国 际 电 信 联 盟

电信和信息技术安全

关于电信安全的若干议题综述及相关ITU-T建议书应用简介

ITU-T 电信标准化部门

2009 年

国际电信联盟

ITU-T – 电信标准化局 (TSB)
Place des Nations – CH-1211 Geneva 20 – Switzerland
电子邮件: tsbmail@itu.int 网址: www.itu.int/ITU-T

电信和信息技术安全

关于电信安全的若干议题综述
及相关*ITU-T*建议书应用简介

2009年9月

前言

国际电联电信标准化局主任

马尔科姆•琼森

直到不久前，电信和信息技术安全问题还主要存在于银行、航空航天和军事应用等专业领域。不过，随着数据通信，尤其是互联网应用的迅速、广泛增长，安全几乎已成了每个人的事。

信息通信技术（ICT）安全问题日渐受到重视的现象在某种程度上可能受到流传甚广的病毒、蠕虫、黑客和对个人隐私的威胁等事件的影响，但摆在我们面前的现实是，随着计算技术和联网成为日常生活极为重要的组成部分，迫切需要采取有效的安全措施来保护政府、业界、商务、关键基础设施和消费者个人的计算机和电信系统。此外，越来越多的国家已经制定了数据保护方面的法律，这些法律也要求与数据机密性和完整性的示范标准相一致。

目前，人们已普遍认识到，安全技术和措施应嵌入系统，而不应事后补救；人们还普遍认识到，为了充分发挥安全技术和措施的效用，应将安全作为一个重要的问题来考虑，贯穿系统生命周期的所有阶段，从系统构想和设计，到系统实施和部署，直到最后的系统退役。在项目设计阶段和系统开发阶段对安全问题考虑不周，很容易导致产生易受攻击的弱点。标准委员会在保护电信和信息技术系统方面起着至关重要的作用，采取的方式包括对安全问题保持清醒的认识、确保对安全问题的考虑成为规范的一个基本组成部分以及提供技术标准和指导原则，以帮助实施者和使用者将通信系统和服务建设得足够牢靠，有能力抵抗网络攻击。

多年来，国际电联电信标准化部门（ITU-T）一直积极参与电信和信息技术的安全工作。但是，随着网络应用的日益增长，为了应对新出现的和正在形成的威胁并满足各成员对有助于应对这些威胁的标准的需求，我们的工作量也急剧增加。本手册概述了我们工作中的一些主要方面，介绍了ITU-T 可提供的众多资源，以帮助所有使用者应对我们面临的网络安全挑战。

在构建全球网络安全文化的过程中，标准化是一个重要的构件。我们有能力并且必将赢得抵御网络威胁这场战争的胜利。我们的胜利将建立在成千上万为此而努力奉献的人的工作基础之上，他们来自公共管理部门、私营部门、学术界，在国际电联这样的机构组织下，团结协作，制定安全标准和最佳做法指导原则。虽然他们的工作不很刺激或者不很引人注目，但对保卫我们数字化的未来而言至关重要。我向国际电联电信标准化局的工程师们表示感谢和赞赏，他们与来自国际电联成员的专家们一道，坚持不懈地致力于制定这些标准和指导原则。 这一努力仍将继续。

本手册除了意在为技术专家、负责制定和执行电信规则的相关人员以及希望更多了解信息通信技术安全问题和涉及这些问题的相关 ITU-T 建议书的其他人员提供一份指南外，也面向中高层管理人员/资深经理。对那些希望探讨信息通信技术安全问题的人，我相信本手册将是一份有用的指南。欢迎广大读者为本手册的修订再版提出意见和建议。

国际电联
电信标准化局主任

马尔科姆 • 琼森

目录

页码

页码

页码

页码

致谢

本手册的编写得到了众多作者的帮助，他们或者参与制定了相关的ITU-T建议书，或者参加了ITU-T的研究组会议、讲习班和研讨会。对国际电联研究组的各位特别报告人、编辑和安全协调员以及参与安全问题研究工作的国际电联电信标准化局各位顾问，特别是ITU-T电信安全工作牵头研究组前主席Herb Bertine以及安全项目前特别报告人 Mike Harrop，谨致谢意。

概要

本手册旨在大致介绍ITU-T的安全工作，面向的是负责信息和通信安全问题以及相关标准工作的人员或对其感兴趣的人员，以及只是想更多了解信息通信技术（ICT）安全问题与相关ITU-T建议书的人员。

手册引言部分首先概述ITU-T的各项安全活动。这部分包含一些主要的ITU-T安全资源和延伸信息的链接。此外，手册引言部分包含一个汇总表，指明不同的读者如何使用本手册。

下一部分介绍保护信息通信技术应用、服务和信息的基本要求，说明了推动这些要求的威胁和弱点，描述了标准在满足这些要求中的作用，阐述了保护各不同团体所需的某些特性，主要关注的是信息通信技术设施的使用和运营。此外，在本节中还给出了制定各信息通信技术（ICT）安全标准的理由，并勾勒了该领域ITU-T工作的发展历程。

此后一部分介绍开放系统和端对端通信的通用安全体系结构以及一些应用特定的体系结构。这些体系结构各建立了一种框架，在所建框架内，可以以一种一致的方式来解决多个方面的安全问题。它们也对安全服务和机制的各基本概念做了标准化，并提供了有关信息通信技术安全术语和基本概念的标准词汇表。在这些体系结构中引入的通用原则构成了有关安全服务、机制和协议的众多其他标准的基础。在本节中还提供了与涉及网络安全生命周期的关键活动有关的安全指导原则的线索。

接着一节论述有关安全管理问题的各选定主题，旨在考察信息安全管理、风险管理以及事故响应与处置情况。

另一节讨论号码簿及其在支持安全服务中的作用，以及与认证和身份管理有关的主题。在本节中陈述了诸如公开密钥基础设施、远程生物特征识别（即在电信环境中利用生物特征识别设备进行个人身份识别和认证）和隐私等主题，并说明了保护好号码簿信息库的重要性。

有关如何保证网络基础设施安全的主题涉及网络管理和公共安全管理服务。

手册专有一节阐述一些特定的网络安全例子和方法。本节首先描述了下一代网络的安全要求，而后讨论了移动通信网络，它从基于单一技术（如CDMA或GSM）的移动性转换到了利用网际协议实现跨异构平台的移动性。接着讨论了有关家庭网络和有线电视的安全规定，最后分析了无处不在的传感器网络安全面临的挑战。

尽管现在的应用开发商更多地考虑一开始就在其产品中植入安全性，而不是在应用进入产品后再来考虑安全性的改进问题，但面对日益严峻的威胁环境和产品固有的弱点，各种应用仍存在风险。有关应用安全的一节论述了众多的信息通信技术应用，包括IP话音（VoIP）、IPTV和安全传真，并特别强调了在ITU-T各建议书中所定义的安全特性。

下一节阐述如何应对一些常见的网络威胁，如垃圾邮件、恶意代码和间谍软件，并说明了及时通告和发布更新资料的重要性，以及在处置安全事故时做好组织和协调工作的重要性。

手册在结尾处概括了信息通信技术安全标准化的未来发展方向，并介绍了各种额外信息源。

本手册还包括若干附件，分别涉及安全定义、本手册所用缩写、与安全有关的研究组简介以及本手册所参考的建议书的详细清单。

第四版介绍

这是手册的第四版，结构和内容做了重大修订。自2003年第一版手册出版以来，ITU-T开拓了许多新的工作领域。此外，2008年世界电信标准化全会（WTSA）后，完成并公布了许许多多新的建议书，各研究组自身也都进行了重组。要完整、详细地论述这项工作，必将形成一份规模庞大、内容繁杂、难于使用的文件。在咨询ITU-T各成员后，为第四版的编写建立了一些指导原则。这些原则包括：

- 出版物应能吸引众多读者，并应尽力避免出现有可能只有专业人士才能理解的复杂术语；
- 文本应有新内容，而不只是对现有其他形式（如建议书）可用材料的重复；
- 文本应适于出版发行，既可以作为单独印制的文件，也可以作为电子文档；
- 对文本中出现的各建议书和其他可公开使用的材料来源，应尽可能挂上万维网链接；对超过完成基本目标所需的详细信息，也应挂上万维网链接，以备参考；以及
- 文本应尽可能集中阐述已经完成和发布的工作，而不是计划开展或正在进行的工作。

为达成这些目标，本手册不会论及ITU-T已经完成或正在进行的全部安全工作。相反地，它将主要集中于选定的关键主题，对额外信息将提供万维网链接。

本手册以硬拷贝形式和电子版形式公布。对使用电子版形式手册的读者，对文本中出现的各建议书和其他在线文档将提供直接的超级链接。对使用硬拷贝形式手册的读者，在手册附件D中列出了所有参考到的建议书。对这些建议书，可以通过以下网址在线访问：www.itu.int/rec/T-REC/en。

1. 引言

1 引言

1.1 手册目的和范围

本手册旨在向负责或关注信息通信技术安全问题和相关标准的高层管理人员/资深经理介绍ITU-T 的电信安全工作。此外，相信其他希望更多了解信息通信技术安全问题和相关 ITU-T 建议书的人士也会对本手册感兴趣的，手册可以帮助他们更好地解决面临的安全问题。其他希望更多了解信息通信技术安全问题和探讨这些问题的相关 ITU-T 建议书的人员。

本手册概述了电信和信息技术安全问题，描述了一些相关的实际问题，并说明了如何通过ITU-T 标准化工作来解决当前面临的不同方面的信息通信技术安全问题。手册提供了辅导材料，对更详细的指南和额外的参考资料，则提供了链接。具体而言，对 ITU-T 各建议书以及相关的参考文献和延伸的文档，手册提供了直接链接。它将从 ITU-T 建议书中选择的安全相关材料汇编成一个出版物，并说明了工作不同方面之间的关系。当前正在开展的工作的结果将在本手册的后续版本中进行阐述。

除了ITU-T的工作，国际电联总秘书处和其他一些部门也正在着手安全工作。例子包括网络安全（www.itu.int/cybersecurity）方面的工作以及ITU-D最佳做法报告。

1.2 如何使用本手册

本手册旨在从高层面上对ITU-T的各项安全标准活动做一综述。考虑到对已出版建议书和相关文档更详细的信息需求，手册还为这些信息提供了直接链接。对本手册可以有几种使用方式。表1指明了如何使用本手册，以解决不同读者的需求。

表 1 – 本手册如何满足不同读者的需求

组织机构	特定的读者	需求	本手册如何满足这些需求
电信服务提供商	高层管理人员/资深经理	标准化工作范围综述 相关标准的高层路线图	手册直接解决这些需求
	设计师和安装工程师	相关标准的路线图 与特定领域有关的技术细节	手册提供路线图以及对详细的解释性文本的链接 建议书提供技术细节
电信服务供货商	高层管理人员/资深经理	标准化工作范围综述 相关标准的高层路线图	手册直接解决这些需求
	产品经理	相关标准的高层路线图	手册提供路线图以及对详细的解释性文本的链接
	产品设计师	与特定领域有关的技术细节	手册提供对特定领域详细的解释性文本的链接 建议书提供技术细节
最终用户	技术人员	可能对与特定领域有关的技术细节感兴趣	手册提供对特定领域详细的解释性文本的链接
	非技术人员	可能对标准化工作范围综述感兴趣	手册直接解决这些需求
学术界	学生/老师	相关标准的路线图 与特定领域有关的技术细节 对新的和将要开展的标准化工作的认识	手册提供路线图以及对特定领域详细的解释性文本的链接
政府	高层管理人员/资深经理	标准化工作范围综述 相关标准的高层路线图	手册直接解决这些需求
	监管者		
	政策制定者		
非政府组织	高层管理人员/资深经理	标准化工作范围综述 相关标准的高层路线图	手册直接解决这些需求
	开发和能力建设人员	相关标准的路线图 与特定领域有关的技术细节	手册提供对特定领域详细的、解释性文本的链接 建议书提供技术细节

2. ITU-T安全活动概述

2 ITU-T安全活动概述

2.1 引言

在信息通信技术安全方面，ITU-T已开展了二十多年的工作，在这二十几年间，几个研究组已为多个关键领域制定了建议书和指南。第17研究组（SG 17）目前对ITU-T的安全工作付主要责任，并被指定为负责安全问题的牵头研究组。不过，安全问题涉及ITU-T的大部分工作，大多数研究组都在开展与其所负责领域有关的安全工作。

作为安全问题牵头研究组责任的一部分，SG 17推出了众多参考文献和延伸出版物。包括本手册在内的这些出版物，有助于协调ITU-T内部的安全工作，并有助于将安全工作推向更多的团体，鼓励它们使用这些建议书。

本节概括介绍了ITU-T的参考文献和延伸出版物，并以表格形式对当前正在进行的安全工作做了概述。

2.2 参考文献和延伸文件

ITU-T负责一些出版物和网页的维护，从这些网页可以获得更加详细的、有关各种建议书和ITU-T安全工作的信息。

在SG 17安全问题牵头研究组的网站上，有对SG 17各项责任和活动的概括介绍。在该网站上，还包括了对文献和延伸材料的介绍，有关过去各讲习班、讲座和延伸活动的信息，以及对安全指南的链接，包括一份有关如何编写安全保障程序的教材。

有关安全工作各方面问题的更详细信息以及对更详细信息的直接链接，请查看第12节。

2.3 主要的安全主题和建议书概述

表2为本手册中所讨论的各关键主题和各相关建议书提供了便捷索引。为使用本手册电子版的读者，提供了对各主题和分主题文本以及所列各建议书的直接超级链接。附件D包含了一份在本手册中所参考建议书的完整清单。在附件D中包括了超级链接，这样，手册电子版文本的读者就可直接实现链接，方便地下载各建议书。

表 2 – 一些关键的主题和选定的建议书概述

主题	分主题	相关建议书和出版物的例子
3. 安全要求	3.2 威胁、风险和弱点 3.3 安全目标 3.4 安全标准的理由 3.6 人员和物理安全要求	X.1205：网络安全概述 E.408：电信网络安全要求 X.1051：电信组织的信息安全管理指导原则 公众网的外部设施 应用计算机和微处理器来构建、安装和保护电信电缆
4. 安全体系结构	4.1 开放系统安全体系结构 4.2 安全服务 4.3 提供端对端通信的系统的安全体系结构 4.3.2 网络及其组成部件的可用性 4.4 实施指南 4.5 应用特定的体系结构	X.800：开放系统安全体系结构 X.805：提供端对端通信的系统的安全体系结构 X.810：安全框架概述 X.Sup3：ITU-T X.800-X.849系列 - 系统和网络安全实施指导原则增补 X.1162：对等网络的安全体系结构和运作 X.1161：安全对等通信的框架 X.1143：保证移动万维网服务报文安全的安全体系结构
5. 安全管理	5.1 信息安全管理 5.2 风险管理 5.3 事故管理	X.1051：电信组织的信息安全管理指导原则 X.1055：电信组织的风险管理和风险剖面指导原则 E.409：事故组织和安全事故处置
6. 号码簿、认证和身份管理	6.1 号码簿信息的保护 6.1.4 隐私的保护 6.2 公开密钥安全机制 6.2.3 公开密钥基础设施 6.4 身份管理 6.5 远程生物特征识别	X.500：概念、模型和服务综述 X.509：号码簿：公开密钥和属性证书框架 X.1171：在采用基于标签识别的应用中对保护个人可识别信息的威胁和要求 Y.2720：下一代网络（NGN）身份管理框架 X.1081：远程生物特征识别安全规范和安全问题框架 X.1089：远程生物特征识别认证基础设施
7. 保证网络基础设施安全	7.1 电信管理网 7.2 网络管理体系结构 7.4 保证监控和控制活动安全 7.5 保证基于网络的应用安全 7.6 常用安全管理服务 7.6.4 基于CORBA的安全服务	M.3010：电信管理网的原则 X.790：ITU-T应用的故障管理功能 X.711：通用管理信息协议 X.736：安全告警报告功能 X.740：安全审计跟踪功能 X.780：定义CORBA被管对象的TMN指导原则
8. 一些特定的网络安全方法	8.1 下一代网络（NGN）安全 8.2 移动通信安全 8.3 家庭网络的安全 8.4 IPCablecom的安全要求 8.6 无处不在的传感器网络的安全	Y.2001：下一代网络（NGN）综述 Y.2701：下一代网络（NGN）安全要求（第1版） X.1121：移动端对端数据通信的安全技术框架 X.1111：家庭网络的安全技术框架 J.170：IPCablecom安全规范
9. 应用安全	9.1 IP话音（VoIP）和多媒体 9.2 IPTV 9.3 安全传真 9.4 万维网服务 9.5 基于标签的服务	H.235：H系列多媒体系统的安全框架 X.1191：IPTV安全问题的功能要求和体系结构 T.36：用于三类传真终端的安全能力 X.1141：安全声明标记语言（SAML 2.0）
10. 应对常见的网络威胁	10.1 应对垃圾邮件 10.2 恶意代码、间谍软件和欺骗软件 10.3 软件更新的通告和发布	X.1231：应对垃圾邮件的技术策略 X.1240：应对垃圾电子邮件中涉及的技术 X.1244：应对基于IP的多媒体应用中垃圾邮件的诸方面问题 X.1207：电信服务供应商用于解决间谍软件和潜在有害软件风险的指导原则 X.1206：一个与供货商无关的、用于安全相关信息自动通告和最新消息发布的框架
若想查看全套的ITU-T安全建议书，请查询以下网址： http://www.itu.int/ITU-T/recommendations/。		

3. 安全要求

3 安全要求

3.1 引言

在形成任何安全框架的过程中，对安全要求有一个清楚的认识是非常重要的。在对安全要求进行综合评估时，必须考虑到：涉及的各方、要保护的资产、保护这些资产必须应对的威胁、与这些资产有关的弱点，以及这些威胁和弱点对资产构成的总的风险。

本节介绍有关信息通信技术应用、服务和信息安全保护的基本要求，说明促动这些要求的威胁和弱点，论述标准在满足这些要求过程中的作用，并确定所需的一些特性，以便保护在信息通信技术设施使用和操作中涉及的各方。

安全要求既是通用的，也与特定的应用背景有关。此外，一些要求已得到大家的认可，而对另一些要求，还要在新的应用和变化的威胁环境下做进一步完善。本节大部分的讨论都带有普遍意义。有关特殊应用和环境的要求将在后面各节讨论。

3.2 威胁、风险和弱点

一般而言，在信息通信技术安全中，我们需要保护以下各方的资产安全：

- *客户/订户*：需要树立对网络和所提供服务的信心，包括服务的可用性（尤其是应急服务）；
- *公共团体/政府机构*：通过指令和/或立法提出安全要求，以保证服务可用、公平竞争和隐私保护；以及
- *网络运营商/服务提供商*：自身需要安全，以在国家和国际层面保护其运营和商业利益，承担他们对客户和公众的义务。

要保护的资产包括：

- 通信和计算服务；
- 信息和数据，包括与安全服务有关的软件和数据；
- 人员；以及
- 设备和设施。

*安全威胁*是一种潜在的破坏安全的行为。威胁的例子包括：

- 未经授权泄露信息；
- 未经授权毁坏或修改数据、设备或其他资源；
- 窃取、移走或丢失信息或其他资源；

- 中断或拒绝服务；以及
- 假冒或顶替得到授权的实体。

威胁可能是*偶发的*或*故意的*，也可以是*主动的*或*被动的*。偶发威胁是没有预谋的威胁，如系统或软件功能失常或实际设备失效。故意威胁是实施蓄意行为的某人造成的威胁。故意威胁可以是使用容易获得的监控工具进行的随意检查，也可以是使用特殊的系统知识进行的精心攻击。故意威胁如果得以实现，则称为*攻击*。主动威胁是导致系统状态或工作有所改变的威胁，如改变数据或毁坏实际设备。被动威胁不引起状态的改变。窃听和搭线窃听就是被动威胁的例子。

*安全弱点*是可被用来破坏系统或系统所含信息的瑕疵或不足。如果存在弱点，那么它有可能使威胁成为现实。

ITU-T建议书认为有四种类型弱点：

- 威胁型弱点来源于很难预测未来可能的威胁；
- 设计和规范型弱点来源于系统或协议设计中的错误或疏忽，使其本质上具有弱点；
- 实现型弱点是在系统或协议实现过程中由错误产生的弱点；以及
- 运行和配置型弱点来源于实现过程中选项的错误使用或软弱的部署策略和做法（例如在无线网络中未采用加密）。

*安全风险*是在安全弱点被利用，即在威胁得以实现的情况下，衡量其所致消极影响的尺度。尽管风险是无法消除的，但一个安全目标是把风险降至可接受的水平。为了做到这一点，有必要理解可能被利用的威胁和弱点，并采取适当的应对措施。这些就是通常所说的安全服务和机制，它们可以通过非技术手段和措施来补充，如实物安全和人员安全。

尽管威胁或威胁的促发因素会改变，但安全弱点在系统或协议的寿命周期内是一直存在的，除非采取处理弱点的具体措施。采用得到非常广泛应用的标准化协议，基于协议的安全风险就会非常高并且是全局范围的。因此，了解和辨识协议中的弱点并在确认弱点后采取措施加以解决是十分重要的。

标准化机构既有责任，也有独特的能力来解决各规范（如体系结构、框架和协议等）中固有的安全弱点。即便充分了解了与信息处理和通信网络有关的威胁、风险和弱点，如果不按照相关的策略系统地实施安全措施，那么也无法达到足够的安全。对这些策略本身，也需要定期进行复审和更新。另外，还需要对安全管理和事故响应做出适当的规定。这包括明确责任并规定在预防、检测、调查和响应安全事故过程中必须采取的措施。

安全服务和机制可以保护电信网络免遭恶意攻击，如拒绝服务、窃听、欺骗、篡改报文（修改、延迟、删除、插入、重播、重选路由、错选路由或者改变报文顺序）、抵赖或伪造。保护技术包括防止攻击、发现攻击和从攻击中恢复，以及管理安全相关信息。保护技术还必须包括预防服务因自然事件（如风暴和地震等）和恶意攻击（如故意或暴力行为）而中断的措施。必须制定有关规定，允许得到正式授权的合法机构进行侦听和监测。

电信网络安全还需要各服务提供商之间开展广泛合作。ITU-T E.408 建议书《电信网络安全要求》对安全要求和框架做了概述，它介绍了电信网络（固定网、移动网、话音网和数据网）常见的安全威胁，并提供了用于规划应对措施的指导原则，以便采取措施减轻源自各种威胁的风险。实施 ITU-T E.408 建议书的要求将有助于推动以下电信网络安全领域的国际合作：

- 信息共享和信息分发；
- 事故协调和危机响应；
- 安全专业人员的招聘与培训；
- 法律实施的协调；
- 保护关键基础设施和关键服务；以及
- 制定适当的法规。

不过，为了成功实现这种合作，对网络的国家级组成部件的要求必须在国家级层面上予以实施。

站在组织观点上，ITU-T X.1205 建议书《网络安全概述》对不同的安全威胁进行了分类，并讨论了在网络不同层面上的安全威胁。

3.3 信息通信技术网络的一般安全目标

电信网的一般安全目标如下：

a) 只有得到授权的用户才能访问和使用电信网；

b) 得到授权的用户应能访问他们获准访问的资产并对其进行操作；

c) 电信网应能根据网络的安全策略设定的水平提供保密功能；

d) 所有用户均应对自己在电信网中的行为负责，也只对自己的行为负责；

e) 为了确保可用性，应保护电信网免受未经请求的访问或操作；

f) 应有可能检索来自电信网的安全相关信息（但只有得到授权的用户才能检索此类信息）；

g) 在检测到破坏安全的行为时，应按照预定计划以受控的方式对其进行处理，尽量减小潜在危害；

h) 在检测到违反安全的行为之后，应有可能恢复正常的安全级别；以及

i) 电信网的安全体系结构应能提供一定的灵活性，以便支持不同的安全策略和不同强度的安全机制。

通过实施以下安全服务，可以实现安全目标 (a) - (e)：

- 机密性；

- 数据、系统和程序完整性；
- 责任制，包括认证、不可抵赖和访问控制；以及
- 可用性。

一种越来越重要的信息通信技术网络是下一代网络（NGN）。NGN的安全要求和目标将在第8节中讨论。

3.4 安全标准的理由

对国际电信通用网络安全框架的要求来自不同的源头，包括客户/订户、公共团体/政府机构以及网络运营商/服务提供商。对电信网络的安全要求宜通过国际公认的安全标准来解决，因为相比为每一个方案提出一种单独的方法，这样做有助于提高方法的共性，有助于实现互联，以及有助于提高成本效益。

在某些情况下，与被保护的资产价值相比，提供和使用安全服务与机制可能相当昂贵，因此，根据被保护对象的要求来提供客户定制的安全服务与机制的能力就显得非常重要。不过，具备提供定制安全服务的能力可产生多种多样可能的安全特性组合。因此，最好有一个覆盖大范围电信网络服务的*安全简表*，以确保能在不同的实施方案中使用不同的选项组合。标准化以及使用标准化的简表有助于实现解决方案和产品的互操作性和重复利用，意味着可以更快、更便宜地达成安全目标。

标准化的安全解决方案对系统的供应商和用户的重要益处包括：达成产品开发的规模效益，实现电信网络中各组成部件之间的互操作性。

3.5 ITU-T安全标准的发展

如在下文中所要看到的那样，近年来，ITU-T的安全工作取得了巨大发展，在下文中将对许多建议书单独进行更加详细的论述。在此只对发展过程中与安全要求密切相关的一些关键问题做一论述。

通常依据网络和/或系统面临的威胁、网络和/或系统内在的弱点以及为了应对威胁和减少弱点而必须采取的措施来定义信息通信技术的安全要求。保护要求扩展至网络及其组成部件。在1991年版的ITU-T X.800建议书《CCITT应用的开放系统互连的安全体系结构》中对安全的基本概念进行了定义，包括威胁、弱点和安全应对措施。之前提到的2004年版的ITU-T E.408建议书《电信网络安全要求》构建于ITU-T X.800的概念和术语之上。ITU-T E.408建议书是通用性质的，未确定或讨论具体网络的要求。未考虑任何新的安全服务。相反地，建议书主要关注的是现有安全服务的使用问题，这些安全服务由其他ITU-T建议书进行定义或者来自其他机构的相关标准。

在2008年版的ITU-T X.1205《网络安全概述》中，阐明了需要应对数量和种类都在日益增长的网络威胁（病毒、蠕虫、特洛伊木马、欺骗攻击、身份窃取、垃圾邮件和其他形式的网络攻击）。该建议书旨在奠定一个知识基础，以便为安全的未来网络提供帮助。对可用来应对威胁的各种不同技术进行了讨论，包括路由器、防火墙、抗病毒保护、入侵检测系统、入侵保护系统、安全计算、审计和监控。也对网络保护原则进行了讨论，如深度防御和接入管理等。对风险管理策略和技术进行了评估，包括在保护网络安全中培训和教育所起的作用。还提供了基于所讨论的技术来保护网络安全的例子。

ITU-T X.1205建议书将网络安全定义为可用于保护网络环境、组织和用户资产的工具、策略、安全概念、安全防卫措施、指导原则、风险管理方法、行动、培训、最佳做法、保障和技术的集合。所谓的资产包括连接的计算设备、计算用户、应用/服务、通信系统、多媒体通信以及网络环境中所传送和/或所储存信息的总和。如此处所定义的那样，网络安全确保达成和维护组织的安全特性（包括可用性、完整性和机密性），并保护好用户的资产，以应对网络环境中相关的安全风险。

在当今的商业环境中，边界的概念正在消失。内部网络和外部网络之间的边界正变得“越来越窄”。各种应用以分层的方式在网络上运行。对这些层的每一层以及层与层之间，都必须保证安全。分层式的安全方法使得各组织能够创建多层防御体系，以应对各种威胁。

可利用网络安全技术来保证系统的可用性、完整性、真实性、机密性和不可抵赖性，以及确保用户的隐私得到适当保护。也可利用网络安全技术来建立用户的可信赖性。

各组织需要制定一个全面的计划来处理各自特定的安全问题。安全无法“一劳永逸”。应将安全看做一个不断变化的过程，它涉及系统、网络、应用和资源的保护。此外，安全必须是全面综合的，虑及系统的所有层。采用分层式的安全方法，并结合强劲的策略管理和具体实施，将为安全解决方案提供各种可能的选择，解决方案应是模块化的、灵活的和可升级的。

当前的网络安全技术包括：

– 加密：这项功能强大的技术支持众多的安全服务，包括在传输过程中以及在储存状态下对数据进行加密；

– 访问控制：旨在限制用户访问、使用、查看或修改主机或网络上信息的能力；

– 系统完整性：旨在确保系统及其数据不被未经授权的各方或以未经授权的方式修改或破坏；

– 审计、日志和监控：在遭受攻击期间以及遭受攻击之后，帮助系统管理员收集和评估网络日志。日志中的数据可用来评估网络所用安全策略的有效性；

– 管理：帮助系统管理员评估和配置其主机和网络上的安全设置；管理控制措施可用来验证网络的适用性以及其所属各要素的设置情况。

3.6 人员和物理安全要求

大部分ITU-T安全相关建议书主要关注系统和网络的技术方面问题。在ITU-T X.1051建议书《电信组织的信息安全管理指导原则》中，对人员安全问题的某些方面进行了论述。物理安全也是保护方面一个非常重要的问题，但总的说来，它不在ITU-T的主要工作范围内。不过，在ITU-T X.1051建议书中对一般性的物理安全要求进行了论述，对与外部设施有关的物理安全问题在下述的两个文件中进行了论述。

有关外部设施的物理保护要求包括需要确保硬件能够抵御火灾、自然灾害以及偶然或故意破坏的威胁。实现对系统组成部件、线缆、外壳、机箱等保护的防线在ITU-T出版物《公众网的外部设施技术》（1991年）和《应用计算机和微处理器构建、安装和保护电信电缆》（1999年）中进行论述。这些文件还论述了系统监控问题，以防止遭到损害，并提出了如何以最快的方式对出现的问题做出反应并恢复系统功能性的建议。

4. 安全体系结构

4 安全体系结构

安全体系结构以及相关的模型和框架，规定了一种结构和范畴，在这种结构和范畴下，可以以一种一致的方式来制定相关的技术标准。20 世纪 80 年代初期，确定需要一个框架，在此框架下，可以将安全性施用于分层的通信体系结构。开放系统安全体系结构（ITU-T X.800 建议书）由此形成。这是为支持安全服务和机制而开发一套体系结构标准的第一步。这一工作大多是与国际标准化组织（ISO）协作完成的，导致形成了更多的标准，包括规定如何将特定类型的保护施用于特定环境的安全模型与框架。

之后，确定了对通用安全体系结构和应用特定的安全体系结构的需求。《提供端对端通信的系统的安全体系结构》（ITU-T X.805 建议书）以及诸多应用特定的体系结构由此形成，用于解决诸如网络管理、对等通信和移动万维网服务器等方面的问题。将在本节后面论述的 ITU-T X.805 建议书，通过给出旨在提供端对端网络安全的安全解决方案而对 X.800 系列的其他建议书做了补充。

4.1 开放系统安全体系结构和相关标准

第一个要标准化的通信安全体系结构是 ITU-T X.800 建议书《开放系统安全体系结构》。该建议书规定了可以按照所需保护的环境施用的安全相关体系结构要素。尤其是 ITU-T X.800 建议书，概括描述了安全服务和用于提供这种服务的相关安全机制。它还按照七层开放系统互连（OSI）基本参考模型规定了实施安全服务最适宜的位置。

ITU-T X.800 建议书关注的只是某条通信路径直观的性能，这些性能允许终端系统间进行安全的信息传送。该建议书并未打算提供任何种类的实施规范，也未给出任何方法来评估某种实施方案与该标准或任何其他安全标准的一致性。该建议书也根本没有表明终端系统为支持通信安全特性可能需要的任何附加安全措施。

尽管 ITU-T X.800 是作为 OSI 安全体系结构而专门制定的，但 ITU-T X.800 的基础概念已经显示出具备更广的适用性和包容性。该标准特别重要，因为其中的基础安全服务（*身份认证、访问控制、数据机密性、数据完整性*和*不可抵赖性*）以及如*可信功能性、事件检测*和*安全审计*与*安全恢复*等更一般性（普遍）服务的定义，代表了这方面第一个国际一致意见。它还指明了可以使用哪种安全机制来提供安全服务。在 ITU-T X.800 建议书之前，关于所需的基础安全服务都有哪些以及每种安全服务到底都起什么作用，存在各种各样的意见。ITU-T X.800 反映了关于这些安全服务的、强烈的国际一致意见。

ITU-T X.800 建议书代表了关于描述安全特性所用术语的含义、关于保护数据通信所需的安全服务集以及关于这些安全服务的性质的一种重要的一致意见，其价值和普遍适用性就来自这个事实。

在 ITU-T X.800 建议书的形成过程中，还确定了对额外的相关通信安全标准的需求。结果是，开展了关于若干辅助性标准和补充性体系结构建议书的工作。下文将讨论其中的一些建议书。

4.2 安全服务

制定安全框架是为了对 ITU-T X.800 建议书中定义的各个安全服务提供全面、统一的描述。这些框架旨在从各方面讨论安全服务如何施用于特定的安全体系结构，包括未来可能出现的安全体系结构。

框架重点关注的是为系统、系统内的对象和系统间的交互提供保护。框架不涉及系统或机制的构建方法。

框架既涉及数据要素，也涉及用于提供特定安全服务的操作序列（不包括协议要素）。这些服务可用于系统内相互通信的实体，也可用于系统间交换并由系统管理的数据。

安全框架（ITU-T X.810 建议书）综述介绍了其他框架，阐述了在所有框架中使用的共同概念，包括安全域、安全授权和安全策略。该建议书还说明了可用于安全地传送认证与访问控制两种信息的一种通用数据格式。

*认证*是对一个实体声称的身份提供保证。实体不仅包括人类用户，还包括设备、服务和应用。认证还对一个实体未试图冒名顶替或未经授权地重播一个先前的通信提供保证。ITU-T X.800 建议书确定了两种形式的认证：*数据来源认证*（即证实所收数据的来源是声称的那个来源）和*对等实体认证*（即证实某个关联中的对等实体是声称的那个对等实体）。*认证框架*（ITU-T X.811 建议书）定义了认证的基本概念；确定了认证机制的可能类别；定义了这些机制类别的服务；确定了支持这些机制类别的协议的功能要求；确定了认证的一般管理要求。

*访问控制*是为了防止未经授权地使用资源，包括防止以未经授权的方式使用资源。访问控制确保只有得到授权的人员或设备才被允许访问网络单元、储存的信息、信息流、服务和应用。*访问控制框架*（ITU-T X.812 建议书）对一个模型做了说明，包括开放系统中访问控制的各个方面、与其他安全功能（如认证和审计）的关系以及访问控制的管理要求。

*不可抵赖性*是防止实体事后否认其实施了某一行为的能力。不可抵赖性涉及确认可在事后用于戳穿虚假主张的证据。ITU-T X.800 建议书说明了两种形式的不可抵赖服务：*有交付证据的不可抵赖*，它用于戳穿接收者否认曾收到数据的谎言；*有来源证据的不可抵赖*，它用于戳穿发送者否认曾发出数据的谎言。不过更一般地讲，不可抵赖性的概念可以适用于许多不同的范围，包括数据生成、提交、储存、传输与接收的不可抵赖性。*不可抵赖性框架*（ITU-T X.813 建议书）扩展了 ITU-T X.800 建议书中所述的不可抵赖安全服务的概念，并给出了开发这些服务的框架。它还确定了支持这些服务的可能机制和不可抵赖性的一般管理要求。

机密性是不向未经授权的个人、实体或过程提供信息或泄露信息的属性。机密性服务的目的是防止未经授权泄露信息。机密性框架（ITU-T X.814 建议书）通过定义机密性的基本概念和可能类别以及每一类别机密性机制所需的设施，论述了在信息检索、发送与管理中的机密性问题。它还确定了所需的管理与支持服务，以及同其他安全服务与机制的交互作用。

