网络空间安全导论

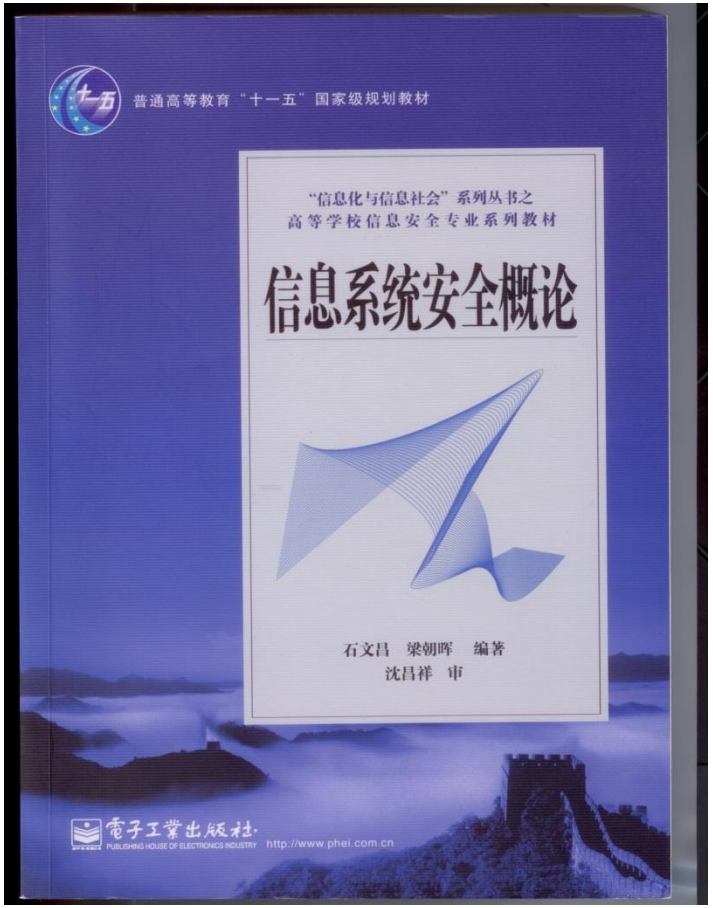
主讲人： 杜瑞颖



目录

主要参考书


“十一五”国家重点图书
可信计算
TRUSTED COMPUTING
张焕国 赵 波 等著
武汉大学出版社


普通高等教育“十一五”国家级规划教材
“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材
信息系统安全概论
石文昌 梁朝晖 编著
沈昌祥 审
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信息系统安全

