Architecture and Practice for VoIP Lawful Interception Using Session Border Controller (SBC)

draft-yang-sipping-voipli-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 28, 2009.

Abstract

Recently broadband Voice over IP (VoIP) has a clear trend to substitute for traditional telephone services such as wire telephone, wireless telephone and mobile telephone service, it has become increasingly clear that VoIP services will be expected to provide Lawful Intercept to the same level experienced in the Public Switched Telephone Network (PSTN)[7]. In an effort to provide lawful interception for broadband VoIP, an architecture using session border controller was proposed, and a prototype implementation of the broadband VoIP lawful interception was created and basic performance evaluation was conducted on this prototype system. This document
reports on the prototype implementation and the test results.

Table of Contents

1. Introduction .............................................. 4
2. Terminology .............................................. 5
3. A Prototype of Broadband VoIP LI Implementation .......... 6
   3.1. Interfaces ............................................ 7
       3.1.1. Internal network interface INI-1 ................. 8
       3.1.2. Internal network interface INI-2 ................. 9
       3.1.3. Internal network interface INI-3 ................. 9
       3.1.4. Internal network interface HI-2 ................. 9
       3.1.5. Internal network interface HI-3 ................. 9
       3.1.6. Internal network interface HI-1 ................. 10
   3.2. Components ........................................... 10
       3.2.1. Session border controller ........................ 10
       3.2.2. Delivery Functions ............................... 11
       3.2.3. Collection functions in LEMF ..................... 12
       3.2.4. Administration Function .......................... 12
4. Test ...................................................... 12
   4.1. Test environment ....................................... 13
   4.2. Test Scenarios and Results ............................. 14
       4.2.1. SBC Intercepted Maximum Concurrent Session Number
              without media ........................................ 14
       4.2.2. SBC Intercepted Maximum Concurrent Session Number
              with media ........................................... 16
       4.2.3. Delivery Function 2 CII Maximum Transactions
              Throughput ........................................... 18
       4.2.4. Delivery Function 2 CII Minimum, Average and
              Maximum Transactions Response Time ................. 19
       4.2.5. Delivery Function 3 CC Maximum Transactions
              Throughput ........................................... 20
       4.2.6. Delivery Function 3 Minimum, Average and
              Maximum Transactions Response Time ................. 21
       4.2.7. Collection Function CII Maximum Transactions
              Throughput ........................................... 22
       4.2.8. Collection Function CII Minimum, Average and
              Maximum Transactions Response Time ................. 23
       4.2.9. Collection Function CC Maximum Transactions
              Throughput ........................................... 24
       4.2.10. Collection Function CC Minimum, Average and
               Maximum Transactions Response Time ............... 25
5. Limitations and Issues .................................... 26
   5.1. General Issues ........................................ 26
   5.2. Security Issues ....................................... 27
   5.3. Protocol Details ...................................... 28
6. Conclusion ................................................ 28
1. Introduction

Lawful Interception (LI) is a requirement placed upon service providers to provide legally sanctioned official access to private communications. With the existing PSTN, lawful intercept is performed by applying a physical ‘tap’ on the telephone line of the target in response to a warrant from a Law Enforcement Agency (LEA). However, VoIP technology has enabled the mobility of the end-user, so it is no longer possible to guarantee the interception of calls based on tapping a physical line. So, interception of VoIP based on traditional lawful interception regulatory framework, which focused on PSTN-based telephone service, is not reasonable. LI of PSTN-based telephone service can be done by wiretapping of the switch, with assistance of telecommunications service providers with LEA. But, for LI of VoIP, interception capability should be developed and installed or separate interception equipment should be deployed.

Current broadband VoIP services show that there are two types of providers: Access providers and Service providers. Access providers are those that actually provide broadband connectivity to the premises (cable, DSL, etc.). Service providers are those providing the VoIP services. In some cases, the Access provider can also be a Service provider (e.g., a cable operator that provides VoIP telephony services). The latest large-scale additions to the VoIP offering are peer-to-peer connections. These services bypass the traditional centralized call-control mechanisms and work directly with proxies and end points.