数据完整性是指数据没有以未经授权的方式被改变的属性。总的来说，完整性服务涉及需要确保数据没有受损，或者如果受损，让用户了解这一事实。完整性框架（ITU-T X.815 建议书）论述了在信息检索、发送与管理中的数据完整性问题。它定义了完整性的基本概念，确定了完整性机制可能的类别以及支持每一类别完整性机制所需的设施、管理和相关服务。（注意，尽管安全体系结构标准主要关注的是数据的完整性问题，但完整性方面的其他问题对安全而言也很重要，如系统的完整性。）

4.3 提供端对端通信的系统的安全体系结构

2003 年，在对网络安全体系结构进行了更深入的审查后，批准了 ITU-T X.805 建议书《提供端对端通信的系统的安全体系结构》。该体系结构建立在 ITU-T X.800 建议书基础之上，并对某些概念以及上面讨论的安全框架进行了扩展，可适用于各种各样的网络，并与具体的技术无关。

4.3.1 ITU-T X.805体系结构的要素

ITU-T X.805 体系结构是根据三个主要概念为端对端网络而定义的，即安全层、平面和尺度。为保证端对端安全，在区分跨不同层和平面的要求时使用了分层次的方法，方法是在各个尺度中都设计了安全措施，用以应对特定的威胁。图 1 描述了该体系结构的各要素。

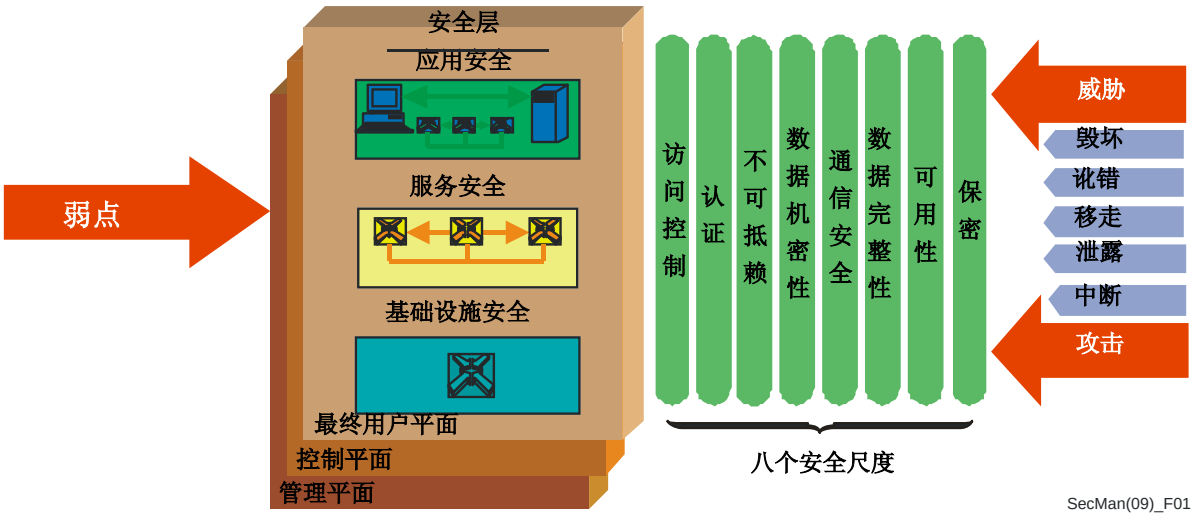


图 1 – ITU-T X.805建议书安全体系结构的要素

在 ITU-T X.805 建议书中，一个*安全尺度*指的是一组旨在解决某个特定的网络安全问题的安全措施。ITU-T X.800 建议书的基本安全概念（*访问控制*、*认证*、*数据机密性*、*数据完整性*和*不可抵赖性*）与 ITU-T X.805 建议书相应的*安全尺度*的功能性是匹配的（如图 1 所示）。另外，ITU-T X.805 建议书引入了三个不在 ITU-T X.800 建议书中的安全尺度（*通信安全*、*可用性*和*保密*）。这些安全尺度提供了额外的网络保护，以抵御所有主要的安全威胁。这些安全尺度不受网络所限，可扩展至各种各样的应用和最终用户信息。安全尺度适用于向其客户提供安全服务的各服务提供商或企业。

ITU-T X.805建议书的八个安全尺度如下所述：

- *访问控制*安全尺度：防止未经授权使用网络资源，并保证只允许得到授权的个人或设备接入网络单元、储存的信息、信息流、服务和应用；
- *认证安全*尺度：用于证实通信实体的身份，确保参与通信的各实体（如个人、设备、服务或应用）所声称之身份的合法性，并对一个未试图冒名顶替或未经授权地重播一个先前通信的实体提供保证。
- *不可抵赖性*安全尺度：通过给出各种网络相关活动的可用证据（如义务、意图或承诺的证据；数据来源的证据；所有权的证据；资源使用的证据），为防止个人或实体否认实施了涉及数据的某种行为提供了方法；它还确保可提供给第三方用于证实已发生某种事件或行为的证据是可用的；
- *数据机密性*安全尺度：防止数据遭受未经授权的泄露，确保未经授权的实体无法理解数据内容；
- *通信安全*安全尺度：确保信息只在得到授权的端点间流动，也就是说，信息在这些端点间流动时无法改向或被中途拦截；
- *数据完整性*安全尺度：确保数据得到保护，防止数据遭受未经授权的修改、删除、生成和复制，并在出现可能对数据完整性造成破坏的活动时发出告警；
- *可用性*安全尺度：确保对网络单元、储存的数据、信息流、服务和应用的授权访问不因影响网络的事件而被拒绝；以及
- *保密*安全尺度：对从观察网络活动中可能得出的信息提供保护；这种信息的例子包括用户访问过的网站、用户的地理位置以及服务提供商网络中设备的IP地址与DNS名称。

如图1所示，除了安全尺度，ITU-T X.805建议书还定义了三个安全层和三个平面。为了提供一种端对端安全解决方案，安全尺度必须适用于网络设备和设施组的某一层次，这些层次指的就是*安全层*。一个*安全平面*代表的是一种受安全尺度保护的网络活动。一个安全平面代表一种类型的受保护网络活动。

安全层涉及适用于网络单元和系统的要求，以及与这些单元相关的服务和应用。定义这些层的好处之一是在提供端对端安全时不同应用允许重复使用。每一层的弱点是不同的，因此应根据每层的不同要求来分别确定各层的应对措施。这三个层是：

- 基础设施层：包括网络传输设施和单独的网络单元；属于基础设施层组成部件的例子有单独的路由器、交换机和服务器以及其间的通信链路；
- 服务层：涉及为客户提供的网络服务的安全；这些服务的范围从基础连接性服务（如租用线服务）延伸到增值服务（如即时消息服务）；以及
- 应用层：涉及对客户所用的网络应用的要求；这些应用可能像电子邮件那么简单，也可能像协同视觉化那么复杂，例如在石油勘探或汽车设计等场合，需要使用清晰度非常高的视频传送。

安全平面涉及与网络管理活动、网络控制或信令活动和最终用户活动相关的特定安全要求。网络应设计得能使在某一安全平面上发生的事件独立于其他的安全平面。

这些安全平面是：

- 管理平面：关注的是运营、管理、维护和提供服务活动，如向某个用户或网络提供服务；
- 控制平面：与通过网络建立（和修改）端对端通信的信令有关，与网络中所用的媒介或技术无关；
- 最终用户平面：涉及订户访问与网络使用的安全；该平面还负责最终用户数据流的保护问题。

ITU-T X.805体系结构可用于指导制定安全策略、技术体系结构以及事故应对与恢复计划。该体系结构还可用做安全评估的基础。一旦实施了安全计划，就必须予以维护，以适应不断变化的威胁环境。ITU-T X.805安全体系结构可以通过确保对安全计划的修改顾及每一安全层与平面的适用安全尺度，来协助维护安全计划。

尽管ITU-T X.805是一种网络安全体系结构，但某些概念可以延伸至最终用户设备。在ITU-T X.1031建议书《安全体系结构中最终用户和电信网络的角色与作用》中对该主题进行了论述。

4.3.2 网络及其组成部件的可用性

网络可用性是信息通信技术可用性的一个重要方面。如上所述，ITU-T X.805建议书可用性安全尺度的目的是确保服务的连续性，以及确保经过授权地接入网络单元、信息和应用。灾难恢复解决方案也包括在该安全尺度内。

基础设施安全层由网络传输设施以及受安全尺度保护的单独的网络单元组成。基础设施层代表了网络、网络服务与应用的基本构件。归属基础设施层的组成部件的例子包括路由器、交换机和服务器，以及路由器、交换机和服务器之间的通信链路。

用于限制网络资源不可用性风险与后果的功能、实施和运行要求数量众多、五花八门。需要考虑的因素很多，包括差错性能、拥塞控制、失效报告和纠正措施。ITU-T G.827建议书《端对端国际恒比特率数字路径的可用性性能参数和目标》定义了路径单元的网络性能参数和目标，以及国际恒比特率数字路径的端对端可用性。ITU-T G.827建议书附件A提供了详细的、用于评估端对端可用性的方法，并提供了路径拓扑结构和端对端路径可用性计算的例子。其他涉及网络性能的建议书包括：ITU-T G.1000《通信服务质量：框架和定义》、ITU-T G.1030《为数据应用估计IP网络的端对端性能》、ITU-T G.1050《用于评估经由IP协议的多媒体传输性能的网络模型》以及ITU-T G.1081《IPTV的性能监控点》。

4.4 实施指南

ITU-T安全体系结构标准是ITU-T X.800-Ⅹ.849系列建议书的一部分。实施指导原则作为该系列建议书的一个增补提供（ITU-T X.800-X.849系列X.Sup3 － 《系统和网络安全实施指导原则增补》）。该增补提供了有关网络安全生命周期中关键活动的指导原则。这些指导原则涉及四个领域：技术安全策略；层次型资产鉴别；基于层次型资产的威胁、弱点和减缓；安全评估。这些指导原则及其相关的模版旨在系统实施网络安全规划、分析和评估。

4.5 一些应用特定的体系结构

在本节中，介绍了一些与特定应用有关的体系结构的问题。

4.5.1 对等通信

对等通信（P2P）网络是网络体系结构的一种实例化。相对客户端/服务器模型，在P2P网络中，所有的对等体拥有相等的权限和责任。在P2P通信中，一个对等体既可以是服务器，也可以是客户端。当在P2P网络中交换数据或报文时，一个对等体直接与其他对等体进行通信。由于需要将业务流量和处理分发给每一个对等体，因此P2P网络无需高性能的计算能力或大宽带的网络。

P2P网络是在电信网络和互联网之上的一种重叠网络。不同于传统的集中式资源，在P2P网络中，在不同节点之间它可以采取各种各样不同的连接方式，在每个节点上它都拥有计算能力和储存空间。

随着电信网络和计算技术的迅猛发展，在分布节点上将可获得越来越多的信息和计算资源，而不仅仅来自有限数量的集中式服务器。

通常，使用P2P网络，通过特别的连接方式来连接各节点。此类网络可用于众多目的。包含话音、视频、文本或其他数字格式内容的共享数据文件非常常见。实时通信数据也采用P2P技术，如电话业务。

4.5.1.1 对等网络的安全体系结构和运作

在ITU-T X.1162建议书中描述了一种可用于各种各样P2P网络的、通用的安全相关体系结构模型。

图2显示了基本的P2P服务体系结构。各对等体处理的信息在不同用户间直接进行交换。由于没有任何中央服务器来储存信息，因此各对等体在能对目标数据进行检索之前，需要找到是哪些对等体拥有这些目标数据。此外，各对等体必须允许来自其他对等体的访问，以便进行数据交换。

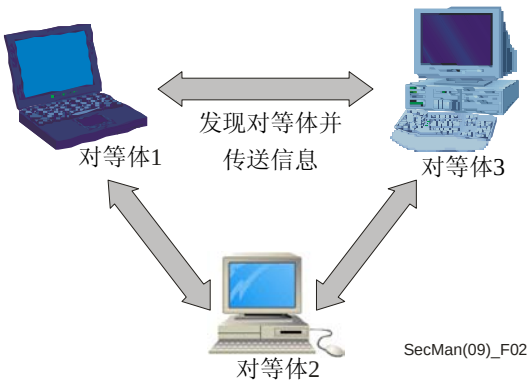


图 2 – P2P服务体系结构

图3显示了P2P网络物理和逻辑退休金。在物理的P2P网络中，用户可以通过一台设备来加入P2P服务。术语“对等体”通常用于表示一个用户或者用户所有的一台设备。P2P网络中不同实体之间的连接类型可以分类为：

- 通过某个域内对等体的连接；
- 通过某个域间对等体的连接；
- 通过位于另一个网络域中的某个服务提供商对等体的连接。

图3还显示了作为传送层上一个虚拟网络的P2P网络逻辑体系结构。它假定各对等体的工作不受网络物理体系结构的限制，一个对等体可以与任何其他对等体进行通信，而不管它位于何处（需要的话，在某个超对等体的帮助下完成）。对等网络的结构分为两层：P2P重叠层和传送层。传送层负责传送来自/去往上一层的分组，重叠层负责提供P2P服务。

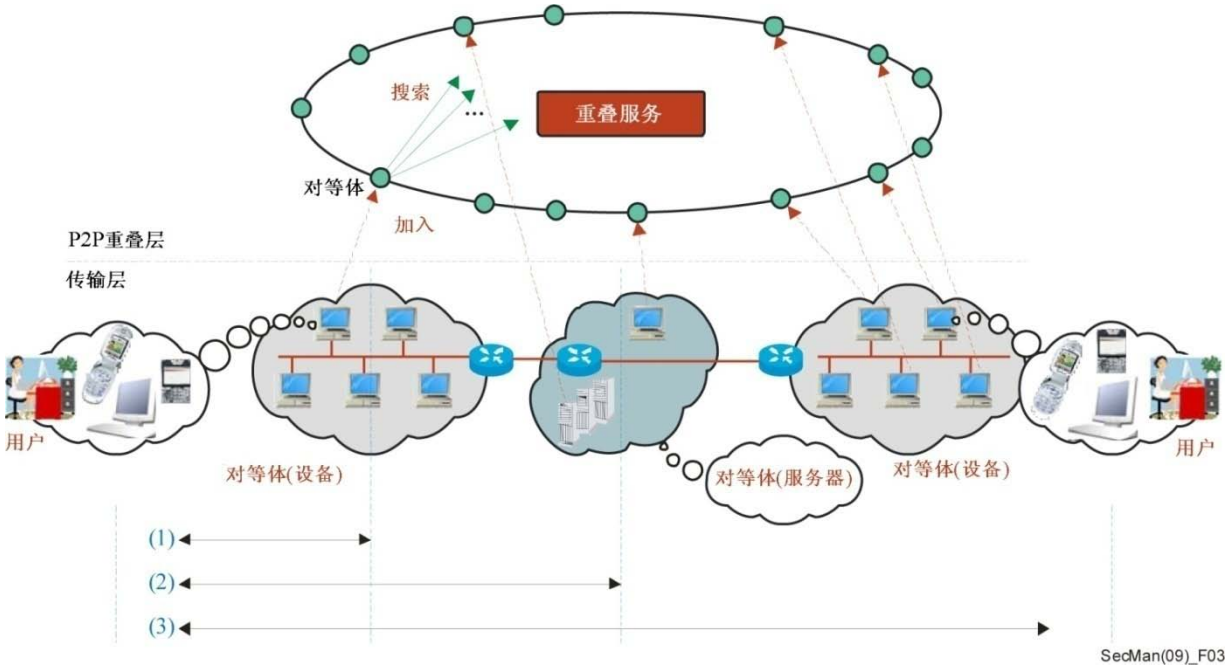


图 3 – P2P网络的体系结构参考模型

4.5.1.2 安全对等通信的框架

在ITU-T X.1161建议书《安全对等通信框架》中，规定了P2P网络的安全要求，以及满足这些要求所需的服务和机制。

对P2P通信的威胁包括窃听、干扰、接入与修改、未经授权的访问、抵赖、中间人攻击、女巫攻击。应对P2P威胁的各种措施如表3所示。

表 3 – P2P安全要求与应对措施之间的关系

功能 / 要求	加密	密钥交换	数字签名	信任管理	访问控制	数据完整性机制	认证交换	公证	安全路由	业务流量控制机制	标识指派
用户认证	X	X	X	X	X		X				X
匿名	X			X							X
隐私	X				X		X				
数据完整性	X	X	X		X	X	X				
数据机密性	X	X			X		X				
访问控制					X		X				X
不可抵赖			X				X	X			X
易用性					X						
可用性					X		X		X	X	
可追溯性			X						X		X
业务流量控制		X								X	

4.5.2 保证移动万维网服务中报文安全的安全体系结构

在ITU-T X.1143建议书《保证移动万维网服务中报文安全的安全体系结构》中，对用于保证移动万维网服务中报文安全的安全体系结构以及背景知识进行了阐述。该标准提供了：

- 一种用于保证报文安全的安全体系结构，它依赖于适当的万维网服务策略机制；
- 支持完全万维网服务安全协议组的各应用间的相互作用机制和服务情景，以及不支持完全万维网服务安全协议组的各传统应用间的相互作用机制和服务情景；
- 报文认证、完整性和机密性机制；
- 基于报文内容的报文过滤机制；以及
- 一种报文安全参考体系结构和安全服务参考情景。

图4显示了ITU-T X.1143用于移动万维网服务的安全体系结构。

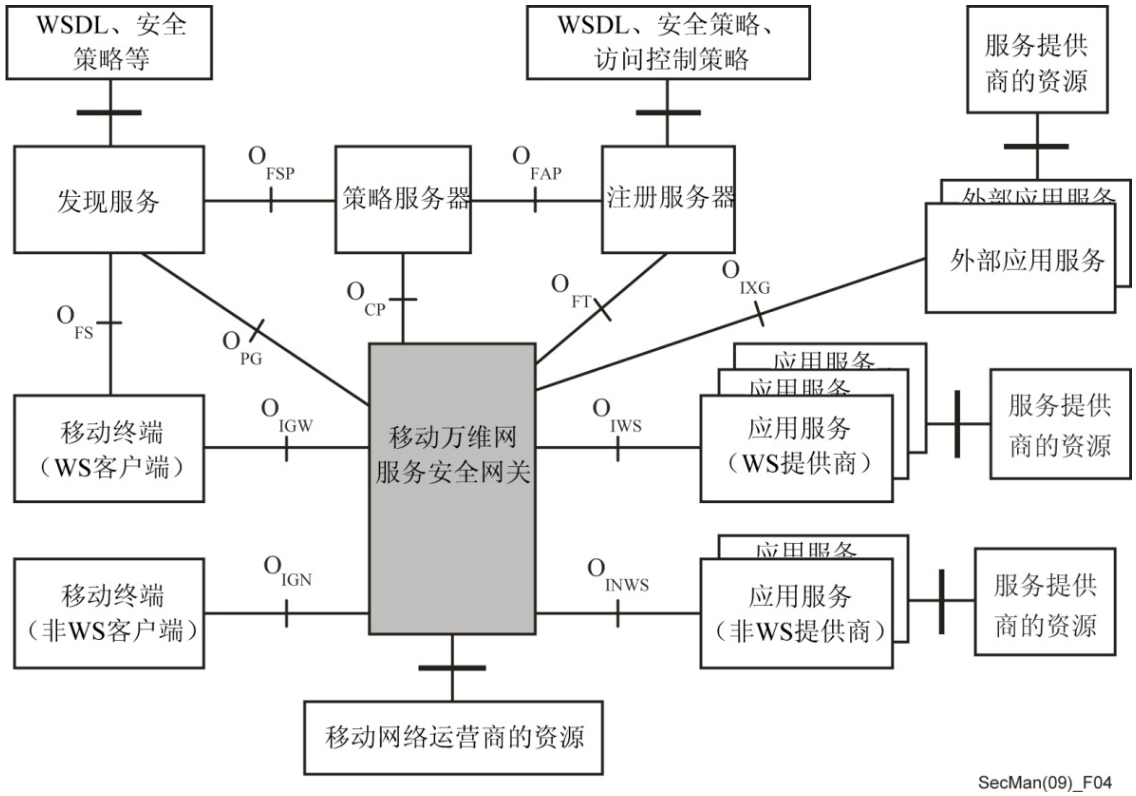


图 4 – 用于移动万维网服务的安全体系结构

安全体系结构包括以下组成部件：

- 移动终端，它们是移动万维网服务的客户端；
- 一个移动万维网服务安全网关（MWSSG），来自各移动客户端的所有请求均送至MWSSG，它还执行访问控制；
- 策略服务器，负责管理与报文安全处理有关的安全策略以及报文访问控制策略；
- 应用服务，负责向客户端提供各种各样的增值服务；
- 号码簿服务，负责储存应用服务的接口信息以及客户端接入应用服务的相关安全策略；以及
- 注册服务器，驻留于移动运营商的内部域，负责管理应用服务的接口信息、客户端接入应用服务的相关安全策略以及与目标服务有关的访问控制策略。

4.6 其他网络安全体系结构和模型

将在下文论述有关网络安全体系结构的其他方面问题。具体而言，见第7.2节“网络管理体系结构”、第8.1节“下一代网络（NGN）安全”、第8.4.1节“IPCablecom体系结构”、第8.5.1节“IPCablecom2体系结构”以及第9.2节“IPTV”。

5. 安全管理问题

5 安全管理问题

安全管理是一个宽泛的主题，涉及许多与系统和网络资源接入控制和保护、事件监控、报告、策略与审计有关的活动，并涉及与这些功能和活动有关的信息管理。在本节中，论述了一些通用的安全管理活动。与保证网络基础设施安全有关的安全管理活动将在第7节中进行讨论。

5.1 信息安全管理

像其他资产一样，信息是维持组织业务正常运转的一个重要因素。信息可以打印、可以以电子形式储存、可以通过邮件传送、可以以电子形式通信、可以在屏幕上显示、可以以口头形式交流或以其他方法传达。不管采用何种形式或具有何种功能，或者采取何种方式来共享或储存，信息都应得到适当的保护。

一旦信息安全遭到破坏，例如未经授权地接入一个组织的信息处理系统，那么该组织可能遭受巨大的损害。因此，对一个组织而言，通过实施结构化的安全管理过程，保护其信息安全是至关重要的。

有效的信息安全管理通过实施一系列适当的控制措施来实现。用于电信设施、服务和应用的这些控制措施，需要建立、实施、监控、评估并持续改进。不能成功部署实施有效的安全控制措施将导致组织无法达成其安全和商业目标。

订户使用其设施来处理信息（保护个人数据、机密数据和敏感的商业数据）的电信组织，需要确保拥有适当的安全保护水平，以防止对信息造成破坏，也就是说，它们需要建立一个有效的信息安全管理系统（ISMS）。

得到最广泛认可的信息安全管理系统（ISMS）规范是在ISO/IEC 27000 ISMS系列标准中定义的规范，它包括有关信息安全管理系统基础、要求、工作准则、实施指导原则和相关主题的各种标准。基于ISO/IEC 27002《信息安全管理系统行为准则》，ITU-T和ISO/IEC联合制定了ITU-T X.1051 | ISO/IEC 27011《电信组织信息安全管理指导原则》。

ITU-T X.1051建议书建立了在电信组织中启动、实施、维护和改进信息安全管理的指导原则和一般准则，并为信息安全管理提供了实施基线，以确保电信设施和服务的机密性、完整性和可用性。针对电信部门的特定指南包括了以下主题：

- 信息安全组织；
- 资产管理；
- 人力资源安全；
- 物理和环境安全；
- 通信和运营管理；
- 访问控制；

- 信息系统采办；
- 开发和维护；
- 事故管理；以及
- 业务连续性管理。

除了应用在ITU-T X.1051建议书中所述的安全目标和控制措施，电信组织还需考虑到以下特殊的安全问题：

- 必须保护号与电信组织有关的信息，以防未经授权的泄露；这意味着不泄露所通信的信息，包括信息是否存在、信息内容、信息来源、信息目的地、日期和时间；
- 应对电信设施的安装和使用情况实施控制，以确保通过有线、无线或任何其他方法传送、中继或接收的信息的真实性、准确性和完整性；以及
- 为提供通信服务而对电信信息、设施和媒体进行的所有访问都必须是经过授权的，并应只在需要的时候才提供；作为可用性规定的一个扩展，对在紧急情况下的重要通信，电信组织应提供优先权，并符合监管要求。

不论媒体或传输模式是什么，都需要对电信组织中的信息安全实施管理。如果不实施适当的信息安全管理，那么与系统使用有关的风险将上升。

在其他组织用户和个人用户传送数据时，电信组织作为中介来提供其服务。因此，必须考虑到以下实时，即电信组织内的信息处理设施不仅被其自身的雇员和承包商所访问和使用，还被组织外各种各样的用户所访问和使用。

记住，电信服务和设施可能与其他服务提供商共享，和/或与其他服务提供商互连，因此电信组织中的信息安全管理必须延伸至网络基础设施、服务应用和设施的各个领域。

5.2 风险管理

风险管理是评估和定量化风险并采取行动确保存在之风险低于某个预先确定之可接受水平的过程。在第3节中，在讨论ITU-T X.1205建议书《网络安全概述》时，对该主题进行了简要介绍。在ITU-T X.1055建议书《电信组织的风险管理和风险简表指导原则》中，包含有更详细的风险管理指导原则，确定了用于减少信息安全风险的各个过程和各种技术。这些过程和技术可用于评估电信安全要求和风险，并帮助选择、实施和更新适当的控制措施，以维持要求的安全水平。

开发了许多特定的方法来解决风险管理问题。ITU-T X.1055建议书为电信组织提供了用于评估和选择适当方法的准则。不过，它未推荐任何具体的风险管理方法。

风险管理过程如图5所示。

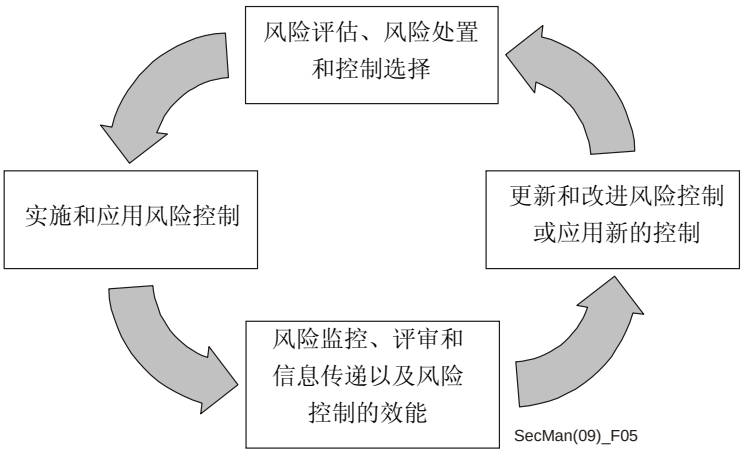


图 5 – ITU-T X.1055风险管理过程

风险简表用于指导整个风险管理过程。特别是用它们来帮助决策过程，并依据其紧迫性，帮助确定各种风险的优先级，以及帮助确定如何分配资源和应对措施。它们还可帮助确定适当的度量方法，与其他工具（如间距分析法）一起，用于风险管理。ITU-T X.1055建议书提供了确定风险简表的指导原则，并包括了一个模版和若干个风险简表的例子。

5.3 事故处置

保持检测、响应和安全相关事故信息分发的协调一致，是安全管理日常工作的一部分。除非所有此类事故均得以适当评估和正确处理，否则对后续的、可能更严重的攻击而言，组织将是脆弱的。

除非拥有一套适当的事故处置程序，否则当检测到一个安全相关的事故时，可能无法正确报告事故或对事故做出正确分析。也可能没有任何程序来提交报告或者获得技术支持或管理指导，尽管因此类事故而引起的问题常常殃及信息技术或网络连接之外的事物。例如，事故可能隐含法律、财政或声誉方面的风险，或者牵涉法律执行方面的问题。缺少有效的事故处置程序可能会出现“很快就修复”或“绕道而行”的现象，而问题并没有真正得到解决、归档和报告，在这种情况下，将存在之后可能出现更严重问题的风险。

随着各组织对一致、有效的网络和运营安全管理需求变得强烈起来，事故处置正成为一件越来越平常的工作。一个经过适当培训和授权的单位或团体可以以一种迅速而正确的方式来处置各种安全事故。

为了能够完成事故处置和事故报告，必须了解事故是如何检测、处置和解决的。通过确定事故处置的一般性结构（即物理事故、行政或组织方面的事故以及逻辑事故），就有可能获得一个有关事故的结构与流程全景图。ITU-T E.409《事故管理机构和安全事故处置：用于电信组织的指导原则》提供了一个概貌和框架，给出了用于规划检测和处置安全相关事故机构的指导原则。ITU-T E.409 建议书是通用性质的，未确定或讨论具体网络的要求。

在报告或处置事故时有一套统一的术语至关重要。使用不同的术语可能造成误解，导致安全事故不能得到足够重视，并无法得到及时处置，以便消除事故，防止事故再次发生。此外，在对事故的定义和理解上，不同的专业、不同的组织、不同的人会各有不同。ITU-T E.409 试图标准化有关事故检测和报告的术语，并依据其严重程度对事故进行分类，如图 6 所示。

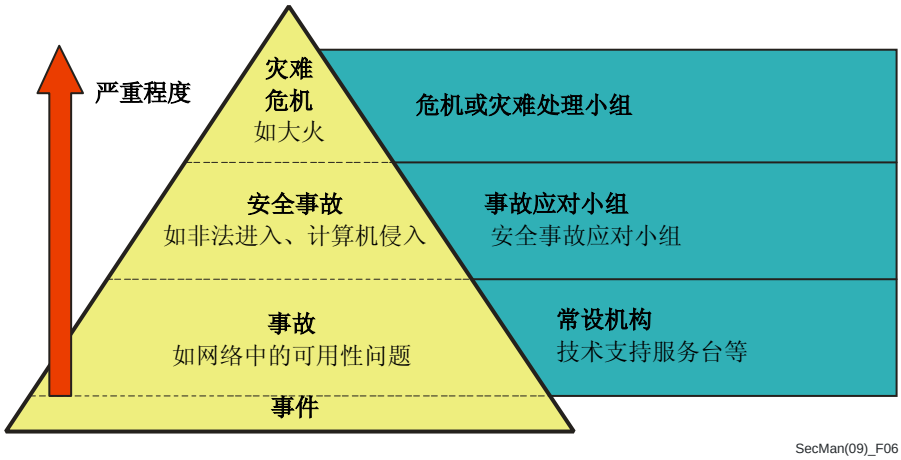


图 6 – ITU-T E.409事件和事故金字塔

ITU-T E.409建议书还定义了事故处置结构（如图7所示），阐述了检测、分类、评估、处置和事故善后工作的程序。

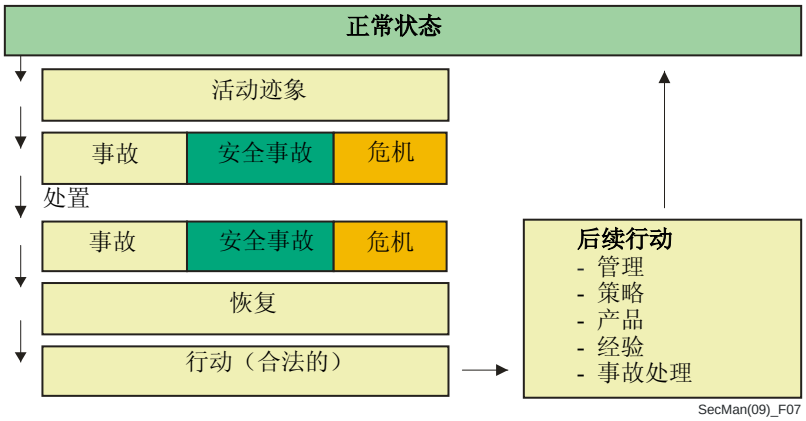


图 7 – ITU-T E.409事故处置结构

最近批准的ITU-T X.1056建议书《电信组织的安全事故管理指导原则》建立在ITU-T E.409建议书基础之上。电信组织需要有适当的过程来处置事故，并防止事故再次发生。在ITU-T X.1056建议书中描述了五个高层事故管理过程以及与安全管理的关系，如图8和图9所示。

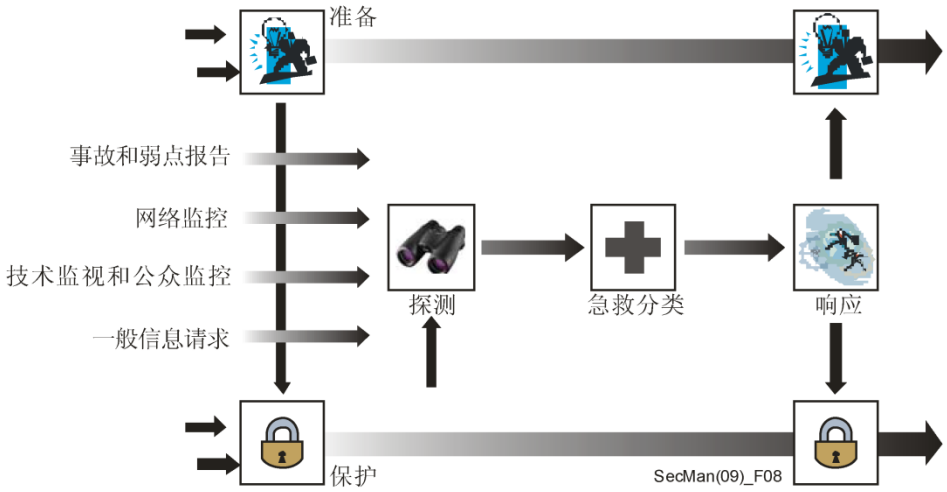


图 8 – 五个高层事故管理过程

（来源：SEI MOSAIC概述：技术报告CMU/SEI-2004-TR-015-定义CSIRT的事故管理过程：一项正在开展的工作）

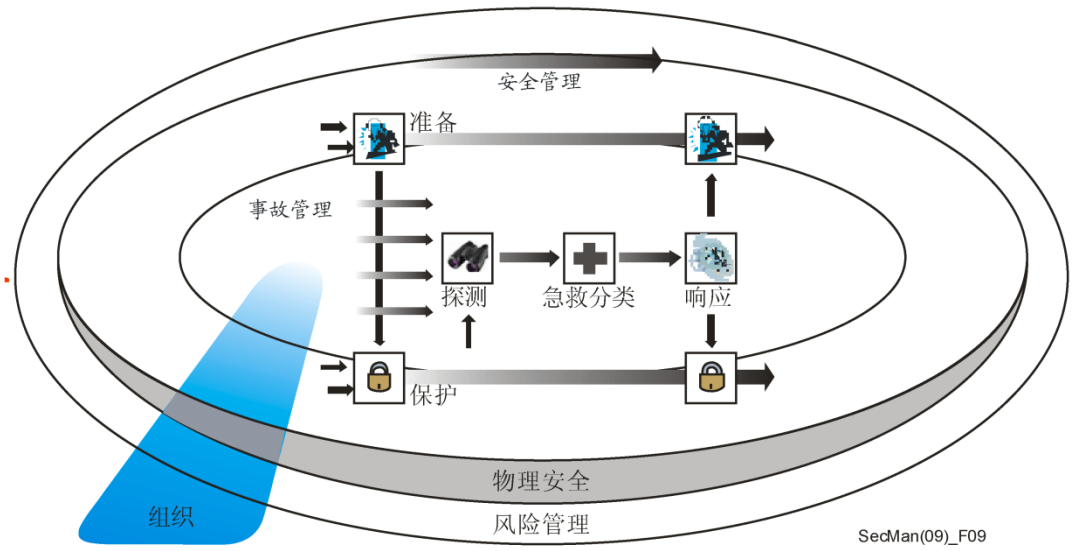


图 9 – 事故管理和安全管理比较

（来源：SEI MOSAIC概述：技术报告CMU/SEI-2004-TR-015-定义CSIRT的事故管理过程：一项正在开展的工作）

此外，ITU-T X.1056建议书还确定了安全事故管理小组能够提供的、一系列积极主动的安全质量管理服务。

6. 号码簿、认证和身份管理

6 号码簿、认证和身份管理

通常，术语“号码簿”是指一个组织有序的信息集或文件集，对其进行查询可以获得特定的信息。在ITU-T内，更一般而言，在安全和电信标准化范畴内，依据ISO/IEC联合制定的ITU-T X.500系列建议书，术语“号码簿”指的是一个信息库。在ITU-T X.500建议书《号码簿：概念、模型和服务概述》中引入并在ITU-T X.501建议书《号码簿：模型》、ITU-T X.509建议书《号码簿：公开密钥和属性证书框架》和ITU-T X.519建议书《号码簿：协议规范》中细化的号码簿，提供了号码簿服务，以方便实体与实体、人与人、终端与终端、分发列表与分发列表等之间的通信和信息交换。除了传统的号码簿服务（如命名、名称至地址的映射以及允许对象与其位置之间的绑定）之外，通过以安全证书的形式定义和持有认证证书，号码簿在支持安全服务方面起着重要作用。特别是ITU-T X.500系列建议书涵盖了两方面的安全问题：

