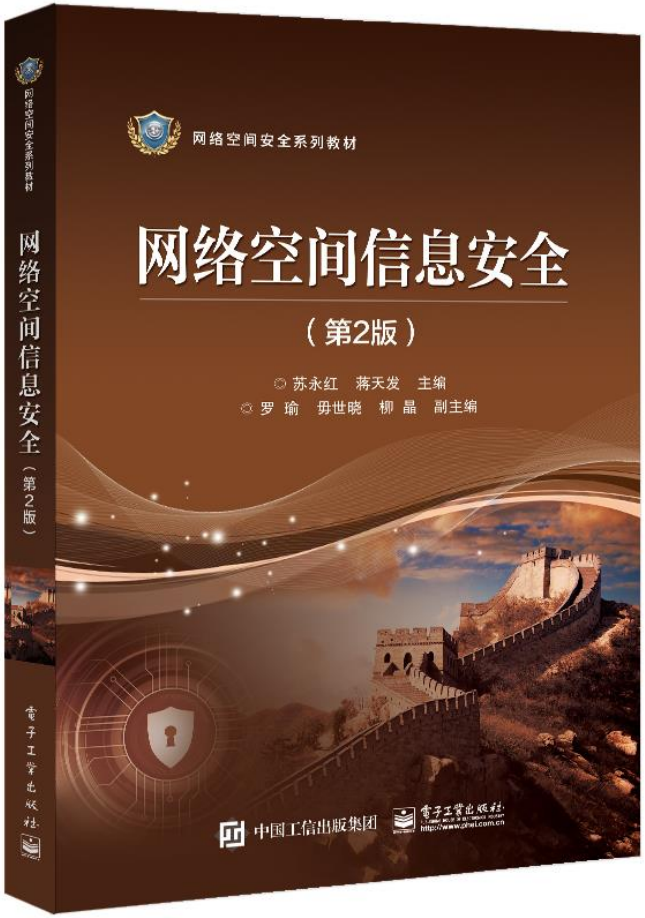
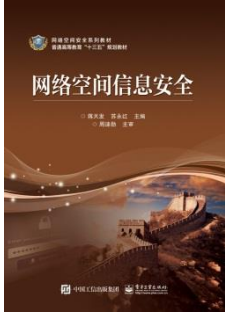
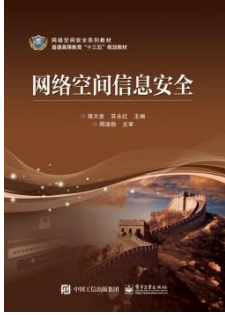
信息安全

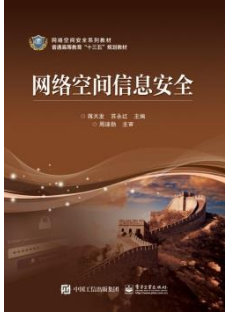

网络空间安全系列教材
网络空间信息安全
（第2版）
◎苏永红　蒋天发　主编
◎罗 瑜　毋世晓　柳 晶　副主编
中国工信出版集团
电子工业出版社


网络空间信息安全



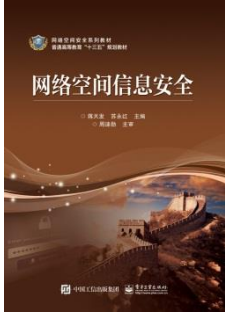
信息安全

目　录



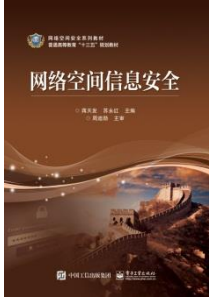
信息安全

- 第1章 网络空间信息安全概论

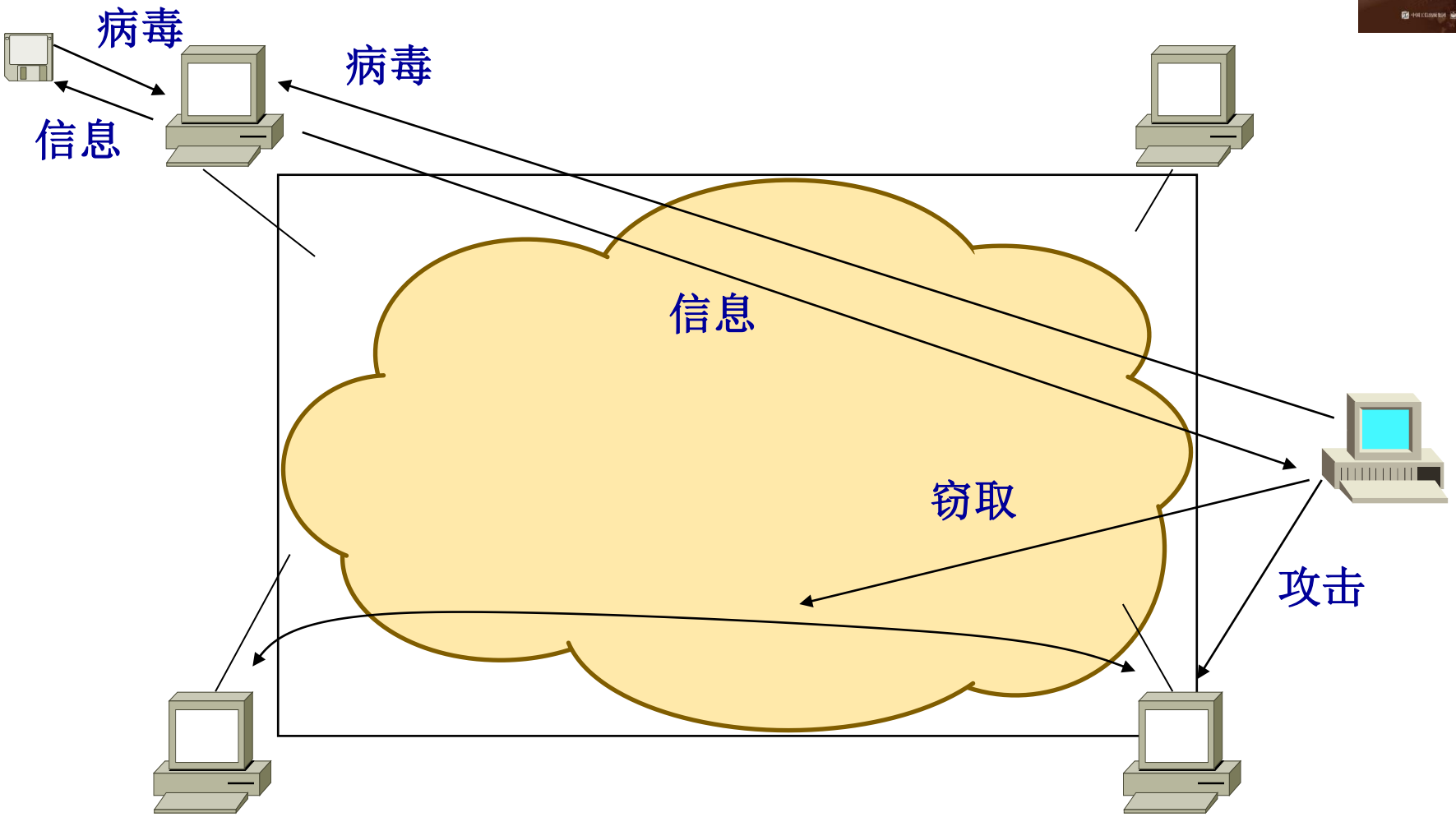


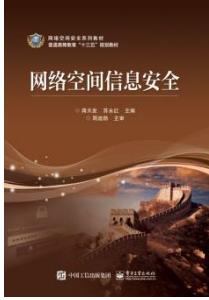
本章主要内容

- 1.1 网络空间信息安全的重要意义
- 1.2 网络空间面临的安全问题
- 1.3 网络空间信息安全的主要内容
- 1.4 信息安全网络安全网络空间信息安全的区别
- 1.5网络空间信息安全的七大趋势



