信息安全系列教材

物理安全

主编 徐云峰 郭正彪

WUHAN UNIVERSITY PRESS
武汉大学出版社

信息安全系列教材

物理安全

主　编　徐云峰　郭正彪

本书的编写得到
公安部应用创新计划项目（2005yycxhbst117）、
湖北省科技攻关计划项目（2007AA301C33）的资助，
在此一并致谢！

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

物理安全/徐云峰,郭正彪主编. —武汉:武汉大学出版社,2010.2
信息安全系列教材
ISBN 978-7-307-07558-0

Ⅰ.物… Ⅱ.①徐… ②郭… Ⅲ.信息系统—安全技术—高等学校—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2010)第 002432 号

责任编辑:刘 阳 责任校对:刘 欣 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)
(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)
印刷:通山金地印务有限公司
开本:787×1092 1/16 印张:13.75 字数:338 千字
版次:2010 年 2 月第 1 版 2010 年 2 月第 1 次印刷
ISBN 978-7-307-07558-0/TP·350 定价:22.00 元

信息安全系列教材

编 委 会

何明星，西华大学数学与计算机学院副院长，教授
代春艳，重庆工商大学计算机科学与信息工程学院
陈　龙，重庆邮电大学计算机科学与技术学院，副教授
杨德刚，重庆师范大学数学与计算机科学学院
黄同愿，重庆工学院计算机学院
郑智捷，云南大学软件学院信息安全系主任，教授
谢晓尧，贵州师范大学副校长，教授

华　东

徐炜民，上海大学计算机工程与科学学院，教授
楚丹琪，上海大学教务处，副教授
孙　莉，东华大学计算机科学与技术学院，副教授
李继国，河海大学计算机及信息工程学院，副教授
张福泰，南京师范大学数学与计算机科学学院，教授
王　箭，南京航空航天大学信息科学技术学院，副教授
张书奎，苏州大学计算机科学与技术学院，副教授
殷新春，扬州大学信息工程学院副院长，教授
林柏钢，福州大学数学与计算机科学学院，教授
唐向宏，杭州电子科技大学通信工程学院，教授
侯整风，合肥工业大学计算机学院计算机系主任，教授
贾小珠，青岛大学信息工程学院，教授
郑汉垣，福建龙岩学院数学与计算机科学学院副院长，高级实验师

中　南

钟　珞，武汉理工大学计算机学院院长，教授
赵俊阁，海军工程大学信息安全系，副教授
王江晴，中南民族大学计算机学院院长，教授
宋　军，中国地质大学（武汉）计算机学院
麦永浩，湖北警官学院信息技术系副主任，教授
亢保元，中南大学数学科学与计算技术学院，副教授
李章兵，湖南科技大学计算机学院信息安全系主任，副教授
唐韶华，华南理工大学计算机科学与工程学院，教授
杨　波，华南农业大学信息学院，教授

内容提要

本书把物理安全作为信息系统安全战略的一个重要组成部分，系统地对与信息系统实体有关的威胁、缺陷和防范措施进行了具体阐述，包括物理安全概述、物理安全需要注意哪些方面以及相关的法律、法规等内容。本书分析了物理安全设计和配置方面的因素，保护设施免遭非授权访问的方法，设备和信息失窃以及保护人员、设施及其资源所需的环境和相关措施，并在此基础上针对每一个问题研究相关技术，提出预防策略，旨在建立基于物理、技术和行政等多方面有效控制的物理安全机制，构筑安全的物理网络。

序 言

21世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达50多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国40多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2006年9月19日

前 言

当今世界，高新技术的竞争已经成为综合国力竞争胜负的关键。世界各国都在充分利用信息技术特别是计算机技术和网络系统带来的巨大利益。1994 年 9 月，美国提出了建立全球信息基础设施计划的倡议，以进一步实现全球信息共享。尽管这有利于加强国际经济、科技、教育合作和文化交流，但也将成为美国等一些国家向世界各国进行经济扩张、政治渗透和文化入侵的最方便快捷的途径。再则，现在计算机犯罪日益猖獗，信息网络的安全已成为信息社会的严重问题。目前世界上已有不少国家制订了计算机间谍计划，因而，很多国家都在抓紧研究信息安全保密技术，组建信息安全保密工作机构，制定相关法规，提出信息安全保密方案和实施措施，以保护国家秘密信息的安全。为迎接高技术条件下窃密与反窃密斗争形势的挑战，应抓紧制定切实可行的对策，尽快建立起我们的信息安全防范体系，以保障我国社会主义现代化建设的顺利进行，保证在今后的国防竞争中立于不败之地。

人类的生存离不开信息，社会和经济的发展对信息资源、信息技术、信息产业的依赖程度越来越大。计算机网络的飞速发展推动着各行各业的变革。与此同时，信息安全问题也已摆到世人的面前，随着世界各地发生危及网络系统安全事件的增多，信息安全问题日益突出，受到越来越多人的关注，已成为关系国家安全的战略问题。

