第3章 物理安全

主要内容

3.1 概述

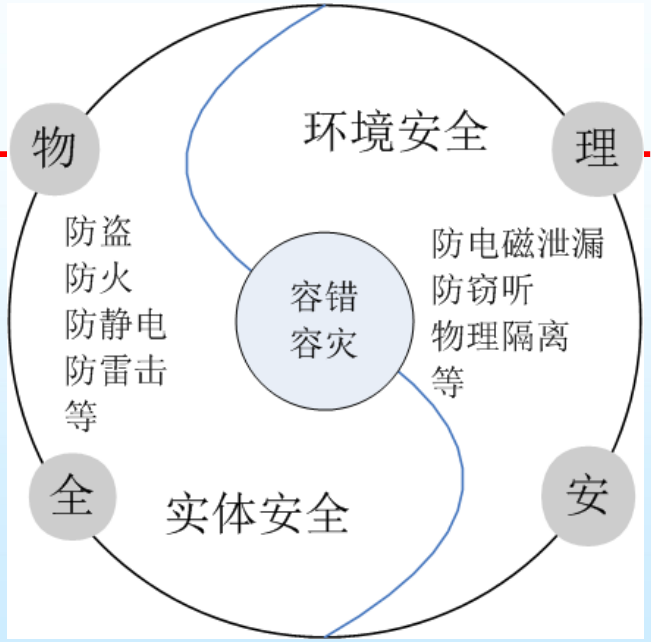
3.2 设备安全防护

3.3 防信息泄露

3.4 物理隔离

3.5 容错与容灾

3.1 概述



- 物理安全:实体安全和环境安全
- 解决两个方面问题:
  - 对信息系统实体的保护；
  - 对可能造成信息泄漏的物理问题进行防范。
- 物理安全技术包括:
  - 防盗、防火、防静电、防雷击、防信息泄漏、物理隔离；
  - 基于物理环境的容灾技术和物理隔离技术也属于物理安全技术范畴。
- 物理安全是信息安全的必要前提
  - 如果不能保证信息系统的物理安全，其他一切安全内容均没有意义。

3.2 设备安全防护

3.2.1 防盗

- 计算机也是偷窃者的目标，计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，
- （1）安全保护设备
  - 有源红外报警器、无源红外报警器和微波报警器等；
  - 计算机系统是否安装报警系统，安装什么样的报警系统，要根据系统的安全等级及计算机中心信息与设备的重要性来确定。
- （2）防盗技术
  - 在计算机系统和外部设备上加无法去除的标识；
  - 使用一种防盗接线板，一旦有人拔电源插头，就会报警；
  - 可以利用火灾报警系统，增加防盗报警功能；
  - 利用闭路电视系统对计算机中心的各部位进行监视保护等。

3.2.2 防火

- ◆火灾因素：
  - ➢ 电气原因、人为因素或外部火灾蔓延引起的
- ◆计算机机房的主要防火措施如下：
  - ➢ 计算机中心选址
  - ➢ 建筑物的耐火等级
  - ➢ 不间断供电系统或自备供电系统
  - ➢ 防雷设施与抗静电地板
  - ➢ 严禁存放腐蚀性物品和易燃易爆物品
  - ➢ 禁止吸烟和随意动火

3.2.3 防静电

- 静电产生：接触 → 电荷 → 转移 → 偶电层形成 → 电荷分离。
- 静电是一种电能，具有高电位、低电量、小电流和作用时间短的特点。
- 静电放电火花造成火灾，还能使大规模集成电损坏，这种损坏可能是不知不觉造成的。
- 静电防范：
  - 静电的泄漏和耗散、静电中和、静电屏蔽与接地、增湿等。防范静电的基本原则是“抑制或减少静电荷的产生，严格控制静电源”。

