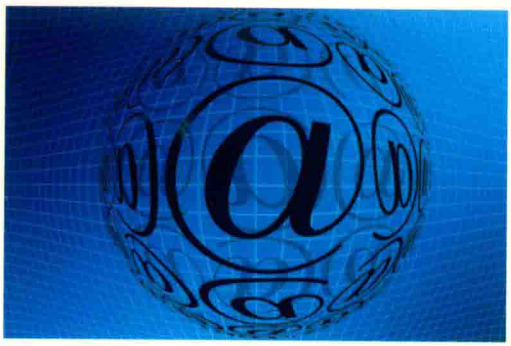
网络信息安全传输技术及其测评研究



宋颜云◎著

WANGLUO XINXI ANQUAN CHUANSHU JISHU
JI QI CEPING YANJIU

中国水利水电出版社
www.waterpub.com.cn

网络信息安全传输技术及其测评研究

宋颜云　著

中国水利水电出版社
www.waterpub.com.cn
·北京·

内 容 提 要

现代社会，计算机科技的迅速发展使互联网对人们日常生活的影响逐渐加深，人们不仅可以通过互联网迅速传递消息，还能通过互联网购物、出行、住宿等，这对现代人来说极为便利。可是随之而来的便是一些信息传输安全方面的问题。本书是对计算机网络中的信息传输安全及其评估问题的探讨分析。内容主要是网络中的信息传输安全技术研究（信息安全概述、网络安全传输技术简介、网络安全的相关基础、网络信息的安全传输技术、网络路由的抗毁和自愈）和网络信息安全测评技术（安全测评的概念、信息安全评估标准分析、网络信息安全测评理论、数据安全的测评评估、主机安全的测评评估、网络安全的测评评估）等。

本书适合从事网络安全工作的专业人员阅读，也可作为网络安全爱好人士的参考用书。

图书在版编目（CIP）数据

网络信息安全传输技术及其测评研究 / 宋颜云著
. -- 北京 : 中国水利水电出版社, 2018.9
ISBN 978-7-5170-6940-9

Ⅰ. ①网… Ⅱ. ①宋… Ⅲ. ①计算机网络－网络安全－数据传输－研究 Ⅳ. ①TP393.083

中国版本图书馆CIP数据核字（2018）第221632号

责任编辑：陈　洁　　封面设计：王　斌

书　名	**网络信息安全传输技术及其测评研究** WANGLUO XINXI ANQUAN CHUANSHU JISHU JI QI CEPING YANJIU
作　者	宋颜云　著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市元兴印务有限公司
规　格	170mm×230mm　16开本　16.75印张　306千字
版　次	2018年9月第1版　2018年9月第1次印刷
印　数	0001-2000册
定　价	74.00元

前　言

随着计算机科技的发展，互联网在现代人们的生活中已经必不可少，它不仅加快了信息的传播速度，使人们之间的联系日益密切，还极大地丰富和便利了现代人的日常生活。网络信息技术融入人们生活方方面面的同时，信息传输所产生的安全问题也日益受到关注。网络信息安全一直是伴随网络信息技术应用的难题。为了应对这一难题，有必要对信息安全传输及其测评技术进行研究。

网络信息安全传输技术及其测评研究，主要是对信息网络安全性进行分析描述、测试与评估，从而检验、评估它的安全性效果。经过测评，不仅能够分析、评估网络信息在网络攻击环境条件下的安全性，而且还能够在测试中发现和解决问题，并不断消除网络中存在的一些缺陷与隐患，让网络信息的安全性得到提高。

本书共6章，第1章为信息安全简述，主要包括网络安全的定义、信息安全的特点与定义、网络信息安全的内容及意义、信息安全弱点和信息安全风险来源、网络信息安全的主要目标。第2章主要讨论网络信息安全传输方法与管理，包括保证信息安全的方式，网络安全传输的定义、目标及功能，信息加密技术研究，防火墙技术研究，主动防御技术研究，新技术领域安全挑战的应对处理，非技术领域的网络信息安全管理等。第3章主要介绍网络信息安全测评技术，包括网络信息安全测评定义、网络信息安全测评基本要求、网络信息安全测评基本流程等。第4章主要讨论信息系统安全性相关评估标准，包括信息系统安全性评估标准之可信计算机系统评价标准、信息系统安全性评估标准之通用评估准则、我国信息系统的安全性评估标准等。第5章探讨研究网络信息安全测评技术，主要包括数据安全测评技术研究、主机安全测评技术研究、仿真技术在网络信息安全测评中的实际应用等。第6章分析讨论了网络信息安全测试评估模型，包括基于AHP的信息网络安全测试定量评估模型研究、基于等效分组级联BP的信息网络安全评估模型研究。

