

NEW PLAN

软考高级架构师

信息安全技术



01.

考点介绍



历年出题和本章知识点

- 本章在每年考情中一般占**2~4**分，基本无超纲。
- 第二版教材里新增了一些抗攻击技术，安全架构，风险评估以及组织框架等内容。

1. 信息安全基础
2. 安全系统组成框架
3. 信息安全技术
4. 信息安全的抗攻击技术
5. 信息安全的保证体系和评估方法
6. 网络安全技术
7. 网络安全协议

· 02 ·

信息安全基础



系统安全防范体系

系统安全防范体系也是分层次的，不同层次反映了不同的安全问题，根据网络的应用现状情况和结构，可以将安全防范体系的层次划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理。

- ① 物理环境的安全性。物理层的安全包括通信线路、物理设备和机房的安全等。
- ② 操作系统的安全性。系统层的安全问题来自计算机网络内使用的操作系统的安全。主要表现在3个方面，一是由操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制和系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。
- ③ 网络的安全性。网络层的安全问题主要体现在计算机网络方面，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等。
- ④ 应用的安全性。应用层的安全问题主要由提供服务所采用的应用软件和数据的安全性产生，包括Web服务、电子邮件系统和DNS等。此外，还包括病毒对系统的威胁。
- ⑤ 管理的安全性。安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。



信息安全基本要素

- 信息安全包括5个基本要素：机密性、完整性、可用性、可控性与可审查性。
1. 机密性：确保信息不暴露给未授权的实体或进程。
 2. 完整性：只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改。
 3. 可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。
 4. 可控性：可以控制授权范围内的信息流向及行为方式。
 5. 可审查性：对出现的信息安全问题提供调查的依据和手段。

信息安全范围

- 信息安全的范围包括：设备安全、数据安全、内容安全和行为安全。
- 1. 信息系统设备的安全是信息系统安全的首要问题，是信息系统安全的物质基础，它包括3个方面：设备的稳定性、可靠性、可用性。
- 2. 数据安全即采取措施确保数据免受未授权的泄露、篡改和毁坏，包括3个方面：数据的秘密性、完整性、可用性。
- 3. 内容安全是信息安全在政治、法律、道德层次上的要求，包括3个方面：信息内容政治上健康、符合国家法律法规、符合道德规范。
- 4. 信息系统的服务功能是指最终通过行为提供给用户，确保信息系统的行为安全，才能最终确保系统的信息安全。行为安全的特性包括：行为的秘密性、完整性、可控性。

信息存储安全

◆ 信息的存储安全包括信息使用的安全、系统安全监控、计算机病毒防治、数据的加密和防止非法的攻击等。

1. 信息使用的安全 。包括用户的标识与验证 、用户存取权限限制 。
2. 系统安全监控 。系统必须建立一套安全监控系统 ，全面监控系统的活动 ，并随时检查系统的使用情况，一旦有非法入侵者进入系统，能及时发现并采取相应措施，确定和填补安全及保密的漏洞 。还应当建立完善的审计系统和日志管理系统 ，利用日志和审计功能对系统进行安全监控。
3. 计算机网络服务器必须加装网络病毒自动检测系统，以保护网络系统的安全 ，防范计算机病毒的侵袭，并且必须定期更新网络病毒检测系统。

网络安全

- ◆ 网络安全隐患（漏洞）：物理安全性、软件安全漏洞、不兼容使用安全漏洞、选择合适的安全哲理。
- ◆ 网络安全威胁：非授权的访问、信息泄露或丢失、破坏数据完整性、拒绝服务攻击、利用网络传播病毒。
- ◆ 安全措施的目标：访问控制、认证、完整性、审计、保密。



信息安全系统组成框架

◆ 框架通常由**技术体系**、**组织机构**、**管理体系**共同构建。**技术体系**：从实现技术上来看，信息安全系统涉及以下技术：

- ① **基础安全设备**包括**密码芯片**、**加密卡**、**身份识别卡**等，此外还涵盖运用到**物理安全**的物理环境保障技术，建筑物、机房条件及硬件设备条件满足信息系统的机械防护安全，通过对电力供应设备以及信息系统组件的抗电磁干扰和电磁泄漏性能的选择性措施达到相应的安全目的。
- ② **计算机网络安全**指**信息在网络传输过程中的安全防范**，用于防止和监控**未经授权破坏**、**更改和盗取**数据的行为。通常涉及物理隔离，防火墙及访问控制，加密传输、认证、数字签名、摘要，隧道及VPN技术，病毒防范及上网行为管理，安全审计等实现技术。
- ③ **操作系统安全**是指操作系统的**无错误配置**、**无漏洞**、**无后门**、**无特洛伊木马**等，能防止非法用户对计算机资源的非法存取，**一般用来表达对操作系统的安全需求**。操作系统的安全机制包括标识与鉴别机制、访问控制机制、最小特权管理、可信通路机制、运行保障机制、存储保护机制、文件保护机制、安全审计机制，等等。
- ④ **数据库安全**可粗略划分为**数据库管理系统安全**和**数据库应用系统安全**两个部分，主要涉及物理数据库的完整性、逻辑数据库的完整性、元素安全性、可审计性、访问控制、身份认证、可用性、推理控制、多级保护以及消除隐通道等相关技术。
- ⑤ **终端安全设备**从电信网终端设备的角度分为**电话密码机**、**传真密码机**、**异步数据密码机**等。



考试真题

网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行。其中，数据库容灾属于（ ）。

- A. 物理线路安全和网络安全
- B. 应用安全和网络安全
- C. 系统安全和网络安全
- D. 系统安全和应用安全

答案：D

试题解析：数据库属于应用系统，又与操作系统相关，因此属于系统安全和应用安全。



考试真题

在进行软件系统安全性分析时，（）保证信息不泄露给未授权的用户、实体或过程；完整性保证信息的完整和准确，防止信息被非法修改；（）保证对信息的传播及内容具有控制的能力，防止为非法者所用。

A.完整性

B.不可否认性

C.可控性

D.机密性

A.完整性

B.安全审计

C.加密性

D.可控性

答案：D、D

完整的信息安全系统至少包含三类措施，即技术方面的安全措施、管理方面的安全措施和相应的（）。其中，信息安全的技术措施主要有：信息加密、数字签名、身份鉴别、访问控制、网络控制技术、反病毒技术、（）。

A.用户需求

B.政策法律

C.市场需求

D.领域需求

A.数据备份和数据测试

B.数据迁移和数据备份

C.数据备份和灾难恢复

D.数据迁移和数据测试

答案：B、C