

Methods for Lawful Interception in IP Telephony Networks Based on H.323

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

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

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

Abstract – Emergence of IP telephony applications in recent years has opened numerous technical and legal problems. A particular problem in implementing IP telephony services is complying with legal requirements imposed on telephony service providers in many countries. Certain legal requirements are easy to fulfill in the conventional public circuit-switched telephone network, but present significant problems in IP telephony. One of these requirements is the possibility of electronic surveillance by authorized law enforcement agencies, i.e. wiretap service. Currently, there is no standard solution for call interception in IP telephony networks.

We describe four proposed basic methods for implementing a call interception system in IP telephony networks based on the ITU-T H.323 standard. The proposed methods are Wiretap on Gateway, Wiretap Routing on the Gatekeeper, Fixed Route Wiretap, and Promiscuous Wiretap. We examine each of these four methods and show their basic advantages and disadvantages.

Index Terms – IP telephony, Voice over IP, VoIP, Lawful Interception, Electronic Surveillance, Wiretap, CALEA

I. INTRODUCTION

An important legal requirement imposed on telephone service providers in most countries is the possibility of lawful call interception [1]. The telephone service provider is required to provide the authorized law enforcement agencies with contents of telephone calls conducted by each user designated for surveillance. Because the call interception must not violate the privacy of other users, only the contents of calls designated for surveillance may be recorded. The users under surveillance must not be able to detect the call interception.

In the public switched telephone network (PSTN), all calls involving a single network access point pass through the same physical route to the local switching station. Thus, a single permanent physical channel carries both directions of the voice stream and signaling messages of all calls, for their entire duration. Therefore, providing the call interception service is not problematic. With authorization from the

telephone service provider, call interception can be performed at the local switching station. As the details of network functioning are completely hidden from the user, it is impossible to detect the interception.

In the IP telephony, calls are carried over an IP-based packet-switched network. In a packet-switched network, there is no permanent path assigned to each user that would resemble the fixed route to the local switching station in the PSTN. Each data packet transmitted over the network may be routed to the destination over various routes that overlap only partially or not at all. Individual data packets representing fractions of media streams and signaling belonging to a single call may take different, unpredictable paths to the destination.

In IP networks that support quality of service, the situation is somewhat different, but it is still impossible to locate and utilize a fixed access point for call interception. For each media stream, a fixed route with guaranteed quality of service is established using the Resource Reservation Protocol (RSVP) [2]. However, paths allocated for media streams in opposite directions may be different. During the call, path teardown and reestablishment over a different route may occur. The variable signaling path presents additional problems. Messages of various IP telephony signaling protocols [3], [4] may take arbitrary, unpredictable routes, regardless of the fixed route allocated for the media stream.

Another difference between IP telephony and the PSTN is the user's insight into details of network functioning. By examining the functionality of the underlying network layer, an IP telephony user may be able to draw conclusions about the media and signaling path and detect the interception.

An important feature of IP telephony is the user mobility. Each user is identified by one or more alias addresses. The alias addresses are usually in form of telephone numbers or textual names. The location service enables the user to be available by the alias address on various locations with different IP addresses. The wiretap service must be able to register users for surveillance both by alias addresses and by IP addresses. Calls conducted by users registered by their alias addresses must be intercepted, regardless of their current location and IP address.

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.

In this paper, we describe four methods for implementing a call interception service in IP telephony networks based on the ITU-T H.323 standard [4]. Section II describes the *Wiretap on Gateway* method, Section III describes the *Wiretap Routing on Gatekeeper* method, Section IV describes the *Fixed Route Wiretap* method and Section V describes the *Promiscuous Wiretap* method. A short comparison of these methods as well as future work is presented in Section VI.

II. WIRETAP ON GATEWAY

Wiretap on Gateway can be used with calls that utilize internetworking between an H.323-based IP telephony network and the PSTN. The gateways are H.323 network components that are physically connected to both the H.323 network and the PSTN. They perform translation of H.323 signaling messages and voice streams to the signaling protocol and voice format used on the PSTN and vice versa.

