第 34 卷 第 8 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.8 Computer Engineering April 2008
·多媒体技术及应用· 文章编号：1000—3428(2008)08—0243—03 文献标识码：A 中图分类号：TP277

基于 SIP 的合法监听

赵 凯，王永娟
(上海交通大学网络学院，上海 200030)

摘 要：针对下一代网络的特点，提出一套可用于下一代网络中的基于会话初始协议(SIP)的合法监听解决方案。该文通过分析思科提出的基于 IP 网络的合法监听架构并结合 SIP 呼叫建立流程的特点，将该架构扩展到下一代网络中。结果证明其在下一代网络中实施合法监听是可行的、安全的。

关键词：下一代网络；VoIP 技术；SIP 协议；合法监听

Lawful Interception Based on SIP

ZHAO Kai, WANG Yong-juan
(College of Network System, Shanghai Jiaotong University, Shanghai 200030)

【Abstract】 In view of the Next Generation Network(NGN)'s characteristic, this article proposes a Session Initiation Protocol(SIP)-based lawful interception solution which may be used in the next generation network. After thorough analysis of the Cisco's IP-based Lawful Interception architecture and combined with SIP call setup flow, it is introduced into the NGN. The result proves this implementation of lawful interception in NGN is feasible and safe.

【Key words】 Next Generation Network(NGN); VoIP; Session Initiation Protocol(SIP); lawful interception

近年来，随着VoIP技术的不断发展，特别是SIP[1-2]和MEGACO[3]等协议的提出和不断完善，使得NGN全面进入商用阶段。这项基于IP的技术能降低长途通信的费用，同时也带来了一些技术和法律上的问题，如目前正在研究的安全、全局管理、计费、合法监听等。目前基于IP的下一代网络的合法监听还没有标准的解决方案。本文以SIP为基础提出了一套NGN中的合法监听解决方案。

1 背景知识

1.1 VoIP 简介

Voice over IP 简单来说，就是将模拟的声音进行数字抽样打包后，通过 Internet 传送到接收方。因成本极其低廉，受到业界广泛的瞩目和推广。为了可以顺利地在 Internet 上建立通话并传送语音包，一套公认的通信协议必不可少。两大通信协议制定组织 International Telecommunication Union(ITU)和 Internet Engineering Task Force(IETF)分别都制定了适用于网络电话的 VoIP 通信协议。

1.2 SIP 协议简介

会话发起协议(Session Initial Protocol, SIP, RFC2543, RFC3261)是一套点对点(Peer to Peer)、主从式(Client/Server)的传输架构，它是 IETF 多媒体数据和控制架构的重要组成部分。SIP 最大的优点就是简单、适用性强。

SIP 是一个以基于文本的通信协议，使用 ISO10646 定义的字元，并使用 UTF-8 的方式编码，所以 SIP 的消息体看起来类似于 HTTP。与使用二进制编码相比，用文本传输需要占用更多的带宽。

SIP 作为一个主从式(Client/Server)的架构，由客户端(client)发出请求(request)，服务器端(server)接收到请求后，发送相应的响应(response)给客户端。

SIP request 消息可以分为 6 个基本类型：(1)INVITE，用来发出邀请；(2)ACK，用来确认最后的 response 已经收到；(3)BYE，用来结束通话；(4)OPTION，用来询问服务器的负载等信息；(5)CANCEL，用来取消一个 request；(6)REGISTER，由 SIP user 发出，用来注册到 SIP 代理。

SIP 基本呼叫的建立流程如图 1 所示。

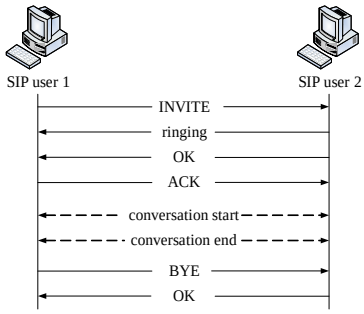

图 1 SIP 基本呼叫建立流程

1.3 思科提出的 IP 网络合法监听架构

思科提出一个可以提供IP网络合法监听的架构[4]，它可以提供基本的监听功能，在这种架构下监听可以获得 2 种资料：一是通话内容，也就是被监听者所有的通话内容都被记录下来；另一种是监听的相关信息(Intercept Related Information, IRI)，例如双方的电话号码，或者是被监听者曾经拨打过哪些电话号码。

如图 2 所示，该架构中包括的各要素：(1)LI 管理功能(LI administration function)，当有关机构得到授权，可以用这个管理功能来执行监听。(2)监听设备(Intercept Access Point, IAP)，用来执行监听动作的设备。IAP 有 2 种类型：一种负

