第6章 物理安全

6.1 物理安全概述

6.2 物理安全技术

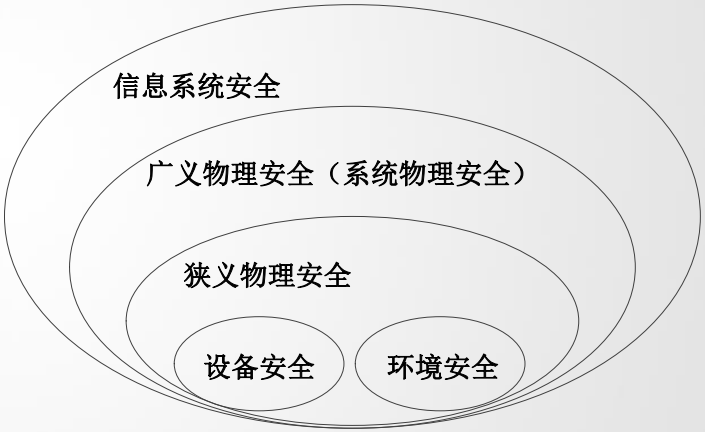
6.3 物理安全管理

6.1 物理安全概述

- 物理安全（Physical Security）研究如何保护网络与信息系统的物理设备、设施和配套部件的安全性能、所处环境安全以及整个系统的可靠运行，使其免遭自然灾害、环境事故、人为操作失误及计算机犯罪行为导致的破坏，是信息系统安全运行的基本保障。

物理安全内涵

- 传统意义的物理安全包括设备安全、环境安全/设施安全以及介质安全；
- 广义的物理安全还应包括由软件、硬件、操作人员组成的整体信息系统的物理安全，即包括系统物理安全。



物理安全威胁

环境因素

人为因素

物理安全内容

- 环境安全
  - ✓ 安全保卫技术
  - ✓ 计算机机房用电安全技术
  - ✓ 计算机机房环境条件保持技术
  - ✓ 计算机机房安全管理技术
- 电源系统安全
- 设备安全
- 通信线路安全
- 基于物理环境的容灾技术
- 物理隔离技术

物理安全技术标准

- 《信息安全技术 信息系统物理安全技术要求》（GB/T 21052-2007），针对信息系统的物理安全制定的，将物理安全技术等级分为五个不同级别，并对信息系统安全提出了物理安全技术方面的要求。
- 《信息安全技术 信息系统安全通用技术要求》（GB/T 20271-2006）
- 《计算机场地安全要求》（GB/T 9361-2011）和《电子计算机场地通用规范》（GB/T 2887-2000），是计算机机房建设应遵循的标准，满足防火、防磁、防水、防盗、防电击等要求，并配备相应的设备。
- 《信息系统安全等级保护基本要求》（GB/T 22239-2008）
- 《电子信息系统机房设计规范》（GB 50174-2008）
- 《信息技术设备用不间断电源通用技术条件》（GB/T 14715-1993）

6.2 物理安全技术





物理访问控制

生物识别技术

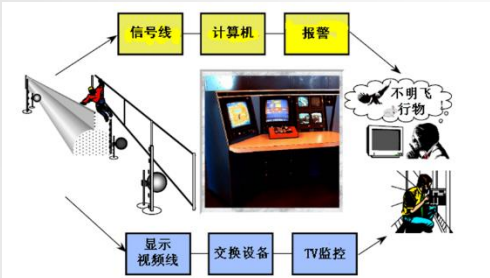
检测和监控技术

物理隔离技术

防信息泄露技术

6.2.1 物理访问控制

- 物理访问控制（Physical Access Control）主要是指对进出办公楼、实验室、服务器机房、数据中心、电力供应房间、数据备份存储区、电话线和数据线的连接区等关键资产运营相关场所的人员进行严格的访问控制。
  - ✓ 门卫
  - ✓ ID卡
  - ✓ 电子门禁卡
  - ✓ 电子监控
  - ✓ 金属探测器
  - ✓ 电围栏
  - ✓ 报警系统
  - ✓ 生物识别
  - ✓ 密码锁


