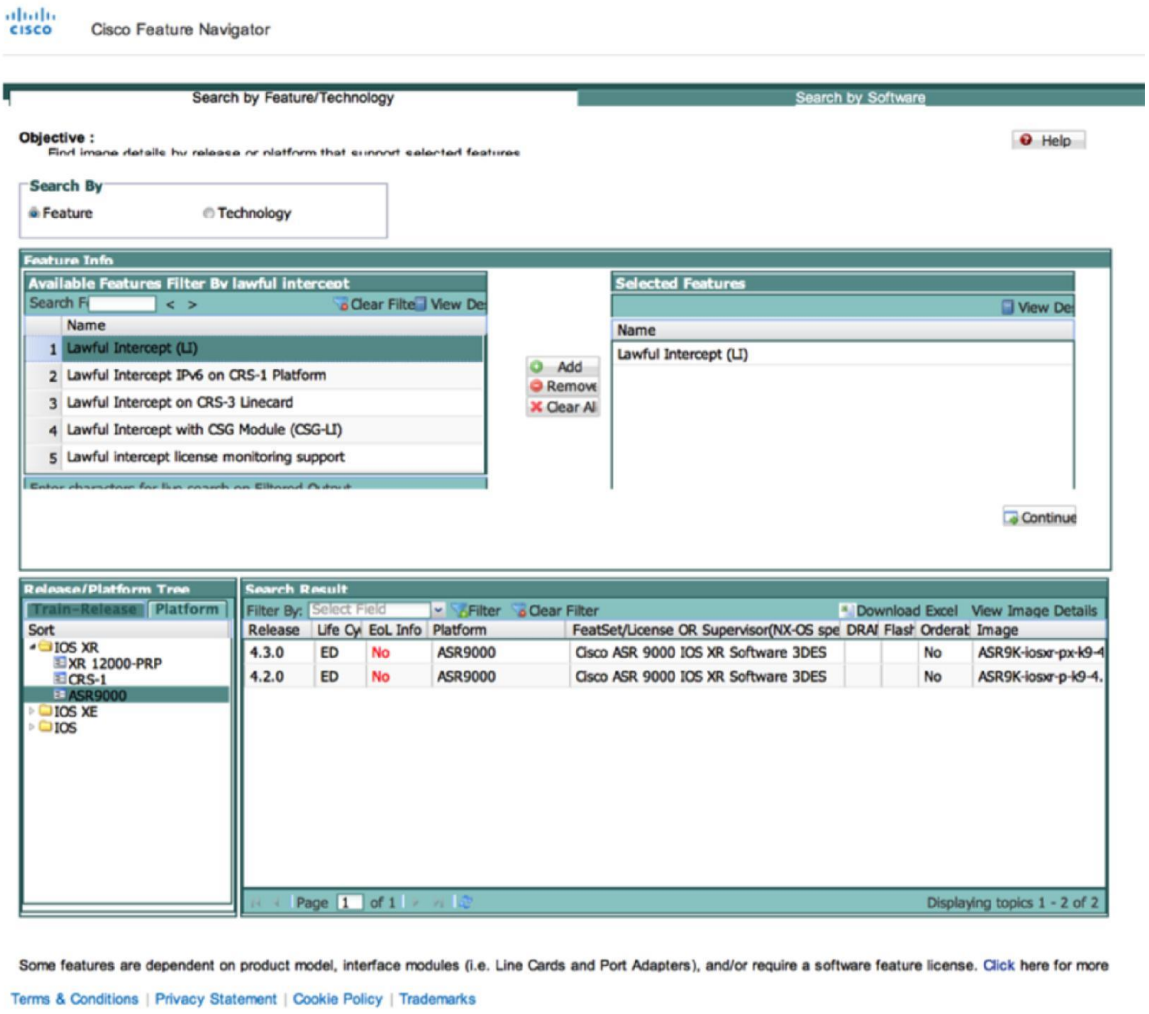
2. Choose **Research Features**.
3. Choose **Search by Feature**.
4. Enter **Lawful Intercept** in the filter box. Select **Lawful Intercept** and Click **Add** (see Figure 2).

Figure 2. Selecting the Correct Research Features



5. Lawful Intercept will appear on the selected feature.
6. Click **Continue** under the selected feature box.
7. Choose **Platform** on the Release/Platform tree (see Figure 2) and then select the platform.
8. Select the platform under the release tree you are checking to display the versions of supported code (see Figure 3).

Figure 3. Selecting the Correct Platform



When you have completed steps 1 through 8, compare the results with the versions of code you are running on your network to determine if your device supports the Lawful Intercept feature.

How to Determine if Lawful Intercept Is Enabled

Creating a tap with Lawful Intercept requires creating a Simple Network Management Protocol (SNMP) view that includes the CiscoTap2Mib, and either CiscoIpTapMIB, Cisco802TapMIB, or CiscoUserConnectionTapMIB.

RADIUS-based Lawful Intercept requires the command **aaa intercept** to be configured.

