que
CERTIFICATION

CISSP 认证考试指南

Certified Information Systems Security Professional Training Guide

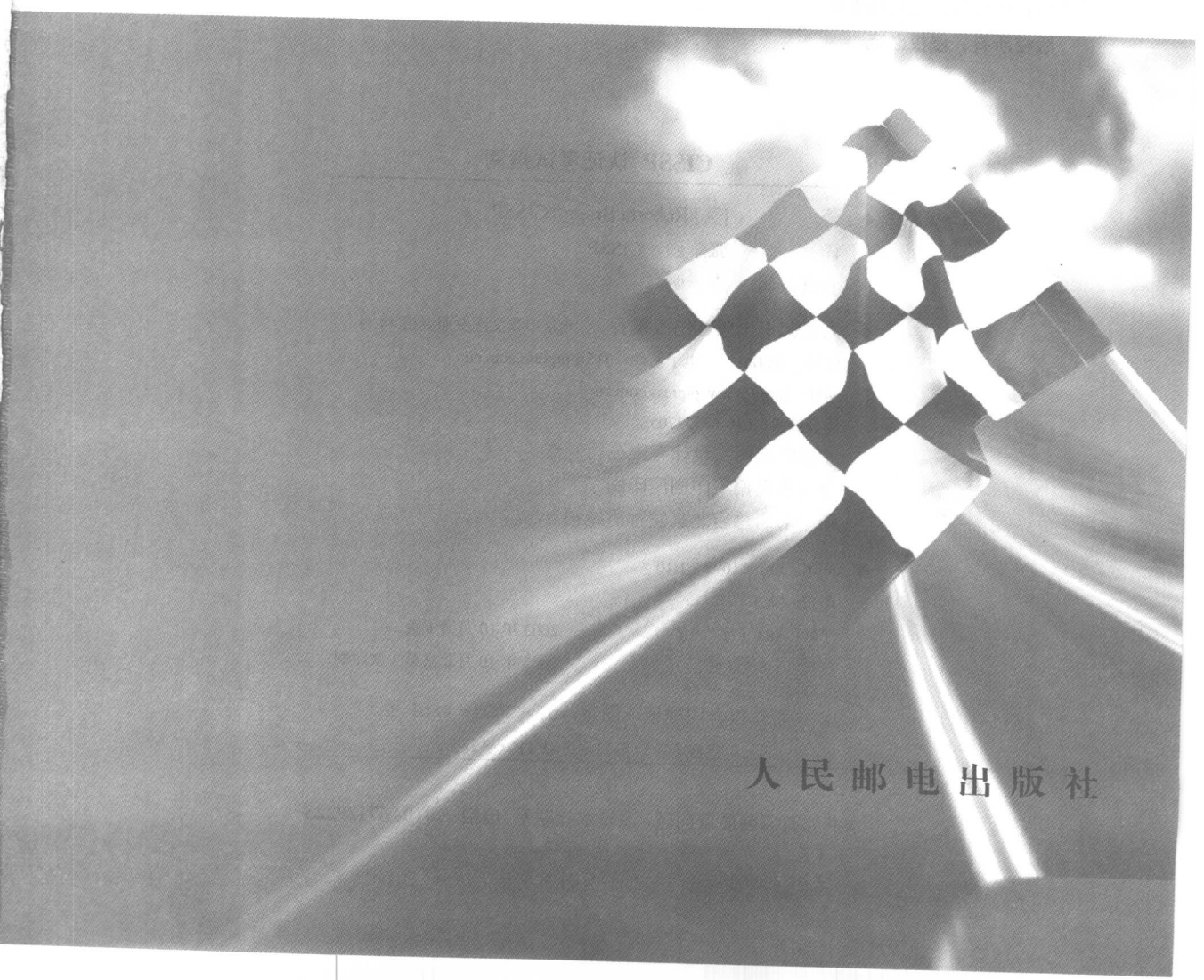
〔美〕Roberta Bragg, CISSP 著
张耀疆, CISSP 译

人民邮电出版社
POSTS & TELECOM PRESS

CISSP 认证考试指南

[美] Roberta Bragg, CISSP 著

张耀疆，CISSP 译



人民邮电出版社

图书在版编目（CIP）数据

CISSP 认证考试指南/（美）布拉格（Bragg，R.）著；张耀疆译.
—北京：人民邮电出版社，2003.10
ISBN 7-115-11568-0

I. C… II. ①布… ②张… III. 信息系统—安全技术—资格考核—自学参考资料
IV. TP309

中国版本图书馆 CIP 数据核字（2003）第 088187 号

版 权 声 明

CISSP 认证考试指南

◆ 著 [美] Roberta Bragg , CISSP
译 张耀疆，CISSP
责任编辑 李 际

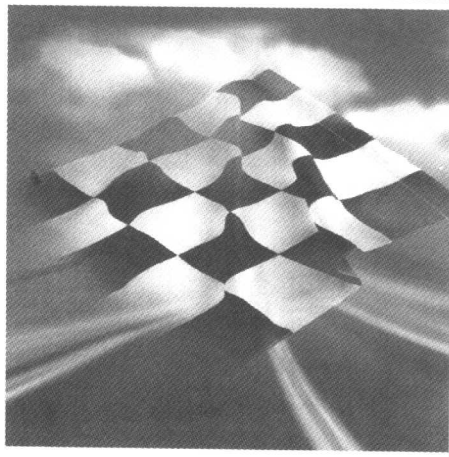
◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：36.5
字数：883 千字 2003 年 10 月第 1 版
印数：1-3 500 册 2003 年 10 月北京第 1 次印刷

著作权合同登记 图字：01－2002－4861 号
ISBN 7-115-11568-0/TP・3585

定价：78.00 元（附光盘）

本书如有印装质量问题，请与本社联系 电话：（010）67129223

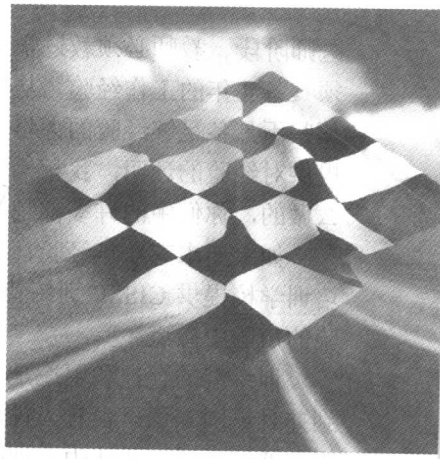


内 容 提 要

本书为通过 CISSP 认证考试提供了完整的解决方案。全书分为三大部分，第一部分是对（ISC）^{2}建立的通用知识体系（CBK）10 个知识域相关内容的详细描述，适合长时间深入而全面地学习；第二部分是对所有知识的概括和总结，适合复习和考前强化；第三部分包含了众多附录内容，包括模拟考题、应试技巧和光盘内容介绍等。

