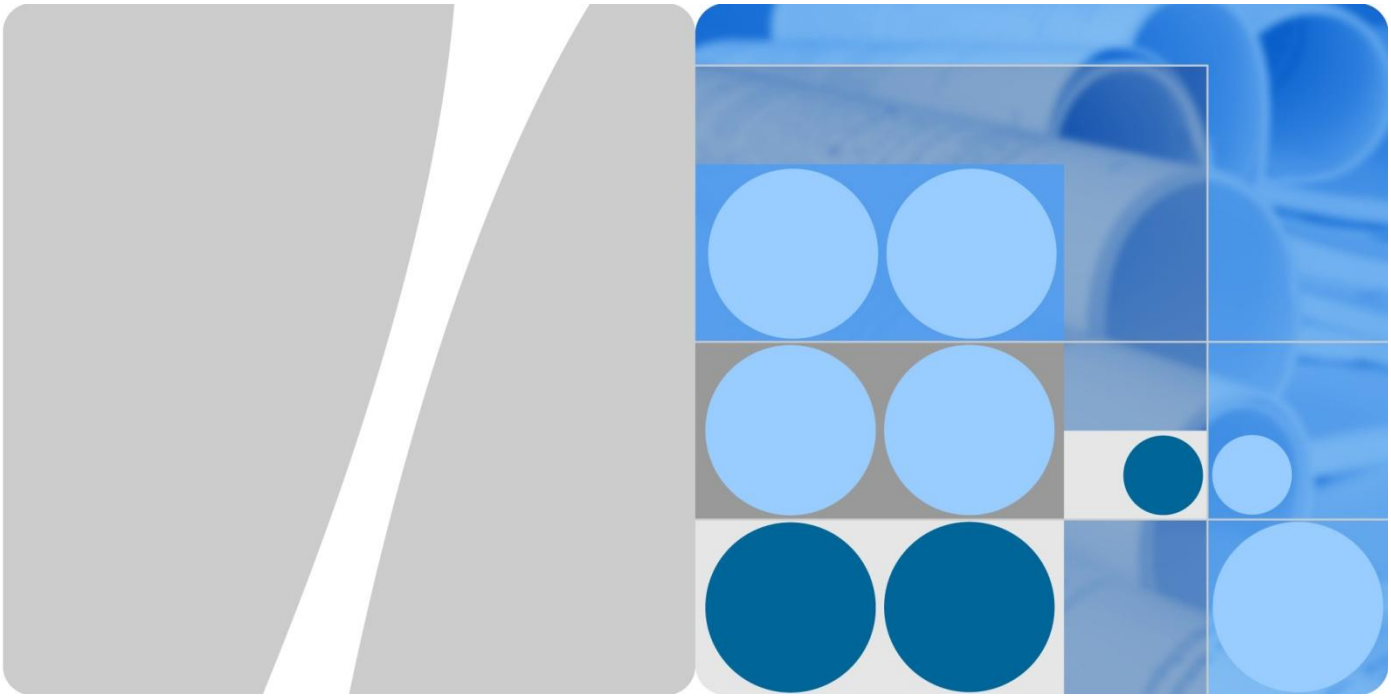
资料编码



视讯产品/解决方案
安全技术白皮书

文档版本　V1.0

发布日期　2012-12-18

华为技术有限公司

商标声明

 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

目　录

1 概述

1.1 视讯解决方案概述

系统架构

视讯解决方案提供面向行业、企业用户的语音、视频会议的 H.323/SIP/H.320 多点会议接入、控制功能。支持大、中容量的 IP/E1/4E1/ISDN/PSTN 混合接入，支持 1080p60f 分辨率的高清解决方案，配合新一代业务管理平台 SMC2.0，提供更完善、更易用的会议管理和预约调度功能。

MCU 是视讯会议系统的核心设备，提供终端的接入和会议功能的实现。对于公众运营网络，部署于骨干层。对于专网部署于各级汇聚点，对于企业网部署于外部出口。

如下图所示，在运营组网里面，MCU 处于媒体交换层，向下接入各种网络类型的终端，向上接受控制和支撑层的管理，同时与同处媒体交换层的其他 MCU 有级联交互。提供多种网络类型（IP/E1/4E1/ISDN/PSTN）的接入。