Doing a search of the router configuration for either **Tap** or **intercept** using the following commands should display the relevant lines in the configuration. The following commands work on all Cisco IOS, IOS XE, and IOS XR Software platforms:

```
show running-config | include Tap
show running-config | include intercept
Configuration
.
.
snmp-server view tapV ciscoTap2MIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV cisco802TapMIB included
snmp-server view tapV ciscoUserConnectionTapMIB included
.
aaa intercept
.
```

Cisco ASR 1000 Example

The following is an example for the Cisco ASR 1000 Aggregation Service Router that indicates Lawful Intercept is enabled:

```
asr1000-2#show run | include intercept|Tap
aaa intercept
snmp-server view liView ciscoTap2MIB included
snmp-server view liView ciscoIpTapMIB
included asr1000-2#
```

Cisco ASR 9000 Example

The following is an example for the Cisco ASR 9000 that indicates Lawful Intercept is enabled. Note that no license is required for the Cisco ASR 9000 to enable Lawful Intercept (see the **show license** command):

```
RP/0/RSP0/CPU0:ASR9K#show run | include intercept
Wed Feb 19 02:00:22.887 UTC
Building configuration...
aaa intercept


RP/0/RSP0/CPU0:ASR9K#show run | utility egrep
'intercept|tap' Wed Feb 19 02:33:51.320 UTC
Building configuration...
aaa intercept
snmp-server view tapV ciscoTap2MIB included
```

```
RP/0/RSP0/CPU0:ASR9K#show license
Wed Feb 19 02:52:54.930 UTC
Info: There are no features or licenses to display.
```

Detecting with Show License

On some platforms, it is possible to look at license information for Lawful Intercept by entering the following command lines:

```
3900-6#show license | begin
LI Index 6 Feature: LI
     Period left: Life time
     License Type: Permanent
     License State: Active, In Use
     License Count: Non-Counted
     License Priority: Medium
```

This command is not supported on all platforms, and some platforms or versions of code do not need any special license to enable Lawful Intercept.

Runtime Detection if Lawful Intercept Is Enabled for Cisco IOS and IOS XE Software

Due to the sensitive nature of Lawful Intercept, the feature only logs configuration change events such as creating or deleting the SNMP views but does not log information about taps. The Cisco Embedded Event Manager (EEM) can be used to detect and block Lawful Intercept configurations and send logs of configuration changes through email and/or a syslog server.

The following command has been verified on the Cisco Integrated Services Routers Generation 2 (ISR G2) and the Cisco ASR 1000 routers. It will not, however, work on the Cisco ASR 9000. Using the following EEM configuration will prevent the configuration of Lawful Intercept on this device. In other words, if you try to configure Lawful Intercept through either SNMP or RADIUS, the system will ignore the command. At the same time, EEM will send a **syslog** and an **email** to the specified recipient.

The SNMP configuration follows:

```
event manager applet li-snmp-mon
 event cli pattern "^snmp-server.*cisco.*Tap.*MIB" sync no skip yes
 action 1.0 syslog msg "LI-SNMP-Cfg" facility "<router name>"
 action 2.0 mail server "<mail server>" to "<email address>" from
"<email address>" subject "LI-SNMP" body "configuration attempted"
```

The RADIUS configuration follows:

```
event manager applet li-radius-mon
 event cli pattern "aaa.* intercept" sync no skip yes
 action 1.0 syslog msg "LI-Radius-Cfg" facility "<router name>"
 action 2.0 mail server "<mail server>" to "<email address>" from
"<email address>" subject "LI-Radius" body "configuration attempted"
```

Note: Replace <**router name**>, <**mail server**>, and <**email address**> with your own information.

Runtime Detection if Lawful Intercept Is Enabled for Cisco IOS XR Software

You can use Cisco EEM to detect Lawful Intercept configurations. Configuring EEM on Cisco IOS XR Software is beyond the scope of this document. Please see the EEM documentation to create the appropriate scripts and environment for your network infrastructure.

The EEM Configuration Guide for Cisco IOS XR Software Version 4.2 is available at: Configuring and Managing Embedded Event Manager Policies in IOS XR.

How to Disable Lawful Intercept

Routers running Cisco IOS XR Software have a command to disable Lawful Intercept:

```
RP/0/RSP0/CPU0:ASR9K#conf t
Wed Feb 19 04:53:30.549 UTC
RP/0/RSP0/CPU0:ASR9K(config)#lawful-intercept disable
RP/0/RSP0/CPU0:ASR9K(config)#commit
Wed Feb 19 04:53:41.185 UTC
```

This command is present only in Cisco IOS XR Software.

Configuration Guides for Specific Product Families

The following are cross references to Lawful Intercept configuration guides for each of the key product families that support Lawful Intercept. These guides include product-specific information that will help you to set up and secure the Lawful Intercept feature in your network.

- Cisco ASR 1000 Configurations Guide for Lawful Intercept:
  - Cisco IOS XE Software 3S Securing User Services Configuration Guide
- Cisco ASR 1000 Role-Based CLI and Lawful Intercept-View Configuration:
  - Cisco IOS XE Software 3S Role-Based CLI Access
- Cisco ASR 9000 Configuration Guide for Lawful Intercept:
  - Cisco ASR 9000 System Security Configuration Guide, Release 5.1.0
  - Cisco ASR 9000 System Security Configuration Guide, Release 4.3
  - Cisco ASR 9000 System Security Configuration Guide, Release 4.2
- Cisco 10000 Lawful Intercept Configuration Guide:
  - Cisco 10000 Lawful Intercept Configuration Guide

Cisco Advanced Services Support

If you are an Advanced Services customer and would like help to determine Lawful Intercept configuration for your network, ask your engineering contact to give you a configuration report. If you are not an Advanced Services customer, contact your local Cisco Account Manager for more information and next steps.

Additional Security Resources

- Tactical security resources: http://tools.cisco.com/security/center/intelliPapers.x?i=55
- Service provider security best practices: http://tools.cisco.com/security/center/serviceProviders.x?i=76

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-731510-02 07/14