信息安全和网络空间安全





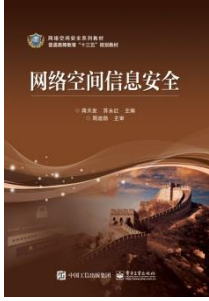
主机安全和网络安全

主机安全

- 信息不被窃取；
- 提供正常服务；
- 不感染病毒。

网络空间安全

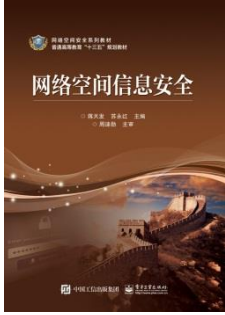
- 信息正常传输；
- 按照授权进行操作。



网络安全成为主因

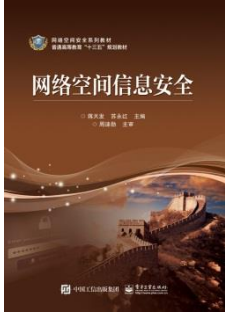
- 病毒通过网络传播；
- 通过网络瘫痪主机；
- 通过网络窃取主机信息；

网络空间成为引发主机安全问题的主要原因！



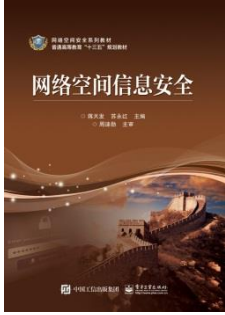
1.1 网络空间信息安全的重要意义

- 进入信息社会，信息已经成为一种非常重要的资源，它的安全与否已经影响到个人、企业甚至国家的根本利益。
- 网络空间信息安全是一个涉及网络技术、通信技术、密码技术、信息安全技术、计算机科学、应用数学、信息论等多种学科的边缘性综合学科。
- 网络空间信息安全是国家安全的重要基础。



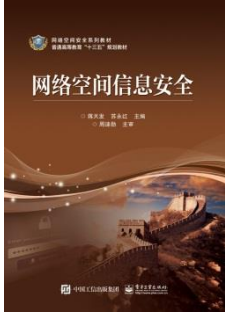
1.1 网络空间信息安全的重要意义

- 网络的快速普及与发展、客户端软件多媒体化、协同计算、资源共享、开放、远程管理化、电子商务、金融电子化等已成为网络时代必不可少的产物。
- 没有网络空间信息的安全就谈不上网络信息的安全应用。
- 计算机网络和通信是促进信息化社会发展的最活跃的因素。然而，任何事物的发展都具有二重性。



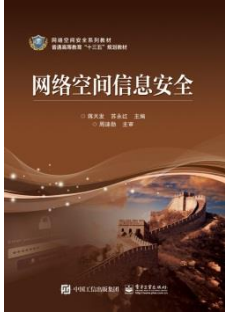
1.1 网络空间信息安全的重要意义

- 由于计算机互联网络的国际化、社会化、开放化、个性化的特点，使得它在向人们提供网络信息共享、资源共享和技术共享的同时，也带来了安全的隐患。
- 网络信息的泄漏、篡改、假冒和重传，黑客入侵，非法访问，计算机犯罪，计算机病毒传播等等对网络信息安全已构成重大威胁。
- 如果这些问题不解决，国家安全会受到威胁，电子政务、电子商务、网络银行、网络科研、远程教育、远程医疗等等都将无法正常开展起来，个人的隐私信息也得不到保障。



1.1 网络空间信息安全的重要意义

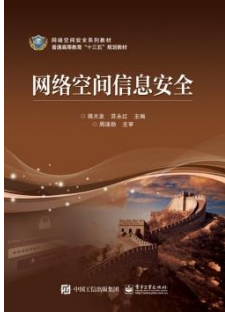
- 网络空间信息安全包括两个部分：
- 第一、防治、保护、处置包括互联网、电信网、广电网、物联网、工控网、在线社交网络、计算系统、通信系统、控制系统在内的各种通信系统及其承载的数据不受损害。
- 第二、防止对这些信息通信技术系统的滥用所引发的政治安全、经济安全、文化安全、国防安全。



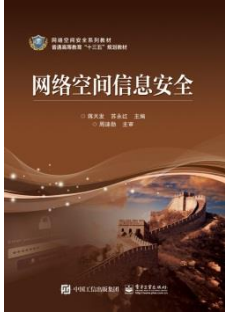
1.2 网络空间面临的安全问题

- 1.2.1 Internet安全问题
- 1.2.2 电子邮件的安全
- 1.2.3 域名系统的安全问题
- 1.2.4 IP地址的安全问题
- 1.2.5 Web站点的安全问题
- 1.2.6 文件传输的安全问题
- 1.2.7 社会工程学的安全问题

Internet安全问题

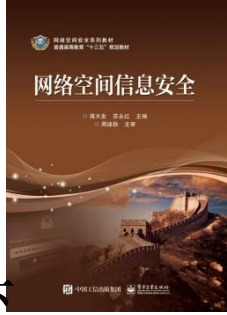


- Internet的安全来自内因和外因的各种因源：
- 1 站点主机数量的增加，无法估计其安全性能；
- 2 主机系统的访问控制配置复杂，软件的复杂等，没有能力在各种环境下进行测试；
- 3 分布式管理难于预防侵袭，一些数据库用口令文件进行分布式管理，又允许系统共享数据和共享文件，这就带来不安全因素；



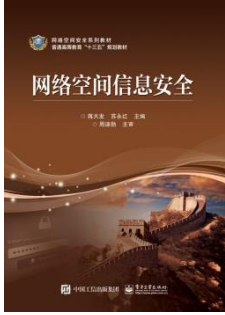
Internet安全问题

- 4 认证环节虚弱；
- 5 Internet和FTP的用户名和口令的IP包易被监视和窃取；
- 6 攻击者的主机易冒充成被信任的主机。
- 一般Internet服务安全内容包括Email安全、文件传输（FTP）服务安全、远程登陆（Telnet）安全、Web浏览服务安全和DNS域名安全、设备的物理安全以及社会工程学的安全问题。



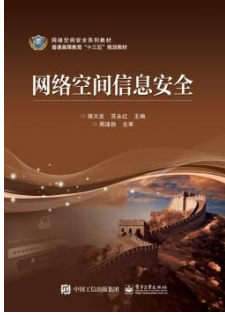
电子邮件的安全

- Email即电子邮件，是一种用电子手段提供信息交换的通信方式，也是全球网上最普及型的服务方式，数秒内通过Email传遍全球，它加速了信息交流。Email除传递信件外，还可以传送文件（当做附件），声音，图形等信息。
- Email不是“终端到终端”的实时服务，而是“存储转发式”服务，它非实时通信，而发送者可随时随地发送邮件，将邮件存入对方电子邮箱，并不要求对方接受者实时在场收发邮件，其优点是不受时空间约束。



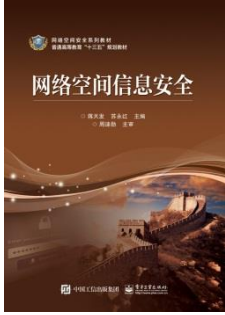
电子邮件的安全

- Email邮件系统的传输过程包括用户代理（Mail User Agent，MUA），传输代理（Mail Transfer Agent，MTA）和接受代理（Mail Delivery Agent，MDA）三部分。
- 用户代理是一个用户端发信和收发的程序。负责将信件按一定标准进行包头，然后送到邮件服务器。
- 传输代理负责信件的交换和传输，将信件传送到邮件主机，再交给接受代理。
- 接受代理按收信人的地址，根据简单邮件传输协议SMTP将信件传递到目的地。



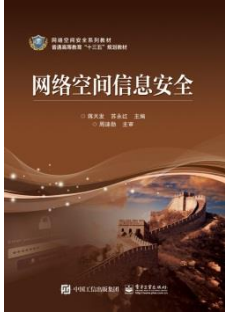
电子邮件的安全

- Email服务器是向全体开放，故有一个“路由表”，列出了其他Email服务器的目的地地址。当服务器读取信头，如果不是发给自己时，会自动转发到目的地的服务器。
  - Email的正常服务靠的是Email服务协议来保证。有这几种Email相关协议：
  - 1 SMTP协议
- SMTP（Simple Mail Transfer Protocol）是简单邮件传输协议。经过它传递的电子邮件都是以明文形式进行的，但这种明文传输很容易被中途窃取，复制或篡改。



