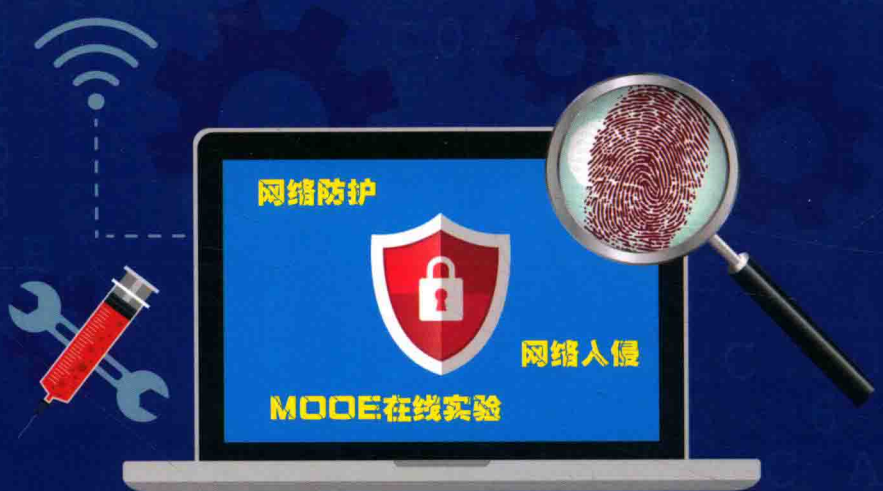
网信干部培训辅导丛书

网络安全实验培训教程

中国网络空间研究院
中国网络空间安全协会 ◎ 编著



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

网信干部培训辅导丛书

网络安全实验培训教程

中国网络空间研究院
中国网络空间安全协会 ◎ 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全实验培训教程 / 中国网络空间研究院，中国网络空间安全协会编著. -- 北京 : 人民邮电出版社，2017.1
（网信干部培训辅导丛书）
ISBN 978-7-115-44130-0

Ⅰ. ①网… Ⅱ. ①中… ②中… Ⅲ. ①网络安全－技术培训－教材 Ⅳ. ①TN915.08

中国版本图书馆CIP数据核字(2016)第289249号

内 容 提 要

本书系统介绍网络安全实践技术的层次模型和各层面的安全实验，共分 5 章，主要通过网络入侵、网络防护以及 MOOE 在线实验 3 个维度进行网络安全知识讲解。网络入侵主要包括 Metasploit 攻击、扫描攻击、木马技术、特权提升、病毒技术、网络资源消耗类攻击等实验。网络防护主要包括防火墙实验、入侵检测与防御实验、防病毒软件实验、安全防御工具实验、安全检测工具实验等。MOOE 是通过线上实验，进行网络入侵与网络防护实验，帮助有效掌握网络安全知识。

本书旨在为全国网信干部提供理论指南、实践指导和趋势指引，也可作为网络与信息安全技术学习、研究、实践、管理和渗透测试等专业人士的培训教材。

◆ 编　　著　中国网络空间研究院　中国网络空间安全协会
责任编辑　邢建春
执行编辑　肇　丽
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京隆昌伟业印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：40.5　　2017 年 1 月第 1 版
字数：986 千字　　2017 年 1 月北京第 1 次印刷

定价：198.00 元

读者服务热线：（010）81055488　印装质量热线：（010）81055316
反盗版热线：（010）81055315

序　言

2014 年 2 月，中央成立了由习近平总书记任组长的中央网络安全和信息化领导小组，统筹协调各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。习近平总书记明确指出：“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，没有网络安全就没有国家安全，没有信息化就没有现代化”“建设网络强国，要把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍”。

2015 年 6 月，“网络空间安全”成为一级学科，把网络安全人才培养提到了一个新的战略高度。2016 年 4 月，习近平总书记在网络安全和信息化工作座谈会上明确指出:“要聚天下英才而用之，为网信事业发展提供有力人才支撑。网络空间的竞争，归根结底是人才竞争”。2016 年 7 月，国家发布《国家信息化发展战略纲要》，指出：“优化人才队伍，提升信息技能。人才资源是第一资源，人才竞争是最终的竞争。要完善人才培养、选拔、使用、评价、激励机制”“全面开展国家工作人员信息化培训和考核”。

