Distributed System for Lawful Interception in VoIP Networks

Andro Milanović, Siniša Srbljić, Ivo Ražnjević*, Darryl Sladden*, Daniel Skrobo, and Ivan Matošević

School of Electrical Engineering and Computing
University of Zagreb, Croatia
{andro.milanovic,sinisa.srbljic,ivan.matosevic,daniel.skrobo}@fer.hr

*Cisco Systems, Inc., San Jose, CA, USA
{ivo,dsladden}@cisco.com

Abstract-- **Voice over IP is one of the most propulsive technologies today. Significant advantages of VoIP over conventional telephone system provide a major incentive for enterprises and service providers to use the new technology. There is a variety of IP Telephony standards, which provide basic models for implementation of VoIP. However, some significant problems still need to be adequately solved. Security, global administration and billing, emergency dialing plans and lawful interception are some of the areas that are being researched.**

This paper proposes a distributed system for the lawful interception in IP Telephony networks. The proposed system has scalable architecture, it supports various interception methods, and it can be deployed on various network infrastructures. In addition, the system design addresses various issues present in IP networks, for instance: security protocols, network configuration, and standardized data formats. A prototype of the interception system, based on the proposed architecture, has been implemented and tested.

Index Terms-- **IP telephony, Voice over IP, VoIP, Lawful Interception, Electronic Surveillance, Wiretap, CALEA, distributed systems**

I. Introduction

Explosive growth of Internet and Internet-based services has encouraged the extensive research efforts in the field of Voice over IP (VoIP) and IP telephony. VoIP is the technology for transporting the voice communication on IP networks and IP telephony is the implementation of VoIP, which is used to create telephone networks based on IP networks. The VoIP and IP telephony have significant benefits for both end-users and service providers. Since the VoIP uses the IP network to transport the voice streams, the unified network is created, which transports both data and voice. The unified network has significantly lower implementation and maintenance costs in comparison to maintaining two separate, voice and data networks. In addition, VoIP uses the smaller portion of network bandwidth than conventional telephone network, thus improving the efficiency of network infrastructure. IP telephony has lower billing rates due to the current low costs of IP connectivity. The cost efficiency is especially notable in long distance IP telephony calls. Another significant advantage of IP telephony are value-added services. The IP telephony enables a number of services like video and voice conferencing, video and voice messaging, data and fax transmission, which are not available in the conventional telephone networks. These advantages are the reason why a rapidly growing number of enterprises and service providers are using the VoIP.

There is a multitude of IP telephony standards, which define the interoperation of VoIP systems. The two most widely deployed standards are H.323 [4] and Session Initiation Protocol (SIP) [5]. However, these standards still do not provide solutions to some issues like emergency dialing plans, security, global usage tracking and billing, as well as lawful interception (LI). Solutions to these issues are the objectives of extensive research efforts.

Originally, LI was required by governments in order to support law enforcement agencies. For example, all telecommunication companies in the USA are subject to CALEA (Communication Assistance for Law Enforcement Act) [2]. According to CALEA, each telecommunication service provider must provide the means for lawful interception. This act was originally intended for conventional telecommunication companies, but with the emergence of IP telephony, it included the IP telephony service providers as well. In addition to law enforcement, LI can provide significant benefits to enterprises as well. LI can be used in order to detect and prevent the disclosure of the confidential company information.

While the conventional telephone systems offer technical solutions for LI, the official organization for regulation of Internet standards, IETF (Internet Engineering Task Force) has announced that no standardized means for lawful interception in VoIP networks would be provided [3].

The research described in this paper is performed at School of Electrical Engineering and Computing, University of Zagreb, Croatia and is supported and sponsored in part by Cisco Systems, Inc., San Jose, CA, USA.

Therefore, new products and standards for LI in IP telephony still need to be developed.

LI in IP telephony systems is a complex issue. Unlike the conventional telephone systems, the VoIP uses end-to-end call model with no centralized control and call processing. The signaling, control and content channels of each VoIP call can follow different routes between endpoints. Additionally, the user profile in IP telephony networks is mobile. This enables the user to use his IP phone number from any host connected to the Internet. Dynamic IP routing and multiplicity of possible routes additionally increase the complexity of the interception of IP telephony.

