10

Computer Security

计算机安全

计算机英语教学PPT

内容提要

计算机安全.内容提要

- A Definition of Computer Security

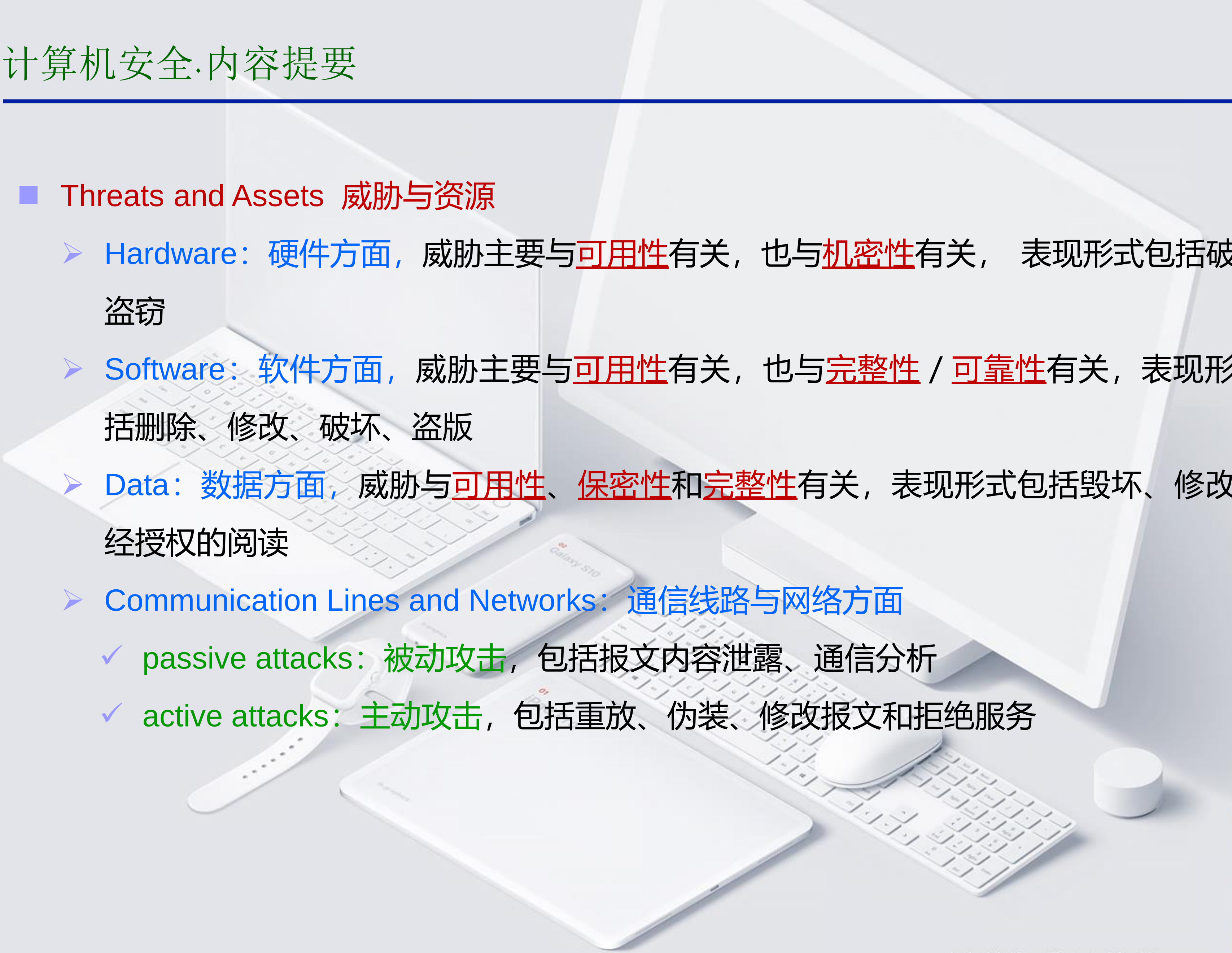
The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (including hardware, software, firmware, information/data, and telecommunications).

给自动化信息系统提供的保护，其目的是达到保持信息系统资源（包括硬件、软件、固件、信息／数据及电信设备）的完整性、可用性和机密性等适当目标。

- The CIA triad（CIA 三位一体）：计算机安全的三个关键目标
  - ✓ Integrity：完整性
  - ✓ Availability：可用性
  - ✓ Confidentiality：机密性
- 计算机安全的其他目标
  - ✓ Authenticity：可靠性
  - ✓ Accountability：可问责性

