21 世纪 CENTURY

高等学校计算机类专业规划教材

信息安全理论与技术

李飞　陈艾东　王敏　编著

西安电子科技大学出版社
http://www.xduph.com

面向21世纪高等学校计算机类专业规划教材

信息安全理论与技术

李飞　陈艾东　王敏　编著

西安电子科技大学出版社

内 容 简 介

本书介绍信息安全的基本概念、方法和技术，详细讲解了信息安全的基础知识、信息安全模型、当代主流的密码技术、访问控制技术、数字签名和信息认证技术、安全审计与监控技术、网络攻防技术、病毒及防范技术、信息安全体系结构以及各种安全服务及安全机制，为今后进一步学习与研究信息安全理论与技术或者从事计算机网络信息安全技术与管理工作奠定理论和技术基础。教材内容涵盖了信息安全的理论、技术与管理三大体系，有助于学生信息安全整体解决理念的形成。

本书可以作为计算机网络安全类课程的相关教材，还可以作为电子商务专业本科生相关课程的教材。

图书在版编目(CIP)数据

信息安全理论与技术 / 李飞，陈艾东，王敏编著. —西安：西安电子科技大学出版社，2010.8

面向 21 世纪高等学校计算机类专业规划教材

ISBN 978-7-5606-2439-6

Ⅰ. ①信… Ⅱ. ①李… ②陈… ③ 王… Ⅲ. ①信息系统—安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2010)第 102276 号

策　　划　李惠萍

责任编辑　李惠萍

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　　邮　　编　710071

网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com

经　　销　新华书店

印刷单位　陕西华沐印刷科技有限责任公司

版　　次　2010 年 8 月第 1 版　2010 年 8 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印　张　18.375

字　　数　430 千字

印　　数　1～3000 册

定　　价　26.00 元

ISBN 978-7-5606-2439-6/TP • 1217

XDUP 2731001-1

前　言

“信息安全理论与技术”课是计算机科学技术、网络工程、通信工程和信息安全专业本科生的专业基础必修课程。一般情况下课程安排 2.5～3 个学分，学时从 32 个学时到 48 个学时不等。但是“信息安全理论与技术”这门课程不仅要介绍信息安全学科相关的理论知识，还要介绍信息安全技术和信息安全管理体系，内容较多。因此，在教学上必须采取一些措施，才能完成大纲要求的教学任务。

目前国内大多数高校推行先进的工程教育理念，如 CDIO 工程教育理念，但许多工科学生有一个通病，即重技术轻理论。如何结合工程教育理念来教育学生，使他们明白，理论是基础，技术只是理论指导下的实现手段，没有理论作指导，技术无法达到一定的高度，这是摆在教师面前的一个巨大问题。解决不了这个问题，将无法教育出优秀的学生，也无法成为一个优秀的教育者。具体到“信息安全理论与技术”这门课程来说，首先要使学生明白系统的概念，这就要求学生能将前面先修的课程，如数学相关课程以及“C 语言程序设计”、“数据结构”、“操作系统原理”和“计算机网络”等课程的理论，与本课程有关理论知识贯穿起来，同时在讲解“信息安全体系结构”相关内容时，使学生明白仅仅一种信息安全技术是无法完成系统安全保障要求的，要有一个系统的概念，即在管理制度约束下，在信息安全相关理论指导下，将多种技术集成，才能构成一个系统安全的保障体系。没有系统的思维，单靠一门技术会给系统留下巨大的隐患。在讲解信息安全理论时，教师要注意理论的承前启后，强调理论指导技术的重要性，让学生明白利用技术做设计时，没有理论作指导，是无法完成好的设计和实现的。在学习方法上，可以预先给学生布置讲述的内容，让学生预习，分组讨论，然后请学生代表在课堂作总结，教师和学生共同点评，培养学生的表达能力、团队协作能力以及发现问题和解决问题的能力。这样，通过一门课程的教学，可以完成工程教育理念所要求的培养学生的目标。

