Monitoring Architecture for Lawful Interception in VoIP Networks

Balamurugan Karpagavinayagam, Radu State, Olivier Festor

Monitoring Architecture for Lawful Interception in VoIP Networks

Balamurugan Karpagavinayagam, Radu State, Olivier Festor
MADYNES Team
LORIA-INRIA Lorraine
Villers-lès-Nancy, France
{balamurugan.karpagavinayagam, radu.state, olivier.festor}@loria.fr

***Abstract*—Lawful Interception is one of the main provisions needed for the security agencies to monitor a suspect or deal with criminal activities. The implementation of this was easy in the traditional telephone networks, because of its centralized administration. However this has become a tedious job with the emergence of VoIP technologies where voice traffic is carried over IP. In this paper, we discuss the challenges and propose a monitoring architecture for Lawful Interception on VoIP networks based on SIP. We also explain how this can be achieved from the existing protocols and solutions like NETCONF and RBAC model. Finally, we present our prototype implementation of the Lawful Interception, the limitations and the difficulties that we found.**

Keywords-lawful interception, NETCONF, RBAC, forensic

I. INTRODUCTION

Lawful Interception (LI) is a service that is legally authorized for monitoring or recording telephone calls in accordance with a court order or authorization of legal bodies. It is mainly used by the security agencies like police, Law Enforcement Agencies (LEA) to deal with criminal activities. Thus service providers are obliged to comply with the Lawful Interception standards to provision this service to the LEA. This service is well implemented in the PSTN networks due to its centralized network architecture, where the entire signaling and voice traffic pass through a centralized location. The recent advancement in the technologies like Voice over Internet Protocol (VoIP) has made the LI for the LEA a more challenging issue because of the diverse use of protocols.

In VoIP networks the voice traffic are carried over IP. Unlike the traditional telephone networks which are circuit switched and have a fixed path for the phone calls, the VoIP networks are packet switched and do not have a fixed path for the calls. This is the major difference which makes the interception of the calls difficult in VoIP networks and still tends to be a challenging issue for the research community. Some of the challenges for LI in VoIP networks are discussed below.

A. Challenges in LI

Before we look into the challenges we should know that there some requirements like confidentiality, security, etc., that are to be accomplished for LI. These requirements are discussed in [1, 2]. Also the various issues dealing with LI in IP networks have been addressed in [1, 3]. Apart from this, the technological challenges in VoIP networks pose a major difficulty for LI. Some of them are

- Signal and data messages travel in different paths
- Users can be anywhere in the internet
- Use of Multiple protocols from different standard bodies
- Use of Security Mechanisms at various protocol levels
- Convergence of diverse technologies (fibre optics, ADSL, etc.,)

One another solemn issue on the Intercept target that was addressed in [4] is that if the target lies in another service provider network, then the monitoring of RTP packets could not be done. This is because of the lack of information about the user to the gateway where the target is located and also because these networks would be physically located in different locations.

To fulfill all the requirements and issues related to lawful interception is a quite difficult task with prevailing heterogeneous technologies. Therefore, we only address some of the issues which we consider to be important and how the use of certain new technologies can be helpful to perform LI. We also propose an architectural model which is slightly different from the existing standards for the LI. This model however has some advantages and also disadvantages over the present LI models which are discussed in the paper.

In this paper, we discuss and present the architecture that we propose for Lawful Interception in VoIP networks based on Session Initiation Protocol (SIP) [5]. The paper is organized as follows: we discuss the Monitoring Architecture in the section II, followed by the configuration setup needed for the LI in section III. In section IV, we explain our Prototype implementation for LI and filter policies needed for LI in VoIP networks. In section V we discuss some of the limitations and threat models for this approach. Finally we discuss the related woks in section VI and conclude the paper with future works in section VII.

II. MONITORING ARCHITECTURE

In the monitoring architecture that we propose in this paper, we consider that the target (user), to be monitored or intercepted is mobile and can connect from anywhere in the internet. This is a scenario in which the monitoring requires to be done at various locations and cannot be done from one place. But monitoring in various locations is not a practically possible solution, unless the locations come in the same country or LI authorization. Also in this case, using the IP address [4] or MAC address [6] to do the monitoring is not feasible solution as well. In the design phase of the monitoring, we also considered a more realistic scenario in which the target can receive or make calls to other users which are from different VoIP service providers. The proposed solution however is suitable for other architectural model in which the targets are might be in the same network. This is rather a simple scenario where both the signaling and data traffic travel in the same network.