- 保护号码簿信息，主要如ITU-T X.501和ITU-T X.509建议书中所定义的那样；以及
- 公开密钥基础设施（PKI）和特权管理基础设施（PMI）的基本原则，如ITU-T X.509建议书所定义的那样。

本节首先讨论号码簿自身安全的重要性以及保护号码簿信息的需求，而后评述号码簿在支持强认证、公开密钥基础设施、身份管理和远程生物特征识别中的作用。

6.1 号码簿信息的保护

6.1.1 号码簿保护的目标

数据保护是身份管理中需要考虑的一个主要问题，常常集中在号码簿的工作上。号码簿数据保护主要是一个保密问题（即防止未经授权地泄露敏感的个人信息），但它也涉及确保数据完整性和保护数据所代表之资产的问题。

号码簿持有关于各实体的信息。实体信息可能是敏感的，应只透露给那些拥有相应权限和需要知晓的人。

有三个数据保护方面的问题：

- 对试图访问信息的用户进行认证；
- 访问控制，防止数据被未经授权地访问（注 — 访问控制依赖于适当的认证）；以及
- 数据保密，它依赖于适当的访问控制。

几乎从一开始，数据保护特征就是ITU-T X.500建议书的一个重要组成部分。ITU-T X.500建议书是拥有这些重要特征的、唯一的号码簿规范。

6.1.2 号码簿用户的认证

ITU-T X.500号码簿可能允许匿名访问它的某些非敏感信息。不过，为了能够访问更敏感的数据，需要对用户进行某种程度的认证。ITU-T X.500建议书允许进行若干层次的认证，包括：

a) 仅对姓名；

b) 姓名和未经保护的口令（即姓名和以明文形式传送的口令）；

c) 姓名和经保护的口令（即口令与某些额外的信息一起经散列化处理，以确保任何通过重播散列值来访问号码簿的企图都将被检测到）；以及

d) 强认证，当中发送者以数字形式签署某些信息。签署的信息由接收者姓名和某些额外的信息组成，也允许对重播企图进行检测。

对不同类型的访问用户，需要不同程度的数据保护。某个用户的认证程度也影响该用户的访问权限。

6.1.3 号码簿访问控制

使用访问控制来允许或拒绝对号码簿信息片段的操作。出于访问控制的目的，在如何细分号码簿信息和用户上，ITU-T X.500建议书非常灵活。有待保护的信息片段称为保护项。可以对保护项进行分组，以实现共同的访问控制特性。同样，也可以依据访问许可或访问拒绝，对用户进行分组。

一个用户或一组用户的访问权限依赖于认证的程度。相比检索不太敏感的信息，检索敏感信息或更新条目通常需要更高程度的认证。

访问控制还需要考虑数据访问的类型，如读取、增加、删除、更新和改名。在某些情况下，用户可能甚至并不知道某些信息片段是否存在。

访问控制关乎*知情权*。不过*需要知晓*则超出了访问控制的范畴。如果未确定*需要知晓*，那么即使拥有*知情权*，也不允许用户检索信息。如果未确定*需要知晓*，那么泄露信息就可认为是一种侵害秘密行为。

还有其他几种*知情权*不够的例子。例如：

— 即使用户有权检索某些实体的单个邮政地址，它也可能不允许对邮政地址进行批量检索；以及

— 即使用户有权访问某些信息，它也可能与所检索的特定应用无关，在没有任何*需要知晓*的情况下，不得泄露信息。

6.1.4 隐私的保护

ITU-T X.500数据保密很独特，功能非常强大。主要在以下情况下数据保密将成为一个重要的问题，即用户通过提供通用的搜索准则来搜索号码簿，而其结果是可能返回大量的信息。（此类搜索有时称为数据挖掘。）

ITU-T X.500有一个表驱动的服务管理概念，除了提供对通常服务的管理之外，它还提供了数据保密能力。管理者为服务类型和用户组的每种组合创建一个或多个表。为成功实现数据检索，必须有一个表准确匹配服务类型和用户组类型。不过，这还不够。表受到访问控制的保护，也就是说，用户还必须拥有访问相关表的许可。

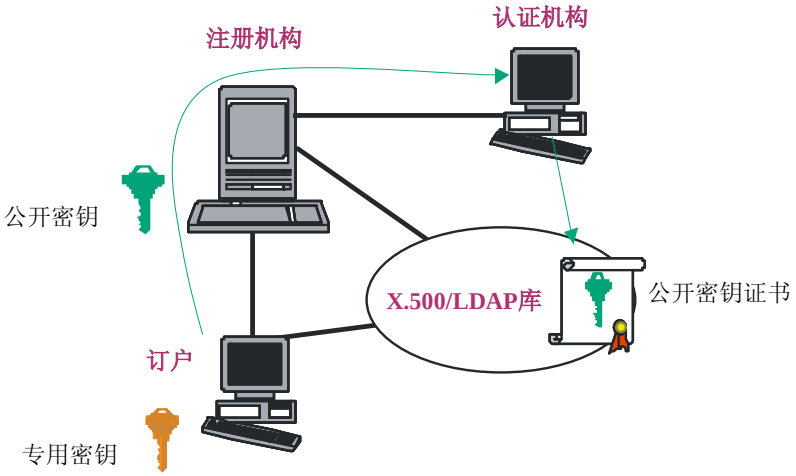
一个表，也称为一个搜索规则，可以持有如下信息：

- 要求的搜索准则，以确保搜索的目标是返回有关一个或很少几个实体的信息；这防止搜索返回大量信息，并防止出现数据挖掘；
- 与服务类型相关的信息片段列表；以及
- 有关号码簿所代表之单个实体的控制信息；在用的表与某个实体的控制信息相互作用，以限制该实体的返回信息；这使得可以依据保密准则为每个实体单独裁剪数据；一个实体可以有特殊的要求，如不泄露邮政地址而可能返回一个伪造的地址；其他实体可能不想其电子邮件泄露给某些用户组。

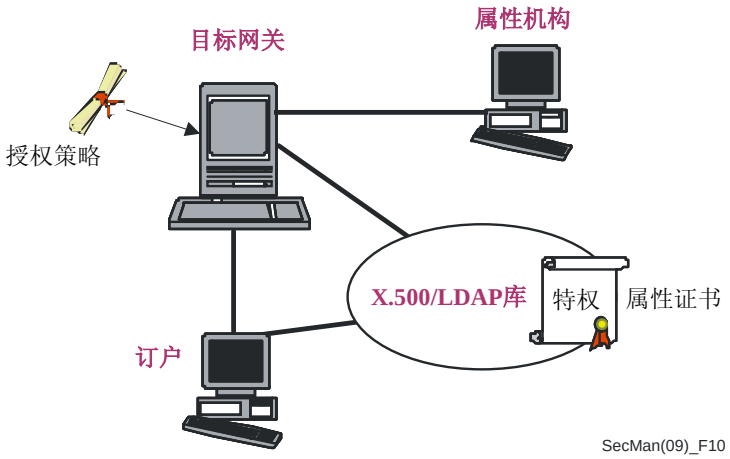
出于许多理由，需要考虑保护敏感的个人信息。若干安全标准、尤其是那些与个体认证和身份管理有关的安全标准，涉及敏感的个人识别信息的收集和储存。越来越多的权限有与收集和使用此类信息有关的法律要求。许多安全服务和机制基于ITU-T标准，作为信息保护机制，来保护从保密角度而言是敏感的信息。许多建议书论及了保密问题，一些建议书直接论述某些技术对保密的影响。例子包括新近批准的ITU-T X.1171建议书《在采用基于标签识别的应用中对保护个人可识别信息的威胁和要求》在有关基于标签的服务的第9.5节中，对此有更详细的论述；以及有关射频识别（RFID）应用中保护个人识别信息的指导原则，作为身份管理（IdM）工作的一部分，现正由第17研究组在制定中（见第6.4节）。

6.2 强认证：公开密钥安全机制

公开密钥基础设施（PKI）支持公开密钥管理，由此支持认证、加密、完整性和不可抵赖性。PKI 的基础技术是公开密钥加密，下文对它做了说明。ITU-T X.509 建议书《号码簿：公开密钥和属性证书框架》提供了基于公开密钥证书和认证机构的强认证公开密钥基础设施（PKI）标准。除规定 PKI 的认证框架之外，ITU-T X.509 建议书还以属性证书和属性机构为基础，规定了特权管理基础设施（PMI），用于在强授权环境中确保用户的权利与特权。PKI 与 PMI 的构成如图 10 所示。



(a) 公开密钥基础设施的组成部件



(b) 特权管理基础设施的组成部件

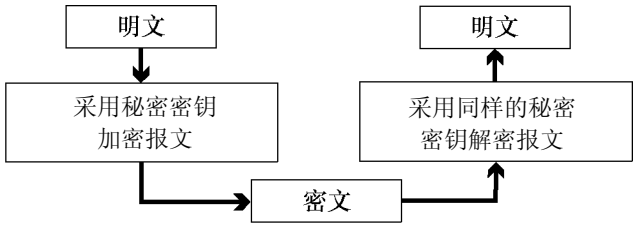
图 10 – PKI和PMI的构成

6.2.1 秘密密钥和公开密钥密码学

对称（或秘密密钥）密码术是指加密和解密使用同一密钥的密码系统，如图11 (a) 所示。在对称密码系统中，通信各方共享一个独特的秘密密钥。由于获知加密密钥即获知解密密钥，反之亦然，因此密钥必须通过安全的途径分发给通信各方。

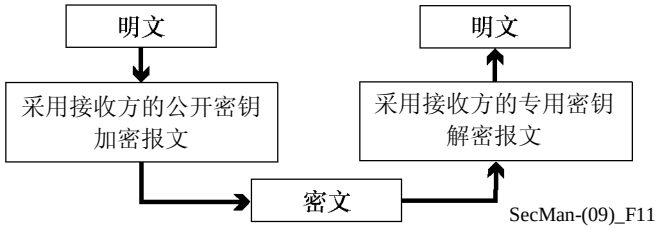
非对称（或公开密钥）密码术系统如图11 (b) 所示使用一对密钥 — 一个公开密钥和一个专用密钥。公开密钥可以广而告之，而专用密钥则必须总是秘而不宣。专用密钥通常存在一个智能卡或令牌上。公开密钥从专用密钥产生，尽管这两种密钥在数学上相关，但没有可行的办法反过来从公开密钥算出专用密钥。要采用公开密钥加密来安全地将保密数据发送给某人，发送者使用接收者的公

开密钥对数据进行加密。接收者用其相应的专用密钥对数据进行解密。公开密钥密码术也可用于对数据施加数字签名，以证实某个文档或报文确实是自称发送者（或发报者）的人发送的。数字签名实际上是一份数据摘要，用签字者的专用密钥产生并附在文档或报文上。接收者用发送者的公开密钥来证实数字签名的有效性。（注 — 某些公开密钥系统采用两对不同的公开密钥/专用密钥，一对用于加密/解密，另一对用于数字签名/验证。）



— 双方共享一个单一的秘密密钥
— 问题：在完全保密的情况下交换密钥是困难的，且不易调整，
也就是说，对大量用户而言是不实用的
— 著名例子：DES(数据加密标准)

(a) 对称（或秘密）密钥加密



— 每一个参与者都有
— 一个不与别人共享的专用密钥
— 一个众人皆知公共密钥
— 问题：比秘密密钥加密慢
— 著名例子：RSA

(b) 非对称（或公开）密钥加密

图 11 – 秘密密钥和公开密钥加密过程说明

采用对称加密，每对用户必须有一对不同的密钥，且必须安全地分发和持有这些密钥。另一方面，采用非对称加密，可以在一个号码簿中公布公开加密密钥，且每个人都可以用同一个（公开）加密密钥向一个特定用户发送数据。这就让非对称加密比对称加密更容易产生变化。不过，从计算时间来看，非对称加密成本较高，因此采用非对称加密对整个报文加密的效率较低。因此，实际上，非对称加密通常用于安全地分发对称密钥，然后采用一种计算效率更高的对称算法，用该对称密钥来对报文的正文进行加密。如果需要一个数字签名，那么先使用一个安全的单向散列函数（如 SHA1 或 MD5）来产生报文摘要（或散列值），而后（采用发送者的专用密钥）对散列值进行加密，并附在报文上。利用发送者的公开密钥，对数字签名进行解密，获得发送者生成的散列值，接收者可以利用这种方式来确认数字签名的有效性，然后建立其自身的、有关所接收报文的散列值。对有效的签名而言，两个散列值必须相同。

如果整个报文（包括报头）是加密的，那么无论采用对称加密还是非对称加密，都不可能将报文发送给接收者，因为经转节点无法确定接收者的地址。因此，报头通常必须是未加密的。

公开密钥系统的安全运转在很大程度上取决于公开密钥的有效性。公开密钥通常以数字证书的形式公布，而数字证书保存在某个 ITU-T X.500 号码簿中。证书不仅含有公开加密密钥以及视情况含有个人使用的签名验证密钥，而且还含有包括证书有效性在内的附加信息。因任何原因而撤销的证书通常都列在号码簿的证书撤销列表（CRL）中。在使用公开密钥之前，通常要按照 CRL 检查其有效性。

6.2.2 公开密钥证书

公开密钥证书（有时被称为“数字证书”）是验证非对称密钥对所有者的一种方式。公开密钥证书将一个公开密钥与其所有者紧紧联系在一起，并经证明这一关联的可信机构数字签发。这一可信机构被称为认证机构（CA）。国际认可的、标准的公开密钥证书格式在ITU-T X.509 建议书中定义。一个ITU-T X.509 公开密钥证书包含一个公开密钥、使用该密钥的非对称算法的一个标识符、密钥对所有者的名称、证明这一所有关系的认证机构的名称、证书的序列号和有效期、该证书符合的ITU-T X.509版本号以及一组可选的、包含该认证机构证书策略信息的扩展字段。整个证书然后用该认证机构的专用密钥进行数字签发。ITU-T X.509 证书可以广而告之，比如说在万维网站点上、在LDAP号码簿中或者附在电子邮件的电子名片（vCard[1]）上。认证机构的签字保证证书的内容不会在不知晓的情况下被改动。

为了验证证书的有效性，用户需要获得签发该证书的认证机构的有效公开密钥，以验证该证书上认证机构的签字。一个认证机构可以让另一个（上级）认证机构证明它的公开密钥，所以验证公开密钥可能涉及一个证书和认证机构链。最终这个链必须在某处结束，通常就是作为“可信根”的认证机构证书。“根”认证机构的公开密钥作为自我签发的证书予以发布（该“根”认证机构由此证明这是它自己的公开密钥）。签字让用户得以验证密钥和认证机构名称自该证书生成以来未被篡改。不过，无法对一个自我签发的证书中嵌入的认证机构名称信以为真，因为这个名称是认证机构自己加进去的。因此，公开密钥基础设施的一个关键组成部分是，应以让我们相信该公开密钥确实属于自我签发的证书中提到的“根”认证机构的方式，来安全地分发“根”认证机构的公开密钥。如果没有这种保证，我们将无法确信是否有人冒充“根”认证机构。

6.2.3 公开密钥基础设施

公开密钥基础设施（PKI）的主要目的是发布和管理公开密钥证书，包括“根”认证机构（CA）签发的证书。密钥管理包括密钥对的生成、公开密钥证书的生成、公开密钥证书的撤销（例如，当用户的专用密钥有了变动时）、密钥与证书的保存和记录及其到期后的销毁。每个认证机构依据一套策略来运转，ITU-T X.509 建议书提供了在该认证机构发放之 ITU-T X.509 证书的扩展字段中发布某些这种策略信息的机制。认证机构采用的策略规则和程序通常在该认证机构颁布的证书策略（CP）和认证惯例声明（CPS）文件中予以规定。这些文件有助于确保对认证机构发放之证书的

1 vCard是一种标准格式的电子业务卡，常常通过电子邮件来交换。

信任评估有一个共同的基础，不论是国际性的还是跨行业的。这些文件还提供了建立机构间信任所需的部分法律框架，并规范了有关如何使用所发布之证书的限制。

ITU-T X.509 建议书的早期版本（1988 年版、1993 年版和 1997 年版）规定了公开密钥基础设施的基本要素，包括公开密钥证书的定义。2001 年批准的 ITU-T X.509 建议书修订版（并在 2005 年和 2008 年进行了修订）包含对属性证书的重要增补以及一个有关特权管理基础设施（PMI）的框架。

6.2.4 特权管理基础设施

与公开密钥基础设施（PKI）相比，特权管理基础设施（PMI）管理的是支持综合授权服务的特权。这些规定的机制考虑了在多供货商和多应用的环境下设置用户访问特权。PMI 和 PKI 的概念相似，但 PMI 涉及授权，而 PKI 集中在认证。表 4 说明了这两种基础设施之间的相似之处。

表 4 – 特权管理和公开密钥基础设施特性比较

特权管理基础设施	公开密钥基础设施
源机构（SoA）	根认证机构（信任锚）
属性机构（AA）	认证机构
属性证书	公开密钥证书
属性证书撤销列表	证书撤销列表
PMI 机构撤销列表	PKI 机构撤销列表

为用户指配特权的目的是保证他们遵循源机构规定的安全策略。属性证书中策略相关信息与用户名称绑定在一起，并包括若干组成部分，如表 5 所示。

表 5 – X.509属性证书结构

版本
持有者
发布者
签字 (算法标识)
证书序号
有效期
属性
发布者独特标识
扩展字段

属性证书也用在远程生物特征识别中（见第6.5节），以创建生物特征识别证书，来将用户与其生物特征识别信息相绑定。生物特征识别设备证书定义生物特征识别设备的性能和限制。生物特征识别策略证书定义安全水平与生物特征识别算法参数之间的关系。

ITU-T X.509 建议书中描述了 PMI 控制的五个组成部分：特权主张者、特权验证者、对象方法、特权策略和环境变量（见图 12）。特权验证者能控制特权主张者按特权策略获得对象方法。

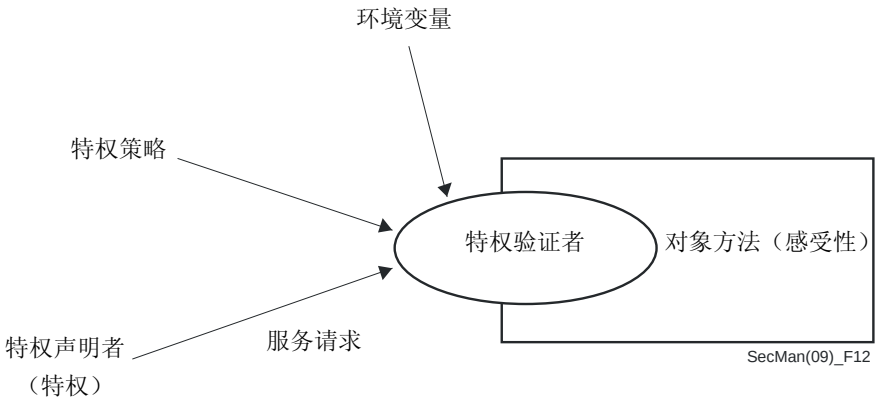


图 12 – X.509 PMI控制模型

在有必要为某种实现指派特权时，ITU-T X.509 建议书中考虑的 PMI 指派模型包括四个部分：特权验证者、源机构、其他属性机构和特权主张者（见图 13）。

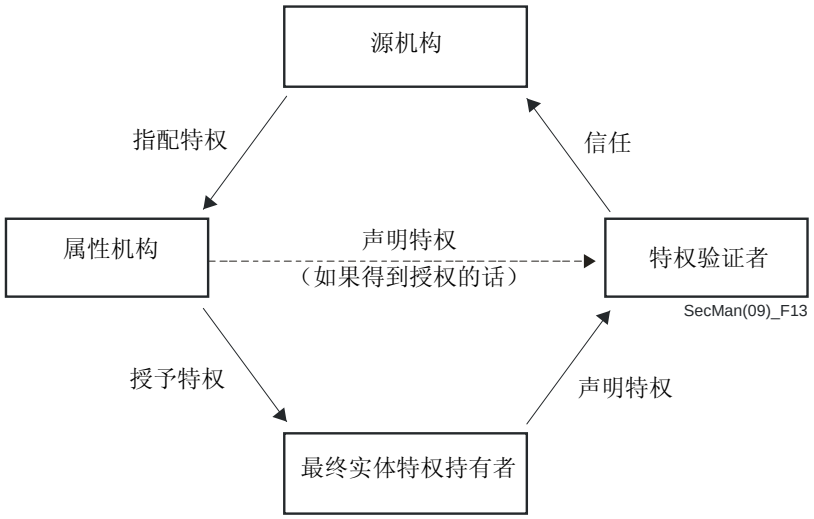


图 13 – X.509 PMI指派模型

近来有些授权方案是按照基于角色的访问控制（RBAC）模型来实现的，认为用户也是一个角色。授权策略将一组许可与某个角色联系起来。在访问某种资源时，按策略检查用户的角色，以便开展后续的行动。

6.3 认证指导原则

制定了许多指导原则来解决具体的认证问题，如下所述。

6.3.1 利用密钥交换实现的、安全的基于口令的认证协议

利用密钥交换实现的、安全的基于口令的认证协议（SPAK）是一种简单的认证协议，在该协议中，在客户端与服务器之间使用一个人可记忆的口令来实现相互认证，一个共享的秘密可用做下一次会话的会话密钥。

在ITU-T X.1151建议书《利用密钥交换实现的基于口令的安全认证协议的指导原则》中定义了有关SPAK的要求，以及有关从各种各样安全的口令认证协议中选择最合适SPAK的指导原则。该协议非常简单，易于实现和使用，不需要任何其他的基础设施（如PKI）。在不久的将来，它对许多应用将越来越重要。SPAK以一个简单的口令既提供了用户认证，又提供了强密钥交换，这样，通过认证过程中共享的一个秘密，即可实现对后续通信会话的保护（如图14所示）。

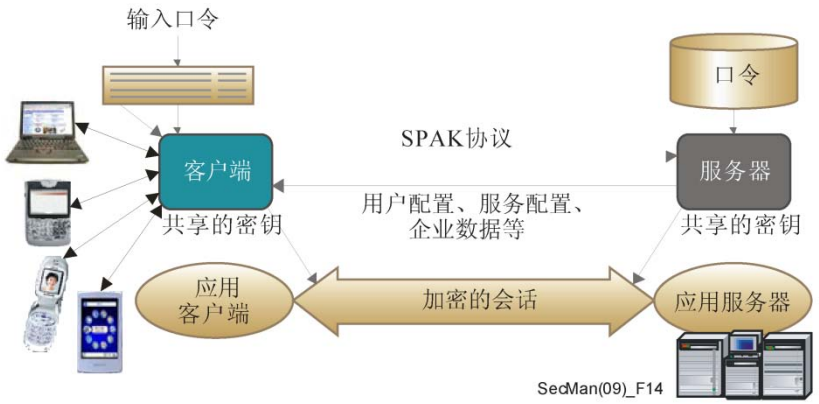


图 14 – 典型的SPAK协议工作过程

6.3.2 可扩展的认证协议

可扩展的认证协议（EAP）支持数据通信网络中请求者与认证服务器之间的多种认证机制。EAP可用做一个基本的工具，来完成用户认证和分发会话密钥。它可实施设备认证，以便建立一个安全的点对点连接，并防止来自未经授权设备的访问。

ITU-T X.1034建议书描述了一个针对基于EAP的认证的框架，以及用于保证通信网络低层安全的密钥管理。它提供了有关EAP方法选择的指导原则，并描述了有关数据通信网络低层密钥管理的机制。该框架既适用于带有共享媒体的无线接入网络，也适用于带有共享媒体的有线接入网络。

认证和密钥管理需要三个实体：一个请求者（或对等体）、一个认证者和一个认证服务器，如图15所示。请求者充当最终用户，从最终用户站点处接入网络。认证者充当策略执行点，在请求者与认证服务器之间传送EAP报文。认证服务器对请求者进行认证，可选地，共享一个秘密，可利用该秘密来获得加密密钥，将对最终用户的认证结果提交给认证者，并将共享的秘密传送给认证者。该共享的秘密可用来获得认证者与请求者之间的加密密钥，以确保机密性和完整性，并完成报文认证。

认证和密钥管理通常由四个工作阶段组成：安全能力发现、EAP认证、密钥分发和密钥管理（如图15所示）。在安全能力发现阶段，请求者与认证者商定安全能力以及将要使用的各种各样协议参数。在EAP认证阶段，认证服务器对请求者进行认证，并作为EAP协议的一个结果，获得与请求者共享的主秘密。在密钥分发阶段，认证服务器将主秘密传送给认证者，以便认证获得各种各样的加密密钥，用于请求者与认证者之间的后续会话。为防止反复使用相同的秘密密钥，应在每次会话中使用新的加密密钥。最后，在密钥管理阶段，认证者与请求者交换随机数，以便获得一个新的加密密钥，从而实现完美的前向保密。

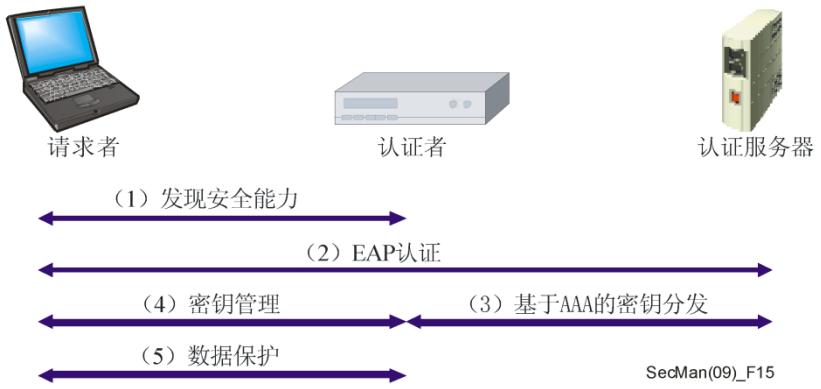


图 15 – 低层认证和密钥管理的四个工作阶段

6.4 身份管理

6.4.1 身份管理概述

身份管理（IdM）指的是安全地管理和控制身份信息（如证书、标识符、属性和声誉）的过程，使用身份信息来描述通信过程中的各种实体（如服务提供商、最终用户组织、人员、网络设备、软件应用和服务）。一个单个实体可以有多个数字身份，以便按照不同的要求来访问各种不同的服务，这些数字身份可以位于多个位置上。IdM支持对实体的认证。出于ITU-T的目的，一个实体声称的身份表述了该实体在某个特定情形中的唯一性。

IdM是网络安全的一个关键组成要素，原因是它提供了在各实体间建立和维护可信通信的能力，并使对网络和电子服务的移动、按需接入成为可能。它还使对一系列特权（而非所有特权或没有特权）的认证成为可能，使在实体的角色发生变化时更易于改变特权。通过使实体有关网络的活动得到适当监控和审计，IdM提高了组织运用其安全策略的能力，并提供了对组织内和组织外各种实体的接入能力。

IdM以支持安全、可信访问控制的方式提供了对身份信息的保证。通过单独签署/单独注销、用户控制个人识别信息以及用户能够选择身份提供方这种方式来实现该能力，相对为每个服务提供商提供证书而言，这种能力能代表用户来提供验证和指派功能。IdM还支持众多基于身份的服务，包括：定向广告；基于地理位置和兴趣的个性化服务；以及旨在减少欺诈和身份盗窃的、经过认证的服务。

IdM是一项复杂的技术，包括：

- 建立、修改、挂起、归档和终止身份信息；
- 认可部分身份，用于描述在某个特定情形或某种角色下的实体；
- 建立和评估各实体之间的信任；以及
- 定位一个实体的身份信息（例如，通过某个权威身份提供方，法律上，由之负责维护标识符、证书以及实体的某些或全部属性）。

ITU-T X.1250系列《有关网络安全中身份管理概述的增补》简要介绍了身份管理主题。

6.4.2 ITU-T身份管理工作

尽管仍在讨论某些基本概念和基本词汇，第17研究组（有关身份管理的牵头研究组）以及第2研究组（服务提供和电信管理的运营方面问题）和第13研究组（包括移动网络和下一代网络（NGN）的未来网络）在许多领域中的工作正在进行中。

第2研究组负责研究与确保身份管理标识符格式和结构一致性有关的问题，并负责规范与管理系统的接口，以支持组织域内或组织域间的身份信息通信。

第13研究组负责下一代网络（NGN）特定的身份管理功能体系结构，它支持增值的身份服务、安全的身份信息交换以及在各种不同的身份信息格式之间应用桥接/互操作性。第13研究组还负责确定在下一代网络中存在的任何身份管理威胁，并确定应对这些威胁的措施。ITU-T Y.2720建议书《下一代网络身份管理框架》已经获得批准。该标准描述了一种用于设计、定义和实施身份管理解决方案以及推动异构环境中互操作性的结构化方法。

第17研究组负责研究与开发一种通用身份管理模型有关的问题，它独立于网络技术，并支持各实体之间安全的身份信息交换。这项工作还包括：研究用于发现权威性身份信息源的过程；用于桥接/互操作各种不同身份信息格式的通用机制；身份管理威胁与应对措施；保护个人识别信息（PII）；以及仅在必要之时才授权开发用于确保对个人识别信息（PII）访问的各种机制。2009年9月，批准通过了两个建议书：ITU-T X.1250建议书《增强型全球身份管理和互操作性的基本能力》和ITU-T X.1251建议书《用户控制数字身份的框架》。另外，正在准备一个与身份管理有关的定义的基本集，以便确保ITU-T各身份管理标准中术语的统一和一致。

已经确立一个有关身份管理的联合协调行动（JCA-IdM），以协调ITU-T的身份管理工作。已经确立一个身份管理全球标准倡议（IdM-GSI），以协调世界范围内不同的身份管理方法，并与致力于该主题的其他团体开展合作。身份管理牵头研究组主页提供了大量有关身份管理活动的信息、已经批准和正在制定的身份管理建议书以及其他与身份管理工作有关的信息。

6.5 远程生物特征识别

远程生物特征识别主要关注电信环境中使用生物特征识别设备的个人识别和认证。它尤其关注如何通过使用安全可靠的远程生物特征识别方法来改进对用户的识别和认证。ITU-T通过与其他标准制定组织开展密切合作，来推动有关该主题的工作，涵盖的主题保护：人与环境的交互；生物特征识别数字密钥；X.509证书的生物特征识别扩展；开放网络中的生物特征识别认证。

6.5.1 远程生物特征识别认证

生物特征识别能够支持非常安全的认证设备，但有关开放网络中生物特征识别认证的标准化工作面临诸多挑战：

- 服务提供商没有任何有关最终用户环境中有哪些生物特征识别设备在用、此类设备安全等级/设置或者如何工作的信息；
- 在不同的生物特征识别产品之间，由门限参数确定的精度（错误接受率）是不同的，因此，服务提供商无法要求保持一个统一的精度水平；以及
- 生物特征识别验证的精度可能随最终用户的老化而下降，原因是生物特征识别要用到人体的特性。

在ITU-T X.1084建议书《电信系统的通用生物特征识别认证协议和系统模型概况》中说明了开放网络中电信系统的通用生物特征识别认证协议和概况。

图16显示了通过一个非面对面开放网络而进行的最终用户认证过程。

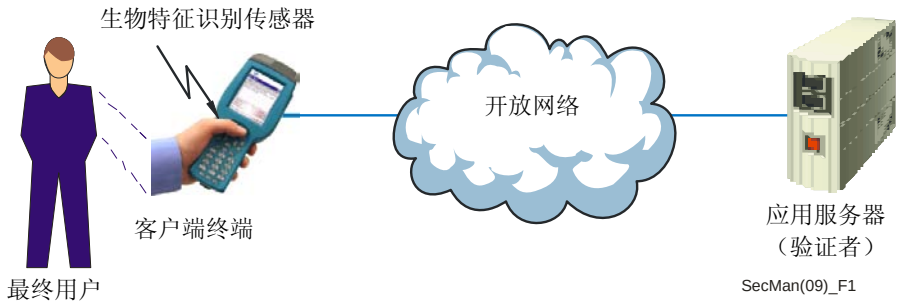


图 16 – 最终用户的远程生物特征识别认证

6.5.2 远程生物特征识别数字密钥的生成和保护

在ITU-T X.1088建议书《生物特征识别数字密钥生成和保护框架》中定义了生物特征识别数字密钥生成框架。该框架定义了使用生物特征识别模版和公开密钥证书与生物特征识别证书的保护措施，以便在开放网络上提供密码安全的认证和安全的通信。还定义了有关生物特征识别数字密钥生成和保护的安全性要求。该框架可用于生物特征识别加密和数字签名。推荐了两种方法：

- 生物特征识别密钥生成，在该方法中，密钥创建自一个生物特征识别模版（图17）；以及
- 生物特征识别密钥绑定/恢复，在该方法中，密钥保存在一个数据库中，可通过生物特征识别认证来提取（图18）。

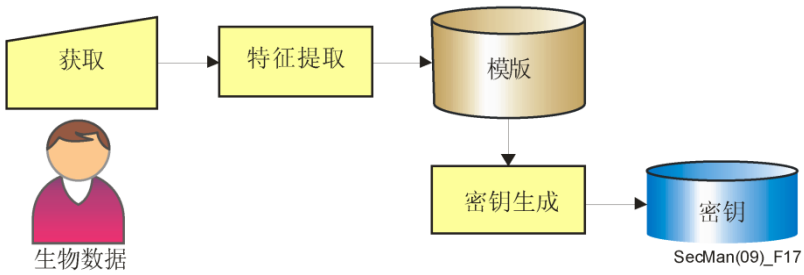


图 17 – 生物特征识别密钥的生成

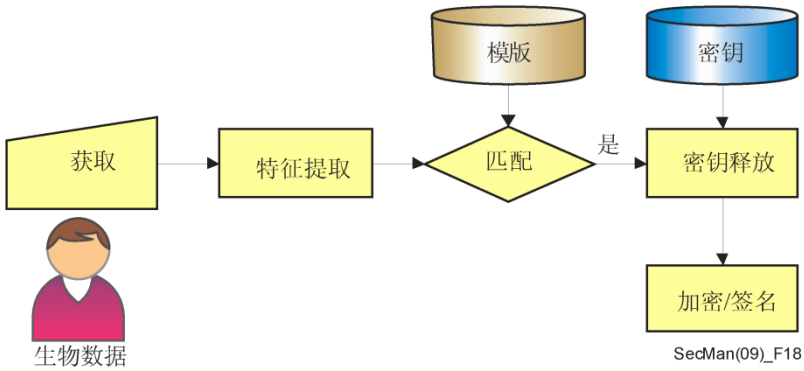


图 18 – 生物特征识别密钥的绑定/恢复

6.5.3 远程生物特征识别的安全性和安全问题

在远程生物特征识别多模模型中（ITU-T X.1081建议书《远程生物特征识别安全规范和安全问题框架》）定义了一个有关远程生物特征识别安全问题的框架，它定义了人与环境之间的交互，还定义了用于度量这些交互的数量和单位。远程生物特征识别多模模型不限于只考虑纯粹的物理交互，它还认可目前尚未被各标准单位所量化的动作交互。

6.5.4 与人体生理有关的远程生物特征识别

在ITU-T X.1082建议书《与人体生理有关的远程生物特征识别》中，还论述了远程生物特征识别的安全问题，它定义了有关生理、生物或行为特征的数量和单位，这些特征可以作为远程生物特征识别或验证系统（识别系统）的输入或输出，包括任何已知的检测或安全门限。它给出了与人体生理有关的远程生物特征识别数量和单位的名称、定义和符号（即传感器可探测的人体特征和辐射信号）。它还包括有关因使用远程生物特征识别设备而引起的人体效应的数量和单位。

