普通高等教育电子通信类国家级特色专业系列规划教材

通信网络安全

主　编　刘　云　孟嗣仪
副主编　赵红礼　张长伦
李　勇　贾　凡

科学出版社

普通高等教育电子通信类国家级特色专业系列规划教材

通信网络安全

主　编　刘　云　孟嗣仪
副主编　赵红礼　张长伦
　　李　勇　贾　凡

科学出版社
北　京

内 容 简 介

本书以现代通信网络为背景，系统、深入地介绍了通信网络安全的主要技术以及保证网络安全的各种方法和防御手段，使读者可以灵活地掌握通信网络安全的基本知识和基本技能。全书共 8 章，内容包括通信网络安全体系结构、密码学、安全认证与访问控制、网络安全技术基础、无线通信安全概述、无线通信安全机制、电信网及下一代网络安全技术。本书内容丰富、概念清楚、取材新颖，充分反映了近年来通信网络安全的先进技术及发展方向。

本书可作为高等学校电子信息、通信等专业的高年级本科生教材，也可作为通信技术人员和研究人员继续教育的参考书。

图书在版编目(CIP)数据

通信网络安全/刘云，孟嗣仪主编. —北京：科学出版社，2011. 7
（普通高等教育电子通信类国家级特色专业系列规划教材）
ISBN 978-7-03-031764-3

Ⅰ. ①通… Ⅱ. ①刘…②孟… Ⅲ. ①通信网-安全技术-高等学校-教材
Ⅳ. ①TN915. 08

中国版本图书馆 CIP 数据核字(2011)第 125155 号

丛书策划：匡 敏 潘斯斯
责任编辑：潘斯斯 张丽花 / 责任校对：陈玉凤
责任印制：张克忠 / 封面设计：迷底书装

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

腾龙印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2011 年 7 月第 一 版 开本：787×1092 1/16
2011 年 7 月第一次印刷 印张：17
印数：1—4 000 字数：410 000

定价：32.00 元

（如有印装质量问题，我社负责调换）

前　言

通信网络的普及和演进让人们改变了信息沟通的方式，并且在推进信息化的过程中与多种社会经济生活有着十分紧密的关联，这种关联一方面带来了巨大的社会价值和经济价值，另一方面也意味着巨大的潜在危险，一旦通信网络出现安全事故，就有可能使成千上万人之间的沟通出现障碍，带来无法预料的损失。本书以当前广泛应用的通信系统和代表发展趋势的通信网络安全新技术为背景，在介绍基本原理的基础上，注重取材的新颖与先进性，力求充分反映近年来国内外通信网络安全技术的发展。本书作者均有多年从事通信网络安全工作的经验。本书是近些年来作者从事本科生和研究生教学实践经验的总结，其宗旨是系统深入地阐述通信网络安全的相关技术和基本原理，使读者可以灵活掌握通信网络安全的基本知识和基本技能。

本书共 8 章，除了第 1 章绪论以外，其余内容分为 6 个部分：通信网络安全体系结构（第 2 章）、密码学（第 3 章）、安全认证与访问控制（第 4 章）、网络安全技术基础（第 5 章）、无线网络安全（第 6 章、第 7 章）、电信网及下一代网络安全技术（第 8 章）。

第 1 章绪论主要介绍了通信网络安全的安全威胁与攻击、信息系统安全保护等级，其内容包括安全服务、安全体制和安全管理等，使读者能够全面地了解和掌握安全基本知识、安全保护等级和安全的国内外标准，也可以全面地了解通信网络安全的现状和信息安全的重要性。

第 2 章主要介绍了国家电信网安全防卫系统、通信网络与计算机网络安全体系结构和电信网络安全模型，具体包括电信网络面临的典型攻击及其防卫措施、电信网络的安全对抗体系结构、各种通信网络与计算机网络安全体系结构以及电信网络的保密通信模型、网络访问模型以及安全防御体系，使读者可以全面地了解电信网的安全现状，并能掌握电信网络以及计算机网络等网络的安全模型与防御体系。

第 3 章介绍了网络安全与信息安全、保密与保密系统、典型的古典密码、密码体制、密码攻击及网络加密方式等内容，并介绍数据加密标准（DES）的设计思想、设计原理及实现方法、RSA 算法及其应用、认证理论基础及密钥管理。