In a Broadband access environment, the access provider doesn’t know what services the subscriber is utilizing because access providers only supply a pipe from the subscribers premises to the Internet. In this case, the service provider doesn’t provide any switching equipment and the subscriber can work with any Service provider they choose via the pipe to the Internet. The subscriber can also decide to utilize peer-to-peer services over this same broadband pipe. In this environment, the access provider is unable to identify or determine certain events or information due to the service provider not owning or controlling the switching and routing equipment.

One of the primary problems that service providers face when managing VoIP and multimedia calls is the separation of the signaling and media streams. In other words it is quite possible that the two streams may take completely different paths through the network. In addition, even when they do pass through the same device, it may not be aware of the relationship between the streams. Some devices within the network are however specifically designed to understand and manage the separate signaling and media streams - session border
controllers (SBC)[8].

SBC is a session-aware device that manages VoIP calls at the borders of an IP network. Unlike most network devices, SBC are aware of the relationship between the two parts of a VoIP call: signaling and media. Session Border Controllers handle both media and signaling, intercept can be performed in a completely undetectable manner.

SBCs usually sit between two service provider networks in a peering environment, or between an access network and a backbone network to provide service to residential and/or enterprise customers. They typically are deployed at the border between two VoIP networks, and they offer an ideal location to implement a Lawful Intercept solution.

Whilst the detailed requirements for VoIP Lawful Interception may differ from one jurisdiction to another, the general requirements are the same. The LI system must provide transparent interception of specified traffic only and the subject must not be aware of the intercept. The service provided to other users must not be affected during interception.

As part of the effort in developing a broadband VoIP lawful interception architecture, we implemented a prototype and conducted evaluation experiments on the prototype system. In this document, we first describe the prototype solutions and then report experimental results. We hope that this document can provide useful information to those interested in the subject.

The prototype implementation and experimental results presented in this report serve only as an input, and by no means preempt any solution development that may be carried out by future IETF effort. Indeed, the presented solutions are experimental approaches and have a number of limitations as discussed in Section 5 and 6.

2. Terminology

Lawful Intercept (LI) "C The targeted intercept of VoIP services, by a service provider on the behalf of Law Enforcement, when authorized by a court.

Session Border Controller (SBC) — provides a variety of functions to enable or enhance session-based multi-media services (e.g., Voice over IP), provides access to an interception subject!_s.

Call-Identifying Information (CII) — refers to information that identifies the origin, direction, destination, or termination of each
call generated or received by a subject.

Call Content (CC) – audio and video media flow.

Collection Function (CF) "C A law enforcement facility designated as the transmission destination for CC and CII.

Delivery Function (DF) "C The mechanism responsible for delivering intercepted communications form a VoIP network operator/service provider to a CF via HI.

Administration Function – provides provisioning interface for the intercept as a result of a court order or warrant delivered by the Law Enforcement Agency (LEA)

Internal Network Interface (INI) "C The VoIP network_s internal interface between SBC and DF. Consists of INI1,INI2, and INI3 matching HI1,HI2, and HI3 interfaces.

Handover Interface (HI) "C Interface for delivering CC and CII from DF to CF.

3. A Prototype of Broadband VoIP LI Implementation

A new VoIP Lawful intercept architecture based on SBC is proposed, as shown in Figure 1.
This methodology utilizes a TCP/IP interface to the SBC to both provision it and receive call data events (originate, ring back, hook lash, etc.) from it. Those interfaces are described as INI-1 for provisioning and INI-2 for call data. A third interface INI-3 receives a copy of the media stream. All of this information is sent to the Delivery functions from SBC. The Delivery functions then sorts, filters, and formats the information for delivering to Law Enforcement. The interfaces used to deliver the call data events and media content to Law Enforcement are TCP/IP interfaces called HI-2 and HI-3, respectively. Lawful Interception deals with two products, these are: contents of call (CC) and call-identifying information (CII). CC is exactly what it sounds like: the voice, video or message contents. CII refers to information that identifies the origin, direction, destination, or termination of each call generated or received by a subject. In the following sections, we describe the specific mechanism implemented in detail.