In order to provide the feasible solution, a specialized LI system has to be created. The LI system for IP telephony should have some important capabilities. It should be distributed and scalable, in order to manage heavy traffic in large-scale networks, as well as to support diverse network configurations, like sub-networks and remote locations. It should support various IP telephony protocols and various interception methods. Finally, it should have centralized management in order to ease the control and maintenance.

The architecture of the custom designed distributed LI system is described in Section II. Section III presents the Wiretap Information Exchange Protocol (WIEP), which defines the communication procedures used in the distributed LI system. A prototype of a distributed LI system is described in Section IV. Section V concludes the paper and describes the future work.

II. Distributed System Architecture

In order to fulfill all requirements of lawful interception, we have designed a distributed system for LI in IP telephony networks. The system is scalable and supports heterogeneous IP telephony protocols and heterogeneous interception methods. The system architecture is distributed, with hierarchical control structure. The control structure consists of four component classes and a proprietary communication protocol. The communication mechanisms provide automatic component communication as well as procedures for automatic and manual transmission of control information and recorded data. There are four component classes, which are based on the hierarchy level: Top-Level Device (TLD), Intermediate-Level Device (ILD), Bottom-Level Device (BLD), and Storage Device (SD). All communication in the distributed LI system is based on the WIEP protocol, which is described in Section III.

The components exchange the information that falls into two categories: Wiretap Information and Wiretap Data. Wiretap Information consists of a set of VoIP endpoints that are subject to LI. It also includes the specific information that describes LI policies. All intercepting components of the distributed LI system use this information to identify the calls that are designated for LI. Thus, according to legal requirements, no information about the calls that are not listed in the Wiretap Information will be recorded. The other category of information, Wiretap Data, is acquired during the interception of VoIP calls. It includes information like recorded call start and call end times, addresses of endpoints participating in a call, recorded content of a call, and other categories of data acquired through LI.

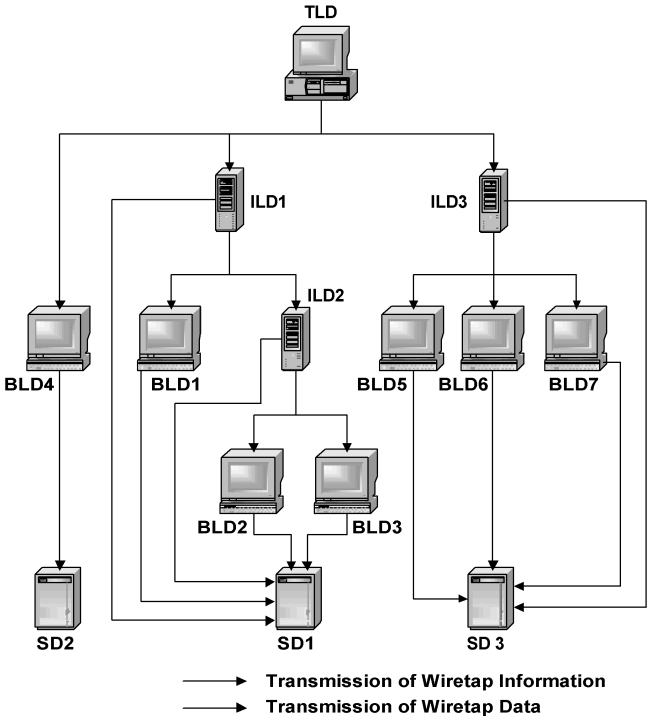

Fig. 1. A distributed LI system

Figure 1 presents the hierarchical overview of a sample distributed LI system. The presented system consists of a number of devices, which are divided into four categories. TLD is the central management component of the distributed system. All Wiretap Information is entered and stored at the TLD, which automatically relays the Wiretap Information to the lower-level components of the system hierarchy. It does not perform any interception of VoIP calls and there is only one TLD in each distributed LI system. TLD can have multiple descendants, which can be both ILDs and BLDs.