电子邮件的安全

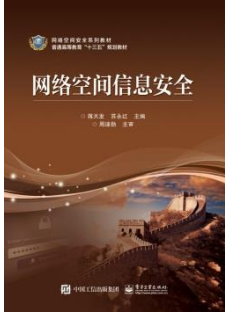
- 2 ESMTP协议
- ESMTP(Extended SMTP)是扩展型SMTP协议。主要有不易被中途截取，复制或篡改邮件的功能。
- **3 POP3协议**
- POP3（Post Office Protocol 3）协议是邮局协议，其在线工作方式，有邮件保留在邮件服务器上允许用户从邮件服务器收发邮件的功能。POP3是以用户当前存在邮件服务器上的全部邮件为对象进行操作的。并一次性将它们下载到用户端计算机中。同时用户不需要的邮件也下载了。



电子邮件的安全

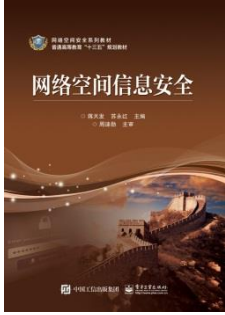
- **4 IMAP4协议**
- IMAP4（Internet Message Access Protocol）是Internet消息访问协议。为用户提供了有选择地从邮件服务器接收邮件的功能。IMAP4在用户登陆到邮件服务器之后，允许采取多段处理方式，查询邮件，用户只读取电子信箱中的邮件信头，然后再下载指定的邮件。
- **5 MIME协议**

- MIME（Maltipurpose Internet Mail Extensions）协议的功能是将计算机程序，声音和视频等二进制格式信息首先转换成ASCII文本，然后利用SMTP协议传输这些非文本的电子邮件，也可随同文本电子邮件发出。



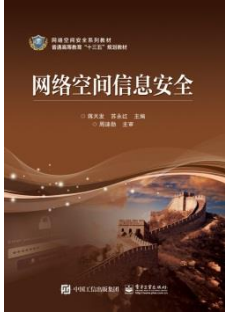
电子邮件的安全

- Email的安全漏洞有以下几种：
- （1）窃取Email；
- （2）伪造指令攻击；
- （3）Email轰炸；
- （4）Email欺骗；
- （5）虚构某人名义发出Email ；
- （6）电子邮件病毒。



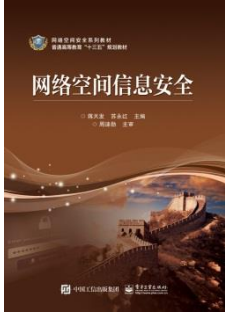
电子邮件的安全

- Email的安全措施包括这几种：
- (1) 在邮件系统中安装过滤器，在接收任何Email之前，先检查（过滤）发件人的资料，删去可疑邮件，不让它进入邮件系统。
- (2) 防止Email服务器超载，超载会降低传递速度或不能收发Email。
- (3) 如有Email轰炸或遇上Email Spamming，就要通过防火墙或路由器过滤来自这个地址的Email炸弹邮包。



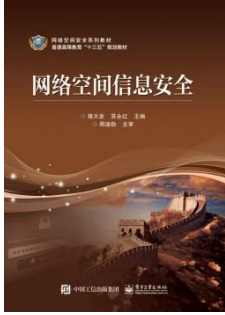
电子邮件的安全

- (4) 防止Email炸弹是删除文件或在路由的层次上限制网络的传输。
- 另一种方法是写一个Script程序，当Email连接到自己的邮件服务器时，它就会捕捉到Email炸弹的地址，对邮件炸弹的每一次连接，它都会自动终止其连接，并回复一个声明指出触犯法律。
- (5) 严禁打开Email附件中的可执行文件（.exe，com）及Word、Exel文档。因为这些多是病毒“特洛伊木马”的有毒文件。



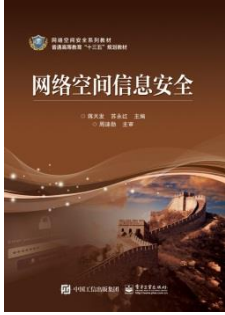
域名系统的安全问题

- 域名系统（DNS：Domain Name System）是一种用于TCP/IP应用程序的分布式数据库，它的作用是提供主机名字和地址的转换信息。
- 网络用户通过UDP协议与DNS域名服务器进行通信，而服务器在特定的53个端口监听，并返回用户所需要的相关信息，这是正向域名解析的过程，而反向域名解析是一个查询DNS的过程。当用户向一台服务器请求服务时，服务器会根据用户的IP反向解析出该IP对应的域名。



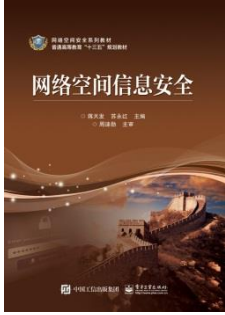
域名系统的安全问题

- 域名系统的安全威胁有这几种：
- (1) DNS会查漏内部的网络拓扑结构，故DNS存在安全隐患。整个网络架构中的主机名，主机IP列表，路由器名，路由器IP列表，计算机所在位置等可以被轻易窃取。
- (2) 攻击者控制了DNS服务器后，就会篡改DNS的记录信息，利用被篡改的记录信息达到入侵整个网络的目的,使到达原目的地的数据包落入攻击者控制的主机。



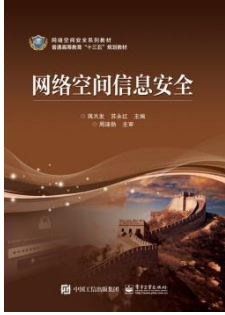
域名系统的安全问题

- (3) DNS服务器有其特殊性，在Unix中，DNS需要UDP53和TCP53的端口，它们需要使用root执行权限，这样防火墙很难控制对这些端口的访问，导致入侵者可窃取DNS服务器的管理员权限。
- (4) DNS ID欺骗行为：黑客伪装的DNS服务器提前向客户端发送响应数据报，使客户端的DNS缓存里域名所对应的IP变成黑客自定义的IP，于是客户端被带到黑客希望的网站。



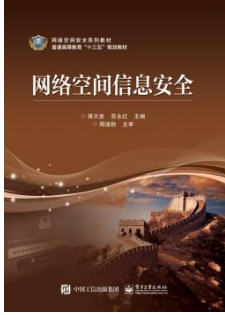
域名系统的威胁解除办法

- 遇到DNS欺骗，先禁止本地连接，然后启用本地连接就可消除DNS缓存。
- 如果在IE中使用代理服务器，DNS欺骗就不能进行，因为这时客户端并不会在本地进行域名请求。
- 如果访问的不是网站主页，而是相关子目录的文件，这样在自定义的网站上不会找到相关的文件。所以禁用本地连接，然后再启用本地连接就可以清除DNS欺骗。



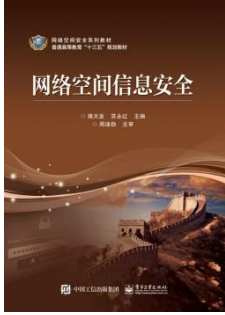
IP地址的安全问题

- IP地址的安全威胁有这几种：
- (1) 盗用本网段的IP地址，但会记录下物理地址。在路由器上设置静态ARP表，可以防止在本网段盗用IP。路由器会根据静态ARP表检查数据，如果不能对应，则不进行处理。
- (2) IP电子欺骗：IP欺骗者通过RAW Socket编程，发送带有发送伪造的源IP地址的IP数据包，让一台机器来扮演另一台机器达到的目的，获得对主机未授权的访问。即使设置了防火墙，如果没有配置对本地区域中资源IP包地址的过滤，这种IP欺骗仍然奏效。



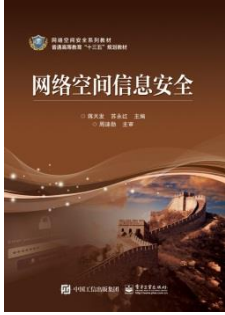
IP欺骗攻击的防备

- 有这几种办法：
- （1）通过对包的监控来检查IP欺骗。可用netlog或类似的包监控工具来检查外接口上包的情况，如发现包的两个地址，源地址和目的地址都是本地域地址，就意味有人试图攻击系统。
- （2）安装一个过滤路由器，来限制对外部接口的访问，禁止带有内部网资源地址包的通过。当然也应禁止（过滤）带有不同的内部资源地址内部包通过路由器到别的网上去，这就防止内部的用户对别的站点进行IP欺骗。
- （3）将Web服务器放在防火墙外面有时更安全。如果路由器有支持内部子网的两个接口，则易发IP欺骗。
- （4）在局部网络的对外路由器上加一个限制条件，不允许声称来自内部网络包的通过，也能防止IP欺骗。