本书提供了丰富的案例，在每章的最后，都安排有场景案例的研究，一方面能够加深读者对考试内容的理解，另一方面也可以将相关知识运用到实际的工作当中。本书每一章最后都有仿真的练习题和众多资源链接，前者便于读者即刻评估自己的学习效果，后者便于追本溯源由此及彼地扩大知识掌握的范围和深度。

本书是准备 CISSP 认证考试的指南，同时也是广大信息安全专业人员不可多得的参考书。



原 书 序

追求 Paper

摘自 *Security Watch*，2002 年 6 月 3 日，星期一
作者：Roberta Bragg

不得不承认，我获得的是一个 Paper 证书。我参加了酒吧招待学校并且通过了考试，但我并没有受雇当一名招待员，也没有任何实际的经验。你们谁会相信，只凭几页纸我就有资格去接管你们本地排水通道的活儿？

这和一个 Paper MCSE 有什么不同呢？其实就是市场。参加酒吧招待学校之后，你就获得了申请某个极度渴望的位置的资格，这对那些没有多少经验的人来说是很有帮助的，当你亮出信任凭证时，其意义也就不言而喻了。

但在其他某些专业圈子里，持有 Paper 证书就不见得是什么好事了。Paper MCSE（那些通过了考试但却没有经验的人）的迅速增多已经对我们所有人造成了伤害。（不要误会我，在我的书中，即使是 Paper MCSE，只要她能走出去获得经验并且不会只凭这个 Paper 就自称是富有经验的专家，这样的人是会得到我的尊重的。）现在，我们面临一个更危险的事情：Paper CISSP。CISSP 表示信息系统安全认证专家（Certified Information System Security Professional），由（ISC）^{2}组织管理。为了获得这样的称号，你必须通过严格的考试，此外，你还要证明自己具有 4 年信息安全方面的经验并且签署一份道德声明。（更多信息可以参见 www.isc2.org 和本人的文章 http://certcities.com/editorial/exams/print.asp?EditorialsID=25。）

要取得证书，必须具备相关的经验，这种要求没什么好奇怪的。一名医生必须经过实习

医师阶段、教师必须教过学生、CPA 必须在此领域任过职。同样的道理，CISSP 的候选者必须具备 4 年的工作经验。从今年开始，每位申请者必须让一个资深人士签名以支持其声明，那些不具备足够经验的人将不允许参加考试。事实上，某些声明是要经过审查的。因为要求提供对经验的证明，我相信这个证书将会保持其价值，但不幸的是，有些学校却明显不是这么做的，你们中的许多都是这样。

如果要求有 4 年经验，那怎样才能成为 Paper CISSP？最近，我收到了这样的报告：一些培训学校提供 CISSP 训练营（bootcamp），并且鼓励参加者申请 CISSP 证书时在有关真实经验的声明中撒谎。

训练营的存在和用途是个有争议的话题，反对者声称没有人能够在如此短暂的时间内学到并且巩固知识；也有人说，对富有经验的技术人员来讲，应该利用训练营来精炼他们的知识并通过考试。我认为，训练营可能是件好事情，但也可能不是，如果它创造的是 Paper 证书，我就不看好它，但对那些有经验的人来说则是有用的。

对于这些培训中心，我的疑问在于：

- 向那些不符合 CISSP 经验要求的人发出能够获得证书的保证，实际上是一种惟利是图欺骗学生的行为。
- 降低了证书的价值，实际上是欺骗了那些合法证书的持有者。
- 所引荐的网络安全方面的工作申请者是没有做好足够准备的，实际上是欺骗了这个行业。
- 鼓励学生在填写经验表格时撒谎，并且让人签名验证这些欺骗行为，实际上欺骗的是所有的参与者。

撒谎者总会撒谎，骗子总会行骗，我们无法抓住所有这样的人，但也许我们可以天真地认为能够改变这种局面。我猜想，这正是你们——具有道德心的 IT 人所要做的。训练营公司应该停止过份的吹嘘，应该事先向学生介绍 CISSP 的要求，不要鼓励他们撒谎。人事经理应该对经验声明进行调查。如果你想找到获取安全证书的不道德的捷径，尽快收手吧，步入正途，先从获得经验开始。

够了，是时候了，让我们这些从事 IT 职业的人控制住我们的道德行为，并让其他人都知道我们遵守的是相同的标准。

转摘得到了 Security Watch *的许可（http://lists.101com.com/NLS/pages/main.asp），©2002 101 Communications，LLC。*

Roberta Bragg，MCSE，CISSP，管理着自己的公司 Have Computer Will Travel, Inc.，她是一位安全、操作系统和数据库方面的咨询专家。

CISSP 训练营：问题澄清

摘自 *Security Watch*，2002 年 8 月 12 日，星期一

作者：Marc Thompson

Roberta Bragg 在 6 月 3 日的 *Security Watch* 上表达了对 CISSP 训练营迅速增多的担心，我们也有同感。

首先，应该注意到，这些训练营与（ISC）^{2}（International Information Systems Security Certification Consortium）没有任何关系，（ISC）^{2}是管理 CISSP 认证的一个非盈利组织。还应该注意的是，（ISC）^{2}通过其教育机构即（ISC）^{2} Institute 向 CISSP 报考者提供唯一经过官方授权的培训。

此外，（ISC）^{2} Institute 有时候也会通过获准的培训伙伴来提供官方的回顾研讨会，这些培训伙伴负责组织，（ISC）^{2} Institute 提供所有的教师和课件。相关的培训程序列在（ISC）^{2}的网站上。

由此可知，（ISC）^{2}是无权阻止他人声称提供 CISSP 认证培训的。同样道理，其他允许第三方伙伴为报考者提供认证准备的 IT 培训程序也是如此，例如 Cisco 或 Microsoft。

所有的 CISSP 报考者在面对这些训练营时都应该小心行事，如果发现有人对其过去的工作经验撒谎，就像 Roberta 所说的一些训练营鼓励学生撒谎那样，他就会因为违反了 CISSP 的“道德规范（Code of Ethics）”而被取消证书，这样的道德规范在报考者参加考试之前必须签署，而且具有法律效力。

过去几年里，（ISC）^{2}采取了几项措施以减少报考者谎报工作经验的可能，包括随机审查申请，并让一个 CISSP 签署推荐（endorsement）以表示对报考者工作经验的认可，推荐人能够证明报考者关于工作经验的声明是真实的，也能证明报考者在信息安全领域具有较好的名声。