The internetworking gateways can be identified as fixed points of call routing suitable for call interception. Any call that utilizes internetworking between the H.323 network and the PSTN must pass through a gateway. The gateway has access to the entire signaling and voice content of the call. Each gateway is modified to examine the signaling of each call and to determine if the call participant on the H.323 network side is designated for surveillance. If the call interception is required, the gateway can duplicate the signaling messages and voice stream, and record them to a storage device. This process is shown in Figure 1.

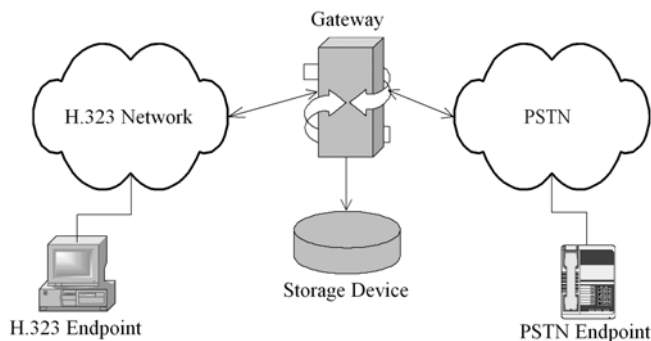


Fig. 1. Wiretap on gateway

Wiretap on Gateway is not limited to H.323 and PSTN networks. Regardless of the signaling protocol used, internetworking between any two telephony networks always includes the gateways as separate physical devices that present fixed points of routing for both media and signaling.

In order to be able to recognize calls that must be intercepted, the gateway must maintain a list of endpoints that have been designated for surveillance. The entries in that list must be matched to the participants of calls on the H.323 network side. We assume that surveillance of users on the PSTN side is handled by the wiretap service on the PSTN. If the caller endpoint is on the H.323 network side, its alias

addresses and the IP address can be extracted from the Q.913 Setup message. If the called endpoint is on the H.323 network side, its telephone number can be extracted from the signaling received on the PSTN side, and the IP address is obtained from the gatekeeper during H.323 call setup. Therefore, users can be registered for surveillance on the gateway by their IP addresses or telephone numbers by which they are accessible from the PSTN.

This method does not require installation of any additional components in the H.323 network. It does not require modification of any existing network components except the gateway. However, major modifications of the gateway are required. This can present a problem for IP telephony providers that use gateways implemented in hardware or third-party proprietary software and are thus unable to implement these modifications.

Wiretap on Gateway does not alter the paths and contents of voice and signaling in intercepted calls. Therefore, this call interception method is not prone to detection. It also does not introduce any additional delay in the call setup procedure and does not increase the latency in transport of the voice stream. It does not affect the quality of service in any way.

The main disadvantage of this method is that it does not provide a universal solution for the call interception problem. It does not enable interception of calls that occur within the H.323 network and do not pass through gateways.

III. WIRETAP ROUTING ON GATEKEEPER

Wiretap Routing on Gatekeeper method is applicable to gatekeeper operated H.323 networks [4]. The wiretap device is added to the H.323 network as a logically separate component. A single wiretap device is assigned to each H.323 zone. The calls conducted by parties under surveillance are selectively routed through the wiretap device by modifying the H.323 call setup procedure. The wiretap device then splits each received call into a pair of calls. One call is established between the caller and the wiretap device, and another between the wiretap device and the callee. All signaling messages and voice streams are forwarded from one call participant to another by the wiretap device.

We assume that each endpoint is required to register with its zone gatekeeper and invoke the address translation service at each call initiation. These assumptions normally hold in H.323-based IP telephony networks. The users are expected to be known to each other solely by their alias addresses, which are usually in form of telephone numbers or alias names.