作者简介：赵 凯(1979－)，男，硕士研究生，主研方向：VoIP；王永娟，学士

收稿日期：2007-04-23 **E-mail：**kai.a.zhao@gmail.com

责提供通话内容(Content IAP)，一种负责提供 IRI(IRI IAP)。(3)司法机构(Law Enforcement Agency, LEA)，司法机构发出监听要求给 MD，并接收监听结果。(4)调解设备(Mediation Device, MD)，MD 要求 IAP 进行监听，并收集 IAP 返回的监听结果，将这些结果转换为 LEA 要求的格式，并传送给 LEA。

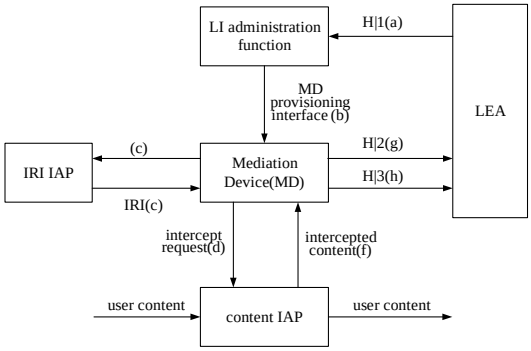

图 2　思科 IP 网络合法监听架构

思科提出的合法监听架构，大致说明了合法监听可能需要哪些设备配合，每个设备应该负责做什么事情，但是没有更详细的定义，也没有针对 VoIP 加以讨论，所以，电信运营商想要真正地加以实现，还有一定差距。

2　以 SIP 为基础的合法监听

2.1　系统简介

本文提出的系统架构结合思科提出的合法监听架构和 SIP 协议的架构，为使用 SIP 协议建立的 VoIP 通话提供合法监听的功能。本架构满足合法监听的几项基本要求：(1)监听目标不会发现自己正在被监听；(2)除了监听通话内容，还能够提供 IRI；(3)监听结果如果有加密，能够给出加密的密钥。

本架构具有安全性，并假设被监听目标发送的所有 SIP 消息一定会经过 SIP 代理服务器，而且被监听者需要认证才能够使用 VoIP 业务，也就是说被监听目标无论作为主叫还是被叫，都必须先经过认证，这个假设也符合电信运营商的运营目的。

2.2　系统架构

图 3 是 SIP 合法监听的网络示意图，它参考了思科的合法监听架构和 SIP 协议架构，其中有 7 种网元，分别负责不同的功能。在这个架构之下，能使 SIP 提供合法监听的功能，而且不会改变原本 SIP 的架构。

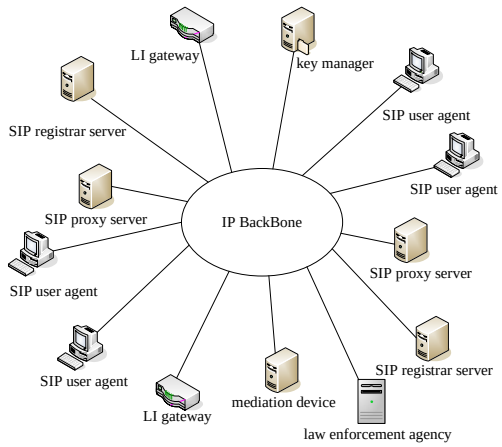

图 3　SIP 合法监听网络示意图

以图 4 为例，SIP user1 首先发出 INVITE 请求，代理服务器(proxy server)收到该消息之后，会向注册服务器(registrar server)确认 SIP user1 的身份认证，认证通过并经过授权后，代理服务器才允许 SIP user1 拨打 VoIP 呼叫，将 INVITE 消息传送到 SIP user2 的代理服务器，进而传送到 SIP user2。如果 SIP user2 要回应这个呼叫，会返回一个 OK 的消息，代理服务器收到 SIP user2 的消息，同样会向注册服务器确认 SIP user2 的身份认证，确定他有权限可以接通这个呼叫之后，才会将 OK 的消息传送给 SIP user1 那边的代理服务器，进而传送到 SIP user1，并通过 SDP 指定本通话所使用的 RTP 连接要通过哪一台合法监听网关(LI gateway)。接下来 SIP user1 和 SIP user2 可能会需要加密通话内容的密钥，这个密钥是由密钥管理器(Key Manager)产生并维护的。SIP user1 和 SIP user2 在建立通话连接之前，会先与密钥管理器建立加密的连接(使用 Diff-Hellman 或者 RSA 交换密钥)，然后密钥管理器会把之后通话加密所使用的密钥发送给通话双方。最后，SIP user1 和 SIP user2 都会与合法监听网关建立 RTP 连接，这时 SIP user1 和 SIP user2 就可以开始通话了，而且这个通话的内容使用了密钥管理器所产生的密钥进行了加密，也就是说合法监听网关所监听的通话内容是经过加密的，这样可以防止电信运营商私自取得通话内容。

