第 33 卷 第 7 期 计 算 机 工 程 2007 年 4 月
Vol.33 No.7 Computer Engineering April 2007
·开发研究与设计技术· 文章编号：1000—3428(2007)07—0269—03 文献标识码：A 中图分类号：TP393.08

加强认证的 IPSec 多媒体通信系统设计

聂 丹
(辽东学院信息技术学院，丹东 118003)

摘 要：针对 H.323 多媒体通信系统，从整体角度出发，提出了基于 IPSec 的安全系统思想。设计中为 H.323 多媒体通信体系各个阶段的通信提供了安全机制并进行了有效论证。通过将 IPSec VPN 网关与 H.323 网守的联动机制，将 IPSec 无缝集成进入 H.323 的系统框架中。为实施有效的 IPSec 保护，针对 IPSec 的策略管理提出了安全便捷的解决方案。

关键词：H.323；IPSec；虚拟专用网

Design of Strengthened IPSec Authentication Multimedia Communications

NIE Dan
(Information and Technology Institute, Liaodong University, Dandong 118003)

【Abstract】 This article in view of the H.323 multimedia communications system, embarked from the overall angle, proposes thought based on the IPSec safety system. The design provides H.323 multimedia communications system for all stages of communication with the security and effective verification mechanism. At the same time, the IPSec VPN gateway and H.323 network regard joint mechanism, IPSec is integrated into H.323 system framework. In the end, for the implementation of effective IPSec protection against IPSec management strategy, security convenient solution is proposed.

【Key words】 H.323; IPSec; Virtual private network (VPN)

1 概述

在实施多媒体通信的技术中，H.323 标准[1]作为目前在IP网中最为流行的实时多媒体通信系统标准，已经被广泛应用于IP电话、实时视频会议、多媒体新闻发布、远程教育、远程医疗和会诊、远程科研合作和工程设计等互联网信息服务的许多方面。H.323 协议为通过基于IP网络(例如 Internet)进行音频、视频与数据通信提供了一个可以遵循的标准。采用H.323 标准，可以对IP网络中的多媒体流实施有效的编/解码、传输及控制。

另一方面，在安全领域，虚拟专用网(Virtual Private Network，VPN)[2]可以以较高的性价比作为企业网在因特网等公共网络上的延伸，通过一个私有的通道在公共网络上创建一个安全的私有连接，保护信息流的通信安全。这一技术也得到了广泛的应用。

在用来实现虚拟专用网的众多技术当中，IPSec 协议是一个应用广泛、开放的 VPN 安全协议。IPSec 用密码技术提供以下安全服务：接入控制，无连接完整性，数据源认证，防重放，机密性，数据完整性。IPSec 协议可以设置成在两种模式下运行：一种是隧道(tunnel)模式，另一种是传输(transport)模式。

事实上，在 H.323 标准框架中，采用 IPSec 加密数据报文，具有如下优点：

(1)IPSec 是现今比较通用而且使用广泛的 IP 安全协议，而且已经拥有比较成型的模型可以参考引用。同时 IPSec 协议本身具有较高的安全性。

(2)IPSec 作为一种位于应用程序之下的对用户透明的加密层，在对数据包提供安全保证的同时又不影响系统数据的应用。

(3)相对直接修改应用协议实现安全机制而言，IPSec 在通用性和可移植性上具有较大优势。

通过以上几点的描述，得出了设计基于 IPSec 的自适应多媒体通信安全系统技术的主要原因。

2 设计目标

要满足H.323 标准架构下多媒体通信的安全性要求，就必须针对H.323 各阶段各组件间的通信过程，在用户身份认证、数据完整性、数据加密及密钥管理等安全机制方面进行综合全面的考虑[3]。

同时，H.323 标准作为一个控制多媒体通信的标准框架，对于系统通信的实时性、可用性及灵活性亦提出了要求。对于 H.323 框架的安全保护机制同时应该满足尽可能少地影响系统性能、尽可能地保证视频服务的质量、尽量简化终端用户的使用程序以及尽量方便域管理者的配置管理工作。

