ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25068.2—2012/ISO/IEC 18028-2:2006

信息技术　安全技术　IT网络安全 第2部分:网络安全体系结构

Information technology—Security techniques—IT network security—Part 2:Network security architecture

(ISO/IEC 18028-2:2006,IDT)

2012-06-29 发布　　2012-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T 25068《信息技术　安全技术　IT 网络安全》分为以下 5 个部分：

——第 1 部分：网络安全管理；

——第 2 部分：网络安全体系结构；

——第 3 部分：使用安全网关的网间通信安全保护；

——第 4 部分：远程接入的安全保护；

——第 5 部分：使用虚拟专用网的跨网通信安全保护。

本部分为 GB/T 25068 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用翻译法等同采用国际标准 ISO/IEC 18028-2:2006《信息技术　安全技术　IT 网络安全　第 2 部分：网络安全体系结构》。

根据国情和 GB/T 1.1 的规定，做了如下一些编辑性修改：

——原文 CCITT X.800 中的内容已在本部分引用的国家标准 GB/T 9387.2—1995 中体现，故本部分不再引用 X.800。

——在原文正文里使用的缩略语没有全部反映在第 4 章中，本部分在其中做了增补，增加的缩略语在其页边切口用单竖线“|”指示。

——为避免干扰章节编号，第 5 章中几个问题的数字编号改为字母编号。

——由于我国尚未有隐私和数据保护的相关法律法规，故在 6.8 中删掉“依据国家隐私和数据保护的法律法规”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息安全标准化技术委员会(TC 260)提出并归口。

本部分起草单位：黑龙江省电子信息产品监督检验院、中国电子技术标准化研究所。

本部分主要起草人：黄俊强、王希忠、方舟、马遥、王大萌、张清江、宋超臣、段志鸣、树彬、上官晓丽、许玉娜、王运福。

引　言

通信和信息技术业界一直在寻找经济有效的全面安全解决方案。安全的网络应受到保护，免遭恶意和无意的攻击，并且应满足业务对信息和服务的保密性、完整性、可用性、抗抵赖、可核查性、真实性和可靠性的要求。保护网络安全对于适当维护计费或使用信息的准确性也是必要的。产品的安全保护能力对于全网的安全(包括应用和服务)是至关重要的。然而，当更多的产品被组合起来以提供整体解决方案，互操作性将决定这种解决方案的成功与否。安全不一定只是对每种产品或服务的单线关注，而必须以促进全面的端到端安全解决方案中各种安全能力交织的方式来开发。因此，GB/T 25068 的目的是为 IT 网络的管理、操作和使用及其互连等安全方面提供详细指南。组织中负责一般 IT 安全和特定 IT 网络安全的人员应能够调整 GB/T 25068 中的材料以满足他们的特定要求。GB/T 25068 的主要目标如下：

——GB/T 25068.1 定义和描述网络安全的相关概念，并提供网络安全管理指南——包括考虑如何识别和分析与通信相关的因素以确立网络安全要求，还介绍可能的控制领域和特定的技术领域(相关内容在 GB/T 25068 的后续部分中涉及)；

——GB/T 25068.2 定义一个标准的安全体系结构，它描述一个支持规划、设计和实施网络安全的一致框架；

——GB/T 25068.3 定义使用安全网关保护网络间信息流安全的技术；

——GB/T 25068.4 定义保护远程接入安全的技术；

——GB/T 25068.5 定义对使用虚拟专用网(VPN)建立的网络间连接进行安全保护的技术。

GB/T 25068.1 与涉及拥有、操作或使用网络的所有人员相关。除了对信息安全(IS)和/或网络安全及网络操作负有特定责任的、或对组织的全面安全规划和安全策略开发负有责任的管理者和管理员外，还包括高级管理者和其他非技术性管理者或用户。

GB/T 25068.2 与涉及规划、设计和实施网络安全体系结构方面的所有人员(例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管)相关。

GB/T 25068.3 与涉及详细规划、设计和实施安全网关的所有人员(例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管)相关。

GB/T 25068.4 与涉及详细规划、设计和实施远程接入安全的所有人员(例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管)相关。

GB/T 25068.5 与涉及详细规划、设计和实施 VPN 安全的所有人员(例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管)相关。

信息技术　安全技术　IT网络安全
第2部分:网络安全体系结构

1　范围

GB/T 25068的本部分规定了用于提供端到端网络安全的网络安全体系结构。

本部分适用于体系结构能应用于关注端到端安全且独立于网络下层技术的各种类型的网络。其目的是作为开发详细的端到端网络安全建议的基础。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(ISO 7498-2:1989,IDT)。

3　术语和定义

GB/T 9387.2—1995中界定的下列术语和定义适用于本文件。

3.1

访问控制　access control

防止未授权使用资源,包括防止以未授权方式使用某一资源。

3.2

数据原发鉴别　data origin authentication

确认接收到的数据的来源是所声称的。

3.3

对等实体鉴别　peer-entity authentication

确认某一关联中的对等实体是所声称的实体。

3.4

可用性　availability

已授权实体一旦需要就可访问和使用的特性。

3.5

保密性　confidentiality

使信息不泄漏给未授权的个人、实体或过程或不使信息为其利用的特性。

3.6

数据完整性　data integrity

数据未经未授权方式修改或破坏的特性。

3.7

原发证据抗抵赖 non-repudiation with proof of origin

为数据接收方提供数据源证据的安全服务。

注 1：这将防范发送方否认发送数据或其内容的任何企图。

注 2：改编自 GB/T 9387.2—1995。

3.8

交付证据抗抵赖 non-repudiation with proof of delivery

为数据发送方提供数据交付证据的安全服务。

注 1：这将防范接收方否认接收数据或其内容的任何后续企图。

注 2：改编自 GB/T 9387.2—1995。

3.9

隐私 privacy

每个人都享有的控制或影响与其相关的什么信息可被收集和存储以及这些信息可被何人或对何人泄露的权利。

4 缩略语

ASP	应用服务提供商(Application Service Provider)
ATM	异步传输模式(Asynchronous Transfer Mode)
DHCP	动态主机配置协议(Dynamic Host Configuration Protocol)
DNS	域名系统(Domain Name System)
DS-3	DS3 数字信号(Digital Signal Level 3)
Ipsec	IP 安全协议(IP Security Protocol)
MD5	消息摘要第 5 版(Message Digest Version 5)
Megaco/H.248	媒体网关控制协议(Media Gateway Control Protocol)
MPLS	多协议标签交换(Multi-protocol Label Switching)
OAM&P	操作、管理、维护和配置(Operations Administration Maintenance and Provisioning)
OSI	开放系统互连(Open Systems Interconnection)
POP	邮局协议(Post Office Protocol)
PSTN	公用电话交换网(Public Switched Telephone Network)
PVC	永久虚电路(Permanent Virtual Circuit)
QoS	服务质量(Quality of Service)
SHA-1	安全散列算法(Secure Hash Algorithm)
SIP	会话发起协议(Session Initiation Protocol)
SMTP	简单邮件传输协议(Simple Mail Transfer Protocol)
SNMP	简单网络管理协议(Simple Network Management Protocol)
SONET	同步光纤网络(Synchronous Optical Network)
SS7	信令系统 7(Signalling System #7)
SSL	安全套接层(加密和鉴别协议)(Secure Socket Layer (encryption and authentication protocol))
TLS	传输层安全(加密和鉴别协议)(Transport Layer Security(encryption and authentication protocol))