总体上看，本书内容本着理论联系实际的精神，在严密探讨理论知识的前提下，紧跟网络信息安全测评技术前沿，内容全面而丰富，兼顾了系

统性、科学性和实用性。作者在撰写本书的过程中参考了大量国内外学术文献与专业资料，并引用了其中一些重要的图表和数据。由于时间仓促和作者水平所限，而且网络信息技术发展非常之快，因此书中难免存在不足之处，望同行专家学者及广大读者批评指正！

作者

2018年5月

目　录

第1章　信息安全简述

随着互联网技术的快速推进，21世纪已然成了信息化的时代。网络使人们的生活方式全面更新，并在很大程度上深刻地影响着人们的行为习惯和思考方式。因此，网络信息安全就成了现代社会和谐稳定发展的重要保证。本章主要讲解网络信息安全的概念、基本功能、主要内容、重要意义、风险来源和目标等。

1.1 网络安全

网络安全是一门涵盖多个学科的综合性学科，其中包括计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。现如今，网络安全与国民经济有着紧密联系，在其各个领域，网络信息的安全建立都是重中之重。下面就网络安全的基础知识、基本概念和属性做深入探讨。

1.1.1 网络安全的基础知识

随着互联网的蓬勃发展，全球化、信息化、资源共享等名词就成了当今世界的主流。网络占据了越来越重要的地位，从过去的重心放在军事、科技、文化、商业等领域，到现在网络信息已经慢慢渗透到了人们生活的方方面面。不论是整个社会，还是人们本身，都不可避免地越发依赖网络，也因此，网络信息的安全就变得尤为重要。

同世界上的其他物质一样，信息也是带有其本质属性的，如传播、共享以及自增值。但是，这些属性在发挥其用处的同时，又有一定的要求限制。例如，信息的传播是要有所控制的，信息的共享是要被授权的，信息的自增值是要求确认的。在网络信息不断全球化的进程中，保证其安全就成了网络信息新技术开发工作的重心。

为了进一步扩大互联网的应用范围，让网络为人们认识世界提供更多的便利，人们对网络信息的安全程度也有了更高的要求。针对网络信息本身所具备的开放性、国际性和自由性，下面就关于其具体要求做

论述。

（1）开放性。互联网最大的特征就是其所具备的开放性。可以说，互联网的技术基本上是全面共享的，不论是个人还是群体，也因此，网络信息存在着巨大的安全隐患。对互联网的攻击可以是多个方面的，如物理传输线路、网络通信协议、系统软件和硬件等，网络信息一旦遭到破坏，可能会造成无法挽回的损失。

（2）国际性。互联网的覆盖范围涵盖全球，这就意味着任何一台接入互联网的计算机都有可能受到来自世界上任意国家、任意地区、任意机器的攻击。网络信息安全所遭受的威胁不是来自某一区域的，而是全球化的安全隐患。

（3）自由性。对于使用互联网的用户来说，它在网络上可以拥有相对最大化的自由。网络技术和网络信息的使用和分享，在互联网发展的过程中并没有严格的法律限制，用户只对自己的言语行为负责任。

互联网具有的开放性、国际性、自由性使得网络飞速发展，尤其是带给政府机构和事业单位的改革是跨越性的。利用网络信息的开放和自由，政府单位的办事效率和市场大幅度提升，竞争力也明显增加。但是互联网的巨大便利性又是把双刃剑，在不断优化人们生活的同时，又要时刻注意网络信息的泄露。如何保护政府、企事业单位的机密信息不受黑客和间谍的入侵，已成为政府机构和企事业单位信息化健康发展所要考虑的重要事情之一。

1.1.2　网络安全的基本概念

从实际意义出发，保障网络信息的安全就是最大程度保障网络信息的完整和私密，防止个人信息和企业机密被泄露。从广义层面上叙述，保障网络安全所涉及的领域包括有关网络信息的保密性、完整性、可用性、真实性等专业技术和原理。