3.2.4 防雷击

- 雷电防范的主要措施是：
  - 根据电气及微电子设备的不同功能及不同受保护程序和所属保护层来确定防护要点做分类保护。
- 常见的防范措施主要包括：
  - 接闪：让闪电能量按照人们设计的通道泄放到大地中去。
  - 接地：让已经纳入防雷系统的闪电能量泄放入大地。
  - 分流：一切从室外来的导线与接地线之间并联一种适当的避雷器，将闪电电流分流入地。
  - 屏蔽：屏蔽就是用金属网、箔、壳、管等导体把需要保护的对象包围起来，阻隔闪电的脉冲电磁场从空间入侵的通道。

3.3 防信息泄露

3.3.1 电磁泄露

◆目前利用计算机的电磁泄漏窃取信息是国内外情报机关获取信息的重要途径。因此防止信息电磁泄漏已成为网络信息安全的重要课题，应受到我们足够重视。

TEMPEST

◆ TEMPEST技术（Transient Electromagnetic Pulse Emanation Surveillance Technology）

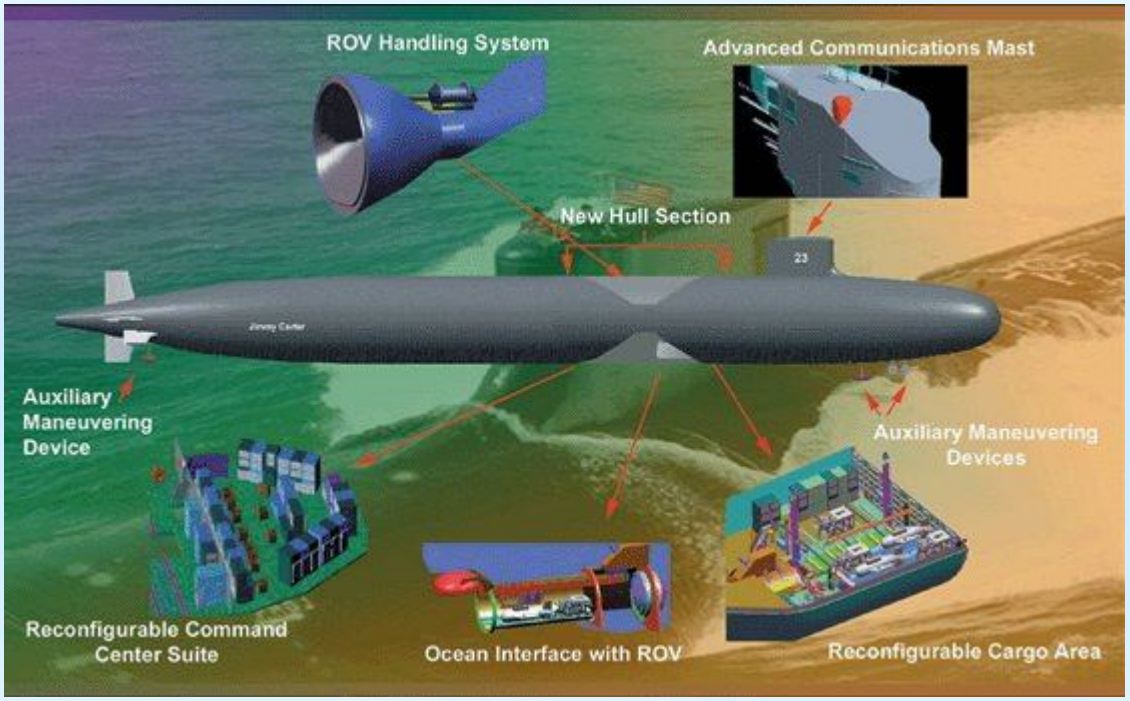
- 通常我们把输入、输出的信息数据信号及它们的变换称为核心红信号
- 那些可以造成核心红信号泄密的控制信号称为关键红信号，红信号的传输通道或单元电路称为红区。
- 所谓的“TEMPEST”要解决的问题就是防止红信号发生电磁信息泄漏。