VLAN　　虚拟局域网(Virtual Local Area Network)

5　网络安全参考体系结构

该参考体系结构被创建来应对服务提供商、企业、客户的全球安全挑战，适用于无线、光纤和有线的语音、数据和聚合网络。在本部分的内容中“参考”一词与“体系结构”一词结合，用于表达以下含义：该规范提供一个高层次安全体系结构实例，可以此体系结构为基础，来为不同网络设计更详细的安全解决方案。对网络基础设施、服务和应用而言，该参考体系结构处理其管理、控制和使用的安全关注点。该参考体系结构提供全面的、自顶向下的、端到端的网络安全视图并且能应用于网络元素、服务和应用，以预测、检测和改正安全脆弱性。

该参考体系结构将一组复杂的、与端到端网络安全相关的特性按照逻辑划分到单独的体系结构组件中。这种划分支持端到端安全的系统化方法，此类方法可用于规划新的安全解决方案和评估现有网络的安全。

该参考体系结构处理的是覆盖以下至关重要的问题的网络安全需求：

a)　何种信息需要得到保护？

b)　什么是安全风险？需要何种保护来管理这些风险？

c)　哪些不同类型的网络活动需要得到保护？

d)　哪些不同类型的网络设备及设施分组需要得到保护？

宜进行风险评估以区分保护要求的优先次序并帮助确立安全体系结构的适当安全措施。

这些问题由体系结构的3个组件(安全维、安全面和安全层)来处理。

这个多面参考体系结构描述的原则能够应用于独立于网络技术或者协议栈中位置的各种网络。

后面章节针对主要安全威胁来详细描述体系结构元素及其功能。

6　安全维

通常在风险管理过程中识别适当的安全措施以管理或减轻评估风险。安全维引入一组用于实施特定网络安全方面的安全措施。安全维的概念并不局限于网络，在应用或终端用户信息的环境中也可使用。此外，安全维适用于服务提供商或向客户提供安全服务的企业。安全维包括：(1)访问控制；(2)鉴别；(3)抗抵赖；(4)数据保密性；(5)通信流安全；(6)数据完整性；(7)可用性；(8)隐私。

适当设计和实现的安全维支持为特定网络规定的安全策略，使得安全管理容易设置规则。

6.1　访问控制安全维

访问控制安全维提供对使用网络资源的授权。访问控制确保只允许得到授权的人员或设备访问网络元素、存储的信息、信息流、服务和应用。例如，基于角色的访问控制(RBAC)提供不同的访问级别以保证人员和设备只能对已授权的网络元素、存储的信息和信息流进行访问并在其上执行操作。

6.2　鉴别安全维

鉴别安全维的作用是确认通信实体的身份或其他授权属性。当鉴别被参与通信的实体的授权或访问控制(如人员、设备、服务或应用)使用时，它确保所声称身份的有效性和提供实体未企图冒充或未授权重放以前通信的保证。使用基于用户身份标识和口令对、双因子鉴别(如令牌)、生物统计特征技术的鉴别方法被广泛使用。

6.3 抗抵赖安全维

抗抵赖安全维提供技术手段，通过使各种与网络相关行动的证据（例如责任、意图或承诺的证据、数据原发证据、所有权证据、资源使用证据）可用，来防止个人或实体否认已执行与数据相关的特定动作。它有助于确保证据的可用性，这些证据能作为某种已发生的事态或动作的技术证据呈现给第三方。然而，需注意的是通过技术方法提供的抗抵赖不会导致必要的法律结论。经常使用密码学的方法来提供抗抵赖。

6.4 数据保密性安全维

数据保密性安全维保护数据免遭未授权的泄漏。加密是一种经常用于确保数据保密性的方法。访问控制列表和文件权限是有助于保持数据保密性的方法。

6.5 通信流安全维

通信流安全维确保信息只在授权端点之间流动（信息在这些端点之间流动时不会被转向或拦截）。通信流安全维的安全机制不能抵御修改/损坏；这是数据完整性的功能。MPLS 隧道、VLAN 和 VPN 是能提供通信流安全的技术实例。

6.6 数据完整性安全维

数据完整性安全维确保数据的正确性或准确性（亦即数据只能被授权的过程或授权的人或设备的动作处理）。数据得到保护免遭未授权的修改、删除、创建和复制，且提供这些未授权活动的指示。散列消息鉴别码方法（如 MD5、SHA-1）常用于确保数据的完整性。

6.7 可用性安全维

可用性安全维确保未因对网络元素、存储的信息、信息流、服务和应用的授权访问影响网络而拒绝这些事态。灾难恢复解决方案也包含在此范畴中。

6.8 隐私安全维

隐私安全维对可能源自网络活动观察的任何信息（通信方的身份或任何数据——包括包头——属于此方承载的任何活动）提供保护。这些信息的实例包括用户已访问的万维网站点、用户的地理位置、服务提供商网络中的 IP 地址和设备的 DNS 名称。网络地址转换（NAT）和应用代理是能用于隐私保护技术的实例。隐私安全维也宜对个人信息的收集、处理和传播提供适当的保护结构和控制措施。

7 安全层

为了提供端到端安全解决方案，第 6 章中描述的安全维必须应用于网络设备和设施分组的层次结构，称作安全层。这个参考体系结构定义 3 个安全层，即基础设施安全层、服务安全层和应用安全层，它们相互依赖以提供基于网络的解决方案。

各个安全层是用于安全网络解决方案的一组使能器：基础设施安全层使能服务安全层、服务安全层使能应用安全层。该参考体系结构处理每一层都有不同的安全脆弱性的事实并提供以最适合特定安全层的方式来对抗潜在威胁的灵活性。是否较高级别必须假定较低级别安全已起到想要的作用或者是否它们宜包含检测失效的过程，其决定权留给实施。

宜注意的是安全层(前面已定义)有着与 OSI 层不同的含义。

安全层通过提供网络安全的连续视角来识别安全必须被置于产品和解决方案中的何处。例如,首先为基础设施安全层处理安全脆弱性,然后为服务安全层,最后为应用安全层处理安全脆弱性。安全维识别需要在每个安全层中处理的域。图 1 描述每个安全维的机制如何应用于安全层,以降低每层中存在的脆弱性,从而缓解安全攻击。

