ICS 33 050 99
M 40

YD

中华人民共和国通信行业标准

YD/T 1666-2007

远程视频监控系统的安全技术要求

Technical Specification for Long Distance Remote Visual Surveillance System Security

2007-07-20 发布　　2007-12-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是远程视频监控系统系列标准之一。该系列标准的名称和结构预计如下：

1. 远程视频监控系统业务需求；
2. 远程视频监控系统总体技术要求；
3. 基于IP的远程视频监控设备的技术要求；
4. 基于IP的远程视频监控设备的测试方法；
5. 远程视频监控系统的安全技术要求；
6. 远程视频监控系统的安全测试方法。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院

本标准主要起草人：　刘志勇、落红卫、刘晓红、李明慧

远程视频监控系统的安全技术要求

1 范围

本标准规定了基于IP网络的前端监控设备、监控管理平台、监控中心和远程监控客户端、运营支撑平台和通信网络应采用的安全技术，包括用户接入认证和业务认证、数据机密性和完整性、可用性、日志等方面。

本标准适用于远程视频监控系统。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8-2001	信息技术 词汇 第8部分：安全
GB/T 18119	低比特率通信的视频编码（等效于ITU-T H.263）
YD/T 822-1996	p×64kbit/s会议电视编码方式（等效于ITU-T H.261）
ISO/IEC 13818-2（1995）	信息技术—运动图像和相关音频信息的通用编码：视频（MPEG-2）
ISO/IEC 14496-2（2001）	信息技术—视听对象编码—第二部分：视频（MPEG-4）
ITU-T G.711	48kbit/s、56kbit/s、64kbit/s、50Hz～3.5kHz脉冲编码调制（PCM）
ITU-T G.723.1（1996）	以5.3 kbit/s和6.3 kbit/s为速率的多媒体通信的双速语音编码器
ITU-T G.728（1992）	采用线性预测激励的低时延码在16kbit/s速率上的语音编码
ITU-T G.729（1996）	采用共轭结构代数码本激励线性预测（CS-ACELP） 在8kbit/s速率上的语音编码
ITU-T H.235（2005）	H系列（H.323和其他基于H.245）多媒体终端的安全与加密
ITU-T H.264	高级视频编解码协议（H.264）
RFC 3261	SIP:会话初始协议

3 术语和缩略语

下列术语和缩略语适用于本标准。

3.1 术语

访问控制（access control）

一种安全保证手段，即数据处理系统的资源只能由被授权实体按授权方式进行访问。

授权（authorization）

授予权限，包括允许基于访问权的访问。

可用性（availability）

数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

机密性（confidentiality）

数据所具有的特性，即表示数据所达到的未提供或未泄露给未授权的个人、过程或其他实体的程度。

数据完整性（data integrality）

数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变。

拒绝服务（Denial of Service）

资源的授权访问受阻或关键时刻的操作的延误。

数字签名（digital signature）

添加到消息中的数据，它允许消息的接收方验证该消息的来源。

加密（encryption）

对数据进行密码变换以产生密文。

密钥管理（key management）

在一种安全策略指导下密钥的产生、存储、分配、删除、归档及应用。

伪装（masquerade）

指一个实体假装成另一个实体，以便获取未经授权的访问权。

抵赖（repudiation）

通信系统中涉及的若干实体之一对于参与全部或部分通信过程的否认。

路由选择控制（routing control）

在路由选择过程中应用规则，以便具体地选取或回避某些网络、链路或中继。

安全审计（security audit）

对数据处理系统记录与活动的独立的审查和检查，以测试系统控制的充分程度，确保符合已建立的安全策略和操作过程，检测出安全违规，并对在控制、安全策略过程中指示的变化提出建议。