第 4 章主要介绍了身份认证技术、Kerberos 认证和 X.509 认证，访问控制技术包括访问控制策略、机制、方案和安全审计技术等，其中重点介绍了自主访问控制 DAC、强制型的访问控制 MAC 以及基于角色的访问控制 RBAC 等访问控制策略。

第 5 章主要介绍了防火墙的基本概念、特点、类型、体系结构以及实现防火墙的关键技术，同时深入介绍了病毒的概念、特点、种类、防范技术等，并对入侵检测系统（IDS）的功能、分类、系统结构、分析方法，虚拟专用网（VPN）技术的基本原理、应用领域和实现方法作了简要介绍。

第 6 章、第 7 章主要介绍了无线通信安全特点以及无线通信安全机制，其中主要对蓝牙协议及无线应用协议、蜜罐主机和欺骗网络 WAP、IEEE802.11、UMTS 网络安全、GSM 网络的安全机制、3G 网络的安全机制、IMS 安全、基于公钥的网络访问等技术作了重点介绍。

第 8 章主要介绍了电信网络安全防范及下一代网络涉及的安全技术，其中包括各种电信网络的安全防范技术、IPSec 协议、软交换、物联网、下一代无线网安全等，使读者可以了解现代通

信网络安全的现状和发展方向。

本书由刘云、孟嗣仪任主编，负责全书的统一协调、编纂和定稿；由孟嗣仪、张长伦、李勇、贾凡、赵红礼共同编写。其中，第1章由孟嗣仪执笔编写，第2章、第5章、第8章第1节由张长伦执笔编写，第3章由李勇执笔编写，第4章和第8章第2节由贾凡执笔编写，第6章、第7章和第8章第3节由赵红礼执笔编写。穆海冰副教授在本书材料整理中给予了帮助，在此表示感谢。

在编写本书的过程中，我们得到了北京交通大学电子信息工程学院各位领导以及老师的大力支持和帮助，在此一并表示感谢。

由于作者水平有限，书中难免有不妥和错误之处，恳请读者批评指正。

作　者

2011年5月

目　录

第1章 绪 论

从20世纪90年代末开始，随着互联网的成熟和广泛应用，信息技术在全球范围内引发了一场革命，全球信息化的步伐不断加快，信息型社会正在形成并走向成熟。信息逐渐被作为一种重要的社会战略资源，而与物质、能源和人才一起被列为现代社会生产力要素中的重要因素。随着信息化的发展，各种信息化系统已经成为国家的关键基础设施，它们支持着网络通信、电子商务、电子政务、电子金融、电子税务和网络教育，以及公安、医疗和社会福利保障等各个方面的应用。相对于传统系统而言，数字化网络的特点使这些信息系统的运作方式在信息采集、储存、数据交换、数据处理、信息传送上都有着根本的区别。无论是在计算机上的储存、处理和应用，还是在通信网络上的交换、传输，信息都可能由于非法授权访问而泄密，被篡改破坏而不完整，被冒充替换而不被承认，更可能因为阻塞拦截而无法存取，这些都是网络信息安全上的致命弱点。因而，信息安全问题越来越受到各国政府部门和众多计算机专家、学者的广泛重视和研究，越来越多的研究机构开始对信息安全问题展开探讨和研究。

1.1 信息安全基础

要理解信息安全，首先要了解信息与信息系统的定义。

1.1.1 信息与信息系统

信息是用语言、文字、数字、符号、图像、声音、情景、表情和状态等方式传递的内容。它是适合于通信、存储或处理表示的知识或消息。信息的获取需要经过对数据的处理。数据是记录下来的可以被鉴别的符号，数据经过解释后成为信息。

信息系统是将用于收集、处理、存储和传播信息的部件组织在一起而成的相关联的整体，一般是由计算机硬件、网络和通信设备、计算机软件、信息资源和信息用户组成。它是以处理信息流为目的的人机一体化系统。

信息系统主要有输入、存储、处理、输出和控制五个基本功能，各基本功能的主要功能如下。

(1)输入功能：输入功能决定于信息系统所要达到的目的及系统的能力。

(2)存储功能：存储功能指系统存储各种信息资料和数据的能力。

(3)处理功能：主要是对信息的收集、处理和分析，最后得出结论，是基于数据仓库技术的联机分析处理和数据挖掘(DM)技术。

(4)输出功能：信息系统的各种功能都是为了保证最终实现最佳的输出功能。

(5)控制功能：对构成系统的各种信息处理设备进行控制和管理，对整个信息加工、处理、传输、输出等环节通过各种程序进行控制。

信息系统的类型按照其发展历史和应用领域可分为数据处理系统(Data Processing System，DPS)、管理信息系统(Management Information System，MIS)、决策支持系统(Decision Sustainment System，DSS)、专家系统(人工智能(Artificial Intelligence，AI)的一个子集)和办公自动化(Office Automation，OA)五种类型。

