基于 SIP 的信令安全网关安全模块①

张金玲[1,2], 廉东本[2], 李 想[2]

[1](中国科学院研究生院, 北京 100049)
[2](中国科学院沈阳计算技术研究所, 沈阳 110171)

摘 要: GB/T 28181 标准制定了安全防范视频监控联网系统信息传输、交换、控制技术要求, 其中信令安全路由网关是一种应用服务器, 负责接收或转发域内外 SIP 信令, 完成信令安全路由网关间信令身份标识的添加和鉴别等功能. 本文通过分析 GB/T28181 标准中信令安全网关的基本功能需求, 提出信令安全网关安全模块的设计方案. 它通过对域内外转发的信令进行加解密和数字签名操作实现了身份认证、信息保密性和完整性的安全保障. 通过实际运行测试出此设计方案具有较好的性能和稳定性.

关键词: SIP 信令; 信令安全网关; 加/解密; 数字签名; 身份认证

SIP-Based Signaling Security Gateway Security Module

ZHANG Jin-Ling[1,2], LIAN Dong-Ben[2], LI Xiang[2]

[1](Graduate School of Chinese Academy of Sciences , Beijing 100049, China)
[2](Shenyang Institute of Computering Technology of Chinese Academy of Sciences, Shenyang 110171, China)

Abstract: GB/T 28181 standards formulate information transmission, switching,control technology requirements of security video surveillance network system, as an application server, the signaling security gateway is responsible for receiving or forwarding the SIP signaling between domains, adding identification and authentication. This paper analyzes the basic functional requirements of signaling security gateway, proposes design of security module. It achieves authentication, confidentiality and integrity of information by encrypting, decrypting the forwarding signaling and digital signature. This design has better performance and stability through the actual running.

Key words: SIP signaling; signaling security gateway; encryption/decryption; digtal signature; authentication

1 引言

2011 年, 国家制订了《安全防范视频监控联网系统信息传输、交换、控制技术要求》(GB/T 28181-2011)并于 2012 年正式实施, 为我国平安城市视频监控系统的建设做出了顶层规划参考[1]. 公安部强制要求于 2015 年之前实现基于 GB/T 28181 协议的视频监控系统的搭建. 目前全国的安防监控系统都要陆续升级到符合此协议标准的系统.

GB/T 28181 以 SIP 协议为交互准则. 由于 SIP 协议的不同实现细节和扩充, 即便各厂商先前用 SIP 网络结构, 相互之间也无法直接与 GB/T 28181 规定的 SIP 互通. 同时, 各厂商所依据的开发协议互不兼容, 导致平台对接、完成统一软件平台的开发有很大的困难. 对于已经部署的视频管理平台来讲, 上述问题实际上是一个 SIP 网关问题.

由于监控系统形成的网络是公安部的专用网, 其要求安全级别更高, 因此设计基于 SIP 的信令安全路由网关来保障安全是十分重要和必要的.

SIP 协议的大部分认证机制是发送 SIP 信令时进行身份认证[2,3], 本文在符合 GB/T 28181 标准的前提下提出了改进的认证方式, 在发送 SIP 信令前先进行角色权限检查, 没有分配则进行服务器与客户端的双向身份认证. 并在此基础上加入加解密保护和数据完整性保护来保障信息传输安全.

① 基金项目:国家水体污染控制与治理科技重大专项(2012ZX07505004)
收稿时间:2013-08-16;收到修改稿时间:2013-09-02

2　信令安全网关安全模块的设计

信令安全网关在转发 SIP 监控域信令前首先需要确认通信双方的身份, 经过身份认证后, 再对信令进行处理保证数据的保密性和完整性. 图 1 为信令安全网关的功能模块图.

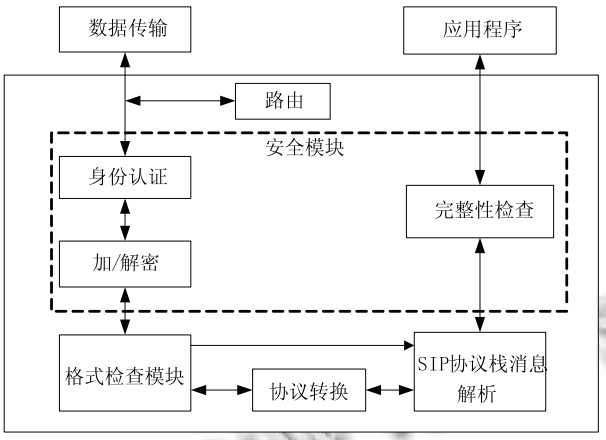

图 1　信令安全网关功能模块图

模块图中身份认证、加解密和完整性检查为信令安全网关的安全模块部分. 下面为安全模块的具体设计:

2.1 身份认证

对于安全网关, 对数据包的转发和根据安全规则对数据包进行判断、处理前, 需通过身份认证来判断用户的合法性并控制内部资源是否被外界用户访问. 首先定义角色集合, 并为每一类角色分配一组相应的权限, 管理员可以通过为用户分配、更改角色来分配权限. 当安全网关获得用户的访问请求时, 解析出源 IP 地址, 分析这个 IP 地址对应的用户是否有对应角色, 如果有对应的操作权限则认证通过, 否则将处理该认证请求, 进行身份认证[4].

假设网关 A 向网关 B 发送认证请求, 首先 A 和 B 通过 RSA 算法产生自己的公钥、私钥对$\{PU_A,PR_A\}$和$\{PU_B,PR_B\}$. 通过非密码途径分发公钥, 使得 A 和 B 知道对方的公钥. 认证的过程如下:

① A 向 B 发出认证请求消息.

② B 给 A 发送的消息包括 nonce 和 algorithm, nonce 为服务器给出的随机数, algorithm 为网关 B 提供的数字摘要算法, 为 MD5、SHA 等算法.

③ A 端接收到消息后, 取字符串 M 为用户名 username, 域名 realm, 服务器端随机数 nonce, 客户端提供的随机数 cnonce. 选择的数字摘要算法 algorithm, response 为数字摘要算法对 username, realm, nonce, cnonce 和口令运算所得结果.

用 A 的私钥和 B 的公钥加密消息发送给 B: $E(PU_B,E(PR_A,M+algorithm+response))$, 这样保证此信息为 A 发送, 只有 B 能接收解密, 并且保证数据在传输过程中的保密性.

④ B 接收到消息后, 用自己的私钥和 A 的公钥解密获得认证字符串, 将消息中 username, realm, nonce, cnonce 和服务器上存储的口令用摘要算法做哈希运算, 与 response 匹配, 相等则认证通过, 否则不通过. 下图为双方身份认证的流程:

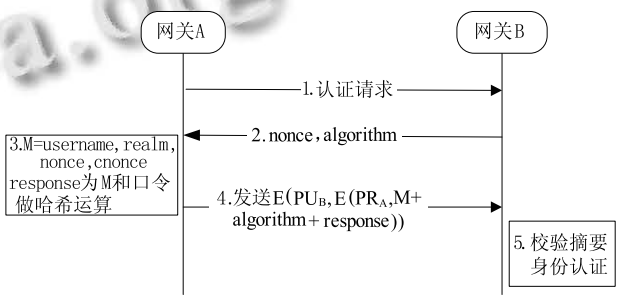

图 2　身份认证和密钥分配过程

2.2 加解密

当域内数据往域外转发时, 需要通过数据加密方法将数据加密, 一般采用 DES/3DES 算法, DES/3DES 是对称加密算法, 密钥我们称为会话密钥, 此密钥是一次性的用来保护数据的传输. 当收到从域外发来的信令时, 需要解密信令然后进行完整性检验等操作.

系统提供多种加密算法供用户选择, 不同的算法由 KDC(Key Distribution Center)密钥分配中心产生不同的会话密钥. 在传输数据同时需要传输会话密钥, 因此需要对会话密钥进行加密[5].

对会话密钥加密采用 RSA 公钥加密算法, 发送方 A 和接收方 B 通过 RSA 算法产生自己的公钥、私钥对$\{PU_A,PR_A\}$和$\{PU_B,PR_B\}$, 并将自己的公钥公开, 下面为会话密钥分配的过程:

(1) A 给 B 发送用 PU_B 加密的消息, 该消息包括 A 的标识 ID_A 和临时交互号 N_1. N_1 用来唯一标识本次交易.

(2) B 用 PU_A 加密含有 A 的临时交互号 N_1 和 B 的临时交互号 N_2 的消息, 因为只有 B 能解密(1)中的消息, 所以此消息中的 N_1 使得 A 确定对方为 B.

(3) A 给 B 发送用 B 的公钥加密含有 N_2 的消息, 因为只有 A 能解密(2)中的消息, 所以此消息中的 N_2 使得 B 确定通信伙伴为 A.

(4) A 选择会话密钥 K_S, 并将 $E(PU_B,E(PR_A,K_S))$发给 B, 用 PU_B 加密消息保证了只有 B 才能解密, 用 PR_A 加密保证了此消息只有 A 才能发送.