网信人才的培养受到党和国家的高度重视，网信干部不仅是网信人才的重要组成，更是推进网信事业发展的中坚力量。为了提高网信干部的业务和知识水平，加强网信干部培训工作，完善培训教材体系，中央网信办提出需要编写一系列与网络安全和信息化密切相关的培训教材，确保培训教材具备针对性、实用性、科学性、可读性，力争出精品、创特色。根据上述要求，开展了网络安全领域培训的调研工作，并组织专家编写本丛书，作为开展网信干部相关培训工作的辅导教材。

为了保证质量，对丛书做了规划，丛书的目录和大纲征求了信息安全专业教学指导委员会专家的意见，由中国网络空间安全协会秘书处负责丛书编写的组织工作，由中国网络空间研究院与中国网络空间安全协会负责编写，并以自愿申领与定向邀请相结合的方式，委托国内知名科研院所和企事业单位的专家学者参与丛书的编写和统稿工作。

衷心希望本丛书能够提高网信干部的网络安全知识水平，促进网信干部的培训工作，为推进网信人才培养和网信事业发展做出应有的贡献。

中国工程院院士 方滨兴

2016 年 8 月 23 日

前　言

当前，网络空间安全问题已成为全世界关注的热点，也是国家安全的重要部分。提升国家网络空间安全的整体实力，需要推动和普及信息安全全民教育水平。其中，学科建设是培养网络攻击安全高端专业人才的基础，把网络安全人才培养提到一个战略的高度。2015 年 6 月，为加快网络空间安全高层次人才培养，国务院学位委员会、教育部在“工学”门类下增设了“网络空间安全”的一级学科。

针对网络安全的人才培养，实践是一个非常重要的环节，目前，学习网络空间安全的现状是没有关于网络空间安全比较全面且有很强实践性的书籍。

本书特别感谢方滨兴院士，首次提出四横八纵的网络空间安全技术的领域架构，高屋建瓴地从设备层、系统层、数据层和应用层的 4 个层次，信息安全、信息保密、信息对抗、云的安全、大数据、物联网安全、移动安全和可信计算的 8 个领域，为本书建立了一套系统、完备的基础理论体系。该体系涵盖了网络安全领域的各个方面，覆盖了各层面主流的、有影响力的安全问题、技术和方法，因此，本书是一本不可多得的百科全书式的网络安全实践教材。

作为网信干部培训辅导丛书的重要教材，本书各章节是按照方滨兴院士提出来的四层模型进行组织，根据各个层面的安全问题及特点设计有针对性、有代表性的攻击和防护实验。本书共分为 5 章。第 1 章为概述部分，主要讲解网络空间安全的分层模型以及各层面的安全问题和防护技术等。第 2 章为设备安全，重点讲解网络物理层面的安全实验，包括计算机和网络设备、计算机外设以及电磁辐射等方面的验证性实验。第 3 章为系统安全，主要讲解信息系统从操作系统、域名系统、网络攻击、网络防护、网络协议以及逆向工程技术等方面的安全实验。第 4 章为数据安全，重点讲解密码编码、密码分析应用、数据库以及数据窃取等方面的安全实验。第 5 章为应用安全，讲解了信息内容安全方面，包括信息获取和信息内容分析的安全实验；讲解了 Web 安全、电子邮件服务安全以及其他典型网络服务的安全实验；针对手机安全问题，讲解了 Android 手机系统安全、手机 APP 安全、手机 APP 逆向工程分析以及移动支付等安全实验。

本书由中国网络空间研究院与中国网络空间安全协会负责编著，参与调研与编写的人员还有来自国内知名科研院所和企事业单位的专家学者。本书目录与大纲通过了信息安全专业教学指导委员会专家的咨询论证，并利用中国网络空间安全协会专家群的优势组织开展编写工作，向业界专家发出编写任务认领邀请，经遴选后委派编写工作。聘请专家对提交的稿件进行多次统稿，最终通过专家审稿会的评审。方滨兴院士对本书的整体筹划和布局给予了悉

心指导，贾焰负责本书的内容安排与组织，何慧负责本书的统稿、汇稿和主编工作，参与编写和组稿的还有副主编史建焘、季振洲、陈立章，以及其他编写人员刘君、宁宇。本书在编写过程中还得到哈尔滨工业大学张宏莉、中科院信息工程研究所崔翔、北京工业大学姜伟、北京邮电大学李蕾、哈尔滨工业大学于海宁、合天实验室刘欢迎和姚振宇等的鼎力支持，在此，对他们的工作表示衷心的感谢！