本书的主要任务是介绍信息安全的基本概念、方法和技术，使学生掌握信息安全的基础知识、信息安全模型、当代主流的密码技术、访问控制技术、数字签名和信息认证技术、安全审计与监控技术、网络攻防技术、病毒及防范技术、信息安全体系结构以及各种安全服务及安全机制，为今后进一步学习与研究信息安全理论与技术或者从事计算机网络信息安全技术与管理工作奠定理论和技术基础。书中的内容涵盖了信息安全的理论、技术与管理三大体系，有助于学生信息安全整体解决理念的形成。

本书可以作为计算机类专业、通信工程专业及信息安全专业计算机网络安全类课程的相关教材，还可以作为电子商务专业本科生相关课程的教材。

由于时间仓促，许多地方还不完善，敬请专家指正。

编　者

2010 年 4 月

目　录

第 1 章　信息安全基础知识

1.1　信息与信息的特征

信息是当今社会发展的重要战略资源，也是衡量一个国家综合国力的重要指标。对信息的开发、控制和利用已经成为国家间相互争夺的重要内容；同时，信息的地位和作用也在随着信息技术的快速发展而急剧上升，信息的安全问题也同样因此而日益突出。

信息是客观世界中各种事物的变化和特征的最新反映，是客观事物之间联系的表征，也是客观事物状态经过传递后的再现。因此，信息是主观世界联系客观世界的桥梁。在客观世界中，不同的事物具有不同的特征，这些特征给人们带来不同的信息，而正是这些信息使人们能够认识客观事物。

信息的特征如下：

- 普遍性和可识别性。
- 储存性和可处理性。
- 时效性和可共享性。
- 增值性和可开发性。
- 可控性和多效用性。

此外，信息还具有转换性、可传递性、独立性和可继承性等特征。同时，信息还具有很强的社会功能，主要表现为资源功能、启迪功能、教育功能、方法论功能、娱乐功能和舆论功能等。信息的这些社会功能都是由信息的基本特征所决定和派生的。由此可以看到保证信息安全的重要性！

1.2　信息安全与网络安全

1.2.1　信息安全的定义与特征

“安全”并没有统一的定义，但基本含义可以解释为：客观上不存在威胁，主观上不存在恐惧。

1. 信息安全的定义

“信息安全”没有公认和统一的定义，但国内外对信息安全的论述大致可以分成两大

类：一是指具体的信息系统的安全；二是指某一特定信息体系(比如一个国家的金融系统、军事指挥系统等)的安全。但现在很多专家都认为这两种定义均失之于面过窄，目前公认的“信息安全”的定义是：(一个国家的)信息化状态和信息技术体系不受外来的威胁与侵害。因为信息安全首先应该是一个国家宏观的社会信息化状态是否处于自控之下，是否稳定的问题；其次才是信息技术的安全问题。

在网络出现以前，信息安全指对信息的机密性、完整性和可控性的保护——面向数据的安全。

互联网出现以后，信息安全除了上述概念以外，其内涵又扩展到面向用户的安全——鉴别、授权、访问控制、抗否认性和可服务性以及内容的个人隐私、知识产权等的保护。

因此，在现代信息安全的体系结构中：信息安全包括面向数据的安全和面向用户的安全，即信息安全是指信息在产生、传输、处理和存储过程中不被泄露或破坏，确保信息的可用性、保密性、完整性和不可否认性，并保证信息系统的可靠性和可控性。

2. 信息安全的特征

信息安全具有这样一些特征：

(1) 保密性。保密性是指信息不泄漏给非授权的个人、实体和过程或供其使用的特性。

(2) 完整性。完整性是指信息未经授权不能被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对网络信息安全进行攻击其最终目的就是破坏信息的完整性。