计算机安全.内容提要

- Threats and Assets 威胁与资源
  - Hardware：硬件方面，威胁主要与可用性有关，也与机密性有关， 表现形式包括破坏、盗窃
  - Software：软件方面，威胁主要与可用性有关，也与完整性 / 可靠性有关，表现形式包括删除、修改、破坏、盗版
  - Data：数据方面，威胁与可用性、保密性和完整性有关，表现形式包括毁坏、修改、未经授权的阅读
  - Communication Lines and Networks：通信线路与网络方面
    - ✓ passive attacks：被动攻击，包括报文内容泄露、通信分析
    - ✓ active attacks：主动攻击，包括重放、伪装、修改报文和拒绝服务



计算机安全.内容提要

- Computer Security Strategy 计算机安全策略

  一项综合安全策略涉及三个方面：

  - Specification/policy（明确说明 / 政策）：安全方案（security scheme）应该做到什么?
  - Implementation/mechanisms（实施 / 机制）：安全方案如何做到这些?
  - Correctness/assurance（正确性 / 保证）：安全方案真的能起作用吗?

语言点聚焦

计算机安全·语言点聚焦

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (including hardware, software, firmware, information/data, and telecommunications). 给自动化信息系统提供的保护，其目的是达到保持信息系统资源（包括硬件、软件、固件、信息 / 数据及电信设备）的完整性、可用性和机密性等适当目标。

  applicable：a. 可应用的；适当的

  - The black box technique is also applicable for constraint testing, such as system performance or security.（5B）黑盒方法也可应用于约束测试，如系统性能或安全。
  - While the computer graphics techniques used in movies may be applicable to AR as well, movies lack one crucial aspect of AR—interactivity.（12B/II）虽然电影中使用的计算机图形技术也可应用于增强现实，但电影缺少增强现实的一个关键方面——交互性。

计算机安全·语言点聚焦

- Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals. 数据机密性：确保私有或机密信息不为未经授权的个人所获取或不透露给未经授权的个人。 disclose 由 close 加前缀 dis-（表示“否定” “相反” 等）构成。

confidential：a. 秘密的，机密的 → confidentiality：n. 秘密性，机密性

- a confidential report (document) 秘密报告（文件）
- They signed a confidentiality agreement. 他们签署了一份保密协议。

disclose：v. 泄露，透露 → disclosure：n. 泄露，透露

- There is an increasing potential for disclosure of personal information.（10A/II-3）个人信息遭到泄露的可能性在增加。

authorize：v. 授权 → authorized：a. 经授权的，特许的 → unauthorized：a. 未经授权的

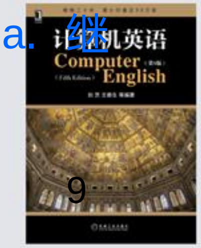
- be authorized to issue the following statement 受权发表下列声明
- gain unauthorized access to the file system（3B/4）未经授权访问文件系统
- Any authorized user can use the service.（5A/I）任何获得授权的用户都可以使用该服务。

计算机安全·语言点聚焦

- Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. 私有性：确保个人对哪些与其有关的信息可被收集和存储，以及该信息可由谁透露和透露给谁予以控制或影响。 control or influence 后面跟有两个并列的宾语从句。
- System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. 系统完整性：确保一个系统以未受削弱的方式执行其预定功能，不受有意或无意的未经授权的操纵。

impair：v. 损害；削弱→impaired：a. 受损的；削弱的→unimpaired：a. 未受损的；未削弱的

- impaired hearing 受损的听觉
- The accident impaired his vision. 事故损伤了他的视力。
- She survived the accident with her sight unimpaired. 她从事故中幸存下来，视力未受损。
- Continued criticism of the leaders could impair efforts to ease tensions in the area. 继续批评领导人会削弱缓和该地区紧张局势的努力。



计算机安全·语言点聚焦

- Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or a message originator. 可靠性：指真实并可验证、可信的特性；对一次传输、一条消息或一个消息来源的有效性的相信。