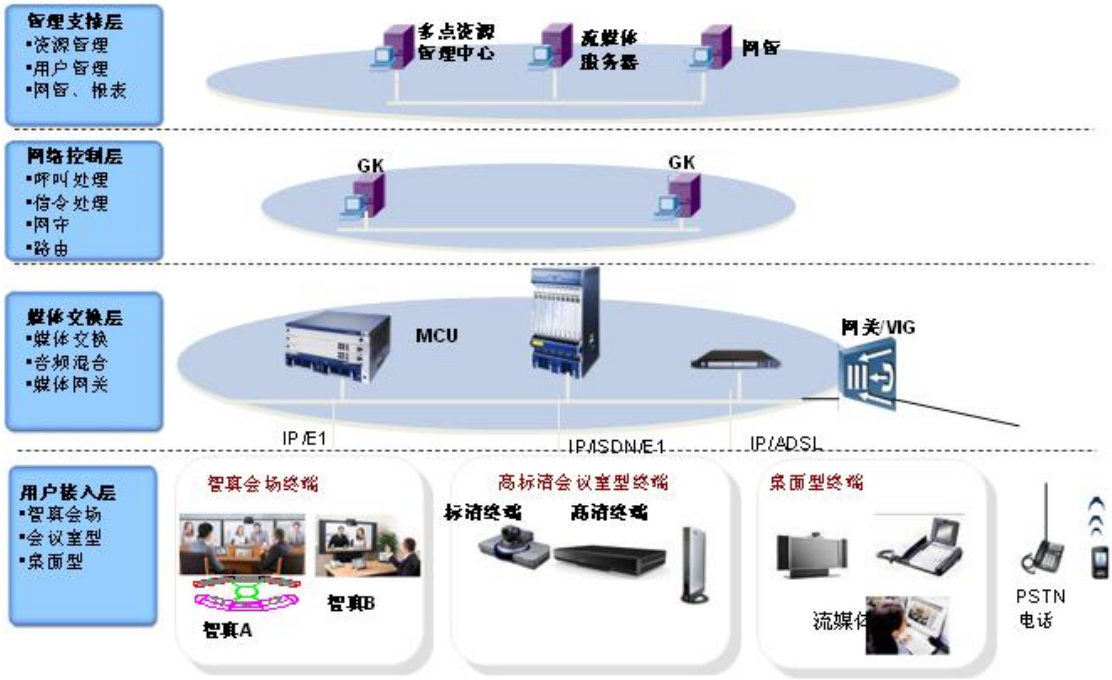


图1-1 视讯解决方案典型组网图

1.2 视讯解决方案面临的安全威胁

应用层安全威胁

- 输入验证：缓冲区溢出，跨站点脚本编写，SQL 注入。
- 身份验证：网络窃听，暴力破解，词典攻击，重放 cookie，盗窃凭据。
- 授权：提高特权，泄漏机密数据，篡改数据，引诱攻击。
- 配置管理：未经授权访问管理接口，未经授权访问配置存储器，检索明文配置数据，缺乏个人可记帐性，越权进程和服务帐户。
- 敏感数据：访问存储器中的敏感数据；窃听网络；篡改数据。
- 会话管理：会话劫持；会话重放；中间人。
- 加密技术：密钥生成或密钥管理差；脆弱的或者自定义的加密术。
- 参数操作：查询字符串操作；窗体字段操作；cookie 操作；HTTP 标头操作。
- 异常处理：信息泄漏；拒绝服务。
- 安全审计：用户拒绝执行某项操作；攻击者利用没有跟踪记录的应用程序；攻击者掩饰他或者她的跟踪记录。

系统层安全威胁

- 病毒、特洛伊木马和蠕虫：病毒就是一种设计的程序，它进行恶意的行为，并破坏操作系统或者应用程序。除了将恶意的代码包含在表面上是无害的数

据文件或者可执行程序中外，特洛伊木马很像一种病毒。除了可以从一个服务器自我复制到另一个服务器，蠕虫类似于特洛伊木马。蠕虫很难检测到，因为它们不是定期创建可以看见的文件。通常只有当它们开始消耗系统资源时，才能注意到它们，因为这时系统运行缓慢或者其他执行的程序停止运行。

- 足迹：足迹的示例有端口扫描、ping 扫描以及 NetBIOS 枚举，它可以被攻击者用来收集系统级的有价值信息，有助于准备更严重的攻击。足迹揭示的潜在信息类型包括帐户详细信息、操作系统和其他软件的版本、服务器的名称和数据库架构的详细信息。
- 破解口令：如果攻击者不能够与服务器建立匿名连接，他或者她将尝试建立验证连接。为此，攻击者必须知道一个有效的用户名和口令组合。如果您使用默认的帐户名称，您就给攻击者提供了一个顺利的开端。然后，攻击者只需要破解帐户的口令即可。使用空白或者脆弱的口令可以使攻击者的工作更为轻松。
- 拒绝服务：可以通过多种方法实现拒绝服务，针对的是基础结构中的几个目标。在主机上，攻击者可以通过强力攻击应用程序而破坏服务，或者攻击者可以知道应用程序在其上寄宿的服务中或者运行服务器的操作系统中存在的缺陷。
- 任意执行代码：如果攻击者可以在您的服务器上执行恶意的代码，攻击者要么就会损害服务器资源，要么就会更进一步攻击下游系统。如果攻击者的代码所运行的服务器进程被越权执行，任意执行代码所造成的危险将会增加。常见的缺陷：允许遍历路径和缓冲区溢出攻击的未打补丁的服务器，这种情况可能导致任意执行代码。
- 未授权访问：不足的访问控制可能允许未授权的用户访问受限制信息或者执行受限制操作。