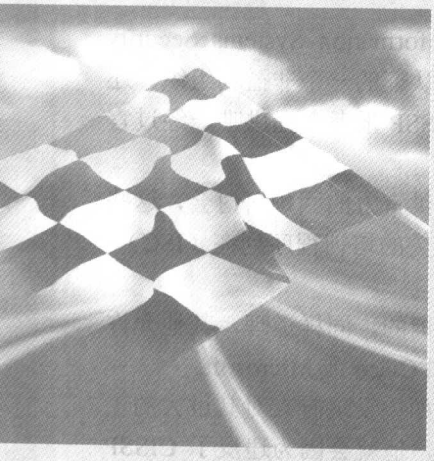
此外，如果 CISSP 报考者参加的训练营提供了来自真实测试的材料，就像某些训练营所声称的那样，报考者也会因为违反了道德规范而失去 CISSP 资格。还有就是，有些训练营声称能够提高 CISSP 考试的通过率，报考者千万别相信，事实上，作为一项策略，（ISC）^{2}从来就没有发布过考试的通过率，训练营根本就没办法去合法地保证高的通过率。

在训练营和（ISC）^{2} Institute 培训之间的关键区别在于：Institute 的目标是提高对 CBK 的广泛的概括的认识，CBK（Common Body of Knowledge）是由（ISC）^{2}编辑和不断更新的信息安全惯例和标准的纲要，是 CISSP 考试的基础。

（ISC）^{2} Institute 的教师全部是经过（ISC）^{2}培训的 CISSP，他们可以帮助 CISSP 报考者在参加考试之前对其 CBK 的 10 个知识域的掌握水平有一个充分的理解。有些 Institute 的教师具备 5 年甚至更久的培训经验，而很多训练营往往运营了才几个月。再次声明，（ISC）^{2}唯一推荐的就是 Institute 的培训。

我们希望 Roberta 和其他关心 CISSP 的人放心，（ISC）^{2}正在做着努力，确保这项证书在信息安全领域保持其金牌标准。对于她所倡导的所有 IT 专业人员都应该具备道德行为，我们表示支持。

Marc Thompson 是（ISC）^{2} Institute 的副总裁（http://www.isc2.org/）。



怎样使用本书

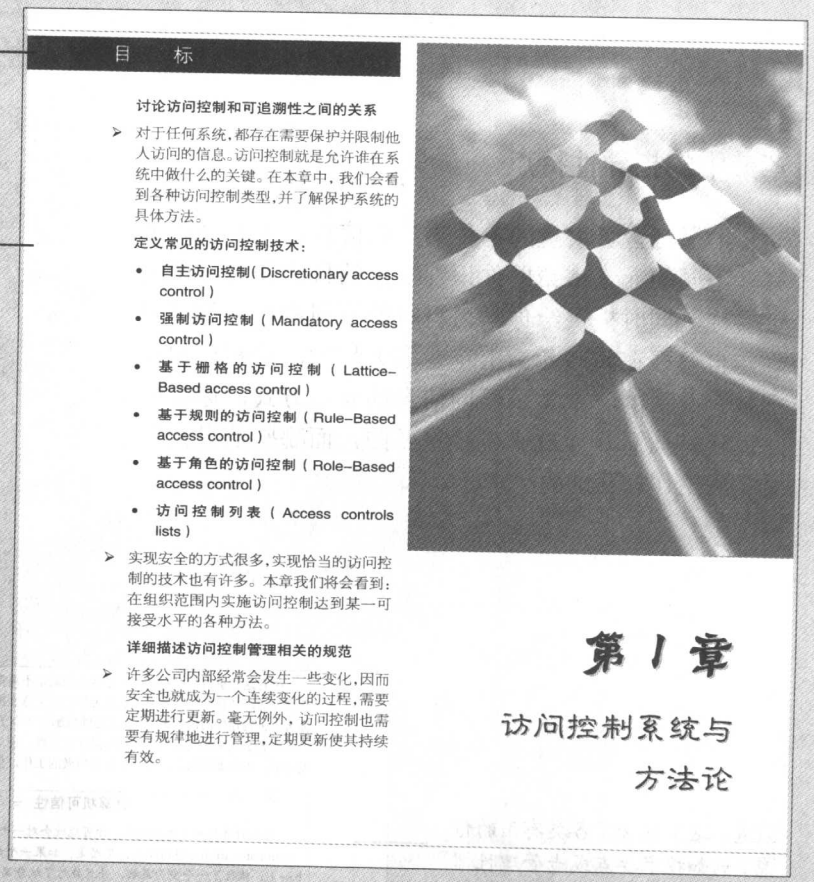
为了尽可能地提供可供认证学习的信息，本书在编排上具有以下特点：

章节开篇

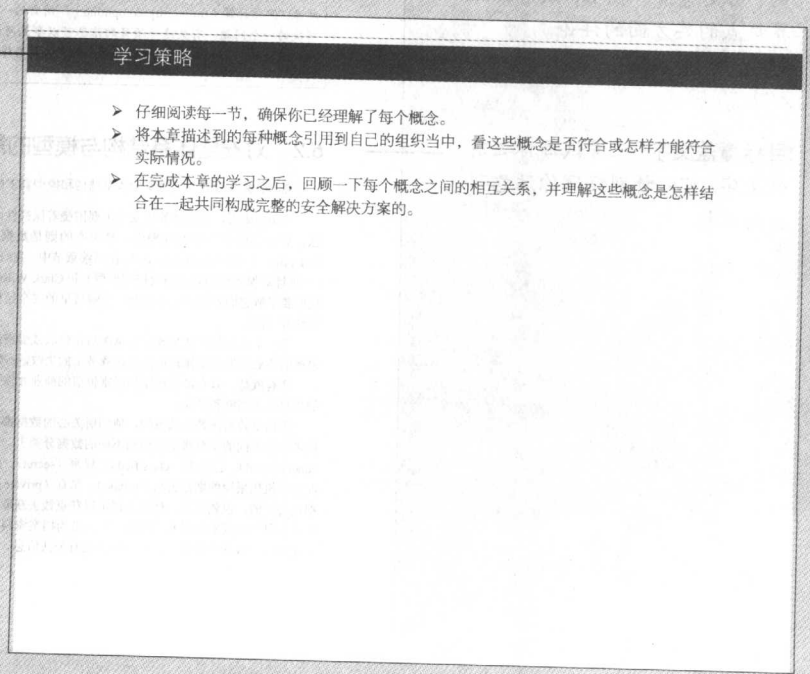
每一章开始时，有一些很有特点的信息可以为你提供最大程度的学习帮助。

列举目标：每一章开始时，都会提供一列考试提供方所期望达到的目标。

目标解释：在每个目标下面紧接着就是对它的解释，即对与考试相关内容的定义和描述。因为考试提供方有时候在提出目标时不是很明确，对目标加以解释就很有必要，从中也能体现出本书作者自身的经验积累。