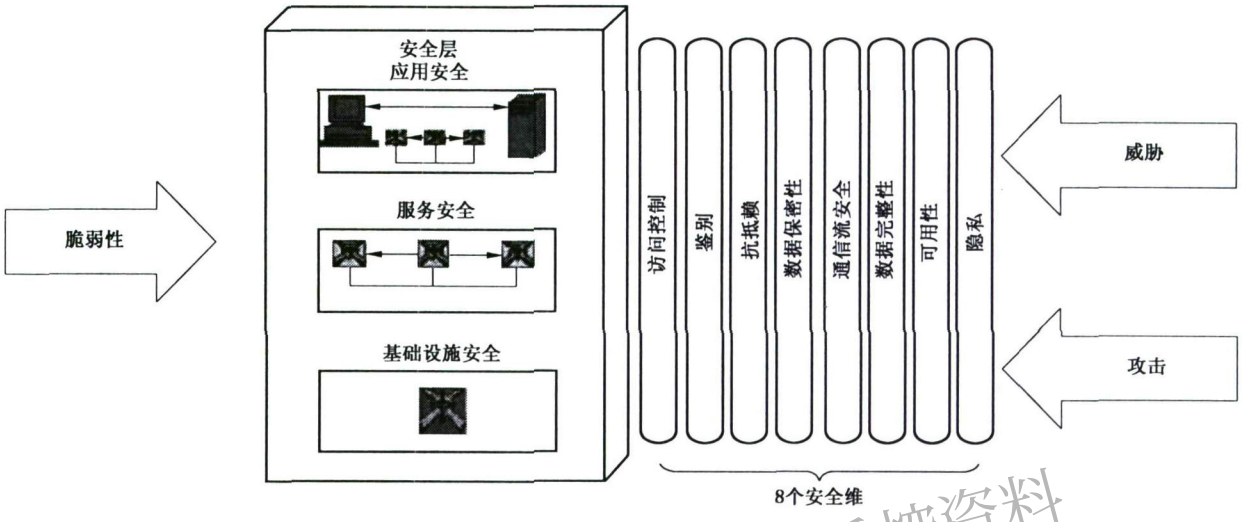

图 1 对安全层应用安全维

7.1 基础设施安全层

基础设施安全层由通过安全维实施的机制所保护的网络传输设施和单个的网络元素组成。基础设施安全层代表网络、网络服务及应用的基本构建块。属于基础设施安全层的组件实例有单个路由器、交换机和服务器以及单个路由器、交换机和服务器之间的通信链路。

7.2 服务安全层

服务安全层处理服务提供商提供给客户的服务的安全。这些服务的范围从基本传输和连通性直到提供互联网访问(如鉴别、授权和计费服务、动态主机配置服务、域名服务等)所必需的服务使能器以及免费电话服务、QoS、VPN、定位服务、即时消息等增值服务。服务安全层用于保护服务提供商及其客户,这两者均为潜在的安全威胁目标。例如,攻击者可能试图否认服务提供商提供服务的能力,或者他们可能试图中断服务提供商(如企业)对某个客户的服务。

7.3 应用安全层

应用安全层关注被服务提供商的客户访问的、基于网络的应用的安全。这些应用被网络服务使用且包括基本的文件传输(如 FTP)和万维网浏览应用、目录、基于网络的语音消息和电子邮件之类的基本应用以及客户关系管理、电子/移动商务、基于网络的培训、视频协同之类的高端应用。基于网络的应用可由第三方应用服务提供商(ASP)、也起到 ASP 作用的服务提供商或由在自己的(或租用的)数据中心运营它们的企业来提供。在这一层中有 4 个潜在的安全攻击目标:应用用户、应用提供商、由第三方集成者提供的中间件(如万维网代管服务)以及服务提供商。

8 安全面

安全面是由为安全维实施的机制所保护的某种类型的网络活动。这一参考体系结构定义 3 个安全面来表示网络中发生的三种受到保护的活动。这些安全面包括:(1)管理安全面;(2)控制安全面;(3)终端用户安全面。这些安全面相应地处理与网络管理活动、网络控制或信令活动和终端用户活动相关的特定安全需求。

网络系统宜用这样一种方式设计:一个安全面上的事态被尽可能多地保存并与其他安全面适当隔离。例如,由终端用户请求发起的终端用户安全面上的 DNS 查询洪泛,不宜把允许管理员改正问题的管理安全面中的 OAM&P 界面排除在外。

图 2 说明包含安全面的参考体系结构。每种描述网络活动的类型都有其自身特定的安全需求。安全面的概念允许与那些活动相关的特定安全关注和独立处理它们的能力之间有差异。例如,考虑由服务安全层处理的 VoIP 服务。VoIP 服务管理(如配置用户)的安全保护必须独立于服务控制(如 SIP 之类的协议)的安全保护,也必须独立于正在由服务传输的终端用户数据(如用户语音)的安全保护。

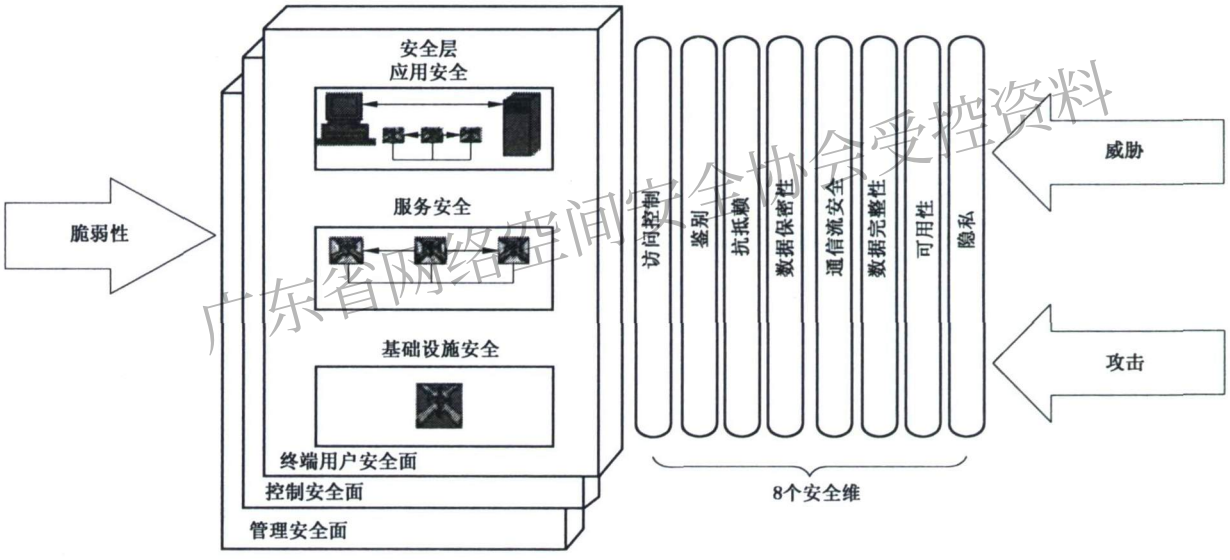

图 2 安全面反映不同类型的网络活动

8.1 管理安全面

管理安全面涉及网络元素、传输设施、后台系统(运行支持系统、业务支持系统、客户服务系统等等)和数据中心的 OAM&P 功能的保护。管理安全面支持故障、容量、管理、配置和安全(FCAPS)功能。宜注意的是,就服务提供商的用户通信流而言,承载这些活动通信流的网络可以是带内或带外的。