通信业务分析（traffic analysis）

通过对通信业务流的观察（出现、消失、总量、方向与频度）对信息作出推断。

非授权访问（unauthorized access）

非授权访问是指一个实体试图在违反安全策略的情况下有效地访问系统，或授权实体超越权限访问系统。

3.2 缩略语

AES	Advanced Encryption Standard	高级加密标准
DDN	Digital Data Network	数字数据网
DES	Data Encryption Standard	数据加密标准
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
GK	Gatekeeper	网守
IP	Internet Protocol	互联协议
IPSec	IP Security	IP 安全
ISDN	Integrated Services Digital Network	综合业务数字网

MD5	Message Digest 5	消息摘要 5
PC	Personal Computer	个人计算机
PPPoE	Point to Point Protocol over Ethernet	以太网上的点对点协议
PSTN	Public Switched Telephone Network	公共电话交换网
RADIUS	Remote Authentication Dial-In User Service	远端拨入用户验证服务
SHA-1	Secure Hash Algorithm-1	安全散列算法-1
SIP	Session Initiation Protocol	会话初始协议
VPN	Virtual Private Network	虚拟专用网

4 远程视频监控系统的体系结构

4.1 体系结构

本标准所阐述的远程视频监控系统，是指能够提供公共电信网络上的运营级远程视频监控业务，网络拓扑为多级分区域结构，采用数字视频压缩编码技术，实现远程视频监视、存储、告警联动等一系列功能的视频监控系统。

远程视频监控系统主要由以下 5 部分构成：

- 前端监控设备；
- 监控管理平台；
- 监控中心和远程监控客户端；
- 运营支撑平台；
- 通信网络（包括IP网、DDN专线、无线网络等）。

系统的各组成部分的结构见图 1 所示。远程监控设备可以采用有线和无线等多种接入方式接入通信网络。远程视频监控系统应具备良好的实用性、稳定性、兼容性、可靠性、可管理性、安全性、互操作性和可扩展性。

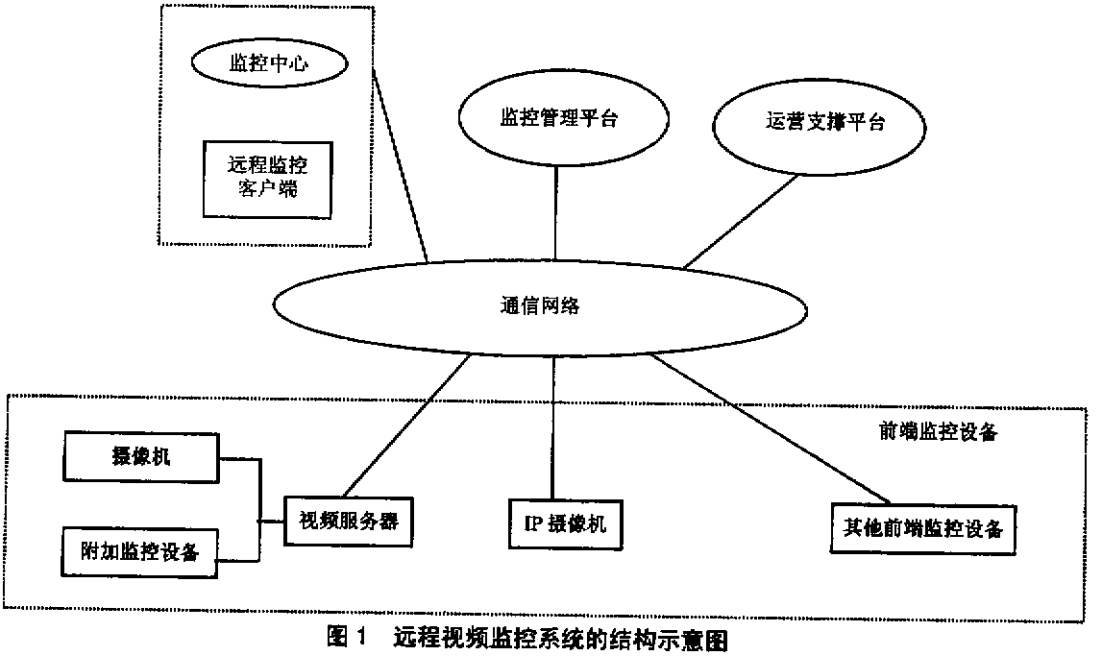

图 1 远程视频监控系统的结构示意图

4.2 远程视频监控系统各部分的功能

4.2.1 前端监控设备

远程视频监控系统中用来完成视音频信号和各种相关监控信息的采集、压缩和编码，并通过数字传输设备将监控信息上传到监控中心，同时接收监控中心下达的控制命令，完成对摄像机控制、报警信息的处理，以及对其他外围设备进行控制的设备。