H.225 Registration, Admission and Status (RAS) messages are exchanged between an endpoint and the gatekeeper. H.225 Q.931 call signaling messages [5] and H.245 call control messages [6] are either exchanged directly between endpoints or routed from one endpoint to another over the gatekeeper. The voice streams are directly transmitted between endpoints.

In explanation of this method, we assume that the network is comprised of a single zone. We also assume that direct call signaling is used between endpoints and that the Fast Connect or H.245 tunneling procedures are not used.

Under these premises, the call setup begins as shown in Figure 2. The caller sends an Admission Request (ARQ) message to the gatekeeper (1). The ARQ message body includes the alias address of the callee. The gatekeeper maintains the registration table, which maps alias addresses of registered endpoints to their call signaling IP addresses. If the admissions control policy allows the call, the gatekeeper replies to the caller with an Admission Confirm (ACF) message (2). The ACF message body includes the call signaling IP address of the callee. The caller reads the call signaling IP address of the callee from the ACF message and opens the call signaling channel by establishing direct TCP connection with the callee. The Q.931 Setup/Call Proceeding message exchange follows over the established call-signaling channel (3, 4). Endpoint B then requests admission through an ARQ/ACF message exchange with the gatekeeper (5, 6), and replies with a Q.931 Alerting message to indicate that the called party is being alerted. The rest of the call setup is not shown in Figure 2. It consists of the Q.931 Connect message from endpoint B to A, opening of the H.245 call control channel and exchange of H.245 call control messages, which handle endpoint capability exchange and opening of the logical channels for RTP voice streams.

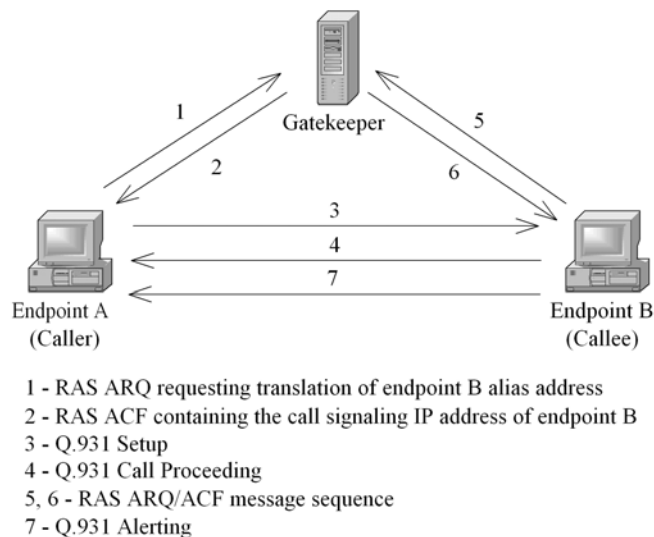


Fig. 2. Initial phase of H.323 call setup

Initial phase of call setup that includes call interception by Wiretap Routing on the Gatekeeper is shown in Figure 3. The gatekeeper is modified to examine each ARQ message that initiates a call (1) and determine if the caller or the callee is designated for surveillance. If at least one of the of the parties is designated for surveillance, the gatekeeper sends an information message to the wiretap device (2), informing it that a call between endpoints A and B is being established and must be intercepted. The information message sent to the

wiretap device includes the IP addresses of both endpoints. The gatekeeper then replies to the ARQ message from the caller with an ACF message that contains the IP address of the wiretap device instead of the callee (3). Because of the modification of the ACF message, the call signaling channel will be opened between the caller and the wiretap device. Simultaneously, the wiretap device opens the call-signaling channel with the callee.