8.2 控制安全面

控制安全面从事于使能穿越网络高效交付信息、服务和应用的活动保护。它通常包含机器对机器的信息通信,以允许机器(如交换机或路由器)确定如何最好地选择路由或交换穿越下层传输网络的通信流。这种类型信息有时被称作控制或信令信息。就服务提供商的用户通信流而言,承载这些类型消息的网络可是带内或带外的。例如,IP 网络系统在带内承载其控制信息,而 PSTN 在一个分离的带外信令网络(SS7 网络)中承载其控制信息。这种类型通信流的实例包括路由协议、DNS、SIP、SS7 和

Megaco/H.248 等。

8.3 终端用户安全面

终端用户安全面处理客户访问和使用服务提供商网络的安全。这个平面也涉及实际终端用户数据流的保护。终端用户可使用只提供连通性的网络，他们可使用它来提供 VPN 之类的增值服务，或者可使用它来访问基于网络的应用。

9 安全威胁

这一参考体系结构定义一个规划和一套原则以描述端到端安全解决方案的安全结构。为防止有意威胁以及偶然威胁，该体系结构识别需要被处理的安全问题。下列威胁在 GB/T 9387.2—1995 中描述：

a) 信息和/或其他资源的破坏；

b) 信息的损坏或修改；

c) 信息和/或其他资源的窃取、移动或丢失；

d) 信息泄漏；

e) 服务中断。

每个安全层与每个安全面的交集表示一个安全维应用于对抗威胁的安全视图。表 1 提供一个安全维至安全威胁的映射。该映射对每个安全视图相同。

表格的行与列的交集所形成单元中的字母“Y”表示特定安全威胁被相应的安全维对抗。

表 1 安全维至安全威胁的映射

安全维	安全威胁				
	信息或其他资源的破坏	信息的损坏或修改	信息和其他资源的窃取、移动或丢失	信息泄漏	服务中断
访问控制	Y	Y	Y	Y	
鉴别			Y	Y	
抗抵赖	Y	Y	Y	Y	Y
数据保密性			Y	Y	
通信流安全			Y	Y	
数据完整性	Y	Y			
可用性	Y				Y
隐私				Y	

图 3 说明具有所示体系结构元素的参考体系结构并指出前面描述的安全威胁。此图描述用每个安全层的每个安全面上的安全维来保护网络的概念以提供全面的安全解决方案。宜注意的是，根据一个给定网络的安全要求，可能不必让所有的体系结构元素（即具有一整套安全维、安全层和安全面）都得到实施。

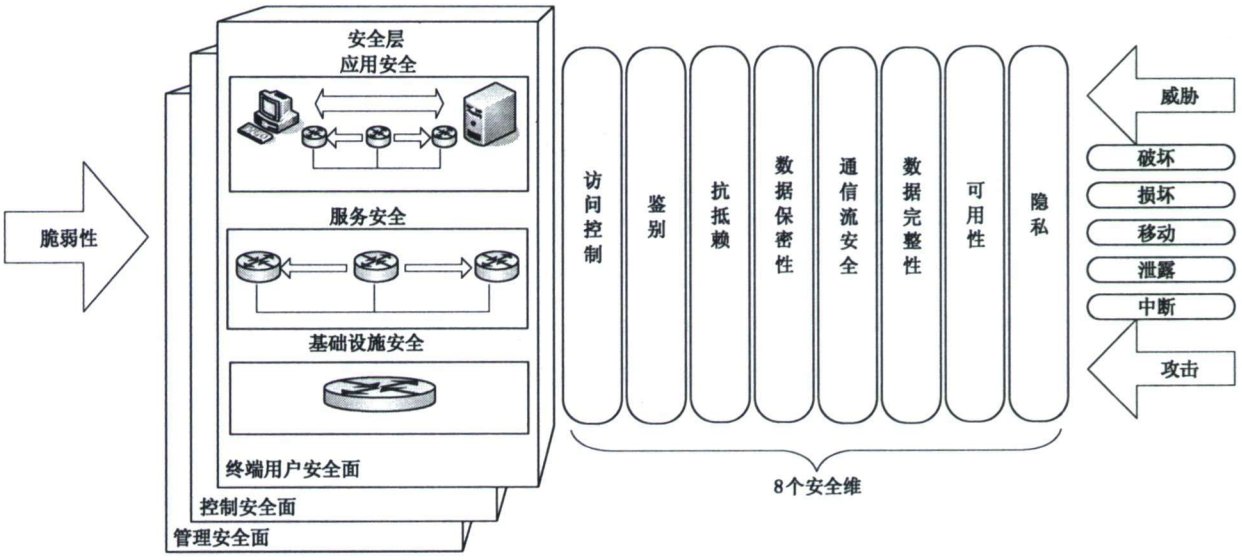

图 3　端到端网络安全参考体系结构

10　对安全维应用于安全层所实现目标的描述

该参考体系结构能应用于图 4 中所描述的安全项目的所有方面和阶段。如图 4 所示，安全项目除技术外还包括策略和规程，并且贯穿其生命期过程的 3 个阶段：(1)定义和规划阶段；(2)实施阶段；(3)维护阶段。该参考体系结构连同 ISO/IEC 13335 的指南能跨越安全项目的所有 3 个阶段，应用于安全策略和规程以及技术。

网络体系结构、策略定义、事件响应和恢复规划基于业务要求而确定。在此过程中，该参考体系结构能够通过在定义和规划阶段考虑每个安全层和安全面上的安全维，来指导全面安全策略定义、事件响应和恢复计划及技术体系结构的开发。随着策略和规程的推行和技术的部署，该参考体系结构也能用作安全评估的基础，用以检验安全项目的实施如何处理安全维、安全层和安全面。一旦安全项目被部署，就必须得到维护以使其在不断变化的安全环境中保持更新。该参考体系结构能通过确保对安全项目的修改处理每个安全层和安全面上的每个安全维，从而帮助管理安全策略和规程、事件响应和恢复规划及技术体系结构。