信息系统的开发涉及计算机技术基础与运行环境，主要涵盖的开发技术包括计算机硬件技术、计算机软件技术、计算机网络技术和数据库技术。

1. 计算机硬件技术

计算机硬件包括运算器和控制器(CPU)、存储器(内存和外存)、输入设备(键盘、鼠标、手写板、绘图仪)、输出设备(打印机、扫描仪、显示器、音响)等。计算机的硬件技术从根本上决定了计算机可达到的运行速度和存储能力。只有硬件的计算机称为裸机，需要安装操作系统才可以运行，操作系统属于系统软件，再加上应用软件才能构成完整的计算机系统。

2. 计算机软件技术

计算机软件分为系统软件和应用软件。

系统软件是指为管理、控制和维护计算机及外设，并提供计算机与用户界面的软件。主要包括各种语言和它们的汇编或解释程序、编译程序、计算机的监控管理程序(Monitor)、调试程序(Debug)、故障检查和诊断程序、程序库、数据库管理程序、操作系统(Operating System，OS)。应用软件则指专门为某一应用目的而编制的软件，是用各种程序设计语言编制的应用程序的集合，是利用计算机为解决某类问题而设计的可供多用户使用程序的集合。

3. 计算机网络技术

计算机网络技术是用通信介质把分布在不同的地理位置的计算机、计算机系统和其他网络设备连接起来，以功能完善的网络软件实现信息互通和网络资源共享的系统。计算机网络包括网络介质、协议、节点和链路。计算机网络具有共享硬件、软件和数据资源的功能，具有对共享数据资源进行集中处理及管理和维护的能力。

计算机网络技术实现了资源共享。人们可以在办公室、家里或其他任何地方访问查询网上的任何资源，极大地提高了工作效率，促进了办公自动化、工厂自动化和家庭自动化的发展。

4. 数据库技术

数据库技术是信息系统的一个核心技术，研究解决了信息处理过程中大量的数据有效组织和存储的问题，主要包括信息、数据、数据处理、数据库、数据库管理系统及数据库系统等。数据模型包括用户层次模型(Hierarchical Model)、网状模型(Network Model)和关系模型(Relation Model)数据库系统。

实体联系模型(ER 模型)是对现实世界的一种抽象，它抽取了客观事物中人们所关心的信息，忽略了非本质的细节，并对这些信息进行了精确的描述。

数据库设计的步骤包括用户需求分析、数据库逻辑设计、数据库物理设计，以及数据库的实施和维护四个阶段。关系的规范化理论是数据库设计过程中的有力工具。范式是指规范化的关系模式。所以，数据库在设计时，不仅要考虑到自身结构的完整性，还要考虑到数据的使用要求，使数据的组织更加合理。

1.1.2 通信系统

通信系统是用以完成信息传输过程的技术系统的总称。一种基本的通信系统一般由信源、信宿(收信者)、发送设备、接收设备和传输媒介等部分组成，如图 1-1 所示。

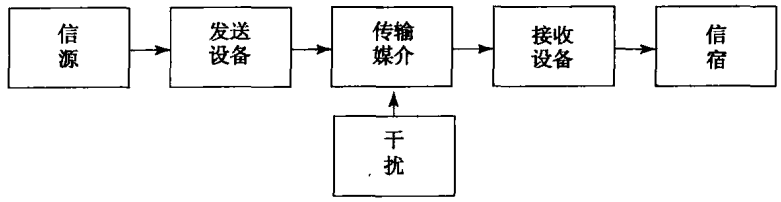

图 1-1　通信系统的一般模型

图 1-1 各模块的具体功能描述如下。

1. 信源和信宿

根据信源输出信号的不同性质，信源可以分为模拟信源和离散信源。模拟信源输出连续幅度的信号，离散信源输出离散的符号序列。模拟信源可以通过采样和量化的方式将其离散化，使其成为离散信源，随着通信技术的发展，离散信源的种类和数量会变得越来越多。在大多数场合中，由于信源也可以成为信宿，通信的双方需要随时交流信息，所以信宿的性质和信源是相同的。