1996年，美国出现了两次大的互联网瘫痪事件，人们开始真正感受到信息安全的巨大威胁。著名的美国联机公司因为人为操作和技术上的失误，使其600万用户网络瘫痪10小时；另一家大公司网络联机通信服务公司的主干网出现重大故障，40万用户被迫中断联络40小时。互联网瘫痪和服务局部中断现象造成的损失已呈明显上升趋势。

目前我国的互联网络虽然不是很发达，但是却在以惊人的速度发展着。由于因特网的开放性，给国家的信息安全带来了严重威胁。随着中国上网用户的增加，上网信息的多元化，不可避免地带来了泄密隐患，增加了国内信息网络被“入侵”、被窃密的机会和可能，因而必须提高认识。要从国家安全角度重视信息安全，以保证国家通信和计算机基础的安全。

信息安全是国家工作的重要组成部分，关系着一个国家和民族的根本利益。要从国家和军队的最高利益出发，把信息安全作为一项重要工作来抓。

本书系统讲述了物理安全的内涵、产生根源以及物理安全策略，最后还整理了相关的法律、法规，为读者提供了便利。根据 GB/T 21052—2007《信息安全技术　信息系统物理安全技术要求》中对物理安全的定义和分类，本书主要从自然灾害，电、磁环境影响，物理环境影响，软硬件故障，物理攻击，管理不到位，越权或滥用等方面介绍物理安全。

本书共分七章。第一章介绍了物理安全概论，主要使读者从整体上了解物理安全；第二章介绍了物理安全中的环境安全，包括场地安全、环境安全以及人员安全；第三章主要介绍物理安全中的设备安全，主要探讨设备的安全存放以及防干扰问题；第四章介绍介质安全，主要涉及介质的分类、备份以及彻底销毁等内容；第五章主要介绍物理安全的管理制度，包括人员管理和监视设备；第六章浅谈了一下物理安全中的一些技术，包括窃取技术和隔离技

术；第七章介绍了一个机房的设置与维护，算作一个实例；最后在附录里面把与物理安全相关的评测标准介绍了一遍。

信息之间的对抗无处不在，手段也是无穷无尽。我们既要保护好核心数据，也没有必要过度保护，即保护成本与被保护目标的价值要相匹配，其中保护数据最常用也是最有效的手段就是数据备份，包括本地备份和异地备份，而这显然会不可避免地带来更多的安全难题。同时，技术无时不在进步，手段也在不断改进，这就需要信息保护者要随时了解最新的技术和产品，按实际需要来实现自己的安全策略。同时，重要的核心系统，一定要加强技术研究，包括一些反间谍手段研究，即使是一台民用的UPS，也极有可能成为敌方窃取资料的秘密武器。所以，物理安全的概念和意识，要深深融入到系统管理者的心中。

本书由徐云峰、郭正彪主编，李珂在生活上也给予了莫大的支持，在此一并感谢。

本书的最大特点就是仔细分析了物理安全的相关条文，给出了大量的例证，使读者对物理安全有了深刻的印象。内容上由浅入深，适用于从事计算机安全系统设计的工程技术人员，也可作为高校相关研究人员的教辅资料。

由于作者水平有限，书中可能会有不少谬误之处，敬请读者批评指正。

作　者

2010年1月

http://www.nirg.org

xu.lotus8340@gmail.com

目 录

第 1 章　物理安全概论

1.1　信息安全概述

1.1.1　引言

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，对于人类具有特别重要的意义。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、保密性和可靠性。

信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。但是，对于不同的部门和行业来说，对信息安全的要求和重点却是有区别的。

我国的改革开放带来了各方面信息量的急剧增加，并要求大容量、高效率地传输这些信息。为了适应这一形势，通信技术发生了前所未有的突破性发展。目前，除有线通信外，短波、超短波、微波、卫星等无线电通信也正在越来越广泛地应用。与此同时，国外敌对势力为了窃取我国的政治、军事、经济、科学技术等方面的秘密信息，运用侦察台、侦察船、卫星等手段，形成固定与移动、远距离与近距离、空中与地面相结合的立体侦察网，截取我国通信传输中的信息。

从文献中了解一个社会的内幕，早已是司空见惯的事情。在 20 世纪后 50 年中，从社会所属计算机中了解一个社会的内幕，正变得越来越容易。不管是机构还是个人，正把日益繁多的事情托付给计算机来完成，敏感信息正经过脆弱的通信线路在计算机系统之间传送：专用信息在计算机内存储或在计算机之间传送；电子银行业务使财务账目可通过通信线路查阅；执法部门从计算机中了解罪犯的前科；医生们用计算机管理病历……所有这一切，最重要的问题是不能在对非法（非授权）获取（访问）不加防范的条件下传输信息。