需要声明的是，本书的目的是希望帮助读者从实践层面全面了解网络安全的基本技术，以期建立起安全方面的防范意识，绝不是为怀有不良动机的人提供支持，也不承担因为技术被滥用而产生的连带责任。

本书编写过程中实验主要来源于合天实验室的 MOOE 平台，平台实验均已得到编写者的授权，如出现任何版权纠纷问题由合天实验室进行协商解决。同时，本书编写过程中参考了互联网上公布的相关资料，由于互联网上的资料较多，引用复杂，无法一一注明原出处，故在此声明，原文版权属于原作者。

由于作者水平有限，书中难免有疏漏之处，希望读者多多批评斧正，以期再版修改。

目 录

第1章 概 述

1.1 引 言

随着网络安全对国家经济及社会生活的影响日益增强，网络空间安全问题成为了重要话题。要想实现信息产业的持续健康发展，需要网络安全空间应急体系强有力的保障。当前，网络空间已经成为各个国家意识形态对抗的重要战场。中国作为国际影响越来越大的国家，正不可避免地面临来自网络空间的安全威胁。

为实施国家安全战略，加快网络空间安全人才培养，国务院学位委员会、教育部于2015年6月决定增设“网络空间安全”一级学科[1]，2015年10月决定增列“网络空间安全”一级学科博士学位授权点[2~4]，这对加快我国网络空间安全人才队伍建设和核心技术的自主创新具有重要意义。

美国有关文件对网络空间（Cyber Space）的定义是[5, 6]：“网络空间是连接各种信息技术基础设施的网络，包括互联网、各种电信网、各种计算机系统、各类关键工业设施中的嵌入式处理器和控制器，还涉及人与人之间相互影响的虚拟信息环境。”该定义强调网络空间是大范围连接的网络，这种说法有一定的局限性，导致物理隔离的网络、ad hoc网络等局域连接的网络不包含在网络空间中。

方滨兴院士给出易于公众理解的网络空间定义[7]：“网络空间是一种人造的电磁空间，以终端、计算机、网络设备等为载体，人类通过在其上对数据进行计算、通信，来实现特定的活动。在这个空间中，人、机、物可以被有机地连接在一起进行互动，可以产生相应的内容、商务、控制等影响人们生活的各类信息。”同时，从学术上，网络空间定义为：“网络空间是人类通过‘网络角色’、依托‘信息通信技术系统’进行‘信号与信息’交互的人造‘活动’空间。其中，‘网络角色’是指产生、传输信息的主体，反映的是人类的意志；‘信息通信技术系统’包括各类互联网、电信网、无线网、广电网、物联网、传感网、工控网、数字物理系统（CPS）、在线社交网络、计算系统、通信系统、控制系统等光电磁或数字信息处理设施；‘信号’是指包括光信号、量子信号、电子信号、电磁信号、生物信号等在内的各类能够用于表达、存储、加工、传输的信号形态，信号通过在信息通信技术系统中进行存储、处理、传输、展示而成

为‘信息’；‘活动’是指用户借助信息，以信息通信技术手段达到产生数据、传送信号、展示信息、修改状态等表达人类意志的行为，统称为‘信息通信技术活动’”。

一个安全模型由保护者、保护手段、破坏者、破坏手段以及被保护对象 5 个部分组成。对于信息安全模型来说，被保护对象本质是信息，但由于信息本身不是物质，必须依赖于信息载体来存储、发布、传输和加工，并且信息本身有些安全属性完全依赖于信息载体或者说信息系统的安全属性，如完整性、机密性和可用性等。因此，一直以来，信息系统的安全研究是学术界关注的重点。

但是，信息系统的安全性只能保护信息形式的真实性，即信息形式以及发布时的原始内容在信息载体上不变形地出现，强调的是信息形式在保存和复制过程中的一致性，是从保护信息形式的角度来研究的，忽略了内容安全的重要性。本书模型将内容安全纳入其中，增加依据内容来对信息的安全进行判断，强调信息内容的正确性、真实性和合法性，内容安全关注的信息是真正意义上的信息，不是信息形式也不是信息系统，而是信息发布者意欲表达的意思。就技术层面而言，信息内容安全技术的表现形式是对信息流动的选择控制能力，换句话说，表现出来的是对数据流动的攻击特性。这是本书模型的独有之处。