6.5.5 远程生物特征识别标准方面的其他进展

为在公开密钥基础设施（PKI）或特权管理基础设施（PMI）中使用的ITU-T X.509证书定义了各种扩展，以生成生物特征识别证书。在ITU-T X.1089建议书《远程生物特征识别认证基础设施》中对这些做了详细说明。

ITU-T X.1083建议书《BioAPI互通协议》规定了报文的语法（使用ASN.1）、语义和编码，使符合BioAPI要求的应用能够跨节点或跨过程边界，来向符合BioAPI要求的生物特征识别服务提供商（BSP）请求生物特征识别操作，并告知在这些远程BSP中发生的事件。

7. 保证网络基础设施安全

7 保证网络基础设施安全

用于监视和控制电信网络管理流量的数据通常是在一个只承载网络管理流量（即没有用户流量）的独立网络上传输。这个网络通常被称为如ITU-T M.3010建议书《电信管理网的原则》所述的电信管理网（TMN）。强制要求保证该业务流量的安全。管理流量通常按照完成故障、配置、性能、会计和安全管理功能所需的信息进行分类。网络安全管理既涉及安全管理网络的建立，也涉及与X.805安全体系结构三个安全平面有关的信息安全的管理。

必须始终以一种安全的方式来开展有关网络基础设施元素的管理活动。例如，必须只能由经过授权的用户来开展网络活动。为了提供一个安全的端对端解决方案，对于网络基础设施、网络服务和网络应用的每一类型网络活动都要采取安全措施（如访问控制、认证）。已经制定了许多ITU-T建议书，具体讨论管理平面的安全问题，涉及作为网络基础设施一部分的网络元素和管理系统。

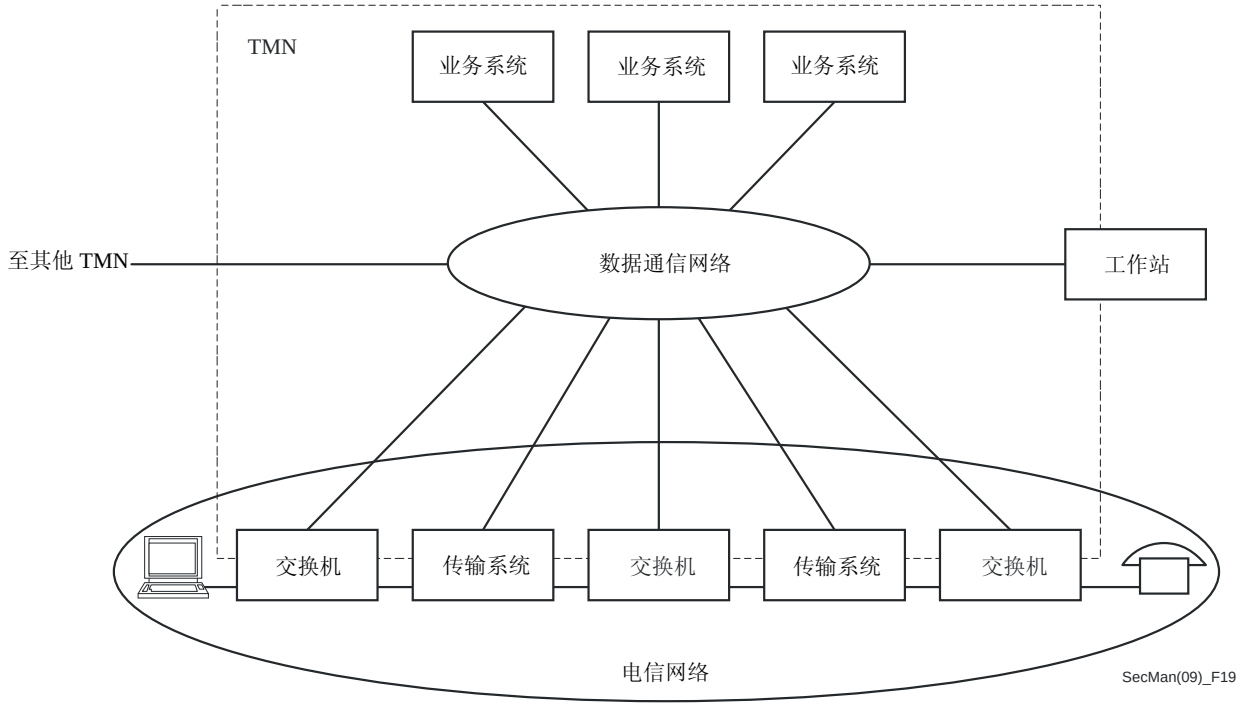
其他的网络管理应用包括那些与环境有关的应用，在这些环境中，不同的服务提供商需要相互合作，以提供端对端服务。例子包括向监管机构或政府部门提供通信设施，用于支持救灾，以及支持像跨越地理边界向客户提供租用线路这样的情况。

7.1 电信管理网

TMN是单独的，与公共网络基础设施隔开，因此任何由公共网络最终用户平面的安全威胁引起的破坏都不会扩散到TMN。由于这种分离，保护管理网络业务流量的安全就比较容易，原因是访问该平面只限于得到授权的网络管理员，流量也仅限于有效的管理活动。随着下一代网络的引入，用于最终用户应用的业务流量有时可能会和管理业务流量混和在一起。虽然这个方法只需要一个单一的综合网络基础设施，最大限度地降低了成本，但它也带来了许多新的安全难题。最终用户平面的威胁现在成为了管理和控制平面的威胁，原因是管理平面现在已经变得多数最终用户都能访问，且多种类型的恶意活动也变得可能。

7.2 网络管理体系结构

ITU-T M.3010建议书规定了用于确定电信网络的网络管理的体系结构，一个TMN与一个电信网络的关系如图19所示。管理网络体系结构规定了各种接口，用于确定完成操作、管理、维护和提供服务（OAM&P）功能所需的交换。



注 – 虚线代表的 TMN 边界可以延展并管理客户/用户服务和设备。

图 19 – TMN和电信网络之间的关系

ITU-T M.3016.0建议书概述了TMN面临的安全威胁，并给出了确定这些安全威胁的框架。在ITU-T M.3016系列建议书中，ITU-T M.3016.1建议书规定了详细的要求，ITU-T M.3016.2建议书概括了安全服务，ITU-T M.3016.3建议书则规定了在ITU-T M.3010建议书所定义的TMN功能体系结构内能够应对威胁的机制。由于各组织没必要对所有要求都提供支持，因此ITU-T M.3016.4建议书给出了一种根据安全要求、安全服务和安全机制拟定安全简表的书写格式，可以用这种书写格式来遵守某个组织独特的安全策略。

当讨论网络安全管理问题时，涉及两个方面。一方面涉及用户端对端活动（如VoIP服务）的管理平面。掌管用户的管理活动必须用安全的方式来实现。这指的是为支持端对端应用而在网络上交换的*管理信息的安全*；第二方面涉及*安全信息的管理*，不论何种应用，都应该得到管理。例如，两个服务提供商之间的故障报告活动，必须安全地得到管理。这可能要求对所交换的信息进行加密，在这种情况下，必须对加密密钥的管理做出规定。

涉及X.805体系结构的安全管理功能，制定了若干建议书，它们可用于管理平面的三个层（如图1所示）。另外，如下面几小节所述，还有其他建议书规定了一般的或普通的服务，例如当存在破坏安全的行为时的告警报告、审计功能以及为不同目标规定保护等级的信息模型。

7.3 保证网络基础设施要素安全

端对端的连接可以按接入网和核心网来考虑。这些网络可能使用不同的技术。已经制定了建议书，对接入网和核心网都做了论述。这里讨论的一个例子是宽带无源光网络（BPON）。这种接入网的用户特权的管理是用ITU-T Q.834.3建议书中的统一建模方法学来规定的，而采用公共对象请求代理体系结构（CORBA）的管理交换则在ITU-T Q.834.4建议书中做了具体规定。在这些建议书中描述的接口适用于单元管理系统与网络管理系统之间。单元管理系统用于管理单独的网络单元，并由此了解由一个或多个供应商提供的单元的软硬件体系结构的内部细节；而网络管理系统是在端对端网络层面上开展活动，并涉及多供应商管理系统。图20显示了单元管理系统的用户用于创建、删除、分配和使用访问控制信息的各种各样对象。用户许可清单包含每个得到授权的用户的许可管理活动清单。访问控制管理器验证管理活动用户的用户标识符和口令，并授权使用许可清单中允许的功能性。

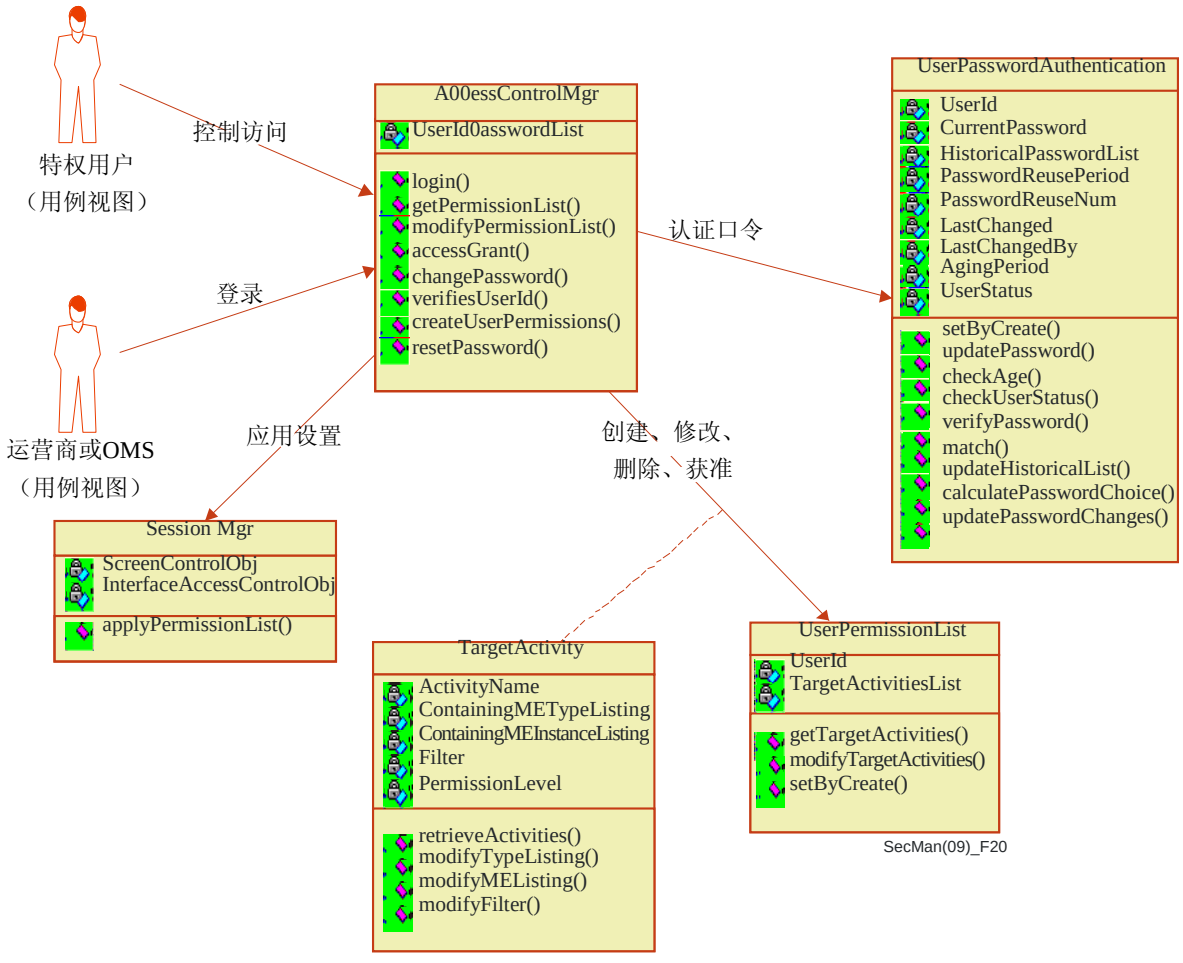


图 20 – ITU-T Q.834.3中的用户特权管理

7.4 保证监控和控制活动安全

在管理平面和服务层的交叉处，安全问题的这两个方面是相关的。一方面是确保网络提供的服务有适当的安全措施。例如，确保只有合法的用户才允许执行与提供服务相关的操作。第二方面是规定哪些行政管理交换是合法的，以便帮助检测破坏安全的行为。

ITU-T M.3208.2建议书《旨在形成租用电路服务的可按需提供的服务链路连接的连接管理》探讨第一方面的问题，即服务管理活动。这种连接管理服务允许订户在预配置资源范围内建立/激活、修改和删除租用电路。由于是用户提供端对端连接，因此有必要确保只有得到授权的用户允许执行这些操作。与该服务相关的X.805安全尺度是：对等实体认证、数据完整性控制（防止在传输中未经授权地修改数据）和访问控制（确保一个订户不能恶意地或无意地获取另一个订户的数据）。

ITU-T M.3210.1建议书《用于IMT-2000安全管理的TMN管理服务》规定了与无线服务管理平面相关的管理活动，是用于解决第二方面问题标准的一个例子。在一个无线网络中，当用户从归属网漫游到被访网时，他们可能跨越不同的管理域。在ITU-T M.3210.1建议书中规定的服务描述了归属地的欺诈管理域如何收集有关一个被访网注册订户的适当信息。图21中的情形a)和情形b)显示了或者由归属网或者由被访网发起的监视管理活动。在某个订户向被访网注册至从该网络注销离开该网络期间，归属网中的欺诈检测系统会要求关于订户此期间活动的信息。然后根据具体服务级别的或某个订户的呼叫记录分析，形成与使用情况有关的简表。欺诈检测系统可做分析，当检测到欺诈行为时生成适当的告警。

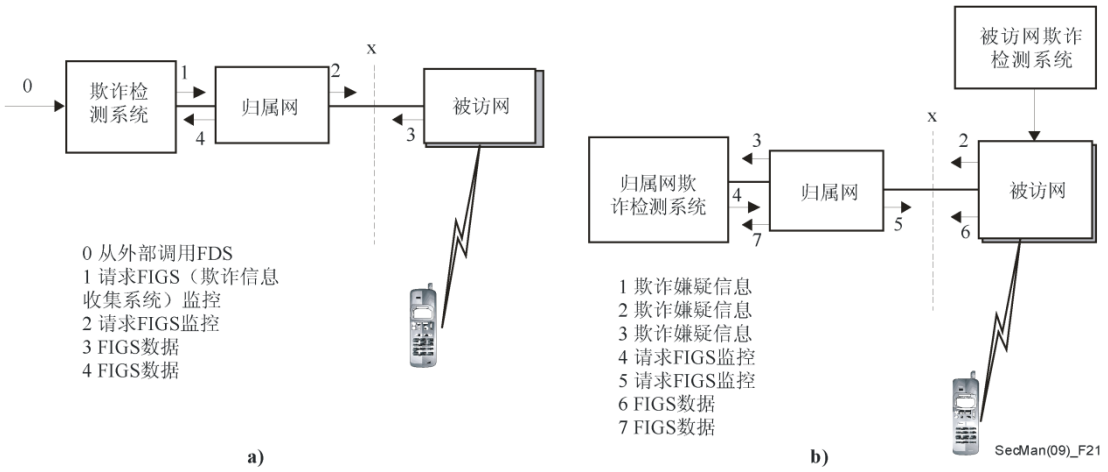


图 21 – 针对无线服务的欺诈管理

7.5 保证基于网络的应用安全

ITU-T X.805 建议书中管理平面和应用层的交叉对应保护最终用户基于网络的应用的安全。这包括如报文发送和号码簿等应用。需要保证管理活动安全的另一类应用是管理应用本身。这最好还是用例子来解释。这些应用的最终用户是服务提供商的管理（操作）人员。考虑一下服务提供商为了提供端对端连接服务而使用其他服务提供商的连接服务的情况。根据规章制度或市场环境，一些服务提供商可能提供接入服务，而其他运营商，称为*局间运营商*，可能提供长途连接。局间运营商租用本地服务提供商的接入服务来提供跨地区的端对端连接。在出现服务损失时，采用叫做*故障报告管理*的应用来报告出现的问题。这些系统的用户以及这个应用本身为了报告出现的问题而要求授权。得到授权的系统和用户应采取必要措施来检索所报问题的状况。图 22 说明了必须用安全的方式执行的相互作用。要对访问特权加以管理，以防止未经授权地获取故障报告。一个服务提供商只允许报告自己租用之服务出现的故障，不得报告其他提供商租用之服务出现的故障。

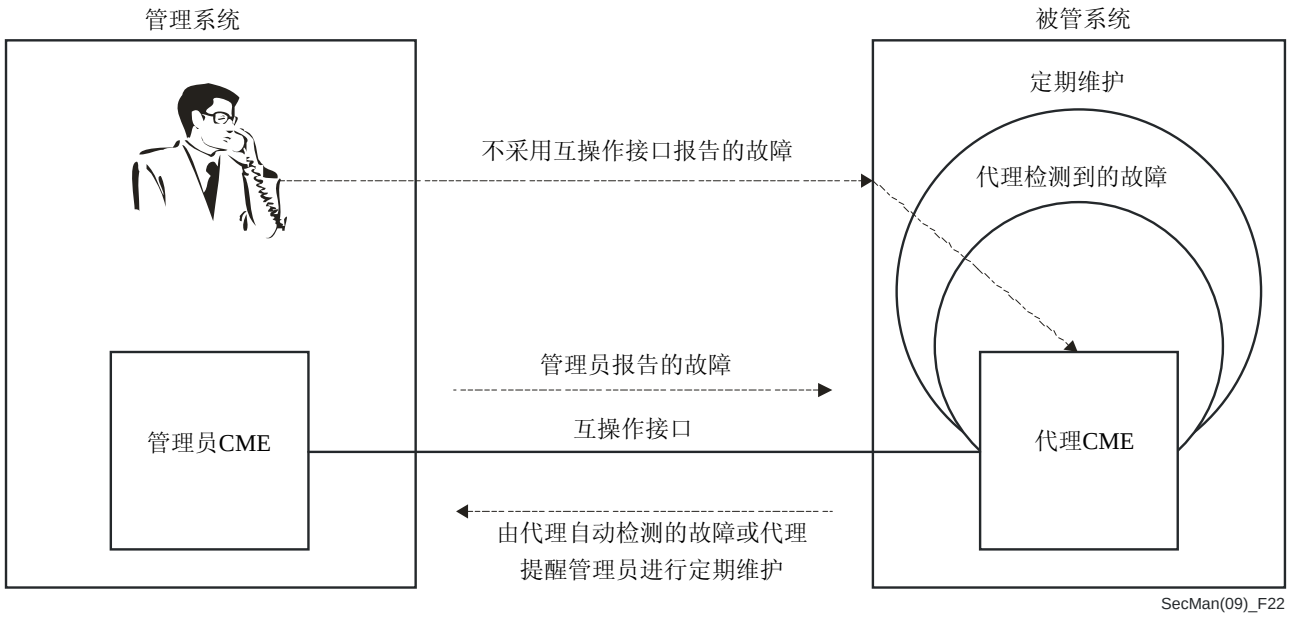


图 22 – 故障管理报告生成

ITU-T X.790 建议书《ITU-T 应用的故障管理功能》对这种管理应用做了规定，并采用如访问控制列表和双向认证这样的机制来保护这些活动的安全。

7.6 通用安全管理服务

有许多通用服务被认为是 X.805 管理平面活动。在使用*通用管理信息协议*（CMIP）（ITU-T X.711 建议书）的地方，这些尤其适用。下面简要介绍这些建议书中包含的服务。

7.6.1 安全告警报告功能

告警报告在管理接口中是一个关键功能。当检测到一个故障时，不管是由于操作原因（如电路组件出现故障），还是由于违反了安全策略，都向管理系统发出告警报告。告警报告含有许多参数，以便管理系统能够确定故障原因并采取纠正措施。任何事件的参数都含有一个强制性字段，称为*事件类型*，还含有一组其他字段，叫做*事件信息*。后一组信息包括告警的严重程度、告警的可能原因、破坏安全行为的检测装置等信息。告警原因与事件类型有关，如表 6 所示。

表 6 – 安全告警原因

事件类型	安全警报原因
完整性破坏	复制信息 信息遗失 检测到信息改动 信息失序 意外信息
业务破坏	拒绝服务 服务中断 程序错误 未加规定的原因
实物破坏	线缆改动 检测到侵入 未加规定的原因
安全服务或机制破坏	认证失效 泄露机密 不可抵赖失效 未经授权的访问尝试 未加规定的原因
时域破坏	迟到的信息 密钥过期 营业时间之外的活动

对这些安全告警原因，在ITU-T X.736建议书《安全告警报告功能》中有更详细的说明。

7.6.2 安全审计跟踪功能

安全审计跟踪用于记录与安全有关的事件，尤其是违反安全的事件。与安全有关的事件可以包括连接、断开、安全机制利用、管理操作和使用量结算。在 ITU-T X.740 建议书中定义了安全审计跟踪功能。

7.6.3 被管实体的访问控制

ITU-T X.741 建议书《访问控制的对象和属性》非常详细地规定了与为各种各样被管实体分配访问控制权有关的模型。该建议书满足的要求包括：防止未经授权地生成、删除和更改管理信息；确保各项操作符合操作发起者的访问权限；防止向未经授权的接收者发送管理信息。规定了各种级别的访问控制权以满足这些要求。对于管理操作来说，可以在多个层次上应用访问限制。一项访问控制策略可以基于所定义方案中的一种或多种（如访问控制清单；以能力为基础、以标签为基础和以内容为基础的访问控制）。在 ITU-T X.741 模型中，根据访问控制策略和访问控制信息（ACI）确定允许还是不允许访问。举例来说，ACI 包括规则、发起者身份、请求访问的目标的身份、关于发起者的认证信息等。

7.6.4 基于CORBA的安全服务

在许多 ITU-T X.700 系列建议书设想采用 CMIP 作为管理接口协议的同时，目前在这些建议书中也出现一些其他趋势，包括采用基于公共对象请求代理（CORBA）的协议、服务和目标模型，用于管理接口。尤其值得注意的是 ITU-T X.780 建议书《定义 CORBA 被管对象的 TMN 指导原则》、ITU-T X.780.1 建议书《定义粗粒度的 CORBA 被管对象接口的 TMN 指导原则》、ITU-T X.780.2 建议书《定义面向服务的 CORBA 被管对象和外观对象的 TMN 指导原则》、ITU-T X.781 建议书《实施与基于 CORBA 的系统有关的一致性声明形式的要求和指导原则》。此外，ITU-T Q.816 建议书规定了在管理接口范畴中采用这些服务的框架。为了支持这些接口的安全要求，ITU-T Q.816 建议书引用了用于安全的公共服务的对象管理组（OMG）规范。

8. 一些特定的网络安全方法

8 一些特定的网络安全方法

本节评论用于保护各种不同类型网络的方法。首先看一下有关下一代网络的安全要求；而后看一下移动通信网络，它们正从基于单一技术的移动性（如CDMA或GSM）向使用网际协议跨异构平台的移动性转变；接着分析有关家庭网络和有线电视的安全规定；最后，陈述了无处不在的传感器网络面临的安全挑战。

8.1 下一代网络（NGN）的安全

下一代网络（NGN）是一种基于分组的网络，它能够向用户提供电信服务，并能够利用多种宽带、支持服务质量（QoS）功能的传送技术。此外，服务相关的功能独立于传送相关的基础技术。下一代网络使自由用户能够接入各种网络，并竞争服务提供商和服务。它支持通常的移动性，允许向用户提供一致、普遍的服务。在ITU-T Y.2001建议书《下一代网络（NGN）综述》中提供了有关下一代网络一般特性的更详细信息。

8.1.1 下一代网络（NGN）的安全目标和要求

认识到安全性是下一代网络的一个关键特性，提出并实施一系列标准显得至关重要，这将在可能的最大程度上确保下一代网络的安全。随着下一代网络的发展以及新的安全弱点的出现（对这些弱点没有任何已知的、即时的、自动的修复措施），必须对此类弱点做好记录，以便网络管理员和最终用户能够减少这些弱点。

下一代网络安全研究工作必须开发出好的网络体系结构，解决好以下问题：

- 为网络和最终用户资源提供最大的保护；
- 允许高度分布的端对端智能；
- 允许多种联网技术共存；
- 提供端对端安全机制；
- 提供适用于多个管理域的安全解决方案；
- 提供安全的身份管理，它涉及但不限于：
  - 下一代网络实体（如用户、用户设备、网络提供商、服务提供商、身份提供方等）的可靠认证；
  - 防止未经授权地访问下一代网络中的身份数据；
  - 在下一代网络的各结盟实体间安全交换身份信息；
  - 支持保留有关下一代网络中身份信息使用情况的记录；
  - 支持下一代网络中的用户保密和匿名；以及
  - 支持下一代网络用户的能力，帮助它们安全地管理好其身份信息（如修改用户简表、修改口令、支持基于位置的服务、查看记账记录等）；

- 为IPTV提供高效费比的安全解决方案，对性能、服务质量、适用性和扩展性有适当的影响。IPTV安全性应提供的保护类型包括但不限于：
  - 内容保护；
  - 服务保护；
  - 网络保护；
  - 终端保护；以及
  - 订户保护。

基于ITU-T X.805原则的ITU-T Y.2701建议书《下一代网络（NGN）安全要求（第1版）》规定了抵御安全威胁、保护下一代网络的安全要求，涉及身份管理技术方面的一些问题。

在多网络环境中，必须保护好以下元素：

- 网络和服务提供商的基础设施及其资产（如下一代网络资产和资源，如网络元素、系统、组成部件、接口以及数据和信息）、它的资源、它的通信（即信令、管理和数据/载体业务量）和它的服务；
- 下一代网络服务和能力（如话音、视频和数据服务）；以及
- 最终用户通信和信息（如专用信息）。

各要求必须为最终用户在多网络管理域上的通信提供基于网络的安全，如图23所示。

ITU-T Y.2701建议书中规定的各要求被看做是要求的一个最小集。除了规定的那些措施之外，下一代网络提供商可能还需要采取额外的措施。

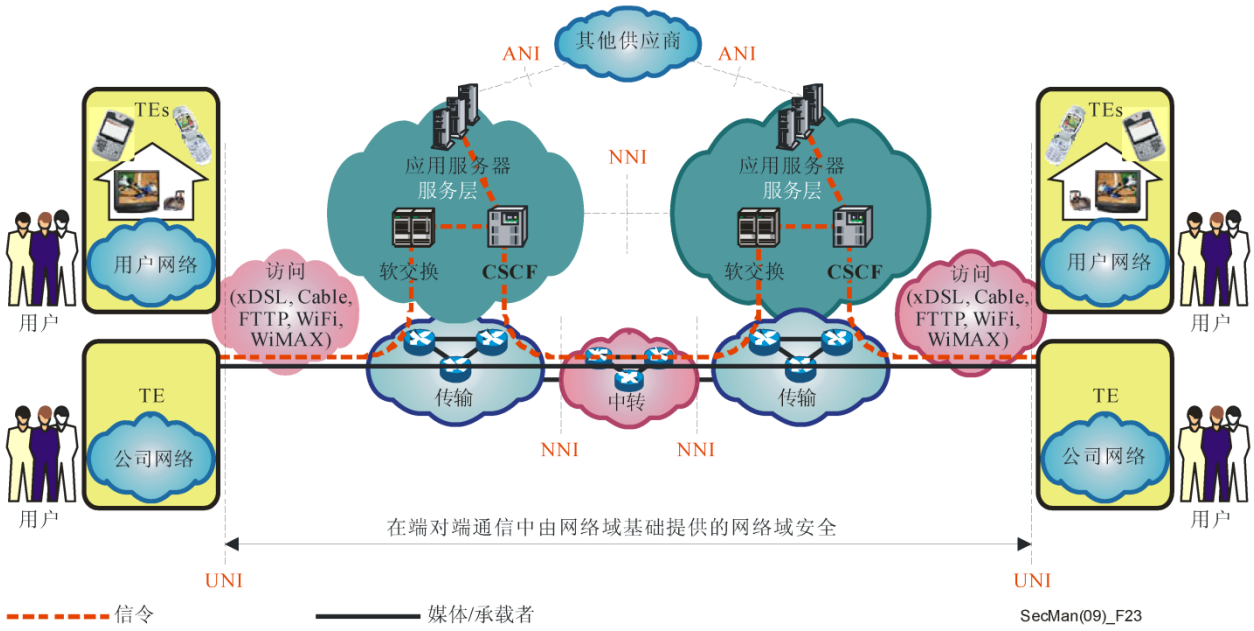


图 23 – 跨多个网络的通信安全

8.2 移动通信安全

随着网际协议（IP）的使用，移动通信正从限于某种特定技术（如GSM或CDMA）的移动性发展成为跨异构网络（如GSM、Wi-Fi、PSTN）的移动性。换言之，未来的网络将涉及无线网络和有线网络的集成，从而能够提供众多新的服务，而单个的现有网络则无法提供这些服务。

随着真正的固定-移动融合（FMC）得以实现与应用，一个移动用户可以跨异构网络（如GSM、无线局域网和蓝牙）进行漫游。需要以不同的方式来满足每种类型访问的安全要求，但必须满足所有的安全要求，以保护用户以及正在访问的网络和应用。

安全问题主要可分为：

- 因在移动无线网络中使用网际协议（IP）而引起的问题；以及
- 因使用多个多技术网络而引起的问题。

互联网攻击和弱点将威胁使用网际协议作为其传送协议的无线移动网络。此外，新的威胁将源自无线网络自身独有的特性，即移动性。已为IP网络开发的安全机制可能无法满足基于IP的无线系统的全部安全需要，因此必须开发新的或增强型的IP安全措施。此外，不仅要为无线接口解决安全问题，还要为完全的端对端服务解决安全问题，并且解决方案必须足够灵活，以便提供各种不同等级的安全性，以适应正在提供的服务/应用。随着移动IP服务和应用得以实现，安全措施对用户、运营商和服务提供商来说变得越来越重要。

多个网络的介入增加了威胁的机会，如非法截获用户简表、内容（如话音或数据通信）以及认证信息。

“国际移动电信2000”（IMT-2000）是有关第三代（3G）无线通信的全球标准。它通过一组相互依赖的国际电联建议书来定义。IMT-2000提供了一个用于全球范围无线接入的框架，它把各种不同的陆地系统和/或卫星网络连接在一起。它将开发利用固定和移动无线接入系统中各种数字移动电信技术和系统之间潜在的协同能力。

国际电联有关IMT-2000的活动由国际标准化（包括频谱以及无线电与网络组成部件的技术规范）、资费和记账、技术援助以及监管和策略方面的研究工作等组成。

ITU-T Q.1701建议书《IMT-2000网络框架》、ITU-T Q.1702建议书《超IMT-2000系统网络方面的远期展望》、ITU-T Q.1703建议书《超IMT-2000系统网络方面的服务和网络能力框架》涵盖了有关IMT-2000网络安全的广泛要求。

此外，ITU-T Q.1741（3GPP）系列建议书包含了3G规范，ITU-T Q.1742（3GPP2）系列建议书包含了一个对已发现威胁所做的评估报告以及一个用于解决这些威胁的安全要求列表。这些建议书还包含有关移动通信的安全目标和原则、一个确定的安全体系结构、加密算法要求、法律许可的截获的要求以及法律许可的截获的体系结构和功能。

8.2.1 安全的移动端对端数据通信

具备数据通信能力的移动终端（如IMT-2000移动电话、便携式计算机或带有无线卡的PDA）广泛可用，各种各样的应用服务（如电子商务）使用连至移动网络的移动终端。对商务应用和保护最终用户来说，有效的安全性是必要的。

由于无线网络的特性以及无线通信技术的内在弱点，移动网络显得尤其脆弱。必须从移动运营商、应用服务提供商和最终用户的角度对安全问题进行考虑。保证移动终端与应用服务器之间的安全显得尤其重要。为了解决移动端对端数据通信的安全问题，ITU-T提出了一整套安全解决方案，下面对其中的一些方案进行论述。

8.2.1.1 安全的移动端对端数据通信框架

ITU-T X.1121建议书《移动端对端数据通信的安全技术框架》描述了移动用户与应用服务提供商（ASP）之间移动端对端数据通信的两个模型：“通用模型”和“网关模型”，如图24和图25所示。应用服务提供商通过应用服务器向移动用户提供服务。在网关模型中，安全网关将数据包从移动终端转向应用服务器，把以网络为基础的移动通信协议转换成以开放网为基础的协议，反之亦然。图26描绘了移动端对端数据通信网络中的威胁。图27显示了哪些地方对各实体有安全特性要求以及实体与实体之间的关系。