一 信息系统安全的概念

二 信息系统的硬件系统安全

三 信息系统的操作系统安全

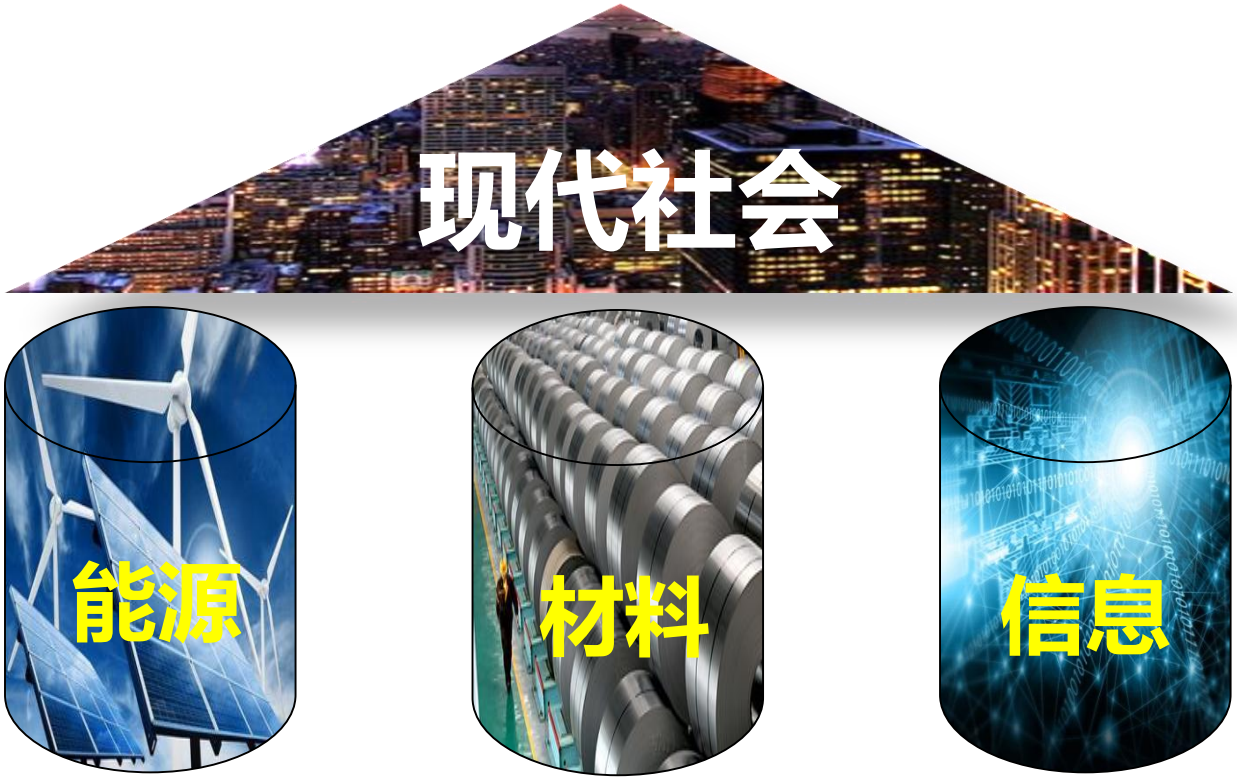
四 信息系统的数据库系统安全

五 可信计算

六 工业控制系统安全

一. 信息系统安全的概念

信息系统安全的概念

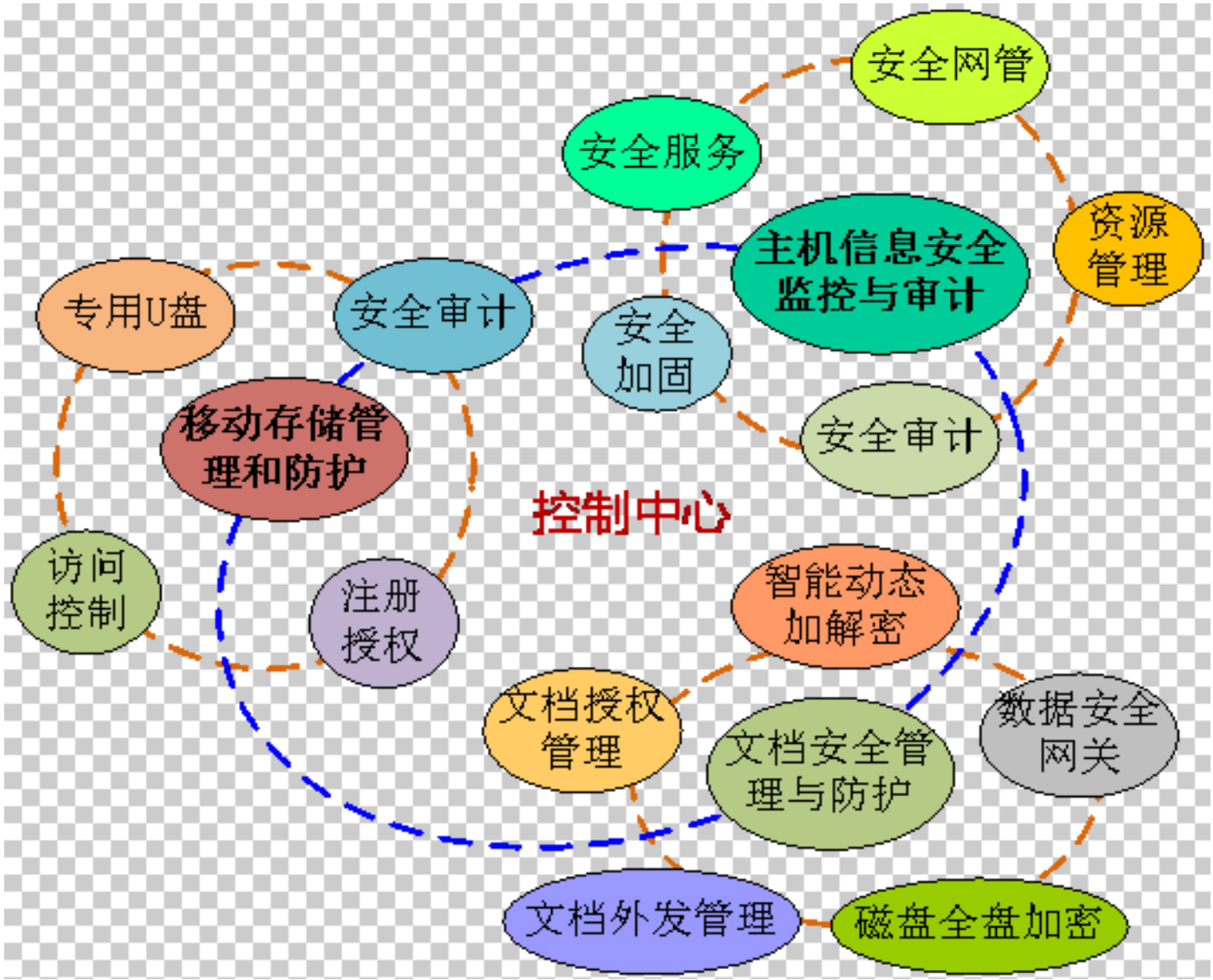


- 从系统角度考虑信息安全是《系统论》科学思想的体现！

- 信息是逻辑的，不能脱离信息系统而独立存在。因此，不能脱离信息系统孤立的谈信息安全。

一. 信息系统安全的概念

信息系统安全的概念



主机安全

一. 信息系统安全的概念

信息系统安全的立体视角

四个层次

1. 设备安全 ⇐ 物理层次的安全
2. 数据安全 ⇐ 逻辑层次的安全
3. 内容安全 ⇐ 语义层次的安全
4. 行为安全 ⇐ 行为层次的安全

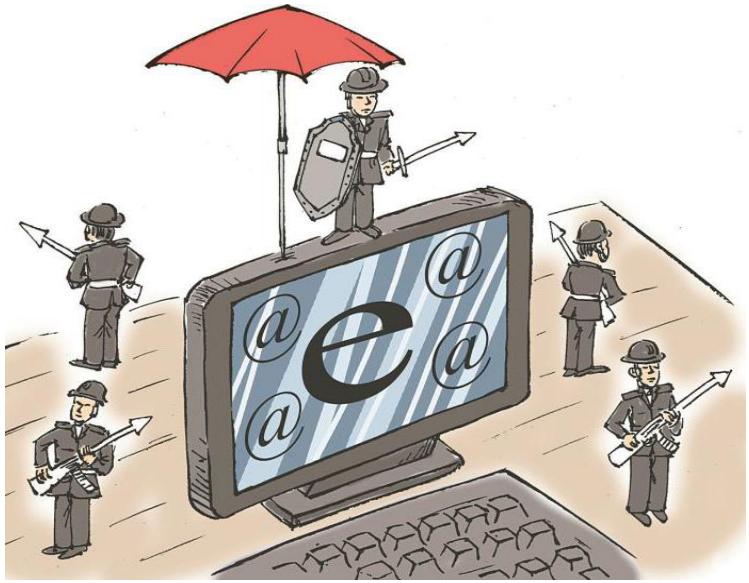
一. 信息系统安全的概念

信息系统安全的概念

- 信息系统是信息的载体，是直接面对用户的服务系统。
- 信息系统安全的特点是从系统级的整体上考虑安全威胁与防护。
- 它研究信息系统的安全威胁、信息系统安全的理论、信息系统安全技术和应用。

研究方向与内容：

- 硬件系统安全
- 软件系统安全
- 访问控制
- 可信计算
- 信息系统安全测评认证
- 信息系统安全等级保护