  originator 由动词 originate 加名词后缀 -or 构成，表示“创始人” “起源”等意思。

  valid：a. 有效的 → validity：n. 有效性

  ➢ a valid address 有效地址；a valid passport 有效护照

  ➢ the validity of a contract 合同的有效性

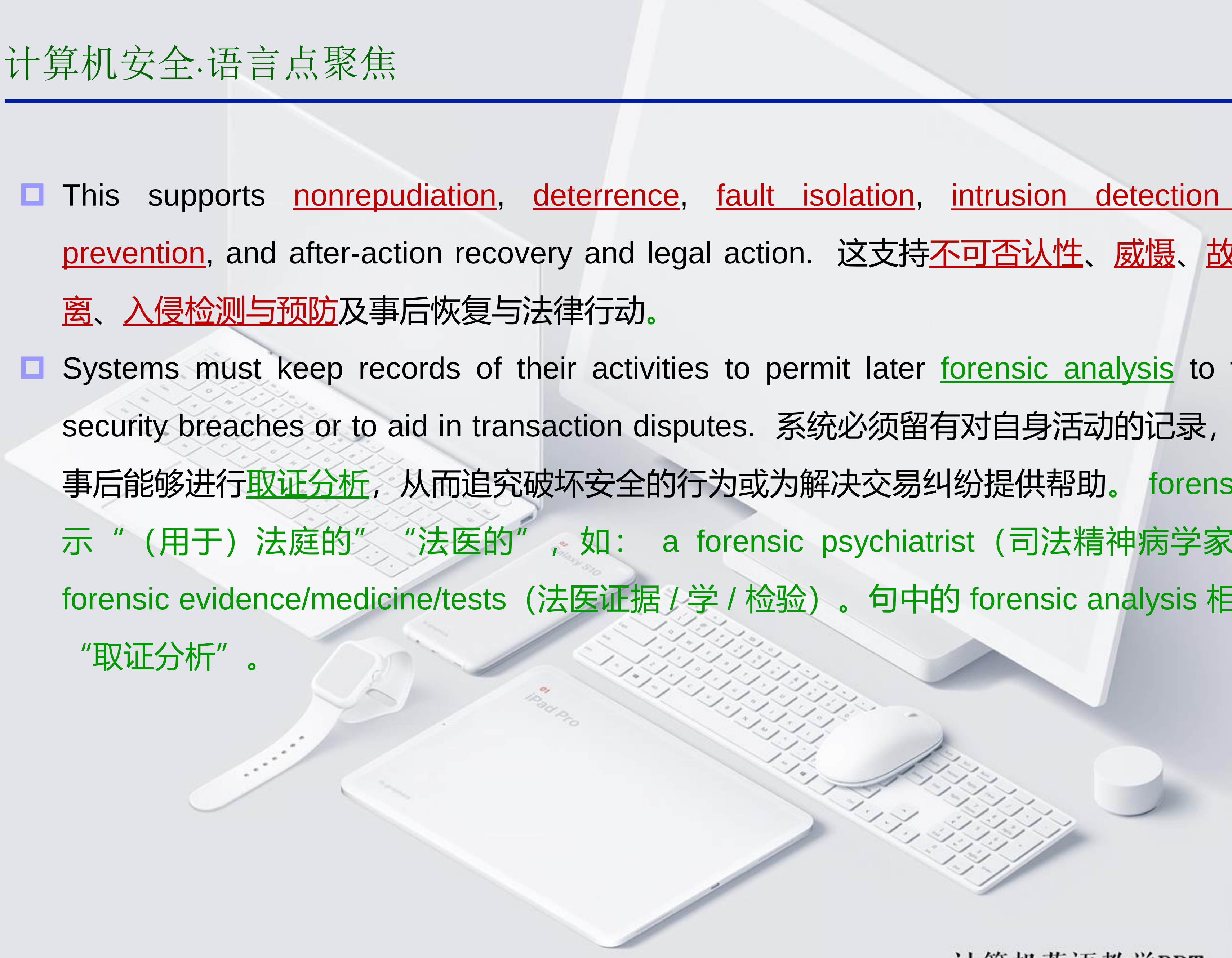
- Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. 可问责性：指这样的安全目标，该目标要求一个实体的行为只会追究到该实体。

  accountable：a. 负有责任的 → accountability：n. 负有责任

  ➢ the accountability of a company‘s directors to the shareholders 公司董事向股东所负之责

  ➢ They should be held accountable for their acts. 他们应该对自己的行动负责。

计算机安全·语言点聚焦



- This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. 这支持不可否认性、威慑、故障隔离、入侵检测与预防及事后恢复与法律行动。
- Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes. 系统必须留有对自身活动的记录，以便事后能够进行取证分析，从而追究破坏安全的行为或为解决交易纠纷提供帮助。 forensic 表示“（用于）法庭的”“法医的”，如： a forensic psychiatrist（司法精神病学家）；forensic evidence/medicine/tests（法医证据 / 学 / 检验）。句中的 forensic analysis 相当于“取证分析”。

计算机安全·语言点聚焦

- The assets of a computer system can be categorized as hardware, software, data, and communication lines and networks. 计算机系统的资源可分类为硬件、软件、数据及通信线路与网络。

categorize：v. 将…分类，将…归类

- Most of the buildings are categorized as obsolete. 这些建筑物大多被划定为陈旧建筑物。
- Indeed, much of the research in artificial intelligence can be categorized in terms of an agent’s behavior.（12A/I）事实上，人工智能的许多研究都可按主体的行为来分类。

计算机安全·语言点聚焦

- Hardware is the most vulnerable to attack and the least susceptible to automated controls.