基于以上需求，本文提出以下的设计目标，用来构筑一个安全的多媒体通信系统。

(1)基于 IPSec 的数据保密性及数据完整性安全机制；

(2)基于 Verifier-based 机制的身份鉴别机制；

(3)H.323 网守组件与 IPSec VPN 网关的集成联动机制；

(4)在应用 IPSec 策略保护实时多媒体流通信时提供一定程度的 QoS 支持。

作者简介：聂 丹(1971－)，女，讲师，主研方向：计算机软件开发
收稿日期：2006-05-11 **E-mail：**nd9906@126.com

3 系统设计

3.1 整体结构

在基于 IPSec 的自适应安全多媒体通信系统中，由 IPSec VPN 网关隔离出多媒体通信安全域，由安全网守负责对安全域中的其它组件(包括终端和多点控制单元)实施访问控制策略。

安全域内的组件与安全网守以 SRP 协议互相完成身份认证，并依靠身份认证过程中协商出的共享密钥保证组件与网守间 RAS 信道的通信安全。IPSecVPN 的策略由安全策略服务器集中管理，并通过策略管理安全协议完成安全策略的安全及透明的分发管理。不同安全域间的多媒体流通信以 IPSec 隧道保证通信安全。

IPSec VPN 网关与安全网守之间实现联动机制，通过延迟评估－反馈机制实现安全系统中针对 IPSec 承载多媒体流的部分 QoS 功能。

3.2 安全网守

(1)网守必须支持的 H.323 功能

1)地址翻译；

2)呼叫接纳控制；

3)带宽控制；

4)呼叫授权。

(2)注册网守的身份认证机制

为了实现多媒体通信系统的安全性，首先我们必须保证在呼叫的初始阶段，即 RAS 信道的初始通信过程中，终端能安全地与网守实现身份认证。

身份认证机制的要求在有关 RAS 协议的安全性分析中有描述，概括起来包括：认证的安全性要求，认证的双向性要求，认证的方便性及性能要求和认证的密钥协商需求。基于身份认证机制的这些要求，选择基于安全远程密码协议(SRP)的身份认证机制。

在认证的安全性方面，首先 SRP 协议是基于鉴别符的认证机制，即认证服务器上只保存与密钥不等价的鉴别符。鉴别符由密钥产生，但不能反向推出密钥。与在服务器上直接保存用户密钥的明文等价的认证机制相比，安全性得到很大提高。

在认证的双向性方面，由 SRP 协议的通信过程可知，SRP 协议能同时为通信双方提供身份验证，即具有双向性认证的特点。

在认证的方便性方面，SRP 协议仅需用户提供一个有限的口令，同时 SRP 协议只需要身份认证的双方参与，不需要密钥服务器、仲裁者、CA 等可信第三方参与。

与此同时，SRP 协议通过协商，能够生成一个新的共享密钥，满足了 H.323 系统对于身份认证协议的最后一个要求。

3.3 H.323 架构与 IPSec 的集成与联动设计

为满足 H.323 架构与 IPSec 的集成联动，我们设计将加强了安全性的 H.323 网守组件与 IPSec VPN 的安全网关相结合，成为 SecGK-IPSec 组件。

安全网守对域内的组件实施管理；IPSec VPN 安全网关对网守所管理的域提供安全隔离并为域间的终端通信提供 IPSec 隧道保护；为了建立安全的 IPSec 隧道，由分级的安全策略集中机制对 IPSec 策略进行管理；由 IKE 在 IPSec 策略的指导下创建 IPSec 隧道必须的安全联盟 SA；同时 GK 与 IPSec VPN 之间采用联动机制以实现自适应系统的功能。SecGK-IPSec 的结构如图 1 所示。

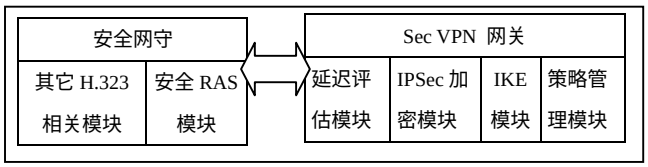

图 1 SecGK-IPSec 结构设计

(1)针对 H.323 系统的 IPSec 分级安全策略

本文采用了分级的IPSec安全策略，将 IPSec 的安全策略分为基于SA的策略(SA Policy)以及基于数据包的策略(Packet Policy)。其中，SA Policy用于指导IPSec 安全联盟 SA 的建立，SA Policy中描述了SA必须配置的参数，包括源/目地址、应用协议、所用算法/长度等[4]；而基于数据包的策略用于在 IPSec 安全联盟建立之后，在数据包一级对用户的安全访问进行进一步的控制，这一策略通过对安全联盟SA的扩展加以实现。同时SA也相应地区分为两种：实施访问规则的SA以及不实施访问规则的SA，以SPI区别。