信息系统安全

一 信息系统安全的概念

二 信息系统的硬件系统安全

三 信息系统的操作系统安全

四 信息系统的数据库系统安全

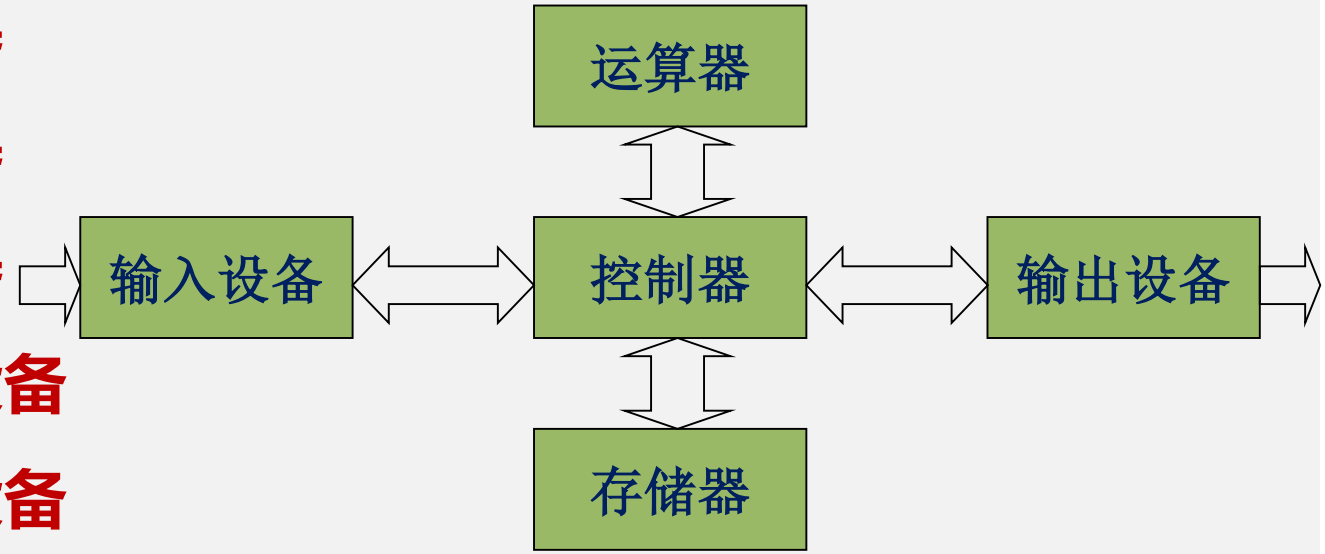
五 可信计算

六 工业控制系统安全

二. 信息系统的硬件系统安全

计算机系统的硬件结构

- 计算机系统是信息系统的核心，所有的信息系统都由计算机作为核心，进行信息数据处理与行为控制。
- 计算机系统的硬件结构
  - 运算器
  - 控制器
  - 存储器
  - 输入设备
  - 输出设备



二. 信息系统的硬件系统安全

计算机硬件系统的安全

计算机硬件系统的安全问题属于信息系统安全四个层次中的物理安全层次，即设备安全

- 设备的稳定性(Stability)
  设备在一定时间内不出故障的概率。
- 设备的可靠性(Reliability)
  设备能在一个给定时间内正常执行任务的概率。
- 设备的可用性(Availabity)
  设备随时可以正常使用的概率。

- 如果仅考虑物理原因，则确保设备稳定、可靠、可用的技术，称为容错（Fault Tolerant）技术
- 如果仅考虑自然灾害原因，则确保设备稳定、可靠、可用的技术，称为容灾（Disaster Tolerant）技术
- 如果仅考虑恶意攻击原因，则确保系统安全、可用的技术，称为容侵(Intrusion Tolerant)技术。

