# 基于身份的 VoIP 媒体流安全方案与实现

## Identity base media – stream security solution of VoIP and implement

侯 宾 (北京邮电大学电子工程学院 100876)
叶德信 (加拿大渥太华大学)
吕玉琴 (北京邮电大学电子工程学院 100876)
娄大富 (加拿大渥太华大学)

**摘要:** 以基于身份的非对称加密技术为核心,构建媒体流加密方案,解决了基于 SIP 协议的 VoIP 中媒体流机密性问题。着重对基于身份的非对称加密系统中密钥获取、密钥交换等问题进行了分析,并且针对 VoIP 应用中的实际问题提出了解决措施。

**关键词:** VoIP SIP IBE 媒体流加密

## 1 前言

随着 VoIP 技术步入实用,其安全问题成为行业的关注焦点;其中,保证通信数据的机密性和完整性尤为重要。VoIP 通信数据(即媒体流)的主要威胁包括来自传统 TCP/IP 网络的数据包截取和监听以及基于信令的呼叫欺骗等;由于媒体流数据要求很强的实时性,所以如果对媒体流进行加密和认证,必须在考虑安全性的同时,还保证数据传输流畅;此外,还要着重考虑会话密钥协商等问题。对于密钥协商,通常会采用非对称加密算法加密会话密钥的方法,而在传统的 PKI/CA 体系下,当用户间进行信息交互时,需要先从目录服务器查询对方证书并进行验证。但在 VoIP 应用中,如果用户每次呼叫都需要查询对方证书,会造成很长的延时、极大的网络和系统维护开销,严重阻碍了 VoIP 系统的商用。本文方案采用基于身份的加密体系(IBE,Identity Based Encryption)[1],来取代传统的 PKI/CA 体系,构建基于 SIP 协议的 VoIP 系统[4]的媒体流加密系统。将用户 ID(或电话号码)作为公钥,制定了无第三方介入交换密钥策略、减少了呼叫时的延迟,系统可以兼顾安全性和易用性,比较采用 IPSec 等协议组建解决方案,具有独特的优势。

## 2 基于身份的安全方案介绍

本文描述的媒体流安全方案主要分为两个部分,一是用户身份确认及私钥获取,二是密钥交换和数据加密。图 1 为本方案的总体结构。

### 2.1 私钥获取的原理和流程

在 IBE 体制下,用户私钥由系统产生。为实现 IBE 体制下的私钥发放,可以有两种作法:一是采用门限密码学中秘密共享原理构建系统[1,6],架设多个具有独立用户身份认证功能的私钥发放中心(PKG)。这种方法用户需要向多个 PKG 进行认证,这在实施、维护上难以进行,且私钥片段在传输过程中仍然存在泄密危险[2]。二是将独立的认证中心结合 PKG 构建系统[1]。用户首先从可信的认证机构取得证明自己身份的数字证书,凭证书以安全的方式从单个 PKG 获取自己的私钥。认证机构只负责审核用户身份并进行签名,结构上比较简单,甚至可以委托可信的第三方机构代理;而方案中的 PKG 为简化的 PKG,采用单个网络节点的方式,在功能上只具有私钥的发放功能,不对用户身份进行审核。

身份认证与私钥申请流程如下:

(1) 首先用户根据系统参数选一个随机数 x,作为自己的临时主密钥。并根据自己的 ID,与系统公共参数产生自己的一个临时公钥(xID)。再向可信任的认证机构发送 ID 和 xID,请求认证;

(2) 认证机构验证用户身份,生成关于 ID 和 xID 的证书,颁发给用户;