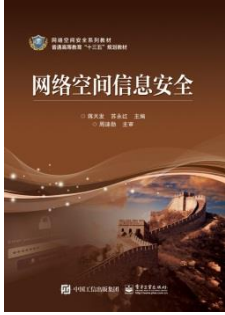
Web站点的安全问题

- Web服务器有以下安全漏洞：
- （1）安全威胁类来由渠道有以下几种：
- a.外部接口，b.网络外部非授权访问，c.网络内部的非授权访问，d.商业或工业间谍，e.移动数据；
- （2）入侵者会重点针对访问攻击某一数据库、表、目录，达到破坏数据或攻击数据的目的；
- （3）进行地址欺骗，IP欺骗或协议欺骗；
- （4）非法偷袭Web数据，如电子商务或金融信息数据；
- （5）伪装成Web站点管理员，攻击Web站点或控制Web站点主机；
- （6）服务器误认闯入者是合法用户，而允许他的访问；
- （7）伪装域名，使Web服务器向入侵者发送信息，而客户无法获得授权访问的信息。



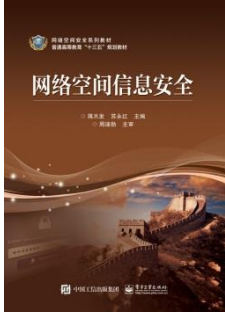
常用的Web站点安全措施

- （1）将Web服务器当作无权限的用户运行，很不安全，故要设置权限管理；
- （2）将敏感文件放在基本系统中，再设置二级系统，所有敏感文件数据都不向Internet网开放；
- （3）要检查HTTP服务器使用的Applet和脚本，尤其与客户交互作用的CGI脚本，以防止外部用户执行内部指令；
- （4）建议在Windows NT之上运行Web服务器，并检查驱动器和共享的权限，将系统设为只读状态；



常用的Web站点安全措施

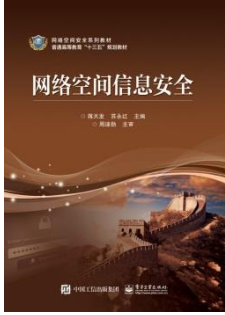
- （5）采用Macintosb Web服务器更为安全，但又缺少Windows NT的一些设置特性；
- （6）要克制daemons系统的软件安全漏洞。daemons会执行不要执行的功能，如控制服务、网络服务、与时间有关的活动以及打印服务；
- （7）为防止入侵者用电话号码作为口令进入Web站点，要配备能阻止和覆盖口令的收取机制和安全策略；



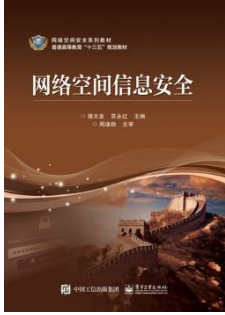
常用的Web站点安全措施

- （8）不断更新，重建和改变Web站点的连接信息，一般Web站点只允许单一种类的文本作为连接资源；
- （9）假定Web服务器放置在防火墙的后面，就可将“Wusage”统计软件装在Web服务器内，以控制通过代理服务器的信息状况，这种统计工具能列出站点上往返最频繁的用户名单；
- （10）安装在公共场所的浏览器，以防被入侵者改变浏览器的配置，并获得站点机要信息、IP地址、DNS入口号等，故要作防御措施。

文件传输（FTP）的安全问题

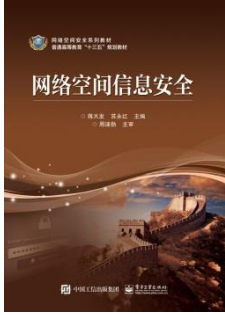


- FTP（File Transfer Protocol，文件传输协议）是提供用户在Internet网上主机之间进行收发文件的协议。FTP使用客户机/服务器模式。
- 目前，FTP的安全问题是FTP协议自身的安全问题及协议的安全功能如何扩展。安全防火墙，黑客仍有可能访问FTP服务器，故FTP存在安全问题。



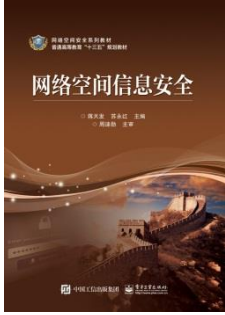
文件传输（FTP）的安全问题

- FTP的安全漏洞有这几种：
- （1）代理FTP中的跳转攻击
- 代理FTP是FTP规范PR85提供的一种允许客户端建立的控制连接，是在两台FTP服务器传输文件的机制。可以不经过中间设备直接传给客户端，再由客户端转给另一个服务器，这就减少了网络流量，但攻击者可以发出一个FTP“PORT”命令给目标FTP服务器，其中包括该被攻击主机的网络地址和与命令及服务相对应的端口号。这样，客户端就能命令FTP服务器发送数据给被攻击的服务器。



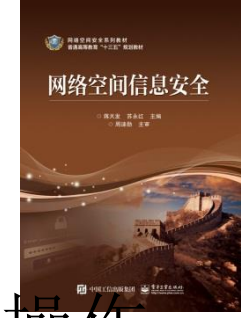
文件传输（FTP）的安全问题

- （2）FTP软件允许用户访问所有系统中的文件，且FTP文件系统存在可写区域会供攻击者删改文件。
- （3）地址被盗用（Spoof）
- 基于网络地址的访问，会使FTP服务器易受地址被盗用。
- （4）用户名和密码被猜测
- （5）端口盗用



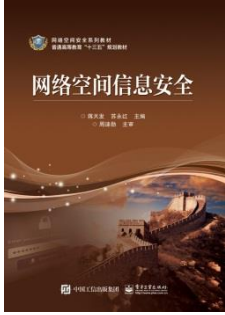
FTP的安全措施

- （1）未经授权的用户禁止进行FTP操作，FTP使用的账号必须在Password文件中有记载；并且它的口令不能为空。
- （2）保护FTP用的文件和目录
- 1）FTP\bin目录的所有者设为root；
- 2）FTP\exe目录的所有者设为root；
- 3）FTP\pub目录的所有者设为FTP；
- 4）FTP的主目录的所有者设为“FTP”。



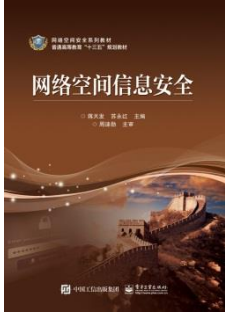
社会工程学的安全问题

- 网络信息保护中采用的技术和最终对安全系统的操作都是人来完成的。
- 所以从网络信息安全对安全策略的依赖性，已经知道保护的信息对象、所要达到的保护目标是人通过安全策略确定的。
- 因此，在网络信息安全系统的设计、实施和验证中也不能离开人，人在网络信息安全管理中占据着中心地位。特别是网络内部客户，不正确地使用系统，他可以轻而易举地跳过技术控制。



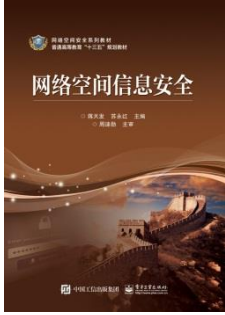
社会工程学的安全问题

- 例如，计算机系统一般是通过口令来识别用户的。如果用户输入正确的口令，则系统自动认为该用户是授权拥护。假设一个授权用户把他的用户名/口令告诉了其他人，那么非授权用户就可以假冒这个授权用户，而且无法被系统发现。
- 非授权用户攻击一个机构的网络计算机系统是危险的。而一个授权的网络内部用户攻击一个机构的网络计算机系统将更加危险。因为，内部人员对机构的计算机网络系统结构、操作员的操作规程非常清楚，而且通常还会知道足够的口令跨越安全控制，而这些安全控制已足以把外部攻击者挡在门外了。可见，内部用户的越权使用是一个非常难应对的问题。