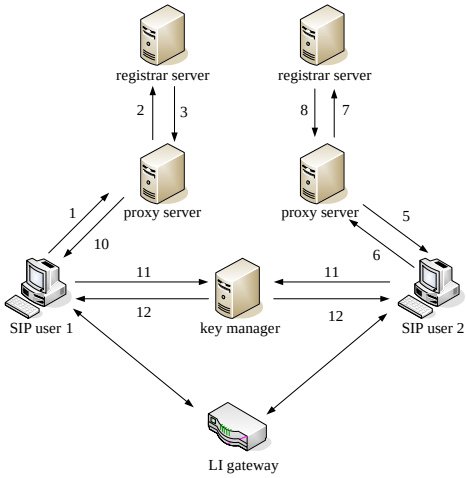

图 4　SIP 结合合法监听

在这个架构中，由 SIP 代理服务器执行 IRI IAP 的工作，由合法监听网关执行 content IAP 的工作。为了让司法机构能够解密监听结果，密钥管理器会将该通话的密钥发送到调解设备(MD)，再由调解设备送到 LEA。为了避免密钥被窃取，在增强系统安全的考虑下，本架构将密钥管理器(KM)和调解设备合二为一，这样可以大大降低通话密钥在网络上传输过程中被窃取的风险。图 5 是本系统的架构图。

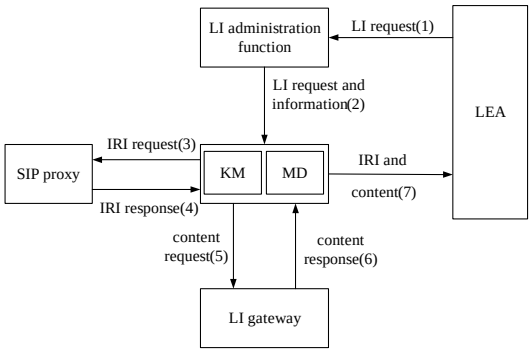

图 5　系统架构

当 LEA 决定要进行合法监听之后，会向 LI administration function 要求进行监听。LI administration function 收到请求之后，会把监听的格式和要求发送给调解设备，调解设备就可

以开始执行监听的流程。它会先判断监听目标所属的 SIP 代理服务器，发出监听的要求，SIP 代理服务器就会将 IRI 回传到调解设备。

在 SIP 通话建立成功而且通话双方开始传送语音包时，密钥管理器会给通话分配一个密钥，这时调解设备会发出监听通话的指令给合法监听网关，告诉合法监听网关要监听的通话 ID 以及监听结果回传地址，此时合法监听网关就开始记录通话内容并传送到调解设备。最后，调解设备会把 IRI 和通话内容收集起来，转换为 LEA 要求的格式，并传送给 LEA。而且，因为密钥管理器和调解设备合二为一，所以调解设备也知道通话内容加密的密钥，那么调解设备既可以选择将通话内容解密后传送给 LEA，也可以将密钥传送给 LEA，让 LEA 自行解密通话内容。

2.3 系统网元介绍

在本架构中用到了 SIP 协议中的 SIP 代理服务器和 SIP 注册服务器，其中 SIP 代理服务器要做一些修改。

(1)SIP 注册服务器(SIP registrar server)

SIP 注册服务器负责 SIP 使用者的注册以及身份认证，与 SIP 协议中的定义相同。

(2)SIP 代理服务器(SIP proxy server)

在本文提出的合法监听架构下，SIP代理服务器除了SIP协议定义的功能外，还必须增加一个功能，就是向调解设备提供通话的IRI。因此代理服务器要能够记录通话的建立时间、结束时间、呼叫保持时间、被监听目标的IP地址、被监听目标曾经拨打过的号码等信息。这些信息要整理后传送给调解设备，最终送到LEA。SIP代理服务器还有一个重要功能就是指定被监听目标和哪一台合法监听网关建立RTP连接。当SIP消息最后出现OK时，SIP代理服务器就会在SDP[5]消息中加入合法监听网关的IP地址，这样就实现了合法监听网关对通话RTP连接的中间人攻击(man-in-the-middle)，将通话内容记录下来。

(3)合法监听管理功能模块(LI administration function)