(3) 用户向 PKG 递交 ID、xID,以及相应证书。

(4) PKG 验证用户证书;PKG 用系统公钥 s 结合用户 ID,以及生成包含用户私钥的信息,并(利用 IBE 加密算法)将 M 加密为密文 C。

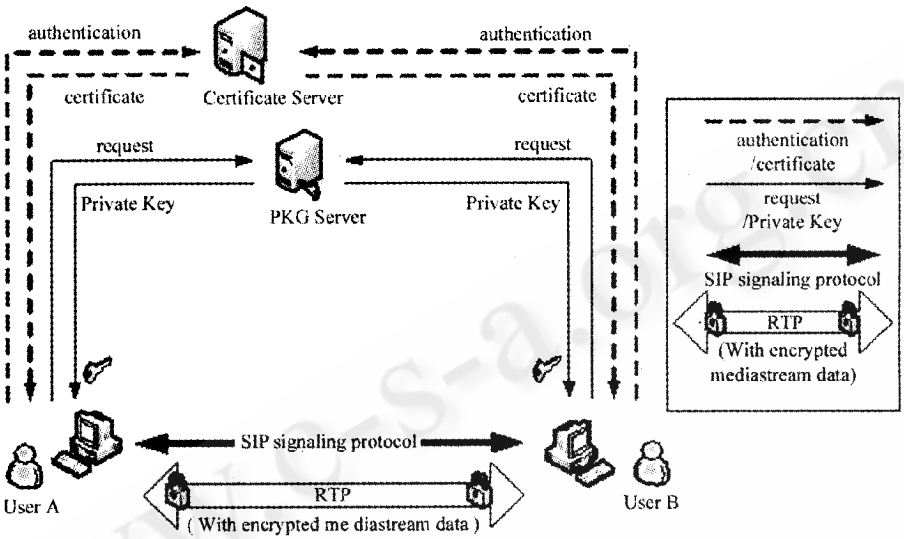


图 1　基于身份的媒体流安全方案总体结构图

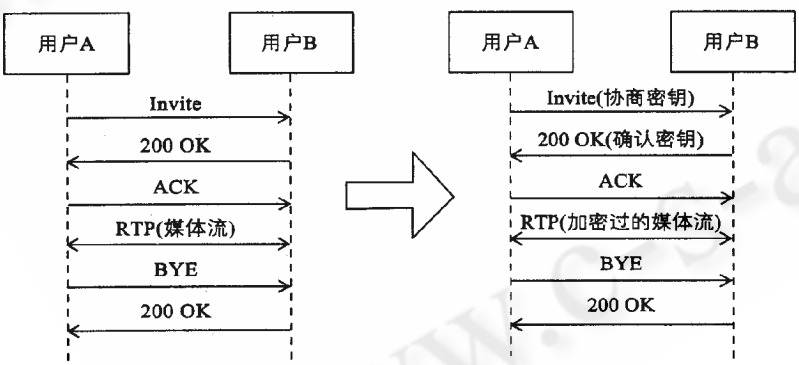


图 2　SIP 基本呼叫流程及改进流程图

(5) 用户用 x 解密 C 得到,再计算,得到 sID 即为用户私钥。

(6) sID 可采用口令机制进行加密,保存于本地存储器或于独立存储介质中。

### 2.2 密钥交换流程

系统的第二部分为呼叫建立期间的密钥交换,解决在进行电话呼叫时,如何安全方便的进行会话密钥的协商,以及对于媒体流数据进行加密的问题。核心思路是利用 SIP 协议建立会话时的信令交互来进行会话密钥的传递;会话密钥是由主叫方和被叫方共同随机生成,并在传输中采用对方公钥(ID)以 IBE 算法加密。

在密钥协商时,会话密钥被嵌入会话描述协议 SDP[3] 消息体内携带。SDP 中规定了可以传输密钥的可选项——key 域。Key 域可以包含在 SDP 消息体中的会话级描述部分,也可存在于媒体级描述部分。它包含两个字段:key – type 和 key – data。Key – type 定义了四种方法[3],本文方案使用 clear 关键字,并在 key – data 字段载入加密后的会话密钥。由于 SDP 中并没有会话密钥的细节标准,因此,key – data 数据被提取后的处理流程为自定义方法。通信流程如图 2。

改进的 SIP 会话建立过程如下:

(1) SIP 主叫方(用户 A)发送 Invite 请求之前,从 ENUM 服务器查询电话号码对应的对方 ID 和网络位置。这样就可以得到被叫方——即用户 B 的公钥;

(2) 用户 A 生成媒体流加密的会话密钥 session – key1,长度为 64 位;并用加密,得到密文 C1;之后,用户 A 向 B 发送 Invite 请求,在 Invite 的 SDP 消息体中加载 C1;

(3) 用户 B 接到请求,读出并验证 session – key1,若果解密正确,则随机生成 64 位的 session – key2,并将商定的会话密钥 = session – key1 + session – key2 保存。之后用户 B 利用用户 A 的公钥加密得到密文 C2;并将 C2 封装到"200 ok"响应中的 SDP 消息体中发回;

(4) 用户 A 验证用户 B 的返回信息中的会话密

钥,解开,看其中的 session – key1 字段是否正确;如果正确,则发送"ACK"响应,建立媒体流连接;

(5) 媒体流连接建立后,双方分别将本方采样编码后的声音(或图像)信号,用协商好的密钥何算法进行加密,这里加密算法为采用 128 位密钥长度的 AES 算法,加密密钥为。加密后的数据经过 RTP 协议封装后发送,对端则采用相同密钥,将 RTP 包中负载数据解密,再将这些数据解码,还原为声音(或图像)信号。

(6) 如果双方在密钥交换过程中发现密钥解码失败或密钥不符,则终止会话。

## 3 媒体流安全方案分析

### 3.1 私钥申请的安全性和可行性

首先,由于在 IBE 体制下,PKG 可以生成所有用户的私钥。因此,系统的整体安全性还在于 PKG 及系统主密钥具有绝对的安全性(类似 PKI 系统中的 CA)。而系统的可信性在于用户可以在既定安全等级下对 PKG 及其拥有者可以足够信任。本文论述的 VoIP 系统,在实际部署中,PKG 的拥有者一般为电信运营商(也可以为安全增值业务提供商)。在一般民用或商用通信下,基本可以保证用户对其的信任。

其次,私钥发放环节的可行性和安全性已经得到过证明和分析[2]。当认证机构可信时,用户 ID、xID 等公开信息,由证书保证合法性;用户私钥由用户临时公钥 xID 进行加密,来保证保密性和合法性。总体流程可以保证合法用户安全取得自己私钥。