目前各个厂家用来实现前端监控的设备类型很多，一般包括视频服务器、摄像机和附加监控设备。也可以采用IP网络数字摄像机直接将模拟信号转换为TCP/IP网络标准的数据包，直接传送到网络上实现上述功能。另外还有其他类型的视频监控前端设备，如基于PC机加视频采集卡等形式。

附加监控设备主要包括音频采集设备、报警输入输出设备、云台及云台解码器等。

4.2.2 监控管理平台

远程视频监控系统中用来实现对系统进行管理和控制的中心平台，主要功能包括对远程现场的音视频等信息的实时存储、检索、回放、内容分发功能、网管和用户认证等。

监控管理平台通常包括通信服务器、存储服务器等设备。

4.2.3 运营支撑平台

在可运营的远程视频监控系统中，实现对监控系统的运营支撑和业务运营管理，包括开户、销户、用户信息管理，同时能够实现与计费营账系统的互通，保障业务的运营。

4.2.4 通信网络

高效可靠稳定的网络传输系统是保证整个远程视频监控系统可靠运行的关键。远程视频监控传输通信网络包括 IP 网络、ISDN 和移动网络等。

前端设备、监控中心、监控管理平台设备和远程监控客户端及其他系统的设备可以通过光缆、电缆和无线方式接入。视频监控系统要取得比较满意的视频质量，通道带宽至少应在384 kbit/s 以上。

4.2.5 监控中心

远程视频监控系统中用来实现对各个现场的实时监控的中心平台，主要功能包括实时监视、云台控制、镜头变焦、图像参数调整、视频存储检索回放、报警联动等。

4.2.6 远程监控客户端

远程监控系统中通过远程方式接入到监控管理平台，并根据授权实现对监控现场的远程监视、控制等功能。

4.3 远程视频监控系统中的数据类型

4.3.1 视音频数据

视频监控系统各部分之间传输的主要信息，视频通常采用 H.261、H.263、H.264、MPEG2、MPEG4、MJPEG 编码，音频通常采用 G.711、G.723、G.728 和 G.729 等编码。

4.3.2 控制数据

控制数据主要包括管理数据和呼叫信令协议数据。

管理数据用于对远程视频监控系统设备的管理，例如可以对前端监控设备的云台控制、摄像机控制、帧速率、码速率控制等。

呼叫信令协议数据根据实际情况，一般可以采用H.323、SIP协议或者自定义的协议。

5 远程视频监控系统的安全威胁

安全威胁是对安全的潜在的侵犯，是一种可能导致系统被破坏、服务被拒绝、信息暴露、数据被篡改的潜在环境或事件，这些威胁可能影响网络服务的各项功能。远程视频监控系统的安全威胁是多方面的，包括前端监控设备、监控管理平台、监控中心和远程监控客户端、运营支撑平台的主要安全威胁以及视音频、报警、控制数据在不同的通信网络中传输时的安全威胁。

5.1 前端监控设备的主要安全威胁

- 伪装：非法监控中心或监控管理平台等设备伪装成一个授权实体与前端监控设备通信，对前端监控设备进行操作、非法获取监控现场信息等。
- 非授权访问：监控中心或远程监控客户端在未经授权的情况下访问前端监控设备。
- 抵赖：监控中心或远程监控客户端访问前端监控设备后否认曾经访问的事实。
- 数据窃取：前端监控设备发出的视音频和报警等信息可能在传输过程中被截获，导致信息被非授权的泄漏。
- 完整性破坏：监控管理平台、监控中心等设备发向前端监控设备的控制信息和认证相关信息等可能会受到未授权的修改、删去、重放、插入和重排序等操作，导致数据的完整性受到破坏。