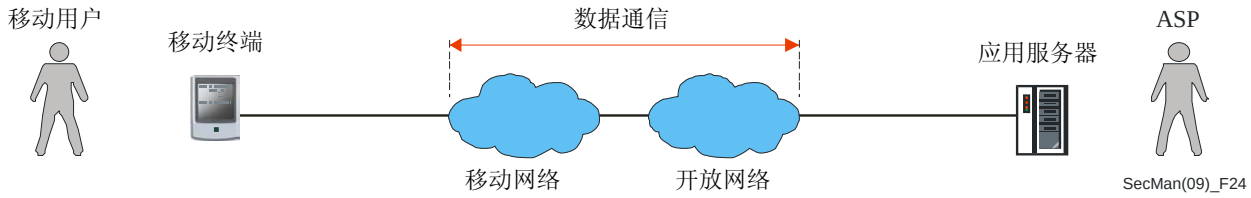


图 24 – 用户与ASP之间端对端数据通信的通用模型

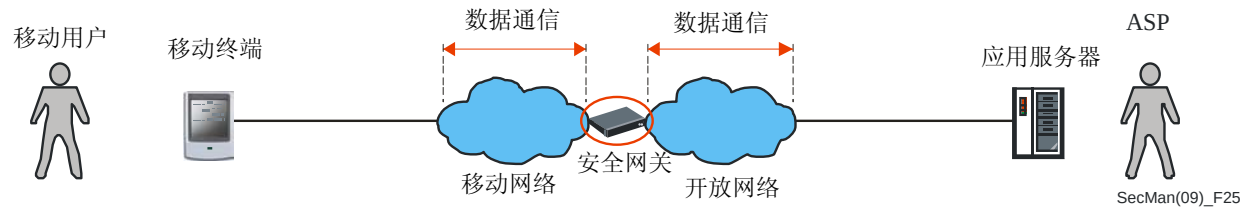


图 25 – 移动用户与ASP之间移动端对端数据通信的网关模型

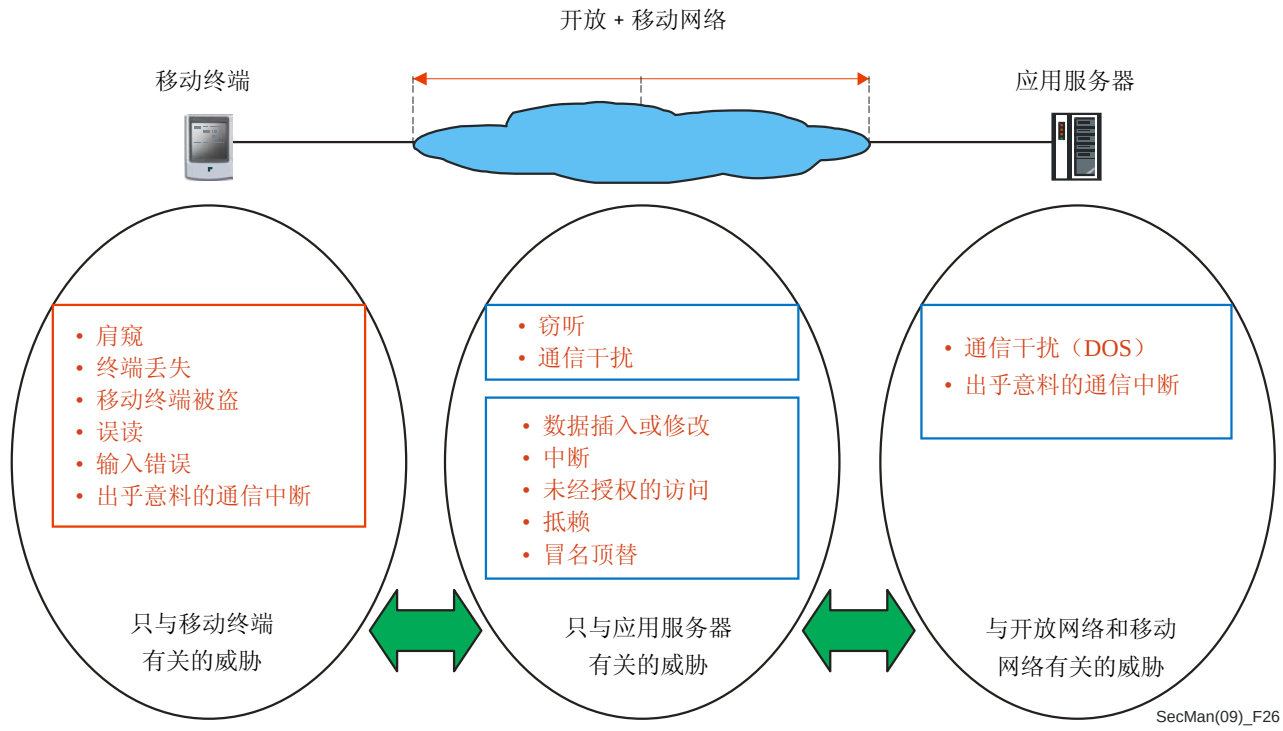


图 26 – 移动端对端通信中的威胁

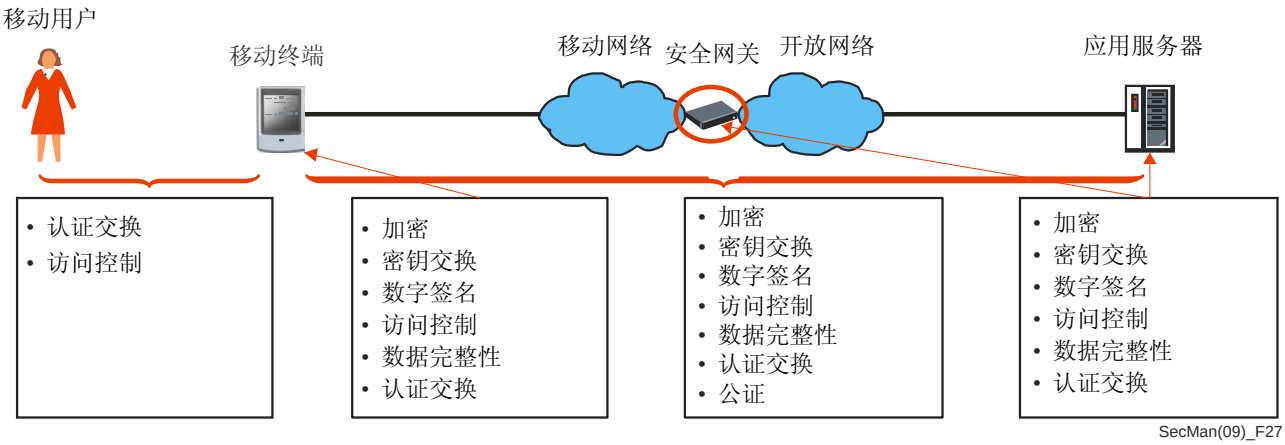


图 27 – 各实体要求的安全功能以及实体与实体之间的关系

8.2.1.2 移动端对端数据通信的PKI

PKI对提供移动端对端数据通信所需的某些安全功能（如机密性、数字签名、数据完整性）来说非常有用，但由于移动数据通信的特性，因此需要对PKI做某些改进。在ITU-T X.1122建议书《基于PKI实施安全移动系统的指导原则》中，规定了有关在移动环境中实施PKI的指导原则，它既规定了一个通用PKI模型，又规定了一个网关PKI模型。

在通用PKI模型中（如图28所示），移动用户的认证机构（CA）发放用户证书，并管理信息库和证书撤销列表（CRL）。移动用户的验证机构（VA）向移动用户提供在线证书验证服务。ASP的认证机构发放ASP证书，并管理ASP的信息库和证书撤销列表（CRL）。ASP的验证机构提供对ASP证书的在线证书验证服务。

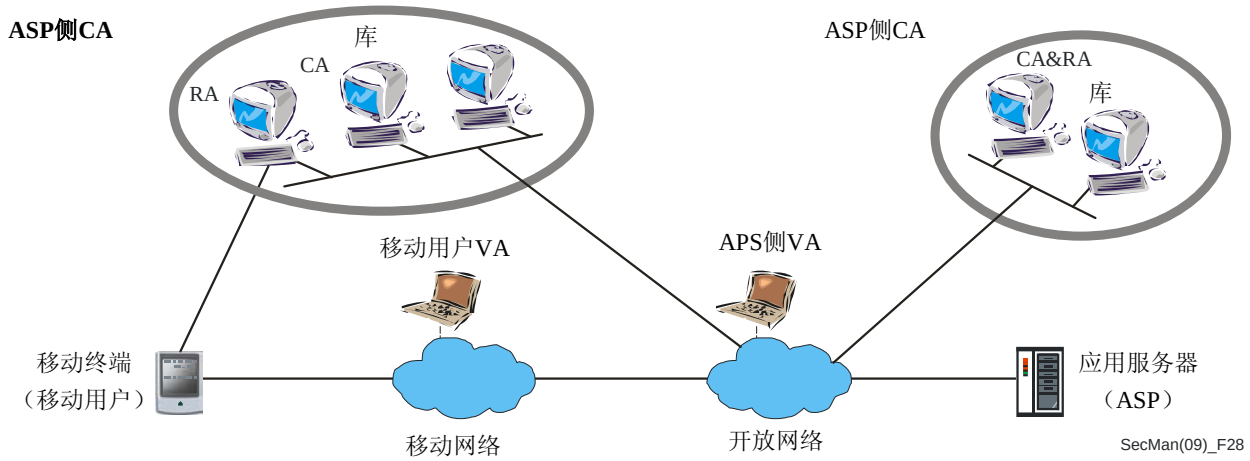


图 28 – 移动端对端数据通信的通用PKI模型

根据公开密钥/专用密钥产生位置的不同，存在两种证书发放方法：一种方法是在移动终端的生产厂家产生和编制加密密钥对；另一种方法是在移动终端上或者在移动终端附带的、无法改动的令牌上产生加密密钥对。图 29 描绘了移动终端获取证书的程序，其中加密密钥对在移动终端上产生。

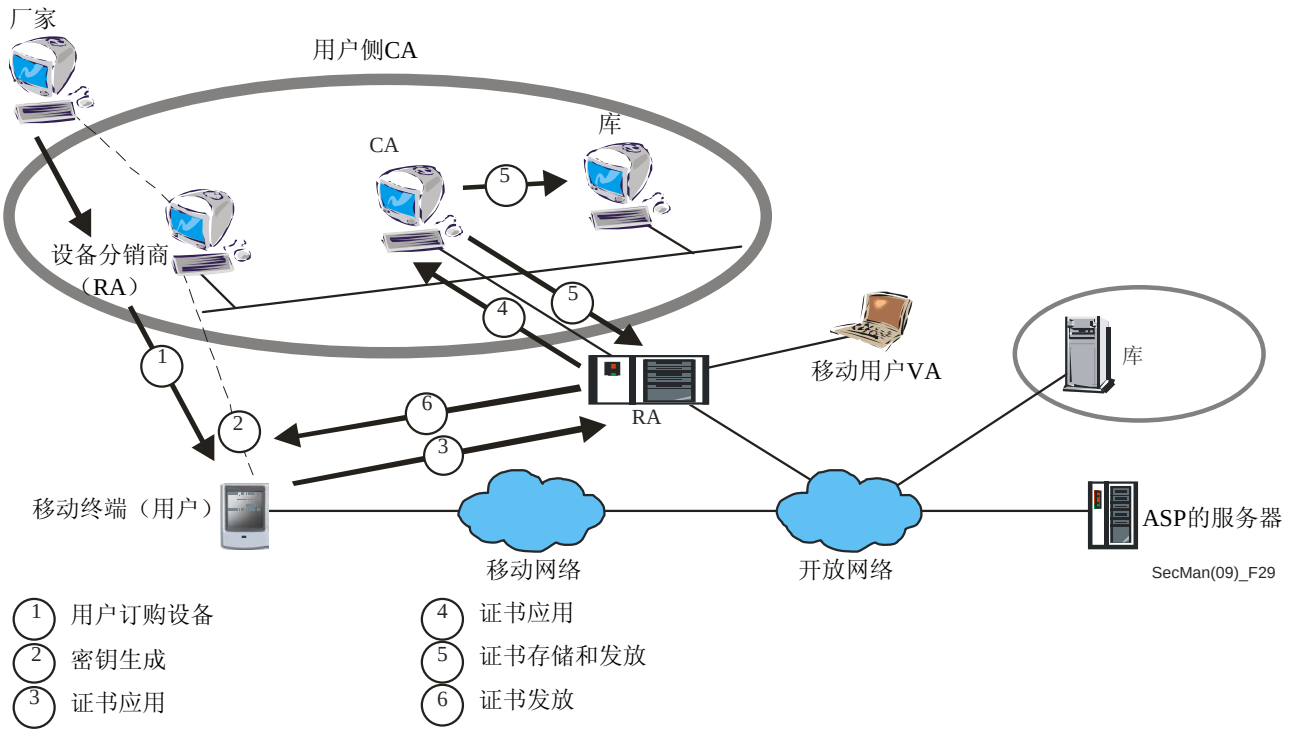


图 29 – 移动终端的证书发放程序

移动终端的计算能力和存储容量都有限。因此，在线证书验证方案优于根据CRL进行的离线证书验证方案。图30描绘了移动终端的在线证书验证程序。

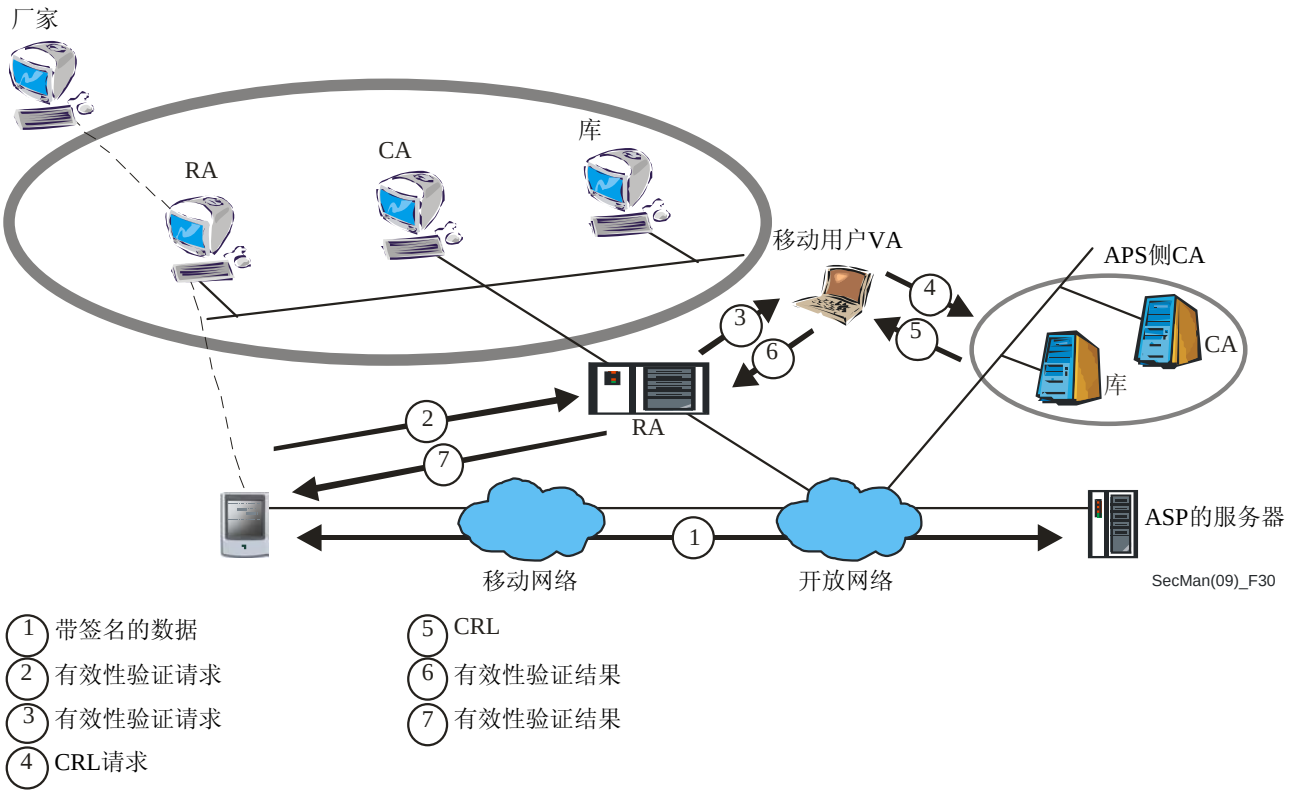


图 30 – 移动端对端数据通信的证书验证程序

移动端对端通信的PKI可用于会话层或者应用层。当用于会话层时，它可支持诸如客户端认证、服务器认证和机密性与完整性服务等安全服务；当用于应用层时，它可提供不可抵赖和机密性服务。

8.2.1.3 移动数据通信的关联反应系统

已设计完成关联反应系统，以便移动终端或设备和网络能够联合起来应对安全威胁。ITU-T X.1125建议书描述了关联反应系统的通用体系结构，在该体系结构中，移动网络及其用户终端能够相互合作，以应对各种各样的安全威胁，从而实现安全的端对端数据通信。此类威胁包括如病毒、蠕虫、特洛伊木马等，或者其他针对移动网络及其用户的网络威胁。

该体系结构通过移动站点安全更新、网络访问控制和应用服务限制，为运营商网络提供了增强的安全能力。这形成了一种机制，用于防止病毒或蠕虫通过运营商网络快速传播。

8.3 家庭网络的安全

由于家庭网络使用各种各样有线的或无线的传输技术，因此它遇到的威胁类似于任何其他有线或无线网络遇到的那些威胁。为了保护家庭网络免受这些威胁，ITU-T为家庭网络服务制定了一整套解决方案，下面将对其中的一些解决方案进行讨论。

8.3.1 家庭网络的安全框架

ITU-T X.1111建议书《家庭网络的安全技术框架》建立在ITU-T X.1121建议书的威胁模型基础之上，旨在为家庭网络建立一种安全框架。家庭网络的特性可概述如下：

- 在网络中可使用各种各样的传输媒体；
- 网络可能包含有线的和/或无线的技术；
- 从安全角度来看，有许多可能的环境有待分析；
- 远程用户可能带着远程终端到处走动；以及
- 各种不同类型的家庭网络设备要求不同的安全等级。

如图31所示的通用家庭网络安全模型可以包含众多设备，如PDA、PC和TC/VCR。在该模型中，家庭设备被分为三种类型：

- 类型A设备，如遥控器、PC或PDA，它们能够控制一个类型B或类型C设备；
- 类型B设备是连接类型C设备（没有任何通信接口）和网络的网桥，即类型B设备与网络中使用专用语言或控制机制的其他设备进行通信；以及
- 类型C设备，如安全相机和A/V设备，它们向其他设备提供某项服务。

一些设备结合了类型A和类型C的功能。

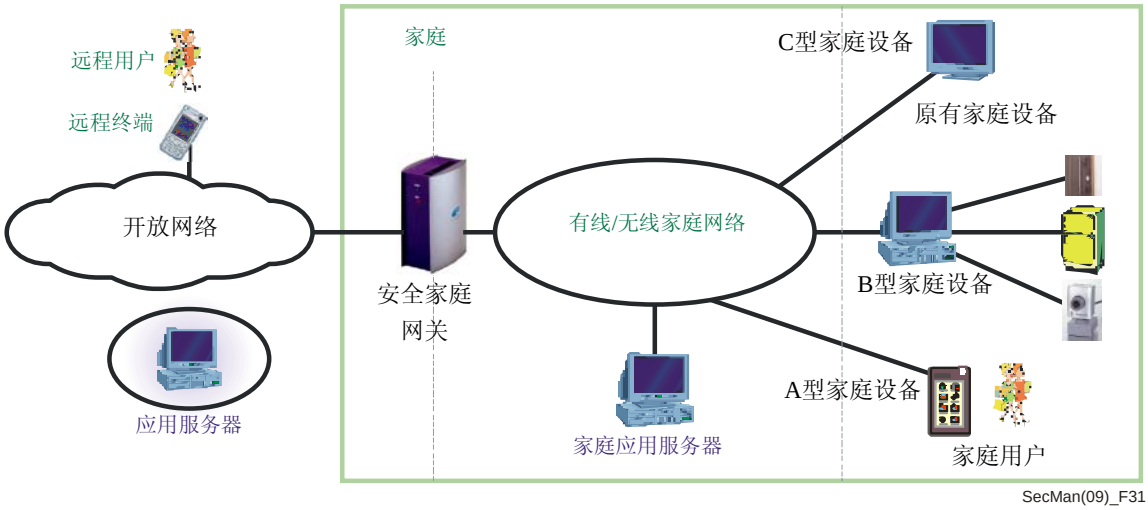


图 31 – 安全的通用家庭网络模型

ITU-T X.1111建议书从家庭用户和远程用户的角度，对安全威胁和安全要求进行了描述。另外，它还依据满足安全要求的功能以及必须应用安全技术的位置，对安全技术进行了分类。

8.3.2 家庭网络中的设备证书和认证

对家庭网络中的设备认证有两种选择：一是外部证书发放模型，在该模型中，由一个外部认证机构（CA）来发放所有的家庭设备证书；二是内部证书发放模型，在该模型中，由家庭网络中的一个内部认证机构来发放设备证书（包括自签署的证书和最终实体的证书）。通常，一个内部认证机构是一个安全的家庭网关，它有能力来生成一个密钥对，并发放证书，也就是说，家庭网关既可以发放认证机构的证书，也可以发放家庭设备的证书。安全的家庭网络本身就可以拥有一个由外部认证机构发放的设备证书，以供外部的家庭服务使用。这种外部发放的家庭网关设备证书可用于家庭网关与网络服务提供商之间的认证。

ITU-T X.1112建议书描述了一种用于设备证书发放以及家庭网络管理和使用的内部模型的框架。图32对该模型进行了说明。

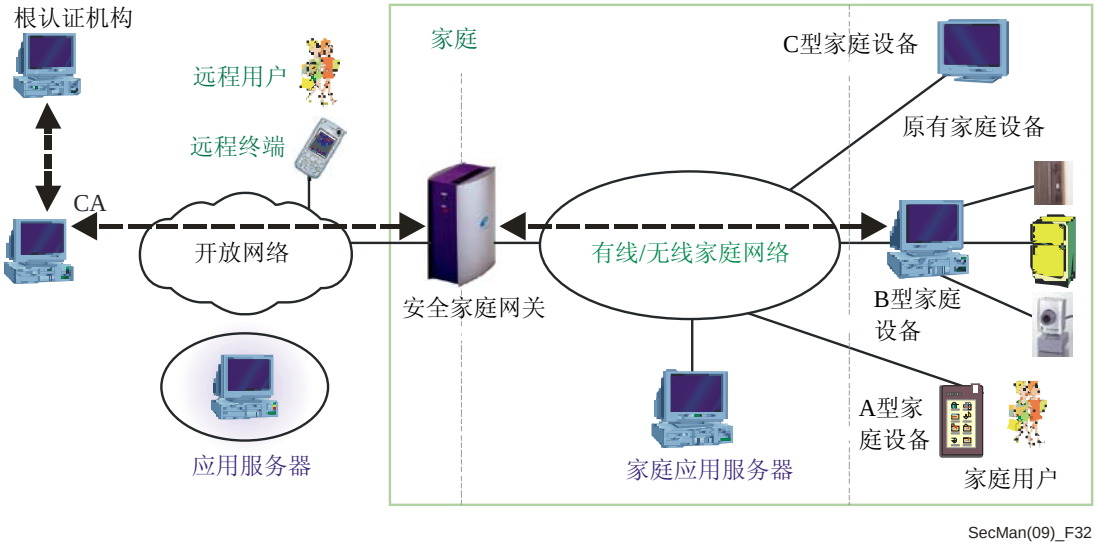


图 32 – 安全的家庭网络的设备认证模型

对设备认证，家庭网络中的每一个设备都需要一个唯一的标识符。特别是当用在家庭网络中时，家庭设备证书将作为唯一的信任元素。

图33显示了四种典型的设备证书使用案例：1) 在远程终端与安全的家庭网关之间；2) 在应用服务器与安全的家庭网关之间；3) 在家庭设备与安全的家庭网关之间；4) 在家庭设备与家庭设备之间。

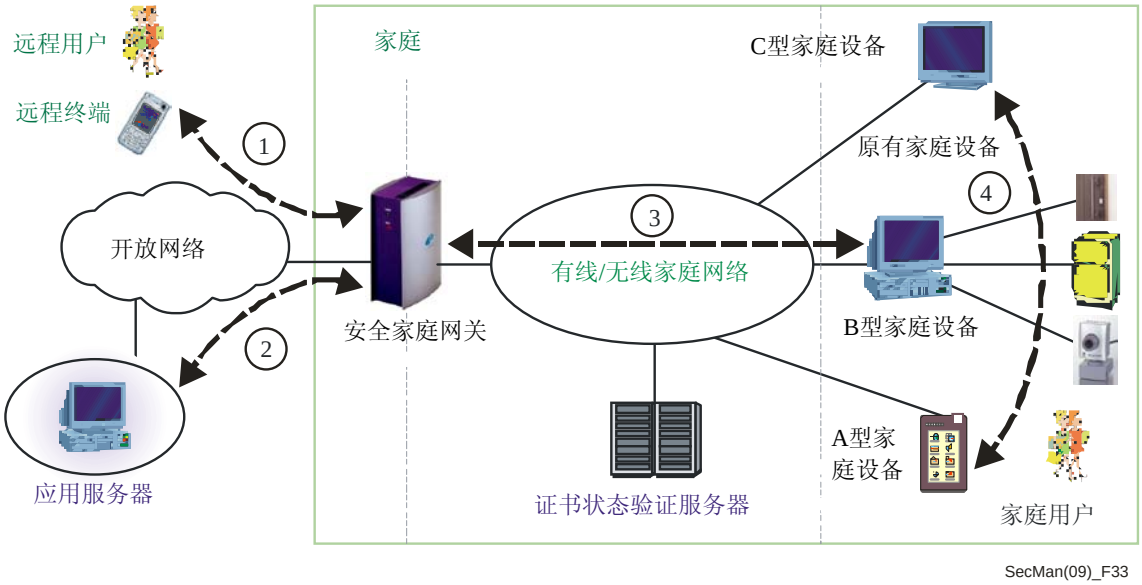


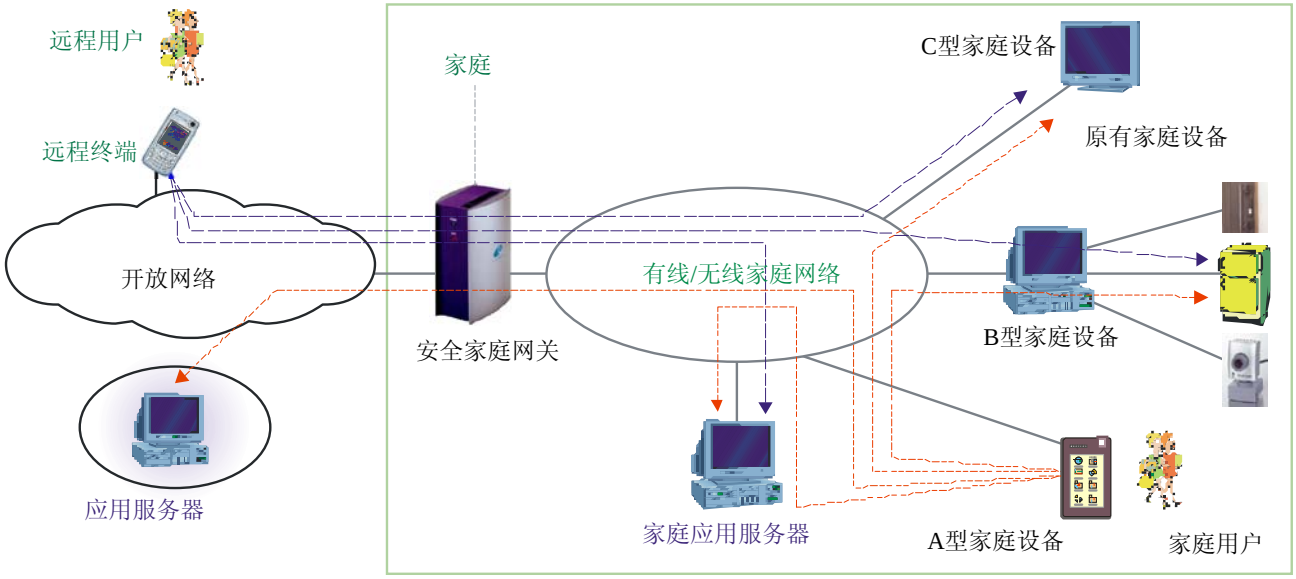
图 33 – 基于安全的通用家庭网络模型的设备认证应用案例

对从家庭设备到外部应用服务器的外部互联网服务，应首先利用安全的家庭网关（它使用自身的设备证书）对家庭设备进行认证，然后利用外部应用服务器（它使用外部认证机构发放的家庭网关证书）对安全的家庭网关进行认证。这些使用案例可以用于各种各样的应用协议，以支持安全的家庭网络服务。

8.3.3 家庭网络服务的用户认证

一些环境要求对用户进行认证，而不是对过程或设备进行认证。在这些情况下，认证系统要求用户证明其唯一性。这种唯一性通常以特性为基础，如已知的某事、已有的某事或者用户某些不可改变的特性。

ITU-T X.1113建议书为家庭网络提供了有关用户认证的指导原则，使之能够使用各种各样的认证技术，如口令、证书和生物特征识别技术。它还依据认证服务情形，定义了安全保证等级。图34显示了基于ITU-T X.1111建议书中所定义的家庭网络安全通用模型的认证服务流程。在该例子中，一个远程用户试图访问家庭内的实体，而家庭用户试图访问家庭内和家庭外的实体。



SecMan(09)_F34

图 34 – 家庭网络的认证服务流程

8.4 IPCablecom

IPCablecom系统可以使得有线电视运营商在它们已经改造成支持电缆调制解调器的网络上提供基于IP的实时服务（例如话音通信）。

8.4.1 IPCablecom体系结构

在ITU-T J.160建议书中规定了IPCablecom体系结构。IPCablecom各组成部件如图35所示。IPCablecom体系结构既包含可信的网络元素，又包含不可信的网络元素。通常，可信的网络元素位于电缆运营商的被管骨干网内。通常，不可信的网络元素，如电缆调制解调器和媒体终端适配器（MTA），位于订户家中电缆运营商的设施外。

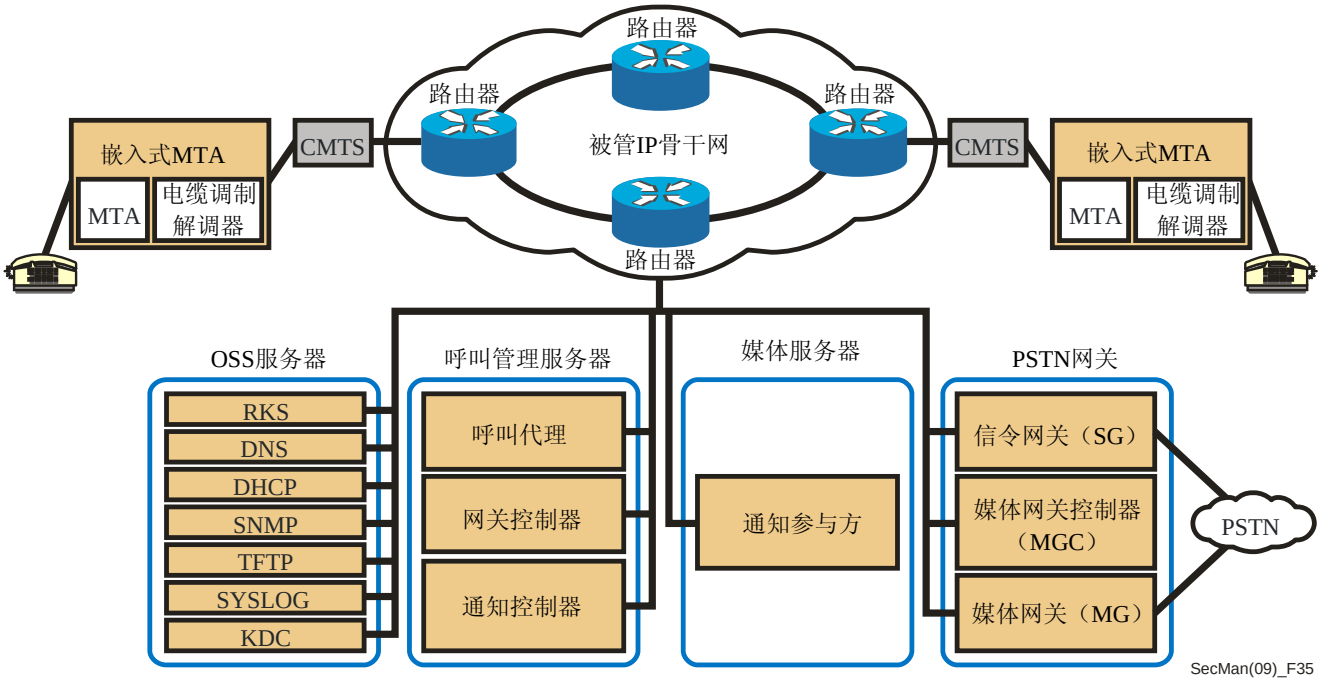


图 35 – IPCablecom构成参考模型

8.4.2 IPCablecom的安全要求

每个IPCablecom的协议接口都面临可能对订户和服务提供商二者造成影响的威胁。例如，媒体流通路可能穿越大量潜在未知的互联网服务和骨干网服务提供商。结果是，媒体流可能会很容易受到恶意窃听，以致泄露通信秘密。在IPCablecom体系结构中确定的安全设计目标是：

- 使住家的话音能力具有与PSTN等同的或比PSTN更高的保密性；
- 提供保护，抵御对MTA的攻击；以及
- 保护电缆运营商免遭网络破坏、拒绝服务和盗窃服务攻击。

设计时必须考虑的因素包括机密性、认证、完整性和访问控制。

在ITU-T J.170建议书《IPCablecom安全规范》中，规定了安全要求。对有待解决的各种威胁，概述如下：

- 盗窃服务，包括：订购欺诈、不支付服务费用、MTA克隆（例如，当MTA注册在一个欺骗性的账号下时，就认为它被克隆了）、假冒网络服务器、协议操纵；
- 泄露载波信道信息，包括：简单的窥探、MTA克隆（例如，对一个可公开接入的MTA）、协议操纵、离线密码分析、破坏服务；
- 泄露信令信息；
- 盗窃基于MTA的服务；以及

- 与一个不同的服务提供商非法注册一个租用的MTA。

8.4.3 IPCablecom的安全服务和机制

IPCablecom的安全是在低层堆栈元素上实现的，因此大多使用IETF规定的机制。IPCablecom体系结构通过为每个已定义的协议接口具体规定向协议接口提供所需安全服务的基础安全机制（如IPSec），来应对这些威胁。在X.805体系结构范畴内，IPCablecom安全服务的概述部分论及了源百图1中三个平面和三层的所有九个方格。

通过IPCablecom的核心服务层实现的安全服务是认证、访问控制、完整性、机密性和不可抵赖性。这些安全机制既包括安全协议（如IPSec、实时协议（RTP）层安全和SNMPv3安全），也包括支撑的密钥管理协议（如IKE、PKINIT/Kerberos）。此外，IPCablecom的核心安全服务包括一种为RTP媒体流提供端对端加密的机制，从而大大减少对通信秘密的威胁。

8.5 IPCablecom2

IPCablecom2是一个电缆行业倡议，旨在支持话音、视频、数据和移动性技术的融合。

8.5.1 IPCablecom2体系结构

IPCablecom2基于第6版IP多媒体分系统（IMS），如第三代合作伙伴计划（3GPP）所定义的那样。3GPP的工作范围包括制定有关GSM和第三代（3G）移动系统网络的技术规范，为移动网络开发一个基于SIP的IP通信体系结构。形成的体系结构 — *IP多媒体分系统*，作为ITU-T J.360建议书中定义的IPCablecom2体系结构的基础。

8.5.2 IPCablecom2的安全要求

IPCablecom2安全体系结构的设计目标包括：

- 支持机密性、认证、完整性和访问控制机制；
- 保护网络免遭拒绝服务、网络破坏、盗窃服务攻击；
- 保护用户设备（UE）（即客户端）免遭拒绝服务攻击、安全弱点、网络未经授权的访问；
- 通过加密和控制访问订户数据（如订户是否存在的信息）机制，保护最终用户的秘密；
- 有关设备、用户设备和用户认证的机制；安全提供服务、安全信令和安全软件下载；以及
- 进一步扩大IMS安全体系结构的作用和影响，延伸之前所述的目标。

针对IPCablecom2的常见威胁有：

信任域威胁

一个信任域指的是网络元素的一个逻辑分组，对通信而言，这些网络元素是可信的。可以通过物理边界或逻辑边界来划分信任域。必须总是利用认证和授权手段对跨信任域的通信实施保护。另

外，必须保证一个域内连接网络元素的接口、域与域之间的接口、用户设备与服务提供商之间的接口的安全，以抵御各种各样的威胁。

盗窃服务

盗窃服务可以通过许多方式来实现，包括但不限于：操纵用户设备；利用协议弱点；窥探身份；克隆用户设备（即模仿一个合法用户设备的行为）；以及订户欺诈和不支付服务费用。

破坏和拒绝服务

这包括一般性的拒绝服务攻击；“注水”式的攻击（即：使某个特定的网络元素无法使用，通常通过向其接口发送过量的媒体网络业务流量来达成此破坏目的）；以及使用“僵尸”（即：许多中间的端点系统）进行攻击。

信令信道威胁

在多媒体环境中，信令报文包括与身份有关的数据、业务、路由以及其他敏感的和关键的数据。多媒体部件，如各种代理，存在于访问域中，将之暴露于更多的威胁面前。针对信令威胁的攻击包括：破坏信令信息的机密性；中间人攻击，这些攻击截获并可能修改在两个通信方之间传送的业务；以及信令信道范畴的拒绝服务攻击。

载波信道威胁

对载波信道的威胁与在通信各方之间传送的媒体业务有关。

协议特定的安全威胁

存在众多针对单个多媒体协议的威胁。

8.5.3 IPCablecom2的安全服务和机制

IPCablecom2广泛利用在3GPP IP多媒体分系统（3GPP 23.002 v6.10.0，《网络体系结构》，2005年12月）中提到的传输层安全和其他机制。以下各节概述对IMS安全体系结构做了哪些有关IPCablecom2方面的增强。

8.5.3.1 用户和UE认证

IPCablecom2体系结构支持以下认证机制：

- IP多媒体分系统认证和密钥协定；
- 会话开始协议（SIP）摘要认证；以及
- 证书引导。

体系结构通过多种认证证书来适应各种用户设备（UE）。例如，当在电缆网络中时，用户设备可以拥有一个有关接入服务的证书；当在一个蜂窝网络中时，用户设备可以拥有一个有关接入服务的通用集成电路卡（UICC）。

一个订户可以拥有多个证书。一个用户可以拥有多个用户设备，具有与这些证书相关的不同能力。例如，一个订户可以拥有一个媒体终端适配器（MTA），其证书针对的是家庭应用，并拥有一个基于UICC的用户设备，其证书针对的是移动应用。