学习策略：每一个主题都有其自身特点，为了更好地支持你的学习，Que Certification 提供了最能把握章节内容的学习策略，特别是针对考试的策略。

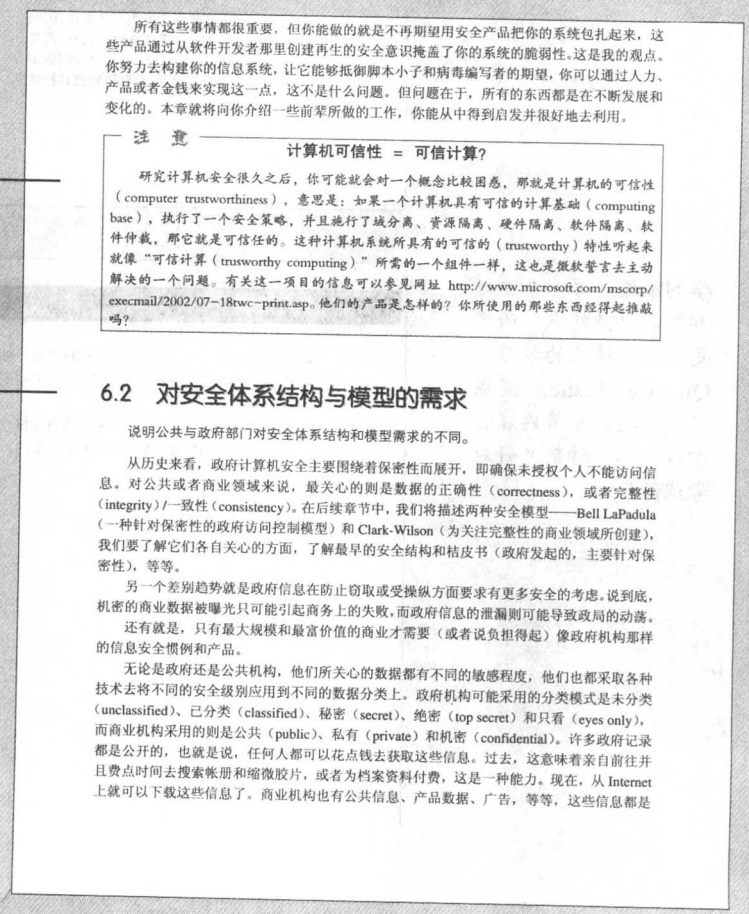


章节中的指导性特点

本书包含了大量的各种类型的信息，作者设计了许多不同的元素来帮助你识别信息的目的和对考试的重要性，同时提供给你学习材料的不同途径。你可以确定自己要在某些元素上花费多大精力，这和你的目标是有关系的。熟悉了不同信息的表示方式，你就能知道哪些信息对应试来说是重要的，而哪些信息又是对实际工作有帮助的。

注意：这里包含了各类有用的信息，例如技术要点或者管理性惯例、历史背景和技术，或者就业界热点的某方面的评论。

目标覆盖文字：在考试目标之前的文字，可以特别提醒你注意列出的目标。



所有这些事情都很重要，但你能做的就是不再期望用安全产品把你的系统包扎起来，这些产品通过从软件开发者那里创建再生的安全意识掩盖了你的系统的脆弱性。这是我的观点。你努力去构建你的信息系统，让它能够抵御脚本小子和病毒编写者的期望，你可以通过人力、产品或者金钱来实现这一点，这不是什么问题。但问题在于，所有的东西都是在不断发展和变化的。本章就将向你介绍一些前辈所做的工作，你能从中得到启发并很好地去利用。

注意

计算机可信性 = 可信计算?

研究计算机安全很久之后，你可能就会对一个概念比较困惑，那就是计算机的可信性（computer trustworthiness），意思是：如果一个计算机具有可信的计算基础（computing base），执行了一个安全策略，并且施行了域分离、资源隔离、硬件隔离、软件隔离、软件仲裁，那它就是可信任的。这种计算机系统所具有的可信的（trustworthy）特性听起来就像“可信计算（trusworthy computing）”所需的一个组件一样，这也是微软誓言去主动解决的一个问题。有关这一项目的信息可以参见网址 http://www.microsoft.com/mscorp/execmail/2002/07-18twc-print.asp。他们的产品是怎样的？你所使用的那些东西经得起推敲吗？

6.2 对安全体系结构与模型的需求

说明公共与政府部门对安全体系结构和模型需求的不同。

从历史来看，政府计算机安全主要围绕着保密性而展开，即确保未授权个人不能访问信息。对公共或者商业领域来说，最关心的则是数据的正确性（correctness），或者完整性（integrity）/一致性（consistency）。在后续章节中，我们将描述两种安全模型——Bell LaPadula（一种针对保密性的政府访问控制模型）和 Clark-Wilson（为关注完整性的商业领域所创建），我们要了解它们各自关心的方面，了解最早的安全结构和桔皮书（政府发起的，主要针对保密性），等等。

另一个差别趋势就是政府信息在防止窃取或受操纵方面要求有更多安全的考虑。说到底，机密的商业数据被曝光只可能引起商务上的失败，而政府信息的泄漏则可能导致政局的动荡。

还有就是，只有最大规模和最富价值的商业才需要（或者说负担得起）像政府机构那样的信息安全惯例和产品。

无论是政府还是公共机构，他们所关心的数据都有不同的敏感程度，他们也都采取各种技术去将不同的安全级别应用到不同的数据分类上。政府机构可能采用的分类模式是未分类（unclassified）、已分类（classified）、秘密（secret）、绝密（top secret）和只看（eyes only），而商业机构采用的则是公共（public）、私有（private）和机密（confidential）。许多政府记录都是公开的，也就是说，任何人都可以花点钱去获取这些信息。过去，这意味着亲自前往并且费点时间去搜索帐册和缩微胶片，或者为档案资料付费，这是一种能力。现在，从 Internet 上就可以下载这些信息了。商业机构也有公共信息、产品数据、广告，等等，这些信息都是