5.2 监控管理平台的主要安全威胁

- 伪装：一台非法远程监控客户端用户伪装成一个授权用户与监控管理平台通信，或一台非法前端监控设备伪装成一个正常的前端监控设备向监控管理平台发送虚假的视音频和报警信息。
- 非授权访问：监控中心或远程监控客户端在未经授权的情况下访问监控中心。
- 抵赖：监控中心或远程监控客户端访问监控管理平台后否认事实，或不合法前端监控设备在向监控管理平台提供虚假的视音频和报警信息后否认事实。
- 拒绝服务攻击：非授权的远程监控客户端向监控管理平台发送大量服务请求，致使监控管理平台的资源被大量占用，不能正常、实时地响应其他授权远程监控客户端用户的访问请求，或不能正常处理前端监控设备的视音频和报警信息。
- 数据窃取：远程监控客户端访问监控管理平台时，监控管理平台发出的视音频等信息在传输过程中可能会被截获，导致信息被非授权的泄漏，或者监控管理平台向前端监控设备发出的一些控制信息在传输过程中可能会被截获，导致信息被非授权的泄漏。
- 完整性破坏：前端监控设备发向监控管理平台的视音频和报警等信息可能会受到未授权的修改、删去、重放、插入和重排序等操作，导致数据的完整性受到破坏。
- 病毒威胁：监控中心的各种服务器可能遭到病毒攻击导致监控管理平台不可用。

5.3 监控中心和远程监控客户端的主要安全威胁

- 伪装：不合法的前端监控设备伪装成合法的前端监控设备向监控中心或远程监控客户端提供虚假的视音频和报警等信息。
- 完整性破坏：监控中心发向监控中心或远程监控客户端的视音频和报警等信息可能会受到未授权的修改、删去、重放、插入、重排序等操作，导致数据的完整性受到破坏。

5.4 运营支撑平台的主要安全威胁

• 完整性破坏：监控管理平台发向运营支撑平台的用户信息、原始计费信息、管理信息等可能会受到未授权的修改、删去、重放、插入、重排序等操作，导致数据的完整性受到破坏。

• 病毒威胁：运营支撑平台的各种服务器可能遭到病毒攻击导致运营支撑平台不可用。

5.5 远程视频监控系统通信网络的主要安全威胁

• 可用性威胁：远程视频监控通信网络可能会遭受流量攻击造成网络不可用。

• 通信业务分析：攻击者对通信网络上信息的流向、流量、通信频度和长度等参数进行分析，从中推测出信息源、目的、用户名和口令等重要信息，从而导致信息泄漏和系统被攻击。

6 安全技术要求

6.1 远程视频监控系统的业务安全要求

6.1.1 远程视频监控系统业务安全接口模型

基于远程视频监控系统的结构示意图，远程视频监控系统业务安全接口模型如图 2 所示。

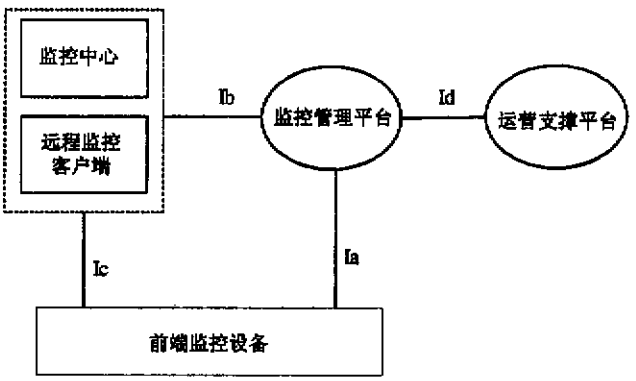

图 2 远程视频监控系统业务安全接口模型

6.1.2 接口描述

（1）Ia接口：前端监控设备和监控管理平台之间的接口，提供前端监控设备和监控管理平台之间的数据机密性和完整性保护等功能。

Ia接口上传递的信息主要包括由前端监控设备发向监控管理平台的视音频等信息、状态信息和同步信息，以及监控管理平台发向前端监控设备的控制信息。Ia接口应对这些信息进行机密性和完整性保护，以对抗前端监控设备和监控管理平台面临的数据窃取和完整性破坏等威胁。