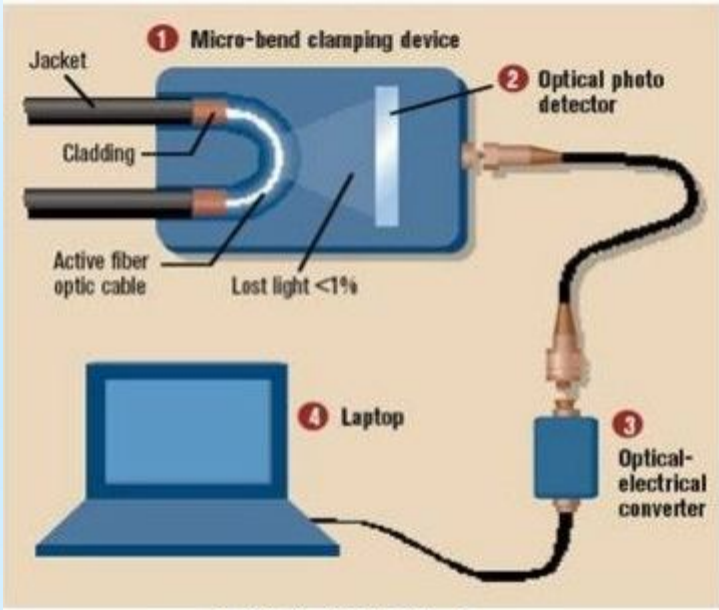
防电磁信息泄漏

- 主要包括三个层面，
  - 一是抑制电磁发射，采取各种措施减小“红区”电路电磁发射；
  - 二是屏蔽隔离，在其周围利用各种屏蔽材料使红信号电磁发射场衰减到足够小，使其不易被接收，甚至接收不到；
  - 三是相关干扰，采取各种措施使相关电磁发射泄漏即使被接收到也无法识别。

3.3.2 窃听

◆ 窃听是指通过非法的手段获取未经授权的信息。





光纤窃听的原理

3.4 物理隔离

◆3.4.1 物理隔离的理解

- **较早时描述的单词Physical Disconnection**
- **后来Physical Separation和Physical Isolation**
- **目前开始使用Physical Gap这个词汇，直译为物理隔离，意为通过制造物理的豁口，来达到物理隔离的目的。**

3.4.2物理隔离与逻辑隔离

◆ 物理隔离与逻辑隔离

- **物理隔离的哲学是不安全就不连网,要绝对保证安全；**
  - ✓物理隔离部件的安全功能应保证被隔离的计算机资源不能被访问（至少应包括硬盘、软盘和光盘），计算机数据不能被重用（至少应包括内存）。
- **逻辑隔离的哲学是在保证网络正常使用下,尽可能安全**
  - ✓逻辑隔离部件的安全功能应保证被隔离的计算机资源不能被访问，只能进行隔离器内外的原始应用数据交换。