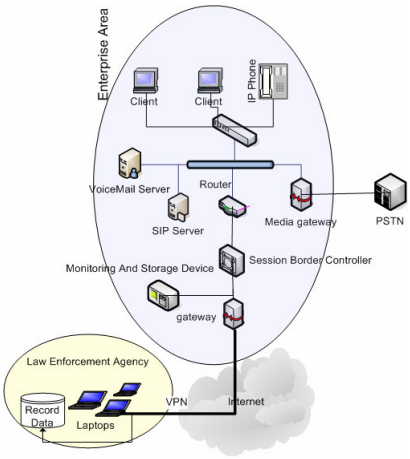

Figure 1. Typical VoIP service Provider Network

The first step in Lawful interception is to find the right intercepting point for the target. This was easy in the regular telecommunication networks due to centralized management. Whereas, identifying the intercepting points in the IP network is difficult because the IP packets travel in dissimilar path and the presence of diversified internet technologies. Determining intercepting points according to different technologies has been discussed in [7, 8 and 9]. On the contrary, our architecture we only consider the VoIP service provider's network to be the right place for interception. Here the term, VoIP Service provider means that it can be an Internet Service Provider (ISP) that provides VoIP Services or it can just be a VoIP Service provider.

In our model we mainly concentrate on collecting all the interception data from the service provider's network. This can be achieved with some modifications at the protocol level. The architecture to perform the LI is detailed in the following subsection.

A. Architecture Model

In our LI architectural model, we focus on the SIP based VoIP providers for the interception. But can also be extended to technologies like H.323 [8]. An example of conventional network architecture of a VoIP service provider that we consider is shown in Fig.1. We consider the VoIP services provider's site as the right location for interception, because this is where we can get the needed information on the target, like the user IP address, location, etc. The architectural model that we propose is composed of two parts:

- Entities related to the Service providers and
- Entities related to the LEA

In the fig.2, we explain the different entities and their functions that are used in our LI model.

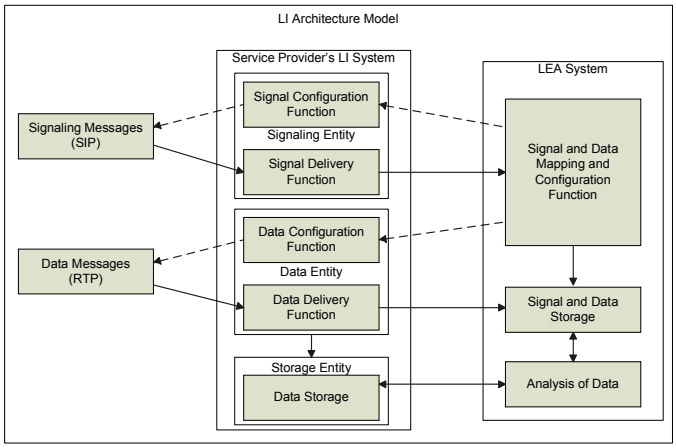

Figure 2. Lawful Interception Architecture

1) Entities related to the Service providers

There are three major entities in the Service provider's network. The first, being the *Signaling Entity*, where we do the configuration to get the target information (location, IP address, etc.,). These are the devices on the service provider's site that the LEA will need access to configure for intercepting calls of the target entity. In our scenario, we consider only the SIP Server and Voicemail server as shown in the fig.1 to be the devices to be configured for LI. But this could vary according to the services to be monitored and depending on the information required for LEA. The configuration and operations of these devices are:

- Collecting User Information
- Monitoring
- Provide the key in case of encryption
- Send the collected Information to the LEA

Once we have done the configuration and started intercepting, the information gathered will be transmitted to the LEA system for storage and mapping the configuration details for the RTP session.

The second part is the *Data Entity*. These are the devices that are to be configured to collect the voice or RTP traffic. It can be a gateway, media gateway or a separate monitoring device attached to these components. The configuration of these devices is not previously determined but is dynamically received or pushed from the LEA system from the information

provided by the Signaling *Entity*. This is due to the fact that, we do not know the exact IP address and port number of the target to be intercepted before hand. This information can only be received when a call is made. The main functions of these devices are

- Monitoring
- Provide the key in case of encryption
- Send the collected Information to the LEA

The third Entity on the service provider's network will be the *Storage Entity*. This may or may not be attached to the Data *Entity*. The main functions of these devices are:

- Storage of collected data (only Voice)
- Send the collected Information to the LEA system for analysis

2) Entities related to the LEA

The monitoring and storage devices that are used in the LEA location come under this category. In some cases, the LEA might also put some monitoring and storage devices in the operator's network, which might be under direct control of the LEA. These devices also fall in the category. The main functions of the LEA system are:

- Push configuration to both the Signaling and Data Entity
- Mapping of the received Data (Signaling, RTP, key, etc.,)
- Storage and analysis of the Collected Data

In our model, we consider that the LEA would place a monitoring device in the service provider's location to collect the RTP information of the target. Depending on the necessity or preference, this might be accompanied by a storage device as well. In our case, we consider to have the monitoring device with storage facility. The advantages of this will be discussed in the following sections.

B. Connection Method

In the Architectural model description we have described the various entities and functions that are needed for LI. The second important factor that we need to consider is how these configurations are going to be done and how the interception of the traffic is to be collected. As Lawful Interception is a mission critical application and concerns also the security of the enterprise, these applications should not be compromised in anyway. Thus we need a secure way of handling LI. Therefore we consider the Virtual Private Network (VPN) connection to be a better choice for connecting to the enterprise network in a secure mode. We deliberate that all the configuration exchange and collection of data is done through VPN.

C. Collection and Storage

Collection and storage is one of the foremost factors that are to be well organized for LI and forensic purpose, because even a little loss of information or improper storage will become a waste. Since the interception of the VoIP calls involves traffic collection from various devices like the SIP messages, RTP messages, these messages should be reorganized to have a clear data.

TABLE I. DATA COLLECTION INFORMATION

Data collection	**Protocols**	
	SIP Messages	***RTP Session***
Header	From: User I.D, IP address, To : User I.D, IP address	Session Start : IP Session End : IP
Messages	Via, Refer, SIP Info (for DTMF)	Call Duration, Call length

One important factor in the storage phase will be, "What interception data are to be stored?" This way we can avoid unwanted data and store only the needed data. According to our model, we collect both the SIP and RTP packets. The messages that we collect are detailed in Table.I but are not limited. In the Fig.3, we explain the use case of the Interception process and also the dependencies.

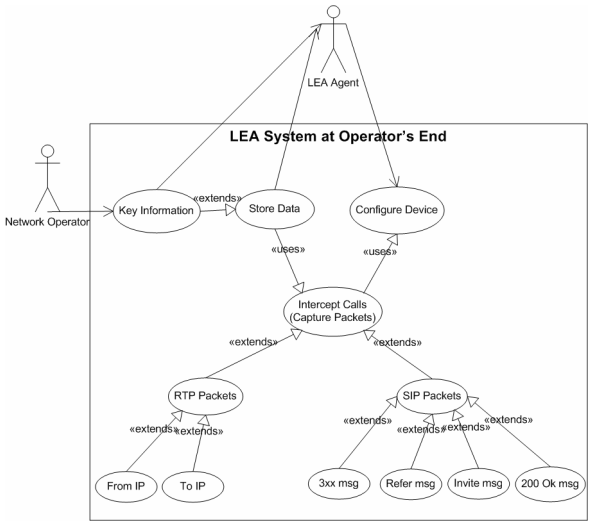

Figure 3. Use case of call Interception

We strongly recommend having the storage facility in two places, both in the service provider and LEA site. The reason behind this is twofold:

- We can have the intercepted information for sure, even in case of failure and
- For forensic purpose i.e., for the proof of originality of the data. This can be achieved by signing the stored data eventually in both places by the service provider and the LEA.

III. CONFIGURATION SETUP

In the previous section we have discussed about the architectural model and the components that are to be configured for performing lawful interception. The next step would be how these configurations could be done in a secure way. In this section we briefly discuss how some of the existing technologies could be employed in the configuration setup for

LI. The key components that we consider in the Lawful interception configuration are as follows:

A. *Management Protocol (Netconf)*

NETCONF [9] is a XML based network management protocol which can be used to install, delete, or modify the configuration of the devices. We consider the use of this protocol because of its diversified advantages. The first one is that we can configure the devices from a remote location in a secure manner. This gives the privilege for LEA to do the configuration of the devices from its locations. Also, as this protocol is based on XML, this provides an easy method to push configuration files in a human understandable form. This approach is mainly beneficial in the case where we have many administrators for the same device.