  硬件最容易受到攻击，最不易受到自动控制。

  vulnerable：a. 脆弱的；易受攻击的 → vulnerability：n. 易遭攻击的地方；脆弱（性）；漏洞

  - Why is C or C++ more vulnerable than Java?（3B/4）为什么 C 或 C++ 比 Java 易受攻击?
  - Many insecure devices, once deployed, cannot be recalled or upgraded, and thus remain vulnerable.（11B/III）许多不安全的设备一旦部署就无法召回或升级，因此一直处于脆弱状态。
  - the vulnerabilities of the system（10A/III-1）系统的脆弱之处

  susceptible：a. 易受影响的，敏感的

  - He‘s highly susceptible to flattery. 他听几句奉承话就忘乎所以。
  - James is very susceptible to colds. 詹姆斯很容易感冒。

计算机安全·语言点聚焦

- The proliferation of personal computers and workstations and the widespread use of LANs increase the potential for losses in this area. 个人计算机和工作站的激增，以及局域网的广泛使用，增加了这个领域内遭受损失的可能性。

  proliferation：n. 激增；扩散

  - the proliferation of nuclear weapons 核武器的扩散
  - Thanks to the proliferation of smartphones, these apps are universally available. （12B/III-2）由于智能手机的激增，这些应用可供普遍使用。

- Careful software configuration management, which includes making backups of the most recent version of software, can maintain high availability. 通过仔细的软件配置管理，包括备份最近的软件版本，可保持高度的可用性。

  backup：n. & a. 备份（的），后备（的）

  - reload the database from a backup copy（6B/I）用备份重新装载数据库
  - Every part of the system has a backup. 系统每个部分都有备份。

计算机安全·语言点聚焦

- A final problem is protection against software piracy. Although certain countermeasures are available, by and large the problem of unauthorized copying of software has not been solved. 最后一个问题是针对软件盗版的保护。尽管可采取某些对策，但未经授权复制软件这个问题总的说来尚未解决。 by and large：大体上，总的说来，一般地说。
- Security concerns with respect to data are broad, encompassing availability, secrecy, and integrity. 与数据有关的安全关切范围广泛，包括可用性、保密性和完整性。

  encompass：v. 包含，包括

  - The Web encompasses these and hundreds of thousands of other sites.（8C/I）万维网包含了这些以及其他无数的网站。
  - This encompasses both system design and system implementation.（10A/III-3）这既包括系统设计，也包括系统实现。

计算机安全·语言点聚焦

- which can occur either accidentally or maliciously 这可能意外发生，也可能恶意为之。

  malicious：a. 恶意的

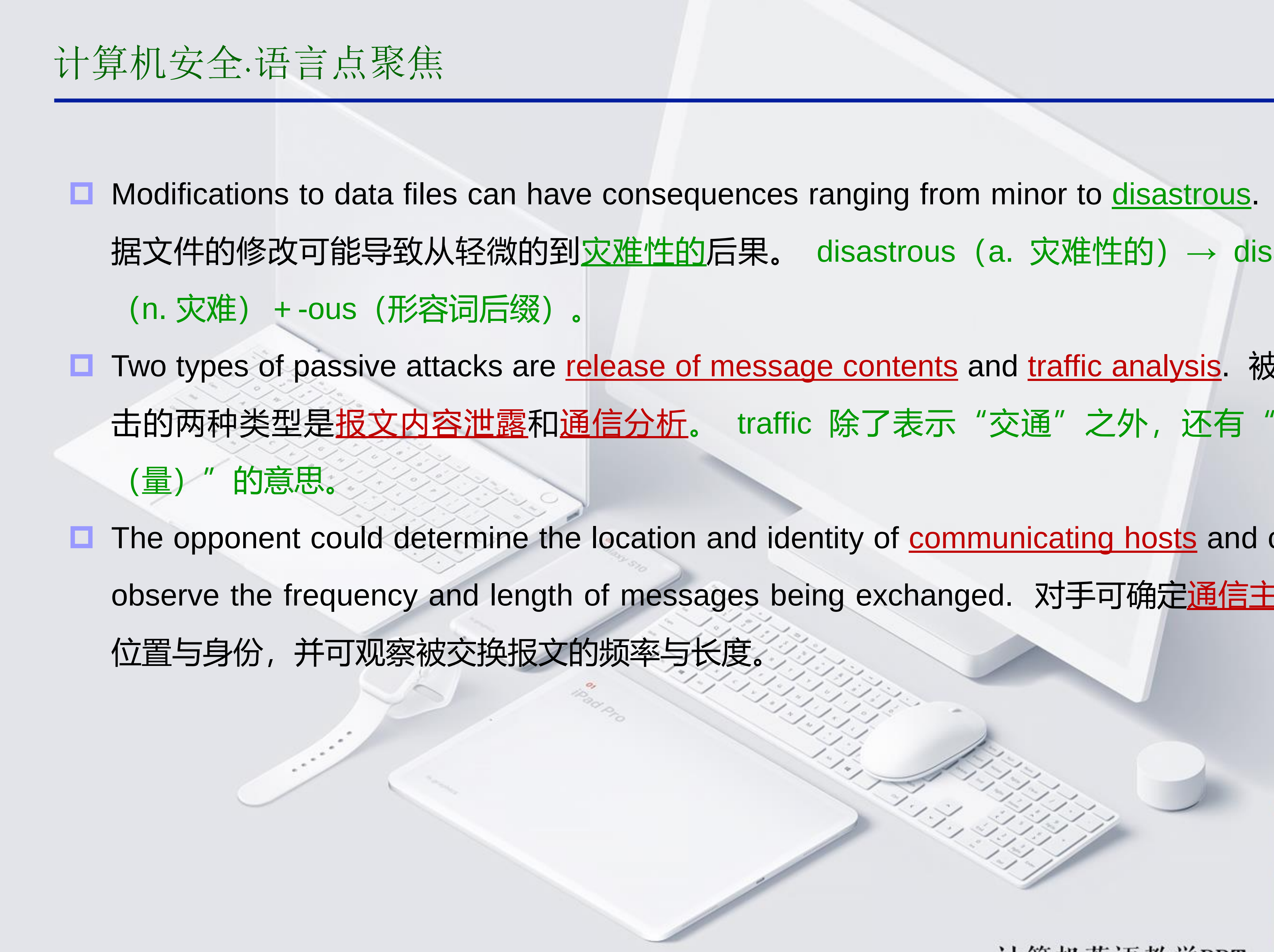
  - malicious software 恶意软件
  - malicious code 恶意代码