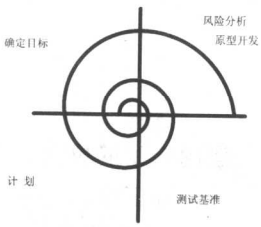


图 4.10 螺旋生命周期模型

图：为了增强可读性，图片尽量放在页边，这样就不至于打断学习正文的思路。

STED BY STEP

遵循生命周期模型

（1）开发一个预先设计。
（2）从设计出发，开发一个原型（prototype）。
（3）开发下一个原型。
（4）评估。
（5）定义进一步的需求。
（6）计划和设计另一个原型。
（7）构建并测试该原型。
（8）重复步骤 3-7，直到客户满意，原型符合需求。
（9）构建系统。
（10）全面测试最终系统。

Step by Step：手把手的指导步骤，让你能够掌握特殊的任务或者与考试目标相关的功能。

实 践

禁用与删除（Disabling versus deleting）

这里有个很关键的词语，某人离开公司，你应该*禁用*其账号而不是*删除*。删除某个离职人员的账号是一种常见的错误。正确的做法是：在某人离职后，先禁用其账号一段时间，期满后再删除。这么做有两个主要原因：首先，某人离开公司后不久又决定回到原公司工作是常有的事；其次，一旦删除账号，某些操作系统会删除其对资源的访问权。假定公司有个市场人员离职了，另一个新职员顶替了这个职位，你可能就想让新职员拥有与前职员相同的访问权，可要是前职员的账号已经被删除了，你就很难知道他的访问权曾经是怎样设置的，因而给新职员指派权限就比较困难。反过来说，如果你仅仅禁止掉前职员的账号，那么只需简单的重新命名，新职员就立即拥有了和前职员完全相同的权限。

实践：与材料相关的更带有扩展性的讨论，也许和考试并不直接相关，但作为参考资料或者工作实践都是很有用的。这里可能也会提供有用的背景或上下文信息，对理解主题很有帮助。

REVIEW BREAK

1.5.3 对 BLP 模型和 Biba 模型的小结

笔者建议大家记住以下关于 BLP 和 Biba 的要点：

BLP 模型：

- 简单安全规则。
- 星型特性。
- 针对的是保密性。

Biba 模型：

- 针对的是完整性。
- Biba 的规则与 BLP 的正好相反。

Review Break：以列表或表格方式对关键信息进行小结。在一个很长的章节之后，中间复习在你把注意力转移到下一个章节之前会增强你对关键点的理解。

案例研究

贯穿本书的案例研究提供给你另一种更概念性的运用知识的机会，它们反映了作者的现实经验，不但对你的考试准备很有帮助，也有助于你的实际工作。在每一个案例研究中，你都会发现类似的元素：场景描述（description of a scenario）、案例要点（essence of the case）和分析（analysis）。

案例要点：列举在此场景中需要注意的要点问题。

案例研究：可信计算

案例要点

关于此案例和可信计算的要点如下所列：

- **可用性**（Availability）—— 系统不能停运，必要时要能自我恢复。
- **安全**（Security）—— 数据和系统应该得到保护。
- **私密性**（Privacy）—— 用户控制自己的数据。
- **可信性**（Trustworthiness）—— 从芯片到客户服务，在很宽的范围内让客户能够信赖微软的产品。
- **易管理性**（Manageability）—— 相对于大小和复杂性，系统应该是很容易安装和维护的。
- **响应**（Responsiveness）—— 公司会对产品负责，帮助客户解决问题。
- **透明性**（Transparency）—— 公司对客户开放。
- **正确性**（Accuracy）—— 结果是消除错误，得到保护。
- **易用性**（Usability）—— 软件容易使用。

场景（scenario）

能否改变软件开发过程，以便提供更安全的代码？2002 年 1 月，一份内部备忘录被泄漏给媒体，它描述的正是一个寻求生成更安全代码的内部项目。

该项目的目的是资助那些生产“可信计算（trustworthy computing）”的公司，普遍认为这是一种必要的态度上的变化。出自首席软件构架师 Bill Gates 之手的这份备忘录，要求所有的职员都参与到该项目中来。要了解备忘录的主旨，请查看网址 http://www.computerbytesman.com/security/billsmemo.htm。

（待续）

场景：形象地描述了专业人员在此领域可能面临的某种情况，该场景所要解决的问题是和本章节覆盖的目标相关的，并且包含了各种提供分析判断的细节。

分析：解决案例要点中提出的问题。在这里，也许你能看到一个概括性的列表方案、一个文字叙述的例子，或者是二者的结合。

案例研究：可信计算

分析

微软并没有预示这是一个可在几个月的代码复查和程序员培训中就能完成的任务，在随后由高级副总裁及 CTO Craig Mundie 发布的白皮书（Advanced Strategies and Policy）中做了进一步解释：要取得明显的成功，准备长期的努力（10 到 15 年）并且让所有的组织都参与到其中是非常必要的。你可以在以下网址读到这篇文章：

http://www.microsoft.com/presspass/exec/craig/05-01trustworthywp.asp

很快就有人批评说这只不过是个市场炒作而已。因为产品的安全弱点和 bug，使微软长期以来一直遭受着严厉的批评，这份备忘录也被看成是不做实事只想改变公众态度的企图。微软宣布即刻中断.NET 的工作，.NET 是 Windows 操作系统的下一个版本。微软宣称的目的是为程序员提供安全编码培训，同时检查.NET 和其他现有产品中的软件 bug。来自微软的不同的消息源声称：有 9000 位程序员得到培训，工作中断时间长达两个月，许多 bug 被纠正，.NET 的方向也转入到安全方面而不再是功能。

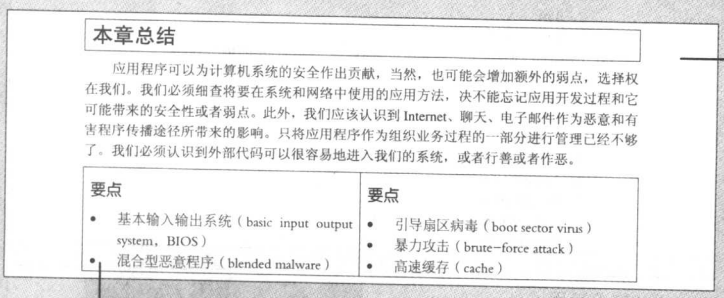
为了对备忘录和随后的宣告作出响应，一个 Web 网站创建了 www.trustworthycomputing.com，在 www.google.com 搜索引擎中搜索“Microsoft security or privacy flaw or flaws or hole or holes”，该网站就跃然屏幕之上。网页上的新闻最初全都被媒体对微软战略的响应占据着。