Ia接口可支持监控管理平台和前端监控设备间的单向认证或双向认证。

（2）Ib接口：监控中心/远程监控客户端和监控管理平台之间的接口，Ib接口上传递的信息主要是对监控中心/远程监控客户端对前端监控设备的控制信息。当监控管理平台采用内容分发方式传输数据时，Ib接口上直接传递视音频等信息、状态信息以及同步信息。

监控中心/远程监控客户端必须经过监控管理平台的认证，认证通过后才能在一定的权限下访问前端监控设备或对前端监控设备进行控制，Ib接口应提供监控管理平台对监控中心/远程监控客户端的认证，可提供双向认证功能。

当监控中心/远程监控客户端通过监控管理平台浏览或回放监控现场的图像时，Ib接口提供监控中心/远程监控客户端和监控管理平台之间的数据机密性和完整性保护等功能，这些数据包括视音频等信息。

（3）Ic接口：监控中心/远程监控客户端和前端监控设备之间的接口，Ic接口上传递的信息主要是前端设备采集到的视音频等信息。

Ic接口提供监控中心/远程监控客户端和前端监控设备之间的视音频等信息的安全传送，包括机密性保护、完整性保护等功能。

（4）Id接口：监控管理平台和运营支撑平台之间的接口，提供监控管理平台和运营支撑平台之间的用户信息、原始计费信息、管理信息的传送功能。

Id接口应提供监控管理平台和运营支撑平台之间的通信安全，主要包括监控管理平台和运营支撑平台之间的单向认证或双向认证功能，Id接口可提供对计费、管理等敏感信息的数据完整性、数据机密性保护等功能。

6.1.3 用户和设备管理

远程视频监控系统应能够提供完善的用户管理机制，对管理员和用户进行分级授权，至少实现三级管理。三级用户管理分级方式可以是系统管理员、普通管理员和普通用户。系统管理员可以完成包括系统和用户管理在内的所有操作，普通管理员可以对系统和用户进行部分操作，普通用户只能浏览图像并对某些前端监控设备进行操作。具体的分级方式可以依据运营商或系统使用者自身的安全和运营策略制订，如管理员用户不能浏览前端监控设备的图像信息等策略。

当不同级别的用户同时要求对某一设备操作时，系统应首先满足高优先级用户操作。

系统应支持集中用户管理，所有用户信息可以集中存放在运营支撑平台中，在没有运营支撑平台时，也可以集中存放在监控中心的服务器中。

为便于对用户和设备进行统一管理和认证，提高系统的开放性和安全性，需要对系统的各级用户和各种设备进行统一编码，为用户分配用户名，为设备分配标识符，编号采用统一的编码规则。

在使用远程视频监控系统提供的业务前，用户必须首先注册，管理员应为用户开户，并设置用户在各个设备中的相应操作权限。用户使用系统提供的业务或对系统进行管理时，需提供认证信息，经过运营支撑平台或监控中心认证授权后才能在规定的权限下进行操作。

6.1.4 业务认证

为检查用户的身份并确定访问者是否合法，或者确定对端设备是否合法，对抗伪装威胁和非授权访问威胁，可采用对用户和设备的认证技术。

当远程监控客户端需要查看监控现场和操作前端监控设备，或管理员用户需要对设备和用户进行操作时，运营支撑平台或监控中心应对用户进行认证以确定用户身份和操作权限，主要在Ib接口或Ia接口上进行。