3.1. Interfaces

This section provides a brief description of the interfaces in the architecture (Figure 1). One of the objectives in defining these interfaces is to keep both the internal interfaces (INI-1, INI-2, and INI-3) and the handover interfaces (HI-1, HI-2, and HI-3) the same.
regardless of country-specific requirements.

3.1.1. Internal network interface INI-1

This is an intercept request provisioning interface, through which the Administration function provisions warrants on SBC, and activate, deactivate or interrogate the Delivery functions.

Administration function uses this interface to provide the provision for the intercept as a result of a court order or warrant delivered by the LEMF. It involves separate provisioning interfaces for SBC and Delivery functions. Administration function takes care of provisioning of SBC and Delivery functions with some policy.

In order to provide a generic interface for intercepting, replicating, encapsulating and transporting call information packets to Delivery function, the intercept request interface should specify:

1 the identification of the subject to be intercepted, such as a SIP URI;
2 the destination address and port of the Delivery function or Collection function (where to send the intercepted packets);
3 encapsulation and transport parameters;
4 start time, end time, and duration.

INI-1 involves separate provisioning interfaces, INI-1(1), INI-1(2), and INI-1(3). INI-1(1) is an interface between the SBC and Administration function for delivering provisioning information to point out the intercepted subject identify, when to start and end, which delivery function the intercepted information should be sent to, etc. INI-1(2) and INI-1(3) interfaces between the Delivery functions and Administration function are used to config the Delivery function which SBC will send intercepted information to it, and which Collection function the intercepted information should be sent to, etc. 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 LEMF has to be translated into an identity that can be used by the network to enable the intercept.

In this prototype implementation, INI-1 is implemented with Abstract Syntax Notation One (ASN.1) [1] and Basic Encoding Rule (BER) [2] encoded to be binary compatible.
3.1.2. Internal network interface INI-2

This is the VoIP call data (e.g., SIP signaling) intercepting interface, over which SBC sends call-identifying information (e.g., SIP signaling) to the DF server. The intercepted call data is encapsulated using DIAMETER protocol [3]. This encapsulation method retains all of the information in the original packets (source and destination addresses as well as payload) and provides an identifier for correlating the CC with the CII.

Note, however, this interface implemented in prototype 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). The underlying networks should be engineered to meet the overall reliability requirements for delivery of content.

3.1.3. Internal network interface INI-3

This is the call content (e.g., RTP media stream) intercepting interface, over which SBC sends the RTP media stream to the DF server. The transferred information in this interface is encapsulated into Diameter event messages [3].

Since the media path is independent of the signaling path, the media may not traverse through the operator's network unless the SBC modifies the session description exchanged between the user-agents. By modifying the session description the SBC can force the media to be sent through SBC. The SBC behaves as a Back-to-Back User Agent (B2BUA) and inserts itself in the media path, and modifies the session descriptions carried in the SIP messages. As a result, the SBC receives media from one user-agent and relays it to other user-agent and performs the identical operation with media traveling in the reverse direction.

3.1.4. Internal network interface HI-2

The Handover Interface, HI-2, is the interface between DF 2 and LEMF for delivering CII. This interface transmits the result of intercepted SIP signaling to the LEMF, and is implemented with Abstract Syntax Notation One (ASN.1) and Basic Encoding Rule (BER) encoded to be binary compatible.

3.1.5. Internal network interface HI-3

The Handover Interface, HI-3, is the interface between DF 3 and LEMF for delivering CC. This interface transmits the result of intercepted RTP media stream to the LEMF, and is implemented with Abstract Syntax Notation One (ASN.1) and Basic Encoding Rule (BER)
encoded to be binary compatible.