与此相对，那些力推工程化“可信系统（trusted systems）”以提供安全方案的厂商抓住了这次机会，开始大力宣传他们的方案。2002 年 4 月 4 日，http://www.wired.com/news/business/0,1367,51521,00.html 上登出了一篇名为“Signs of Trustworthy Computing”的文章，作为应答，嵌入键盘的智能卡阅读器、专用的 BIOS 级例程，以及其他硬件设备都开始大做宣传。

可信计算可能是许多年内并不能实现的一个目标，不过，它对计算机安全肯定是有促进作用的。

广泛复习和自测项目

在每章的最后，除了一些总结性元素，你还会发现一部分称为“知识运用（Apply Your Knowledge）”的内容，它为你提供了几种用来测试知识掌握程度的方法。



本章总结

应用程序可以为计算机系统的安全作出贡献，当然，也可能会增加额外的弱点，选择权在我们。我们必须细查将要在系统和网络中使用的应用方法，决不能忘记应用开发过程和它可能带来的安全性或者弱点。此外，我们应该认识到 Internet、聊天、电子邮件作为恶意和有害程序传播途径所带来的影响。只将应用程序作为组织业务过程的一部分进行管理已经不够了。我们必须认识到外部代码可以很容易地进入我们的系统，或者行善或者作恶。

要点

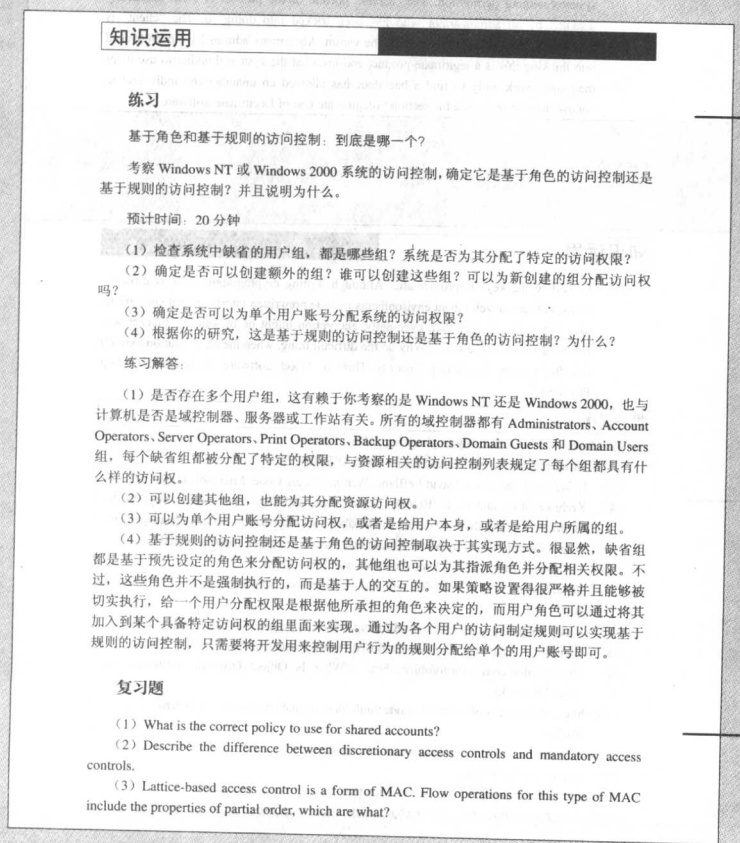
- 基本输入输出系统（basic input output system，BIOS）
- 混合型恶意程序（blended malware）

要点

- 引导扇区病毒（boot sector virus）
- 暴力攻击（brute-force attack）
- 高速缓存（cache）

本章总结：在“知识运用”部分之前，“本章总结”会带你复习你应该学会的本章的知识。

要点：在每一章的最后都会列出相关的关键术语，你应该知道并深刻理解这些术语。



知识运用

练习

基于角色和基于规则的访问控制：到底是哪一个？

考察 Windows NT 或 Windows 2000 系统的访问控制，确定它是基于角色的访问控制还是基于规则的访问控制？并且说明为什么。

预计时间：20 分钟

（1）检查系统中缺省的用户组，都是哪些组？系统是否为其分配了特定的访问权限？

（2）确定是否可以创建额外的组？谁可以创建这些组？可以为新创建的组分配访问权吗？

（3）确定是否可以为单个用户账号分配系统的访问权限？

（4）根据你的研究，这是基于规则的访问控制还是基于角色的访问控制？为什么？

练习解答

（1）是否存在多个用户组，这有赖于你考察的是 Windows NT 还是 Windows 2000，也与计算机是否是域控制器、服务器或工作站有关。所有的域控制器都有 Administrators、Account Operators、Server Operators、Print Operators、Backup Operators、Domain Guests 和 Domain Users 组，每个缺省组都被分配了特定的权限，与资源相关的访问控制列表规定了每个组都具有什么样的访问权。

（2）可以创建其他组，也能为其分配资源访问权。

（3）可以为单个用户账号分配访问权，或者是给用户本身，或者是给用户所属的组。

（4）基于规则的访问控制还是基于角色的访问控制取决于其实现方式。很显然，缺省组都是基于预先设定的角色来分配访问权的，其他组也可以为其指派角色并分配相关权限。不过，这些角色并不是强制执行的，而是基于人的交互的。如果策略设置得很严格并且能够被切实执行，给一个用户分配权限是根据他所承担的角色来决定的，而用户角色可以通过将其加入到某个具备特定访问权的组里面来实现。通过为各个用户的访问制定规则可以实现基于规则的访问控制，只需要将开发用来控制用户行为的规则分配给单个的用户账号即可。

复习题

（1）What is the correct policy to use for shared accounts?

（2）Describe the difference between discretionary access controls and mandatory access controls.

（3）Lattice-based access control is a form of MAC. Flow operations for this type of MAC include the properties of partial order, which are what?

练习：这些活动让你有机会掌握具体的操作任务，我们的目标是增强你对产品或技术的熟练程度。为了通过考试，你必须要有进行这些操作的能力。

复习题：这些很短的开放式的问题可以让你快速评估刚刚阅读本章后的理解程度。这里并没有提供可供选择的答案，而是要求你以自己的语言来叙述正确的答案。尽管考试中不会碰到这样的问题，但这些问题能够真实地测试你对关键概念的理解水平。

测试题：这些问题反映了真正考试中可能出现的问题类型。做这些题目能使你熟悉真正考试的试题格式，并且有助于让你确定哪些知识是已经掌握了的而哪些是需要复习或是进一步去学习的。

知识运用

测试题

（1）Which principle identifies a user and verifies that the user is who he says he is?
A. Authentication
B. Access control
C. Biba
D. Bell-LaPadula

（2）Which principle determines what resources the user can use on the network?
A. Authentication
B. Access control
C. Biba
D. Bell-LaPadula

（3）Which principle makes people respond to access controls?
A. Accountability
B. Authentication
C. Authorization
D. Accreditation

测试题答案：对于每一个复习和考试题，在每一章的末尾都会给出完整的解答。

知识运用

privileges to run them, they can attack from a remote location. See the section "Illegitimate Use of Legitimate Software."