8.5.3.2 信令安全

IPCablecom2增加了传输层安全（TLS），作为用户设备（UE）与代理呼叫会话控制功能之间信令安全的一个选项。对信令安全而言，用还是不用TLS（如IP多媒体分系统（IMS）所定义的那样）是任选的。

8.6 无处不在的传感器网络的安全

传感器只是一个能产生电信号的设备，产生的电信号代表一个可度量的物理特性。无处不在的传感器网络（USN）是一种使用低成本、低功率传感器的网络，以提高对周边环境的感知能力，并可在任何时候、在任何地方、向任何人提供感知到的信息和知识服务。一个USN网络可以覆盖一个很大的地理范围，并可支持各种各样的应用。图36显示了潜在的USN应用。

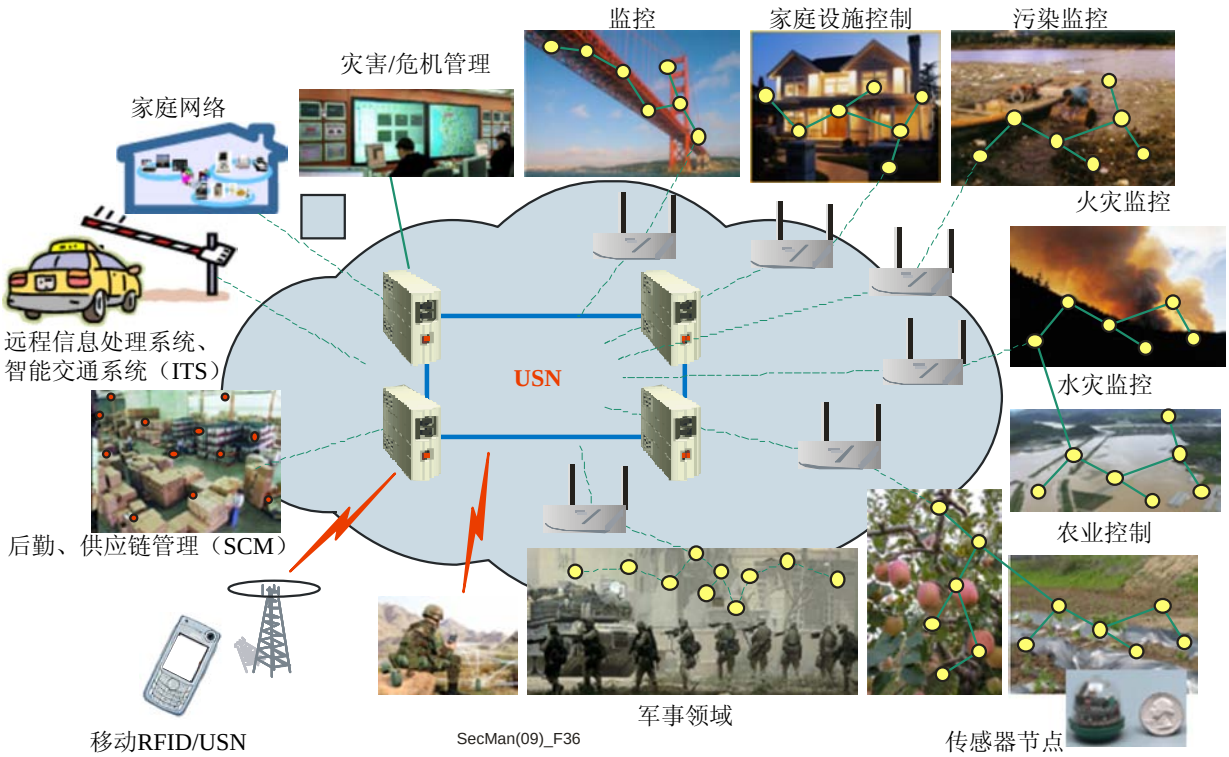


图 36 – 潜在的USN应用

传感器网络通常连接于最终用户网络，在核心传输网络可能使用互联网和下一代网络技术的同时，它将可以使用各种各样的基础技术（如DSL、卫星、GPRS、CDMA、GSM等）。

由于在USN网络中传送的信息面临许多潜在的威胁，因此需要使用有效的安全技术来应对这些威胁。

除了标准的联网威胁（如第3节中所讨论的那些威胁）之外，还存在许多针对USN网络的威胁，它们包括：

- **传感器节点破坏**：单个传感器遭到攻击或破坏，或者攻击者引入不当的传感器；
- **窃听**：监控节点间的传输情况；
- **破坏或泄露感知到的数据**；
- 针对传感器或通信的**拒绝服务攻击**；以及
- **恶意使用或误用网络传感器**：例如，将传感器用于非法目的。

另外，USN网络还面临许多与传感器节点间路由有关的威胁。

传感器网络的特性极大地增加了安全网络设计过程的复杂性。例如，由于传感器节点有限的计算能力和存储空间以及有限的功率和带宽，因此它无法使用公开密钥加密技术或者在节点上保存唯一的密钥。另外，传感器可能位于敌意的环境中，以及在部署后可能并不知道其准确位置。最后，传感器网络高度依赖其基站，基站不仅是潜在的故障单点，而且对潜在的攻击者而言，是一个富有吸引力的攻击目标。

USN中间件提供了一个公共应用平台，用于支持代表USN应用和服务的各种各样功能，并对传感器网络实施控制。传感器网络收集的大量数据通过USN中间件来保存、管理和分析，USN中间件还必须安全地将数据传送给适当的应用。中间件安全措施必须解决储存状态和传输期间数据的安全性问题，以及解决中间件的可用性问题。

尽管尚未达成任何USN建议书，但工作正在顺利进展中，以解决USN网络本身的安全需求以及USN中间件的安全需求。

9. 应用安全

9 应用安全

随着对安全重要性的认识越来越深，目前应用开发商更加关注在其产品中植入安全性，而不是在应用投入生产后再来改进安全性。尽管这样，仍发现大多数应用在其生命周期的某些节点上存在先天不足。另外，新的威胁常常发现和利用先前未知的弱点。

本节分析了众多信息通信技术应用的安全特征，重点强调ITU-T各建议书所论述的安全特征。

9.1 IP话音（VoIP）和多媒体

ITU-T H.323建议书《基于数据分组的多媒体通信系统》是一个总括性的建议书，它为通过包括互联网、局域网（LAN）和广域网（WAN）在内、不提供服务质量（QoS）保证的分组交换网进行话音、视频和数据通信奠定了基础。这些网络主要是目前的企业办公网络，还包括以太网上的分组交换TCP/IP和互联网分组交换（IPX）、高速以太网和令牌环网技术。遵守了ITU-T H.323，多个供货商的多媒体产品和应用就可以互操作，使得用户在通信时不必担心产品的兼容性。ITU-T H.323是第一个规定的VoIP协议，被认为是VoIP类产品的基础，用于消费者、企业、服务提供商、娱乐业和专业应用。在以下文件中包含了有关ITU-T H.323系列建议书的安全规范：文件ITU-T H.Imp235《H.235 V3实施者指南：“H系列（ITU-T H.323和其他基于H.245的）多媒体终端的安全和加密”》、ITU-T H.235.x建议书 — 包含九个安全框架和标准的系列建议书、ITU-T H.530建议书《H.510中有关H.323移动性的对称安全程序》。有关ITU-T H.323多媒体系统和服务的移动性，在ITU-T H.510建议书中进行论述。

ITU-T H.323涵盖的范围宽泛，既涉及独立的设备，也涉及嵌入式个人计算机技术，还涉及点对点和点对多点会议。

ITU-T H.323建议书定义了以网络为基础的通信系统的四个主要组成部分：终端、网关、网守和多点控制单元。此外，可能还有边界元素或对等元素。这些元素如图37所示。

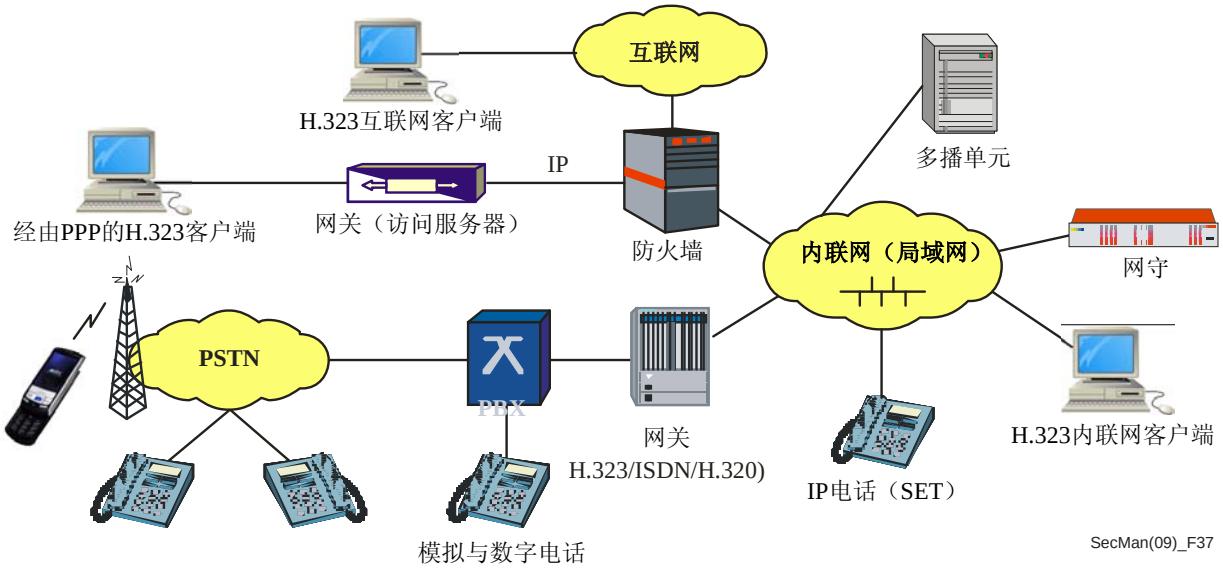


图 37 – H.323系统：组成部件和配置方案

应用ITU-T H.323的例子包括运营商从事的批发转接服务，特别是VoIP骨干网和电话卡服务的转接。在集团通信中，ITU-T H.323用于IP-PBX交换机、IP交换中心、话音虚拟专用网（VPN）、话音和数据集成系统、Wi-Fi电话、呼叫中心的实施以及移动业务。在专业通信中，ITU-T H.323广泛用于话音（或音频）和电视会议，用于话音/数据/电视集成和远程教育。在家庭环境中，用途包括宽带视听接入、个人计算机到电话、电话到个人计算机以及个人计算机到个人计算机的呼叫；它还可以用于定制新闻和信息的传送。

9.1.1 多媒体和VoIP中的安全问题

由于ITU-T H.323系统中的所有元素在地理上都可以是分布式的，且由于IP网络的开放特性，因此出现了一些安全威胁，如图38所示。

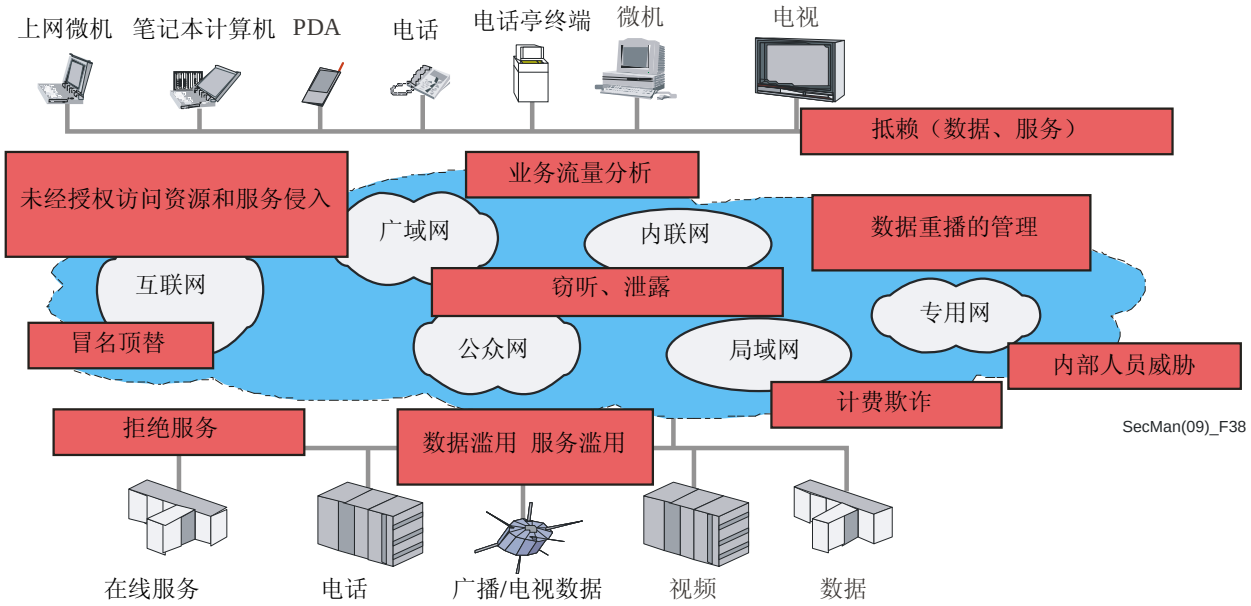


图 38 – 多媒体通信中的安全威胁

多媒体通信和IP电话中的主要安全问题如下所述：

- 用户和终端认证：VoIP服务提供商为了准确搞清服务使用量，也可能为了按服务使用量计费，需要知道谁正在使用其服务。作为认证的一个先决条件，用户和/或终端必须用某种身份来标识。然后，用户/终端必须证实其声称的身份是真实的。这种情形通常通过强密码认证程序（例如受保护的口令或ITU-T X.509数字签名）进行。
- 服务器认证：由于VoIP用户之间通常通过某些带有相关服务器（网守、多播单元、网关）的VoIP基础设施来实现相互通信，因此用户关心的是他们是否连接了正确的服务器和/或正确的服务提供商。这方面的问题涉及固定用户和移动用户。
- 用户/终端和服务器认证：用之来应对安全威胁，例如冒名顶替、中间人攻击、IP地址欺骗和连接劫持。
- 呼叫授权：这是一个决策过程，以确定用户/终端是否真的被允许使用服务特性（如呼叫PSTN）或网络资源（QoS、带宽、编解码器等）。特别常见的是将认证和授权功能结合起来实现访问控制判断。认证和授权有助于阻止类似冒名顶替、误用与欺诈、操纵与拒绝服务等攻击。
- 信令安全保护：这解决的是保护信令协议免遭操纵、误用以及机密性和保密问题。信令协议的保护一般通过密码加密方式以及完整性和重播保护措施来完成。为满足实时通信的关键性能要求，必须格外谨慎，以免因安全处理而对服务造成任何损害。

- 话音机密性：这通过加密话音数据包来实现，并防止窃听。通常，对多媒体应用的媒体数据包（如视频）以及话音数据要加密。进一步的媒体数据包保护还包括对有效载荷的认证/完整性保护。
- 密钥管理：这不仅包括为向用户和服务器安全分发密钥资料而必需的所有任务，而且包括如更新过期的密钥和替换遗失的密钥等任务。密钥管理可以是一个独立于VoIP应用（口令提供）的任务，或者在动态协商表明安全能力的安全简表以及分发基于会话的密钥时，也可以与信令综合在一起。
- 跨域安全：这涉及的问题是，异构环境中的系统因不同的需求、不同的安全策略和不同的安全能力而实施了不同的安全特性。因而有必要能够动态地协商安全简表和安全能力，如密码算法及其参数。在跨越域的边界以及涉及不同的服务提供商和网络时，这一点尤为重要。跨域通信的一个重要安全要求是能够平滑地越过防火墙以及应对网络地址转换（NAT）设备的限制。

该清单虽不全面，但涵盖ITU-T H.323安全性的核心部分。超出ITU-T H.323考虑范围之外的安全问题包括安全策略、网络管理安全、安全服务提供、实施安全、操作安全和安全事故处置。

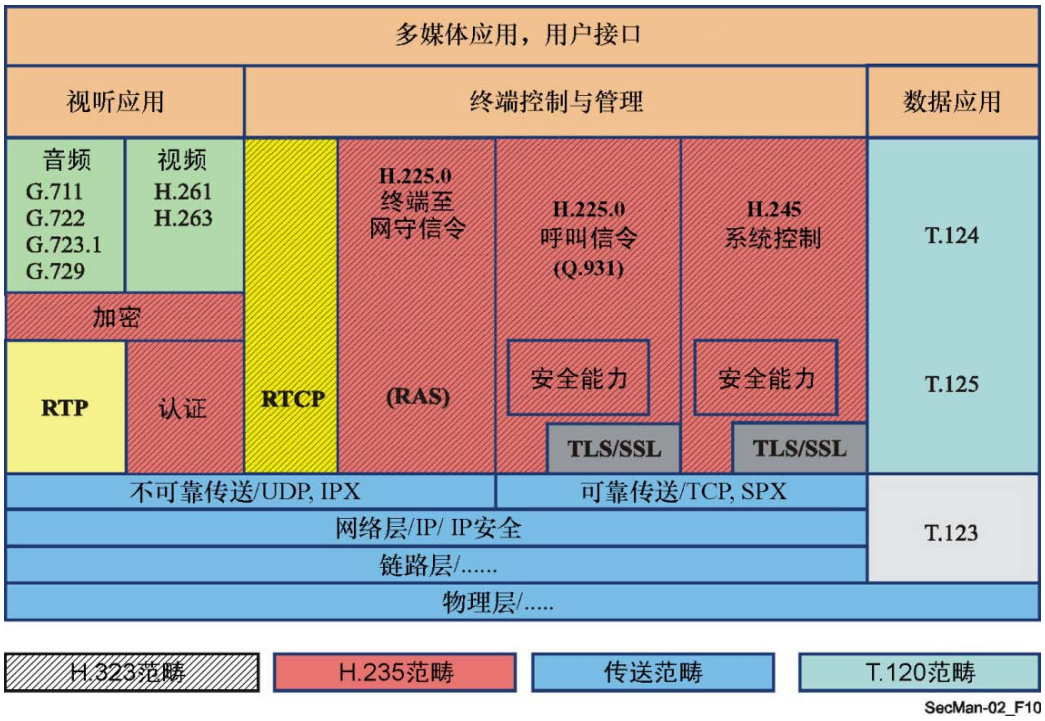
9.1.2 H.235.x分支系列建议书概述

H.235.x系列建议书包括11个标准和1个实施者指南，它们一起规定了安全机制和协议以及详细的、有关在ITU-T H.323系列建议书中实施安全性的指导原则。它们为小型企业集团和大型运营商提供可调整的安全解决方案，并提供控制协议的密码保护以及音频/视频媒体流数据的密码保护。

ITU-T H.235建议书规定了协商所需的密码服务、密码算法和安全能力的方法。建立动态会话密钥的密钥管理功能完全可与信令握手协议整合在一起，这样将有助于减少呼叫建立的延迟时间。支持的配置包括“传统的”点对点通信，还支持多个多媒体终端在集团内通信时带有多播单元的多点配置。

ITU-T H.235利用了专门优化的安全技术来达到严格的性能要求，如椭圆曲线密码算法和AES加密技术。通过加密RTP有效载荷在应用层实现话音加密。这样就有益于通过采用与数字信号处理器（DSP）和话音压缩编解码器的紧密相互作用实现体积小巧的端点，而无需特殊的操作系统平台。

图39给出了ITU-T H.235的应用范围，包括用于建立呼叫（ITU-T H.225.0和ITU-T H.245模块）和双向通信（对含有压缩的音频和/或视频的RTP有效载荷加密）的相关规定。这些功能性包括认证、完整性、保密和不可抵赖性的机制。网守通过对端点的准入控制来实现认证，并提供不可抵赖性机制。基于IP的传送层和低层安全超出了ITU-T H.323和ITU-T H.235的范围，但通常可以用IP安全（IPSec）和传送层安全（TLS）协议来实现。如果最终系统策略需要，那么IPSec或TLS能够用来提供IP层的认证以及非强制性地提供机密性，而无论上面运行的是什么样的（应用）协议。



SecMan(09)_F39

图 39 – ITU-T H.235提供的ITU-T H.323安全

ITU-T H.235.x系列建议书含有各式各样的安全措施，可以适用于不同的目标环境（如企业内/企业间和运营商内/运营商间），依据本地因素，如可用的安全基础设施和终端能力（如简单端点对智能端点），可以对之进行定制，以及适用于特定的情形。

可用的安全简表提供了安全技术，范围从包括口令保护在内的简单秘密共享简表到使用数字签名和ITU-T X.509 PKI证书（ITU-T H.235.2）的更复杂的简表。这样就既可以用较简单但难于升级的技术实施逐跳保护，也可以用可升级的PKI技术实现端对端保护。ITU-T H.235.3被称为混合安全简表，原因是该建议书综合了ITU-T H.235.1中的对称安全程序和来自ITU-T H.235.2的PKI证书与签名，从而达成优化的性能和较短的呼叫建立时间。ITU-T H.235.4放松了对网守路由选择、以服务器为中心的体系结构的高度依赖，并给出了保证对等模式的安全措施。该建议书还定义了公司和跨域环境中的密钥管理程序。

为了给采用个人身份号（PIN）或口令对用户进行认证的系统提供更强的安全性，ITU-T H.235.5提出了另一种用公开密钥法为PIN/口令的使用提供安全保障的“使用弱共享秘密在*RAS*中的安全认证框架”。ITU-T H.235.6建议书《具有本地H.235/H.245密钥管理的话音加密概要》汇集了所有实现RTP媒体流加密所需的程序，包括环绕密钥管理，在ITU-T H.245信令字段内对之做了全面描述。

ITU-T H.530建议书《H.510中有关H.323移动性的对称安全程序》涵盖了在分布式ITU-T H.323环境中安全的用户和终端移动性，它解决了以下安全问题：

- 被访外部域的移动终端/用户认证和授权；
- 被访域的认证；
- 安全的密钥管理；以及
- 移动终端和被访域之间的信令数据保护。

ITU-T H.235.0建议书为H系列多媒体系统提供了总的安全框架，ITU-T H.235和ITU-T H.350系列建议书也采用轻量级号码簿访问协议（LDAP）和安全套接字层（SSL/TLS），规定了可升级的密钥管理。ITU-T H.350系列建议书提出了一些能力，使企业和运营商能安全地管理使用视频和IP话音（VoIP）服务的大量用户，并提出了一种将ITU-T H.323、SIP、ITU-T H.320和通用消息服务与号码簿服务联系起来的方法，令现代的身份管理措施得以应用于多媒体通信。

9.1.3 网络地址转换和防火墙设备

设计互联网时原本考虑了“端对端”原则。也就是说，网络上的任何设备都可以直接与网络上的任何其他设备进行通信。不过，由于担心安全和IPv4网络地址短缺，在网络的边界处常常会使用防火墙（FW）和网络地址转换（NAT）设备。这些边界包括住宅域、服务提供商域、企业域，有时还包括国家域。在某个域内，有时要使用不止一个防火墙或NAT设备。防火墙设备旨在对信息如何跨越网络边界实施控制，通常防火墙要配置为阻断大部分IP通信。除非防火墙明确配置为允许外部设备的ITU-T H.323业务流量通过边界到达内部的ITU-T H.323设备，否则简直无法进行通信。这对ITU-T H.323设备的任何用户来说都是一个问题。

NAT设备将内部域中所用的地址转换成外部域中所用的地址，或者反过来。住宅域或企业域中所用的地址通常、但并不总是从IETF RFC 1918规定的专用网络地址空间得到分配。这些地址空间是：

类别	地址范围	IP地址数量
A	10.0.0.0 – 10.255.255.255	16,777,215
B	172.16.0.0 – 172.31.255.255	1,048,575
C	192.168.0.0 – 192.168.255.255	65,535

NAT设备对大多数IP协议产生的问题更让人烦心，尤其是在协议中承载IP地址的那些协议。ITU-T H.323、SIP和在分组交换网上运行的其他实时通信协议必须提供IP地址和端口信息，以便让参与通信的其他各方了解向何处发送媒体流（如音频和视频流）。

ITU-T对跨越NAT/FW的问题做了研究，形成了三个ITU-T H.460系列建议书，使ITU-T H.323通信得以无缝跨越一个或多个NAT/FW设备。这几个建议书是：ITU-T H.460.17《采用H.225.0呼叫信令连接传送H.323 RAS报文》、ITU-T H.460.18《H.323信令跨越网络地址转换器和防火墙》和ITU-T H.460.19《H.323媒体跨越网络地址转换器和防火墙》。

图40描绘了一个特殊的“代理”设备是如何帮助“不了解”NAT/FW的设备来正确跨越NAT/FW边界的。

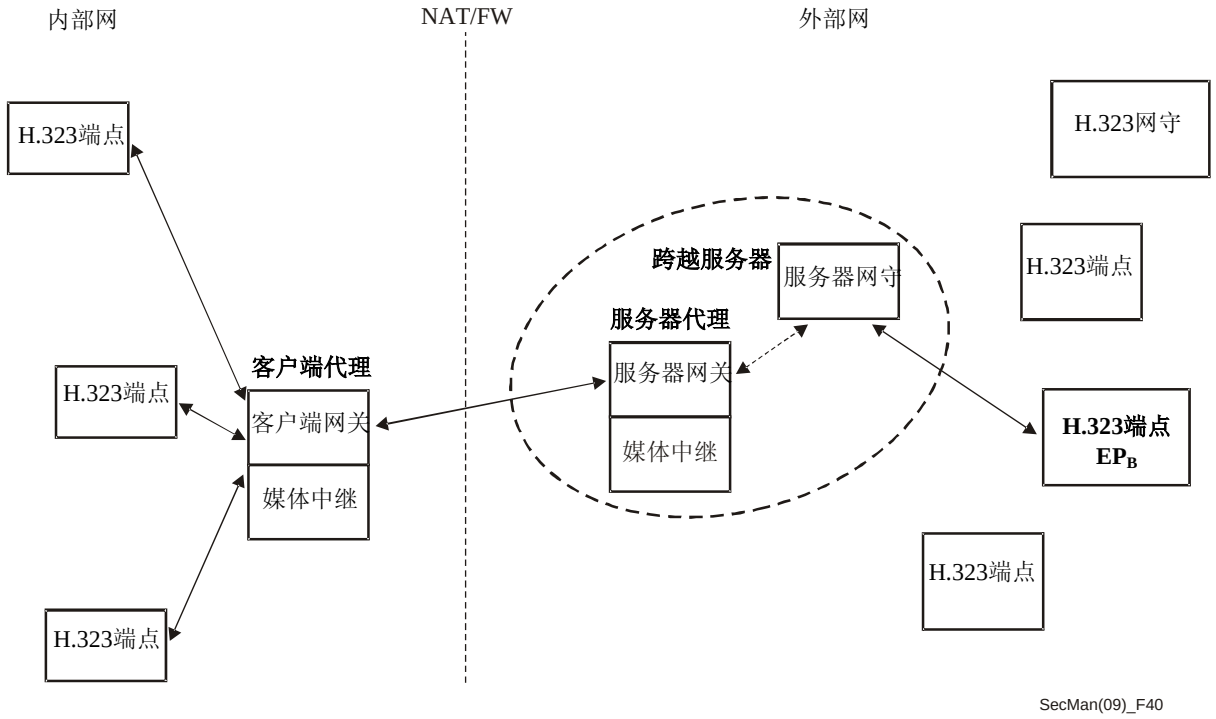


图 40 – H.460.18体系结构中的NAT/FW跨越

上述拓扑结构可能也适合其他情况，比如某个企业希望控制ITU-T H.323呼叫信令和媒体穿越网络所经过的路由。但是ITU-T H.460.17和ITU-T H.460.18也允许端点无需任何特殊内部“代理”设备的帮助而跨越NAT/FW边界。图41对一种这样的拓扑结构做了说明：

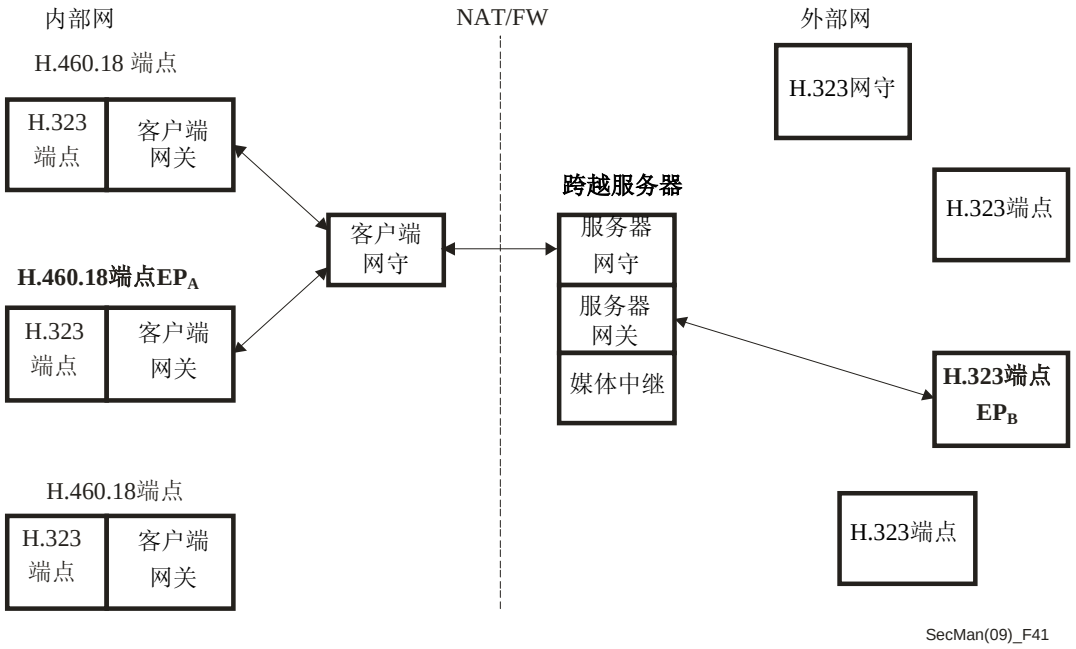


图 41 – 网守通信体系结构

在图41中，内部网上的端点为了解析外部实体的地址（如将一个电话号码或ITU-T H.323 URL转换成一个IP地址）而与内部网中的网守通信。内部网中的网守则与外部网中的网守通信，以便交换该寻址信息，并将该信息返给主叫端点。内部网中的设备在向外部网中的设备发出呼叫时，会采用ITU-T H.460.18建议书中规定的程序，在NAT/FW设备上撕开必要的“小洞”，让内部网的信令到达外部网。另外，该内部网中的设备还会采用ITU-T H.460.19建议书中规定的程序，撕开必要的“小洞”，让媒体流正确地跨越内部网到达外部网，或者反过来。

如果主叫和被叫设备分别位于由NAT/FW设备和公众互联网隔开的不同专用网内，那么必须具备至少一个“服务器网关”或一个“媒体中继”设备（在ITU-T H.460.18建议书中定义），以便在两个专用网之间正确地为信令和媒体选择路由。设备的这种组合通常称为“会话边界控制器”。原因很简单，因为按照设计，没有公众网中某个实体帮助“代传”数据包，一个专用网中的IP数据包就无法进入另一个专用网。

9.2 IPTV

网际协议电视（IPTV）的安全性规定必须涵盖对通过IPTV服务传送的内容、所用的终端设备的保护，以及有关此类服务的规定。

对IPTV，内容保护指的是确保最终用户只能依据权限持有者授予的权限来使用内容。这包括防止内容被非法拷贝和分发、截获、篡改和未经授权的使用。

对IPTV终端设备的保护包括确保最终用户用于接受服务的设备能够安全可靠地使用内容、行使内容使用权、保护内容完整性和机密性，以及保护关键的安全参数，如加密密钥。

IPTV服务保护包括确保最终用户只能获得其有权接受的服务和内容，它还包括防止未经授权地访问服务。

正在制定多个有关IPTV安全性的建议书，其中的ITU-T X.1191建议书《IPTV安全问题的功能要求和体系结构》已经获得批准。在该建议书中定义的IPTV通用安全体系结构如图42所示。注意：在该建议书中，只对那些用于最终用户、网络提供商和服务提供商的功能进行了论述。与内容提供商有关的功能受制于利益相关者之间的专用协定，不在该建议书的讨论范围之内。

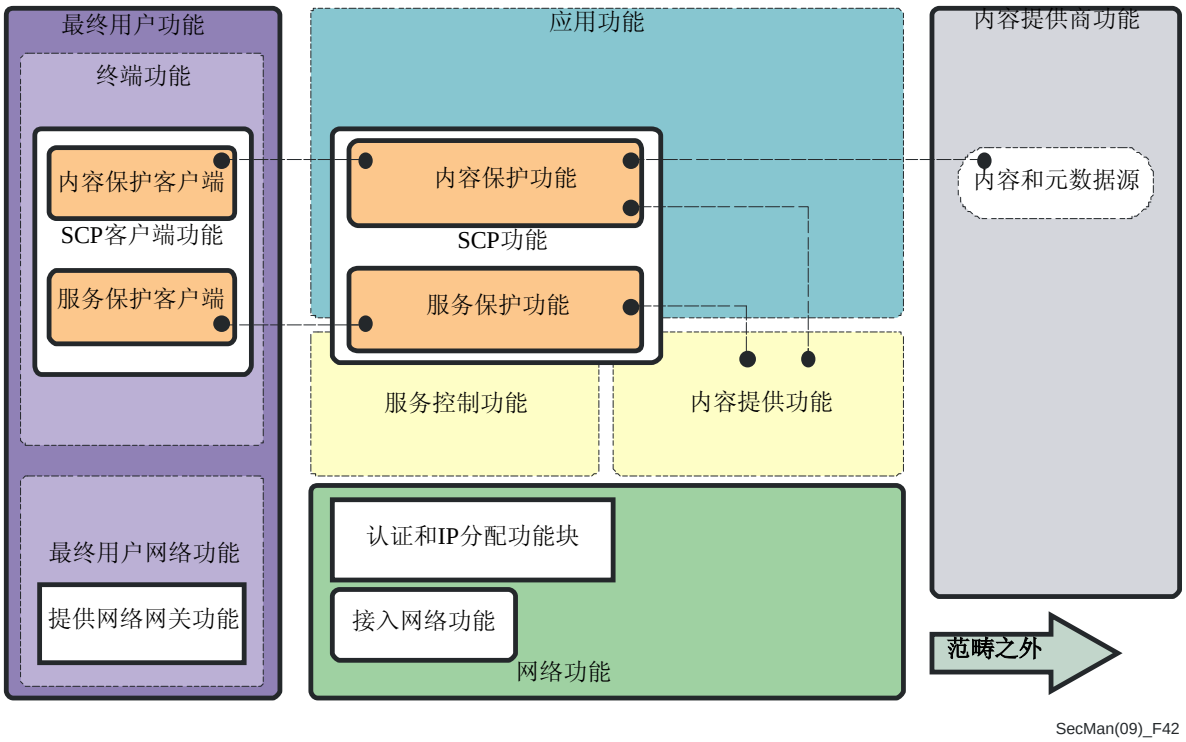


图 42 – IPTV通用安全体系结构

9.2.1 IPTV内容保护机制

可用于保护内容的安全机制包括：

- 内容加密；
- 水印（即使用隐写术来改变某些内容特征，而这种改变不易被察觉）；
- 内容跟踪识别和信息，以便调查未经授权的内容访问和使用；
- 内容标记（如等级信息，以便最终用户对不当内容访问实施某种程度的控制）；以及

- 安全译码（允许中间的网络节点能在不解密的情况下将多媒体内容转换成一种不同的格式或品质，从而保持端对端安全性）。

9.2.2 IPTV服务保护机制

服务保护机制包括：

- 最终用户（订户）和/或终端设备的认证；
- 授权（确保最终用户或终端对服务和/或内容的访问是经过授权的）；以及
- 访问控制（尤其要确保从客户端向服务器上载的内容只能被经过授权的服务提供商访问）。