Intermediate-Level Device is the mediating component of the system. It receives the Wiretap Information from its hierarchical parent and relays it to the descendants. An ILD can have multiple ILDs and BLDs as descendants, while its parent can be either another ILD or the TLD. A distributed LI system can have multiple ILD components. In addition to mediating function, the ILD can also intercept VoIP calls and record some categories of Wiretap Data. Since the lower-level device can benefit from this information, the ILD can use the acquired Wiretap Data to extend and modify the Wiretap Information it received from its parent. The modified Wiretap Information is then sent to its descendants. This is a significant capability because it can improve the performance of the system as well as extend its interception capabilities.

For instance, H.323 endpoints can be listed in Wiretap Information by their aliases. Due to the mobility of IP telephony user, there is no direct mapping between user's alias and the actual IP address. However, if ILD intercepts a call on an H.323 gatekeeper, it can use the intercepted information to map the alias to the corresponding IP

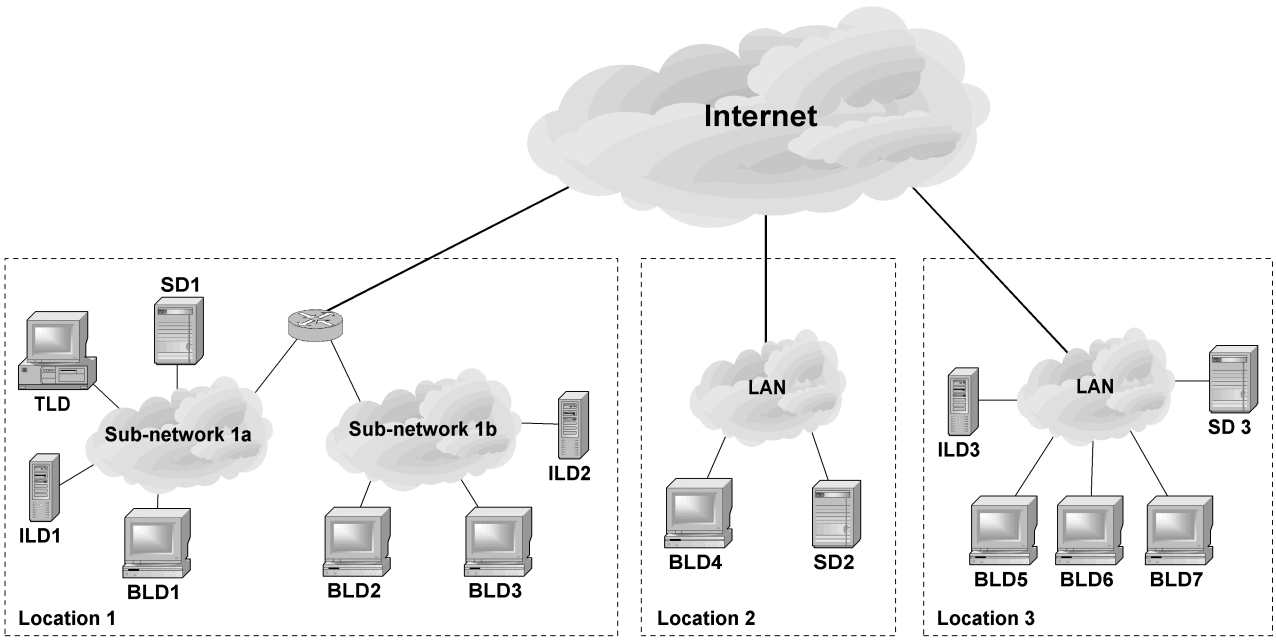

Fig. 2. A sample network configuration of a distributed LI system

addresses. The received Wiretap Information can then be extended with the acquired IP address. Finally, a lower-level device can use the extended information provided by ILD to improve the performance or to intercept a call that would otherwise not qualify for interception.

BLD is positioned at the bottom of the hierarchical control structure of the distributed LI system. The main purpose of BLD is to intercept the VoIP calls. Since it has no descendants, the BLD only receives the Wiretap Information from its hierarchical parent without transmitting it to other devices. There can be multiple BLDs in the distributed LI system, which can support various IP telephony protocols and various interception methods. Each BLD can have either ILD or TLD as its parent.

SD is not a part of the hierarchical control structure. The purpose of SD is to provide the remote storage for recorded Wiretap Data. Both ILDs and BLDs can automatically initiate the transfer of the recorded Wiretap Data to a designated SD. However, the system administrator can also request the Wiretap Data to be stored locally on a device that intercepted the call. The Wiretap Data stored at SD can either be locally analyzed or sent through secure Internet connection upon the request from the authorized user.