信息设备的安全是信息系统安全的首要问题

二. 信息系统的硬件系统安全

计算机硬件系统的安全——容错技术

容错技术是利用资源冗余增强系统可靠性的技术

- **数据冗余：利用数据冗余增强系统的可靠性。**

  例如：设有7位二进制数，给它增加1位，形成一个8位的二进制数。所增加的这个第8位数据要使得这个8位二进制数中含有偶数个“1”。

  举例：设7位二进制数为0 1 1 0 0 1 1，增加一个0，最终的8位二进制数为：0 1 1 0 0 1 1 0，把它发送到对方，对方收到后重新数一下其中1的个数，若为偶数则认为正确，若为奇数则肯定发生了错误。从而检测了错误。这种方法能够检测所有奇数个错误。

二. 信息系统的硬件系统安全

计算机硬件系统的安全——避错技术

- **容错技术是被动的，最好是不发生故障。但是不发生故障是不可能的。**
- **最好是能够减少故障的发生，这种技术称为避错技术。**

- **设计阶段**：精心设计，减少设计错误。
- **试验阶段**：反复试验，精心分析，发现并改正可能的错误。
- **实现阶段**：采用高可靠性的元器件，进行元器件老化。
- **测试间断**：充分测试，发现并改正可能的错误。

二. 信息系统的硬件系统安全

- **容灾技术：应对自然灾害**
  - 自然灾害的破坏性很大。
  - 因此，一般采用多备份的应对方法。
  - 美国911事件之后，增加考虑异地备份。

二. 信息系统的硬件系统安全

计算机硬件系统的安全——容侵技术

■ **容侵技术：在有恶意攻击时，确保系统安全可用的技术。**

- **可生存性：在存在攻击的情况下，系统仍可以正常工作的概率。**
- **容侵度：容忍攻击的程度。**
  - 容侵程度高是指系统、数据库、应用遭受到侵犯后的容忍程度比较高，能使受攻击侵犯的影响降到最低。
  - 重构
  - 降级服务

二. 信息系统的硬件系统安全

计算机硬件系统的安全——故障安全性

- **故障安全性(safety):确保系统在故障时能够处于无危险的状态。**

- 举例：我国动车在温州发生相撞，造成严重灾难。调查的结果是雷击信号设备，使信号灯常亮绿色。对面的动车看到绿色信号，便照常行使，结果造成撞车。设想一下，**如果信号设备被雷击后信号灯常亮红色，则不会造成撞车。**
- 数据不合理，可引发产生故障
- 程序不合理，也可引发产生故障

二. 信息系统的硬件系统安全

计算机硬件系统的安全

- 由于计算机硬件系统处于任何信息系统的最底层，所以硬件系统安全是信息系统安全的基础。
- 由于集成电路技术的发展，使得在硬件中植入病毒和木马成为轻而易举的事。
- 硬件中的病毒木马更隐蔽，更不易检测，因此危害更大。

二. 信息系统的硬件系统安全

计算机硬件系统的安全

- **密码芯片的侧信道攻击(Side Channal Attack):**
  - **原理：在二进制情况下，0和1在工作时所消耗的电能不同，据此可以推测出密钥或密码算法。**
  - **除了电能消耗外，还有其它参数可用于攻击。如时间、声音等。**
  - **目前，基于物理参数的侧信道攻击已于数学攻击结合起来，攻击威力更大。**