- A less obvious threat to secrecy involves the analysis of data and manifests itself in the use of so-called statistical databases, which provide summary or aggregate information. 对保密性的一种不那么明显的威胁涉及数据分析，这种威胁表现在对所谓的统计数据库的利用。统计数据库提供总计或合计信息。

  manifest：v. 显示；使显现

  - Frequently, the output is not even presented to the screen, but it is manifested in database changes.（5B）经常，输出数据甚至都未呈现在显示屏上，但却在数据库变更上表现出来。

计算机安全·语言点聚焦



- Modifications to data files can have consequences ranging from minor to disastrous. 对数据文件的修改可能导致从轻微的到灾难性的后果。 disastrous（a. 灾难性的）→ disaster（n. 灾难）+ -ous（形容词后缀）。
- Two types of passive attacks are release of message contents and traffic analysis. 被动攻击的两种类型是报文内容泄露和通信分析。 traffic 除了表示“交通”之外，还有“通信（量）”的意思。
- The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. 对手可确定通信主机的位置与身份，并可观察被交换报文的频率与长度。

计算机安全·语言点聚焦

- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: replay, masquerade, modification of messages, and denial of service. 主动攻击涉及对数据流的某种修改或假数据流的创建。主动攻击可细分为四类：重放、伪装、修改报文和拒绝服务。 subdivide（再分，把…分得更小）是在 divide 前面加了前缀 sub-（下面，次于，亚）。之所以用 subdivide，是因为在 passive attacks/active attacks 分类下面将 active attacks 再进行分类。
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. 重放涉及被动地捕获一个数据单元和随后重新传输该数据单元，以产生未经授权的效果。

计算机安全·语言点聚焦

- For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. 例如，可在一个有效验证序列发生后捕获并重放验证序列，从而使一个只拥有少数特权的特许实体能够通过假冒一个拥有额外特权的实体而获得这些特权。

  authenticate：v. 验证，鉴别 → authentication：n. 验证，鉴别

  - authentication procedure 验证过程
  - If all messages were encrypted and authenticated, it would be harder to commit mischief.（11C）如果所有报文都进行了加密和验证，要恶作剧就变得困难了。

- The denial of service prevents or inhibits the normal use or management of communications facilities. 拒绝服务指阻止或抑制通信设施的正常使用或管理。

- an entity may suppress all messages directed to a particular destination 一个实体可能压制发往一个特定目的地的所有报文。

计算机安全·语言点聚焦

- Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance. 拒绝服务的另外一种形式是扰乱整个网络，采取的方式或者是致瘫网络，或者是使其报文过载，从而使其性能退化。

overload：v. 使过载，使超载（offload：v. 卸下，卸载；upload：v.上传，上载；download：v. 下载）

- ➢ upload this information to a database（9C）把该信息上传数据库
- ➢ Some computationally intensive processing and exception handling can be offloaded to external services.（5A/I）一些计算密集型的处理和异常处理可以迁移到外部的服务上。

degrade：v. 使降级，使退化 → degraded：a. 降级的，退化的；degradation：n. 降级，退化

- ➢ In this case, the extended star topology is all but necessary to prevent degraded signals.（7B/III）在这种情况下，为防止信号衰减，扩展星型拓扑结构几乎是必需的。
- ➢ This implies a degradation of performance.（7C） 这意味着性能退化。