Proposed distributed LI system has central management device and the hierarchical control structure, which is used to automatically transmit the control information to all components of the system. Therefore, system management and control is simplified and limited to only one location. In addition, all recorded Wiretap Data can be collected and analyzed at the central location. Distributed architecture of the LI system provides the necessary scalability and adaptability to various network configurations. In addition, components of the distributed system can support various IP telephony protocols and interception methods [1]. An example of a network configuration of the distributed LI system is presented in Figure 2.

The system presented in the Figure 2 consists of the same components as the system presented in Figure 1. Moreover, these systems have the same hierarchical control structure. Figure 2 presents the network configuration consisting of three distinct locations. The Location 1 is the central management location where the TLD is placed. There are two sub-networks at this location. The VoIP clients in the sub-network 1a use the H.323 protocol. The calls are intercepted by ILD1 and BLD1, while the recorded Wiretap Data is stored at SD1. Sub-network 1b is a mixed environment, which uses both H.323 and SIP protocols. In this sub-network, ILD2 and BLD2 intercept the H.323 traffic, while the BLD3 intercepts the SIP traffic. Recorded Wiretap Data is stored at SD1.

At the Location 2, there is only a small number of SIP VoIP clients, which are connected to the same LAN. Therefore, there is only one intercepting device, BLD4. In order to improve data transmission rate, BLD4 stores the Wiretap Data at the SD2 located in the same LAN. Location 3 consists of a large number of H.323 VoIP clients connected to the LAN. In order to improve the performance, three BLDs are used at this location. The VoIP clients are logically divided among BLD5, BLD6 and BLD7. Under ideal conditions, each of these devices would have to handle only 1/3 of the total VoIP traffic at the Location 3. The recorded Wiretap Data is stored at the locally placed SD3.

The whole system is controlled from the TLD at the Location 1. System administrator needs to define Wiretap Information list and interception policies only once for all devices in the distributed LI system. In addition, all Wiretap Data stored at SD1, SD2 and SD3 can be collected from this location. The configuration presented in Figure 2 is just one of many possible configurations of the same distributed LI system presented in Figure 1. Therefore, the presented architecture of the distributed LI system is highly adaptable, and it can be applied in a virtually unlimited set of VoIP network configurations.

III. Wiretap Information Exchange Protocol

Wiretap Information Exchange Protocol (WIEP) defines the communication procedures for the proposed distributed LI system. Components of the distributed LI system exchange two distinct categories of information, Wiretap Information and Wiretap Data. In order to create a standardized and extensible message format, WIEP uses the XML to format both information categories.

The Wiretap Information is the control information that specifies the list of endpoints under surveillance and the interception policies. The user defines this information at the TLD and it automatically propagates to all devices in the distributed LI system. The Wiretap Information uses four methods for endpoint identification. The first method is to define a host IP address. This method is used to identify a single endpoint. A set of endpoints can be identified in two ways, using the subnet address or using the range of IP addresses. Finally, the endpoint can also be identified by its alias. Alias is a high-level identification element defined by H.323. It is similar to a phone number in PSTN.

In addition to endpoint identification, each record in the Wiretap Information list specifies interception policies, which control the call interception process for the given entry. The policies are specified as a set of attributes. First attribute defines if the distributed LI system will intercept signaling, content, or both. Signaling and content are the categories defined by CALEA. Signaling includes identification of endpoints, call start and call end times, and some other specific call-control information. Content of the call includes any information, like conversation or dial-tone signals, exchanged after the call has been established.

Each entry in the Wiretap Information list also includes two time and date pairs, which define when the interception should start and when it should end. Another attribute defines the storage method, which can be set as local or as remote. The remote storage method includes an IP address of a remote SD. Related to the storage method is the priority level attribute, which defines urgency for transmission of recorded information. The priority level ranges from low, when the recorded information is sent to SD upon the call end, to high priority when the recorded information is sent in real time to the designated receiving device. Since the XML is used to format all information, the set of attributes can easily be extended.