信息系统安全

一 信息系统安全的概念

二 信息系统的硬件系统安全

三 信息系统的操作系统安全

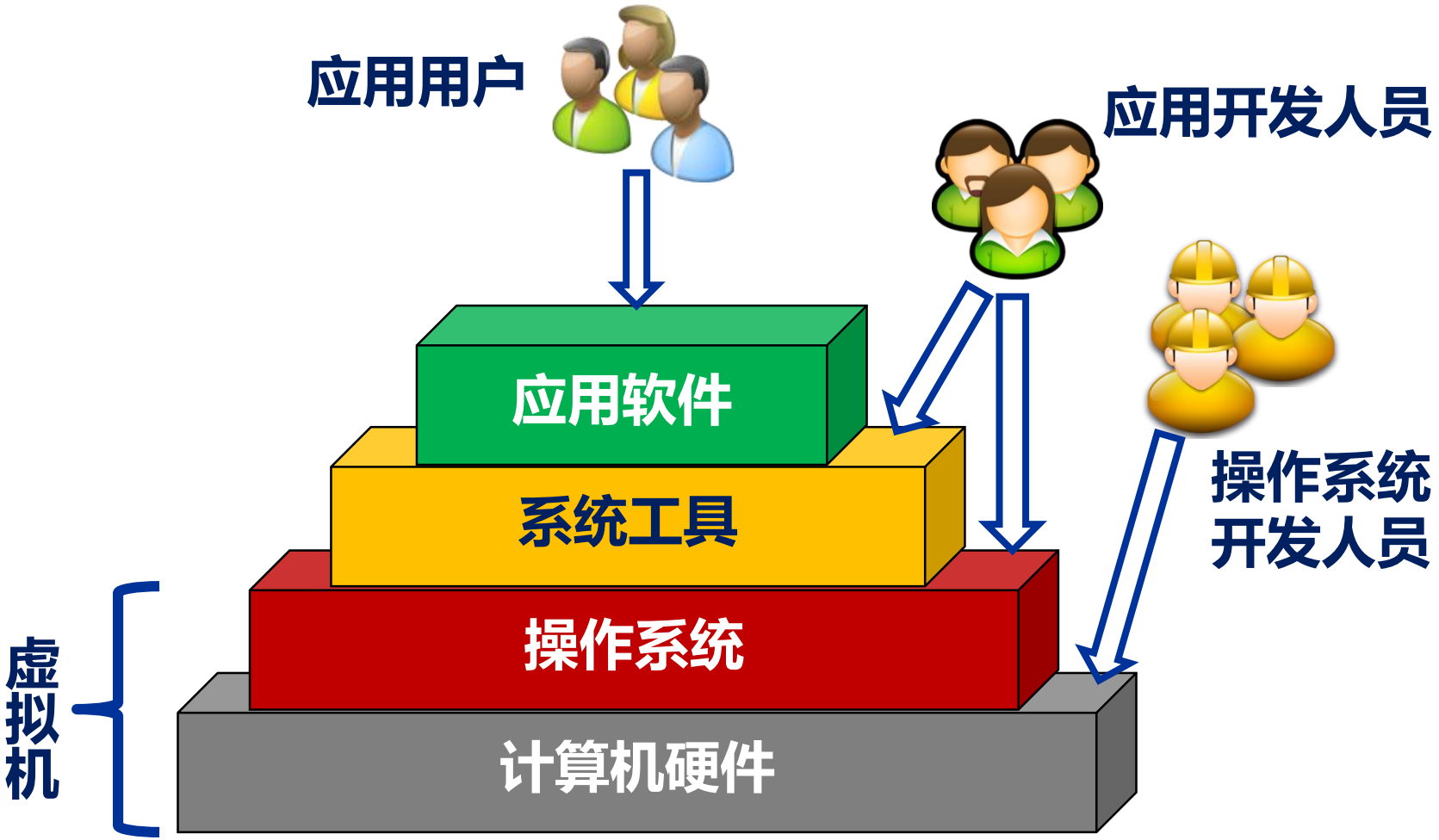
四 信息系统的数据库系统安全

五 可信计算

六 工业控制系统安全

三. 信息系统的操作系统安全

计算机操作系统的概念

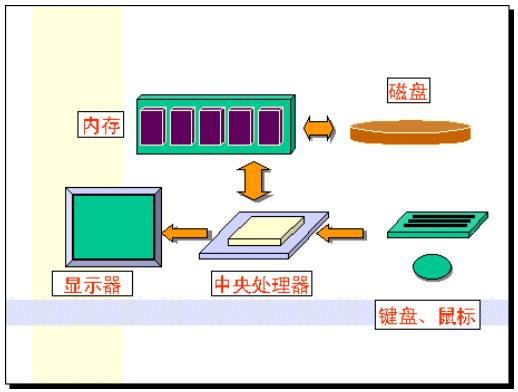


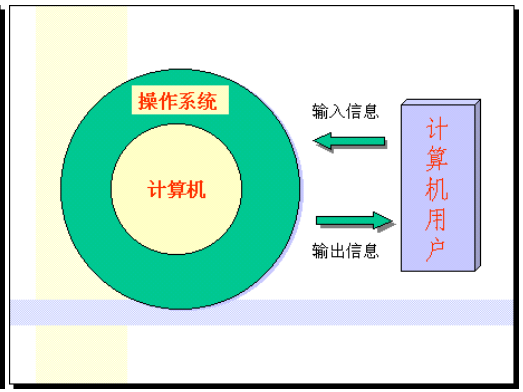
操作系统的地位：紧贴硬件之上，所有其他软件之下（是其他软件的共同环境）。

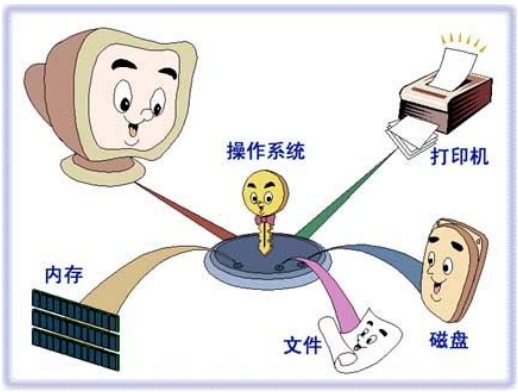
三. 信息系统的操作系统安全

计算机操作系统的概念

- 控制和管理计算机系统内各种硬件和软件资源
- 合理有效地组织计算机系统的工作
- 为用户提供一个使用方便可扩展的工作环境
- 起到连接计算机和用户的接口作用







三. 信息系统的操作系统安全

计算机操作系统的概念

- **操作系统是十分复杂的系统，目前尚没有统一定义:**
  - 定义1：操作系统是介于计算机硬件和用户（人和程序）之间的接口。
  - 定义2：操作系统是一种使其它程序更加方便、有效执行的一组程序。
  - 定义3：操作系统作为计算机资源的管理者，管理着计算机的每个部件的活动，确保每个资源的合理使用。