B. *RBAC (Role-Based Access Control) [10]*

The Netconf protocol provides security in the configuration at the transportation level but however this is not sufficient for the privacy of the configuration data. One of the main goals in the LI is that neither the target nor the operator should know who is monitored. Therefore we use the RBAC approach that we proposed in [11] to enable privacy for the configuration data. The main advantage of the RBAC policy is that we could specify which of the data can be accessed by the users. The RBAC model is based on roles rather than based on the user. This is mainly useful, because when the LEA push some configuration on the devices this could be noticed by network administrator or any other persons, who has rights to access the configuration data. Therefore the use of the RBAC model could provide more security and privacy to the configuration data to avoid such situations.

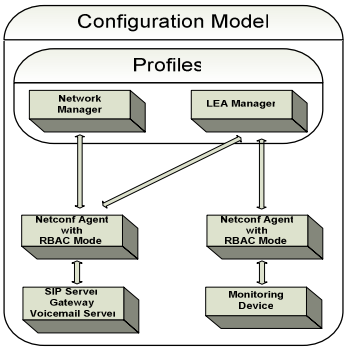

Figure 4. Configuration Model

Taking into consideration the benefits of RBAC, we define the characteristics that are needed, to have a better model for LI, which is shown in Fig.4. There are certain specifications that are desired in the design of the profiles that have access to the configuration data in the devices. Let us consider that we have a top level user called the "Network Manager" in the enterprise which has access to the configuration data. There might also be some other network user who may come under the Network manager hierarchy, but supposed to be less privileged to the Network Manager. We consider these profiles to be in the Network Manager category. We use the Mandatory Access Control Model [12], to define the user profiles and the Network manager is the one in charge of the creating the profiles.

We introduce a new profile called "LEA Manager" which has some unique properties compared to the Network Manager group. The properties that we consider to be imperative for a LEA Manager are:

- Can be created by the Network Manager (But not deleted). Deletion is done on the acceptance of both the Network Manager and LEA Manager. This is where the Mandatory access control is useful.
- Configuration data pushed by the LEA Manager has high priority over other configuration data.
- Configuration data pushed by one LEA Manager should not be viewed by the other LEA Manager. We need this because the network manager has the right to create LEA Manager, and so creating another LEA manager to access the LEA configuration is possible.
- The LEA Manager can authorize access to the configuration for other LEA managers and network Managers in case of necessity.

IV. PROTOTYPE IMPLEMENTATION

In this section, we detail our early prototype implementation. The prototype implementation is based on our network management tool Ensuite [11], which uses Netconf and RBAC for the configuration of the network devices. This tool is generally utilized only for the configuration of the network devices. We now extend this tool with other implementations that can be used for LI. The various integrations are:

- ***Packet Sniffing Module:*** Integration of the packet sniffing tool Scapy [13] for the RTP collection, which will be used in the Monitoring device deployed by LEA in the service provider's site. Also, this is used by the LEA to decode the packets.
- ***SDP Changer Module:*** A Session Description Protocol (SDP) Changer module is integrated in the SIP Server. This is done to modify the SDP Messages to redirect the RTP packets through our service providers gateway where the Monitoring device will sniff the RTP packets
- ***RTP Mediator Module:*** This is the module that is implemented at the Gateway. This module acts as a Man in the Middle for relying of the packets to the respective targets. It is directly integrated with the gateway configuration module but controlled by the Netconf agent and RBAC model.

Fig.4 illustrates the deployment of the Netconf management plane in various devices in the service provider's network, where the LI is to be done. The deployment of different RBAC profiles discussed in previous section is also shown in Fig.5 for each device.

In the above integration modules, the configuration of the SIP Server with the SDP changer module could be a security

breach to the service provider. However this could be overcome, by the integration of the SDP changer module with the Netconf agent and not with the SIP Server directly. There are still some tests going on this. To be more precise, the SDP changer is accessible only through the policies from the Netconf agent. Until now we have explained about the configuration of the devices using our prototype model. The functional part of the tool will be the pushing of policies or configuration to these devices. This is explained in the following subsection.