本书在此基础上，首先提出四横八纵的网络空间安全技术的覆盖领域[8, 9]，该体系横向上分为设备层、系统层、数据层和应用层 4 个层次，纵向上覆盖信息安全、信息保密、信息对抗、云的安全、大数据、物联网安全、移动安全和可信计算 8 个主要领域；然后，分别介绍了每个领域在不同层次所面临的安全问题及对应的安全技术；最后给出结论。

1.2 网络空间安全四层模型

网络空间中的任一信息系统或系统体系自底向上可分为设备层、系统层、数据层和应用层 4 个层次，每个层次都面临着不同的安全问题，相应地形成网络空间安全的四层次模型，如图 1-1 所示。设备层的安全对应网络空间中信息系统设备所面临的安全问题；系统层的安全对应网络空间中信息系统自身所面临的安全问题；数据层的安全对应网络空间中处理数据的同时所带来的安全问题；应用层的安全对应信息应用过程中所形成的安全问题。

图 1-1 网络空间安全的四层次模型

网络空间安全的研究领域主要包括信息安全、信息保密、信息对抗、云的安全、大数据、物联网安全、移动安全、可信计算领域，其中，信息安全是核心和根本，其他领域是信息安全向外的延伸。围绕这 8 个领域，本书归纳总结了网络空间安全的四层次模型所面临的安全

问题（如图 1-2 所示）及相应的研究领域（如图 1-3 所示）。

应用层的安全	有害信息	信息汇聚	制造舆论	恶意滥用	隐私挖掘	控制渗透	支付冒充	信誉不实
数据层的安全	信息篡改	密码破解	情报窃取	操作抵赖	数据混乱	隐私泄露	电话窃听	非法程序
系统层的安全	黑客攻击	远程木马	僵尸网络	平台攻击	运行干扰	传输干扰	传输阻塞	软件故障
设备层的安全	设施损毁	辐射泄密	电磁破坏	平台崩溃	设备失效	电子干扰	终端被攻	有害信息
	信息安全	信息保密	信息对抗	云的安全	大数据	物联网安全	移动安全	可信计算

图 1-2　网络空间安全模型中的安全问题

应用层的安全	内容安全	脱密验证	传播对抗	可控的云	服务确保	控制安全	应用安全	信任可控
数据层的安全	数据安全	新型密码	情报对抗	可信的云	数据确保	信息确保	通信安全	可信证明
系统层的安全	运行安全	网络防窃	网络对抗	安全的云	系统确保	传输安全	信道安全	软件确保
设备层的安全	物理安全	干扰屏蔽	电子对抗	可靠的云	稳定确保	探针安全	终端安全	硬件可靠
	信息安全	信息保密	信息对抗	云的安全	大数据	物联网安全	移动安全	可信计算

图 1-3　网络空间安全模型中的安全技术

1.3　面临的主要问题和技术

1.3.1　设备安全

信息安全领域在设备层主要面临物理设备损毁的安全问题。针对设备损毁问题，应当关注物理安全，物理安全是对网络与信息系统物理装备的保护，如生存性技术、容错、容灾、冗余备份技术等。

信息保密领域在设备层主要面临辐射泄密的安全问题，如侧信道攻击。电磁辐射是指计算机电子线路在运行中所出现的电平翻转形成交变电磁场，其能量形成电磁波在空间进行传播。应该关注干扰屏蔽技术，防止辐射泄密。

信息对抗领域在设备层主要面临电磁破坏的安全问题，如激光枪、高能炸弹、电磁炸弹。事实上，信息对抗是能量的对抗，具体包括维持我方使用与控制的能力、抵挡敌人阻碍我方使用的手段，以及妨碍敌人达到相同目的的方式。针对电磁破坏，应该关注电子对抗技术，如电子防护技术、电子攻击技术以及电子作战支援技术等。

云安全领域在设备层主要面临平台崩溃的安全问题，即云的不可靠性，如大规模平台宕

机、服务中断等。在设备层面实现可靠的云是物理安全灾备问题的一个实例化，可采用多副本冗余方法保证云平台的容灾性，如复云的概念——云服务商之间建立接口、互相备份、按照实际使用的情况结算。

大数据领域在设备层主要面临设备失效的安全问题。大数据的数据量大和传统意义上的数据量大是有区别的，后者要求每条数据是精准的、不可缺失的；而前者关注的是非线性的数据，数据是可缺失的。针对大数据的设备失效问题，要重点关注数据保障技术，它解决的不是传统意义上严格的灾备问题，数据不需要完全恢复，允许在不影响大数据计算的前提下，缺失某些数据。