3.1.6. Internal network interface HI-1

This is an interception administration interface, through which the LEMF provides interception administration information to the service provider administration function.

In this prototype, this interface is under consideration, and is not available now.

3.2. Components

This section provides a brief description of the key components in the architecture (Figure 1).

3.2.1. Session border controller

Session border controller handles all SIP messages which are needed for interworking between different operators who exchange traffic with each other. It takes care of replicating signaling and delivers it to specific delivery function using appropriate format. SBC inserts itself in the media path, and modifies the session descriptions carried in the SIP messages to deliver it to specific delivery function using appropriate format.

Example: Consider the following example scenario: the SBC receives an INVITE request from the outer network, which in this case is an access network. The received SIP message containing the SDP session descriptor is shown as following.

```
v=0 o=- 5 2 IN IP4 218.241.111.22 s=CounterPath X-Lite 3.0 c=IN IP4 218.241.111.22 t=0 0 m=audio 12706 RTP/AVP 107 119 100 106 0 105 98 8 3 101 a=alt:1 1 : IF5eH1Wn YCfz8oLV 218.241.111.22 12706 a=fmtp:101 0-15 a=rtpmap:107 BV32/16000 a=rtpmap:119 BV32-FEC/16000 a=rtpmap:100 SPEEX/16000 a=rtpmap:106 SPEEX-FEC/16000 a=rtpmap:105 SPEEX-FEC/8000 a=rtpmap:98 iLBC/8000 a=rtpmap:101 telephone-event/8000 a=sendrecv
```

In this example, the SBC performs the media intercept function by rewriting the !(R)c!_ and !!(R)m!_ lines in above SDP. The following shows the session description after the intercept function.

```
v=0 o=- 5 2 IN IP4 218.241.111.22 s=CounterPath X-Lite 3.0 c=IN IP4 218.241.111.22 t=0 0 m=audio 30006 RTP/AVP 107 119 100 106 0 105 98 8 3 101 a=alt:1 1 : IF5eH1Wn YCfz8oLV 218.241.111.22 12706 a=fmtp:101 0-15 a=rtpmap:107 BV32/16000 a=rtpmap:119 BV32-FEC/16000 a=rtpmap:100 SPEEX/16000 a=rtpmap:106 SPEEX-FEC/16000 a=rtpmap:105 SPEEX-FEC/8000 a=rtpmap:98 iLBC/8000 a=rtpmap:101 telephone-event/8000 a=sendrecv
```
SBCs can terminate media streams and SIP dialogs by generating BYE requests in a situation where the LI needs.

Note, if an SBC directs many media streams through SBC itself, it is likely to cause a significant amount of additional traffic to a path to that SBC. This might create possible bottleneck in the path.

In this prototype, we used an Open Source software, OpenSBC, written by Joegen Baclor, Solegy LCC. To enhance the OpenSBC to replicate RTP packet, we added media intercept function by using PCAPLIB. We also added some code in OpenSBC to encapsulate SIP and RTP using Diameter AVP.

3.2.2. Delivery Functions

Delivery function implemented the INI-2, INI-3, HI-2 and HI-3 interfaces specification.

Delivery function performs the delivery functions. It converts the information from the INI-2 and INI-3 interfaces to the corresponding information format on the HI-2 and HI-3 interfaces respectively.

It receives the data from the SBC, packets them into the correct format and delivers them to the correct LEMF. In the case where multiple law enforcement agencies are intercepting the same subject, the delivery function may replicate the information many times, and forward them to multiple LEMF interfaces simultaneously.

Signaling messages and RTP media streams are using different delivery functions. Delivery function 2 is used for signaling messages processing and delivering, and Delivery function 3 is used for RTP media streams processing and delivering.