测试题答案

（1） **D**. Back Orifice is a Trojan horse. This software was developed to remotely control systems without permission. The "server" portion of the product is often innocently installed by an administrator who has been tricked into doing so. The "client" is installed on the system used to attack the victim. Also, many admins have been tricked into thinking this is a legitimate product and installed the system thinking to use it for their own work, only to find a backdoor has allowed an unauthorized individual to control their systems. See the section "Illegitimate Use of Legitimate Software."

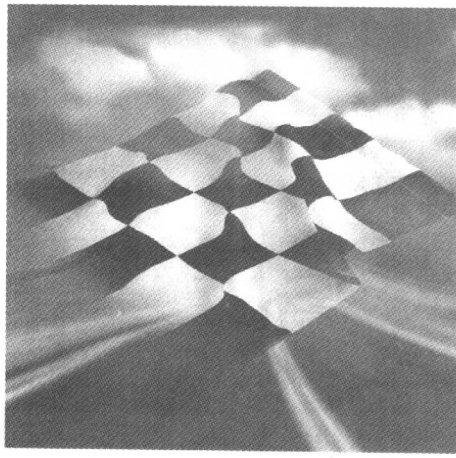
推荐读物：每一章的最后一部分是一些附加的资源，如果你对超出考试水平的知识感兴趣，或者你想进一步钻研理解上还有疑问的问题，你都可以花些时间利用这部分中列出的资源。

知识运用

（9） **C**. Hiding the keys is problematic. Although writing cryptographic code is difficult, many software development environments include prewritten interfaces that simplify its use. Although it is true that, eventually, encryption might be broken, an attacker will first seek to obtain the keys. (Why do the difficult thing, when the easy solution exists?) See the section "Impacting Security Through Good Software Design and Coding Practices."

推荐读物

（1）Anderson, Ross. Security Engineering. Wiley, 2001.
（2） Grimes, Roger A. Malicious Mobile Code. O'Reilly, 2001.
（3） Howard, Michael, and David LeBlanc. Writing Secure Code. Microsoft Press, 2001.
（4） Krehnke M.E., and D. K. Bradley. "Data Marts and Data Warehouses: Keys to the Future or Keys to the Kingdom." In Handbook of Information Security Management, Fourth Edition, edited by Micki Krause and Harold F. Tipton. Auerbach, 2001.
（5） McConnell, Steve. Code Complete. Microsoft Press, 1993.
（6） Vallabhaneni, S. Rao. CISSP Examination Textbooks. SRV Professional Publications, 2000.
（7） Viega, John, and Gary McGraw. Building Secure Software. Addison-Wesley, 2002.
（8） Whitehead, Katherine. Component-Based Development. Addison Wesley, 2002.
（9） http://catalog.com/softinfo/objects.html ("What Is Object Oriented Software?" by Terry Montlick).
（10） http://msdn.microsoft.com/vstudio/techinfo/documentation/default.asp (Microsoft Visual Studio).
（11） http://www.atstake.com/research/lc/download.html.
（12） http://www.CERT.org.
（13） http://www.codagen.com (Gen-it Architect, Codagen code generation).
（14） http://www.computer.privateweb.at/judith/ (A medical expert system).



关于作者

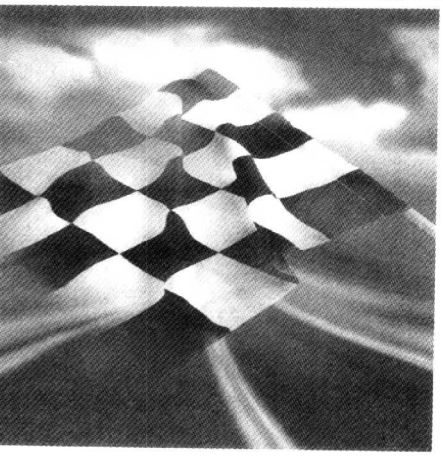
Roberta Bragg，CISSP，MCSE，Security Evangelist 的始创者，有 25 年 IT 领域的经验，包括程序开发、系统管理和 Windows 网络安全设计等。她是具有国际声望的作家和 Windows 安全讲师。

Scott Barman，目前担任 MITRE 公司（www.mitre.org）的信息安全和系统体系结构分析员，MITRE 目的在于帮助 IRS 对其 IT 基础设施进行现代化。Scott Barman 在信息安全领域已经有几乎 20 年的从业经验，为商业组织和政府机构培植了系统发展及其安全需求。从 Internet“爆炸”以来，在加入 MITRE 之前，Scott 为 Washington, D.C.地区的许多组织开发了安全策略，并把注意力集中在安全的各个方面。Scott 获得 Georgia 大学的学士学位和 Carnegie Mellon 大学（www.mism.cum.edu）的信息系统管理（主要是信息安全管理）硕士学位。

Philip Fites，有 34 年的信息领域从业经验，从计算机操作到商业和项目管理，目前他致力于信息系统安全理论研究和实践工作。从 20 世纪 80 年代初期以来，Philip 将对信息安全的兴趣转换为致力于信息系统安全完整性和其他一些方面的研究，并且通过实践工作来帮助客户阐明和实现安全目标。Philip 获得过数学学士和 MBA 学位，并在 Queen's 大学从事计算机学科的博士学习。他与人合作著有（“*Control and Security of Computer Information Systems*”、“*The Computer Virus Crisis*”和“*Information Systems Security: A Practitioner's Reference*”，此外，他还在多个专业和业界出版物上发表了大量有关计算机安全主题、软件研究和教育规划方法的著作。Philip 是（ISC）^{2}的总裁和一名主管，是加拿大标准理事会（Standards Council of Canada）下属的加拿大信息技术顾问委员会（Canadian Advisory Committee on Information Technology）的成员。

Wesley J. Noonan，目前是 BMC 软件公司(www. bmc.com)网络管理产品线的高级质量保障代表。最初，Wes 在美国海军部从事 Banyan VINES 网络的建设工作，在过去的 10 年时间里，他负责建设、维持并保护网络规模从 25 个用户发展到了 25000 个用户。作为一名充满活力的培训讲师，Wes 为其客户开发并讲授基于 Cisco 路由和交换的课程，他获得的认证包括 MCSE、CCNA、CCDA 和 NNCSS。