网络安全即在网络信息的保存、传输以及使用的过程中，计算机的硬件、软件和系统在遭受攻击时，可以切实保护网络系统中的硬件、软件和数据的安全，尤其是保证网络信息不会被泄露或遭受破坏，使其能够保证正常工作，系统也可以正常运行。

站在不同角度看网络安全有着不同的意义。作为普通的互联网使用者，他们希望自己的信息得到全方位的保护，尤其是当涉及商业利益时，要尽可能地防止有人利用非法手段窃取用户信息，造成损失；作为互联网的开发者和技术人员，他们希望互联网的各种程序受到保护，尤其是对本地网络信息常用的访问、读写等技术操作，严格控制电脑病毒、不正当储

存、网络资源的非法占用等安全隐患；作为安全保密部门，他们希望对国家高级机密做到最高防范，把任何对国家安全有害的网络信息都隔绝在外，同时防止任何有关国家的信息被非法分子通过网络窃取、破坏，给国家造成巨大经济损失，甚至对国家的安全造成严重威胁。作为人类教育的一环，网络充斥着大量的不良信息，这些非法资源和信息长期在互联网上流动，会给人们的思想带来不健康的影响，因此对其实行严格管理是非常重要的。

1.1.3 网络安全的属性

网络安全按照其有关定义可以总结出如下特征。

（1）保密性。指除了已授权的网络使用者外，其余网络用户均没有获得或使用其网络信息的权限。

（2）完整性。指用户的所有数据在存储和传输的过程中，没有得到授权之前，拥有保持完整的特征，即网络信息不能被更改、破坏或丢失。

（3）可用性。指网络信息可以按照被授权者的需要进行更改和储存，而在正常使用的网络范围内，网络信息遭到破坏或无法正常运行，都可以算作攻击网络安全的可用性。

（4）可控性。指网络信息在授权范围内可以正常流通，除此之外，网络信息的行为方式要得到严格控制。

（5）可审查性。指若网络用户做出对网络信息有安全隐患的操作时，可以从互联网中找到有关根据，如有必要，要使用户对其行为和操作负全部责任。

（6）可保护性。对计算机的硬件、软件和系统进行保护，避免病毒入侵。

1.2 信息安全的概念与基本功能

目前，信息系统在金融、贸易等多种商务领域占据越来越重要的地位。事实上，网络信息是把双刃剑，在将人们的生活变得愈发便利的同时，随之而来的是高科技犯罪率的提升。越来越多的不法分子钻互联网法律法规制度的漏洞，为自己谋得暴利。因此，保护信息安全就显得尤为重要。

1.2.1 信息安全的概念

在系统地介绍信息安全之前，需要对信息系统和信息安全的概念有所

了解。

信息系统（information system）权威唐纳德·戴维斯（Donald Davies）给信息系统下的定义：用于收集、处理、存储和分发信息的相互关联组件的集合，其作用在于支持组件的决策与控制。

根据《中华人民共和国计算机信息系统安全保护条例》中的定义，信息系统的实质是人机系统，在提前规定好的系统技术目标下，利用与互联网相关的软件、硬件和必备的网络设备对网络信息进行收集、加工、储存、传输和搜索。根据这一定义，在当前技术条件下，信息系统的构成将以计算机系统和网络系统为主。而网络信息安全是对网络信息的各种特征进行严密性的保护，如信息的保密性、完整性、可用性等。

1.2.2　信息安全的基本功能

信息安全技术应具备防御、监测、应急、恢复等基本功能，下面分别简要叙述。

（1）网络信息安全防御。网络信息安全防御是指采取各种手段和措施，使网络系统具备阻止、抵御各种已知网络威胁的功能。

（2）网络信息安全监测。网络信息安全监测是指采取各种手段和措施，使网络系统具备监测、发现已知或未知的网络威胁的功能。

（3）网络信息安全应急。网络信息安全应急是指针对网络系统中的突发事件，采取各种手段和措施，使网络系统具备及时响应、处置网络攻击的功能。

（4）网络信息安全恢复。网络信息安全恢复是指针对已经发生的网络灾害事件，采取各种手段和措施，使网络系统具备恢复网络系统运行的功能。

1.3　网络信息安全的内容及意义

21世纪，以互联网现在的发展趋势和重要地位，可以说信息安全是国家安全的基础，只有守得住信息，才能更好地开展国家的各项工作。因此，本小节主要阐述网络信息安全的主要内容和重要意义。