(5) B 收到消息后, 用自己的私钥和 A 的公钥解密得出会话密钥. 图 3 为会话密钥分配的过程:

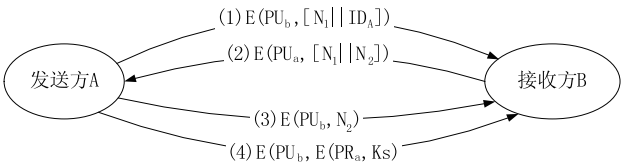

图 3 会话密钥分配过程

系统实现高安全级别, 在应用层采用 S/MIME 机制的端到端加密, 在传输层采用 TLS 协议、在网络层采用 IPSec 协议对 SIP 消息实现逐跳安全加密. 本文将着重讲解应用层 S/MIME 协议实现的安全保障.

Internet 协议安全性(IPSec)通过使用加密的安全服务来保证在 IP 网络上的通讯, 一般在操作系统级别实现. TLS 是处于传输层之上, 应用层之下的传输层安全协议, 通过 TCP 来提供安全. 适用于有动态联系的主机, 实现逐跳加密. 逐跳加密用来保护中间实体访问的信息, 比如 From、TO、Via 等头域, 阻止恶意用户改变呼叫方向或路由信息.

S/MIME 多用途网际邮件扩充协议是对流行的 MIME 电子邮件标准的扩展, MIME 允许消息体中包含复合类型的数据, 如图象、音频、视频及其它应用程序的特定数据, 并支持 GB/T 28181 标准里规定的特定消息体类型 SDP、Application/XML 等. 接收方根据不同的 MIME 类型来选择应用程序打开. S/MIME 提供端到端的加密, 加密不需要中间代理读取的信息, 包括 SIP 消息体和某些 SIP 消息头.

在 SIP 中有两种类型的加密 MIME 包体, 一种是加密的 S/MIME 包体, 另一种是隧道“message/sip”加密整个 SIP 消息.

SIP 消息中有一些头域是必须以明码格式显示的, 比如 From、To、Call-ID、Contact 等用来建立和维护对话状态的头域. 有一部分头域需要端到端的安全保证, 如 Subject、Organization 等, 故采用隧道“message/sip”加密 SIP 消息, 包括消息体和需要端到端保护的头域[6].

发送方 A 和接收方 B 通信, 首先分配会话密钥, 用对称加密算法加密 SIP 消息体和部分消息头. 在加密后的消息前面增加一个新消息头, 包含一些必须明码显示的头域. SIP 消息的认证通过数字摘要算法算出信令摘要存放在 Note 头域来实现, Note 头域需要端到端的保护, 不在新的消息头中显示. 接收方收到消息后先解密得到整个 SIP 消息, 然后对 SIP 消息进行认证, 通过完整性检查后再做其他操作, 具体的认证过程在 2.3 节讲解. 下面是加密的 SIP 消息的例子,在*括起来的文字是加密的:

```
Invite  sip:bob@biloxi.com SIP/2.0
Via:SIP/2.0/UDP
pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From:Alice<sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:pc33.atlanta.com>
Content-Type:application/pkcs7-mime;
    smime-type=enveloped-data;name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
        handling=required
Content-Length: 231
****************************************
Content-Type: message/sip
INVITE sip:bob@biloxi.com SIP/2.0
Via:SIP/2.0/UDP
    pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <bob@biloxi.com>
From: Alice <alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: 2013061410:30
Note:Digest nonce=”50903e318e1267d5” algorithm=MD5
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Sdp Content
****************************************
```

2.3 数据完整性检查

为保证 SIP 信令的完整性, 防止在传输途中被非

法篡改, 采用数字摘要算法做数字摘要认证.

图4 为SIP 信令的认证流程. SIP 信令的认证过程如下:

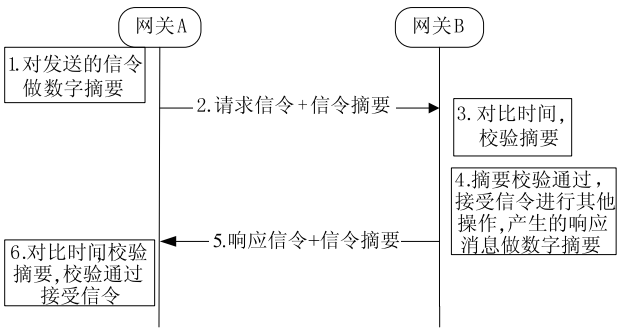

图 4　SIP 信令认证流程

① 在 SIP 消息头域中启用 Date 域记录发送消息时的系统时间, 并增加 Note 域, 其中有两个参数 nonce 和 algorithm, nonce 的值为 algorithm[From+To+Call-ID+Date+ 消息体] 经过 BASE64 编码后的值, “+” 为字符串连接运算, algorithm 的值为数字摘要的算法名称.