网络层安全威胁

- 信息收集：可以用与其他类型系统相同的方法发现网络设备并对其进行剖析。通常，攻击者最初是扫描端口。识别出开放端口后，他们利用标题抓取与枚举的方法检测设备类型，并确定操作系统和应用程序的版本。具有这些信息后，攻击者可以攻击已知的缺陷，这些缺陷可能没有更新安全补丁。
- 嗅探：嗅探查或者窃听 就是监视网络上数据（例如明文密码或者配置信息）传输信息的行为。利用简单的数据包探测器，攻击者可以很轻松地读取所有的明文传输信息。同时，攻击者可以破解用轻量级散列算法加密的数据包，并解密您认为是安全的有用负荷。探查数据包需要在服务器/客户端通信的通道中安装数据包探测器。
- 欺骗：欺骗就是一种隐藏某人在网上真实身份的方式。为创建一个欺骗身份，攻击者要使用一个伪造的源地址，该地址不代表数据包的真实地址。可以使用欺骗来隐藏最初的攻击源，或者绕开存在的网络访问控制列表（ACL，它根据源地址规则限制主机访问）。
- 会话劫持：也称为中间人攻击，会话劫持欺骗服务器或者客户端接受：上游主机就是真正的合法主机。相反，上游主机是攻击者的主机，它操纵网络，这样攻击者的主机看上去就是期望的目的地。
- 拒绝服务（DoS/DDoS）：拒绝服务就是拒绝合法用户访问服务器或者服务。

物理层安全威胁

- 机房安全：非法进入、火灾、水灾、潮湿、雷电、静电等。
- 设备安全：盗窃、毁坏等。
- 线路安全：盗窃、窃听、干扰等。
- 介质安全：盗窃、潮湿、毁坏等。

管理层安全威胁

- 缺乏安全管理规章制度，或者没有严格执行安全管理规章制度。
- 人员安全意识不足。
- 没有及时进行系统及应用安全补丁的安装，导致系统存在安全漏洞。
- 多人共用帐号，责任无法追溯。
- 安全资料不全，无法有效指导安全生产。

2 视讯安全解决方案

2.1 视讯安全概述

视讯产品的安全方案包括以下五个部分：应用层安全解决方案保护视讯的应用程序，如：访问控制、数据安全、通信及编码安全等；系统层安全解决方案保护操作系统、数据库、中间件及应用程序依赖的服务；网络层安全解决方案保护整个网络；物理层安全解决方案从物理上保护整个系统；管理层安全解决方案通过管理使得整个系统提供的安全措施得以执行。

2.2 安全策略（Common Security Policies）

为保护视讯系统中的操作系统、数据库与网络设备，引入了安全策略，这些安全策略中，大部分规则都可应用于操作系统、数据库与应用程序。

视讯产品使用的安全策略包括但不限于以下内容：

密码管理

- 使用强密码策略与密码修改策略，如长度限制、字符组合及弱密码检测等，用于防止密码攻击。强密码策略包括：

  1、口令长度至少 6 个字符（特权用户至少 8 个字符）；

  2、口令必须包含如下至少两种字符的组合:

  - 至少一个小写字母；
  - 至少一个大写字母；
  - 至少一个数字；
  - 至少一个特殊字符：`~!@#$%^&*()-_=+\|[{}];:'",<.>/?和空格；

  3、口令不能和帐号或者帐号的倒写一样；

  若设置的口令不符合上述规则，进行警告。

- 密码修改策略包括：
  - 密码可以被管理员随时修改；
  - 修改密码时验证旧密码，验证通过才能修改；
  - 初始密码可配置为必须修改才可登录系统；

- 密码加密保存，不允许明文保存或显示；
- 在公共网络上进行口令的传输时，使用安全传输通道或者加密后传输；

认证与会话控制

- 设备外部可见的能对系统进行管理的物理接口（如串口、网口、USB 接口等）均有接入认证机制（必须输入正确的用户名和口令才能登录系统）。
- 所有能对系统进行管理的通信端口及协议（如 SSH、SNMP 等）都有接入认证机制（必须输入正确的用户名和口令才能登录系统）。
- 当用户登录时连续多次输入错误密码后此用户名被锁定，锁定状态的用户无法登录系统。
- 当业用户帐号被锁定后，系统自动在一段时间之后解锁，解锁时长可配置。
- 当业用户帐号被锁定后，系统管理员可为该用户解锁。