为方便业务的扩展，可以在全网监控管理平台内设置统一的全网认证服务器，并在各区域的监控管理平台设置本地认证服务器，本地认证服务器负责本区域内用户和设备的认证，全网认证服务器负责整个远程视频监控网络内用户和设备的认证。全网认证服务器可以采取主备倒换机制，以提高系统的可靠性。

对各级用户的认证可以采用用户名和口令的方式。管理员为用户开户时，为用户分配用户名和初始口令，用户可以在系统配合下修改口令。为保证达到一定的安全性，口令长度不应小于6位。协议可采

用 Radius 协议。

以普通用户在通过监控管理平台认证后访问前端监控设备为例，分别给出基于 SIP 协议和 H.323 协议的 Radius 安全认证流程

基于SIP协议的安全认证流程如图3所示。

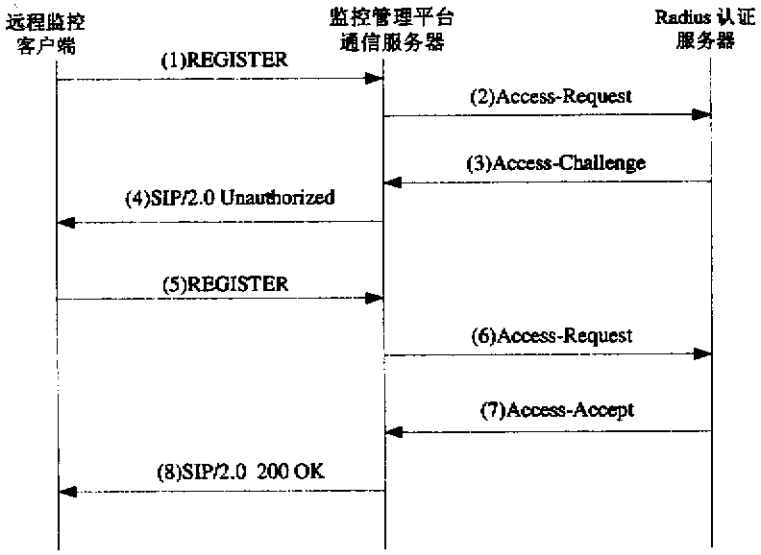

图 3 基于 SIP 协议的安全认证流程

（1）普通用户通过远程监控客户端访问监控管理平台，请求浏览前端监控设备的图像时，远程监控客户端应首先使用 REGISTER 消息向监控管理平台通信服务器发起注册，消息中携带用户 ID 和支持的加密算法 ID 列表等信息。

（2）监控管理平台通信服务器收到 REGISTER 消息后，通过 Access-Request 消息将用户名等认证信息发送到认证服务器。

（3）认证服务器生成随机数 Rand，并通过 Access-Challenge 消息发起挑战，消息中携带认证服务器确定的加密算法 ID。

（4）监控管理平台通信服务器通过 Unauthorized 消息转发认证服务器的挑战，要求远程监控客户端进行认证。

（5）远程监控客户端根据接收到的随机数 Rand、加密算法 ID、用户名、口令等信息计算得到 Response，通过 REGISTER 发送给监控管理平台通信服务器。

（6）监控管理平台通信服务器通过 Access-Request 消息转发客户端的注册消息给认证服务器。

（7）认证服务器根据本地保存的用户口令、用户名、随机数 Rand 和上述确定的加密算法 ID 等信息计算得到认证字 AUTH，如果挑战字等于 AUTH，则回复 Access-Accept 消息允许用户的接入。

（8）通信服务器向远程监控客户端发送 200 OK 消息，注册成功。

基于H.323协议的安全认证流程如图4所示。

（1）普通用户通过远程监控客户端访问监控管理平台，请求浏览前端监控设备的图像时，远程监控客户端应首先使用 RRQ 消息向指定的监控管理平台通信服务器发起注册，消息中携带用户 ID 和支持加密算法 ID 列表等信息。