1.3.1　网络信息安全的主要内容

互联网在不断带给人们生活便利的同时，一些网络技术同时也给人们带来了危害。因此保障网络信息安全对整个社会都意义重大。

1. 物理安全

物理安全就是指以物理方法对网络信息系统的设备和线路采取具体的安全保障手段，其主要目的是确保网络系统在任意正常的互联网环境下，接入正常的机器设备都可以通过正常的中间介质保证其正常运行，即确保网络设备和通信的正常运行。上述提到的环境因素主要指自然灾害，如地震、火灾、洪水等；主要的媒介因素包括电磁的辐射和泄漏等。物理安全历来受到广泛重视，国内外已经制定了许多标准和规范。物理安全所涉及的内容相当广泛，下面就较为重要的几点做具体论述。

（1）媒体安全。在媒体数据使用的过程中，可能会出现被盗取、丢失、媒体本身霉变、破坏等多种不安定因素。因此，为了确保媒体上储存的信息可以正常运行，除了要保护媒体信息的安全，也要对媒体本身的安全做出一定程度的保护。

（2）设备安全。互联网常用的设备不仅仅包括计算机，还有其中涵盖的保证计算机稳定运行的网络系统和计算机中的硬件、软件设备。在机器使用的过程中，要密切注意以下问题：电磁辐射导致的信息泄漏、网络线路非法分子截获、电源设备损坏等。

（3）计算机网络临界点安全。当互联网受到攻击时，即是保障网络安全的“临界点”被攻破了。这道临界的防线是保障互联网被侵入的最后一道“门”。常用的网络信息安全临界点有防火墙、内外网连接设备、无线网络设备、VPN设备等。

2. 密码技术

密码学是现代兴起的一门新型学科，它结合数学和计算机两种科学的精髓，并且不断发展出自己的特色。密码技术指的是将互联网信息在加密和解密之间进行变换的一种科学保护网络信息安全的技术手段。可以说，互联网信息安全的根本就是密码技术。密码技术的起源最早可以追溯到古希腊时期，伴随近代几次的科学革命，得到了跨越式的发展，尤其是作为政治和军事斗争的“一杆枪”，占据了意义非凡的地位。并且，在现代科学技术基础上发展起来的密码学对于网络信息各种特性的安全保护起到了非常重要的作用。

20世纪70年代，互联网技术大范围“入侵”人们的生活，可以说，带给人类以往的行为习惯一次巨大的冲击。同样，新的生活方式使得人们对信息安全保护的要求越来越高，因此，密码技术不断进行研发，开拓新的领域范围，专门研究密码学的机构也不仅仅只局限于官方，更多的私人企业加入其中。密码学在这急切要求科学进步的时代飞速发展。

密码技术所具备的理论知识和实践手段在保护网络信息安全方面居于最根本和最核心的地位，其在很多应用领域内都有着无可替代性。例如在国家机密安全的保护措施中，正是因为密码技术应用的关键，才使得一个国家各项工作的稳定运行。除此之外，密码技术还渗透了人们生活的方方面面，如电子邮件、政府信息上网、网上招生录取、网上购物、网络银行、数字化网络电视、网络远程教育、远程医疗诊断等。到21世纪，已经有几百种信息加密算法被公开发表，但是与此同时，也有多种的密码破解方法在不断地被开发，如唯密文攻击法、已知明文攻击法和选择密文攻击法等。密码技术按照不同的分类标准，有着不同类型的算法。按照加密密钥进行分类，包括对称密码算法和非对称密码算法；按照明文处理方式进行分类，包括序列密码和分组密码。其中，对称密码算法又被称为私钥算法，即对网络信息进行加密和解密的密钥是同一个，目前可以排得上名的私钥算法主要集中在欧美国家，如美国的DES（data encryption standard）及其各种变形Triple DES、GDES、NewDES，欧洲的IDEA，日本的FEAL-N、LOKl-91、Skipjack、RC4、RC5等。与此相对应，非对称密码算法被称为公钥算法，即进行加密和解密的网络信息所使用的密钥是两个完全不同的密钥，正所谓“丁是丁，卯是卯。”与私钥算法相比，公钥系统具备的安全性更高，因为即使掌握了其中一个密码，也无法破解另一个。比较著名的公钥密码系统有RSA密码系统、椭圆曲线密码系统ECC、背包密码系统、McEliece密码系统、Diffe-Hellman密码系统、零知识证明的密码体制和ELGamal密码等。