加密算法

- 使用标准的加密算法和密钥协商机制，不使用私有算法。
- 使用高安全等级加密算法（SHA256、AES128 等），降低敏感信息被破解的风险。
- 在口令不需要还原的场景，如用户登录设备的密码，使用不可逆的 HASH 算法对密码进行加密后存储，防止密码泄露后被解密。

安全协议

- 支持使用高级别安全协议（如 SSHV2/TLS1.0/SSL3.0/FTPS/SNMPV3）对设备进行维护管理。
- 基于 H.323 的会议支持 H.235 安全协议，基于 SIP 的会议支持 TLS 和 SRTP 安全协议。

最小授权规则

- 系统中新建的用户，默认只有最小的权限。
- 可为账号分配不同的角色，一种角色只能拥有必需的权限。

文件权限管理

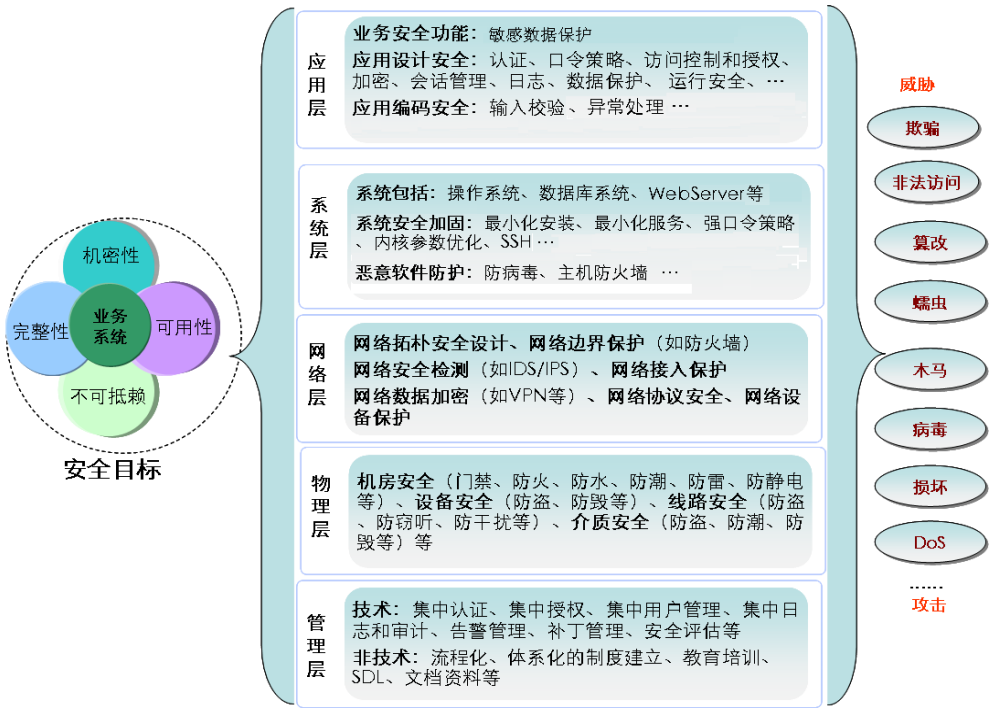
- 系统文件非授权用户不能访问。

安全日志

管理面所有的用户活动和操作指令均记录日志，日志内容能支撑事后的审计，日志有访问控制,只有管理员才能有删除权限。

2.3 安全架构（Security Architecture）

视讯产品的安全架构如下：



应用层

- 在应用层，安全方案包括认证、口令策略、访问控制与授权、加密、会话管理、日志、数据保护、运行安全等等。

系统层

- 通过对操作系统加固，确保应用程序运行在安全的环境中。
- 可通过 SSH 保证安全的远程登录。

网络层

- 通过子网或防火墙将整个网络划分为不同的网络区域，并进行 ACL 控制。

物理层

- 布署实施视频监控系统。
- 布署身份认证系统。
- 布署环境传感器以最小化火灾风险。
- 限制非授权人员进入放置鉴权设备的房间。
- 增设安全岗。

管理层

- 通过完好的规定、策略、定义好的过程、操作指引以避免系统弱点被攻击。
- 对管理员的管理也非常重要。这包括对管理员的职责管理及一些软措施。包括且不限于：发布一些政策、标准、过程与指引，以及提供相关的培训，监控系统的运行，改变控制过程等等。

2.4 视讯产品安全性

2.4.1 应用层安全

隐私保护

- 高清会议终端产品，设备管理员在 web 上对会场进行监控或拍照前，会议终端的显示界面上有提醒图标，与会人员能够感知到监控或拍照行为，与会人员随时可以通过遥控器关闭设备管理员的监控或拍照；
- 业务管理系统（RM）上面添加监控会场用于会议保障时，各会场自动播放“管理员监控会场”的提示音，开会人员能够感知此监控功能；
- 产品出于定位问题目的从客户网络导出数据时，对其中可能包含的个人数据进行过滤或匿名化处理；
- 部分客户需要会议录制和播放功能，视讯产品可在销售合同范围内提供相应的设备满足这个需求。除此之外，视讯产品不提供采集用户原始通信内容（语音和视频）的接口和功能；
- 产品不采集个人数据（姓名、住址、电话等）；