（2）监控管理平台通信服务器收到 RRQ 消息后，通过 Access-Request 消息将用户名等认证发送到

认证服务器。

（3）认证服务器生成随机数 Rand，并通过 Access-Challenge 消息发起挑战，消息中携带认证服务器确定的加密算法 ID。

（4）监控管理平台通信服务器通过 RRJ 消息转发认证服务器的挑战，要求远程监控客户端进行认证。

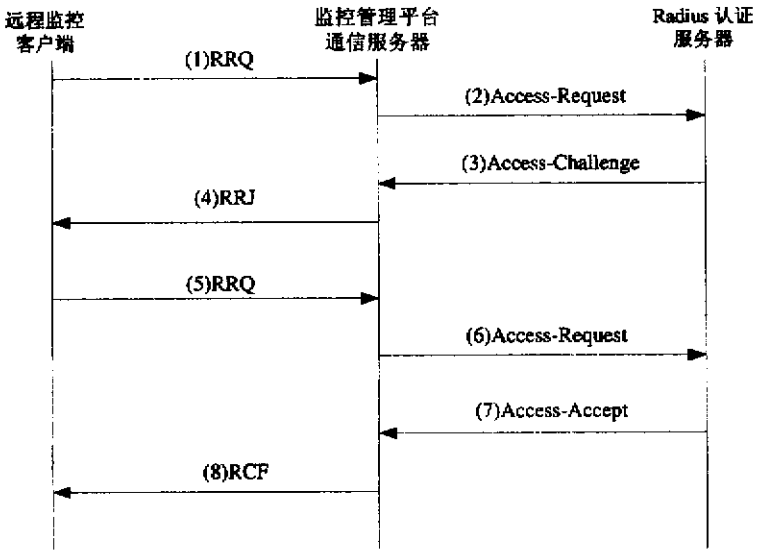

图 4　基于 H.323 协议的安全认证流程

（5）远程监控客户端根据接收到的随机数 Rand、加密算法 ID、用户名、口令等信息计算得到 Response，通过 RRQ 发送给监控管理平台通信服务器。

（6）监控管理平台通信服务器通过 Access-Request 消息转发客户端的注册消息给认证服务器。

（7）认证服务器根据本地保存的用户口令、用户名、随机数 Rand 和上述确定的加密算法 ID 等信息计算得到认证字 AUTH，如果挑战字等于 AUTH，则回复 Access-Accept 消息允许用户的接入，否则回复 Access-Reject 消息拒绝用户的接入请求。

（8）通信服务器向远程监控客户端发送 RCF 消息，注册成功。

对设备的认证是可选功能，包括Ia接口、Id接口上的设备之间的认证。设备间的认证基于设备的标识符，验证设备的合法性，对抗伪装威胁。

用户认证和设备认证的认证信息、认证算法可以是多种多样的，除对用户认证使用的用户名和口令外，还包括基于数字证书的认证、基于智能卡的认证、基于生物技术的认证、基于公开密钥的认证、基于共享密钥的认证等。

6.1.5　数据加密和完整性保护

远程视频监控系统业务安全的数据加密和完整性保护指在系统中前端设备、监控中心、远程监控客户端和运营支撑平台等业务层设备上进行的数据加密和完整性保护，在通信网络上进行的保护不在业务安全规定的范围内。

数据加密和完整性保护主要在Ia、Ib等接口上进行。

数据加密要求是指设备在发送信息之前要对全部数据或部分选择字段进行机密性保护，使非法用户不可能通过观察通信业务流推断出其中的视音频信息、控制信息等。数据加密主要用于对抗数据窃取。

加密算法分为对称密钥加密算法和公钥算法，常见的对称加密算法包括AES、DES、3DES等，推荐业务层设备采用AES、3DES加密算法。远程视频监控系统的视音频信息数据量大，尤其是在多用户同时服务时，加密会产生一定程度的时延影响，因此设备可以对视音频等信息进行选择性加密，比如对H.264视频流的参数集、I帧等关键部分进行加密。