The Wiretap Data is the recorded information obtained by intercepting the calls. It includes both call signaling and call content. The Wiretap Data can be automatically sent to the designated SD or it can be sent upon the user request. The Wiretap Data uses the standardized format based on XML.

Since the security of lawful interception is the major concern, WIEP protocol uses authentication, authorization and secure transmission. The authentication and authorization procedures are used each time a TCP connection is established between two components of a distributed LI system. Therefore, the unauthorized user can neither gain access to a list of endpoints under surveillance, nor initiate any unauthorized call interceptions. The security of Wiretap Information and Wiretap Data transmitted between components is ensured by mechanisms like SSL and IPSec.

IV. The Prototype System

Using the proposed design of a distributed LI system, we have built a prototype LI system. The system supports only H.323 protocol and consists of three component classes. Component named Wiretap Controller is the TLD in the hierarchical control structure. Two components were implemented as ILDs. The first one simply relays the Wiretap Information without any additional functionality. The second component, named Gatekeeper Wiretap Device, can also intercept call signaling. In addition, the Gatekeeper Wiretap Device can extend and modify the received Wiretap Information as specified in Section II. The Promiscuous Wiretap Device is a BLD in the control hierarchy. Its main purpose is to intercept signaling and content. The SD component proposed in the distributed LI system design was not implemented. Therefore, all components store the recorded information locally. The implemented version of WIEP protocol supports a subset of the proposed capability set. It only provides some basic security mechanisms and does not support transmission of Wiretap Data. Figure 3 presents a sample configuration of the prototype LI system.

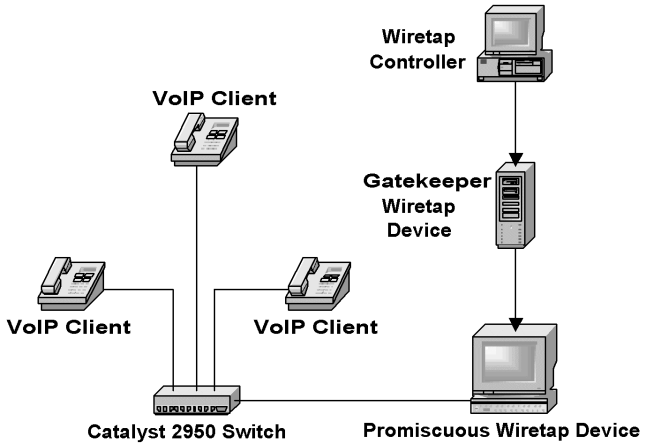

Fig. 3. Configuration of a prototype LI system

The Wiretap Controller is implemented as a stand-alone program that can run on either Windows or Linux PC. The configuration information is stored in local files, which provide the list of descendants and the Wiretap Information list. During the initialization, the Wiretap Controller reads the local configuration information and tries to send the Wiretap Information to its descendants. If any descendant does not respond, the Wiretap Controller will repeat connection attempts. In addition, Wiretap Controller also serves requests from its descendant. Therefore, if any descendant is restarted, due to maintenance or system failures, it can easily obtain the Wiretap Information from the Wiretap Controller without influencing other components of the distributed LI system.

The Gatekeeper Wiretap Device (GKWD) is implemented as a software module and incorporated into the OpenH323 Gatekeeper [7] software. A significant part of the device consists of the ILD code, which is used to relay the Wiretap Information from the parent component to the descendants. The second function of GKWD is to intercept the call signaling information at the gatekeeper. The call-signaling

information is acquired from messages exchanged during the RAS (Registration, Admission and Status) [4] phase of each H.323 call. The primary purpose of RAS is to register the client with the IP telephony system and to obtain the IP address of the called party. All RAS communication is performed between an endpoint and the gatekeeper.

GKWD intercepts the RAS messages and records the intercepted information locally as Wiretap Data. In this way, the information about call participants, call start and call end times can be recorded. However, the interception is performed only for the endpoints listed in the Wiretap Information. Since the H.323 endpoints register their IP address with the gatekeeper, the GKWD can also map an H.323 alias with the valid IP address. Obtained IP address is added to the Wiretap Information list and sent to the hierarchical descendants. Descendants can use the IP address to improve the accuracy and performance of the LI process.