信号线
计算机
报警
不明飞行物
显示视频线
交换设备
TV监控


GARRETT


奥运大厦


Fine Touch

6.2.2 生物识别技术

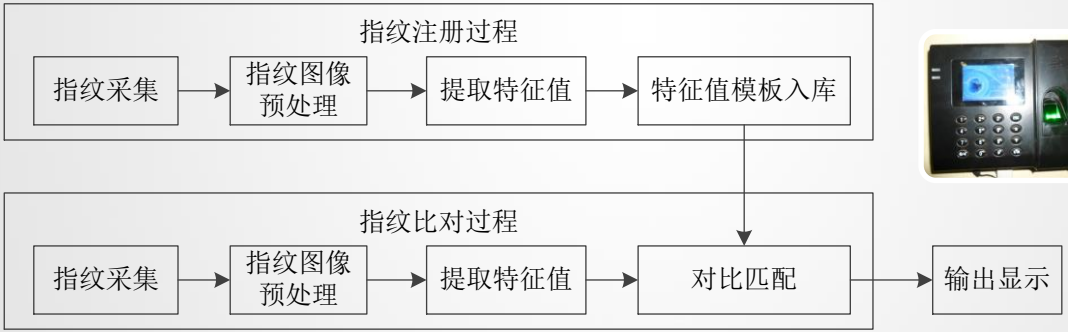
- 生物识别技术（Biometric Technology），是指通过计算机与光学、声学、生物传感器和生物统计学原理等高科技手段密切结合，利用人体固有的生理特性和行为特征来进行个人身份的鉴定。
- 身份鉴别可利用的生物特征必须满足以下几个条件：
  - **普遍性**，即必须每个人都具备这种特征
  - **唯一性**，即任何两个人的特征是不一样的
  - **可测量性**，即特征可测量
  - **稳定性**，即特征在一段时间内不改变

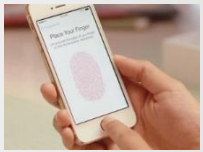
常见生物识别技术

- 现在常用的生物特征识别有：
  - 基于**生理特征**的生物识别技术：指纹识别、人脸识别、虹膜识别、手形识别、掌纹识别、红外温谱图识别、人耳识别、静脉识别、基因识别等。
  - 基于**行为特征**的生物识别技术：签名识别、声音识别、步态识别、击键识别等。

指纹识别（Fingerprint Biometrics）

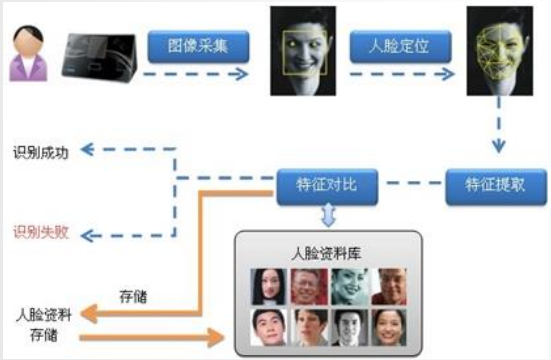
- 指纹识别技术相对成熟，指纹图像提取设备小巧，是目前最方便、可靠、非侵害和价格便宜的生物识别技术。





人脸识别（Facial Biometrics）

- 人脸识别技术通过对面部特征和它们之间的关系，如眼睛、鼻子和嘴的位置以及它们之间的相对位置，来进行识别

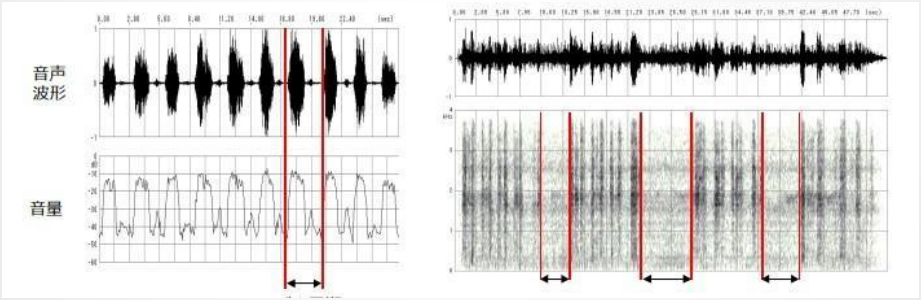


虹膜识别（Iris Biometrics）

- 虹膜识别技术是利用虹膜终身不变性和差异性的特点来识别身份的。
- 虹膜识别是“最精确的”、“处理速度最快的”以及“最难伪造的”生物识别技术，也是最昂贵的识别方式之一。

声音识别（Voice Recognition）

- 声音识别技术是一种依据人的行为特征进行识别的技术。
- 声音识别也是一种非接触的识别技术，用户可自然接受，但声音变化的范围太大，很难进行一些精确的匹配



生物识别系统的准确度

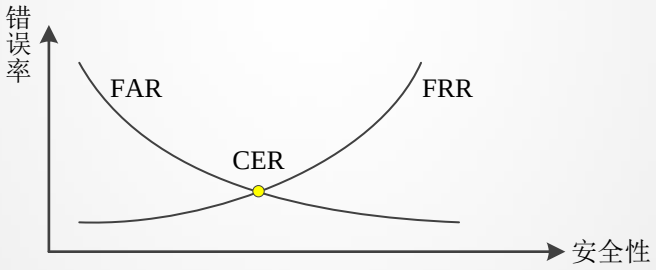
- 生物识别系统并不能保证结果100%准确，其准确度的衡量指标主要由两部分组成：
  - ✓ 错误拒绝率（False Reject Rate，FRR），也就是合法用户被拒绝通过；
  - ✓ 错误接受率（False Accept Rate，FAR），也就是假冒的人被通过。