Any information stored within the SBC and Delivery functions are stored in volatile memory, so that these information are erased if a component of the network node is removed or powered down. Only the encrypted database of the ADMF should be maintained during power-down situations. In the event of a link failure between the DF and the LEMF the intercept products may be buffered for a short time in memory only. Any long term failure of the interface will result in intercept products being lost - this information must not be spooled to permanent storage.

In this prototype, we implemented Delivery functions using C++. 
3.2.3. Collection functions in LEMF

Collection function in LEMF implemented the HI-2 and HI-3 interfaces specification, and can receive intercepted VoIP call signaling and RTP media stream on these two interfaces.

It records and stores the intercepted traffic, and provides analysis tools to track, correlate and interpret intercepted traffic.

Also, collection function can recover the original VoIP call based on the received SIP signaling and RTP media.

In this prototype, we implemented collection function using C++.

3.2.4. Administration Function

Administration function provides the provisioning interface for the intercept as a result of a court order or warrant delivered by the LEMF. This function implemented INI-1 and HI interfaces specification. It is used for receiving warrants from HI-1 interface, and delivering provisioning information to SBC and Delivery functions to point out the intercepted subject identify, when to start and end, which delivery function the intercepted information should be sent to, etc.

It supports user interface, maintains all warrant information from LEMF using encrypted database, creates shared memory image of intercept information.

In this prototype, this component is under consideration, and is not available now.

4. Test

The objective of test is to evaluate SBC behaviors while it performs LI, and the intercepting capability of developed LI interfaces and functions.

The test cases covered in this document provide performance evaluation metrics for this prototype, including:

1. concurrent number of users that completed their run successfully;
2. number of transactions that passed, failed, stopped, or ended with errors;
3. average response time taken to perform transactions during each second;
4. total of number of completed transactions (both successful and unsuccessful) performed during each second;
5. minimum, average, and maximum response time for all the transactions in the
4.1. Test environment

Test environment is shown in Figure 2. SBC is using the OpenSBC which is enhanced with RTP media intercept and supports INI interfaces; The calling and called parties are using SIPP to simulate concurrent calls.

VoIP call flows is shown in Figure 3.
Figure 3 Call flow of VoIP in testing

4.2. Test Scenarios and Results

4.2.1. SBC Intercepted Maximum Concurrent Session Number without media

VoIP call flows is shown in Figure 3, but there are no RTP media stream sent.

Procedure:
1. Configure SIP UDP with an attempted session rate = 10 sessions per second, session duration = 20ms, and media streams per session = 0.

2. Start to initiate SIP Session establishment with the SBC.

3. Measure failed session attempts and total session established at the SBC.

4. If no failed session attempt is recorded then increase the attempted session rate configured on the Tester by 50%.

5. If a failed session attempt is recorded then reduce the attempted session rate configured on the Tester by 50%.

6. Repeat steps 2 through 5 until the maximum concurrent session establishment rate is obtained.

Test result is shown in Figure 4. From result in our test, the maximum concurrent session number is about 80. The average response time for SIP messages is within 30ms when LI was not carried out in SBC. The average response time for SIP messages is within 80ms when LI was carried out in SBC.
4.2.2. SBC Intercepted Maximum Concurrent Session Number with media VoIP call flows is shown in Figure 3.

Procedure:

1. Configure SIP UDP with an attempted session rate =10 sessions per second, session duration=20 sec.

2. Start to initiate SIP Session establishment with the SBC and transmit media through the SBC by modifying the SDP.

3. Measure failed session attempts and total session established, and Packet Loss of the media.

4. If no failed session attempt or packet loss is recorded then
increase the attempted session rate configured on the Tester by 50%.

5. If a failed session attempt or packet loss is recorded then reduce the attempted session rate configured on the Tester by 50%.

6. Repeat steps 2 through 5 until the maximum concurrent session number is obtained.

Test result is shown in Figure 5 and Figure 6. From Figure, we can see the maximum concurrent session number is 80.