计算机安全·语言点聚焦

- □ the manager must consider the following tradeoffs: 管理员必须考虑以下权衡:

  tradeoff: n. 平衡，权衡（亦作 trade-off）

  - ➢ the trade-off between inflation and unemployment 通货膨胀与失业之间的平衡

- □ For example, virus-checking software reduces available processing power and introduces the possibility of system crashes or malfunctions due to improper interaction between the security software and the operating system. 例如，病毒检查软件会降低可用的处理能力，并会因为安全软件与操作系统的不适当交互而带来系统崩溃或发生故障的可能性。

  interact: v. 交互 → interaction: n. 交互（作用）; interactive: a. 交互（式）的; interactivity: n. 交互性

  - ➢ human-computer interaction models（12C/I）人机交互模型
  - ➢ interactive and user-facing applications（9A/I）交互式面向用户应用
  - ➢ Virtual reality, the technology of interacting with a computer using all of the human senses, will also contribute to better human and computer interfaces.（1A/练习-IV）虚拟现实，即使用所有人类官能与计算机进行交互的技术，也将有助于创建更好的人机接口。

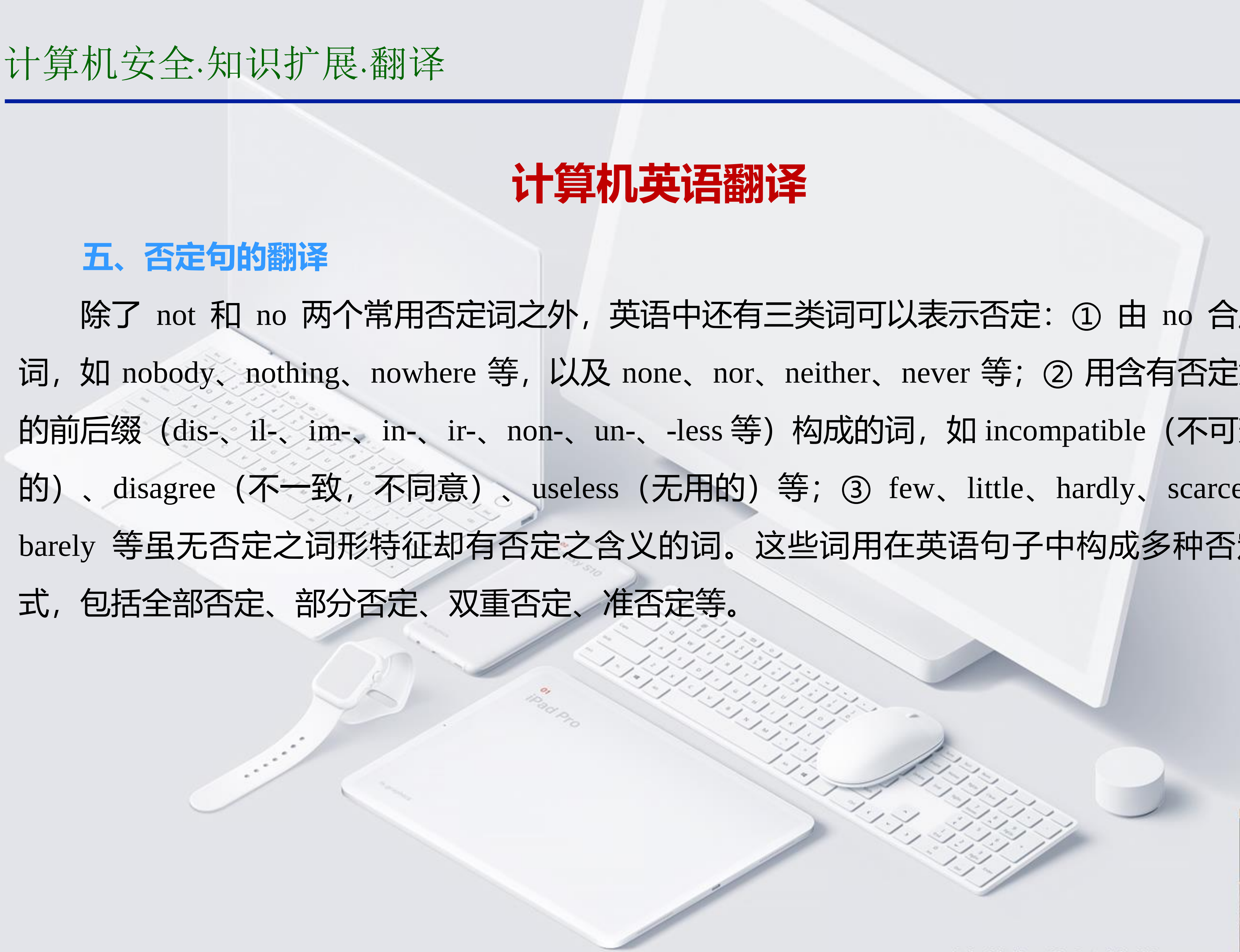
计算机安全·语言点聚焦

- For example, if a secure encryption algorithm is used, and if measures are in place to prevent unauthorized access to encryption keys, then attacks on confidentiality of the transmitted data will be prevented. 例如，如果使用了保密的加密算法，并且已经采取了防止未经授权接触密钥的措施，那么，就会防止对被传输数据的机密性的攻击。
- An example of recovery is the use of backup systems, so that if data integrity is compromised, a prior, correct copy of the data can be reloaded. 恢复的一个例子是使用备份系统，在数据完整性受损的情况下，可重新装入事先复制的正确数据。 compromise 作动词用时，可表示“危及” “损害”之意。
- Assurance is the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. 保证是指一个人对安全措施，既包括技术上的也包括操作上的，可像预期的那样有效保护系统及其处理的信息，所持有的信心程度。 句中 that 引导的从句为同位语从句，其本位语是 confidence。同位语从句与其本位语之间隔了一个定语从句（one has）。

计算机安全·语言点聚焦

- With the present state of the art, it is very difficult if not impossible to move beyond a degree of confidence to absolute proof. 就现在的发展水平而言，即使不是不可能，也很难超越一定的信心程度，做到绝对的证明。
- Evaluation is the process of examining a computer product or system with respect to certain criteria. 评估是指按照某些标准检查计算机产品或系统的过程。 criteria 系 criterion（标准，准则）的复数形式。