物联网安全领域在设备层主要面临电子干扰的安全问题。物联网的物理支撑是传感器，电子电磁波干扰会造成传感器网络以及其他传输通道的安全问题。针对上述问题，应该关注物联网的探针安全技术，如干扰控制技术、安全路由技术、入侵检测技术等。

移动安全领域在设备层主要面临终端被攻击的安全问题。移动终端是移动互联网的重要载体，移动终端逐渐由通信工具向个人的信息处理中心转变，这使移动终端成为新的安全热点。移动终端的智能化，带来了非法篡改信息、非法访问、病毒和恶意代码等新的安全问题。因此，需要关注移动终端安全技术，涵盖终端自身安全性、终端防泄密和终端运行维护管理等。

可信计算领域在设备层主要面临底层设备故障引起的安全问题。为解决此问题，需要提高提供可信计算服务的硬件实体可靠性，包括元器件可靠性、设备可靠性和系统可靠性，以TPM（Trusted plateform Module）为核心提供可信硬件平台，并作为可信计算平台的信任根，建立一级信任一级的信任链。

1.3.2 系统安全

信息安全领域在系统层主要面临针对系统的黑客攻击，如安全漏洞的恶意利用、非法控制系统、系统资源消耗等。黑客攻击导致运行环境出现安全问题，因此需要研究运行安全，运行安全是指对网络与信息系统运行过程和运行状态的保护，主要涉及对网络与信息系统可控性、可用性等信息安全属性的保护，主要保护方式有风险分析、安全策略、入侵防护、入侵检测、应急响应、系统恢复等。

信息保密领域在系统层主要面临远程木马攻击所造成的网络窃密问题。网络窃密是指未经信息持有人授权，通过网络攻击手段窃取秘密信息，以达到个人目的、经济利益、政治或军事优势等。秘密信息包括个人信息、敏感信息、专有信息等。远程木马通过网络从代码的角度窃密信息，因此，在系统层应关注网络防窃技术。

信息对抗领域在系统层主要面临僵尸网络攻击问题。黑客利用蠕虫等手段在互联网中的数百到数十万台计算机上植入僵尸程序以达到暗中操控的目的，这些被操控的计算机所构成的网络被称作僵尸网络。针对僵尸网络，应该关注网络对抗技术，如基于蜜罐密网对僵尸网络监测技术、计算机网络防卫技术等。

云安全领域在系统层主要面临针对平台的攻击问题。应对云平台攻击，需要构建安全的云，保证不让用户受到外来的攻击、保证用户的信息不被外界窃取或篡改、保证用户的程序不被外界劫持，主要防护技术包括云身份认证与访问控制、云风险评估、虚拟运行环境安全等。

大数据领域在系统层主要面临运行干扰引发的安全问题。由于计算量大、数据量大，当某个计算节点中断服务时，就需要通过摆动、浮动等方式转移计算任务，此时，计算的可靠性就成为关键问题。相应地，应该关注系统确保技术，以保证大数据计算的可靠性。

物联网安全在系统层主要面临传输干扰引发的安全问题。物联网多元化、异构化网络环境加剧了数据传输环节的脆弱性，例如，针对传播环节的中间人攻击，攻击者拦截通信双方的通话，使通信的两端认为它们正在通过一个私密的连接与对方直接对话。针对传输干扰，应该关注物联网的传输安全技术防御干扰和欺骗，如安全认证技术、安全数据融合技术等。

移动安全领域在系统层主要面临传输阻塞所引发的安全问题。移动终端的通信依靠运营商的基站，攻击者可以通过攻击基站使其阻塞，进而中断基站服务，如运营商之间的拒绝服务攻击，就是向某基站大量地发送数据，将其资源占满，使其不能提供正常服务。针对上述问题，应该关注移动互联网的信道安全技术，如终端与基站之间的安全通信协议和标准等。

可信计算领域在系统层主要面临软件故障所造成的安全问题。软件故障会导致系统崩溃，为此，需要关注可信计算的软件确保技术，软件确保是使软件在受到恶意攻击的情形下依然能够继续正确运行及确保软件在授权范围内被合法使用的思想，主要技术包括软件可信建模、程序安全性分析以及软件运行监控等。软件确保由信息确保发展而来，未来将进一步发展为系统确保、服务确保，最终成为实体确保。