社会工程学的安全问题

- 如果系统管理员对系统的安全相关配置上出现错误，或未能及时查看安全日志，或用户未正确采用安全机制保护信息，都将会使得机构的信息系统防御能力大大降低。还有没有培训的员工通常会给机构的信息安全带来另一种风险。
- 在一个组织机构中，对任职人员的行为进行适当的记录是一项保障网络信息安全行之有效的方法。因为，网络信息安全不仅靠要求组织和内部人员有安全技术知识、安全意识和领导层对安全的重视，还必须制定一整套明确责任，明确审批权限的安全管理制度，以及专门的安全管理机构，从根本上保证所有任职人员的规范化使用和操作。

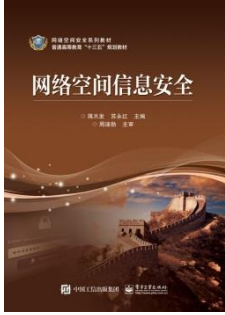


社会工程学的安全问题

- 法律会限制网络信息安全保护中可用的技术以及技术的使用范围，因此决定安全策略或选用安全机制的时候需要考虑法律或条例的规定。
- 例如，中华人民共和国国家密码管理委员会颁布的《商用密码管理条例》（1999）规定，在中国商用密码属于国家密码，国家对商用密码的科研、生产、销售和使用实行专控经营。
- 也就是说，使用未经国家批准的密码算法，或使用国家批准的算法但未得到国家授权认可的产品都属于违法行为。

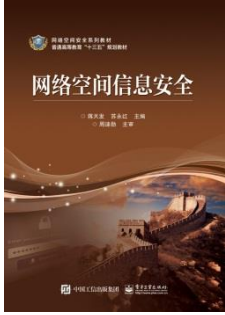
1.3 网络空间信息安全的主要内容

- 1.3.1 病毒防治技术
- 1.3.2 远程控制与黑客入侵
- 1.3.3 网络信息密码技术
- 1.3.4 数字签名与认证技术
- 1.3.5 网络安全协议
- 1.3.6 无线网络安全机制
- 1.3.7 访问控制与防火墙技术
- 1.3.8 入侵检测技术
- 1.3.9 网络数据库安全与备份技术



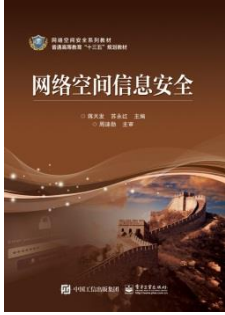
病毒防治技术

- 计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。
- 计算机病毒主要呈现以下特征：
- （1）传染性；
- （2）非授权性；
- （3）隐蔽性；
- （4）潜伏性；
- （5）破坏性；
- （6）不可预见性；
- （7）可触发性。



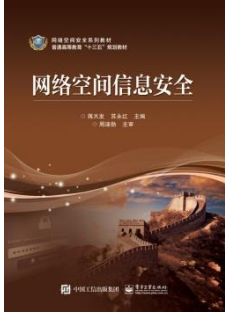
病毒防治技术

- 计算机病毒的发展呈现以下趋势：
- （1）病毒传播方式不再以存储介质为主要的传播载体，网络成为计算机病毒传播的主要载体，使用计算机网络逐渐成为计算机病毒发作条件的共同点；
- （2）传统病毒日益减少，计算机病毒变形（变种）的速度极快并向混合型、多样化发展，网络蠕虫成为最主要和破坏力最大的病毒类型；
- （3）运行方式和传播方式将更加多样化，更具隐蔽性；



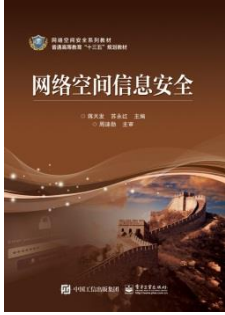
病毒防治技术

- （4）尽管目前windows10比其他版本的Windows系统安全，但随着其日益流行，它将成为黑客的主要攻击目标；
- （5）针对OS X和Unix等其他系统的病毒数量会明显增加；
- （6）跨操作系统的病毒将会越来越多；
- （7）计算机病毒技术与黑客技术将日益融合，出现带有明显病毒特征的木马或者木马特征的病毒；
- （8）物质利益将成为推动计算机病毒发展的最大动力。



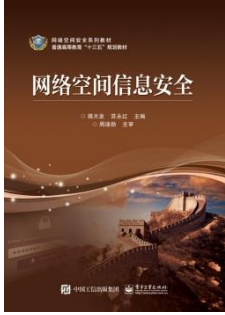
病毒防治技术

- 我们可以采取以下措施加以防范：
- （1）给计算机安装防病毒软件；
- （2）写保护所有系统盘，不要把用户数据或程序写到系统盘上，对系统的一些重要信息作备份。
- （3）尽量使用硬盘引导系统，并且在系统启动时即安装病毒预防或疫苗软件。
- （4）对公用软件和共享软件的使用要谨慎，禁止在机器上运行任何游戏盘，因游戏盘携带病毒的概率很高。
- （5）对来历不明的软件不要不经检查就上机运行。
- （6）使用套装正版软件，不使用或接受未经许可的软件。



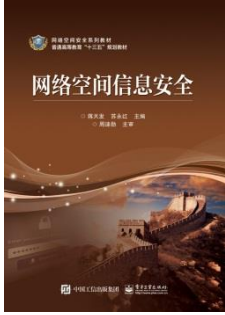
病毒防治技术

- （7）使用规范的公告牌和网络，不要从非正规的公告牌中卸载可执行程序
- （8）对已联网的微机，注意访问控制，不允许任何对微机的未授权访问。
- （9）计算机网络上使用的软件要严格检查，加强管理
- （10）不忽视任何病毒征兆，定期用杀毒软件对机器和软盘进行检测。



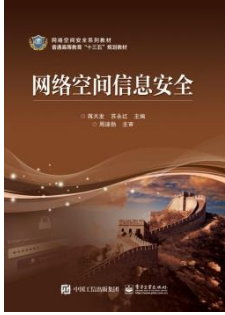
远程控制与黑客入侵

- 一般认为，计算机系统的安全威胁主要来自黑客的攻击，现代黑客从以系统为主的攻击转变为以网路为主的攻击，而且随着攻击工具的完善，攻击者不需要专业的知识就可以完成复杂的攻击过程。
- 首先是远程控制，它只是通过网络来操纵计算机的一种手段而已，只要运用得当，操纵远程的计算机也就如同你操纵眼前正在使用的计算机一样没有任何区别。



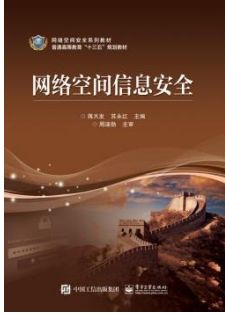
远程控制与黑客入侵

- 随着网络的高度发展，计算机的管理及技术支持的需要，远程操作及控制技术越来越引起人们的关注。远程控制一般支持下面的这些网络方式：LAN、WAN、拨号方式、互联网方式。
- 此外，有的远程控制软件还支持通过串口、并口、红外端口来对远程机进行控制。传统的远程控制软件一般使用NETBEUI、NETBIOS、IPX/SPX、TCP/IP等协议来实现远程控制。
- 随着网络技术快速的发展与普及，目前很多远程控制软件提供通过Web页面以Java技术来控制远程网络计算机。



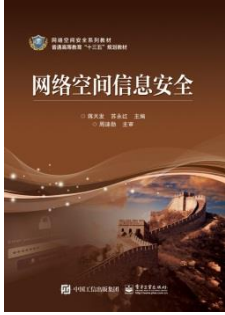
远程控制与黑客入侵

- 黑客（hacker），源于英语动词hack，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。
- 在20世纪的60至70年代之间，“黑客”(hacker)也曾经专用来形容那些有独立思考那里的计算机“迷”，如果他们在软件设计上干了一件非常漂亮的工作，或者解决了一个程序难题，同事们经常高呼“hacker”。
- 后来某些具有“黑客”水平的人物利用通讯软件或者通过网络非法进入他人系统，截获或篡改电脑数据，危害信息安全。于是“黑客”开始有了“计算机入侵者”或“计算机捣乱分子”的恶名。