传输信息的方式很多，有计算机局域网、互联网和分布式数据库，有蜂窝式无线、分组交换式无线、卫星电视会议、电子邮件及其他各种传输技术。信息在存储、处理和交换过程中，都存在泄密或被截收、窃听、篡改和伪造的可能性。不难看出，单一的保密措施已很难保证通信和信息的安全，必须综合应用各种保密措施，即通过技术的、管理的、行政的手段，实现信源、信号、信息三个环节的保护，以达到秘密信息安全的目的。

电脑空间消除了国界，打破了社会和空间的界限，使信息得以迅速传递。但同时操纵和滥用计算机的行为可能产生威胁整个国家利益的严重后果。美国国家安全委员会的一份报告认为：“使用计算机键盘造成的危害，要比使用炸弹的危害严重得多。10 年前人们把保密文件锁在保险柜里，而现在这些文件都储存在计算机中。这些计算机与其他计算机形成网络系统，借助网络系统，人们可以获得小到个人的身份资料，大到每天财政流通中上百亿美元的

资产消息。人们可以用密码来保护自己的文件不被别人查看，但是对于一个诡计多端的计算机犯罪分子来说，破解密码并不比打开一把自行车锁更为困难。”目前，计算机泄密及其主要途径包括：

1. 监视与监听

计算机在信息处理与传输中，伴随着无线电信号的发射，如果配以传感器和接收机，就可以将其发射出的信号接收，经过技术处理后，转换出原有的信息，或者在电视屏幕上把接收到的电子信息转换为清晰的图像。改革开放后，我国先后从国外引进数千台大型计算机和数十亿元的软件，这些进口计算机在工作时多次发现被国外有关机构监听。如某大学引进的一台计算机，按合同规定只能用于非军事目的，有一次偶然用以计算一个军事项目时，立即被对方发现并提出严厉抗议，我国有关部门被迫作出解释。原来监听装置就隐藏在计算机的线路里，只要一工作，对方就能立刻察觉。显然，使用这种计算机根本无保密可言。美苏两国在20世纪80年代初曾开始使用一种电子计算机为主要控制手段的电磁频谱扫描装置，能够捕捉并区别各种无线电频率，从中筛选并解读各种电子信息。日本政府针对此种情况，明令政府部门一律不得使用进口计算机储存国家保密文件和重要资料。

据英国媒体1999年年末披露，美英之间有一个全球间谍网络。这个代号“梯队”的全球间谍网络位于英国北约克郡的沼泽地上，并且直接与在美国本土马里兰州的美国国家安全局连接。该全球间谍网络的能力非常大，它可以使用一个具有声音识别能力的强力计算机监视和监听世界上任何地方的电话、传真和电子邮件，并且搜集被认为是恐怖分子的证据。据一位长期调查“梯队”全球间谍网络的记者报道，美国国家安全局曾监听到一个法国公司在巴西的一项合同投标的电话，并将电话内容告诉一家美国公司，结果这家美国公司中标。这位记者说他们到处窃听和监视，是“一种完全无法无天的行为”。

2. 网上窃密

电子计算机的联网，通过联机网络检索实现信息资源共享，这是信息社会的基本特征之一，也是现代文明的重要象征。但是联机检索和资源共享也给间谍从网上窃取秘密信息提供了可乘之机。其方式是窃取或破译进入对方计算机资料库的密码或口令，好比拿到了对方保险柜的钥匙，就可堂而皇之地坐在家中的计算机终端前，随意查看自己感兴趣的情报和资料，还可通过打印机打印出来或用磁盘下载。这种窃取秘密信息的方法不容易留下痕迹，很难被人发现。美国五角大楼计算机中心与全美及世界各地的美国军事基地、科研单位以及盟国的计算机中心联网，是国防部和北约组织的大脑和神经中枢。按照规定，联网计算机对网内各级资料库的资料存储、使用、检查、调出，都必须履行严格而又繁琐的手续，然后才能获得使用的口令和保密程序。保密等级分为若干，除公共资料库外，并非任何终端机都能随意进入保密资料库。然而联邦德国的电脑工程师赫斯通过破译电脑口令打开了五角大楼电脑系统资料库的大门，并把获取的秘密出卖给了克格勃。

今天的因特网，据估计每天大约有1亿多网民在网络上访问，中国有400万网民依赖网络传递信息和沟通情报，遇到紧急情况甚至通过因特网传递商业合同、沟通谈判文件和消息。许多人没有意识到在网络上传递信息是不安全的，随时会受到他人的窥视、监听或截获信息并篡改甚至删除。但是，利益的驱使或商业需要使很多人放弃了安全保护而一味地追求高效率、快节奏，结果被别有用心者钻了空子，轻而易举地“拿到”情报或数据。他们或转手倒卖给商业谈判的对方，或直接把消息通过网络扩散出去，以达到某些个人利益或商业目的。