(3) 可用性。可用性是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到信息及相关资产。

(4) 可控性。可控性是指授权机构对信息的内容及传播具有控制能力的特性，可以控制授权范围内的信息流向以及信息传播方式。

(5) 可审查性。可审查性指在信息交流过程结束后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

由此，信息安全应包含三层含义：

(1) 系统安全(实体安全)，即系统运行的安全性。

(2) 系统中信息的安全，即通过对用户权限的控制、数据加密等手段确保信息不被非授权者获取和篡改。

(3) 管理安全，即综合运用各种手段对信息资源和系统运行的安全性进行有效的管理。

1.2.2　网络安全的定义与特征

在网络出现以前，信息安全指对信息的机密性、完整性和可获性的保护，即面向数据的安全。互联网出现以后，信息安全除了上述概念以外，其内涵又扩展到面向用户的安全，即鉴别、授权、访问控制、抗否认性和可服务性以及内容的个人隐私、知识产权等的保护。这两者的结合就是现代的信息安全体系结构。

1. 网络安全的定义

网络安全从其本质上讲就是网络上信息的安全，指网络系统的硬件、软件及其系统中数据的安全。网络信息的传输、存储、处理和使用都要求处于安全的状态。

网络安全的定义如下：

网络安全所涉及的领域相当广泛。因为目前的公用通信网络中存在各种各样的安全漏洞和威胁。从广义上讲，凡是涉及到网络上信息的保密性、完整性、可用性和可控性等的相关技术和理论，都是网络安全所要研究的领域。

网络安全，从本质上讲就是网络上信息的安全，即网络上信息保存、传输的安全，指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。

从用户(个人、企业等)的角度来说，他们希望所涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免他人或对手利用窃听、冒充、篡改和抵赖等手段对用户的利益和隐私造成损坏和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。

从安全保密部门的角度来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，防止由于这类信息的泄露对社会产生危害，给国家造成巨大的经济损失，甚至威胁到国家安全。

从社会教育和意识形态的角度来说，网络上不健康的内容会对社会的稳定和人类的发展形成阻碍，必须对其进行控制。

由此，网络安全应包含四层含义：

(1) 运行系统安全，即保证信息处理和传输系统的安全，本质上是保护系统的合法操作和正常运行，包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，电磁信息泄露的防护等。它侧重于保证系统的正常运行，避免因系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免因电磁泄露产生信息泄露、干扰他人(或受他人干扰)。

(2) 网络上系统信息的安全，包括用口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

(3) 网络上信息传播的安全，即信息传播后的安全，包括信息过滤技术。它侧重于防止和控制非法、有害的信息进行传播后所带来的不良后果；避免公用通信网络上大量自由传输的信息失控，其本质上是维护道德、法规法则或国家利益。

(4) 网络上信息内容的安全，侧重于网络信息的保密性、真实性和完整性；避免攻击者利用系统的安全漏洞进行窃听、冒充和诈骗等有损用户利益的行为，本质上是保护用户的利益和隐私。

由此可见，网络安全与其所保护的信息对象有关，本质上是信息的安全期内保证其在网络上流动时或静态存储时不被非法用户所访问，但授权用户可以访问。

因此，网络安全的结构层次包括：物理安全、安全控制和安全服务。

2. 网络安全的特征

网络安全的主要特征如下：

(1) 保密性：指网络上的信息不泄露给非授权用户、实体或过程，或仅供合法用户使用

的特性。

(2) 完整性：指信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性，也即未经授权不能改变信息的特性。

(3) 可用性：指当需要时应能存取所需的信息，也即可以被授权实体访问并按需求使用的特性。网络环境下的拒绝服务、破坏网络和有关系统的非正常运行等都属于对可用性的攻击。

(4) 可控性：指对信息的传播及内容具有控制的能力。

因此，网络安全和信息安全研究的内容是紧密相关的，其发展是相辅相成的。但是信息安全的研究领域包括网络安全的研究领域。

1.3 安全威胁与攻击类型

在网络这个不断更新换代的世界里，网络中的安全漏洞无处不在。即便旧的安全漏洞补上了，新的安全漏洞又将不断涌现。网络攻击正是利用这些存在的漏洞和安全缺陷对系统和资源进行攻击。