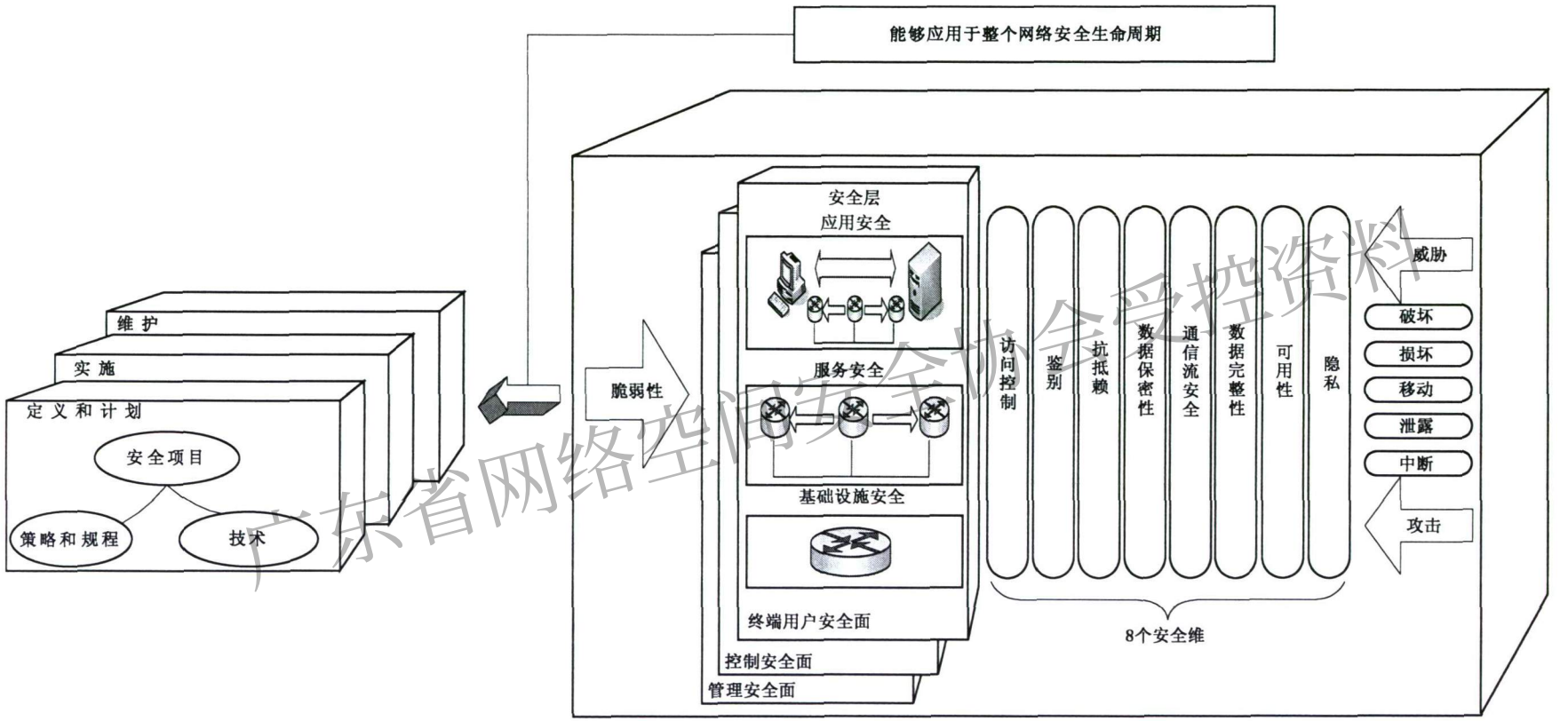

图 4　应用参考安全架构的安全程序

此外，该参考体系结构能够应用于任一级协议栈上的任一种网络。例如，在驻留于协议栈第3层的IP网络中，基础设施安全层是指单个的路由器、路由器（如SONET、ATM PVC等）之间的点对点通信链路以及用于提供IP网络所要求的支持服务的服务器平台。服务安全层是指基本IP服务本身（如互联网连通性）、IP支持服务（如AAA、DNS、DHCP等）以及服务提供商提供的高级增值服务（如VoIP、QoS、VPN等）。最后，应用安全层是指经由IP网络访问的用户应用（如电子邮件等）安全。

同样，对于驻留于协议栈第2层的ATM网络，基础设施安全层是指单个的交换机和交换机之间的点对点通信链路（承载设施，例如DS3数字信号）。服务安全层是指ATM服务提供的不同的传输种类（固定比特率、可变比特率（实时）、可变比特率（非实时）、可用比特率和未指定比特率）。最后，应用安全层是指终端用户正使用ATM网络访问的应用，例如视频会议应用。

图5以表格形式示出该参考体系结构并说明一种保护网络的系统途径。从此图中能发现，安全层与安全面的交叉点表示一个考虑到8个安全维的独特视图。9个模块都与应用于特定安全面的特定安全层的8个安全维相结合。宜注意的是，不同模块的安全维可有不同的目标，因此，可包含不同的安全措施集。表格形式为描述每个模块的安全维目标提供一种便利方式。

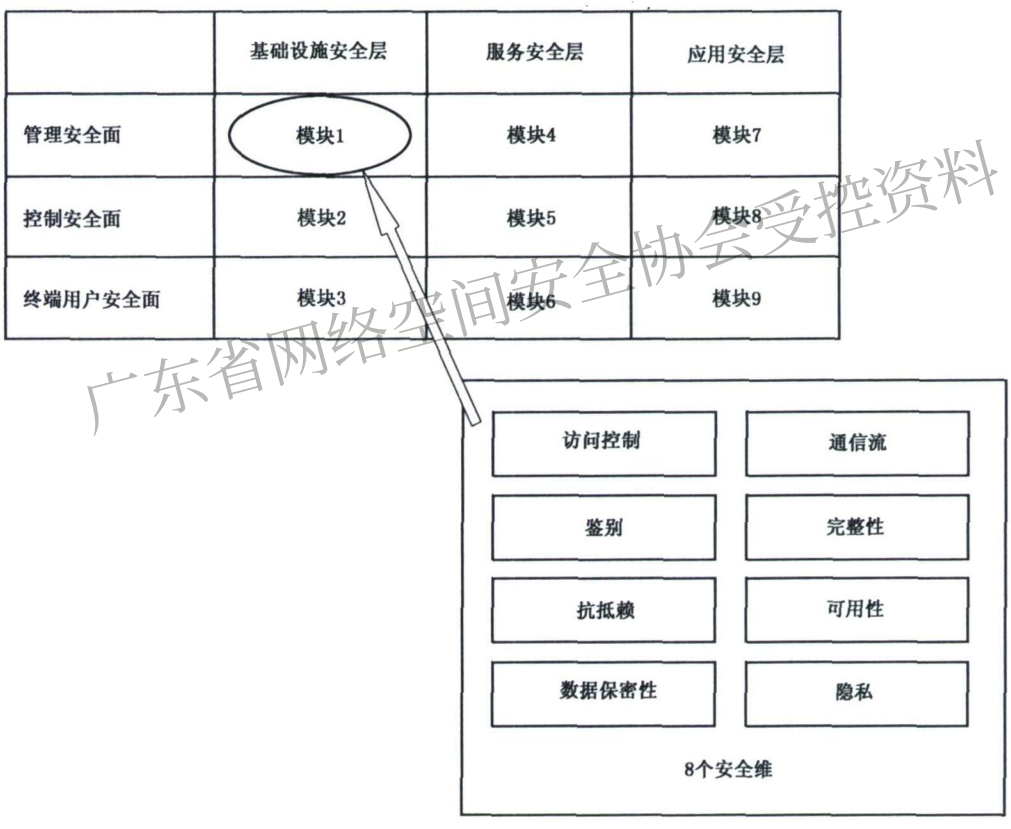

图5　表格形式的参考体系结构

宜注意的是，在后面表格中使用的保护概念包含着创建用于检测控制机制在哪里失效的机制，且确保为动作而报告事态和/或设备/过程适当地纠正这种失效的任何后果。

10.1　基础设施安全层

基础设施安全层的管理安全面的安全保护涉及操作、管理、维护和配置（OAM&P）的安全保护以及单个网络元素、通信链路和包含网络的服务器平台的配置。一个需要得到保护的基础设施管理的实例是由网络操作人员配置的单个路由器或交换机。表2描述将安全维应用于基础设施安全层的管理安