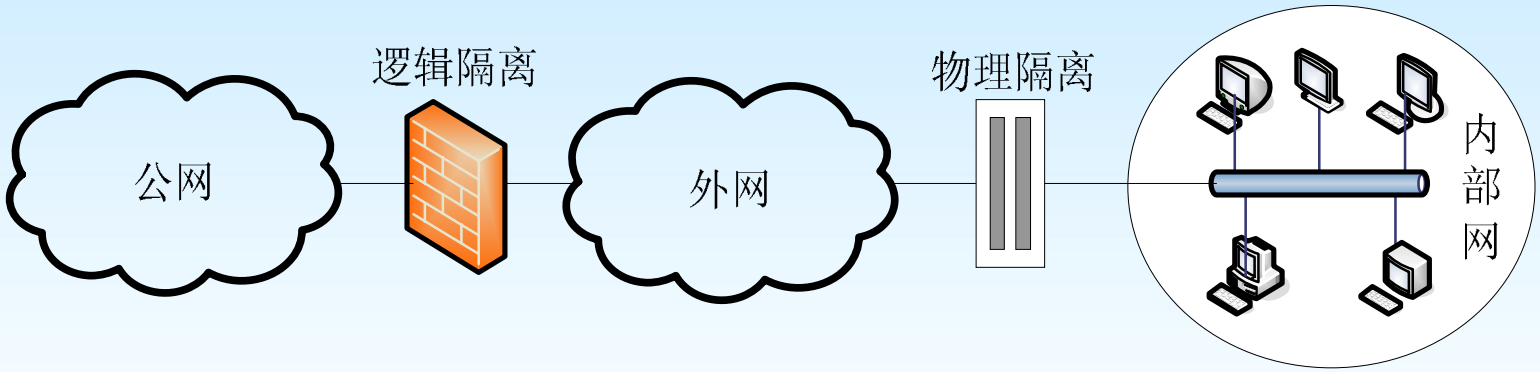


图3.2 企业网络的划分

3.5 容错与容灾

3.5.1 容错

◆保证系统可靠性的三条途径

- 避错是完善设计和制造，试图构造一个不会发生故障的系统，但这是不太现实的
- 纠错做为避错的补充。一旦出现故障，可以通过检测、排除等方法来消除故障，再进行系统的恢复。
- 容错是第三条途径。其基本思想是即使出现了错误，系统也可以执行一组规定的程序；