FRR & FAR

- 错误拒绝率FRR（false reject rate）
  - ✓ 将相同的生物特征，如指纹，误认为是不同的生物特征，而加以拒绝的出错概率
  - ✓ FRR的大小与系统设定的判定相似度的门限阈值呈正相关，即相似度门限阈值定的越高，FRR的数值也越高。
- 错误接受率FAR (false accept rate)
  - ✓ 将不同的生物特征误认为是相同的生物特征，而加以接受的出错概率。
  - ✓ FAR的大小与相似度门限阈值呈负相关。

生物识别系统的准确度

- 通过调整阈值等参数，使系统FRR和FAR相等时，这个错误率被称为交叉错误率(Crossover Error Rate，CER)，是衡量设备准确率的主要指标



多生物识别技术

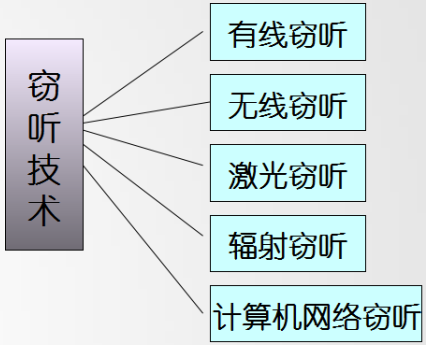
- 捕捉不同的生物特征，同时融合兼顾各种识别算法，形成更精准、更安全的识别和检测机制
  - ✓ **并行融合**：对各种识别特征赋予不同的权值，较为显著、稳定性好、识别效果好的特征赋予大的权值；而易受各类因素干扰、稳定性较差的特征赋予较小的权值，减小这些特征对整体识别的影响。
  - ✓ **串行融合**：赋予权值方法与并行融合一致，只是在形成特征序列时为各特征序列的加权之和，从而使所得到的特征为一个序列。

6.2.3 检测和监控技术

- 检测和监控技术是保证信息系统物理安全的“眼睛”和“耳朵”。
  - ✓ 检测技术是针对窃听、窃照和窃视等的防御技术，防止声音、文字、数据、图像等信息的泄露。
  - ✓ 监控技术主要是指利用光电、超声、微波、红外、压感等传感器，来检测区域访问并报警。

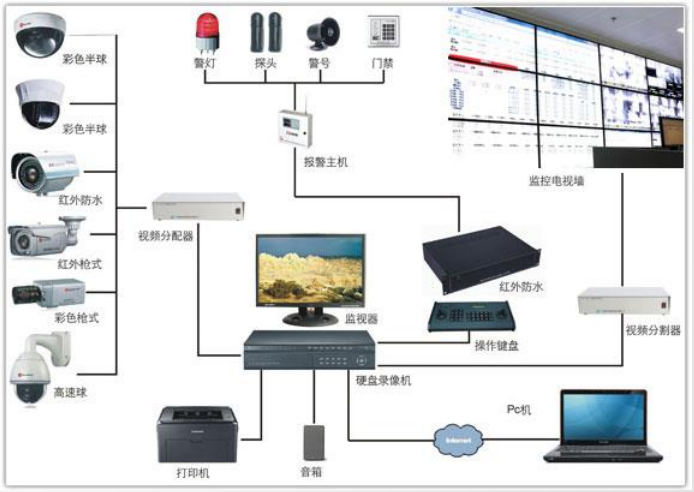
检测技术

- 检测技术可采用电缆加压技术、电磁辐射检测技术、激光探测技术等，搜索发现窃听装置，以消除窃听行为。
- 防窃听技术除了检测之外，还可以采用基于密码编码技术对原始信息进行加密处理，确保信息即使被截获也无法还原出原始信息。
- 此外，电磁信号屏蔽也属于窃听防御技术。



监控技术

- 闭路电视（Closed Circuit Television，CCTV)
  - ✓ 成像设备（摄像机、录像机等）
  - ✓ 传输媒介（如同轴线、光纤、无线电波、红外光束等）
  - ✓ 显示器