- The central thrust of work in this area is the development of evaluation criteria that can be applied to any security system (encompassing security services and mechanisms) and that are broadly supported for making product comparisons. 该领域里的工作要点是制定这样的评估标准，这些标准可应用于任何安全系统（包括安全服务与机制），并在进行产品比较方面得到广泛支持。 evaluation criteria 后面跟有两个定语从句，关系代词 that 在两个定语从句中均为主语，与谓语动词属于被动关系。

知识扩展



计算机英语翻译

五、否定句的翻译

除了 not 和 no 两个常用否定词之外，英语中还有三类词可以表示否定：① 由 no 合成的词，如 nobody、nothing、nowhere 等，以及 none、nor、neither、never 等；② 用含有否定意思的前后缀（dis-、il-、im-、in-、ir-、non-、un-、-less 等）构成的词，如 incompatible（不可兼容的）、disagree（不一致，不同意）、useless（无用的）等；③ few、little、hardly、scarcely、barely 等虽无否定之词形特征却有否定之含义的词。这些词用在英语句子中构成多种否定方式，包括全部否定、部分否定、双重否定、准否定等。

计算机安全.知识扩展.翻译

（一）全部否定

全部否定（total negation）可用 no、not、none、nor、neither、never 一类词；nobody、nothing、nowhere 等由 no 合成的词；by no means、on no condition、under no circumstances 等含有 no 的词组。英语表示全部否定的句子一般不难理解，通常译成汉语的否定句。

- 例句1

No programming language can ensure complete reliability. 没有哪种程序设计语言能够确保完全的可靠性。

- 例句2

A passive attack attempts to learn or make use of information from the system but does not affect system resources. 被动攻击试图了解或利用来自系统的信息，但不影响系统资源。

计算机安全.知识扩展.翻译

□ 例句3

Whereas black box testing assumes that nothing is known about the program, white box testing assumes that you know everything about the program. 黑箱测试假设对程序一无所知，而白箱测试则假设你对程序无所不知。

含有否定前缀或后缀的动词、形容词（作表语）也可在句子中表示全部否定。这种句子虽然从语法结构上讲是肯定句，但意义上是全部否定。

□ 例句4

At some point, it becomes impractical to extend a LAN any further. 局域网扩展到某种程度之后，再进一步扩展就变得不现实了。

计算机安全.知识扩展.翻译

（二）部分否定

部分否定（partial negation）有两种表达方式：① 句中含有 all 或者与其相类似的词（whole、total、both、every、each、many、much 等）时，不管 not 是在它们前面直接否定它们还是在句中否定谓语动词，句子的含义一般是部分否定；② 句中含有 totally、completely、wholly、always 一类副词，同时谓语动词被否定时，句子的含义也是部分否定。

部分否定有时比较难理解，容易被当成全部否定，特别是在 not 不是直接放在 all 一类词的前面而是去否定谓语动词的情况下，例如：All that glitters is not gold. 闪闪发光物，未必尽黄金。因此，在翻译这种结构时要特别谨慎。值得一提的是，all … not 在一定条件下还可表示全部否定，如带有让步意义时（即使所有……也不……），例如：All the money in the world won’t make you happy then. 那么，即使是世界上的所有金钱也不会让你感到幸福。

在现代英语中，尤其是美国英语中，已经有越来越多的人使用 not all … 来表示部分否定，而不用 all … not，以免造成歧义。

计算机安全.知识扩展.翻译

□ 例句1

The individual who authors an e-mail message does not own all rights related to it. 电子邮件的作者并不是所有与电子邮件相关的权利都拥有。