没有后门

- 产品所有的人机接口登录账号和口令通过文档向客户公开，账号可管理（启用/禁用/删除），口令可修改；
- 产品所有的命令行及参数通过文档向客户公开（命令行手册文档）；
- 产品所有的通信端口及协议通过文档向客户公开（通信矩阵文档）；
- 不存在可绕过系统安全机制（认证、权限控制、日志记录）对系统或数据进行访问的功能；

业务安全

- SMC、MCU、会议终端、智真中控设备均有内置 web 服务器，用于设备的维护管理，用户可选择安全的 https 通信方式登录设备，确保用户登录的账号和口令，以及敏感的参数信息不会被窃取。https 的通信示意图如下：

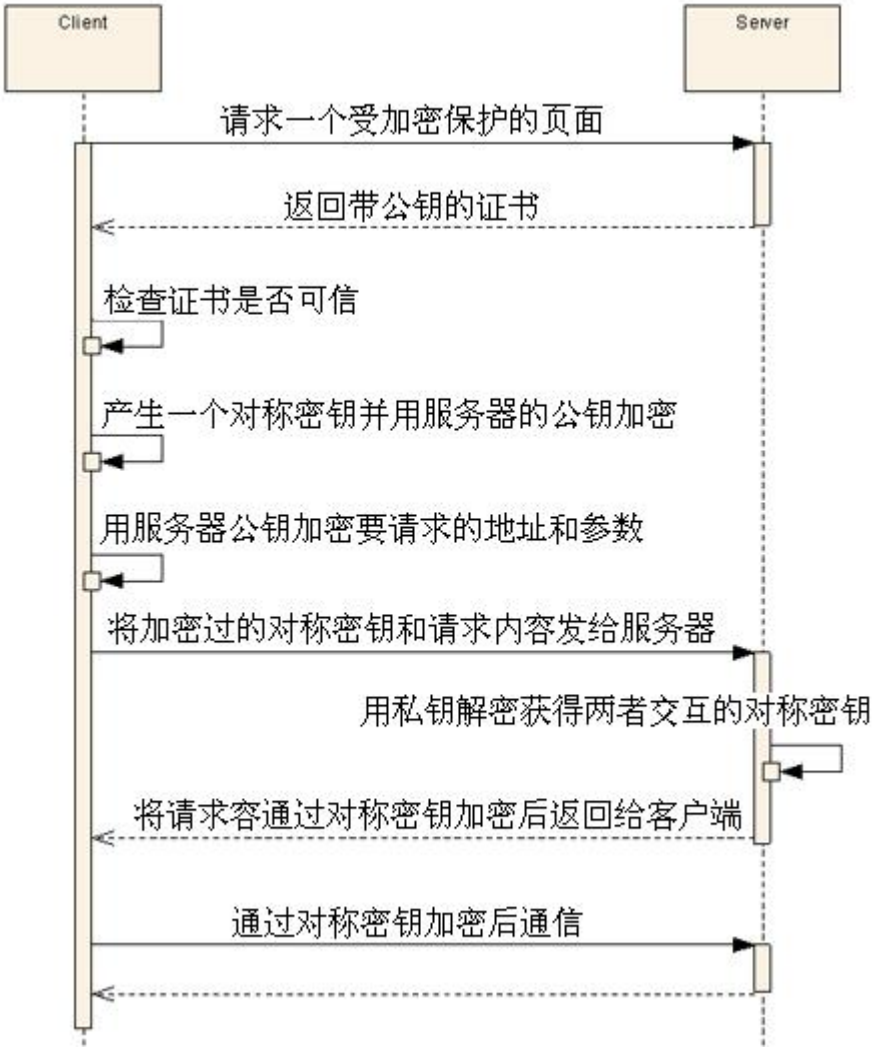


图2-1 https 通信示意图

- 基于 H.323 协议召开会议时，支持启用 H.235 安全协议，启用后系统使用 AES/DES 加密算法对通信信令和媒体流进行加密后传输，保证会议的信息安全。