(2)H.323 呼叫与 IPSec 策略行为联动

利用 IPSec 对 H.323 呼叫过程提供安全保护，应该在呼叫初始阶段制定或更新 IPSec 的安全策略，以提供对相关信息的 IPSec 安全处理；同时在呼叫结束阶段撤销或更新相应的 IPSec 安全策略，结束 IPSec 处理。这一过程需要通过 H.323 呼叫与 IPSec 安全策略的联动加以解决。

通过 H.323 呼叫与 IPSec 策略联动对呼叫过程实施 IPSec 保护遵循如下流程：

1)呼叫请求过程

在 IPSec 安全机制保证的 H.323 系统中，当安全网守在 RAS 信道上收到 ARQ 消息的呼叫接入请求时，对符合授权的呼叫请求，除了完成通常的地址翻译，网守必须与 IPSec 模块联动，进行 IPSec 安全联盟 SA 保护下安全隧道的建立。

2)建立 IPSec 安全联盟过程

在基于 SA 的策略指导下，可以完成 SA 的建立。在建立 IPSec 安全联盟 SA 过程中，即通过 IKE 的第一阶段协商后，由发起方在本地 SA Policy 指导下提出一个 SA 提案，响应方基于本地 SA Policy 接受符合要求的提案请求，接着进行后续的协商过程直至完成 SA 的建立。

3)扩展 IPSec 安全联盟过程

当用户需要进一步的安全访问控制时，必须先向 IPSec 递交在安全网守中完成的身份认证信息，通过身份认证后，IPSec 将用户的身份信息(如 IP 地址)写入本地 IPSecSA 中，修改 SA 的规则表，完成 SA 的扩充。

当 SA 的扩充完成以后，由 IPSec 通知安全网守，安全信道已经建立，该次呼叫请求可以被允许接入。由安全网守通知终端进行后续呼叫通信。

4)呼叫通信及 IPSec 处理过程

当 H.323 后续通信报文经过 IPSec VPN 网关时，在发送端，首先检查是否有匹配的 IPSec SA，如果没有或者丢弃包，或者启动 IKE 协商；如果有匹配的 SA 存在，则在扩展后该 SA 的规则表中查找规则，查询该用户的身份是否符合规则，如果符合，则应用 SA，通过 IPSec 安全机制发送出去。如果找不到符合的规则，则可以丢弃该包。在接收端用类似方法处理。

5)呼叫撤销过程

呼叫结束时，网守应通知 IPSec 更改 SA 规则表或删除 SA。

(3)H.323 呼叫与 IPSec 性能评估联动

由IPSec VPN对H.323呼叫中除RAS信道之外的呼叫通信提供安全保护时，将不可避免的使系统性能受到影响。为尽可能地保障多媒体流的传输质量，我们将IPSecVPN的性能评估与 H.323 呼叫管理进行联动设计。性能评估采用传输延迟作为采样依据，通过统计预测算法，进行评估预测。对于延迟的评估预测结果将通过网守与IPSec之间的通信提交给安全网守[5]。当性能评估超过警戒阈值时，由网守实施域内控制策略以改善性能或防止性能的进一步恶化，实现有限条件下的QoS。通常的域内控制策略包括停止接受新的终端呼叫请求以及针对不同优先级运用网守的带宽管理机制加以控制。

4 结束语

本文主要对应用IPSec实现的H.323 安全多媒体通信系统进行了系统设计。系统设计的目标是为H.323 协议族提供全面的各协议兼容的安全机制。本文通过将IPSecVPN网关作为安全组件引入H.323 标准框架，以及为RAS信道提供的加强的安全认证机制，达到了这一设计目标[6]。

在结构设计中，首先选择了安全远程密码协议(SRP)来实现身份认证，同时针对 H.323 安全系统的实际需求，对 SRP 进行了协议优化以及安全性增强。然后针对为实时多媒体流传输提供的 IPSec 保护设计了 IPSec 与 GK 之间的 QoS 联动机制。整个系统的设计体现了对多媒体通信安全系统在安全性、实时性以及性能方面的要求。

参考文献

1 柳葆芳, 张亚娟. H. 235-多媒体终端安全与加密建议[J]. 信息工程大学学报, 2002, 3(2): 9-12.

2 刘　虎, 李芝棠. 基于域名的 VPN 策略管理系统[J]. 华中科技大学学报(自然科技版), 2003, 31(增刊): 174-176.