在“密码管理”方面主要讨论密码的生成、空间基础；非线性密钥空间可假定能将选择的算法加入到防篡改模块中，要求有特殊保密形式的密钥，从而使能偶然碰到正确密钥的可能性降低；在密钥发送时需要分成许多不同的部分，然后用不同的信道发送，即使截获者能收集到密钥，仍可保证密钥安全性；密钥验证需要根据信道类型判断是发送者传送、发送、验证、更新、存储密钥的管理机制。密钥更新可采用从旧密钥中产生新密钥的方法，改变加密数据链路的密钥。

3. 数字签名与认证技术

随着Internet的发展与应用的普及，除了需要保护用户通信的私有性和秘密性，使非法用户不能获取、读懂通信双方的私有信息和秘密信息之外，还需要在许多应用中保证通信双方的不可抵赖性和信息在公共信道上传输的完整性。数字签名（digital signatures，DS）、身份认证和信息认证等技术可以解决这些问题。

1976年，惠特菲尔德迪菲（Whitfield Diffie）和马丁赫尔曼（Martin Hellman）联合发表论文，第一次提出数字签名的概念。论文的主旨内容是指电子文本的不可抵赖性，即文件的使用者需要像在纸质文件上一样，进行签名和身份认证，这样就保证了电子文件的不可否认性。通常的电子文件是由数据单元组成的，在此基础上，添加一些附带的数据，或者直接利用密码转换处理原数据单元，以此保证电子文件所储存的信息的安全，并且确保该电子文件的有关人员不能否认经过数字签名后的文件的正式性，同时避免文件被仿冒。可以说，数字签名是对网络信息的一种不可抵赖的认证，所具有的签名信息可以通过互联网进行传送。

数字签名是在密码技术的基础上进一步发展得到的，主要运用公钥密码算法和私钥密钥算法，其中，公钥密码算法是数字签名的主要应用方面，具体可以分为普通数字签名和特殊数字签名。普通数字签名算法有椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等。

在现代商务活动中，很多的贸易交往都开始使用电子合同，应用在互联网的虚拟环境中的数字签名就显得尤为重要。因为这是身份认证的主要标志之一，在进行商业交易时，数字签名有着和在纸质合同上亲笔签名一样的法律效力（具体可以参照《中华人民共和国电子签名法》）。因此，站在法律的角度上严格限制数字签名具有非常重要的意义。例如，在有限域上，关于离散对数问题，美国联邦政府在自己国家统一制定了数字签名的标准。与加密邮件技术不同，对信息进行加密时的公钥通过数字签名技术能够很方便获得，但是其私钥被要求严格保管。数字签名所使用的系统集合硬件、软件设备，较为规范和严谨。已经被署名的文件，可以很容易地；对其进行身份识别，使得这些文件的真实性、可靠性以及不可否认性得到了保证。数字签名技术将现代商务的办公模式逐渐向无纸化转移，这不仅极大地提高了工作效率，也使得企业整体运行成本大幅降低。可以说，数字签名技术给人们的生活，尤其是在经济活动上，带来了极大的便利，改变了人们以往的生活方式。

在现代生活中，当人们在办理住宿、求职、银行存款等时，通常要出示自己的身份证来证明自己的身份。但是，如果警察要求你出示身份证以证明你的身份，按照规定，警察必须首先出示自己的证件来证明自身的身份。前者是一方向另一方证明身份，而后者则是对等双方相互证明自己的身份。网络信息认证技术是网络信息安全技术的一个重要方面，它用于

保证通信双方的不可抵赖性和信息的完整性。在Internet深入发展和普遍应用的时代，网络信息认证显得十分重要。例如，人们在互联网上进行电子商务交易时，具体的交易内容可能没有完全保密的必要，但是对于进行整个商业活动的双方人员来说，商务信息的发送者必须确认对方已经接收到完整的，没有被窃取、篡改或替换的原始文件，这不仅仅是进行贸易活动的双方的经济利益的问题，更重要的是涉及网络信息在传输过程中是否安全。