2. 发送设备

发送设备的基本功能是将信源和传输媒介匹配起来，也就是说将信源所产生的信号变换成便于传送的信号，并送往传输媒介。同时，发送设备还具有包括为达到某些特殊要求所进行的各种处理的功能，如多路复用、保密处理和纠错编码处理等。

3. 传输媒介

从发送设备到接收设备信号传递所经过的媒介称为传输媒介。传输媒介可以分为有线和无线两种类型，每一种类型的传输媒介又有很多种传输介质(如光纤和无线电波等)。信号在传输过程中，必然会引入干扰，如热噪声、脉冲干扰和衰落等，这些都会对信号在传输媒介中的传输产生干扰，所以干扰的特性和媒介的固有属性直接关系到信号的变换方式。

4. 接收设备

接收设备的基本功能是完成发送设备的反变换，即进行解调、译码和解密等，主要完成的功能是从带有干扰的信号中正确恢复出原始信号。对于多路复用信号，它还具有解除多路复用和实现正确分路的功能。

以上介绍了通信系统各模块的主要功能。在通信的过程中，来自信源的消息(语言、文字、图像或数据)在发信端先由终端设备(如电话机、传真机或计算机等数据终端设备)变换成原始电信号，然后经发送设备进行编码、调制和放大后；把原始电信号变换成适合在传输媒介中传输的信号，经传输媒介传输到接收端，经接收设备进行反变换恢复成原始电信号，再由终端设备恢复成消息提供给收信者。这种点对点的通信大都是双向传输的，电话就是最好的一个例子。如果两个方向都有各自的传输介质，则双方都可独立进行发送和接收；若双方共用一个传输介质，则必须用频率或者时间分割的办法来共享。

通信系统的分类有很多种，下面主要介绍几种由通信模型所引发的分类。

1. 按信息的物理特征分类

根据信息不同的物理特征，通信系统可分为电报通信系统、电话信息系统、数据通信系统和图像通信系统等。这些通信系统经常是兼容或者并存在一起的。

2. 按调制方式分类

根据是否采用调制方式，通信系统可分为调制传输和基带传输两类。基带传输是将未经调制的信号直接发送，如音频室内电话和数字信号基带传输等；调制传输是对各种信号变换方式后传输的总称，它能将消息变换成易于传送的形式，大大提高了性能和抗干扰能力，又有效地利用了频带。调制的方式有很多，常见的调制方式如表 1-1 所示。

表 1-1　常用的调制方式

连续波调制	线性调制	常规双边带调幅 AM
		抑制载波双边带调幅 DSB
		单边带调幅 SSB
		残留边带调幅 VSB
	非线性调制	频率调制 FM
		相位调制 PM
	数字调制	幅移键控 ASK
		频移键控 FSK
		相移键控 PSK、DPSK 和 QPSK 等
		高效数字调制 QAM 和 MSK 等
脉冲调制	脉冲模拟调制	脉幅调制 PAM
		脉宽调制 PDM
		脉位调制 PPM
	脉冲数字调制	脉码调制 PCM
		增量调制 DM、CVSD 和 DVSD 等
		差分脉码调制 DPCM
		语音编码 ADPCM、APC 和 LPC 等

3. 按传输信号的特征分类

根据信道中所传输的是模拟信号还是数字信号，通信系统可分为模拟通信系统和数字通信系统两大类。数字通信随着通信技术的发展在近些年得到了迅速的发展，相比于模拟通信系统，数字通信系统的抗干扰能力更强，而且易于实现集成化，利于实现综合业务通信网络。

4. 按传送信号的复用方式分类

可以将传送多路信号的复用方式分为频分复用、时分复用及码分复用三大类。频分复用就是将用于传输信道的总带宽划分成若干个子频带（或称子信道），每一个子信道传输 1 路信号。时分复用采用同一物理连接的不同时段来传输不同的信号，也能达到多路传输的目的。时分多

路复用以时间作为信号分割的参量，故必须使各路信号在时间轴上互不重叠。码分复用用一组包含互相正交码字的码组携带多路信号。采用同一波长的扩频序列，频谱资源利用率高，可以大大增加系统容量。频谱展宽靠与信号本身无关的一种编码完成。