三. 信息系统的操作系统安全

计算机操作系统的安全

- 由于操作系统是计算机资源的管理者，因此**对于操作系统来说，计算机的所有资源都是可获得的，是无密可言的。**
- 由于操作系统十分复杂庞大(几千万行程序)，目前任何操作系统公司都不能保证其产品是100%正确的。
  - Windows操作系统几乎每周都在发布漏洞和补丁
- 由于操作系统的不正确所造成的故障，一般是可以被容忍的
- 一般，平均1000行程序就会产生一个漏洞。Win8操作系统的漏洞将是大量的。
- 如果操作系统的漏洞被黑客利用，所造成的损失将是灾难的。

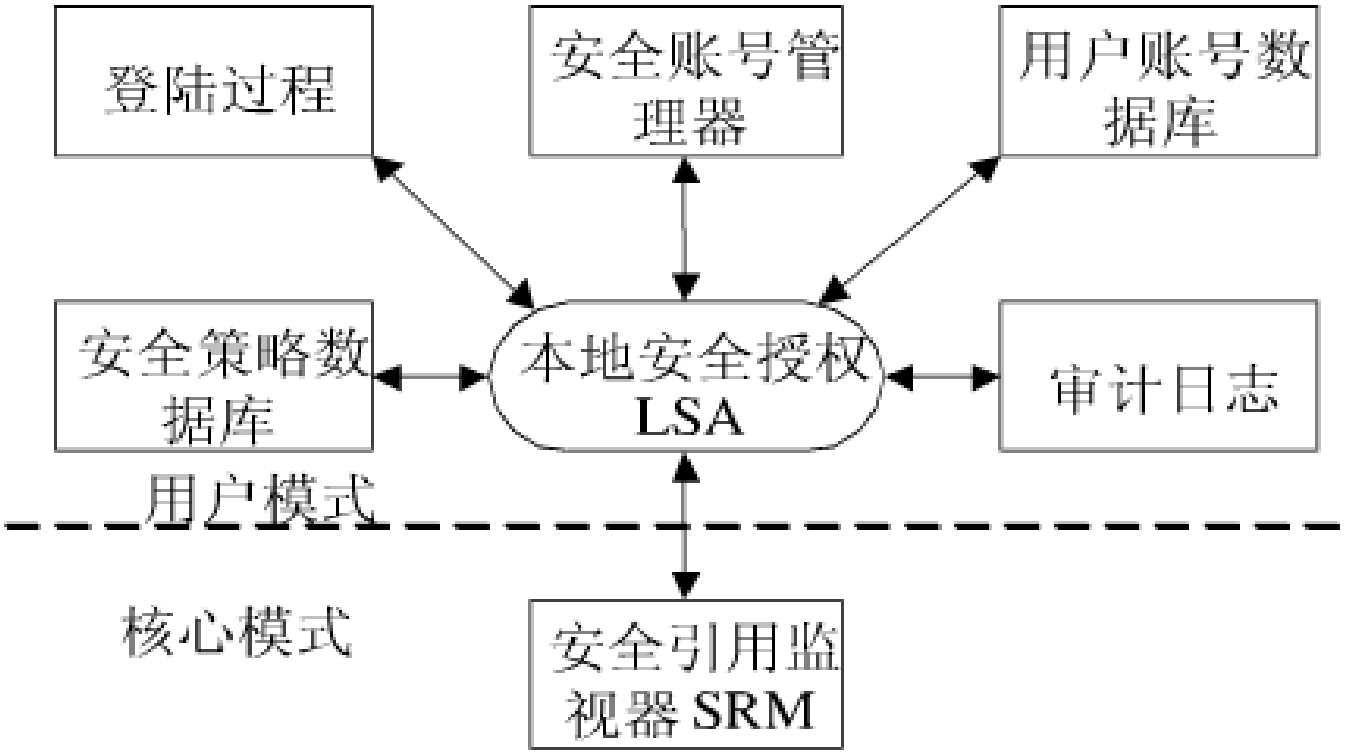
三. 信息系统的操作系统安全

计算机操作系统的安全

三. 信息系统的操作系统安全

计算机操作系统的安全

Windows 系统安全模型



Windows安全模型

三. 信息系统的操作系统安全

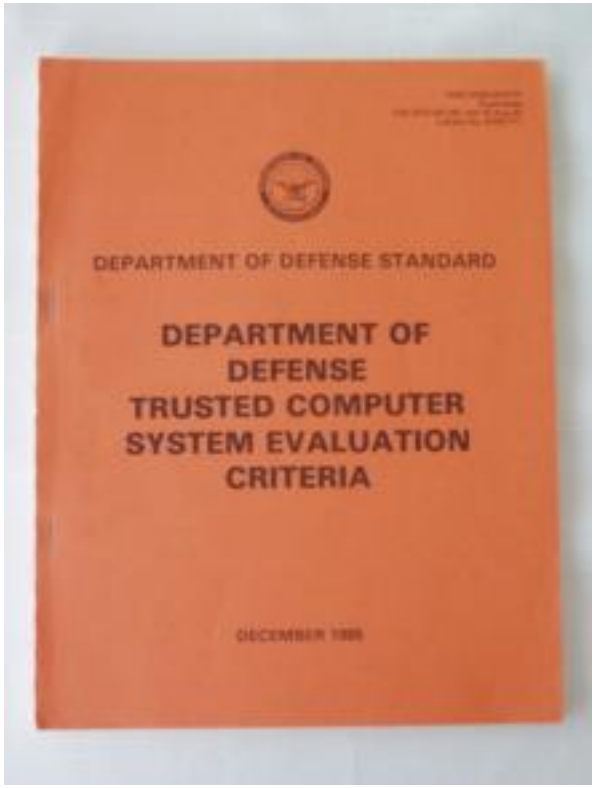
计算机操作系统的安全

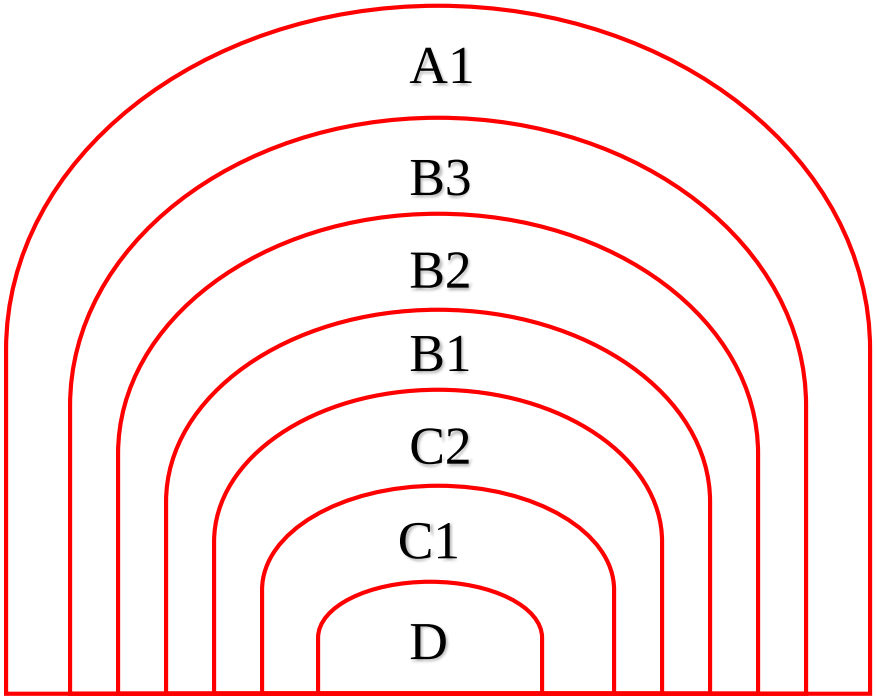
- 1983年美国国防部颁布了《可信计算机系统评价标准》(TCSEC)，简称桔皮书。
- 桔皮书把计算机的安全划分为4个级别(D,C,B,A)，每个级别又可以细分为若干等级。
  - 目前有：D，C1，C2，B1，B2，B3，A1,共7个等级。
  - D级操作系统是不安全操作系统
  - B2级以上的才是安全操作系统
  - Windows属于C2级操纵系统
  - 波音公司使用A1级的操作系统

三. 信息系统的操作系统安全

计算机操作系统的安全

桔皮书把计算机的安全划分为4个级别7个等级。





三. 信息系统的操作系统安全