目前，主要有 10 个方面的网络安全问题急需解决，分别叙述如下：

(1) 信息应用系统与网络的关系日益紧密，人们对网络的依赖性增强，因而网络安全的影响范围日益扩大，建立可信的网络信息环境已成为一个迫切的需求。

(2) 网络系统中安全漏洞日益增多，不仅技术上有漏洞，管理上也有漏洞。

(3) 恶意代码危害性高。恶意代码通过网络途径广泛扩散，其影响越来越大。

(4) 网络攻击技术日趋复杂，而攻击操作容易完成，攻击工具广为流行。

(5) 网络安全建设缺乏规范操作，常常采取“亡羊补牢”的方式进行维护，导致信息安全共享难度递增，并留下安全隐患。

(6) 网络系统有着种类繁多的安全认证方式，一方面使得用户应用时不方便，另一方面也增加了安全管理的工作难度。

(7) 国内信息化技术严重依赖国外，从硬件到软件都不同程度地受制于人。

(8) 网络系统中软硬件产品的单一性，易造成大规模网络安全事件的发生，特别是网络蠕虫安全事件的发生。

(9) 网络安全建设涉及人员众多，安全和易用性特别难以平衡。

(10) 网络安全管理问题依然是一个难题，主要存在下述问题：

* 用户信息安全防范意识不强，例如，选取弱口令，使得攻击者从远程即可直接控制主机。

* 网络服务配置不当，开放了过多的网络服务。例如，网络边界没有过滤掉恶意数据包或切断网络连接，允许外部网络的主机直接 ping 内部网主机，允许建立空连接。

* 安装有漏洞的软件包。

* 缺省配置。例如，网络设备的口令直接用厂家的缺省配置。

* 网络系统中软件不打补丁或补丁不全。

* 网络安全敏感信息泄露，例如 DNS 服务信息泄露。

* 网络安全防范缺乏体系。
* 网络信息资产不明，缺乏分类、分级处理。
* 网络安全管理信息单一，缺乏统一分析与管理平台。
* 重技术，轻管理。例如，没有明确的安全管理策略、安全组织及安全规范。

由于网络安全问题的存在，造成网络攻击技术的泛滥，目前，对计算机用户来说，最大的安全威胁主要是黑客技术和病毒技术。

1.3.1　黑客与黑客技术

1. 黑客和黑客类型

提起黑客，总是那么神秘莫测。在人们眼中，黑客是一群聪明绝顶、精力旺盛的年轻人，一门心思地破译各种密码，以便偷偷地、未经允许地打入政府、企业或他人的计算机系统，窥视他人的隐私。那么，什么是黑客呢？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”。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤指手法巧妙、技术高明的恶作剧。在日本《新黑客词典》中，对黑客的定义是“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数电脑使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”由这些定义中，我们还看不出贬义的意味。他们通常具有硬件和软件的高级知识，并有能力通过创新的方法剖析系统。“黑客”能使更多的网络趋于完善和安全，他们能够以保护网络为目的，而以不正当侵入为手段找出网络漏洞。

在麻省理工学院(MIT)中的学生通常分成两派，一是 tool，意指乖乖牌学生，成绩都拿甲等；另一则是所谓的 hacker，也就是常逃课，上课爱睡觉，但晚上却又精力充沛喜欢搞课外活动的学生。hacker 一开始并没有跟计算机有关系，不过当时 hacker 也区分等级，就如同用成绩比高低一样。真正一流的 hacker 并非整天不学无术，而是会热衷追求某种特殊嗜好，比如研究电话、铁道(模型或者真的)、科幻小说、无线电，或者是计算机。也因此后来才有所谓 computer hacker 的出现，意指计算机高手。对一个黑客来说，学会入侵和破解是必要的，但最主要的还是编程，毕竟，使用工具是体现别人的思路，而程序是自己的想法。一句话——编程实现一切。