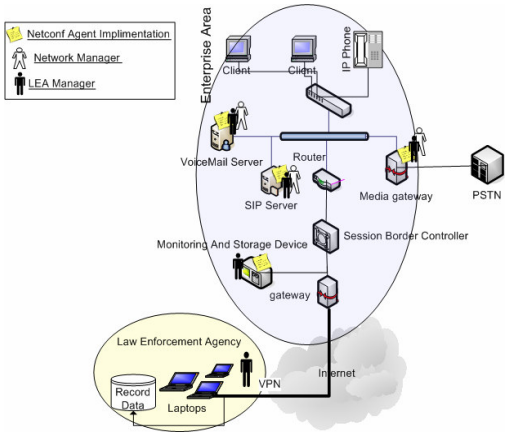

Figure 5. Implemention of the Prototype

A. *Filter Policies*

Filter policies are the configuration data that are to be pushed by LEA Managers for intercepting VoIP calls. These configuration data vary according to the deployed devices in the network. In our architectural model to intercept a VoIP call we consider a basic model in which we configure the SIP server, Monitoring device, Gateway and Voicemail server. Fig.6, illustrates a sample data model of the filter policy. This is generalized according to call interception. This filter policy involves the SIP server and monitoring device.

The Filter policy is the core engine for the Lawful Interception. The behavior of the filter policy has two main functions PolicyPacketHandler (PPH) and PolicyAction (PA). The PPH has the information related to the packets or configuration and the PA does the actions that are to be applied to the PPH information.

In our model the filter policies are manually applied at the SIP server and Voicemail Server first with the LI target's information like User Identity (ID). We explain the working of the filter policy with a simple example. Suppose *Alice* is the LI target. We first manually push the *Alice's* information like the User ID or IP address (if available) to the Configuration Handler in the devices through the Netconf Agent. Now as we have pushed the configuration for monitoring the target, whenever the *Alice* registers or has a call (from or to), the PolicyBehavior is applied, which is shown in Fig.6. Thus, in this way, the LEA system gets to know about *Alice* present location, IP address etc., and also maps this information for monitoring RTP packets. And this information pushed to the monitoring device.

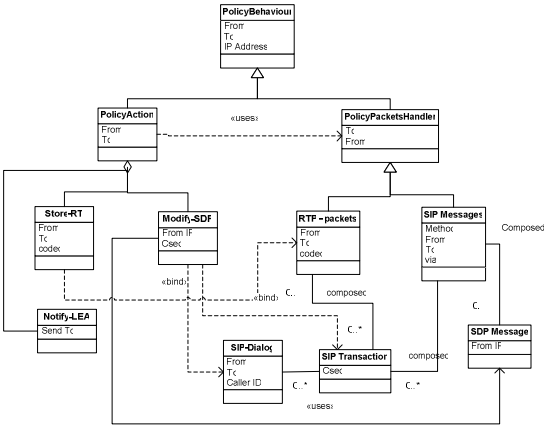

Figure 6. Data Model of Filer Policy

Presently, implementation of the monitoring device lies in the same subnetwork as the gateway, thus enabling monitoring the data that passes through the gateway. We use this model because we do not want to overload the gateway. However this could also be implemented in the gateway by establishing a VPN to send the captured packets to the LEA, but this might affect the QoS. Thus in this way we have both the signaling and data traffic of the *Alice*.

V. LIMITATIONS

There are various problems that we have come across during the designing phase. These are still to be addressed. Some of them are:

- *Standard for Originality:* We do not find specific standards for the storage of data (captured data) which provides proof of originality. We consider that the use of hash codes could solve the problem to an extent.
- *Use delayed RTP Packets***:** The RTP packets that are being captured might have lost some packets due to latency, which may be crucial in case of criminal evolution. So, we prefer that the monitoring devices should be also able to capture these packets and integrate with the mainstream. So there is a strong need for the use delayed RTP packets.

Apart from this the different threat models that we find in this architecture are:

- The monitoring device could be a main target for the malicious users, to know the information related to LI targets
- The SIP server might become a preferred target for the attackers, to gain access over the servers
- The hackers might try to exploit LEA service to attack the operators and LEA
- The attackers can make fake calls to some targets, so that making the LEA to record unwanted calls or to make someone suspicious.

VI. Related Works

Lawful Interception in VoIP networks is an outstanding problem that has got serious insight by the research community recently. There are various monitoring approaches that have been proposed by the different organizations like ETSI [14] in Europe, CALEA [15] in USA and many others in different countries. The proposed models mainly consider the implementation approach where the targets traffic both signaling and data are in the same network. Moreover these approaches have a Mediation device at the service provider's site to perform the LI. This is advantageous because, the LEA can do the monitoring and collection from one device which is good only when both the signaling and data messages are in the same network. They are also good when you need to monitor all the traffic from the same network, which is of not much use for LI. But with evolution of new services based on VoIP like voicemail, messenger service, conferencing, etc., this could become a tedious and an expensive implementation for the LEA.