计算机操作系统的安全

- 仅有操作系统安全是不够的，后来美国国防部又发布了其它系统的安全标准。由于这套文件用了不同的彩色封面，被称为彩虹系列。
- “彩虹系列“丛书以美国国防部《可信计算机系统评测标准（TCSEC）》为核心，对评测标准进行扩充、提供了关键的背景知识、对关键的概念进行深入解释和分析，并且提出了具体的实现方法和措施。该丛书共三十多册。

三. 信息系统的操作系统安全

计算机操作系统的安全

- “彩虹系列”丛书是信息系统安全事业的里程碑，对信息系统安全领域具有深远的影响。
- 它不但建立了一个标准，更建立了一套体系。
- 目前，虽然更新的、更符合网络信息时代要求的国际信息系统安全标准不断涌现，但是“彩虹系列”丛书所提出的基本概念、原则和方法仍然被普遍接受和使用。
- 无论是信息安全领域的研究、信息安全产品的开发和使用还是准备CISSP考试，这套丛书都是不可多得的参考材料。

三. 信息系统的操作系统安全

计算机操作系统的安全

- 2012年微软发布WIN8操作系统，全面支持可信计算，安全性提高到新阶段。
- 中国的操作系统状况
  - 目前广泛使用WINDOWS操作系统
  - 存在严重的安全隐患
- 工信部执行“核高基”计划：
  - 核心芯片，高级计算机，基础软件（操作系统、数据库）
  - 自主开发出《麒麟》和《红旗Linux》操作系统
  - 中标软件与武汉大学合作，使《麒麟操作系统》支持可信计算
  - 军队使用《麒麟操作系统》
- 国产操作系统的困难，不是技术问题，而是市场问题

三. 信息系统的操作系统安全

- **我国操作系统等基础软件长期依赖国外。**
- **操作系统有漏洞、数据库系统有漏洞、BIOS有漏洞、应用软件有漏洞。**
- **漏洞和后门被对手利用实施攻击，可造成严重后果！**