全面的目标。

表 2　将安全维应用于基础设施安全层的管理安全面

模块 1:基础设施安全层的管理安全面	
安全维	安全目标
访问控制	确保只允许授权人员或设备在网络设备或通信链路上执行或试图执行常规管理或管理活动(如 SNMP 管理设备的情形)。这适用于经由端口的设备直接管理和设备的远程管理
鉴别	验证在网络设备或通信链路上执行常规管理或管理活动的人员或设备的身份。可要求鉴别技术作为访问控制的一部分
抗抵赖	提供一个识别在网络设备或通信链路上执行每个常规管理或管理活动的人员或设备及其所执行动作的记录。此记录能用作常规管理或管理活动原发者的证据
数据保密性	保护网络设备或通信链路配置信息免受未授权访问或查看。这适用于驻留在网络设备或通信链路中的配置信息、正被传输到网络设备或通信链路的配置信息以及离线存储的备份配置信息。 保护常规管理鉴别信息(如管理员身份标识和口令)免受未授权访问或查看。 用于处理访问控制的技术可有助于提供数据保密性
通信流安全	在远程管理网络设备或通信链路的情形中,确保管理信息只在远程管理站与正被管理的设备或通信链路之间流动。当管理信息在这些端点之间流动时它不会被转向或拦截。 同样类型的考量适用于常规管理鉴别信息(如管理员身份标识和口令)
数据完整性	保护网络设备和通信链路的配置信息免受未授权修改。此保护适用于驻留在网络设备或通信链路中的配置信息及正在传输或存储于离线系统中的配置信息。 同样类型的考量适用于常规管理鉴别信息(如管理员身份标识和口令)
可用性	确保由授权人员或设备管理网络设备或通信链路的能力不能被否认。这包括抵御拒绝服务(DoS)攻击之类的主动攻击以及抵御对常规管理鉴别信息(如管理员身份标识和口令)进行修改或删除之类的被动攻击
隐私	确保能用于识别网络设备或通信链路的信息对未授权人员或设备是不可用的。此类信息的实例包括网络设备 IP 地址或 DNS 域名。例如,能识别给攻击者提供目标信息的网络设备。 确保通过网络来收集、处理和传播个人信息以便符合当地数据保护的法律法规

基础设施安全层的控制安全面的安全保护包括驻留于网络元素和包含网络的服务器平台中的控制或信令信息的安全保护以及网络元素和服务器平台的控制或信令信息的接收和传输的安全保护。例如,驻留于网络交换机上的交换表需要得到保护而免遭篡改或未授权泄漏。在另一个实例中,路由器需要得到保护以免接收和传播伪造的路由更新或响应源自欺骗路由器的伪造路由请求。表 3 描述将安全维应用于基础设施安全层的控制安全面的目标。

表 3　将安全维应用于基础设施安全层的控制安全面

模块 2:基础设施安全层的控制安全面	
安全维	安全目标
访问控制	确保只允许授权人员或设备访问或试图访问驻留于网络设备(如路由表)中或离线存储的控制信息。 确保网络设备将仅从授权网络设备接收控制信息消息(如路由更新)
鉴别	验证观察或修改驻留于网络设备中控制信息的人员或设备的身份。 验证经网络发送控制信息的设备的身份。 可要求鉴别技术作为访问控制的一部分

表 3（续）

模块 2:基础设施安全层的控制安全面	
安全维	安全目标
抗抵赖	提供一个识别每个观察过或修改过网络设备中控制信息的人员或设备及其所执行动作的记录。此记录能用作访问或修改控制信息的证据。 提供一个识别发起发送给网络设备的控制消息的设备及其所执行动作的记录。此记录能用作设备发起控制消息的证据
数据保密性	保护驻留于网络设备中或离线存储的控制信息免受未授权访问或查看。用于处理访问控制的技术可有助于为驻留于网络设备中的控制信息提供数据保密性。 保护预定送往网络设备的控制信息在穿越网络传输时免受未授权访问或查看
通信流安全	确保正穿越网络传输的控制信息(如路由更新)只在控制信息源与其期望目的地之间流动。当控制信息在这些端点之间流动时它不会被转向或拦截
数据完整性	保护驻留于网络设备中、正穿越网络传输或离线存储的控制信息免受未授权修改
可用性	确保网络设备总是可用于从授权源接收控制信息。这包括抵御拒绝服务(DoS)攻击之类的故意攻击和偶然发生事件(如路由翻动)
隐私	确保能用于识别网络设备或通信链路的信息对未授权人员或设备是不可用的。此类信息的实例包括网络设备 IP 地址或 DNS 域名。例如,能识别给攻击者提供目标信息的网络设备或通信链路。确保通过网络来收集、处理和传播个人信息以便符合当地数据保护的法律法规

基础设施安全层的终端用户安全面的安全保护包括驻留于网络元素中或通过网络正穿越通信链路传输的用户数据和语音的安全保护。在这里驻留于服务器平台上的用户数据的安全保护涉及传输于网络元素中或穿越通信链路传输的用户数据免受非法拦截的安全保护。表 4 描述将安全维应用于基础设施安全层的终端用户安全面的目标。

表 4　将安全维应用于基础设施安全层的终端用户安全面

模块 3:基础设施安全层的终端用户安全面	
安全维	安全目标
访问控制	确保只允许授权人员或设备访问或试图访问在网络元素或通信链路中传输的或驻留在离线存储设备上的终端用户数据
鉴别	验证试图访问在网络元素或通信链路中传输的或驻留在离线存储设备上的终端用户数据的人员或设备的身份。 可要求鉴别技术作为访问控制的一部分
抗抵赖	提供一个识别访问在网络元素或通信链路中传输的或驻留在离线设备上的终端用户数据的每个人员或设备及其所执行动作的记录。 此记录能用作访问终端用户数据的证据
数据保密性	保护在网络元素或通信链路中传输的或驻留在离线存储设备上的终端用户数据免受未授权访问或查看。用于处理访问控制的技术可有助于为终端用户数据提供数据保密性
通信流安全	确保在超越授权访问情形下,在网络元素或通信链路中传输的终端用户数据在这些端点之间流动时不会被转向或拦截(如合法窃听)
数据完整性	保护在网络元素或通信链路中传输的或驻留于离线存储设备上的终端用户数据免受未授权修改

表 4（续）

模块 3:基础设施安全层的终端用户安全面	
安全维	安全目标
可用性	确保授权人员(包括终端用户)或设备访问驻留于设备上的终端用户数据不能被拒绝。这包括抵御拒绝服务(DoS)攻击之类的主动攻击以及抵御对鉴别信息(如用户身份标识和口令、管理员身份标识和口令)进行修改或删除之类的被动攻击
隐私	确保网络元素不向未授权人员或设备提供关于终端用户网络活动的信息(如用户的地理位置、访问的万维网站点等)。确保通过网络来收集、处理和传播个人信息以便符合当地数据保护的法律法规