The Promiscuous Wiretap Device (PWD) is implemented as a stand-alone program running on a Linux based PC connected to the Ethernet. It was built using the open source H.323 protocol stack [6]. The PWD receives the Wiretap Information from its parent, which can be either Wiretap Controller or GKWD. Since the PWD is at the bottom of the hierarchical control structure, it does not relay the received information. The PWD intercepts the content of the calls and any in-band call signaling. The interception is performed only for the endpoints listed in the Wiretap Information. In addition, the Wiretap Information is used to decide if the call content, call signaling or both are intercepted.

In order to intercept the VoIP traffic, the PWD sets the NIC (Network Interface Card) to the promiscuous mode. In this mode, the NIC receives all network traffic it can register on the Ethernet cable. In order to receive all traffic on a LAN, the PWD needs to be connected to the hub or to the monitoring port on a switch. The monitoring port must be configured to receive all traffic from ports to which the VoIP endpoints are connected. Since the switch is a low-level network device, it sends all LAN traffic from the designated ports to the monitoring port. As a result, PWD receives all Ethernet frames coming from VoIP endpoints, even if they do not contain any VoIP information. PWD analyzes the received data and extracts the VoIP information. In-band call signaling, as well as video and audio RTP streams of the intercepted calls are stored locally as Wiretap Data.

The prototype system supports multiple GKWDs, which can be used at each gatekeeper in the IP telephony system. In addition, multiple stand-alone ILD components, which only relay the Wiretap Information without any interception and modifications, can also be used. Likewise, the prototype system supports multiple PWD devices, which can be used to improve the performance or to provide the LI service in complex network configurations.

The system configuration presented in Figure 3 is just one of many possible deployment scenarios of the prototype LI system. The presented configuration was used to test the implemented components and to test the LI process. During functional tests, a set of VoIP clients was used. The VoIP clients were Windows based PCs running either Microsoft NetMeeting or ohPhone [6] application software. The Catalyst 2950 switch was used to connect the VoIP clients and the prototype LI system to the Ethernet based LAN. A range of H.323 parameters have been used in the tests and the prototype LI system has successfully intercepted all calls. The similar configuration will be used in the performance tests, which are planned as future work.

V. Conclusion

This paper proposes distributed system architecture for lawful interception in VoIP networks. The proposed architecture provides major benefits for LI systems. It supports heterogeneous IP telephony protocols and interception methods. Distributed system architecture ensures the scalability and adaptability to various network configurations. Finally, the hierarchical organization simplifies the system management and data collection.

The implemented prototype system provides the base for all future research and development efforts. Although the prototype system implements only a portion of the proposed capabilities, it is already fully functional. The current version of the prototype system can be used in any IP telephony network based on H.323 standard. Since the implemented system uses distributed architecture, it can be used in VoIP systems of various sizes and in various network configurations.

The proposed architecture will be further developed in future, in order to create a truly heterogeneous system. The implemented distributed LI system will be extended with additional interception methods. The support for SIP protocol will be added to existing components, as well as included in future components. The implemented WIEP protocol will be extended with additional attributes and security mechanisms. A Storage Device will be added to the system and the WIEP protocol will be extended to support the transmission of recorded information. A significant part of our research is the performance evaluation. The performance tests on the prototype system have already been started. The tests will be extended to include future components and to compare the performance of various interception methods.

References

[1] A. Milanović, S. Srbljić, I. Ražnjević, D. Sladden, I. Matošević, and D. Skrobo, “Methods for Lawful Interception in VoIP networks”, Submitted for Publishing at Eurocon 2003.

[2] Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279.

[3] Internet Engineering Steering Group, Internet Architecture Board, “IETF Policy on Wiretapping”, RFC 2804, Internet Engineering Task Force, May 2000.

[4] International Telecommunication Union, “Packet-Based Multimedia Communication Systems” Recommendation H.323, Telecommunication Standardization Sector of ITU, Geneva, Switzerland, November 2000.

[5] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, “SIP: session initiation protocol,” RFC 2543, Internet Engineering Task Force, March 1999.

[6] OpenH.323 Project, www.openh323.org, 1998-2003.

[7] OpenH.323 Gatekeeper – The GNU Gatekeeper, www.gnugk.org, 2002/2003.