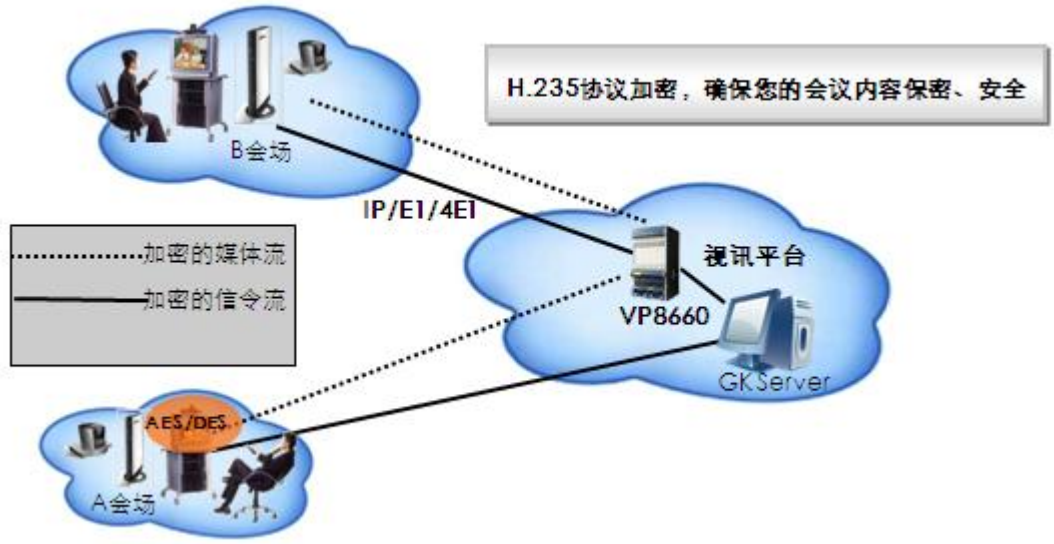


图2-2 H235 安全协议示意图

- 基于 SIP 协议召开会议时，支持启用 TLS 协议对信令进行加密，并支持启用 SRTP（安全实时传输协议）对媒体流进行加密，保证会议的信息安全。
- 主叫呼集功能允许某个用户通过会议终端主动向 GK 发起召集会议请求，并在会议终端上配置会议的相关参数（如会场名、会议接入密码、付费账号及密码等），其中包含了敏感信息，为保障敏感信息的安全传输，主叫呼集功能支持使用安全的 HTTPS 通道进行数据传输，即终端作为 HTTPS 客户端向 HTTPS 服务端（GK）发起主叫呼集请求。
- 产品在执行任何操作前，先对登录用户的权限进行判断，防止用户进行越权访问；
- 对来自其它系统的任何请求均进行参数合法性检查，防止受到畸形报文攻击。
- 支持会议接入密码、会议控制密码，防止非法用户接入会议或控制会议。

敏感数据保护

- 产品的日志、诊断调试信息、告警信息中不包含敏感数据信息；
- 产品在传输敏感数据时，使用安全传输协议，或者对数据进行加密后再传输；
- 在保存敏感数据时，对数据加密后再保存；
- 用户登录设备的口令，使用不可逆 HASH 算法（SHA256 或 MD5）加密后保存在设备的存储器中；
- 采用标准的加密算法和密钥协商机制，不使用私有算法。

安全日志与审计

- 用户登录和注销有日志记录；
- 增加、删除用户和用户属性（帐号、口令等）的变更有日志记录；

- 用户的锁定和解锁，禁用和恢复有日志记录；
- 角色权限变更有日志记录；
- 系统相关安全配置（如安全日志内容配置）的变更有日志记录；
- 重要资源的变更，如某个重要文件的删除、修改等有日志记录。
- 对系统配置参数的修改有日志记录；
- 对系统进行启动、关闭、重启、暂停、恢复、倒换有日志记录；
- 对业务的加载、卸载有日志记录；
- 软件的升级操作，包括远程升级和本地升级有日志记录；
- 所有帐户的非查询类命令行操作命令有日志记录。
- 日志有访问控制，只有管理员才能有删除权限。
- 安全日志可用于审计。

安全通信协议

- 支持通过安全的 HTTPS 协议远程登录设备内置 web 服务器进行维护管理，即 HTTP 下加入 SSL 层，视讯产品支持最新的 SSL3.0 版本，SSL 协议提供的服务主要有：
  - 通过证书认证用户和服务器，确保数据发送到正确的客户机和服务器。
  - 加密数据以防止数据中途被窃取。
  - 维护数据的完整性，确保数据在传输过程中不被改变。
- 支持通过安全的 SSHV2 协议远程登录设备进行维护管理，SSH 可以代替 TELNET。从客户端来看，SSH 提供两种级别的安全验证。

  第一种级别（基于口令的安全验证）

  客户端知道自己帐号和口令，就可以登录到远程主机。所有传输的数据都会被加密，但是不能保证你正在连接的服务器就是你想连接的服务器。可能会有别的服务器在冒充真正的服务器，即“中间人”攻击。