② 网关 A 将带有信令摘要的信令发送给网关 B.

③ 信令接收方收到 SIP 消息后, 首先将 SIP 消息 Date 域中的时间与当前时间做对比, 如果时间差在有效区间之内, 则做数字摘要校验. 解析出 SIP 消息中的 From、To、Call-ID、Date 头域、Note 头域和消息体, 用 algorithm 中的数字摘要算法对其做摘要和 Note 域中 nonce 参数值做对比, 如果相等则校验成功, 信令认证通过, 接受信令. 否则认证不通过, 丢弃该信令并终止该对话.

④ 认证通过并生成响应消息, 响应消息需要同样的方法做数字摘要认证, 将 From、To、Call-ID、Date 和消息体做数字摘要, 作为 nonce 的值添加到 Note 头域中, 使用的数字摘要算法作为 algorithm 的值.

⑤ 将带有信令摘要的响应信令发送到网关 A.

⑥ 网关 A 收到响应消息, 以上述同样方法进行校验认证, 相等则认证通过, 接受信令, 否则丢弃信令.

3　应用

由中心信令控制服务器和注册在服务器上的监控资源等组成的支持 GB/T 28181 标准规定通信协议的监控网络称为 SIP 监控域, 当 SIP 监控域 1 内客户端想访问监控域 2 内设备视频时, 客户端将 SIP 信令发送给监控域 1 内的中心信令控制服务器, 服务器解析信令得出访问端为监控域 2 内设备, 则将信令发往本域信令安全网关 1, 通过传送给域 2 的安全网关 2 最终到达域 2 的服务器来实现信令控制, 由媒体服务器将视频流发送出去.

在网关 1 给网关 2 发送信令前, 首先双方进行身份认证, 通过认证后, 网关 1 将信令做信令摘要存放到信令头域中并将信令整体加密发送出去, 网关 2 收到后解密得 SIP 信令并作完整性检查, 通过检查则接受信令、发送到本域服务器, 进行后续操作. 下图为监控域间互联结构图, 每个监控域的信令安全网关来完成域间信令转发并保障安全.

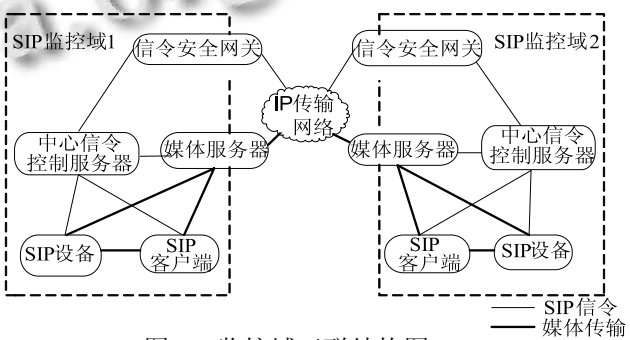

图 5　监控域互联结构图

4　结语

本文所设计的 SIP 信令安全路由网关的安全保障部分符合 GB/T 28181 标准, 完成了网关间身份认证、网关间传递的消息加解密和信令认证的设计方案. 该信令安全网关的设计已经应用到实际项目中, 取得了较好的效果. 今后还要对协议转换部分进行进一步的研究和实现.

参考文献

1 GB/T 28181-2011,安全防范视频监控联网系统信息传输、交换、控制技术要求.

2 李婧,李雪,胡浩.基于 SIP 的安全认证机制的研究与改进. 计算机工程,2009,35(2):162−163.

3 吕武玲,黎忠文.SIP 中基于身份认证的安全机制研究.计算机技术与发展,2009,19(2):159−161

4 赵跃华,刘申君.会话初始协议安全认证机制的分析与改进. 计算机工程,2011,37(20):114−115.

5 Stallings W.孟庆树,王丽娜,傅建明,译.密码编码学与网络安全—原理与实践.北京:电子工业出版社, 2010: 210−212.

6 Rosenberg J, Schulzrinne H, Camarillo G. RFC 3261, SIP: Session Initiation Protocol. June 2002.