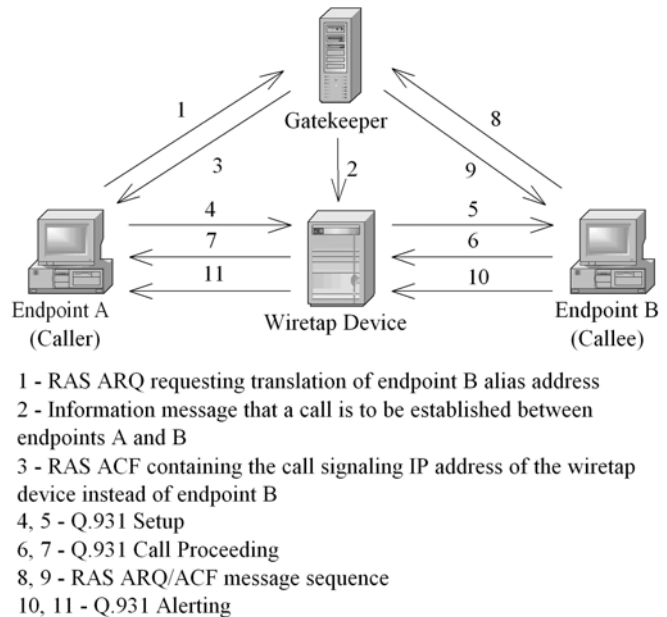


Fig. 3. Initial phase of H.323 call setup with Wiretap Routing on the Gatekeeper

The wiretap device forwards all call signaling messages from each call participant to the other one (4–7, 10, 11). Thus, each endpoint sees a normal call setup, with another participant having the call signaling IP address of the wiretap device. The H.245 call control channels are opened in similar manner. One call control channel is opened between the caller and the wiretap device, and another between the wiretap device and the callee. The wiretap device forwards all call control messages from one call participant to another. Finally, each endpoint transmits its outgoing voice RTP stream to the wiretap machine, which forwards it to the other endpoint. As all signaling messages and the whole voice stream pass through the wiretap device, it is possible to record the entire call content to the local storage of the wiretap device.

Though some assumptions were made in order to simplify the explanation of this method, this method can also be applied to other configurations, like gatekeeper-routed call setup and control signaling. In this case, the role of the wiretap device is simpler and includes only forwarding of voice RTP streams. Gatekeeper is modified to record the necessary signaling information that is routed through it. Calls using H.245 tunneling or Fast Connect methods can also be intercepted by this method. The difference lies only in number of established channels and forwarded messages.

Similar method can be used in a network comprised of multiple zones, for intercepting calls between endpoints registered with different gatekeepers. Gatekeepers exchange information necessary for address translation via Location Request (LRQ) and Location Confirm (LCF) RAS messages. If the caller is designated for surveillance, the caller zone gatekeeper obtains the call signaling IP address of the callee via LRQ/LCF message exchange. The caller zone gatekeeper then sends the necessary information to the wiretap device of the caller zone. IP address of the wiretap device assigned to the caller zone is returned in the ACF message to the caller. If the callee is designated for surveillance, the callee zone gatekeeper performs call splitting by returning the IP address of the wiretap device assigned to the callee zone in the LCF message and informing the wiretap device of the incoming call.

As the gatekeeper simultaneously provides the address translation service and keeps the list of endpoints designated for surveillance, endpoints may be designated for surveillance by their alias addresses, IP addresses, or both.

The Wiretap Routing on Gatekeeper method does not require modification of any H.323 network components except the gatekeeper. The address translation service must be modified to selectively include the IP address of the wiretap machine into the ACF messages. The admissions control service must be modified to include a message exchange with the wiretap device before issuing the ACF message at each call initiation. The wiretap device is not complex and can be built using the same H.323 protocol stack implementation used for other network components.

If each user is only aware of alias addresses of other users, it is not possible to detect any distinguishable feature of the intercepted calls. From the point of view of both the caller and the callee, the only difference between normal and intercepted calls is the call signaling IP address of the other call participant. However, each user may be able to find out the IP address of the other call participant during the call. For example, the user may obtain it by directly asking the other call participant. By comparing this IP address to the IP address of the device to which the connections and logical channels of the current call are established, the user is able to determine if the call is being intercepted.