1.3.3　数据安全

信息安全领域在数据层主要面临数据冒充、数据篡改、数据劫持等信息篡改的安全问题。相应地，应该关注数据安全技术，数据安全是指对信息在数据收集、处理、存储、检索、传输、交换、显示、扩散等过程中的保护，保障信息在数据处理层面依据授权使用，不被非法冒充、窃取、篡改、抵赖。数据安全主要涉及对机密性、真实性、完整性、不可否认性、可用性等信息安全属性的保护。主要技术包括针对信息丢失的数据备份技术、针对信息窃取的加密保护技术、针对信息篡改的完整性检查技术、针对信息抵赖的数字签名技术、针对信息冒充的身份认证技术以及针对数据丢失的数据备份技术等。

信息保密领域在数据层主要面临通过暴力破解密码来非法侵入系统并获取私密信息等安全问题。暴力破解本质上是算法层面的对抗，常用办法有字典攻击和彩虹表，前者通过逐一尝试字典中的各种明文字符串进行密码破解，后者利用彩虹表进行散列值反查明文。针对上述安全问题，应该关注新型密码的设计和实现。

信息对抗领域在数据层主要面临情报窃取的安全问题。攻击者往往通过密码破解、绕过认证以及加密机制破解等方式达到窃取信息的目的，并最终演化为没有硝烟的情报战争。要赢得情报战争的胜利，需要关注情报对抗技术，情报对抗是指敌我双方为获取对方情报和破坏对方搜集己方情报，向对方宣传虚假信息以掩饰己方军事意图而进行的各种对抗活动，主要包括信息窃取、军事谋略、行动保密。

云安全领域在数据层主要面临操作抵赖的安全问题。为防止操作抵赖，需要建立可信的云，保证租户在云中的程序不被其他租户或云服务商所篡改和分析，保证租户在云中的数据不被其他租户或云服务商所篡改和窃取。可信云的研究可从可信云框架、数据安全、审计和权限分割等方面展开。

大数据领域在数据层主要面临数据混乱所造成的安全问题。大数据在数据层存在海量的混乱数据，有价值的数据与噪声数据混杂在一起，导致数据无法被有效利用，如网络水军散布的虚假言论。针对数据混乱问题，主要关注大数据的数据确保技术，建立数据的甄选机制，将有价值的数据从混乱的数据中区分出来，进而解决大数据的可信问题。

物联网领域在数据层主要面临隐私泄露的安全问题。相应地，应该关注物联网的信息确保技术，主要包括数据的隐私保护和访问控制技术。隐私保护是使个人或物体等实体不愿被其他人获取的隐私信息得到应有的保护，隐私信息主要包括数据信息、位置信息。访问控制是按用户身份来限制用户对某些信息的访问，或限制对某些控制功能的使用。

移动安全领域在数据层主要面临电话窃听的安全问题。电话窃听内容包括移动终端之间的音视频数据和文本数据，其本质是数据传输过程中出现的数据篡改问题。针对此问题，应该关注通信安全技术，建立端对端的安全通信。这类技术仍属于传统的信息安全技术范畴，但要考虑终端移动所带来的特殊需求，如端对端加密、身份替换等。

可信计算领域在数据层主要面临非法程序所带来的数据不可信问题。数据可信是一种观念性的概念，涉及数据来源可信、数据传输途径可信、数据处理过程可信等多个方面。要解决非法程序造成的数据不可信问题，需要关注可信证明技术，建立程序的鉴别体系，确定程序的可信性，涉及的主要技术包括加密签名技术、数据溯源技术、数据访问控制/使用控制技术等。

1.3.4 应用安全

信息安全领域在应用层主要面临有害信息传播的安全问题。有害信息包括谣言、暴力渲染、欺诈等。有害信息传播本质上是内容安全问题，因此，应该关注内容安全的相关技术。内容安全是指对信息在网络内流动中的选择性阻断，以保证信息流动的可控能力，主要涉及信息的可控性、可用性等。相关技术包括文本特征抽取、字符串匹配、信息过滤与封堵等。

信息保密领域在应用层主要面临信息汇聚所引发的信息泄露问题。攻击者通过汇聚公开发布内容，利用大数据手段从中挖掘用户隐私。针对此问题，应该关注脱密验证技术，通过归纳学习、机器学习、统计分析等方法得到数据对象间的内在特性，据此分别在数据发布层面和数据查询层面建立脱密验证体系。