The average response time for SIP messages is within 30ms when LI was not carried out in SBC. The average response time for SIP messages is within 90ms when LI was carried out in SBC.
In our SBC implementation, SIP signaling and RTP media are processed in different modules. In our tester, SIP signaling flows are same in above two test cases. From Figure, we can see the RTP media processing reached the peak value at the 80 Concurrent SIP sessions. The throughput of RTP media streams reaches about 600 kilo bytes per seconds.

![Figure 5 Maximum Concurrent Session Number](image)

4.2.3. Delivery Function 2 CII Maximum Transactions Throughput

We use the test tool Load Running to evaluate the Delivery function performance. We create 200 concurrent transactions, and it is the
maximum that can be obtained in this tool.

We can obtain the result of maximum concurrent SIP signaling transactions throughput of Delivery Function 2 is 110 transactions, and average concurrent transactions per second is 32. Figure 7 shows the total number of successful CII transactions performed during each second of a load test.

![Figure 7 Total Passed CII Transactions per Second](image)

This graph helps to determine the actual transaction load on VoIP Lawful Intercept system at any given moment.

4.2.4. Delivery Function 2 CII Minimum, Average and Maximum Transactions Response Time

Figure 8 shows the minimum, average and maximum CII transactions response time for SIP signaling transactions. The minimum response time is 0.002 seconds, the maximum response time is 0.269 second, and the average response time is 0.018 second.
4.2.5. Delivery Function 3 CC Maximum Transactions Throughput

Figure 9 shows the total number of successful CC transactions performed during each second. We can obtain the result of maximum concurrent RTP transactions throughput of Delivery Function 3 is 25 transactions, and average concurrent RTP transactions per second is 7.
4.2.6. Delivery Function 3 Minimum, Average and Maximum Transactions Response Time

Figure 10 show the minimum, average and maximum CC response time for RTP transactions. The minimum response time is 0.02 seconds, the maximum response time is 9.05 second, and the average response time is 3.46 second.
4.2.7. Collection Function CII Maximum Transactions Throughput

From Figure 11, we can obtain the result of maximum concurrent SIP signaling transactions throughput of collection function in LEMF is 105 transactions, and average concurrent transactions per second is 38.
Figure 11 Total Passed CII Transactions per Second

4.2.8. Collection Function CII Minimum, Average and Maximum Transactions Response Time

Figure 12 shows the CF minimum, average and maximum CII transaction response time for SIP signaling transactions. The minimum response time is 0.003 seconds, the maximum response time is 3.029 second, and the average response time is 0.669 second.
4.2.9. Collection Function CC Maximum Transactions Throughput

Figure 13 shows the total number of successful CC transactions in CF performed during each second of a load test. We can obtain the result of maximum concurrent RTP transactions throughput of CF is 63 transactions, and average concurrent RTP transactions per second is 13.
4.2.10. Collection Function CC Minimum, Average and Maximum Transactions Response Time

Figure 14 shows the minimum, average and maximum CC response time for RTP transactions in CF. The minimum response time is 0.013 seconds, the maximum response time is 7.083 second, and the average response time is 3.285 second.
5. Limitations and Issues

There are several issues both within this overall VoIP LI problem area and with the particular approach taken in the prototype.

5.1. General Issues

It seems not to be difficult to decide whether technically mature and widely provided services such as PSTN-based voice services, cellular services and 3G services are to be intercepted or not. However, the situation for recently developed services such as internet telephony service, internet access services and messenger is difficult. The necessary of lawful interception for these services is increasing because of the increase of the users, but LI of the services can be controversial because the boundary of services is not clear, government!'s policy for IP services is not fully established, and so on[4].
For the internet telephone service, the followings can be considered to decide whether to intercept the service or not:

1. Whether it substitutes for traditional telephone services considering the number of the service users or communication time or sales;

2. Telecommunication service management regulations, and so on.

Because VoIP has a clear trend to substitute for traditional telephone services such as wire telephone, wireless telephone and mobile telephone service, it has become increasingly clear that VoIP services will be expected to provide Lawful Intercept to the same level experienced in the PSTN. The FCC [9] in North America for example has mandated that both emergency calls and Lawful Intercept must be available for VoIP. Whilst not all countries mandate this capability, any network operator building a publicly available voice or multimedia over IP service today will need to plan a network which is flexible enough to implement these regulatory services in the future.