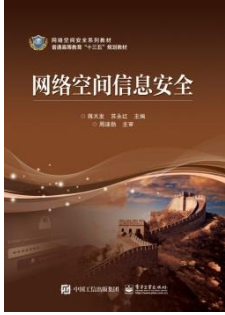
远程控制与黑客入侵

- 典型的黑客会使用如下技术隐藏他们真实的IP地址：利用被侵入的主机作为跳板；在安装Windows 的计算机内利用Wingate软件作为跳板；利用配置不当的Proxy作为跳板。
- 黑客总是寻找那些被信任的主机。这些主机可能是管理员使用的机器，或是一台被认为是很安全的服务器。
- 黑客 会检查所有运行nfsd或mountd的主机的NFS输出。往往这些主机的一些关键目录(如/usr/bin、/etc和/home)可以被那台被信任的主机mount。



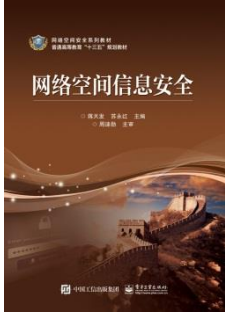
远程控制与黑客入侵

- 黑客会选择一台被信任的外部主机进行尝试。一旦成功侵入，黑客将从这里出发，设法进入内部的网络。
- 但这种方法是否成功要看内部主机和外部主机间的过滤策略了。攻击外部主机时，黑客一般是运行某个程序，利用外部主机上运行的有漏洞的daemon窃取控制权。
- 有漏洞的daemon包括Sendmail、IMAP、POP3各个漏洞的版本，以及RPC服务中诸如statd、mountd、pcnfsd等。



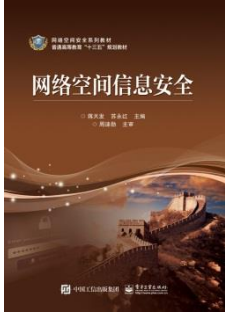
远程控制与黑客入侵

- 一旦计算机被黑客入侵，那么被入侵的计算机将没有任何秘密而言，因此我们要加强网络安全防范意识，学习掌握一些基本的安全防范措施，尽量使其免受黑客的攻击。



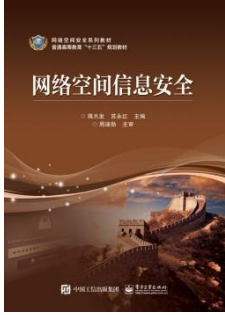
网络信息密码技术

- 网络信息密码技术是研究计算机信息加密、解密及其变换的科学，是数学和计算机交叉的一门新兴学科。
- 密码作为运用于军事和政治斗争的一种技术，历史悠久，无论是在古希腊时代还是在现代都发挥了非常重要的作用。现代密码学不仅用于解决信息的保密性，而且也用于解决信息的完整性、可用性、可控性和不可抵赖性等方面。
- 密码技术不仅在保护国家秘密信息中具有重要的、不可代替的作用，同时，也广泛应用于诸如电子邮件、政府信息上网、网上招生录取、网上购物、网络银行、数字化网络电视、网络远程教育、远程合作诊断等领域中。



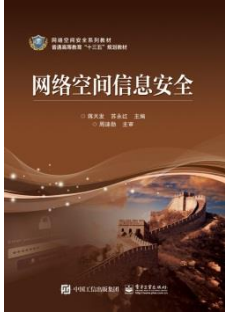
网络信息密码技术

- 密码通信模型由明文空间、密文空间、密钥空间、加密算法、解密算法五个模块组成；安全密码体制根据应用性能对网络信息提供秘密性、鉴别性、完整性、不可否认性等功能。常见密码的破解方法有唯密文攻击法、已知明文攻击法、选择文攻击法。
- 若以密钥为分类标准，可将密码系统分为对称密码(又称为单钥密码或私钥密码)和非对称密码(又称为双钥密码或公钥密码)，若以密码算法对明文的处理方式为标准，则可将密码系统分为序列密码和分组密码系统。



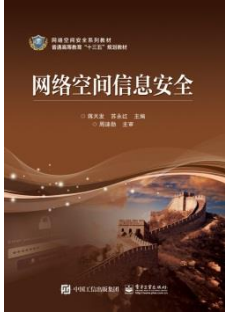
网络信息密码技术

- 在私钥密码体制中，发送方和接收方使用同一个秘密密钥，即加密密钥和解密密钥是相同或等价的。
- 除了以代换密码和转轮密码为代表的古典密码之外，比较著名的私钥密码系统有：美国的DES及其各种变形Triple DES、GDES、NewDES，欧洲的IDEA，日本的FEAL　N、LOK1　91、Skipjack、RC4、RC5等。
- 其中DES（Data Encryption Standard）为美国国家标准局（现美国国家标准与技术研究所NIST）公布的商用数据加密标准，几十年来得到了广泛的应用。



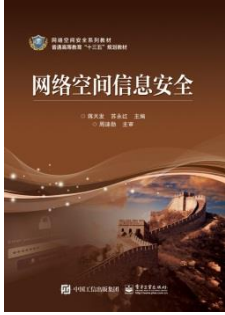
网络信息密码技术

- 对称密码体系中主要的三大密码标准：数据加密标准（DES）、高级加密标准(AES)和序列加密算法。
- 数据加密标准（DES）是20世纪70年代由IBM公司设计和修改经美国国家标准局(NBS)审阅的一种分组加密算法，即对一定大小的明文或密文进行加密或解密工作；
- 其工作模式分为：电子密码本(ECB)、密码分组链(CBC)和密码反馈(CFB)；并可以通过多次使用DES或要求多于56位的密钥进行增强安全性。



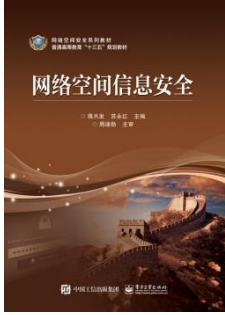
网络信息密码技术

- 高级加密标准(AES)是美国国家标准和技术委员会NIST替代DES的，并要求新算法必须允许128，192，256位密钥长度，不仅能够在128位输入分组上工作，还能在各种不同硬件上工作，速度和密码强度同样也要被重视；
- 在加密算法上AES算法密钥长度限制为128位，算法过程由10轮循环组成，每一轮循环都有一个来自于初始密钥的循环密钥，由4个基本步骤组成：字节转换、移动行变换、混合列变换、加循环密钥，而解密算法则是加密的逆过程。



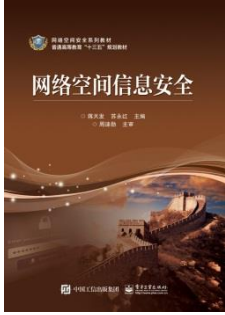
网络信息密码技术

- 在公钥密码体制中，接收方和发送方使用的密钥互不相同，即加密密钥和解密密钥不相同，加密密钥公开而解密密钥保密，而且几乎不可能由加密密钥推导出解密密钥。
- 比较著名的公钥密码系统有：RSA密码系统、椭圆曲线密码系统ECC、背包密码系统、McEliece密码系统、Diffe　Hellman密码系统、零知识证明的密码体制和ELGamal密码等。



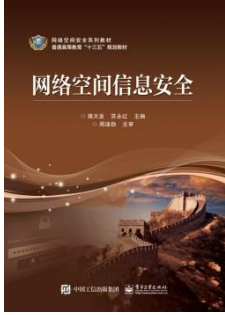
网络信息密码技术

- 理论上最为成熟完善的公钥密码体制RSA算法，以及Diffie-Hellman，Elgamal和Merkle-Hellman三种公钥体制。
- 最有影响的公钥密码体制是RSA和ECC，它们能够抵抗到目前为止已知的所有密码攻击。
- RSA密码体制的安全性是基于大整数素因子分解的困难性。ECC密码系统的安全性是基于求解椭圆曲线离散对数问题的困难性。
- ECC被认为是下一代最有前途的密码系统。



数字签名与认证技术

- 随着Internet的发展与应用的普及，一方面除了需要保护用户通信的私有性和秘密性，使得非法用户不能获取、读懂通信双方的私有信息和秘密信息之外；
- 另一方面，在许多应用中，还需要保证通信双方的不可抵赖性和信息在公共信道上传输的完整性。数字签名（Digital Signatures）、身份认证和信息认证等技术可以解决这些问题。