对于采用SIP协议的远程视频监控系统，在对SIP消息进行数据机密性保护时，由于代理服务器等网络设备为了正确路由消息需要查看消息中的某些头字段，因而建议系统中各种设备在网络设备配合下采用IPSec或TLS以逐跳方式对消息进行加密，在完成密钥协商之后再对视音频等数据进行加密。具体规定参见RFC3261。

对于采用H.323协议的远程视频监控系统，系统中各种设备可以在H.245消息交换期间与对端协商数据流加密密钥和加密算法，然后对发出的数据流进行加密。如果H.245信道是安全的，则对数据流密钥不需要施加任何保护；如果一个预共享秘密与算法在H.245信道外部建立，这个预共享秘密可用于对数据流加密密钥进行保护；当H.245信道不安全时，可以使用证书，利用证书内的公钥加密数据流加密密钥。前端监控设备也可以通过传输层/网络层安全机制，如TLS或IPSec技术对数据流进行加密保护。具体规定参见ITU-T H.235。

数据完整性保护要求前端监控设备对其发出的数据采取完整性保护手段，防止数据因丢失、篡改、重放、插入、乱序等对监控中心造成威胁。

业务层设备可以通过消息校验、顺序号、时间戳等保证数据完整性。常见的消息校验算法包括基于单向Hash函数（MD5或SHA-1）的带密钥的消息认证码和对称密钥加密算法AES、DES等。完整性保护算法推荐推荐采用HMAC-MD5-96或HMAC-SHA-1-96。

部分常见的加密算法在起到数据加密作用的同时完成了数据完整性保护。

6.1.6 日志要求

日志要求系统记录用户管理、设备管理、故障告警、拒绝访问、设备升级等关键安全相关事件。日志系统应定义严重程度级别，并根据安全事件的严重程度以一定的方式提示管理员。基于日志管理员等相关人员可以对安全事件进行追溯和安全审计，保证不可抵赖性。

系统日志可以集中保存在监控管理平台中。日志保存的信息应包括但不限于以下内容：

- 访问/操作时间；
- 访问/操作者的真实身份；
- 访问/操作对象；
- 访问/操作类型；
- 访问/操作结果；
- 设备故障等重大事件发生的时间、设备标识符、严重程度等。

注：对视音频和报警信息的记录不在日志记录范围内。

6.1.7 可用性要求

远程视频监控系统业务层安全的可用性要求的对象主要是各级监控管理平台，这些设备是系统开展监控等业务的核心业务层设备，为了对抗拒绝服务攻击，避免因非授权的远程监控客户端用户/攻击者发送大量服务请求，导致核心业务层设备的资源被大量占用，不能正常响应其他授权远程监控客户端的访问请求或不处理前端监控设备的视音频和报警信息，必须采取手段保证这些设备的可用性。

为保证监控管理平台的可用性，可以在这些设备前布设防火墙与外网隔离，根据需要制定安全策略，允许、拒绝或监测出入设备的信息流，减少这些设备受到攻击的可能。

另外，为防止病毒攻击对系统可用性产生的威胁，在业务层核心设备上必须安装防病毒软件，并禁止在这些设备上进行互联网浏览等活动。

6.2 远程视频监控系统的网络安全要求

6.2.1 网络接入认证

为提高远程监控客户端等设备接入到监控系统时的安全性，通信网络应对远程监控客户端等设备进行网络接入认证。

网络接入认证协议可以采用PPPoE和DHCP等方式，具体规定参见相关标准。

6.2.2 数据保密性和完整性要求

远程视频监控系统底层通信网络可采取机密性和完整性措施保证监控系统数据传输过程的安全性。

构建远程视频监控系统时，一般不会为系统建设专用通信网络，而是利用现有通信网承载监控业务。为增强系统的安全性，建议在建设远程视频监控系统时，采用VPN技术构建虚拟专网，提供一定程度的数据机密性和通信安全，隧道协议推荐采用三层隧道协议IPSec AH或IPSec ESP以保证安全性。