□ 例句2

While all executable programs are eventually read by the computer in machine language, they are not all programmed in machine language. 尽管所有的可执行程序最终都是以机器语言的形式被计算机读入的，但它们并非都是用机器语言编写的。

□ 例句4

A DBMS can support multiple users and not every user should be able to access all the data. 一个数据库管理系统可以支持多个用户，但不是每个用户都应该能够访问所有的数据。

□ 例句5

Hardware and software don’t always do what they are supposed to do. 硬件和软件并不总是做它们该做的事。

计算机安全.知识扩展.翻译

（三）双重否定

双重否定（double negation）是否定之否定，实际上表达的是肯定的意思，所以译成汉语时既可译成双重否定句，也可译成肯定句。

- 例句1

For example, if you receive an e-mail from a client, you cannot immediately post it to your company's website without that client's permission. 例如，如果你收到一位客户的电子邮件，在没有得到该客户允许的情况下，你不能将电子邮件马上发布到你公司的网站上。

- 例句2

Computers, the Internet, and communications technology make it possible to instantly broadcast live reports across the globe, but live reporting is not without controversy. 计算机、因特网及通信技术使即时播出全球现场报道成为可能。但是，对于现场报道不是没有争议的（或：也是有争议的）。

- 例句3

As computers have become more powerful and widespread, operating systems have become extremely complex. Few people can use a computer without one. 随着计算机变得功能更加强大、使用更加广泛，操作系统也变得极其复杂。几乎没有人能使用计算机而不用操作系统。

计算机安全.知识扩展.翻译

英语中有些双重否定结构容易理解错，比如：cannot＋too（或以 over- 为前缀的动词）；否定项＋until（或 till）。

□ 例句4

One can’t be too careful in making the decision as it was such a critical case. 因为这是一个如此重要的问题，所以作出决定时无论怎样谨慎都不会过分。

在这句话中，can’t be too careful 不能理解为“不能太谨慎”，因为联系句子后半部分的状语从句来看，逻辑上讲不通。“cannot … too＋adj / adv”看似只有一个否定项（not），实际上 too 也是一个隐含的否定项，因此它是一个双重否定结构，起加强肯定语气的作用，通常可译作“无论怎样……也不会过分”“越……越好”等。该结构还可有“can never / scarcely / hardly … too＋adj / adv”等变化形式。起相同作用和表示相同意思的还有：“cannot（或 can never / scarcely / hardly 等）＋以 over- 为前缀的动词”；“cannot … enough / sufficient / sufficiently”。

计算机安全·知识扩展·翻译

□ 例句5

Their contribution to computer science can scarcely be overestimated. 他们对计算机科学的贡献无法估量。

□ 例句6

You cannot be careful enough. 你不论怎样小心也不过分。

□ 例句7

For instance, when the computer is printing a document, it cannot start another process or respond to new commands until the printing is completed. 例如，计算机打印文档时，直到打印结束才能开始另外一个进程或响应新的命令。

含有 not 和 until（或 till）的句子容易理解和翻译错，特别是“It is (或 was) not until … that …”的强调结构、以 not until 开头并采用部分倒装的结构、until 在前 not 在后的结构。

□ 例句8

It was not until long afterwards that she wondered if she had made a mistake. 直到很久以后，她才开始思量自己是否犯了一个错误。

计算机安全.知识扩展.翻译

- 例句9

Not until midnight did it stop raining. 直到午夜，雨才停止。

- 例句10

Until the advent of electronic digital computers in the 1940s, computer science was not generally distinguished as being separate from mathematics and engineering. 直到电子数字计算机在20世纪40年代问世，计算机科学才与数学和工程学普遍区别开来。

这句话很容易被错译为“直到电子数字计算机在20世纪40年代问世，计算机科学尚未与数学和工程学普遍区别开来 “。将这样的句子视为双重否定句（像 too 一样，until 是一个隐含的否定项），就容易理解了。也就是说，双重否定等于肯定的意思，可译成 ” 直到……才……” 。

计算机安全.知识扩展.翻译

（四）准否定

准否定（quasi-negation），也称几乎否定、半否定（incomplete negation 或 semi-negation），指含有 few、little、hardly、scarcely、barely、rarely、seldom 等词的句子。这些词虽无否定的词形特征，却含有否定的意思，多翻译为“几乎不……” “几乎没……”等。

□ 例句1

There is hardly any commercial off-the-shelf mobile agent-based application. 几乎没有基于移动主体的现成应用程序。

□ 例句2

Some people treat e-mail informally, so they rarely revise (though they should). 有些人视电子邮件为非正式交流方式，因此他们很少修改（尽管他们应该这样做）。

□ 例句3

A professional can cause great harm through dishonesty, carelessness, or incompetence. Often, the victims have little ability to protect themselves. 一个专业人士可能会因为不诚实、疏忽或不称职造成巨大的伤害。通常情况下，受害者几乎没有能力保护自己。