5. 按传输媒介分类

按传输媒介分类，可以将通信系统分为有线通信和无线通信两大类。有线通信指的是借助线缆线路传送信号的通信方式；无线通信指的是仅利用电磁波而不通过线缆进行的通信方式。

6. 按不同的通信业务分类

按照不同的通信业务，通信系统又可分为电话通信系统、数据通信系统、传真通信系统和图像通信系统等。由于人们对通信的容量要求越来越高，对通信的业务要求越来越多样化，所以通信系统正迅速向着宽带化方向发展，而光纤通信系统将在通信网络中发挥越来越重要的作用。

通信的主要任务是传递信息，因此决定一个通信系统好坏最主要的质量指标便是传输信息的有效性和可靠性。“有效性”是指在给定信道内能传输信息内容的多少；“可靠性”是指接收信息的准确程度。如果把通信系统按照传输信号的特征分类的话，那么通信系统可以分为模拟通信系统和数字通信系统。模拟通信系统的有效性可以用有效传输频带来度量，可靠性可以用接收端最终输出信噪比来度量；对于数字通信系统，有效性可以用信息传输速率来衡量，而可靠性可以用错误率来衡量。可靠性与有效性是可以互换的，具体的内容请参见信息论中著名的香农公式。

1.1.3 网络与信息安全

要实现信息化，就必须重视信息网络安全。信息网络安全绝不仅仅是 IT 行业的问题，而是一个全社会问题，是一个包括多学科的系统安全工程问题，并直接关系到国家安全。因此，我国一些知名的安全专家呼吁，要像重视“两弹一星”那样重视信息安全。通信网络作为信息传递的一种主要的载体，其安全性是信息安全中关键的问题之一。然而，由于通信网络本身的脆弱性，使得通信网络面临国际国内严重的威胁和攻击。通信网络的安全不仅是保障通信正常工作和发展的需求，还是涉及国家安全的大事，已经引起了越来越多的人的重视。

为明确“通信网络安全”的含义，必须首先定义“信息安全”。“信息安全”的定义如下：信息安全通常是指信息在采集、传递、存储和应用等过程中的完整性、机密性、可用性、可控性和不可否认性。所以，为了实现信息安全，需要做到以下几点。

(1)建立信息安全管理机制，制定信息安全策略。

(2)制定信息安全测评标准，评估和划分安全等级。

(3)使用安全管理产品和网络以保障采集、传递、存储和应用时的机密性、完整性、可用性、可控性及不可否认性。

(4)应用检测机制获悉当前安全状态。

(5)通过故障和灾难恢复机制解决出现的问题。

在对信息安全的定义及实现机制有了初步的了解以后，一般认为，“信息网络安全”是指信息在利用网络提供的服务进行传递的过程中，网络自身的可靠性和生存性，网络服务的可用性和可控性，以及信息的完整性、机密性和不可否认性。

1.1.4 通信网络安全

通信网络安全通常包括承载网与业务网安全、网络服务安全及信息传递安全三个部分。因此，根据信息安全的五个特性，通信网络安全同样具有以下五个特点。

(1)可靠性：网络在规定的条件下和规定的时间内完成特定功能的能力，或者网络在质量允许的范围内正常工作的能力。

(2)可用性：信息和通信服务在需要时允许授权人和实体使用，或者网络资源在需要时即可使用的能力。

(3)保密性：防止信息泄露或者提供非授权个人和实体的特性，或者信息只为授权用户使用。

(4)完整性：信息不被偶然或者蓄意地删除、修改、伪造、乱序、重放和插入等。

(5)不可抵赖性：在通信交换中，确认参与者双方真实的同一性，双方都不能否认或者抵赖曾发生的通信联系和通信内容。

可靠性是通信网络安全最基本的要求，是通信网络安全的基础。任何安全措施都必须建立在通信网络可靠性的基础上才能实施。如果通信网络不可靠，通信网络的安全无从保障。但当通信网络能可靠工作时，通信网络却不能为用户提供有效的信息和信息服务，或者是机要的敏感信息被泄露，或者提供的信息被修改和破坏，或者通信双方中任意一方否认和抵赖曾经发生的通信联系和通信内容的话，通信网络仍然被认为是不安全的。