In [8], the authors proposed different methods of LI that are based on the H.323. Although these methods are better in some points as described by the authors, they still have some disadvantages like degradation of QoS and can be detected by the target. However these methods are specific to H.323. The same authors have also proposed a distributed system in [7] that supports various protocols. This approach is good since it has a centralized administration on the distributed platform. But when it comes to implementation, it would be more expensive due to the necessity for more devices to be configured. Though, the collection of data and analysis from various points help in acquiring all the data, this would require a better processing in correlating the collected data.

In [1, 16, and 17], the authors propose a generalized model for the LI in IP networks. These models are mainly concentrated towards service provider's network which is good only when the target is inside the service provider's network. On the contrary if the target gets the service from another operator, the interception could only be made for the signaling messages and not for the Voice messages. One another problem in these approaches is the use of a centralized device for collecting data. This might be a problem if the target is located in the same network and if the target has the possibility to monitor the traffic passing through the monitoring device.

VII. Conclusion and Future Works

Lawful Interception is a challenging solution to be designed for the VoIP Networks, since the signaling and data packets travel in different paths. Another major issue is that the target is mobile. To overcome these problems we have proposed an architectural model based on SIP, which could enhance LI to certain extent. The main advantages of our model are

- Possibility to monitor the target located anywhere on the internet
- The target cannot notice the interception, since we modify the SDP information from INVITE and ACK messages, before relying to the targets
- Has a better way of configuration of the devices with Netconf and RBAC for configuration data security
- Provides Information for the LEA on the fly

In the future, we would extend this work with integration of other VoIP protocols like H.323 and MGCP. One another important enhancement will be the Integration of policy based management to simplify the configuration of multiple devices. Finally we would also like to extend this model for synchronization of multiple LI points and the rapidly advancing Peer-to-Peer (P2P) VoIP technologies.

References

[1] F.Baker, B.Foster, C.Sharp, "Cisco Architecture for Lawful Interception in IP networks," RFC 3294, IETF, October 2004

[2] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[3] ETSI TR 101 944: "Telecommunications security; Lawful Interception (LI); Issues on IP Interception".

[4] S.Bellovin et al., "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", ITAA, June 2006

[5] J.Rosenberg et al., "SIP: Session Initiation Protocol," RFC 3261, Internet Engineering Task Force, June 2002

[6] P. Branch, A. Pavlicic, G. Armitage, "Using MAC Addresses in the Lawful Interception of IP Traffic," Proc. Australian Telecommunications Networks & Applications Conference (ATNAC), Sydney, Australia, December 2004

[7] A.Milanovic, S.Srbljic, I.Raznjevic, D.Sladden, D.Skrobo and I.Matosevic, "Distributed System for Lawful Interception in VoIP Networks," EUROCON 2003. Computer as a Tool. The IEEE Region 8 , vol. 1, pp. 203–207, September 2003

[8] A.Milanovic, S.Srbljic, I.Raznjevic, D.Sladden, D.Skrobo and I.Matosevic, "Methods for Lawful Interception in IP Telephony Networks Based on H.323," EUROCON 2003. Computer as a Tool. The IEEE Region 8 , vol. 1, pp. 198–202, September 2003

[9] R. Enns, Ed. "NETCONF Configuration Protocol", RFC 4741, Internet Engineering Task Force, December 2006

[10] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," ACM Transactions on Information and Systems Security, vol. 4, no. 3, pp. 224–274, August 2001

[11] V.Cridlig, R.State, O.Festor, "An Integrated Security Framework for XML based Management" In Proceedings of the Ninth IFIP/IEEE International Symposium on Integrated Network Management (IM 2005), IFIP Conference Proceedings, May 2005

[12] M.Bishop, "Computer Security: Art and Science". Addison Wesley Professional, December 2002

[13] Philippe Biondi, "Scapy: Packet Maipulation Tool".

[14] ETSI TR 101 943: "Telecommunications security; Lawful Interception (LI); Concepts of Interception in a generic Network Architecture".

[15] "Communications Assistance for Law enforement Act of 1994" (CALEA), Pub.L.No.103-414, 108 Stat.4279, Congress of the United States of America.

[16] "Lawful Interception for IP Networks", White Paper, AQSACOM, November 2005

[17] N.Maloku, T.Aljaz, F.Dolenc,"Legal call interception in next generation networks", Proceedings of ConTEL 2003, Vol: 1, On page(s): 47- 50