容错系统

① 高可用度系统：可用度用系统在某时刻可以运行的概率衡量。高可用度系统面向通用计算机系统，用于执行各种无法预测的用户程序，主要面向商业市场。

② 长寿命系统：长寿命系统在其生命期中不能进行人工维修，常用于航天系统。

③ 延迟维修系统：延迟维修系统也是一种容灾系统，用于航天、航空等领域，要求满足在一定阶段内不进行维修仍可保持运行。

④ 高性能系统：高性能系统对于故障（瞬间或永久）都非常敏感，因此应当具有瞬间故障的自动恢复能力，并且增加平均无故障时间。

⑤ 关键任务系统：关键任务系统出错可能危及人的生命或造成重大经济损失，要求处理正确无误，而且恢复故障时间要最短。

常用的数据容错技术

① 空闲设备：也称双件热备，就是备份两套相同的部件。当正常运行的部件出现故障时，原来空闲的一台立即替补。

② 镜像：镜像是把一份工作交给两个相同的部件同时执行，这样在一个部件出现故障时，另一个部件继续工作。

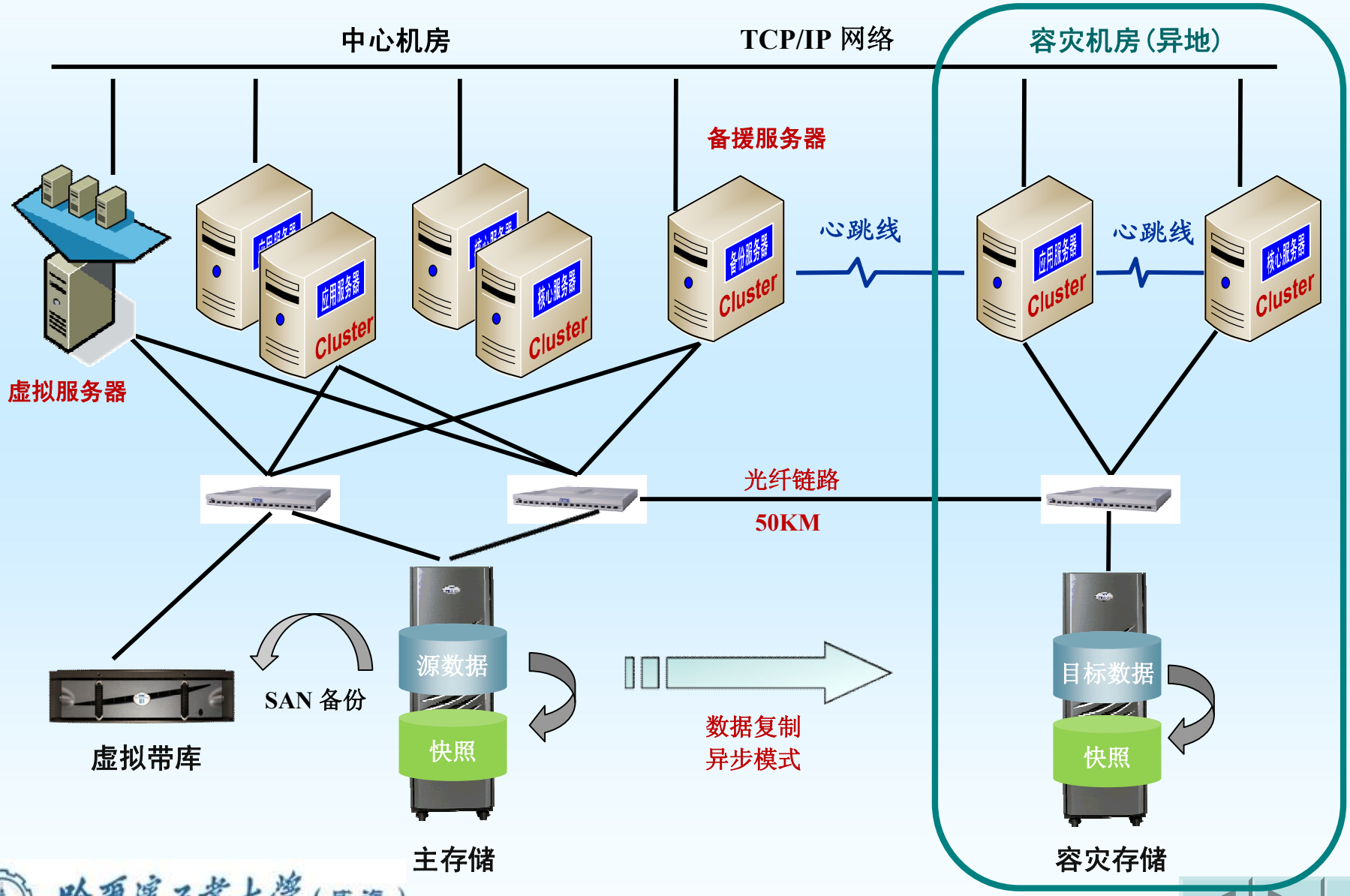
③ 复现：复现也称延迟镜像，与镜像一样需要两个系统，但是它把一个系统称为原系统，另一个成为辅助系统。辅助系统从原系统中接收数据，与原系统中的数据相比，辅助系统接收数据存在着一定延迟。

④ 负载均衡：负载均衡是指将一个任务分解成多个子任务，分配给不同的服务器执行，通过减少每个部件的工作量，增加系统的稳定性。

3.5.2 容灾

- 容灾的含义是对偶然事故的预防和恢复。
- 解决方案有两类
  - 对服务的维护和恢复；
  - 保护或恢复丢失的、被破坏的或被删除的信息。
- 灾难恢复策略
  - （1）做最坏的打算
  - （2）充分利用现有资源
  - （3）既重视灾后恢复，也注意灾前措施
- 数据和系统的备份和还原
  - 是事故恢复能力的重要组成，数据备份越新，系统备份越完整的机构部门就越容易实现灾难恢复操作。

容灾实现拓扑


中心机房
TCP/IP 网络
容灾机房(异地)
备援服务器
心跳线
心跳线
虚拟服务器
应用服务器
Cluster
核心服务器
Cluster
备份服务器
Cluster
应用服务器
Cluster
核心服务器
Cluster
光纤链路
50KM
源数据
快照
目标数据
快照
SAN 备份
数据复制
异步模式
虚拟带库
主存储
容灾存储

Any question?