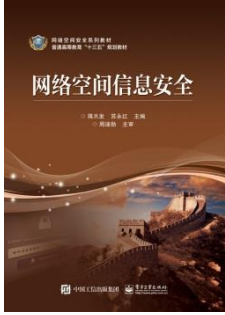


数字签名与认证技术

- 数字签名的概念最早由Whitfield Diffie和Martin Hellman于1976年提出，其目的是使签名者对电子文件也可以进行签名并且无法否认，验证者无法篡改文件。
- 简单地说，所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。
- 这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人(例如接收者)进行伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。

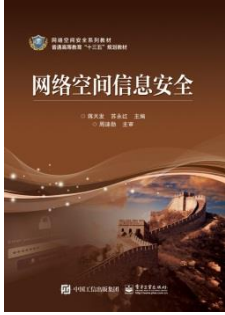
数字签名与认证技术

- Rivest、Shamir和Adleman于1978年提出了基于RSA公钥密码算法的数字签名方案；
- Shamir于1985年提出了一种基于身份识别的数字签名方案；
- Elgamal于1985年提出一种基于离散对数的公钥密码算法和数字签名方案；
- Schnorr于1990年提出了适合智能卡应用的有效数字签名方案；
- Agnew于1990年提出了一种改进的基于离散对数的数字签名方案；
- NIST于1991年提出了数字签名标准DSA；
- 1992年Scott Vanstone首先提出椭圆曲线数字签名算法ECDSA。



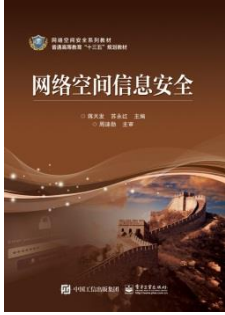
数字签名与认证技术

- 基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名。
- 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数字签名算法、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。



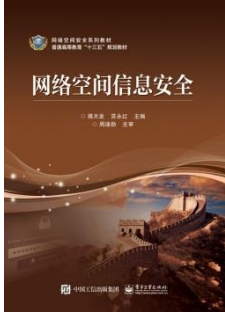
数字签名与认证技术

- 数字签名的应用过程是，数据源发送方使用自己的私钥对数据校验和或其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。



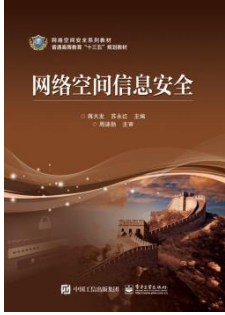
数字签名与认证技术

- 数字签名主要的功能是：保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。
- 数字签名通过一套标准化、规范化的软硬结合的系统，使持章者可以在电子文件上完成签字、盖章，与传统的手写签名、盖章具有完全相同功能。
- 主要解决电子文件的签字盖章问题，用于辨识电子文件签署者的身份，保证文件的完整性，确保文件的真实性、可靠性和不可抵赖性。



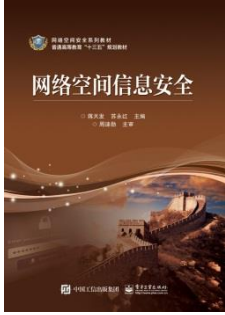
网络安全协议

- 网络协议是网络上所有设备（网络服务器、计算机及交换机、路由器、防火墙等）之间通信规则的集合，它定义了通信时信息必须采用的格式和这些格式的意义。
- 大多数网络都采用分层的体系结构，每一层都建立在它的下层之上，向它的上一层提供一定的服务，而把如何实现这一服务的细节对上一层加以屏蔽。
- 一台设备上的第n层与另一台设备上的第n层进行通信的规则就是第n层协议。在网络的各层中存在着许多协议，接收方和发送方同层的协议必须一致，否则一方将无法识别另一方发出的信息。



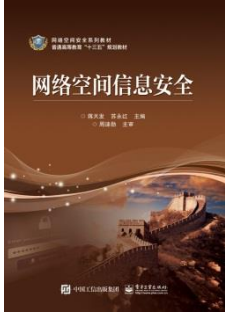
网络安全协议

- 网络安全协议具有以下三种特点：
- ①保密性：即通信的内容不向他人泄漏。为了维护人们的个人权利，因此必须确定通信内容发给所制定的人，同时还必须防止某些怀有特殊目的的人的“窃听”。
- ②完整性：把通信的内容按照某中算法加密，生成密码文件即密文进行传输。在接受端对通信内容进行破译，必须保证破译后的内容与发出前的内容完全一致。③认证性：防止非法的通信者进入。进行通信时，必须先确认通信双方的真实身份。



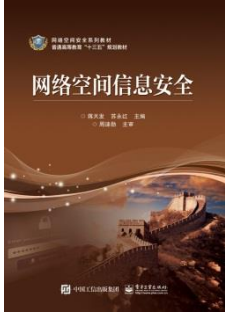
网络安全协议

- 常用的安全协议有SSH（安全外壳协议）、PKI（公钥基础设施）、SSL（安全套接字层协议）、SET（安全电子交易）、IPSec（网络协议安全）等。



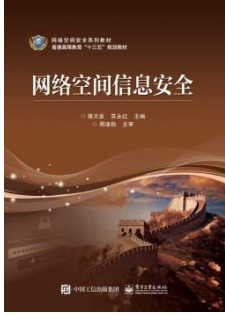
无线网络安全机制

- 所谓无线网络，就是利用无线电波作为信息传输的媒介构成的无线局域网（WLAN），与有线网络的用途十分类似，最大的不同在于传输媒介的不同，利用无线电技术取代网线，可以和有线网络互为备份。
- 目前，无线网络可分为：1无线个人网：主要用于个人用户工作空间，典型距离覆盖几米。目前主要技术包括蓝牙（Bluetooth）和红外（IrDA）。2无线局域网：主要用于宽带家庭、大楼内部以及园区内部，典型距离覆盖几十米至上百米。目前主要技术为802.11系列。3无线LAN-to-LAN网桥：主要用于大楼之间的联网通信，典型距离为几公里，许多无线网桥采用802.11b技术。4无线城域网和广域网：覆盖城域和广域环境，主要用语Internet访问，但提供的带宽比无线网络技术要低很多。



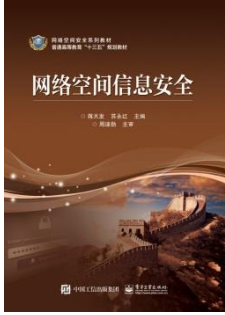
无线网络安全机制

- 目前，无线网络可分为：1无线个人网：主要用于个人用户工作空间，典型距离覆盖几米，可以与计算机同步传输文件，访问本地外围设备，如打印机等。目前主要技术包括蓝牙（Bluetooth）和红外（IrDA）。2无线局域网：主要用于宽带家庭、大楼内部以及园区内部，典型距离覆盖几十米至上百米。目前主要技术为802.11系列。3无线LAN-to-LAN网桥：主要用于大楼之间的联网通信，典型距离为几公里，许多无线网桥采用802.11b技术。4无线城域网和广域网：覆盖城域和广域环境，主要用语Internet访问，但提供的带宽比无线网络技术要低很多。



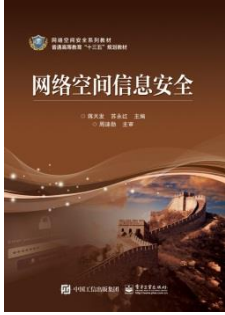
无线网络安全机制

- 在无线网络领域，常见的是IEEE 802.11标准。IEEE 802.11是IEEE最初制定的一个无线网络标准，主要用于解决办公室局域网和校园网，用户与用户终端的无线接入。
- 对不同的无线网络技术，有着不同的安全级别要求。一般地，可分为四级。第一级，扩频、跳频无线传输技术本身使盗听者难以捕捉到有用的数据。第二级，采取网络隔离及网络认证措施。第三级，设置严密的用户口令及认证措施，防止非法用户入侵。第四级，设置附加的第三方数据加密方案，即使信号被盗听也难以理解其中的内容。



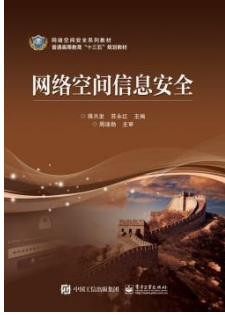
无线网络安全机制

- 针对无线网络的安全问题，采取的常见措施有：
- 第一，运用服务区标示符（SSID）。第二，运用扩展服务集标识号(ESSID)。第三，物理地址（MAC）过滤。第四，连线对等保密(WEP)。第五，虚拟专用网络(VPN)。第六，端口访问控制技术（802.1x）。