- 根据中央国家机关政府采购对《2007-2010年中央国家机关各部门及其下属各级行政事业单位通过协议供货采购通用软件情况的总结》显示，4年来，采购中心共采购通用软件14大类总额为10.69亿元。其中国外品牌通用软件采购总金额为8.79亿元，占通用软件采购金额的82.2%；在操作系统、数据库、办公软件等领域，微软、甲骨文等国外巨头占垄断地位。

三. 信息系统的操作系统安全

操作系统

- 2014年2月10号北京中科红旗软件技术有限公司贴出清算公告，宣布公司正式解散。
- 2014年4月8日WindowsXP正式退役。

这两件大事给中国操作系统行业和相关安全领域带来了巨大影响。

三. 信息系统的操作系统安全

红旗操作系统

- 中国红旗公司自己开发的Linux系统曾多年占据中国国产操作系统占有率第一名，但是从市场份额角度分析来说，这项产品从开发使用开始一直都是计划经济的产物，依靠着政府的采购或者邮政之类的大型系统大客户的支持，所以在面对市场化经济的条件下，一个未能全面参与市场竞争的企业是很难在失去国家资金的支持下走向成功的。

三. 信息系统的操作系统安全

WindowsXP

- 2001年WindowsXP发布至今，互联网技术和互联网安全环境已经让XP系统越来越疲于应对，这也就是出现WindowsXP的漏洞比升级版本还要大还要多，所以WindowsXP就更加容易成为黑客攻击的目标，并且就目前移动互联网大数据与云时代等多方面应用的发展到来，WindowsXP具有的模式没有能力兼容现在发展中的应用，进而阻碍了相关行业的高速发展，包括研发WindowsXP系统的微软也深受其害，所以微软选用暴力手段，让WindowsXP结束它的使命。

三. 信息系统的操作系统安全

WindowsXP事件警告我们：

拥有一个自主独立研发的计算机操作系统的重要性

- 现状是，我国90%以上的企业使用的是Windows系列产品，并且未将Windows的迁移纳入IT发展路线中，从这些角度讲，大到军工军事，社会机构到个人企业，一切的软件安全都由WindowsXP保障，那么当微软选择放弃WindowsXP时，我们就不得不做出选择，要么跟随Windows系列升级，要么就只能继续使用失去安全漏洞保护的WindowsXP系统，但后者要面临巨大的安全风险。

三. 信息系统的操作系统安全

□ 微软为中国政府定制Win10特别提供版系统

◆ Windows 10的免费升级迅速获得了大量用户，但系统安全问题却一再受到质疑。甚至俄罗斯政府将其告上法庭，认为其是间谍软件。但是作为用户基础良好，生态环境完善又免费的Windows最新一代系统，Windows 10得到了中国政府的青睐。

◆ **在2015年12月的乌镇世界互联网大会上，微软宣布将为中国政府打造一款专属的Windows 10系统。2015年12月，微软宣布将与中国电子科技集团公司合资成立C&M Information Technologies（中国微软信息科技），合资公司注册资本金4000万美元，双方股比为中国电科51%，微软公司49%。微软与CETC一起合作，打造出了“Windows特供版”。**

信息系统安全

一 信息系统安全的概念

二 信息系统的硬件系统安全

三 信息系统的操作系统安全

四 信息系统的数据库系统安全

五 可信计算

六 工业控制系统安全

四、信息系统的数据库系统安全

数据库系统的概念

- 数据库系统也要靠操作系统的支持。
- 操作系统和编译系统为系统软件。又因为数据库系统的重要性，于是又把操作系统、编译系统和数据库系统称为基础软件。
- **国产数据系统**：达梦数据库（华科冯玉才），OceanBase（阿里）等。
- 国产数据库系统的困难与操作系统一样，不是技术问题，而是市场问题。

四、信息系统的数据库系统安全

数据库系统的安全

- 数据库系统的特殊性
  - 数据库中的数据量大。
  - 数据库中的许多数据，存储时间长。
  - 数据库要支持查询、插入、删除、更新等操作。
  - 数据库要靠操作系统支持，因此数据库安全措施要与操作系统衔接。
- 数据库的安全措施应适应数据库的这些特点。

四、信息系统的数据库系统安全

数据库系统的安全

- **数据库系统的一个特殊安全问题是存在推理攻击(Inference Attack)。**
  - **推理攻击**：用户利用多次允许的访问结果，通过推理得到他不能访问的结果。
  - **统计数据库**：数据库的个体数据是不允许访问的，但是允许访问数据库的统计信息。
  - **统计数据库特别容易受到推理攻击。**
  - **理论证明：对于统计数据库，完全避免推理攻击是不可能的。**
  - **原因是事物之间是有联系的，俗话说：知道了你的昨天和今天，就知道了你的明天。**
  - **由此可推论：隐私保护作不到完全保护，一点都不泄露。**

四、信息系统的数据库系统安全

数据库系统的安全

- 美国国防部在发表桔皮书（TCSEC）后，又发布了可信数据库解释TDI（Trusted Datebase Interpretation）
- TDI对可信数据库的安全性给出了具体的要求
- TDI需要TCSEC的支持，因此与TCSEC衔接
- TDI的主要内容分五个主题：
  - 系统集成
  - 可分评估
  - 子集约束
  - 局域划分
  - 应用解释

思考题

1. 上网搜集资料，计算机技术的发展。
2. 了解操作系统和数据库系统的安全问题。
3. 了解我国在操作系统和数据库方面的发展。

谢谢！