再次,如果私钥丢失或被窃,则用户可以换 ID,重新申请私钥。在基于 SIP 的 VoIP 系统中,用户采用类似电子邮件地址的字符串来标示身份及位置,并且可以采用 ENUM 等方式将 ID 映射成传统电话号码,如"Alice@ server. com"对应号码"1234 – 5678"。因此,更换 ID 后,只要更新 ID 与电话号码的对应关系,用户仍然可以使用新的 ID 与私钥继续使用系统,对系统和用户没有太大影响。

此外,系统可支持较好的漫游应用。例如用户可将身份信息、密钥等信息存入智能卡等介质,则用户可在不同地点注册自己,并使用相同私钥进行通信。支持移动性,也符合未来 VoIP 业务的应用特点。

### 3.2 密钥交换的安全性和可行性

采用基于身份的加密体制,其好处主要在于减少用户因为查询对方证书、公钥的等待时间以及对网络的访问流量;此外还具有身份确认的功能——只要用户私钥保密,就可以确保参与通信一定为指定 ID 的网络用户或终端。

在安全性方面,攻击者无法从侦听到的信令中解开会话密钥。如果攻击者生成伪造的会话密钥(片断),对被叫进行中间人攻击,但是由于攻击者无法生成真正的会话密钥,而当主叫方验证被叫响应中的密钥数据不正确时,就会终止会话。再者,如果攻击者对被叫进行呼叫欺骗,会由于解不开被叫用"主叫方"公钥加密的会话密钥片段而失败。因此,此流程可以抵御数据窃听或中间人攻击造成的泄密,以及防止呼叫欺骗的发生。

### 3.3 媒体流加密策略的兼容性和实时性

(1) 兼容性。加密策略为端到端方式,密钥协商与信息加解密都在终端进行,加密策略对于传输层设备和通信协议透明;策略并且没有对 SIP/SDP 消息体和交互流程以及 RTP 协议作任何改动,保证对现有信令和媒体流协议的最大兼容性,可以兼容多种穿透 NAT 策略,也可以通过制定信任策略与标准 SIP 终端互通。

(2) 运行速度和实时性。对于媒体流数据,根据 RTP 协议中对于音频采样周期和音频编解码算法编码后数据大小,加密算法处理速度需大于 10k 字节/秒。本文方案使用 128 位密钥长度的 AES 算法,加密速度在主频 200MHz 硬件平台上可达 70M 字节/秒,满足媒体流数据对于实时性的要求。

对于信令通信,由于信令交互时要进行 IBE 算法的加解密运算,会产生约 40 – 80ms 的延时。在实际测试中,主观可以感受到呼叫建立过程略有迟滞,但可以容忍,不影响正常使用;IBE 加密算法加密 128 位的会话密钥的密文长度为 300 – 500 字节左右,虽然略微增加通信开销,但对于信令消息体构成与交互流程没有显著影响。

### 3.4 与 IPSEC 及 SRTP、DTLS 等传输加密协议方案的对比

比较 IPSec,本文方案在实施难度和成本要小得多,对于终端和网络平台要求更加灵活,可以在多种软硬件平台下保障安全性和运行效率;其次,不同与 IPSec 提供的端到网络边缘的安全性,本文提供的端到端安全性显然更加适合 VoIP 应用;再次,本方案选择

(下转第 33 页)

(上接第 28 页)

在多媒体信息经过采集、编码后进行数据的加密,比较经过多层封装后的 IP 数据包,本方案的负载数据量和数据冗余显然较小。而 SRTP 与 DTLS 协议均为正在完善之中的协议,分别是对现有 RTP 协议和 SSL/TLS 的改进,以适用于高实时性要求的场合,虽然对于解决此类问题具有借鉴意义和推动作用,但都还没有得到广泛的支持,无法保证兼容性和稳定性。

## 4 结束语

本文方案分别在 PC、Pocket PC 等平台上对于进行实际实验。在进行音频通信情况下,经实际运行,用户可以顺利得到会话密钥;信令交互顺利;话音流畅,而在没有会话密钥情况下,对媒体流通信的监听,只能听到白噪声,无法重现有用信息;系统兼顾安全性和实用性,具备了实际应用能力,并且可作为 SIP 终端上增值业务的通信安全研究的基础平台。

### 参考文献


1 Boneh D, Franklin M. identity based Encryption from Weil Pairing[A]. Kilian J CRYPTO 2001[C]. Berlin: SpingerVerlag, 2001. 213 – 229.

2 李新国、葛建华、赵春明, IBE 公钥加密系统的用户私钥分发方案. 西安电子科技大学学报(自然科学版), 2004, 4(31): 569 – 571。

3 IETF, SDP: Session Description Protocol [S], RFC2327, 1998. 4.

4 Jonathan Davidson, Tina Fox. 部署 VoIP 解决方案, 人民邮电出版社, 2003. 7。

5 冯登国, 公开密钥基础设施 – 概念、标准和实施, 人民邮电出版社, 2001. 4。