10.2 服务安全层

为满足客户要求而使服务可相互依赖，这个事实使服务安全层的安全保护变得复杂化。例如，为了提供 VoIP 服务，服务提供商必须首先提供基础 IP 服务以及必要的 AAA、DHCP、DNS 之类的使能服务。为满足客户对 VoIP 服务的 QoS 和安全的要求，服务提供商可能也需要部署一个 VPN 服务。因此，基于如下考量的服务必须分解成复合的服务来处理其整体安全。

服务安全层的管理安全面的安全保护涉及到网络服务的 OAM&P 功能和配置的安全保护。需要安全保护管理的服务的一个实例是网络操作人员配置特定终端用户中的授权用户的服务。表 5 描述将安全维应用于服务安全层的管理安全面的目标。

表 5 将安全维应用于服务安全层的管理安全面

模式 4:服务安全层的管理安全面	
安全维	安全目标
访问控制	确保只允许授权人员或设备执行或试图执行网络服务的常规管理或管理活动(如配置该服务的用户)
鉴别	验证试图执行网络服务的常规管理或管理活动的人员或设备的身份。可要求鉴别技术作为访问控制的一部分
抗抵赖	提供一个识别执行网络服务的常规管理或管理活动的人员或设备及其所执行动作的记录。此记录能用作所指示的人员或设备执行了常规管理或管理活动的证据
数据保密性	保护网络服务的配置和管理信息(如可下载的 VPN 服务 IPsec 客户端设置)免受未授权访问或查看。这适用于驻留在网络设备中、正穿越网络传输或离线存储的管理和配置信息。 保护网络服务的常规管理或管理信息(如用户身份标识和口令、管理员身份标识和口令)免受未授权访问或查看
通信流安全	在网络服务远程管理的情形中，确保常规管理或管理信息仅在远程管理站与正作为网络服务一部分被管理的设备之间流动。当常规管理和管理信息在这些端点之间流动时它不会被转向或拦截。 同样类型的考量适用于网络服务鉴别信息(如用户身份标识和口令、管理员身份标识和口令)
数据完整性	保护网络服务的常规管理和管理信息免受未授权修改。此保护适用于驻留在网络设备中、正穿越网络传输或存储于离线系统上的常规管理和管理信息。 同样类型的考量适用于网络服务鉴别信息(如用户身份标识和口令、管理员身份标识和口令)

表 5（续）

模式 4:服务安全层的管理安全面	
安全维	安全目标
可用性	确保由授权人员或设备管理网络服务的能力不能被否认。这包括抵御拒绝服务(DoS)攻击之类的主动攻击以及抵御对网络服务常规管理鉴别信息(如管理员身份标识和口令)进行修改或删除之类的被动攻击
隐私	确保能用于识别网络服务常规管理或管理系统的信息对未授权人员或设备是不可用的。此类信息的实例包括系统 IP 地址或 DNS 域名。例如,能识别给攻击者提供目标信息的网络服务常规管理系统。确保通过网络来收集、处理和传播个人信息以便符合当地数据保护的法律法规

服务安全层的控制安全面的安全保护包括网络服务使用的控制或信令信息的安全保护。例如,在这里处理用于发起和保持 VoIP 会话的 SIP 协议的安全保护问题。表 6 描述将安全维应用于服务安全层的控制安全面的目标。

表 6　将安全维应用于服务安全层的控制安全面

模式 5:服务安全层的控制安全面	
安全维	安全目标
访问控制	在接受网络设备为网络服务接收的控制信息之前确保该信息来自授权源(如 VoIP 会话发起消息来源于授权用户或设备)。例如,抵御未授权设备欺骗 VoIP 会话发起消息
鉴别	验证发送到参与网络服务的网络设备的网络服务控制信息源的身份。可要求鉴别技术作为访问控制的一部分
抗抵赖	提供一个识别发起由参与网络服务的网络设备接收的网络服务控制消息的人员或设备及其所执行动作的记录。此记录能用作人员或设备发起网络服务控制消息的证据
数据保密性	保护驻留于网络设备中、正穿越网络传输或离线存储的网络服务控制信息(如 IPsec 会话数据库)免受未授权访问或查看。用于处理访问控制的技术可有助于为驻留于网络设备中的网络服务控制信息提供数据保密性
通信流安全	确保正穿越网络传输的网络服务控制信息(如 IPsec 密钥协商消息)只在控制信息源与其期望目的地之间流动。当网络服务控制信息在这些端点之间流动时它不会被转向或拦截
数据完整性	保护驻留于网络设备中、正穿越网络传输或离线存储的网络服务控制信息免受未授权修改
可用性	确保参与网络服务的网络设备总是可用于从授权源接收控制信息。这包括抵御拒绝服务(DoS)攻击之类的主动攻击
隐私	确保能用于识别参与网络服务的网络设备或通信链路的信息对未授权人员或设备是不可用的。此类信息的实例包括网络设备 IP 地址或 DNS 域名。例如,能识别给攻击者提供目标信息的网络设备或通信链路。确保通过网络来收集、处理和传播个人信息以便符合当地数据保护的法律法规

服务安全层的终端用户安全面的安全保护包括使用网络服务的用户数据和语音的安全保护。例如,在 VoIP 服务中必须保护用户会话的保密性。同样,DNS 服务必须确保服务用户的保密性。表 7 描述将安全维应用于服务安全层的终端用户安全面的目标。

表 7　将安全维应用于服务安全层的终端用户安全面

模式 6:服务安全层的终端用户安全面	
安全维	安全目标
访问控制	确保只允许授权用户和设备访问或试图访问和使用网络服务
鉴别	验证试图访问和使用网络服务的用户或设备的身份。可要求鉴别技术作为访问控制的一部分
抗抵赖	提供一个识别访问和使用网络服务的每个用户和设备及其所执行动作的记录。此记录能用作终端用户或设备访问和使用网络服务的证据
数据保密性	保护网络服务正在传输、处理或存储的终端用户数据免受未授权访问或查看。用于处理访问控制的技术可有助于为终端用户数据提供数据保密性
通信流安全	确保在超越授权访问情形下,网络服务正在传输、处理或存储的终端用户数据在这些端点之间流动时不会被转向或拦截(如合法窃听)
数据完整性	确保网络服务正在传输、处理或存储的终端用户数据免受未授权修改
可用性	保证授权终端用户或设备访问网络服务不能被否认。这包括抵御拒绝服务(DoS)攻击之类的主动攻击以及抵御对终端用户鉴别信息(如用户身份标识和口令)进行修改或删除之类的被动攻击
隐私	确保网络服务不提供关于终端用户服务的使用信息(如对于 VoIP 服务或被叫用户)给未授权人员或设备。确保通过网络来收集、处理和传播个人信息以便符合当地数据保护的法律法规

10.3　应用安全层

应用安全层的管理安全面的安全保护涉及基于网络应用的 OAM&P 功能和配置的安全保护。对于电子邮件应用来说,需要保护的管理动作的一个实例是用户邮箱的配置和常规管理。表 8 描述将安全维应用于应用安全层的管理安全面的目标。