5.2. Security Issues

The lawful intercept solution should have the ability to provide stringent security measures to combat threats such as impersonation of delivery function!’s, privacy and confidentiality breaches, as well as message forgery and replay attacks.

Illegal interception may be done using facilities, equipment, functions, human resources and procedures prepared for lawful interception. Therefore, it is very important to prepare technical and managerial countermeasures to prevent illegal interception, unauthorized access to call identifying information, call content, or to interception log data.

In general, all interfaces could have the capability of providing strong cryptographic authentication to establish the identity of the principals, and be able to correlate the identity of the principle with the action they are attempting to perform. All interfaces could be capable of performing some sort of cryptographic message integrity checking such as, for example, HMAC-MD5, if needed[5].

While this document doesn’t discuss issues of physical security, operating system, or application hardening within the principals of the lawful intercept solution, they are clearly important.
5.3. Protocol Details

In the current VoIP lawful interception prototype, we defined the HI-2 and HI-3 interface specification with Abstract Syntax Notation One (ASN.1) and Basic Encoding Rule (BER). And also provide methods to encapsulate SIP and RTP using Diameter AVP in INI-2 and INI-3 interfaces specification.

The broadband VoIP lawful intercept solution in this document is merely one option among many. Solutions appear to depend highly on SBC. In any case, the prototyped solution has a number of limitations.

6. Conclusion

Several conclusions can be drawn from the practice.

First, the practice is a proof that a prototype can be built that is deployable on border between two VoIP networks to carry out both interworking and intercepting for VoIP services. The practice also proved a proof of concept for the SBC-based lawful intercept for VoIP service.

SBC is deployed at the border between two VoIP networks to execute a number of access, router, switch, security and quality management roles, and they offer an ideal location to implement a Lawful Intercept solution. Carriers don’t need to learn the LI functions of multiple devices, reduces costs for training, maintenance, etc.

Nevertheless, as discussed in the previous section, there are a number of limitations, issues, and questions in the prototype designs.

Future work in this area should attempt to answer some of the issues raised in section 5. Some of the key issues going forward include:

1. Scalability for SBC and Delivery functions.

2. Interfaces specification design issues, such as INI-1 and HI interfaces, etc.

3. Security considerations, all interfaces could be capable of performing some sort of cryptographic message integrity checking such as, for example, HMAC-MD5, if needed.
7. Security considerations

The purpose of the document is to report broadband VoIP LI architecture prototype implementation and experimental results. Some security considerations of the solution mechanisms of the prototype are mentioned in section 5, but are not the main problem to be described in this document.

8. Acknowledgements

The authors thank Yuanmin Chen, Bin Guo, Wei Zhang, and Hui Chen for their assistance in developing this prototype system. The authors thank their contribution to this document.

9. References

9.1. Normative References


9.2. Informative References


Authors’ Addresses

Menghui Yang
CNNIC
4 South 4th Street, Zhongguancun, Haidian District
Beijing, Beijing  100190
China
Phone: +86 10 5881 3204
Email: yangmenghui@cnnic.cn

Xiaodong Li
CNNIC
4 South 4th Street, Zhongguancun, Haidian District
Beijing, Beijing  100190
China
Phone: +86 10 5881 3020
Email: lee@cnnic.cn

Wei Mao
CNNIC
4 South 4th Street, Zhongguancun, Haidian District
Beijing, Beijing  100190
China
Phone: +86 10 5881 2230
Email: mao@cnnic.cn