  第二种级别（基于密匙的安全验证）

  客户端为自己创建一对密匙，并把公用密匙放在需要访问的服务器上。如果要连接到 SSH 服务器，客户端软件就会向服务器发出请求，服务器收到请求之后，先在服务器上寻找此客户端的公用密匙，然后与客户端发送过来的公用密匙进行比较。如果两个密匙一致，服务器就用公用密匙加密“质询”（challenge）并把它发送给客户端软件。客户端软件收到“质询”之后用私人密匙解密再把它发送给服务器。使用这种认证方式，不仅加密所有传送的数据，而且“中间人”这种攻击方式也是不可能的（因为他没有私人密匙）。
- 支持通过安全的 FTPS 协议进行网络地址本的上传和下载操作，即 FTP 协议下加入 SSL 层，视讯产品支持 SSL3.0 版本。
- 支持通过安全的 SNMPV3 协议与网管系统通信，与 SNMPv1 和 SNMPv2 相比，SNMPv3 增加了三个新的安全机制：身份验证，加密和访问控制。其中，

本地处理模块完成访问控制功能，用户安全模块（USM）提供身份验证和数据保密服务。身份验证是指代理（管理站）接到信息时首先必须确认信息是否来自有权的管理站（代理）并且信息在传输过程中未被改变的过程。加密指以某种特殊的算法改变原有的信息数据，使得未授权的用户即使获得了已加密的信息，但因不知解密的方法，仍然无法了解信息的内容。

- 支持 H.235 安全协议，H.235 是 H.323 系统有关安全方面的一种标准，H.235 主要为 H.323 体系提供了身份认证、信令和媒体流加密、数据完整性功能。
- 基于 SIP 协议召开会议时，视讯产品支持通过 TLS 协议对信令进行加密，并且支持 SRTP（安全实时传输协议）对媒体流进行加密。
- 支持关闭不安全的协议（如 TELNET、FTP）。

2.4.2 系统层安全

操作系统安全

- 产品软件包发布前，经过至少一款主流的防病毒软件扫描，保证产品软件包本身不包含恶意程序或病毒。
- 基于通用操作系统的软件，提供数字签名和验证工具，在软件安装或升级过程中可对软件进行完整性验证，防止软件被篡改。
- SMC2.0 对 windows server 2008 操作系统进行加固，实现操作系统安全，遵循 CIS（Center of Internet Security）的 Windows server 2008 加固策略；

数据库安全

- SMC 2.0 默认使用最新版本的 SQL Server 2008 R2 Express with SP1；
- SMC 2.0 默认使用独立的数据库帐号进行数据库连接，且该帐号的访问权限为 SMC 2.0 需要的最低权限。不使用 sa 帐号进行数据访问，避免帐号泄露对数据库造成影响；
- SMC 2.0 对数据库账号和密码进行加密后存放本机，避免连接数据库使用的帐号和密码泄露后被解密；

Web 服务安全

- SMC 2.0 的 Web 服务依赖 Windows 的 IIS 服务，通过对 Windows 系统的加固和 Windows 最新补丁来保护 IIS 服务的安全；
- 用户可以启用 HTTPS 安全协议与 Web 服务器通信，确保数据传输的安全；
- Web 登录的密码在系统中加密存储，使用不可逆算法，防止泄露后被解密；

2.4.3 网络层安全

- 划分安全区域，通过防火墙进行隔离。

- 智真会议室通过划分交换机 VLAN，将局域网通信（LAN）与广域网通信（WAN）隔离开，保障局域网设备间通信的安全。

2.4.4 物理层安全

布署监控系统

- 建议通过视频监控保护办公区域与设备房间的安全。视频监控可以在出问题后留下足够的线索与证据以分析问题所在，并对蓄意破坏的人员有威摄作用。

布署身份识别系统

- 建议对办公区域区域与设备房间布署身份识别系统，以对进行安全监控区域的人员进行识别。
- 限制非授权人员进入放置鉴权设备的房间以保护设备不被非授权人员直接操作。

布署传感器减少火灾风险

- 建议对存放设备的房间与办公区域布署传感器，以保护工作人员的生命财产安全及设备安全。传感器可以及时发现火灾，极大地减小火灾风险。

对机箱加锁

- 建议在服务器机柜或机箱上提供有锁的情况下，对服务器机柜或机箱加锁，钥匙由专人管理。以防止服务器被有意或无意地关机、插拔器件等。

增设安全岗

- 建议对需要进行安全控制的区域，如办公区域、生产厂区等设置安全岗，以对进入厂区的人员进行登记与监控。

2.4.5 管理层安全

组织与过程

- 建立安全管理规章制度，并严格执行安全管理规章制度。
- 对相关人员进行安全意识培训，以避免因安全意识淡薄带来安全风险。
- 建立安全规范，并对操作人员进行足够的培训，以使安全措施能以得到有效的执行。
- 定期对安全日志进行检查，及时发现与处理安全隐患。