合法监听管理功能模块是 LEA 使用监听功能的用户界面，LEA 由这个界面输入监听目标的资料以及监听结果的格式等。

(4)调解设备(mediation device)

调解设备是整个系统的核心控制模块，它是合法监听管理功能模块和真正执行监听功能其他网元之间的桥梁，它接收合法监听功能模块传来的监听请求，要求被监听目标的 SIP 代理服务器提供 IRI，命令合法监听网关执行通话监听的动作，收集代理服务器回送的 IRI，并将整个监听结果处理后发送给 LEA。

(5)合法监听网关(LI gateway)

为了能够监听通话内容，本架构新增了这个网元，它负责监听通话内容。首先，它从调解设备得到监听的资料，包括通话双方的 IP 地址、监听结果回传地址等，然后它与通话双方建立 RTP 连接，并在转发双发语音包的同时进行复制，最后将监听结果传送给调解设备。

(6)密钥管理器(key manager)

为了让 VoIP 通话既安全又可以合法监听，本架构加入了密钥管理器。它负责产生对通话内容进行加密的密钥，并负责管理这些密钥。当通话双方成功建立通话连接之后，还没有开始传送 RTP 语音包之前，通话双方会从密钥管理器得到一个密钥，并用该密钥对通话内容进行加密。

2.4 系统安全性与可行性分析

(1)安全性

本文提出的合法监听系统架构中，密钥管理器和调解设备是最重要的网元，密钥管理器负责产生和管理所有通话使用的密钥，而调解设备负责监听 IRI 和通话内容，所以这两个网元都对安全性有很高的要求，本架构将二者合而为一，大大降低了可能的安全威胁和进行安全防护的成本。另外，在本架构之下，所有的 VoIP 通话都被 KM 产生的密钥进行了加密，所以就算 RTP 语音包被窃取，也不会泄漏通话内容，可以确保通话是安全的。

(2)可行性

本文提出的合法监听架构能满足合法监听的 3 个要求：

1)不会被监听目标发现。本架构中，配置了一台以上的合法监听网关，这样的设计有 2 个好处，一是可以混淆被监听目标的注意力，二是可以降低合法监听网关的负载，提高整个系统的并发能力。当呼叫建立的时候，SIP 代理服务器会将合法监听网关的 IP 地址传送给通话双方，通话双方各自与合法监听网关建立 RTP 连接。如果 SIP 代理服务器每次给被监听目标的 IP 地址都一样，就很可能被监听目标发现，如果系统中有多个合法监听网关，就会避免这种情况的发生。另外，SIP 代理服务器可以根据合法监听网关的使用状况，来选择当前系统负载最低的那台网关来执行监听任务，达到负载均衡。

2)提供监听相关信息(IRI)。在实际使用中，LEA 往往不只需要被监听目标的通话内容，还需要他的 IRI。在本架构中，SIP 代理服务器可以得到被监听目标的 IRI，并回传给调解设备，进而回传给 LEA。因为每一路通话的建立、修改和删除都必须经过 SIP 代理服务器，所以 SIP 代理服务器可以很容易地得到通话建立时间、通话结束时间、通话保持时间、甚至被监听目标曾经拨打过的电话号码、哪些成功、哪些失败等信息。

3)如果通话内容被电信运营商进行了加密，要让 LEA 能够对通话内容进行解密。这也就是要求监听系统除了能够截取通话内容，还要能够得到加密的密钥。在本文提出的架构下，只要让密钥管理器将通话的密钥回传给 LEA 即可。

3 结束语

本文提出了一套基于 SIP 协议的合法监听网络架构，以思科提出的合法监听架构为基础，再结合 SIP 协议，并加入了密钥管理器和 LI gateway 合法监听网关，使得其在 NGN 中也可以提供合法监听的功能。虽然本文是基于 SIP 协议进行的讨论，但是整体思路同样可以应用于其他 NGN 协议，如 MEGACO/H.248，只要将 SIP 代理服务器的功能在媒体网关控制器(MGC)上实现即可。

参考文献

[1] Rosenberg J, Schulzrinne H, Camarillo G, et al. SIP: Session Initiation Protocol[S]. RFC 3261, 2002.

[2] 中国电信集团公司. SIP 初始会话协议－信令流程[EB/OL]. (2003-12-31). http://bbs.cnttr.com/thread-38070-1-1.html

[3] International Telecommunication Union. ITU-T Recommendation H.248.1 Version 3[S]. 2002.

[4] Baker F, Foster B, Sharp C. Cisco Architecture for Lawful Intercept in IP Networks[S]. RFC 3924, 2004.

[5] Handley M, Jacobson V. SDP: Session Description Protocol[S]. RFC 2327, 1998.