但是到了今天，黑客一词已被用于泛指那些专门利用电脑搞破坏或恶作剧的家伙。对这些人的正确英文叫法是 cracker，有人翻译成“骇客”。hacker 与 cracker 是分属两个不同世界的族群，基本差异在于，hacker 是有建设性的，而 cracker 则专门搞破坏。对于一个骇客来说，他们只追求入侵的快感，不在乎技术，他们不会编程，不知道入侵的具体细节。

黑客和骇客根本的区别是：黑客们建设，而骇客们破坏。

黑客技术，简单地说，是对计算机系统和网络的缺陷和漏洞的发现，以及针对这些缺陷实施攻击的技术。这里说的缺陷，包括软件缺陷、硬件缺陷、网络协议缺陷、管理缺陷和人为的失误。

很显然，黑客技术对网络具有破坏能力。一个很普通的黑客攻击手段可以把世界上一些顶级的大网站轮流考验一遍，即使是如 yahoo 这样具有雄厚的技术支持的高性能商业网站，黑客都可以给他们带来经济损失。这在一定程度上损害了人们对 Internet 和电子商务的

信心，也引起了人们对黑客的严重关注和对黑客技术的思考。

目前，黑客的类型主要有如下几种：

1) 恶作剧型

这种黑客喜欢进入他人网站，以删除某些文字或图像，篡改网址、主页信息来显示自己的厉害，此做法多为增添笑话自娱或娱人。

2) 隐蔽攻击型

此类黑客躲在暗处以匿名身份对网络发动攻击，往往不易被人识破；或者干脆冒充网络合法用户，侵入网络“行黑”。

3) 定时炸弹型

这类黑客在实施攻击时故意在网络上布下陷阱，或故意在网络维护软件内安插逻辑炸弹或后门程序，在特定的时间或特定条件下，引发一系列具有连锁反应性质的破坏行动，或干扰网络正常运行，或致使网络完全瘫痪。这类黑客是企业内部的蛀虫，其危害和影响巨大，有时几乎会导致企业破产倒闭。而混在政府内的这类黑客，破坏性更大。

4) 矛盾制造型

这类黑客非法进入他人网络，修改其电子邮件的内容或厂商签约日期，进而破坏甲乙双方的交易，并借此方式了解双方商谈的报价，乘机介入其商品竞争。有些黑客还利用政府上网的机会，修改公众信息，挑起社会矛盾。

5) 职业杀手型

此种黑客以职业杀手著称，经常以监控方式将他人网站内由国外传来的资料迅速清除，使得原网使用公司无法得知国外最新资料或订单；或者将电脑病毒植入他人网络内，使其网络无法正常运行。更有甚者，进入军事情报机关的内部网络，任意修改军方首脑的指示和下级通过网络传递到首脑机关的情报，篡改军事战略部署，达到干扰和摧毁国防军事系统的目的。严重者可以导致局部战争的失败。

6) 窃密高手型

出于某些集团利益的需要或者个人的私利，这类黑客利用高技术手段窃取网络上的机密资料，甚至进一步干扰、破坏内部网的运行。有关商业秘密的情报，一旦被黑客截获，还可能引发局部地区或全球的经济危机或政治动荡。

7) 业余爱好型

这类黑客指某类计算机爱好者受到好奇心驱使，往往在技术上追求精益求精，丝毫未感到自己的行为对他人造成的影响，属于无意识攻击行为。

2. 黑客技术的传播

在百度上搜索关键词“黑客教程”，显示出的搜索结果超过几十万条，这充分说明了这样一个事实，即黑客虽黑，其传播所走的路线却一点也不黑，这不光是中国，在全球都是一个普遍的问题。黑客培训的主要传播途径是网络，这样既可以实现图文并茂的教学过程，网站和论坛制作者又可以很好地将自己隐藏在网络屏障之后。这些网站和论坛不但为学员提供大量的黑客教程，还附有大量的相关软件和脚本。

网络教程可以说是网络黑客得以延续和传承的命脉，而且编写木马、后门等恶意代码的门槛相对感染式病毒的门槛要低、技术含量少的特征也为黑客的发展和壮大提供了绝好