Benjamin Wright，全世界公认的电子商务领域律师的一个领导者，是“（*The Law of Electronic Commerce*）”的著作者，该书全面阐述了电子交易在法律方面的情况，已由 Aspen Law&Business 出版。Benjamin 在 Georgetown 大学法律中心获得了本科学位，是一名执业于 Dallas, Texas 的计算机安全和电子商务法律领域的独立律师。从 1988 年起，他发表过 500 多次有关电子商务、隐私和计算机安全的演讲，许多言论都被全球众多出版物引述，从 *Wall Street Journal* 到 *Sydney Morning Herald*。2001 年 5 月 26 日，CNBC 在对全国广播的 30 分钟的节目——“*The Cutting Edge Technology Report: Electronic Signatures*”中介绍了 Benjamin 的情况。



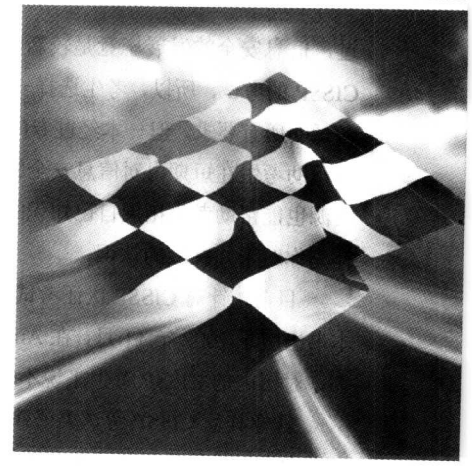
关于技术审稿人

Guy Bruneau，GSEC，GCIA，GCUX，是 InfoPeople Security Solutions, Inc.的高级安全顾问，他的职责是帮助客户管理安全服务、操作并部署计算机入侵检测、审计网络安全、进行事件响应和报告等等。在使用和处理 Cisco Secure IDS、Shadow IDS 和 Snort IDS 等产品上拥有第一手的经验。

Guy 是 SANS 的一名主管和发言人，并且是 IDIC 教程——"Introduction to Logfile Analysis"的作者。作为 SANS 授权的 Unix 安全专家，Guy 目前是 SANS GIAC 认证的入侵分析师顾问委员会的主席。Guy 是 OS hardened Shadow IDS（基于 NSWC 的 Shadow version 1.7，www.whitehats.ca）的作者。在业余时间里，他担任着 New Riders Publishing 的技术评阅者。

Lawrence S. Paccone，是 Northrop Grumman Information Technology TASC 的首席国家/系统安全分析师。作为技术领导者和项目经理，他已经在 Internet 和网络/系统安全领域积累了超过 8 年的经验。Lawrence 在为政府网络/系统安全研发实验室提供支持的数项网络安全项目中担任技术领导者。在此之前，他担任 The Analytical Sciences Corporation（TASC）的国家安全分析师已经有 5 年时间，负责评估传统的军事武装结构。他同时持有信息系统 M.S.、国际关系 M.A.和政治学 B.A.学位。他获得过 8 个专业证书，内容包括网络和系统安全、互联网、广域网、Cisco 路由/交换、Unix 和 Windows NT，同时，他还是目前发表的 8 本 IT 安全著作的技术编辑。

Patrick "Swissman" Ramseier，CCNA，CISSP，是 OKENA 的系统工程师，StormSystem Intrusion Prevention System 的制作者。OKENA 发行了突破性的安全软件产品，可以前瞻性地保护和应用主机系统的操作完整性。OKENA StormSystem 是一种无缝集成的安全产品系统，可以不依赖攻击特征而防止已知和未知的攻击活动。Patrick 一开始是一名 Unix 系统管理员，在过去的 14 年中，他参与了企业级的安全设计、体系结构评审、脆弱性评估、VPN 支持、物理/网络/操作系统（Solaris、Linux、BSD 和 Windows NT/2000）安全、培训、研究、售前和售后等工作。他获得了商业学士学位，目前正在获取计算机科学博士学位的过程当中。



译 者 序

作为国际公认的信息安全领域最权威、最著名的专业认证，CISSP 的发展已经有了 10 多年的历史，其全称是信息系统安全认证专家（Certified Information System Security Professional）。能够获得 CISSP 证书的人，将能证明自己具备在信息安全领域从业所需的足够的能力和资格，并有可能成为职业生涯中的一个分水岭。

CISSP 之所以众望所归，这和 CISSP 的组织和管理机构（ISC）²（International Information Systems Security Certification Consortium，国际信息系统安全认证协会）是分不开的，因为（ISC）² 是一个独立的、非盈利的组织，其目标是发展并管理一个公正而权威的信息安全专业人员认证机构，这就使得 CISSP 完全不同于众多以产品提供商为主的认证，它的全面性、公正性和稳定性得到了业界一致的认可。此外，（ISC）² 对申请 CISSP 证书的人员有较高的要求，比如相关工作经验、权威人士的审核推荐和再认证累积分等。当然，CISSP 考试的费用也相当不菲。所有这些，都使得 CISSP 具有很高的知名度，并以所谓的信息安全领域的“CCIE”（网络界最权威的专业认证）而著称于世。

正因为 CISSP 独具的权威性，有志在信息安全领域有所建树的专业人员才对其关注和倾慕。目前全世界获得 CISSP 证书的人员不超过 10000 人，香港是仅次于北美地区外拥有 CISSP 最多的地区。据统计，亚洲拥有 900 余名 CISSP，其中 55%为管理与咨询专业人员。2002 年 9 月，CISSP 认证考试首次引入祖国大陆（考试在上海举行），译者有幸通过考试并获得证书。尽管相比世界甚至亚洲其他国家和地区（主要是韩国和香港），祖国大陆在 CISSP 认证方面起步较晚，但从目前的趋势来看，随着我们对信息安全认识的加强和不断投入，CISSP 认证会得到较快发展。

CISSP 考试涉及的范围非常广泛，几乎覆盖了信息安全领域的所有方面，对有志于此项认证的人来说，通过考试的难度还是相当大的，即便是在信息安全领域从业多年的专业人员，因为日常工作范围所限，可能也不会对信息安全所有相关的信息都有很好的了解。为此，（ISC）² 建立了一套通用知识体系，即 CBK（Common Base of Knowledge），该体系分为 10 个知识域，覆盖了 CISSP 考试可能涉及的所有范围。有了这套体系，考生就能有的放矢地安排自己的学习计划，规划自己的学习过程，以便充分地为考试做好准备。不