Another problem of this method is the degradation of the quality of service. The message exchange during the setup of intercepted calls is significantly more complex, and the call setup takes a longer time to complete. Routing of voice streams through the wiretap machine may significantly prolong the route that the RTP packets carrying voice take from one endpoint to another. This leads to increased packet loss, jitter, and especially transport latency.

The major advantage of this method is that it enables reliable interception of all calls in a gatekeeper operated H.323 network. However, call interception by this method is prone to detection by an expert user and therefore does not comply with all legal requirements.

IV. FIXED ROUTE WIRETAP

Call interception by Wiretap Routing on the Gatekeeper selectively splits calls conducted by endpoints designated for surveillance in order to establish a fixed point of routing. However, call splitting can be detected by users and serves as an indication that the call is being intercepted. A possible solution to the detection problem is splitting all calls in the H.323 network and selectively recording those conducted by parties designated for surveillance. The wiretap device, similar to that used for Wiretap Routing on the Gatekeeper, is added as a logically separate component to the H.323 network.

This method uses the same call splitting technique as the Wiretap Routing on the Gatekeeper. However, the gatekeeper does not examine the Admission Request messages initiating each call to determine if the call should be rerouted. Instead, the call routing through the wiretap device is applied to all calls. Every call that occurs in the H.323 network is routed by the gatekeeper to the wiretap device. The wiretap device splits each call into two calls – one between the caller and the wiretap device, and another between the wiretap device and the callee. Call setup procedure is similar to that shown in Figure 3. The message sent from the gatekeeper to the wiretap device at the start of each call includes not only the addresses of call participants, but also a flag that indicates whether the call content should be recorded. This is necessary because the wiretap device is not supposed to intercept all calls that are routed through it.

In order to use this method, it is necessary to add the wiretap device as a new logical device to the H.323 network. It is also necessary to introduce the gatekeeper modifications similar to those described in Section III.

Call interception system based on this method complies with all legal requirements. It enables interception of all calls conducted by any endpoint in the network, and the call interception is not prone to detection.

A significant problem of this method is the load imposed on the wiretap device. The wiretap device must be able to route both the signaling messages and the RTP voice streams of all calls that occur in the entire H.323 network. This raises the problem of scalability, which can be solved by implementing the wiretap device as a distributed system of separate physical devices. For this purpose, a special information exchange protocol must be developed to supply gatekeepers with information necessary to determine the proper device for routing each individual call.

Another problem is the degradation of quality of service, similar to that described in Section III. This degradation affects all calls in the IP telephony network in which a call interception system based on this method is implemented.

V. PROMISCUOUS WIRETAP

Methods for call interception described in Sections II–IV are based on modifying the H.323 network components that operate at the application layer, or introducing new ones. An

alternative approach is to implement a device that operates in promiscuous mode and monitors the entire network traffic. The device extracts media streams and signaling messages transmitted or received by parties under surveillance.

The Promiscuous Wiretap Device is connected to the local area network switch or hub. The switch must be configured to forward the entire data traffic from all ports to the monitoring port to which the wiretap device is connected. The wiretap device implements the H.323 protocol stack and is able to extract H.225 call signaling and H.245 control signaling messages, as well as RTP voice streams from the received data. By extracting the call signaling and control messages, the wiretap device recognizes the setup and termination of each call. By extracting the RTP packets transmitted by the endpoints during the call, the wiretap device assembles the voice content of the call. Therefore, the wiretap device is able to maintain call record with the entire signaling and voice contents of each call taking place on the H.323 network. The wiretap device can be implemented in hardware or in software, on a general-purpose computer with network card configured to work in promiscuous mode.