9.2.3 订户信息的保护

在实施IPTV时，一个需要特别关注的问题是要保护好订户信息，它可能包括被追踪的数据信息，如信道改变之前和之后的信道号、改变的时间、用于电子项目指南服务的用户信息、数据包识别信息、参与的时间等。对该数据必须当做敏感数据来对待，必须采取措施，防止经由终端、网络或服务提供商未经授权地泄露这些数据。在ITU-T X.1191建议书的一个附件中包含了有关订户信息保护的建议。

9.3 安全传真

传真仍是一种非常普遍的应用，但传真服务的机密性很大程度上依赖于内置安全措施的有效性。最初，制定传真标准是为了实现在 PSTN 上的传输（ITU-T T.4 建议书），然后是为了实现在 ISDN 上的传输（ITU-T T.563 建议书）。再近一些，对传真标准进行了扩展，目的是为了通过 IP 网络（包括互联网）实时地进行传真传输（ITU-T T.38 建议书），以及通过保存并转发系统进行传真传输（ITU-T T.37 建议书）。

不论传输模式是什么，传真服务面临的安全问题包括传输数据的机密性、认证和不可抵赖性。随着因媒体的开放和分布特性而使业务流量移向互联网，这些问题变得越来越重要。

在 ITU-T T.36 建议书《用于三类传真终端的安全能力》中论述了传真安全问题，它确定了两个独立的技术解决方案，可以用于加密被交换文件。规定的一个解决方案使用的是 *Rivest, Shamir & Adleman*（RSA）密码算法；另一个解决方案结合使用霍索恩密钥管理（HKM）和霍索恩传真密码（HFX）。定义的安全服务是：

- 相互认证（强制性的）；
- 安全服务（非强制性的），包括相互认证、报文完整性和报文接收确认；
- 安全服务（非强制性的），包括相互认证、报文机密性（加密）和会话密钥建立；以及
- 安全服务（非强制性的），包括相互认证、报文完整性、报文接收确认、报文机密性（加密）和会话密钥建立。

霍索恩密钥管理（HKM）和霍索恩传真密码（HFX）组合系统为实体之间的安全文件通信提供以下能力：

- 实体相互认证；
- 秘密会话密钥建立；
- 文件机密性；
- 接收确认；以及
- 文件完整性确认或否认。

9.4 万维网服务

包括面向服务的体系结构（SOA）在内的万维网技术正得到广泛应用，原因是它们使开发商能够有效、高效费比开发和投入应用新的服务，并能够方便、快捷地将来自不同渠道的内容综合在一起，形成复合型服务。万维网服务面临许多安全方面的问题。认证和单一登入（SSO）机制至关重要，并且由于万维网服务正推向移动网络领域，因此做好对万维网服务所需安全机制的分析研究工作也很重要。

规模经济推动计算平台供货商开发具有高通用功能性的产品，以便它们能在尽可能广的领域得到应用。尽可能为这些产品提供大的特权，用于访问数据和执行软件，这样，它们就能在尽可能多的应用环境中得到应用，包括那些安全策略非常随意的应用环境。对需要更严格安全策略的应用环境，必须通过本地配置来限制平台内在的特权。

大型企业的安全策略含有许多元素和许多执行点。策略元素可以由信息系统部门、人力资源部门、法律部门和金融部门来管理。策略可以通过外部网、邮件、广域网和远程接入系统 — 内在地实施许可安全策略的平台来执行。目前的做法是独立管理每个执行点的配置情况，以便尽可能准确地实施安全策略。因此，更改安全策略是一件昂贵的、不可靠的事情，也难以（甚至可能是根本不可能）在整个企业范围内实现牢靠的防卫，以便实施安全策略。同时，消费者、相关利益者和监管者施加给公司和政府执行部门的压力正变得越来越大，以便在保护企业及其客户信息资产中展示“最佳做法”。

出于这些原因，需要一种通用语言来表述安全策略。如果在整个企业范围内实施安全策略，那么通用安全语言允许企业在其信息系统所有组成部件中对其安全策略所有元素的执行情况实施管理。对安全策略的管理可以包括一些或所有以下步骤：起草、评审、测试、批准、发布、结合、分析、修改、撤销、检索和执行策略。

另外，需要一个用于安全信息交换的框架。为了便于进行这些安全信息交换，开发了标记语言，包括安全声明标记语言和可扩展的访问控制标记语言（XACML）。这些最初由OASIS开发，但在OASIS支持下，现已被ITU-T采纳和颁布。

9.4.1 安全声明标记语言

ITU-T X.1141建议书定义了安全声明标记语言（SAML 2.0）。SAML是一个基于XML的框架，用于交换安全信息。以有关主体的声明的形式来对这种安全信息进行描述，主体指的是一个实体，

它在某个安全域中有一个身份。一个单个的声明可能含有若干个不同的、有关认证、授权和属性的内部语句。

SAML声明通常为某个*主体*而做。通常，许多*服务提供商*可以利用有关某个主体的声明来控制访问和提供定制服务，它们因此而变成某个声明方（称为*身份提供方*）的信任方。

ITU-T X.1141建议书定义了三种不同类型的声明语句，可以通过某个SAML机构来创建，SAML定义的所有语句都与某个主体有关。在ITU-T X.1141建议书中定义的三种语句是：

- 认证：在某个特定时间、利用某种特定方式对声明主体进行认证；
- 属性：声明主体与所提供的属性有关；以及
- 授权决定：授予或拒绝一个允许声明主体访问规定资源的请求。

ITU-T X.1141建议书还定义了一个协议，利用该协议，客户端可以向SAML机构请求声明，并从中得到一个回复报文。该协议由基于XML的请求和回复报文格式组成，可以绑定于许多不同的基本通信和传输协议。在构建其回复报文过程中，SAML机构可以使用各种各样的信息源，如在请求中作为输入而接收的外部策略库和声明。

为支持浏览器和其他客户端的单一登入（SSO），定义了一组简表。图43显示了用于实现SSO的基本模版。

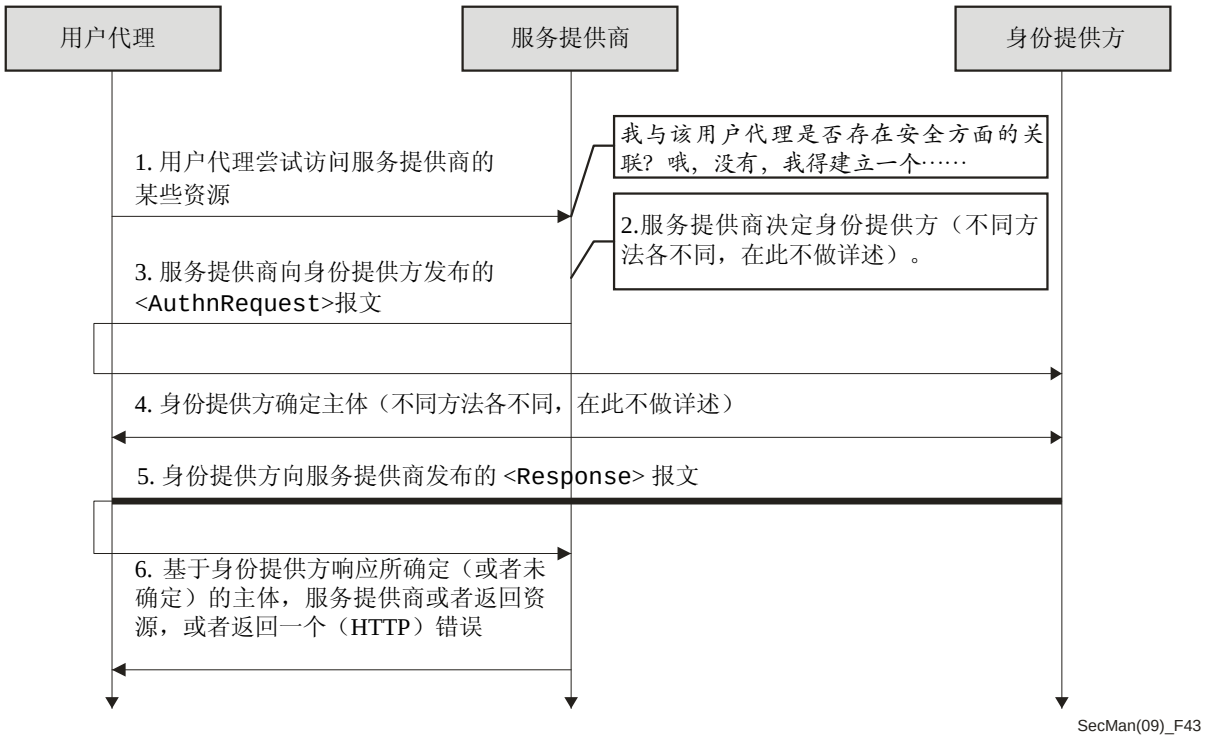


图 43 – 实现SSO的基本样板

9.4.2 可扩展的安全控制标记语言

可扩展的访问控制标记语言（XACML）是一个XML词汇表，用于表述访问控制策略。访问控制由两部分组成：一是决定是否应允许一个请求的资源访问；二是执行所做的决定。ITU-T X.1142建议书定义了核心XACML，包括语言的语法、模型、策略语言模型的范畴、语法和处理规则。为了改善有关交换基于XACML的策略的安全性，ITU-T X.1142建议书还为保证数据安全规定了一个XACML XML数字签名简表。为了向实施者提供指导原则，规定了一个保密简表。XACML适用于各种各样的应用环境。

9.5 基于标签的服务

识别标签（包括RFID标签）现得到广泛应用，但也出现了有关侵犯隐私的风险问题。部分原因是RFID技术可自动收集和处理数据，因此存在有意或无意泄露敏感信息和/或个人信息的风险。

对使用或依赖基于标签的识别技术的应用（在这些应用中涉及个人信息，如健康状况、护照和驾照），保密问题正变得越来越严重。

在学术界和工业界，有关个人识别信息（PII）保护机制的大部分工作主要集中于ID标签与ID终端之间的认证协议。不过，此类工作不能完全解决问题，原因是有关检验者的有意义的信息仍存在于网络域的服务器上。对该问题，一种解决方案是使用基于简表的PII保护机制。

ITU-T X.1171建议书《在使用基于标签的身份识别的应用中面临的威胁以及对保护个人识别信息的要求》分析了在基于商家对客户（B2C）的环境中PII面临的威胁，在这种环境中，各种应用使用基于标签的识别技术。它确定了在这种环境中保护PII的要求，并定义了基于用户定义的PII策略简表的PII保护基本结构。

使用基于标签的识别技术的商家对客户（B2C）应用可分为三类：

a) *设备用户作为客户*：在提供信息内容的服务中，客户利用其拥有的读取设备来检索信息。在这种类型设备中，大多数应用服务提供商可以假定客户拥有一个配备了读取设备的移动终端。图44显示了这种类型应用的基本模型。它由两个基本的网络操作组成：ID解析和内容检索。ID解析是将一个标识符转换或解析为一个地址的过程。配备了读取设备的移动终端首先解析经号码簿服务从ID标签收到的标识符，然后执行内容检索操作。

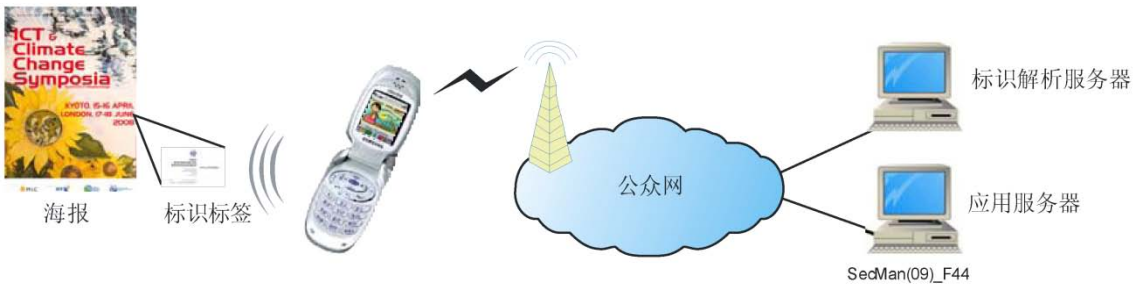


图 44 – 利用基于标签的认证的B2C应用基本模型

b) *ID标签用户作为客户*：这种使用基于标签的识别技术的B2C应用的一个典型例子涉及访问控制和/或认证，如入口检查、护照、证书或售后管理服务。在这种类型应用中，读取设备可以是固定型的终端和/或移动型的终端。客户可能不需要其自身的读取设备。

c) *客户既可以作为ID标签用户，也可以作为设备用户*：在产品信息检索服务中，在用其移动终端浏览产品信息内容并购买带标签的产品后，客户也变成为一个标签用户。在另一个例子中，可以考虑通过一张具有标签功能的病人卡来激活与医疗保健有关的服务。在这种应用中，有许多种客户，他们可以是ID标签用户（如病人、医生、护士）。ID标签用户可以通过配备了读取设备的移动终端读取其具有ID功能的病人卡，来浏览其自身的病历。

对使用基于标签的识别技术的B2C应用，存在两种主要的侵犯PII的风险：

- 泄露与标识符有关的信息：在这种情况下，攻击者从ID标签中读取信息，但不了解带标签产品的用户情况。攻击者首先从用户携带的ID标签中读取一个标识符，然后对标识符进行解析，并从号码簿服务中查询信息位置，最后攻击者请求与ID标签有关的信息。
- 泄露历史数据：攻击者可以从与ID标签有关的历史数据中提取用户的数据（如爱好、习惯、感兴趣的领域等）。攻击者可以不经用户同意就将此类数据用于非法或商业目的。

ITU-T X.1171建议书描述了以下技术要求，用于防止在B2C应用中对PII的侵犯：

- *由ID标签用户来控制PII*：要求ID标签用户能够管理或更新与其网络上ID标签有关的PII。通过这种方式，ID标签用户可以确定应删除或保留应用中的哪个PII。
- *对ID标签用户和/或设备用户进行认证*：要求应用服务器为ID标签用户提供一个认证程序，如果需要（一些使用基于标签的识别技术的应用不需要对用户进行认证），应用服务器可以为设备用户提供一个认证程序。
- *对应用服务器中ID标签用户的PII实施访问控制*：要求应用服务器对与ID标签用户PII有关的相关信息实施访问控制。
- *ID标签相关信息的数据机密性*：要求应用服务器规定数据机密性，以确保未经授权的用户无法读取与ID标签有关的信息。
- *同意收集与设备用户有关的日志数据*：如果应用需要收集这种类型的日志数据，那么应用服务器可以提供一个批准程序，用于收集与设备用户有关的日志数据。

下面的例子说明了基于用户PII策略简表的PII保护服务（PPS）。PPS的服务情形通常源自标签个性化的程序，如购买带标签的产品。图45显示了在使用基于标签的识别技术的应用中的通用PPS服务流程。

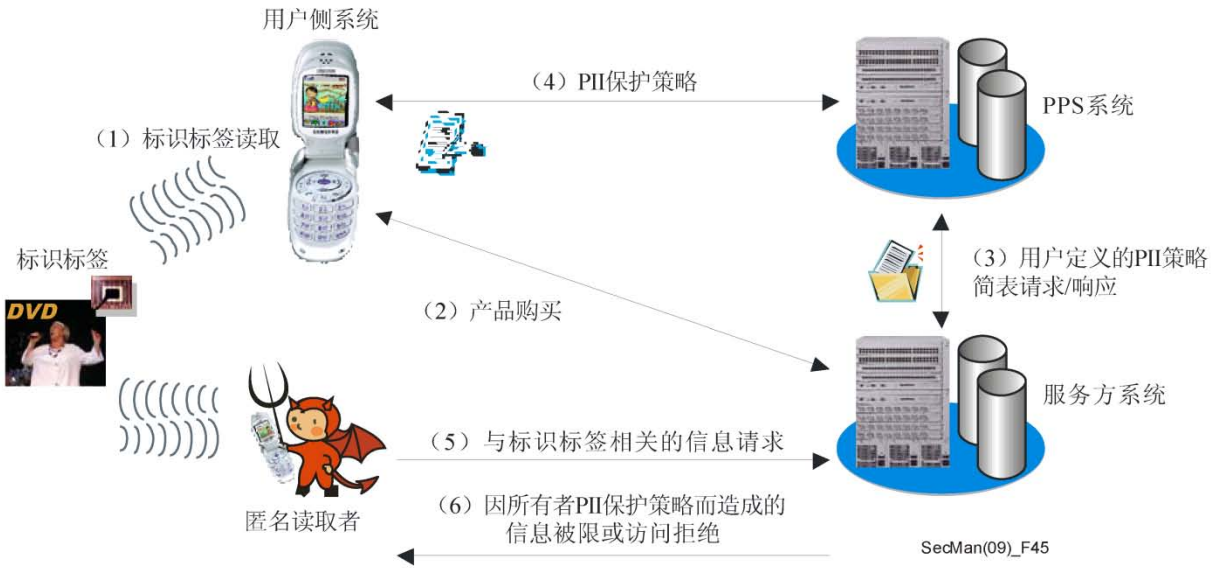


图 45 – 通用PII保护服务（PPS）业务流程

1) 消费者利用其配有阅读器的移动终端读取来自带有标签的产品的标识符。
2) 消费者浏览来自应用服务网络的产品相关信息，然后利用各种各样支付方式中的一种方式来购买产品。此时，消费者变成了标识标签的用户。
3) 然后使用基于标签的标识的应用向PPS系统请求用户定义的PII策略简表，它向应用回应用户定义的PII简表。
4) PPS系统接收有关该应用的用户PII保护策略。
5) 任何人都可以向服务方系统请求与该标识标签相关的信息。
6) 如果请求者为标识标签的用户，那么请求者可以浏览服务方系统提供的所有信息。否则，请求者要么不能访问任何信息，要么只能获得有限信息。

10. 应对常见的网络威胁

10 应对常见的网络威胁

计算机系统和网络面临诸多威胁。尽管许多攻击可以在本地发起，但目前大多数攻击是通过通信网络来实施的。有越来越多的计算机和网络设备连至互联网，并由几乎没有经过多少培训、很少意识到或不了解信息技术安全的人员在家中和工作场所操作着，这一事实极大地提高了远程、频繁、任意攻击的便捷性和可能性。公布的垃圾邮件、间谍软件、病毒和其他攻击形式越来越多。攻击者常常将脆弱的、未经适当保护的系统作为其恶意行为的通道。

本节概述了ITU-T为应对这些威胁中的一些威胁而做的工作。

10.1 应对垃圾邮件

垃圾邮件（即未经要求的、多余的电子邮件）被广泛认为是网络用户和网络与服务提供商面临的一大问题。垃圾邮件干扰合法的操作、耗费带宽和处理周期，在极端情况下，通过向网络“注水”可造成拒绝服务攻击。目前，既用法律措施也用技术措施来应对垃圾邮件，但不同措施的有效性各不相同。没有一种单一的反垃圾邮件措施是有效的，考虑到垃圾邮件发送者的灵活性和足智多谋，几种垃圾邮件应对措施的结合常常证明只能减少垃圾邮件的数量。目前使用的垃圾邮件应对措施的例子包括：规则；技术措施，包括垃圾邮件过滤、国际合作；以及对用户和互联网服务提供商的培训。

ITU-T有关应对垃圾邮件的工作主要集中于技术方面的问题，因此，在本节中，我们主要关注应对垃圾邮件的技术手段，以及反垃圾邮件技术的开发和应用。

10.1.1 应对垃圾邮件的技术策略

ITU X.1231建议书《应对垃圾邮件的技术策略》阐述了与垃圾邮件做斗争的要求，作为工作的一个起点。该建议书描述了不同类型的垃圾邮件及其共性，并概述了应对垃圾邮件的不同技术方法。它还提出了一种通用模型，可用之来制定有效的反垃圾邮件策略。

这是一种层次型的模型，有五种策略，分布在三个层面上。图46显示了不同策略之间的关系。模型表明不同策略之间具有很高的独立性，但费用方面的考虑可能会排除在一种单一情况中使用所有的策略。此外，需要依据特定的应用情形来定制具体的策略。

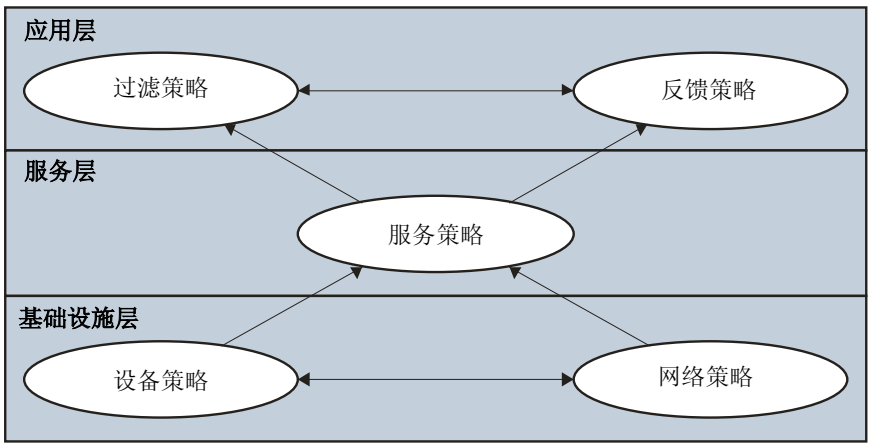


图 46 – 应对垃圾邮件的通用模型

10.1.2 垃圾电子邮件

垃圾电子邮件是最被广泛认可的垃圾邮件形式。它提出了复杂的技术挑战，减少垃圾邮件的解决方案需要得到适当的技术措施的支持。政府的行动和立法是有帮助的，但相对垃圾电子邮件提出的挑战而言，它们是不够的。当使用SMTP协议时，很难确定垃圾邮件的发送者，这给问题的解决带来了困难。

提出了两个旨在帮助应对垃圾电子邮件的建议书。ITU-T X.1240建议书《应对垃圾电子邮件涉及的技术》直接面向想开发技术解决方案以应对垃圾电子邮件的用户。它规定了基本概念、特性、效果以及与应对垃圾电子邮件有关的技术问题。它还确定了当前的技术解决方案以及来自标准制定组织和其他致力于应对垃圾电子邮件的团体的相关活动。

ITU-T X.1241建议书《应对垃圾电子邮件的技术框架》建议了一种用于反垃圾邮件处理域的结构，并定义了域中主要模块的功能。框架建立了一种在不同的电子邮件服务器之间共享有关垃圾电子邮件信息的机制。其目标是推动各服务提供商之间在应对垃圾邮件方面开展更多的合作。具体而言，它提供了一种框架，使通信方法能对确定的垃圾邮件发出告警。另一个文件《ITU-T X.1240系列 — 有关应对垃圾邮件和相关威胁的增补》对有关的国际论坛做了评论，在这些论坛上，对垃圾邮件问题进行了论述，并对一个案例进行了分析。

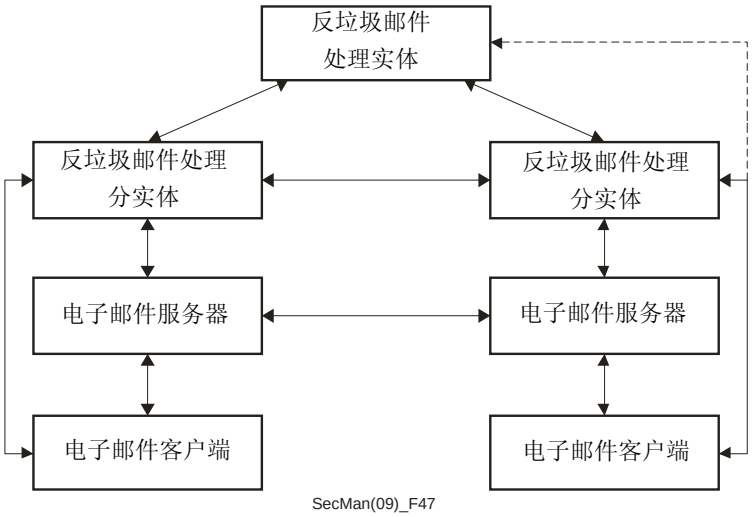


图 47 – 反垃圾电子邮件处理域的通用结构

图47描述了ITU-T X.1241框架的各个过程。反垃圾邮件处理实体位于一个独立的系统中，而各反垃圾邮件处理分实体则位于一个或多个电子邮件服务提供商处。处理实体负责将新的规则传送给各分实体，各分实体必须对这些规则进行验证和细化。还有一种功能，它负责解决规则中存在的任何冲突。

10.1.3 IP多媒体垃圾邮件

ITU-T X.1244建议书《在基于IP的多媒体应用中应对垃圾邮件的方方面面问题》规定了基本概念、特性以及与应对IP多媒体应用（如IP电话和即时消息）中垃圾邮件有关的技术问题。对各种不同类型的IP多媒体应用垃圾邮件进行了分类，依据其特性进行了描述。标准描述了各种各样可引起IP多媒体应用垃圾邮件的垃圾邮件安全威胁，并确定了在应对此类垃圾邮件过程中应引起注意的各种问题。为控制垃圾电子邮件而开发的某些技术也可用于应对IP多媒体应用垃圾邮件。ITU-T X.1244建议书分析了传统的垃圾邮件应对机制，并讨论了其对应对IP多媒体应用垃圾邮件的适用性。

可依据垃圾邮件具体的特性来对IP多媒体垃圾邮件应用反垃圾邮件技术。表7显示了ITU-T X.1244建议书中所用的分类情况。

表 7 – IP多媒体应用垃圾邮件分类

	文本	语音	视频
实时	• 即时消息垃圾邮件按 • 聊天垃圾邮件	• VoIP垃圾邮件 • 即时消息垃圾邮件	• 即时消息垃圾邮件
非实时	• 文本/多媒体消息垃圾邮件 • 通过P2P文件共享服务提供的文本垃圾邮件 • 网站文本垃圾邮件	• 语音/多媒体消息垃圾邮件 • 通过P2P文件共享服务提供的语音垃圾邮件 • 网站语音垃圾邮件	• 视频/多媒体消息垃圾邮件 • 通过P2P文件共享服务提供的视频垃圾邮件 • 网站视频垃圾邮件

10.1.4 短信服务（SMS）垃圾邮件

ITU-T X.1242建议书《基于用户指定规则的短消息业务（SMA）垃圾过滤系统》定义了SMS垃圾邮件过滤系统的结构和功能，以及用户服务管理、通信协议和带SMS功能的终端的基本功能要求。定义了用户可用于管理（查询、删除和储存）经过过滤之短信的方法。可以依据特性来过滤，如地址、电话号码、时间或内容。在ITU-T X.1242建议书的一个附录中提供了支持SMS垃圾邮件过滤的终端软件要求。

10.2 恶意代码、间谍软件和欺骗软件

系统和网络面临巨大的、来自恶意代码（病毒、蠕虫、特洛伊木马）的风险，也面临巨大的、来自其他欺骗软件（即执行未经授权行为的软件）的风险。除非组织和个人采取一系列积极主动的措施（包括防火墙、反病毒措施和反间谍软件）来应对这些威胁，否在“在劫难逃”。不过，可用的应对措施在效能方面存在差异，并且并不总是互补的。

许多国家的监管者越来越多地要求服务提供商在其采取的安全保密措施方面做出承诺，要求服务提供商采取更多措施来帮助用户实现安全可靠的互联网应用。

ITU-T X.1207建议书《电信服务提供商应对间谍软件及潜在有害软件风险的指导原则》是一个用于以下目的的标准：

a) 宣传推广有关万维网宿主服务明确通知、用户准许和用户控制的最佳做法；以及

b) 向家庭用户宣传推广有关安全可靠使用个人计算机和互联网的安全最佳做法（通过电信服务提供商）。

ITU-T X.1207建议书为服务提供商提供了明确的、有关安全风险管理、安全保密产品使用、网络监控和响应、支持、及时更新以及保证万维网宿主安全的指导原则。为最终用户提供了有关用户指导和培训以及技术保护措施的建议。一个非建议书整体构成所必需的附录提供了对额外资源材料的链接。

10.3 软件更新的通告和发布

恶意代码可以以惊人的速度传播，甚至在拥有先进保护措施的情况下，新的威胁也可快速传播，造成未进行最新更新的系统和网络也显得非常脆弱。对“零日”威胁（即新的或之前未知的威胁，对这些威胁尚未开发任何反病毒签名或补丁程序），系统尤其显得脆弱。在这种情况下，及时发布和安装更新程序至关重要。不过，存在许多与发布和执行这些更新程序有关的问题。

大多数成熟的软件，包括操作系统和旨在提供安全保护（反病毒）的系统，包含一个允许自动更新的特征。不过，必须由用户来激活该特征。当只是简单通知用户更新程序可用（或者更新程序可能已经下载）时，用户必须采取行动允许下载和/或安装这些更新程序。许多更新程序要求系统在安装后重新启动；而对一些更新程序，用户可以立即重新启动，也可以不立即重新启动。对安全计划得以良好管理的组织而言，通常对更新采取集中管理，在最终用户系统中进行更新。相反地，单个系统（如家庭计算机）的更新以及小型组织内的更新通常非常随意。

与日常更新有关的另一个问题是软件供货商不采取一致的做法来通知用户更新程序已经可用，或者不告诉用户更新程序安装故障可能产生的后果。它们也没有一种统一的方法来告知用户最新的、用于维护软件安全的最佳做法。另外，也没有一种一致的方法来通告用户在执行更新后发现的问题。

ITU-T X.1206建议书《关于安全信息自动通告和更新发布的厂商中立框架》论述了与维护最新软件有关的各种困难，并提供了一种与供货商无关的问题解决方法。一旦注册了某项资产，那么有关弱点的最新消息以及补丁程序或更新程序可自动提供给用户或者直接提供给应用。ITU-T X.1206建议书提供了一个框架，任何供货商都可以使用该框架来通告并提供弱点信息，以及发布所需的补丁程序/更新程序。它还定义了在各组成部件中以及不同组成部件间使用的信息格式。

ITU-T X.1206建议书使系统管理员有可能知晓其所负责的任何资产的情况。它从资产识别、信息分发以及系统/网络管理角度，描述了资产维护问题。还对应在供货商无关的框架中予以考虑的安全问题进行了描述。

ITU-T X.1206建议书定义了此项工作所需的各组成部件的数据结构，包括有关的XML纲要，并定义了在实施该框架的各组成部件中以及不同组成部件间使用的信息格式。

11. 信息通信技术安全标准化的未来发展方向

11 信息通信技术安全标准化的未来发展方向

三十多年来，ITU-T一直从事信息通信技术标准的制定工作。随着互联网和其他网络使用的快速发展，以及认识到需要为用户和系统提供保护，以应对数量和种类都在不断增加的安全威胁，近年来，这项工作的步伐大大加快。

本手册综述了各ITU-T研究组所提的一些关键的安全相关举措以及它所取得的成就，以便更好地理解这项工作以及网络用户和实施者所面临的日益严峻的技术问题。希望读者利用ITU-T广泛的在线资源来获得本手册所述各主题的更详细信息，并使用这些建议书和指导文件来帮助构建一个更加安全的在线环境，增强用户对在线业务的信心。

展望未来，电信网络和计算机网络将进一步融合。下一代网络和基于万维网的服务将继续快速增长，并将变得越来越重要，但威胁也将继续演变，将继续是一个需要面对的挑战，需要设计和开发出有效的解决措施来应对这些威胁。设计和造就更好、更安全的系统和网络是一个巨大的挑战，只有这样才能减少内在的弱点。

国际电联的191个成员国和551个部门成员将继续勇敢面对这些挑战，在各成员需求的推动下，在2008年世界电信标准化全会建立的组织机构指导下，将继续积极主动地提出各种有关安全的技术建议书和指导原则。只要有可能，为了最大限度地减少重复劳动并集中资源，ITU-T将与其他标准化制定组织开展合作，以便尽可能高效、快速地达成协调一致的解决方案。

12. 额外信息源

12 额外信息源

本手册对ITU-T的安全工作一并做了综述。可在ITU-T的网站上免费获取更加详细的信息，包括诸多标准。

12.1 第17研究组工作概述

作为第一步，在第17研究组的主页上提供了对第17研究组工作信息的链接，包括各种辅导材料和陈述材料，对目前正在制定的各建议书以及关键人员做了概述。对有关电信安全的牵头研究组和有关身份管理（IdM）的牵头研究组的链接提供了这两个牵头研究组的活动信息和工作结果。

12.2 安全概览

汇编包含关于国际电联各建议书的信息、相关的信息以及国际电联安全活动的信息。它由五部分组成，每部分都是可下载的：

- 与电信安全有关的已批准建议书的书目，包括那些为安全目的而设计的建议书，以及那些描述或使用安全功能和需求的建议书；
- 摘自已批准ITU-T建议书的ITU-T已批准安全定义列表；
- 开展安全相关活动的ITU-T各研究组概述；
- ITU-T各研究组内正在审议的涉及安全问题的建议书概述；
- 国际电联其他的安全活动概述。

12.3 安全标准路线图

安全标准路线图是一种在线资源，它提供了有关在各关键标准制定组织中现有的信息通信技术安全标准和正在开展的工作的信息。除了有关ITU-T安全工作的信息，路线图还包括有关ISO/IEC、ATIS、ENISA、ETSI、IEEE、IETF、OASIS、3GPP和3GPP2安全标准工作的信息。

如同汇编，路线图由五部分组成，大多数信息可直接从网上获得：

- 第1部分，信息通信技术标准制定组织及其工作：包含有关路线图结构以及各所列之标准组织的信息，第1部分还提供了对现有安全术语和词汇的链接；
- 第2部分，已批准的信息通信技术安全标准：包含一个可查询的、有关已批准安全标准的数据库，对大多数标准有直接的链接；
- 第3部分，正在制定的安全标准；
- 第4部分，未来需求与提议的新的安全标准；以及
- 第5部分：安全最佳做法。

12.4 安全实施指导原则

ITU-T X.800-X.849系列建议书增补3《系统和网络安全实施指导原则增补》提供了更加详细的、有关本手册中所讨论的一些主题的背景知识，并提供了系统和网络安全实施指导原则，利用这些指导原则可以实现网络安全计划。这些指导原则涉及四个领域：技术安全策略；资产鉴别；威胁、弱点和缓解；安全评估。这些指导原则指明了构建和管理技术策略所需的关键部件，需要利用这些技术策略来管理各个网络，潜在地，这些网络跨接多个运营商，并包含来自多个供货商的各种产品和系统。它还提供了有关监管问题的指导原则。

12.5 有关号码簿、认证和身份管理的额外信息

ITU-T X.500系列建议书本身就是经过授权的信息源，可由此获得关于ITU-T X.500系列建议书的很多信息。额外的辅导信息以及实施者指南可以在以下网址找到：www.x500standard.com。以下各链接包含额外的信息：

http：//www.x500standard.com/index.php?n=X509.X509ProtectingDirectory：包含有关用户认证的信息；

http：//www.x500standard.com/index.php?n=X500.AccessControl：提供了更多的、有关访问控制的信息；以及

http：//www.x500standard.com/index.php?n=X500.DataPrivacyProtection：提供了更广泛的、有关X.500 数据保密特征的描述。

附件 A – 安全定义

附件A
安全定义

下表包含了在本手册中所使用术语的定义，所有的定义都包含在当前的ITU-T建议书中。更完整的安全定义清单包含在《ITU-T批准的安全定义汇编》中，它们摘自ITU-T各建议书，由第17研究组负责维护。

术语	定义	参考文献
access control 访问控制	1. 防止对一个资源的非授权使用，包括防止以非授权的方式使用资源。 2 限制来自一个系统资源的信息流只流向授权的个人、程序、进程或网络上的其他系统资源。	X.800 J.170
access control list 访问控制列表	实体列表及其访问权限，授予了访问资源的权限。	X.800
access control policy 访问控制策略	定义访问条件的规则集。	X.812
accidental threats 偶然的威胁	没有预先意图的威胁。实际的偶然威胁例子包括系统故障、操作出错和软件缺陷。	X.800
accountability 问责制	确保能够唯一认定一个实体的动作确为该实体所为的性能。	X.800
algorithm 算法	一个数学过程，可用于扰乱和理清数据流。	J.93
attack 攻击	为绕过一个系统的安全机制或利用其漏洞而采取的行动。对一个系统的直接攻击利用的是安全机制基础算法、原理或性能的不足。实施间接攻击通常是绕过安全机制或是使系统不正确地使用安全机制。	H.235
attribute 属性	报文处理范畴内的一个信息项、属性列表的一个组成部分，用于描述用户或分发列表，也可依据报文处理系统（或基础网络）的物理或组织结构对其进行定位。	X.400
attribute authority（AA） 属性机构（AA）	1. 通过发布属性证书指派特权的机构。 2. 被一个或多个实体所信任的实体，它负责建立和签署属性证书。注 – CA也可以是一个AA。	X.509 X.842
attribute certificate 属性证书	一种数据结构，由属性机构以数字形式签署，通过证书拥有者的标识信息来绑定某些属性值。	X.509
authentication 认证	1. 确认身份的过程。注 – 见“主体”和“验证者”，以及两种不同形式的认证（数据源认证+实体认证）。认证可以是单边的，或者是双边的。单边认证只对一个主体提供身份保证。双边认证为两个主体提供身份保证。	X.811