3 孔　晖, 徐秋亮, 郑志华. 几种典型的认证 Diffie-Hellman 型密码共识协议的分析与比较[J]. 计算机工程与应用, 2001, 37(18): 72-74.

4 王　琦, 马　跃, 喻　炜. VoIP 中为保证语音质量所采用的关键技术[J]. 中国数据通信, 2002, 15(2): 25-29.

5 Qiong Li, Mills D L. Jitter-based Delay-boundary Prediction of Wide-area Networks[J]. IEEE/ACM Transactions on Networking, 2001, 9(5): 578-590.

6 汪　雁, 黄本雄. DiffServ 网络的拥塞控制和带宽保证[J]. 计算机工程与应用, 2003, 39(3): 177-180.

（上接第 221 页）

参考文献

1 IEEE Standard Test Access Port and Boundary Scan Architecture[Z]. IEEE computer Society, 2001.

2 Altera. IEEE 1149.1 (JTAG) Boundary Scan Testing[Z]. http://www.altera.com.cn.

3 Altrea.ug_bbii ByteBlaster II Download Cable User Guide[Z]. http://www.altera.com.cn.

4 侯整风, 胡　军. VC+ +实现计算机并口的直接输入/输出[J]. 淮南工业学院学报, 2002, 22(2): 35-37.

（上接第 242 页）

4 Kim C M, Choi K H, Cho Y B. Hardware Design of CMAC Neural Network for Control Applications[Z]. 2003: 953-958.

5 Altera Corporation. QuartusII Version 4.0 Software[EB/OL]. 2004. http://www.altera.com.cn/literature/manual/intro_to_quartus2.pdf.

6 Altera Corporation. DSP Builder Version 3.0 Software[EB/OL]. 2004. http://altera.com.cn/literature/ug/ug_dsp_builder.pdf.

7 刘金锟. 先进 PID 控制及其 MATLAB 仿真[M]. 北京: 电子工业出版社, 2003.

（上接第 268 页）

在图 3 中每个活动节点都是一个有限执行的自动机，当接受订单完成后，活动“检查库存”和“检查客户”同时被创建，处于“待激活态”。此时，这些活动可由工作流相关人员挂起，在相关部门执行该活动时，则处于“激活态”；检查完毕，给出结论，两活动均到达“完成态”，其他节点类似。“客户检查”状态图如图 4。

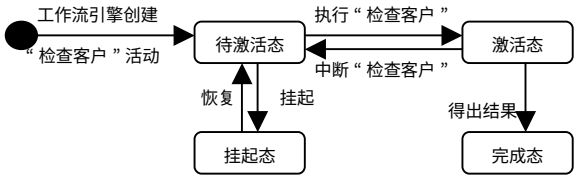

图 4 “检查客户”活动对应状态

以此订单处理工作流建模为基准，可以构造出整个基于工作流技术的柔性 PLM 系统模型。在此基础上，在系统模型分析论证之后，借助适合于本系统的技术进行具体流程实现。

4 总结

产品全生命周期管理是企业信息化的关键技术，设计出合理有效的 PLM 系统，可以使企业提高市场竞争力、提高产品质量和竞争力。本文提出的基于工作流技术的柔性 PLM 系统框架，柔性理论贯穿整个数据控制流程，我们已成功开发出了软件系统并用于一些制造企业，取得很好的效果，这种设计思想可为管理软件开发提供借鉴作用。

参考文献

1 葛杏卫, 段国林, 陶利波, 等. 基于 J2EE/XML 的产品生命周期管理系统体系结构[J]. 河北工业大学学报, 2004, 33(5).

2 申利民柔. 性软件开发技术[M]. 北京: 国防工业出版社, 2003-09.

3 沈建新, 周儒荣. 产品全生命周期管理系统框架及关键技术研究[J]. 南京航空航天大学学报, 2003, 35(5).

4 宁　波. J2EE 结合 UML 在企业级系统中的应用[J]. 计算机工程与科学, 2004, 26(3)

5 李　炜, 张　利, 张建军. 并行环境下的柔性 PDM 系统框架研究[J]. 合肥工业大学学报, 2004, 27(4).

6 谢久红, 刘延林, 谢建平. 基于 Web 的协同设计环境下产品生命周期管理系统研究[J]. 计算机辅助工程, 2003, 25(2).

7 耿翠霞, 傅铅生, 姚　雄. 产品生命周期管理(PLM)技术研究[J]. 电气技术与自动化, 2004, 33(5).