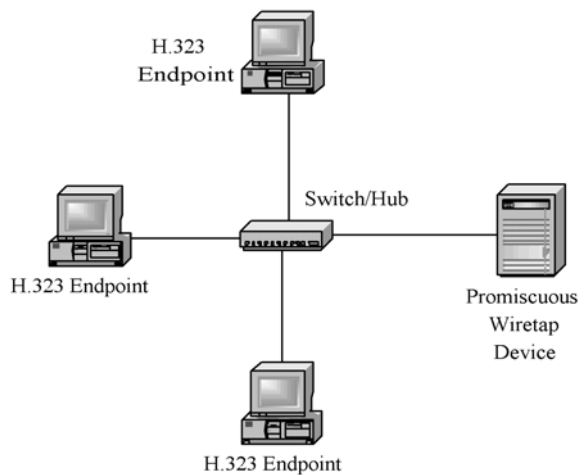


Fig. 4. Promiscuous Wiretap Device

This call interception method can be extended to work on IP telephony networks based on any other signaling standard. It is only necessary to extend the wiretap device to support extraction of additional signaling protocols and voice encoding formats.

The wiretap device must maintain a list of endpoints designated for surveillance and match the endpoint information extracted from signaling messages of each call with entries from that list. From the call signaling, it is possible to extract the IP addresses of both call participants and the alias addresses of the caller. Alias addresses of the callee cannot be extracted from the call signaling. Therefore, the list of endpoints designated for surveillance must contain their IP addresses. It is necessary to implement an additional network component that has access to the address translation service and supplies the wiretap device with this information.

One possible solution is to modify the gatekeeper to maintain a list of endpoints designated for surveillance and send periodic messages that contain lists of their IP addresses to the wiretap device.

Call interception by the Promiscuous Wiretap Device does not alter either the paths or the contents of voice and signaling in intercepted calls. Therefore, it is not possible for the parties under surveillance to detect the call interception. This method does not affect the quality of service.

The Promiscuous Wiretap Device enables interception of all calls in the H.323 network, within limits imposed by performance of the network switch and processing power of the wiretap device. A significant problem is the ability of the wiretap device to monitor the entire traffic in high-speed networks. For example, if the wiretap device is implemented in software on a contemporary personal computer, it is not possible to effectively monitor the traffic in a 100Mb/s LAN. The performance of the network switch can also present a problem. At high levels of network load, it may be impossible for the switch to forward the entire traffic to a single port.

VI. CONCLUSION

In this paper, we have described four methods for call interception in H.323-based IP telephony networks. Wiretap on Gateway enables undetectable interception of all calls that utilize internetworking between H.323 network and the PSTN, but does not enable interception of calls taking place within the H.323 network. Wiretap Routing on the Gatekeeper enables interception of all calls in the H.323 network, but degrades quality of service for intercepted calls and can be detected by an expert user. Fixed Route Wiretap enables undetectable interception of all calls in the H.323 network. However, it degrades quality of service for all calls in the H.323 network and raises scalability problems. Promiscuous Wiretap enables undetectable call interception, but only within limits imposed by performance of the wiretap device and the network switch, which may be problematic at high levels of network load.

Future work will include implementing a call interception system based on methods described in this paper and performance measurements.

REFERENCES

- [1] "Communications Assistance for Law Enforcement Act of 1994" (CALEA), Pub. L. No. 103-414, 108 Stat. 4279, Congress of the United States of America
- [2] R. Braden et al., "Resource Reservation Protocol (RSVP)", RFC 2205, Internet Engineering Task Force, September 1997
- [3] J. Rosenberg et al., "SIP: Session Initiation Protocol", RFC 3261, Internet Engineering Task Force, June 2002
- [4] ITU-T Recommendation H.323, "Packet-Based Multimedia Communications Systems", International Telecommunication Union, November 2000
- [5] ITU-T Recommendation H.225.0, "Call Signaling Protocols And Media Stream Packetization For Packet-Based Multimedia Communication Systems", International Telecommunication Union, November 2000
- [6] ITU-T Recommendation H.245, "Control Protocol For Multimedia Communication", International Telecommunication Union, July 2001