信息对抗领域在应用层主要面临制造舆论的安全问题。信息对抗在应用层关注的是舆情、心理，美国称之传播对抗。中国最早称之为心理战，目前包括心理战、法律战和舆论战。为全面掌控舆情，应对新媒体引发的新问题，应该关注传播对抗技术，主要包括舆情的发现与获取、舆情的分析与引导、舆情的预警与处置等。

云安全领域在应用层主要面临云平台恶意滥用所造成的安全问题。攻击者能够利用云平台进行拒绝服务攻击、僵尸网络攻击等。针对云的恶意滥用，需要在应用层实现可控的云，即云平台不会被利用作为攻击工具，保证在云平台中的程序不是恶意程序，保证在云平台中的用户可以被追溯责任、保证在云平台中的用户没有害人的能力。可控的云涉及的主要技术包括检测和预防云上木马传播、防御云做 DDoS 攻击、防御云做有害信息传播等。

大数据领域在应用层主要面临隐私挖掘所造成的信息泄露问题。隐私泄露是大数据特性

引发的特有安全问题，大数据在应用层面临的安全问题都能够在其他领域找到。没有大数据之前，信息呈现碎片化，且相对安全。大数据的出现导致攻击者能够从海量的数据中挖掘出用户感兴趣的信息，获得更高层次的知识和规律，进而获取用户的隐私信息。针对隐私挖掘，需要关注大数据的服务确保技术，必须建立隐私保护体系，否则，大数据就是一把双刃剑。

物联网安全领域在应用层主要面临恶意渗透所造成的失控问题。物联网的核心应用是控制，物理信息系统将信息和物理环境相结合的目的就是以远程的、可靠的、实时的、安全的、协作的方式控制物理实体。工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件，通过各种方式与互联网等公共网络连接，病毒、木马等威胁正在向工业控制系统扩散。由此，应该关注物联网的控制安全技术，主要技术包括控制安全保障体系、控制安全框架模型、控制安全异常发现等。

移动安全在应用层主要面临支付冒充的安全问题。随着网购消费的快速发展，网上支付日益普及，随之而来的网上支付冒充的安全问题也备受关注。移动终端病毒或木马的侵袭、支付软件自身存在的漏洞，很可能会造成支付隐患。同时，移动支付所追求的便捷用户体验导致支付安全性的降低。针对上述问题，应该关注移动终端的应用安全技术，针对不同操作系统从应用自身和平台安全策略入手，保障应用安全。

可信计算式在应用层主要面临信誉不实所引发的安全问题。可信计算在设备层实现硬件可靠，在系统层实现软件确保，在数据层证明程序可信。那么，在应用层要解决的就是信任缺失问题，要做到信任可控，其中，应用的信任度是应用的行为表现符合主体（使用者）预期的程度，应用的可控度是主体（使用者）对应用行为表现的限制能力。由此，应该关注信任可控技术，主要包括应用级完整性保障技术、应用异常检测技术和应用信任协商技术等。

1.4　网络空间安全实验的意义

随着网络空间安全问题成为全世界关注的热点，网络安全已经成为国家安全的一部分，而提升国家网络空间安全的整体实力，需要推动和普及信息安全全民教育水平。习近平总书记在中央网络安全和信息化领导小组第一次会议当中所做的主要讲话，明确指出要培养造就世界水平的科学家、网络科技领域人才、卓越工程师和高水平的创意团队，并且还要有高素质的网络安全和信息化的人才队伍。由此，2015 年 6 月，为实施国家安全战略、加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证，国务院学位委员会学科评议组评议，报国务院学位委员会批准，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科。学科建设是培养网络攻击安全高端专业人才的基础，这样，就把网络安全人才培养提到了一个战略的高度。

在网络安全的人才培养中，实践是一个非常重要的环节，目前没有关于网络空间安全方面比较全面并实践性很强的书籍。本书是覆盖面很广的一本百科全书式的实验实践书。(1) 在设备层，本书覆盖了网络常用关键设备的安全实验。给出从计算机安全、计算机外设安全、网络设备安全以及网络环境下电磁辐射攻击等方面的精彩实验案例。通过本部分的学习可以使读者从底层了解整个安全的攻击与防护问题。(2) 针对信息系统运行中的典型安全攻击与防护技术，多角度地进行系统层面的实验组织，包括底层操作系统安全、网络协议安全、网络