帐号与权限管理

- 为每个有权限的人分配必要的权限，防止多人共用帐号，造成责任无法追溯。

系统备份

- 定期为数据库系统进行全部及增量备份，把因安全问题带来的损失降到最小。

安全保障

2.5 安全资质

华为认为客户和产品安全问题的至关重要，并尽力推动产品的安全功能提高和质量研究进步。

华为于 2004 年 7 月通过 BSS7799 认证，其后更新为 ISO/IEC27001。2007 年 8 月，华为复检后获得为期 3 年的新认证。

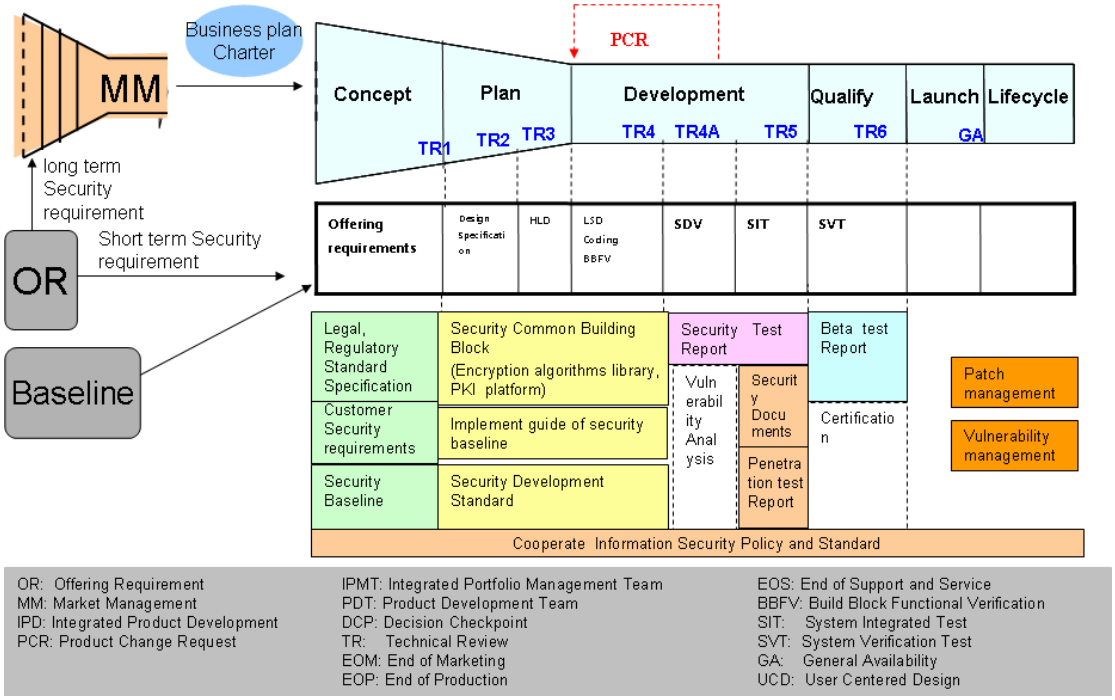
产品安全保证机制贯穿华为的产品开发流程 IPD。安全相关的问题，包括功能和特性在每一个阶段，如构思，设计和验证等都被考虑在内。在安装和现场支持中也采用安全保证机制。

华为建立安全技术管理组 (TMG) 监督和指导每一个产品的安全行为。特别安全解决方案部门对产品的安全性解决方案提供咨询，评估和实施。

华为和其开发团队，包括产品都遵循行业标准，法律和法规，并尊重运营商和他们客户的业务、技术秘密和隐私。我们尊重并理解运营商的安全政策，我们已经准备好，以帮助运营商强制实施企业安全策略。

2.6 安全保证过程

安全已经成为一个重要的电信运营商关注的课题。0.01％的安全事故意味着彻底的失败。遵循正确的机制是保证产品安全特性的最高效的原则。下面的图片描绘产品开发过程中的安全应用流程。



华为建立了专业的安全解决方案部门为电信运营商提供先进的解决方案，并支持指导，监督所有产品周边的安全问题。产品线团队和产品开发团队拥有特别的团队或角色，负责在产品开发过程中的安全问题，并确保安全质量。每个产品团队会在每年的产业技术进步和业务发展调查后，调整自己的短期安全计划和长期安全策略。QA 部门有相应的团队监督检查产品的安全计划和进度。

良好的组织和严格高效的流程管理使产品满足运营商所需的安全质量并提供高品质的长期保证。

3 术语表（Glossary）

英文缩写	英文全称	中文全称
SMC	Service Management Center	业务管理中心
MCU	MultiPoint Control Unit	多点控制单元
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer	超文本传输安全协议
SSH	Secure Shell	安全外壳协议
SNMP	Simple Network Management Protocol	简单网络管理协议
FTPS	FTP-over-SSL	文件传输安全协议