表 8　将安全维应用于应用安全层的管理安全面

模式 7:应用安全层的管理安全面	
安全维	安全目标
访问控制	确保只允许授权人员或设备执行或试图执行基于网络应用的常规管理或管理活动(如为电子邮件应用管理用户邮箱)
鉴别	验证试图执行基于网络应用的常规管理或管理活动的人员或设备的身份。可要求鉴别技术作为访问控制的一部分
抗抵赖	提供一个识别执行基于网络应用的每个常规管理或管理活动的人员或设备及其所执行动作的记录。此记录能用作常规管理或管理活动与执行它的人员或设备的指示一起执行的证据
数据保密性	保护在创建和执行基于网络的应用程序过程中所使用的所有文件(如源文件、目标文件、可执行文件、临时文件等)和应用配置文件免受未授权访问或查看。这适用于驻留在网络设备中、正穿越网络传输或离线存储的应用文件。 保护基于网络应用的常规管理或管理信息(如用户身份标识和口令、管理员身份标识和口令)免受未授权访问或查看
通信流安全	在远程管理或操纵基于网络应用的情形中,确保常规管理或管理信息只在远程管理站与组成基于网络应用的设备之间流动。当常规管理或管理信息在这些端点之间流动时它不会被转向或拦截。 同样类型的考量适用于基于网络应用的常规管理或管理信息(如用户身份标识和口令、管理员身份标识和口令)

表 8（续）

模式 7:应用安全层的管理安全面	
安全维	安全目标
数据完整性	保护在创建和执行基于网络的应用程序过程中所使用的所有文件(如源文件、目标文件、可执行文件、临时文件等)和应用配置文件免受未授权修改。此保护也适用于驻留在网络设备中、正穿越网络传输或存储在离线系统中的应用文件。 同样类型的考量适用于基于网络应用的常规管理或管理信息(如用户身份标识和口令、管理员身份标识和口令)
可用性	确保由授权人员或设备管理或操纵基于网络应用的能力不能被否认。这包括抵御拒绝服务(DoS)攻击之类的主动攻击以及抵御对基于网络应用的常规管理鉴别信息(如管理员身份标识和口令)进行修改或删除之类的被动攻击
隐私	确保能用于识别基于网络应用的常规管理或管理系统的信息对未授权人员或设备是不可用的。此类信息的实例包括系统 IP 地址或 DNS 域名。例如,能识别给攻击者提供目标信息的基于网络应用的常规管理系统。确保通过网络来收集、处理和传播个人信息以便符合当地数据保护的法律法规

应用安全层的控制安全面的安全保护包括基于网络应用使用的控制或信令信息的安全保护。这种信息通常会引发执行响应接收信息动作的应用程序。例如,在这里处理用于控制电子邮件交付的 SMTP 和 POP 协议的安全保护问题。表 9 描述将安全维应用于应用安全层的控制安全面的目标。

表 9　将安全维应用于应用安全层的控制安全面

模式 8:应用安全层的控制安全面	
安全维	安全目标
访问控制	在接受参与基于网络应用的网络设备接收的应用控制信息之前确保该信息来自授权源(如请求电子邮件传输的 SMTP 消息)。例如,抵御未授权设备欺骗 SMTP 客户
鉴别	验证发送到参与基于网络应用的网络设备的应用控制信息源的身份。可要求鉴别技术作为访问控制的一部分
抗抵赖	提供一个识别发起由参与基于网络应用的网络设备接收的应用控制消息的人员或设备及其所执行动作的记录。此记录能用作人员或设备发起应用控制消息的证据
数据保密性	保护驻留于网络设备中、正穿越网络传输或离线存储的应用控制信息(如 SSL 或 TLS 会话数据库)免受未授权访问或查看。用于处理访问控制的技术可有助于为驻留于网络设备中基于网络应用的控制信息提供数据保密性
通信流安全	确保正穿越网络传输的应用控制信息只在控制信息源与其期望目的地之间流动。当基于网络应用的控制信息在这些端点之间流动时它不会被转向或拦截
数据完整性	保护驻留于网络设备中、正穿越网络传输或离线存储的基于网络应用的控制信息免受未授权修改和删除
可用性	确保参与基于网络应用的网络设备总是可用于从授权源接收控制信息。这包括抵御拒绝服务(DoS)攻击之类的主动攻击
隐私	确保能用于识别参与基于网络应用的网络设备或通信链路的信息对未授权人员或设备是不可用的。此类信息的实例包括网络设备 IP 地址或 DNS 域名。例如,能识别给攻击者提供目标信息的网络设备或通信链路。确保通过网络来收集、处理和传播个人信息以便符合当地数据保护的法律法规

应用安全层的终端用户安全面的安全保护包括提供给基于网络应用的用户数据的安全保护。例如,电子商务应用必须保护用户信用卡号的保密性。表10描述将安全维应用于应用安全层的终端用户安全面的目标。

表10 将安全维应用于应用安全层的终端用户安全面

模式9:应用安全层的终端用户安全面	
安全维	安全目标
访问控制	确保只允许授权用户和设备访问或试图访问和使用基于网络的应用
鉴别	验证试图访问和使用基于网络的应用的用户或设备的身份。可要求鉴别技术作为访问控制的一部分
抗抵赖	提供一个识别访问和使用基于网络的应用的每个用户或设备及其所执行动作的记录。此记录能用作终端用户或设备访问和使用应用的证据
数据保密性	保护基于网络的应用正在传输、处理或存储的终端用户数据免受未授权访问或查看。 当它从用户流到基于网络的应用时,同样类型的考量适用于用户数据。 用于处理访问控制的技术可有助于为终端用户数据提供数据保密性
通信流安全	确保在超越授权访问情形下,基于网络的应用正在传输、处理或存储的终端用户数据在这些端点之间流动时不会被转向或拦截。 当它从用户流到基于网络的应用时,同样类型的考量适用于用户数据
数据完整性	保护基于网络的应用正在传输、处理或存储的终端用户数据免受未授权修改。当它从用户流到基于网络的应用时,同样类型的考量适用于用户数据
可用性	确保授权终端用户或设备访问基于网络的应用不能被否认。这包括抵御拒绝服务(DoS)攻击之类的主动攻击以及抵御对终端用户鉴别信息(如用户身份标识和口令)进行修改或删除之类的被动攻击
隐私	确保基于网络的应用不提供关于终端用户服务的使用信息(如访问的万维网站点)给未授权人员或设备。例如,只将这种信息泄漏给有调查许可的执法人员。确保通过网络来收集、处理和传播个人信息以便符合当地数据保护的法律法规

参 考 文 献

[1] GB/T 25068.1—2012 信息技术 安全技术 IT网络安全 第1部分:网络安全管理

[2] GB/T 25068.3—2010 信息技术 安全技术 IT网络安全 第3部分:使用安全网关的网间通信安全保护

[3] GB/T 25068.4—2010 信息技术 安全技术 IT网络安全 第4部分:远程接入的安全保护

中 华 人 民 共 和 国
国 家 标 准
信息技术　安全技术　IT网络安全
第2部分：网络安全体系结构
GB/T 25068.2—2012/ISO/IEC 18028-2:2006
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室：(010)64275323　发行中心：(010)51780235
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.5　字数 37 千字
2012年10月第一版　2012年10月第一次印刷
*
书号：155066·1-45561　定价　24.00 元

GB/T 25068.2-2012