术语	定义	参考文献
authentication 认证	2. 向一个实体所声明的身份提供保证。 3. 见“数据源认证”和“对等实体认证”。术语“认证”的使用与数据的完整性无直接关联；术语“数据完整性”可以替代使用。 4. 确认与关联建立有关的对象的身份。例如，可包括AE、AP，以及应用的用户。注 – 定义该术语旨在表明目前的认证范围比CCITT X.800建议书中对等实体认证所覆盖的范围要宽。 5. 验证一个实体向另一个实体所声明身份的程序。 6. 旨在允许系统确认某方身份的过程。	X.811 X.800 X.217 J.170 J.93
authentication exchange 认证交换	1. 通过信息交换方式来确保实体身份的一种机制。 2. 出于认证目的，一次或多次传送交换认证信息的序列。	X.800 X.811
authentication service 认证服务	认证服务用于证明对象的身份确实是其所声明的身份。依据执行者类型和鉴定目的，可能需要以下类型的认证：用户认证、对等实体认证、数据源认证。用于实施认证服务的机制的例子包括口令和个人身份号码（PIN）（简单认证），以及基于密码的方法（强认证）。	M.3016.2
authority 机构	负责核发证书的实体。定义了两种类型：用于发布公开密钥证书的认证机构和用于发布属性证书的属性机构。	X.509
authorization 授权	1. 授予权利，包括依据访问权利授予访问。注 – 该定义意味着能够执行某些行为的权利（如访问数据），它们授给某个进程、实体或代理人。 2. 依据经认证的身份授予许可权。 3. 使被允许访问者有权使用某个服务或设备的动作。	X.800 H.235 J.170
availability 可用性	能够根据授权实体的要求进行访问和使用的特性。	X.800
capability 能力	用做某个资源标识符的一种标记，拥有该标记表明拥有该资源的访问权利。	X.800
certificate 证书	由安全机构或可信的第三方核发的一套与安全相关的数据，与安全信息一同用于提供数据完整性和数据源认证服务（安全证书 – ITU-T X.810）。该术语指的是“公开密钥”证书，它们是一组数值，表示一个所有者的公开密钥（及其他可选信息）是经过可信的机构以不可伪造的格式验证并签署过的。	H.235
certificate policy 证书策略	一套指定的规则，用于指明一个证书对于具有通用安全要求的某个特定团体和/或应用类别的适用性。例如，一个特定的证书策略可以指明在给定的价格范围内货物贸易中某种类型证书对电子数据交换交易认证的适用性。	X.509
Certificate Revocation List（CRL） 证书撤销列表（CRL）	1. 表明一套证书不再被证书核发者认为有效的签署列表。除了通用术语CRL之外，还为CRL定义了一些涵盖特定领域的特殊CRL类型。 2. 一个CRL包括已撤销各证书的序列号（例如，由于密钥已经受损或由于对象不再属于公司），其有效期尚未到期。	X.509 Q.817
Certification Authority（CA） 认证机构（CA）	1. 得到一个或多个用户信任的机构，创建并指配公开密钥证书。作为一种选择，认证机构可以创建用户密钥。 2. 可信的实体（在安全策略的范畴内），创建包含一个或多个安全相关数据类别的安全证书。	X.509 X.810
ciphertext 密文	经加密生成的数据。使结果数据的语义内容不可知晓。注 – 密文本身也可用做加密操作的输入，这样就可以生成超级加密的输出。	X.800

术语	定义	参考文献
cleartext 明文	可理解的数据，其语义内容可以知晓。	X.800
confidentiality 机密性	防止信息提供或泄露给未经授权的个人、实体或过程的特性。	X.800
confidentiality service 机密性服务	机密性服务提供了防止交换数据非授权透露的保护措施。有以下不同种类的机密性服务：选择性字段机密性、连接机密性、数据流机密性。	M.3016.2
credentials 证明	传送并用于建立实体所需身份的数据。	X.800
cryptanalysis 密码分析	1. 为了到秘密变量和/或包括明文在内的敏感数据，对一个密码系统和/或它的输入和输出进行的分析。 2. 在无权使用密钥的情况下恢复报文明文或加密密钥的过程。 3. 在无权使用密钥（电子密码系统中的电子密钥）的情况下恢复报文明文的学科。	X.800 J.170 J.93
cryptographic algorithm 密码算法	从一个或几个输入值计算结果的数学函数。	H.235
cryptographic system， cryptosystem 密码系统	1. 密码系统是明文和密文进行相互转换的集合，将要使用的特定变换是由密钥选择的。通常用一种数学算法来定义变换。 2. 简单地说，密码系统是一个算法，它可将输入数据转换为某种不可识别的形式（加密），并可将不可识别的数据转换回其初始形式（解密）。RSA加密技术在ITU-T X.509中描述。	X.509 Q.815
cryptography 密码学	为隐藏信息内容、防止它受到未被发现的更改和/或防止非授权的使用而综合了数据转换原理、手段和方法的学科。注 － 密码学决定了加密和解密的使用方法。密码分析学是对密码学原理、手段和方法的攻击。	X.800
data confidentiality 数据机密性	该服务可用于保护数据不被未经授权的泄露。认证框架支持数据机密性服务。该服务可用于防止数据被窃听。	X.509
data integrity 数据完整性	数据没有遭到未经授权的改变或破坏的特性。	X.800
data origin authentication 数据源认证	1. 确认所接收的数据源与所声称的相同。 2. 确认主体的身份负责特定的数据单元。	X.800 X.811
decipherment 解密	相应的可逆加密的逆过程。	X.800
decryption 解密	见“decipherment 解密”。	X.800
delegation 授权	把特权从一个拥有特权的实体转让给另一个实体。	X.509
denial of service 拒绝服务	阻止经授权的资源访问或是延误紧急操作。	X.800
digital signature 数字签名	1. 数据单元的附加数据或数据单元的一种密码转换（见“cryptography 密码学”），使数据接收方能够证明数据源和数据完整性，并防止伪造，例如接收方的伪造。 2. 数据单元的一种密码转换，使数据接收方能够证明数据源和数据完整性，并保护数据单元的发送方和接收方免遭第三方伪造，以及保护发送方免遭接收方的伪造。	X.800 X.843
directory service 号码簿服务	从良好定义的对象目录中搜索和查找信息的一种服务，它可以包含有关证书、电话号码、访问条件、地址等的信息。依据 ITU-T X.500，号码簿服务提供了一个例子。	X.843

术语	定义	参考文献
eavesdropping 窃听	通过监控通信来突破机密性。	M.3016.0
encipherment 加密	1. 对数据进行密码转换（见“cryptography 密码学”）以生成密文。注－加密可能是不可逆的，在这种情况下，无法进行相应的解密操作。 2. 加密是通过实施某种密码算法（加密算法）使数据对于未经授权的实体不可读的过程。解密是加密的逆操作，通过它使密文转化为明文。	X.800 H.235
encryption 加密	1. 将明文信息转换为密文的一种方法。 2. 将信号扰乱的过程，以免遭到未经授权的访问。 （见“encipherment加密”。）	J.170 J.93
end-to-end encipherment 端对端加密	数据在起始端系统加密，相应的解密只发生在目的端系统。	X.800
entity 实体	1. 一个人、一个组织、一个硬件部件或软件的一部分。 2. 任何感兴趣的、具体的或抽象的事情。通常，实体可用于指代任何事情，在建模范畴中，它指的是被建模的事物。	X.842 X.902
entity authentication 实体认证	确认主体的身份，在通信关系范畴内。注 － 主体经认证的身份只有当调用该服务时才能得到保证。通过 ITU-T X.811 第 5.2.7 节中所述的方法可以确保认证的连续性。	X.811
evidence 证据	信息，其自身或当与其他信息一起使用时，可用于解决争议。注 － 证据的特定形式可以是数字签名、安全封装和安全标记。数字签名与公开密钥技术一起使用，安全封装和安全标记与秘密密钥技术一起使用。	X.813
forgery 伪造	一个实体，它伪造信息，并声称这些信息收自另一个实体或发往另一个实体。	M.3016.0
hash function 散列函数	一个将数值从较大（可能非常大）的数值集合映射到一个较小的数值集合的（数学）函数。	X.810
indirect attack 间接攻击	对系统的一种攻击，它不基于特定安全机制的缺陷（如绕过安全机制的攻击，或依赖于系统不正确使用安全机制的攻击）。	X.814
integrity 完整性	数据没有以未经授权的方式加以改变的特性。 （见“data integrity 数据完整性”。）	H.235
integrity service 完整性服务	完整性服务提供了确保所交换数据正确性的手段，使之免遭修改、删除、创建（插入）和重播已交换数据。有以下不同种类的完整性服务：选择性字段完整性服务、不带恢复的连接完整性服务、带恢复的连接完整性服务。	M.3016.2
intentional threats 故意的威胁	指的是从利用可方便得到的监控工具所进行的不经意检查到利用专业系统知识所进行的刻意攻击的威胁。故意的威胁如果得以实现，那么可以认为是“攻击”。	X.800
IPCablecom	ITU-T 的一个项目，包括一个体系结构和一系列建议书，使得能够利用电缆调制解调器经由有线电视网络来提供实时服务。	J.160
Kerberos	一个秘密密钥网络认证协议，选择使用密码算法进行加密和中央密码数据库进行认证。	J.170
key 密钥	1. 控制加密/解密操作的符号序列。 2. 作为被选密码算法输入的数学值。	X.800 J.170
key exchange 密钥交换	用于实体之间加密通信的、实体之间公开密钥的交换。	J.170
key management 密钥管理	依照某种安全策略，生成、存储、分发、删除、存档和应用密钥。	X.800
man-in-the-middle attack 中间人攻击	一种攻击方式，在这种攻击方式中，攻击者能够随意读取、插入和修改通信双方之间的报文，而任何一方都不知道它们之间的链路已遭侵害。	X.1151

术语	定义	参考文献
masquerade 冒名顶替	一个实体伪装成为另一个不同的实体。	X.800
mutual authentication 相互认证	确认两个主体的身份。	X.811
non-repudiation 不可抵赖	1. 防止发送方事后否认其曾发送过某个信息或采取过某个行动的能力。 2. 防止参与通信的若干实体中的一个否认参与过全部或部分通信。 3. 一个过程，利用它，报文的发送方（如一个有关按次计费的请求）不可否认已发送过报文。	J.170 H.235 J.93
notarization 公证	向可信的第三方注册数据，允许之后确保其特性的准确性，如内容、来源、时间和提交。	X.800
passive threat 被动威胁	在不改变系统状态情况下出现的、未经授权的信息泄露威胁。	X.800
password 口令	1. 机密认证信息，通常由字符串组成。 2. 指的是用户进入口令字符串，即指定的安全密钥，为移动用户和其归属域所共享。该用户口令和产生的用户共享秘密将用于用户认证之目的。	X.800 H.530
physical security 物理安全	为防止资源受到故意或偶然威胁而使用的物理保护措施。	X.800
principal 主体	一个实体，其身份可被认证。	X.811
privacy 保密	1. 个人控制或影响可以收集和存储的、与其相关的信息的权利，并且该个人可能泄露该信息或该信息可能泄露给该个人。注 — 因为该术语与个人权利相关，所以它不可能非常精确，除非作为需要安全的动机，否则应避免使用它。 2. 只有明确激活的各方才能解译的一种通信方式，通常通过加密和共享加密密钥来实现。	X.800 H.235
private key 专用密钥	1. （在公开密钥密码系统中）用户密钥对的密钥，只有该用户知晓之。 2. 非对称密码算法中使用的密钥，其所有权受限（通常只属于一个实体）。 3. 在公开密钥密码系统中使用的密钥，它属于某个单个实体，必须保密。	X.509 X.810 J.170
privilege 特权	由某个机构指派给实体的属性或特性。	X.509
Privilege Management Infrastructure（PMI） 特权管理基础设施（PMI）	能够支持特权管理的基础设施，它支持全面的授权服务，并与公开密钥基础设施相关。	X.509
public key 公开密钥	1. （在公开密钥密码系统中）用户密钥对中公开的密钥。 2. 非对称密码算法中所用的密钥，它可以公开。 3. 公开密钥密码学中所用的密钥，它属于一个单独实体，并公开发布。其他实体使用该密钥来对发往密钥所有者的数据进行加密。	X.509 X.810 J.170
public key certificate 公开密钥证书	1. 用户的公开密钥，以及其他一些信息，利用发放它的认证机构的专用密钥进行加密，不可伪造地进行提交。 2. 代表所有者公开密钥（和其他可选信息）的值，由可信的机构以一种不可伪造的方式进行确认和签署。 3. 实体的公开密钥与一项或多项与其身份有关的属性之间的绑定，也称为数字证书。	X.509 H.235 J.170

术语	定义	参考文献
Public Key Cryptography 公开密钥密码学	基于两个密钥算法（专用的和公开的）的加密技术，在该技术中，利用公开密钥对报文进行加密，但只能利用专用密钥才能对报文进行解密。也就是所知的专用－公开密钥（PPK）系统。注 － 知道公开密钥并不能揭露专用密钥。例如，A 方设计这样一个专用密钥和公开密钥，并公开地将公开密钥传送给所有想与 A 方通信的人，但保守专用密钥的秘密。而后，任何拥有公开密钥的人都可以对发往 A 方的报文进行加密，但只有拥有专用密钥的 A 方才可以对报文进行解密。	J.93
Public Key Infrastructure（PKI） 公开密钥基础设施（PKI）	能够支持公开密钥管理的基础设施，它支持认证、加密、完整性或不可抵赖服务。	X.509
relying party 依赖方	在做决定时依赖证书中数据的用户或代理。	X.509
replay 重播	重复某个报文或报文的一部分，以产生未经授权的效果。例如，可以由另一个实体来重播包含认证信息的合法报文，以便认证它（是某某，而实际上它不是某某）。	X.800
repudiation 抵赖	1. 参与通信的一个实体否认曾参与过全部或部分通信。 2. 参与过通信交换的一个实体随后否认该事实。 3. （在MHS情况下）MTS用户或MTS可能在之后否认提交、接收或发送过报文，并且包括：拒绝发送、拒绝提交、拒绝传输。	X.800 M.3016.0 X.402
revocation list certificate 撤销列表证书	确定安全证书列表已被撤销的安全证书。	X.810
secret key 秘密密钥	对称密码算法所用的密钥。秘密密钥的所有权是有限的（通常限于两个实体）。	X.810
security 安全	术语“安全”用于表示最大限度地减少资产和资源的弱点。资产指的是任何有价值的事物。弱点指的是任何可被用于侵犯系统或其所含信息的薄弱之处。威胁指的是对安全构成的潜在侵犯。	X.800
security alarm 安全告警	当检测到安全相关事件（安全策略将之定义为告警条件）时产生的报文。安全告警旨在适时地引起适当实体的注意。	X.816
security audit 安全审计	对系统记录和行为的独立评估和检查，目的是测试系统控制的合适性，确保符合已有的策略和操作程序，检测安全缺口，并对这些控制、策略和程序提出修改建议。	X.800
security audit trail 安全审计跟踪	为便于进行安全审计而收集并可能使用的数据。	X.800
security certificate 安全证书	由安全机构或可信第三方发布的一套与安全相关的数据，与安全信息一起用于提供数据完整性和数据源认证服务。注 － 所有的证书都被认为是安全证书。ITU-T X.800 系列中采用术语“安全证书”是为了避免与 ITU-T X.509 产生术语冲突。	X.810
security domain 安全域	1. 服从通用安全策略的用户和系统集。 2. 服从单个安全策略的资源集。	X.841 X.411
security information（SI） 安全信息	执行安全服务所需的信息。	X.810
security management 安全管理	安全管理，包括用于建立、维护和终止系统安全方面问题的所有行为。覆盖的主题包括：安全服务的管理、安全机制的安装、密钥管理（管理部分）、身份建立、密钥、访问控制信息等；安全审计跟踪和安全告警管理。	M.3016.0

术语	定义	参考文献
security model 安全模型	一个用于描述安全服务（用于抵御对 MTS 的潜在威胁）和安全要素（用于支持这些服务）的框架。	X.402
security policy 安全策略	1. 掌管安全服务和设施使用和供应的安全机构所设定的一套规则。 2. 提供安全服务的一套标准。注 – 见“基于身份的安全策略”和“基于规则的安全策略”。完整的安全策略有必要解决OSI 范围之外的许多问题。	X.509 X.800
security service 安全服务	由正在通信的开放系统的某一层所提供的服务，确保系统或数据传输有足够的安全性。	X.800
security threat (threat) 安全威胁（威胁）	潜在的安全侵犯。	X.800
security token 安全标记	受一个或多个安全服务保护的、在通信实体之间传送的一组数据，与安全信息一起用于提供这些安全服务。	X.810
sensitivity 灵敏度	表明资源价值或重要性的特性。	X.509
shared secret 共享秘密	指密码算法使用的安全密钥，可能源自口令。	H.530
signature 签名	见“digital signature 数字签名”。	X.800
simple authentication 简单认证	通过简单的口令安排实现的认证。	X.509
Source of Authority（SOA） 源机构	一个属性机构，受特定资源的特权验证者委托，作为最终机构来指配一组特权。	X.509
spam 垃圾邮件	未经要求的和多余的电子邮件。	H.235
spoofing 欺骗	冒充一个合法的资源或用户。	X.509
strong authentication 强认证	通过密码证书获取的认证。	X.811
Sybil attack 女巫攻击	一种攻击方式，在这种攻击方式中，通过创建大量化名的实体并使用它们获取夸大的影响，来破坏对等网络的信誉系统。	
threat 威胁	潜在的安全侵犯。	X.800
token 标记	见“security token 安全标记”。	
Trojan horse 特洛伊木马	引入系统后，除了其授权的功能之外，特洛伊木马还具有非授权的功能。将报文拷贝给非授权信道的转发也称为特洛伊木马。	X.800
trust 信任	当且仅当实体 X 相信实体 Y 采用一种特定的方式从事了一系列活动，才能说实体 X 信任实体 Y 的该系列活动。	X.810
trusted functionality 可信功能性	按照某种准则，如由安全策略建立的准则，被认为是正确的功能性。	X.800
trusted third party （TTP） 可信第三方（TTP）	（在某种安全策略的范畴内）就某些安全相关活动而言，（被其他实体）得到信任的某个安全机构或其代理。	X.810

术语	定义	参考文献
ubiquitous sensor network (USN) 无处不在的传感器网络（USN）	指的是一种网络，它使用低成本、低功率的传感器来感知周边的环境，以便能在任何时间将感知的信息和知识服务提供给任何人、任何地方。一个无处不在的传感器网络（USN）可覆盖很宽的地理范围，并可支持各种不同的应用。	
unauthorized access 未经授权的访问	一个实体试图违反有效的安全策略访问数据。	M.3016.0
user authentication 用户认证	证明用户或应用进程的身份。	M.3016.0
verifier 验证者	作为或代表要求具备经认证身份的一个实体。验证者包括认证交换中所需的功能。	X.811
vulnerability 弱点	任何可用于侵犯系统或其所含信息的薄弱之处。	X.800
X.509 certificate X.509 证书	作为 ITU-T X.500 标准号码簿的一部分而制定的一种公开密钥证书规范。	J.170

附件 B – 本手册所用的
首字母缩写词和缩略语

附件 B
本手册所用的首字母缩写词和缩略语

缩写	含义
ACI	访问控制信息
AES	高级加密标准算法
ASN.1	抽象语法记法一
ASP	应用服务提供商
ATIS	电信行业解决方案联盟
A/V	视听
BioAPI	生物特征识别应用程序/编程接口
BPON	宽带无源光网络
B2C	商家对客户
CA	认证机构。一个接受实体证书申请、认证申请、核发证书并负责维护与证书有关的状况信息的可信任组织。
CDMA	码分多址
CMIP	通用管理信息协议
CORBA	公共对象请求代理体系结构
CP	证书策略
CPS	证书生效声明
CRL	证书撤销列表
DNS	域名服务器/系统/服务
DSL	数字用户回路
EAP	可扩展的认证协议
ENISA	欧洲网络和信息安全局
ETSI	欧洲电信标准协会
FMC	固定－移动融合
FW	防火墙
GK	网守、网闸
GPRS	通用分组无线系统
GSM	全球移动通信系统
GW	网关

缩写	含义
HFX	霍索恩传真密码
HKM	霍索恩密钥管理算法
HTTP	超文本传送协议
ICT	信息通信技术
ID	标识符
IdM	身份管理
IEC	国际电工委员会
IEEE	电气和电子工程师协会
IETF	互联网工程任务组
IKE	互联网密钥交换是一种用于协商并为IPSec中SA 产生密钥的密钥管理机制。
IM	即时消息
IMS	IP多媒体分系统
IMT-2000	国际移动电信2000
IP	网际协议
IPSec	网际协议安全
IPTV	网际协议电视
IPX	互联网分组交换
ISMS	信息安全管理系统
ISO	国际标准化组织
ITU-T	国际电信联盟电信标准化部门
LAN	局域网
LDAP	轻量级号码簿访问协议
MD5	五号报文摘要（一个安全的散列算法）
MIS	管理信息系统
MTA	报文传送代理（在报文传送中） 媒体终端适配器（在电缆技术中）
MWSSG	移动万维网服务安全网关
NAT	网络地址转换
NGN	下一代网络
OASIS	结构化信息标准促进组织
OMG	对象管理组
OSI	开放系统互连
P2P	对等

缩写	含义
PC	个人计算机
PDA	个人数据助理
PIN	个人身份号码
PII	个人身份信息
PKI	公开密钥基础设施
PKINIT	公开密钥加密法初始认证
PMI	特权管理基础设施
PSS	个人身份信息保护服务
PSTN	公共交换电话网
QoS	服务质量
RBAC	基于角色的访问控制
RFID	射频识别
RSA	Rivest、Shamir和Adleman（公开密钥算法）
RTP	实时协议
SAML	安全声明标记语言
SG	研究组
SHA1	安全散列算法1
SIP	会话初始协议。应用层控制（信令）协议，用于创建、更改和终止与一个或多个参与者的会话。
SMS	短信服务
SMTP	简单邮件传送协议
SNMP	简单网络管理协议
SoA	源机构
SOA	面向服务的体系结构
SPAK	利用密钥交换实现的、安全的基于口令的认证协议
SSL	安全套接字层
SSO	单一登入
TCP/IP	传输控制协议/网际协议
TLS	传送层安全
TMN	电信管理网
UE	用户设备
UICC	通用集成电路卡
USN	无处不在的传感器网络
VoIP	IP话音

缩写	含义
VPN	虚拟专用网
WAN	广域网
Wi-Fi	无线保真（Wi-Fi联盟的商标，用于基于IEEE 802.11标准的、经过认证的产品）
WTSA	世界电信标准化全会
XACML	可扩展的访问控制标记语言
XML	可扩展的标记语言
3G	第三代
3GPP	第三代合作伙伴计划
3GPP2	第三代合作伙伴计划2

附件 C – ITU-T
安全相关研究组概述

附件C
ITU-T安全相关研究组概述

大多数研究组的工作至少涉及一些与电信和/或信息通信技术安全有关的问题。各研究组负责解决其责任范围内的安全问题，但第 17 研究组的工作焦点就是安全问题，已被指定为有关安全问题的牵头研究组。表 8 概述了各研究组在安全问题上所扮演的角色及其担负的责任，并列出了其相应的牵头研究组的责任。

表 8 – 涉及安全责任的研究组

研究组	名称	责任/安全角色
第2研究组	服务提供和电信管理的运营方面问题	有关服务定义、编号和路由的牵头研究组 有关电信用于救灾/预警的牵头研究组 有关的牵头研究组
第5研究组	环境与气候变化	有关电磁兼容性和电磁效应的牵头研究组 有关信息通信技术和气候变化的牵头研究组
第9研究组	电视和声音传输及综合宽带电缆网络	有关综合宽带电缆和电视网络的牵头研究组
第11研究组	信令要求、协议和测试规范	有关信令和协议的牵头研究组 有关智能网络的牵头研究组 有关测试规范的牵头研究组
第12研究组	性能、QoS和QoE	有关服务质量和用户体验质量的牵头研究组
第13研究组	包括移动网络和下一代网络（NGN）的未来网络	有关未来网络和下一代网络（NGN）的牵头研究组 有关移动性管理和固定-移动融合的牵头研究组
第15研究组	光传输网络和接入网基础设施	有关接入网传输的牵头研究组 有关光技术的牵头研究组 有关光传输网的牵头研究组
第16研究组	多媒体编码、系统和应用	有关多媒体编码、系统和应用的牵头研究组 有关无处不在的应用（“电子万物”，如电子医疗保健）的牵头研究组 有关残疾人所用电信/信息通信技术无障碍牵头研究组
第17研究组	安全	有关电信安全的牵头研究组 有关身份管理的牵头研究组 有关语言和描述技术的牵头研究组

附件 D – 本手册中
参考的安全建议书

附件D
本手册中参考的安全建议书

本附件包含了一份在本手册中参考的所有ITU-T建议书以及超级链接的完整清单，以便使用电子版文本的读者能够直接链接并下载建议书。如文本所述，在其他标准制定组织协作下，ITU-T已制定了许多与安全有关的标准。本清单还包括目前颁布的、与信息通信技术安全有关的各通用/双文本建议书。通过以下网址可以找到全套的ITU-T建议书：www.itu.int/rec/T-REC/en。ITU-T各安全相关建议书可以通过安全标准路线图（www.itu.int/ITU-T/studygroups/com17/ict/index.html）第2部分（数据库）找到。

建议书	名称	对应文本
E.408	电信网络安全要求	
E.409	事故管理机构和安全事故处置：用于电信组织的指导原则	
G.827	端对端国际恒比特率数字路径的可用性性能参数和目标	
G.1000	通信服务质量：框架和定义	
G.1030	为数据应用估计IP网络的端对端性能	
G.1050	用于评估经由IP协议的多媒体传输性能的网络模型	
G.1081	IPTV的性能监控点	
H.235.0	H.323安全：H系列（H.323和其他基于H.245的）多媒体系统的安全框架	
H.235.1	H.323安全：基本安全简表	
H.235.2	H.323安全：签名安全简表	
H.235.3	H.323安全：混合安全简表	
H.235.4	H.323安全：直接和选择性路由的呼叫安全	
H.235.5	H.323安全：使用弱共享秘密的RAS的安全认证框架	
H.235.6	具有本地H.235/H.245密钥管理的话音加密概要	
H.Imp235	H.235 V3实施者指南：“H系列（H.323和其他基于H.245的）多媒体终端的安全和加密”	
H.323	基于数据分组的多媒体通信系统	
H.350	多媒体会议的号码簿服务体系结构	
H.460.17	采用H.225.0呼叫信令连接传送H.323 RAS报文	
H.460.18	H.323信令跨越网络地址转换器和防火墙	
H.460.19	H.323媒体跨越网络地址转换器和防火墙	
H.510	H.323多媒体系统和服务的移动性	

建议书	名称	对应文本
H.530	H.510中有关H.323移动性的对称安全程序	
J.160	使用电缆调制解调器通过有线电视网络提供紧急服务的体系结构框架	
J.170	IPCablecom安全规范	
J.360	IPCablecom2体系结构框架 一 主文件	
M.3010	电信管理网的原则	
M.3016.0	管理平面的安全：概述	
M.3016.1	管理平面的安全：安全要求	
M.3016.2	管理平面的安全：安全服务	
M.3016.3	管理平面的安全：安全机制	
M.3016.4	管理平面的安全：简表形式	
M.3208.2	专用的和可重配置的电路网络的TMN管理服务：旨在形成租用电路服务的可按需提供的服务链路连接的连接管理	
M.3210.1	用于IMT-2000安全管理的TMN管理服务	
Q.816	基于CORBA的TMN服务	
Q.834.3	宽带无源光网络管理接口要求的UML描述	
Q.834.4	基于UML接口要求的宽带无源光网络的CORBA接口规范	
Q.1701	IMT-2000网络框架	
Q.1702	超IMT-2000系统网络方面的远期展望	
Q.1703	超IMT-2000系统网络方面的服务和网络能力框架	
Q.1741.1	带有UTRAN接入网的GSM演进的UMTS核心网1999年版本的IMT-2000参考	3GPP
Q.1742.1	带有cdma2000接入网的ANSI-41演进的核心网的IMT-2000参考	3GPP2
T.4	用于文档传送的三类传真终端的标准化	
T.36	用于三类传真终端的安全能力	
T.37	通过互联网存储转发的传真数据传送程序	
T.38	经由IP网络的实时三类传真通信程序	
T.563	四类传真设备的终端特性	
X.500	号码簿：概念、模型和服务概述	ISO/IEC 9594-1
X.501	号码簿：模型	ISO/IEC 9594-2
X.509	号码簿：公开密钥和属性证书框架	ISO/IEC 9594-8
X.511	号码簿：抽象服务定义	ISO/IEC 9594-3
X.518	号码簿：分布操作的程序	ISO/IEC 9594-4
X.519	号码簿：协议规范	ISO/IEC 9594-5
X.520	号码簿：选择的属性类型	ISO/IEC 9594-6
X.521	号码簿：选择的对象类别	ISO/IEC 9594-7

建议书	名称	对应文本
X.525	号码簿：复制	ISO/IEC 9594-9
X.530	号码簿：对号码簿管理使用系统管理措施	ISO/IEC 9594-10
X.711	通用管理信息协议：规范	ISO/IEC 9596-1
X.736	系统管理：安全告警报告功能	ISO/IEC 10164-7
X.740	系统管理：安全审计跟踪功能	ISO/IEC 10164-8
X.741	系统管理：访问控制的对象和属性	ISO/IEC 10164-9
X.780	定义CORBA被管对象的TMN指导原则	
X.780.1	定义粗粒度的CORBA被管对象接口的TMN指导原则	
X.780.2	定义面向服务的CORBA被管对象和外观对象的TMN指导原则	
X.781	实施与基于CORBA的系统有关的一致性声明形式的要求和指导原则	
X.790	ITU-T应用的故障管理功能	
X.800	CCITT应用的开放系统互连的安全体系结构	ISO/IEC 7498-2
X.802	低层安全模型	ISO/IEC TR 13594
X.803	高层安全模型	ISO/IEC 10745
X.805	提供端对端通信的系统的安全体系结构	ISO/IEC 18028-2
X.810	开放系统安全框架：概述	ISO/IEC 10181-1
X.811	开放系统安全框架：认证框架	ISO/IEC 10181-2
X.812	开放系统安全框架：访问控制框架	ISO/IEC 10181-3
X.813	开放系统安全框架：不可抵赖框架	ISO/IEC 10181-4
X.814	开放系统安全框架：机密性框架	ISO/IEC 10181-5
X.815	开放系统安全框架：完整性框架	ISO/IEC 10181-6
X.816	开放系统安全框架： 安全审计和告警框架	ISO/IEC 10181-7
X.830	通用高层安全：概述、模型和记法	ISO/IEC 11586-1
X.831	通用高层安全：安全交换服务要素（SESE）服务定义	ISO/IEC 11586-2
X.832	通用高层安全：安全交换服务要素（SESE）协议规范	ISO/IEC 11586-3
X.833	通用高层安全：保护传送语法规范	ISO/IEC 11586-4
X.834	通用高层安全：安全交换服务要素（SESE）协议实施一致性声明（PICS）形式	ISO/IEC 11586-5
X.835	通用高层安全：保护传送语法协议实施一致性声明（PICS）形式	ISO/IEC 11586-6
X.841	安全技术 — 访问控制的安全信息对象	ISO/IEC 15816
X.842	安全技术 — 可信第三方服务的使用和管理指导原则	ISO/IEC TR 14516
X.843	安全技术 — 支持数字签名应用的TTP服务规范	ISO/IEC 15945
X.800-X.849 X.Sup3	系统和网络安全实施指导原则增补	

建议书	名称	对应文本
X.1031	安全体系结构中最终用户和电信网络的角色与作用	
X.1034	基于数据通信网络中认证和密钥管理的可扩展认证协议的指导原则	
X.1035	口令认证的密钥交换（PAK）协议	
X.1036	创建、储存、分发和执行网络安全策略的框架	
X.1051	安全技术 — 基于ISO/IEC 27002的电信组织信息安全管理指导原则	ISO/IEC 27011
X.1055	电信组织的风险管理和风险简表指导原则	
X.1056	电信组织的安全事故管理指导原则	
X.1081	远程生物特征识别安全规范和安全问题框架	
X.1082	与人体生理有关的远程生物特征识别	ISO/IEC 80000-14
X.1083	生物特征识别 — BioAPI互通协议	ISO/IEC 24708
X.1084	远程生物特征识别系统机制 — 第1部分：电信系统的通用生物特征识别认证协议和系统模型概况	
X.1086	远程生物特征识别系统机制 — 第1部分：生物特征识别数据安全的技术性和管理性应对措施指导原则	
X.1088	远程生物特征识别数字密钥框架（TDK） — 生物特征识别数字密钥生成和保护框架	
X.1089	远程生物特征识别认证基础设施（TAI）	
X.1111	家庭网络的安全技术框架	
X.1112	家庭网络的设备证书简表	
X.1113	家庭网络服务的用户认证机制指导原则	
X.1114	家庭网络的授权框架	
X.1121	移动端对端通信的安全技术框架	
X.1122	基于PKI实施安全移动系统的指导原则	
X.1123	用于安全的移动端对端数据通信的不同的安全服务	
X.1124	移动端对端通信的认证体系结构	
X.1125	移动数据通信中相关的反应系统	
X.1141	安全声明标记语言（SAML 2.0）	OASIS SAML 2.0
X.1142	可扩展的访问控制标记语言（XACML 2.0）	OASIS XACML 2.0
X.1143	保证移动万维网服务中报文安全的安全体系结构	
X.1151	利用密钥交换实现的基于口令的安全认证协议的指导原则	
X.1152	使用可信第三方服务的、安全的端对端数据通信技术	
X.1161	安全对等通信框架	

建议书	名称	对应文本
X.1162	对等网络的安全体系结构和运行	
X.1171	在采用基于标签识别的应用中对保护个人可识别信息的威胁和要求	
X.1191	IPTV安全问题的功能要求和体系结构	
X.1205	网络安全概述	
X.1206	关于安全信息自动通告和更新发布的厂商中立框架	
X.1207	电信服务提供商应对间谍软件及潜在有害软件风险的指导原则	
X.1231	应对垃圾邮件的技术策略	
X.1240	应对垃圾电子邮件涉及的技术	
X.1241	应对垃圾电子邮件的技术框架	
X.1242	基于用户指定规则的短消息业务（SMA）垃圾过滤系统	
X.1244	打击IP多媒体应用中垃圾信息的概述	
X.1250	增强型全球身份管理和互操作性的基本能力	
X.1251	用户控制数字身份的框架	
X.1303	通用告警协议（CAP 1.1）	OASIS CAP v1.1
X.Sup6	ITU-T X.1240系列 － 有关应对垃圾邮件和相关威胁的增补	
X.Sup7	ITU-T X.1250系列 － 有关网络安全中身份管理概述的增补	
Y.2001	下一代网络（NGN）综述	
Y.2701	下一代网络（NGN）安全要求（第1版）	
Y.2720	下一代网络身份管理框架	
	其他出版物	
	公众网的外部设施技术	
	应用计算机和微处理器构建、安装和保护电信电缆	

瑞士印刷
2009年，日内瓦