用户与互联网主机之间进行的身份认证是目前最为常用的网络认证之一，其身份认证措施基本都是根据具体的互联网使用者自己设定的，如口令、密码、印章、信用卡、指纹、声音等。

为解决因特网的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的因特网安全解决方案，即目前被广泛采用的公钥基础设施（public key infrastructure，PKI）。PKI是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。用户可利用PKI平台提供的服务进行安全的电子交易、通信和互联网上的各种活动。PKI技术采用证书管理公钥，通过第三方的可信任机构——证书授权（Certificate Authority，CA）认证中心把用户的公钥和用户的其他标识信息捆绑在一起，在互联网上验证用户的身份。目前，通用的办法是采用建立在PKI基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。PKI是创建、颁发、管理、注销公钥证书所涉及的所有软件、硬件的集合体。其核心元素是数字证书，核心执行者是CA认证机构。

授权管理基础设施是一个综合性的系统，其集合了各种属性部件，如证书、权威、证书库等，建立在资源管理核心的基础上，统一控制互联网的访问。授权管理基础设施配置有授权机构，其具备有关资源和证书访问权限的基本功能，如产生、管理、储存、分发、撤销等。授权管理基础设施在实际应用中，可以与公钥基础设施、目录服务等集合操作，建立新型的信息保护基础设施。根据授权管理的定义，可以对认可用户建立一个特定的授权服务。与公钥基础设施不同，授权管理主要是对互联网用户开放权限，但是需要公钥基础设施提供该用户的身份信息。

4. 安全协议

计算机网络安全以保证其自身的安全为目的，主要内容包括网络设备

安全、网络系统安全和数据库安全等。网络安全协议对网络通信时，信息要求采取的格式和其所具备的含义做出了规定，即网络安全协议集合了互联网设备之间进行通信的所有规则，如网络服务器、计算机及交换机、路由器、防火墙等。互联网系统的结构通常为分层结构，即在建立完一层后才能再向上建立下一层，且相邻的两层之间，总是底下的一层服务上面的一层，但是却并不公开其具体的服务细节。因此规定了第n层协议，即不同设备之间的同一层（第n层）进行跨越式通信。由于互联网的分层结构，使得其每层的服务协议都有所差别，因此，要准确接收网络信息并能够将其识别，要求进行通信的两个层级之间具有的服务协议必须保持一致。正是这些网络协议才能使得不同计算机设备之间准确无误的传递信息。

网络安全协议就是在协议中采用了加密技术、认证技术以保证信息安全交换的安全的网络协议。它运行在计算机通信网或分布式系统中，为安全需求的各方提供一系列步骤。具体地讲，就是建立在密码体系上的一种互通协议，为需要安全的各方提供一系列的加密管理、身份认证及信息保密措施，以保证通信或者电子交易的安全完成。为了保证计算机网络环境中信息传递的安全性，促进网络交易的繁荣和发展，各种网络信息安全标准及协议应运而生，为网络信息交换提供了强大的安全保护。

常用的安全协议有安全外壳协议（secure shell orotocol，SSH）、安全套接字层协议（secure sockets layer，SSL）、安全电子交易（secure electronic transaction，SET）、网际安全协议（IP Security，IPSec）和公钥基础实施等。

5. 无线网络安全机制

无线网络就是利用无线电波作为信息传输的媒介构成的无线局域网（Wireless Local Area Networks，WAN）。与有线网络相比，无线网络的最大特点就是其传输网络信息的媒介为无线电波，并且，在实际应用中，两者可以相互补充，互为备份。在无线网络安全机制中，通常使用可以进行区域覆盖的无线局域网，其优点是网络覆盖面积大，可以跨越多维度进行信息传输。除此之外，还有点对点传输方式，对信息传输的对象要求较为准确。

在现代社会中，建立在有线网络基础上的无线网络发展迅速，已经逐渐取代了部分有线网络。无线网络具有较高的自由度，能够随时随地接入网络，进行信息传输，有效地解决了有线网络通信道路限制的问题；并且，无线网络搭配专业的辅助装备，可以最快的速度对互联网数据进行处