通信网络主要的功能是提供有效的通信信息和信息服务，通信网络容纳了社会各行各业大量的信息，而信息本身就是财富，其中还有包括涉及国家安全和利益的敏感信息，因此保障信息的安全是通信网络安全的核心。建立通信网络最终的目的是为了获取安全可靠的信息，所以要确保通信网络安全，首先必须保证通信网络的信息安全。但是在保证信息安全的基础上，还需要对信息安全提供保护，在安全政策和安全法规的保护下建立相应的安全检测和安全管理机制，通过安全检测和安全管理机制充分确保通信网络的物理安全，从而为通信网络的信息安全最大限度的提供了外层保护。通信网络安全的层次结构图如图 1-2 所示，其中，外层的安全功能对内层的安全功能提供保护作用。

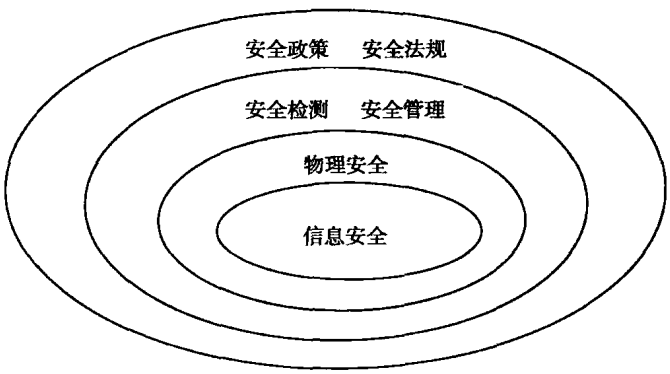

图 1-2 通信网络安全的层次结构图

在通信网络中，信息大致可以分为两类：用户信息和网络信息。用户信息主要是指面向用户的话音、数字、图像、文字和各种媒体库的信息，主要分为以下四种类型。

(1)个人隐私信息：主要指一般的用户信息。

(2)公共信息服务：主要包括公用多媒体信息服务、公用声讯信息服务及公用信息库的信息。

(3)商业信息：主要包括商务信息、知识产权信息和金融税务信息等。

(4)敏感信息：主要包括涉及国家机密的信息。

网络信息是面向网络运作的信息，包括网络通信软件、支撑软件、各种通信协议、信令、数字同步信息和通信管理信息等，主要分为通信程序、信令信息、通信设备中的操作系统、数字同步信

息、通信设备中的数据库、通信管理信息及通信协议七种信息。在一般情况下，通信网络的安全主要是保障用户信息和网络信息的安全，所以通信网络安全面临的威胁除了对通信网络硬件系统的安全攻击以外，还包括陷门、逻辑炸弹、非法通信、遥控旁路和病毒等软件方面的安全隐患。

通信网络按照传输媒介可以分为有线通信网络和无线通信网络，而随着无线网络和互联网的不断融合，通信网络发展的下一个目标即为下一代网络。下一代网络是基于 IP 的分组网，支持多种业务，能够实现业务与传送分离，且控制功能独立，接口开放，保证服务质量，支持通用移动性。由于传输媒介及采取技术的不同，每一种类型的通信网络对自身安全性的定义及实现的技术都有所不同。下面分别介绍无线网络安全、有线网络安全和下一代网络安全的定义及其安全性的基本实现技术。

1. 有线网络安全

有线网络就其功能属性而言应是包括有线电视传输和宽带数据互联的多业务多媒体网络系统。有线网络的安全性问题主要有三个层次：第一层次是网络的实体安全，第二层次是网络的运行安全，第三层次是网络的信息安全。

第一层次有线网络的实体安全，主要是机房的物理条件、物理环境和设施的安全，以及计算机硬件、附属设备和网络传输线路的安装和配置，如线路接地、防雷、电源、设备可靠性和线路设计施工的合理性等。这一层次上，有网络本身器材或施工质量引起的问题，特别是由于早期的有线电视网络设计起点低、施工不合理、材料质量差和检测仪器落后等因素造成部分网络有线电视收看质量不稳定；有分配网中人为破坏或私拉乱接造成网络短路或中断等问题。从有线网络的技术特征来看，整个网络的安全存在于网络建设的各个环节，存在于数据网 OSI 七层模型的各个层之中。

第二层次有线网络的运行安全，主要是运用软件检测手段，保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、篡改和破坏，不受病毒的侵害等。这一层次有线网络的安全隐患主要是有线电视网络可能遭到非法信号侵入或干扰、病毒侵害或黑客破坏；在前端机房，由停电或管理问题还会引起停播等。