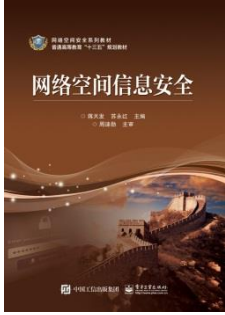
访问控制与防火墙技术

- 访问控制是通过一个参考监视器来进行的。每次用户对系统内目标进行访问时，都由它来进行调节。
- 将计算机和网络安全更紧密地统一起来，发展信息安全是非常必需的。访问控制策略尽管在这方面已取得了很大进步，却还在发展之中。为此，必须引入防火墙技术。
- 一般而言，安全防范体系具体实施的第一项内容就是在内网和外网之间构筑一道防线，以抵御来自外部的绝大多数攻击，完成这项任务的网络边防产品就是防火墙。



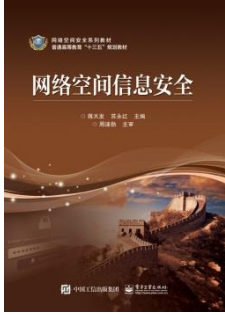
访问控制与防火墙技术

- 自从1986年美国Digital公司在Internet上安装了全球第一个商用防火墙系统后，提出了防火墙的概念，防火墙技术得到了飞速的发展。第二代防火墙，也称代理服务器，它用来提供网络服务级的控制，起到外部网络向被保护的内部网络申请服务时中间转接作用，这种方法可以有效地防止对内部网络的直接攻击，安全性较高。第三代防火墙有效地提高了防火墙的安全性，称为状态监控功能防火墙，它可以对每一层的数据包进行检测和监控。



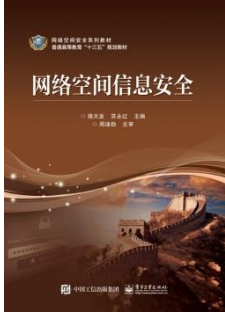
访问控制与防火墙技术

- 未来防火墙的发展趋势是：
- （1）高速化。目前防火墙一个很大的局限性是速度不够。应用ASIC、FPGA和网络处理器是实现高速防火墙的主要方法，其中以采用网络处理器最优。实现高速防火墙，算法也是一个关键，因为网络处理器中集成了很多硬件协处理单元，因此比较容易实现高速。对于采用纯CPU的防火墙，就必须有算法支撑，例如ACL算法。
- （2）多功能化。鉴于目前路由器和防火墙价格都比较高，组网环境也越来越复杂，一般用户总希望防火墙可以支持更多的功能，满足组网和节省投资的需要。
- （3）更安全。未来防火墙的操作系统会更安全。



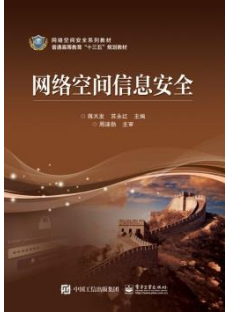
入侵检测技术

- 特征检测(Signature-based detection)又称Misuse detection，这一检测假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。它可以将已有的入侵方法检查出来，但对新的入侵方法无能为力。
- 异常检测(Anomaly detection)的假设是入侵者活动异常于正常主体的活动。根据这一理念建立主体正常活动的“活动简档”，将当前主体的活动状况与“活动简档”相比较，当违反其统计规律时，认为该活动可能是“入侵”行为。



网络数据库安全与备份技术

- 网络数据库应用是计算机的一个十分重要的应用领域。数据库系统由数据库和数据库管理系统两部分组成。安全数据库的基本要求可归纳为：数据库的完整性（物理上的完整性、逻辑上的完整性和库中元素的完整性）、数据库的保密性（用户身份识别、访问控制和可审计性）、数据库的可用性（用户界面友好，在授权范围内用户可以简便地访问数据）。



网络数据库安全与备份技术

- 当前，实现数据库安全的方案有用户身份认证、访问控制机制和数据库加密等。
- 当前的主流商品化数据库管理系统（Oracle、SyBase、Informix和Jasmine等）都支持多种验证方案。主要有基于密码的验证、基于主机的验证、基于公钥基础设施PKI（Public Key Infrastructure）的验证以及其他基于第三方组件的验证方案。

信息安全网络安全网络空间信息安全的区别

- 信息安全可泛指各类信息安全问题，网络安全可指网络所带来的各类安全问题，网络空间安全则特指与陆地空间、海洋空间、天域空间、太空空间并列的全球五大空间中的网络空间安全问题。三者均类属于非传统安全领域，都聚焦于信息安全，可以相互使用，但各有侧重；三者的概念不同，提出的背景不同，所涉及的内涵与外延不同。

信息安全网络安全网络空间信息安全的区别

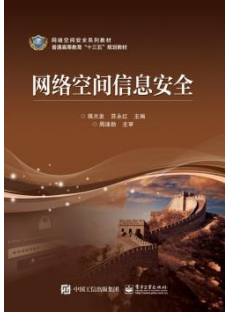
- 信息安全使用范围最广，可以指线下和线上的信息安全，既可以指称传统的信息系统安全和计算机安全等类型的信息安全，也可以指称网络安全和网络空间安全，但无法完全替代网络安全与网络空间安全的内涵；网络安全可以指信息安全或网络空间安全，但侧重点是线上安全和网络社会安全；网络空间安全可以指信息安全或网络安全，但侧重点是与陆、海、空、太空等并行的空间概念，并一开始就具有军事的性质；网络安全与网络空间安全与信息安全相比较，前两者反映的信息安全更立体、更宽域、更多层次，也更多样，更体现出网络和空间的特征，并与其他安全领域有更多的渗透与融合。

信息安全网络安全网络空间信息安全的区别

- 信息安全作为非传统安全的重要领域，以往较多地注重信息系统的物理安全和技术安全。随着信息技术的发展，先后出现了物联网、智慧城市、云计算、大数据、移动互联网、智能制造、空间地理信息集成等新一代信息技术和载体，这些新技术和新载体都与网络紧密相联，伴随着这些新技术和新载体的发展而带来的新的信息安全问题，形成了隐蔽关联性、集群风险性、泛在模糊性、跨域渗透性、交叉复杂性、总体综合性等新特点。

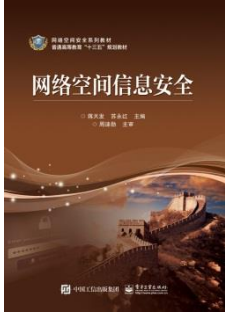
信息安全网络安全网络空间信息安全的区别

- 在网络空间，安全主体易受攻击，安全侵害迅即发生，威胁不可预知，易形成群体极化，安全主体易受攻击，安全侵害迅即发生，威胁不可预知，安全防范具有非技术性特点。如大数据在云端汇聚之后，就给网络安全带来了信息大泄露的新威胁；物联网、智慧城市、移动互联网在提供高效、泛在和便捷的同时，也使巨量的个人信息和机构数据在线上不时处于裸露的状态，为网络犯罪提供了可能。

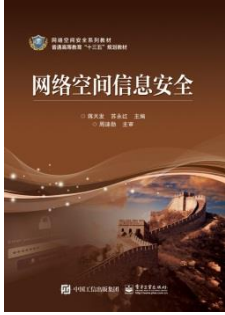


网络空间信息安全的七大趋势

- 趋势一：安全漏洞不可避免
- 趋势二：信息泄露在劫难逃
- 趋势三：攻防技术的矛与盾
- 趋势四：互联网巨头进军企业市场
- 趋势五：漏洞奖励、众测服务持续升温
- 趋势六：网络安全立法指日可待
- 趋势七：网络空间战争危及国家安全



- 思考题
- 1.1 试述网络空间信息安全的重要意义。
- 1.2 试述网络空间面临的安全问题有哪些？
- 1.3 试问计算机病毒的发展经历了哪几个阶段？
- 1.4 试问数字签名主要的功能是什么？
- 1.5 试问网络安全协议具有哪几个特点？
- 1.6 试问针对无线网络的安全问题，一般采取哪些常见措施？
- 1.7 试问未来防火墙的发展趋势怎样？
- 1.8 试问现在数字水印怎样进行分类？各分哪几类？
- 1.9 现在网络安全主要测试工具有哪几个种类？



谢谢！