第三层次有线网络的信息安全，主要是保护网络信息的数据安全，不被非法存取。保护其完整性、一致性和保密性。保证网络信息合法使用，如运行时对突发事件的安全处理，防止黑客侵入等措施包括建立安全管理制度、开展安全审计和建立用户认证体系。目前，有线网络在这一层次上的隐患主要是有线电视的非授权接入。

2. 无线网络安全

无线网络具有组网简单、安装容易和移动方便等特点。但由于无线网络具有信号的开放性和数据传播范围很难控制等特点，网络的可靠传输必然会产生不稳定因素。无线网络信号由于利用无线电波在空中辐射传播，所以发送的数据可能到达预期之外的接收设备，这些外部接收设备给网络带来了不安全因素，因为外部可以利用这些广播信号对网络发起攻击。无线网络比有线网络更容易受到入侵，因为被攻击端的计算机与攻击端的计算机并不需要物理上的连接，攻击者只要在网域的无线路由器或中继器的有效范围内，就可以进入被攻击者的内部网络，访问被攻击者的资源。常用的无线网络攻击手段包括非法的 AP、未经授权使用服务、地址欺骗和会话拦截、流量分析与流量侦听，以及高级入侵等。

目前，无线网络安全技术有很多，但由于无线网络存在较大的安全隐患，因此单一的技术不

能完全解决问题。必须明白，只有结合多种安全设置和技术才能构建安全的无线网络。以下列举几种主要的安全技术。

(1)完善连线保密协议。

(2)设置 SSID 坚固网络。

(3)VPN 技术增强安全性能。

(4)MAC 过滤防不速之客。

(5)禁用动态主机配置协议。

(6)端口访问控制技术(IEEE 802.1x)控制网络接入。

3. 下一代网络安全

下一代移动通信网络具有开放、灵活、可管理、移动的网络架构等特点，因此其安全问题比以往的移动通信系统更加复杂。下一代移动通信系统的核心思想其实就是泛在网络的内涵，泛在网络是下一代移动通信系统发展的必然趋势，这在全球已达成共识。

移动泛在业务环境是一个拥有许多机制的业务环境，通过各个异构网络的协同以支持不同的移动无缝连接，同时泛在智能终端及传感器网络能够进行环境感知和上下文信息采集，支持信息空间与物理空间的融合。泛在网络将不再是被动地满足用户的需求，而是主动感知用户场景的变化并进行信息交互，通过分析用户的个性化需求而主动提供服务。相应地，终端设备也具备智能型接口及环境感知能力，使用户的使用更加简单和方便。

根据下一代移动通信系统的网络结构，结合 2G 和 3G 系统出现的安全问题，下一代移动通信系统存在的安全威胁主要来自以下几个方面。

(1)窃听：在无线链路或服务网内窃听用户数据、信令数据及控制数据，这是最常用也是最容易理解的窃取信息的手段。

(2)伪装：伪装成网络单元截取用户数据、信令数据及控制数据。因为直接窃听到的信息是经过加密的，一般情况下解密并不容易，所以通过伪装来窃取信息的威胁性比窃听更大。

(3)流量分析：主动或被动进行流量分析以获取信息的时间、速率、长度、来源及目的地。

(4)破坏数据完整性：修改、插入、重放、删除用户或信令数据以破坏数据完整性，这些情况将引起比窃听和伪装更加严重的后果。

(5)拒绝服务：在物理上或协议上干扰用户数据、信令数据及控制数据在无线链路上的正确传输，实现拒绝服务攻击。

(6)否认：用户否认业务费用、业务数据来源及发送或接收到其他用户的数据，网络单元否认提供的网络服务。

(7)非授权访问服务：用户滥用权限获取对非授权服务的访问，服务网滥用权限获取对非授权服务的访问。

(8)资源耗尽：通过网络服务过载耗尽网络资源，导致合法用户无法访问。

结合下一代移动通信系统的特点及以上几种可能面临的安全威胁，归纳起来，下一代网络的安全体系结构应该具有以下五个特点。

(1)网络接入安全：主要指为用户提供安全接入移动通信网络服务，特别强调防止无线接入链路的攻击。

(2)网络域安全：主要包括在运营商节点间安全传输数据，并保护有线网络。

(3)用户域安全：主要包括安全接入异构移动站及以用户为中心的安全域的安全特性，如用