监控技术

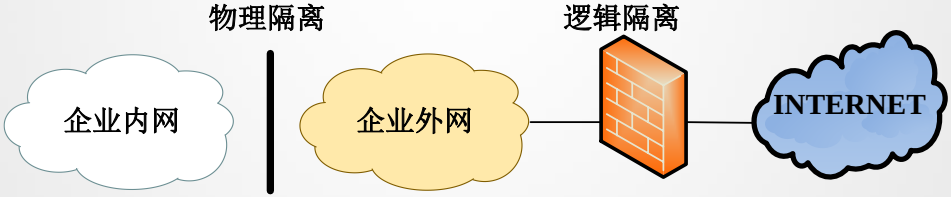
- 监控系统是安防系统中应用最多的系统之一
- 监控技术是一种被动的设备，并不能阻止入侵。因此，可以与其他的控制措施配合使用，如围墙、巡逻、报警系统等。

6.2.4 物理隔离技术

- 即使是最先进的防火墙技术，也不可能100%保证系统安全。
- 屡次发生的网络入侵及泄露事件，使人们认识到：理论上说，只有一种真正安全的隔离手段，那就是从物理上断开连接。
- 《计算机信息系统国际互联网保密管理规定》第二章第六条要求：“涉及国家机密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连，必须实行物理隔离。”

什么是物理隔离？

- 物理隔离（Physical Gap）实际上就是指，内部网不直接或间接的连接公共网。
- 物理隔离的解决思路是：在同一时间、同一空间单个用户是不可能同时使用两个系统的，使两个系统在空间上物理隔离，就可以使它们的安全性相互独立。
- 如果将一个企业涉及的网络分为内网、外网和公网，其安全要求如下图：

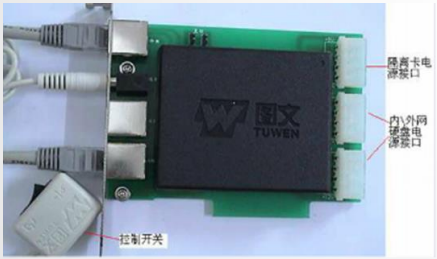


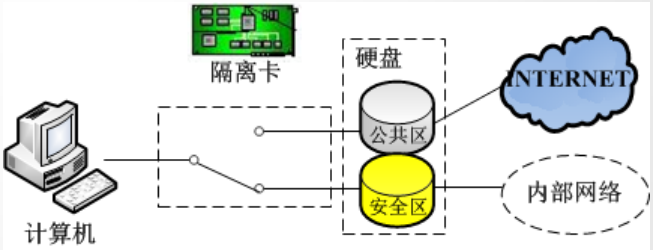
网络物理隔离技术

- 第一代物理隔离技术：完全隔离
  - ✓ 完全隔离主要采用双机物理隔离技术，其主要原理是将两套主板、芯片、网卡和硬盘的系统合并为一台计算机使用，用户通过客户端的开关来选择两套计算机操作系统，切换内外网络的连接。
  - ✓ 双机物理隔离的维护和使用都不够便利。

网络物理隔离技术

- 第二代物理隔离技术：硬件卡隔离
  - ✓ 硬件卡隔离的原理是在主机的主板插槽中安装物理隔离卡，把一台普通计算机分成两台虚拟计算机，来实现物理隔离。
  - ✓ 硬件卡隔离，分为双硬盘、单硬盘物理隔离系统两种。



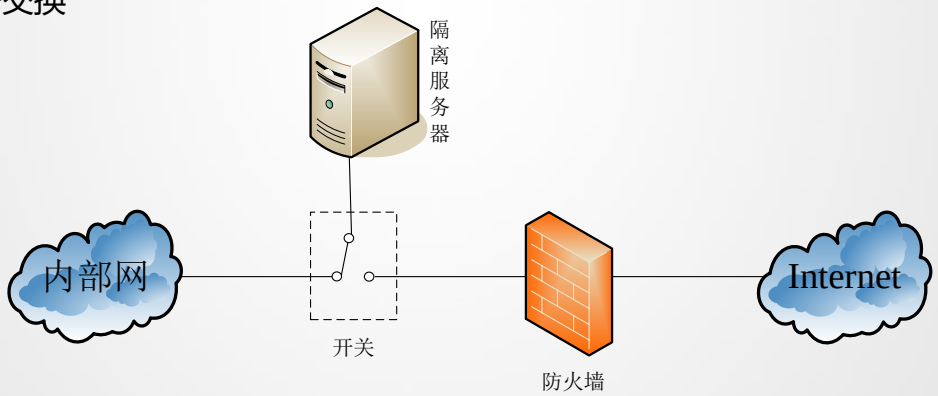


网络物理隔离技术

- 第三代物理隔离技术：数据转播隔离
  - ✓ 数据转播隔离，利用因特网信息传播服务器分时复制转播文件的途径实现隔离，是一种非实时的因特网访问方式。
  - ✓ 采集服务器下载指定网站的内容，转播服务器使用下载的数据建立网站的镜像站点，向内部用户提供虚拟的Internet站点访问。
  - ✓ 用户只是访问了指定站点的镜像，访问内容有较大的局限性。

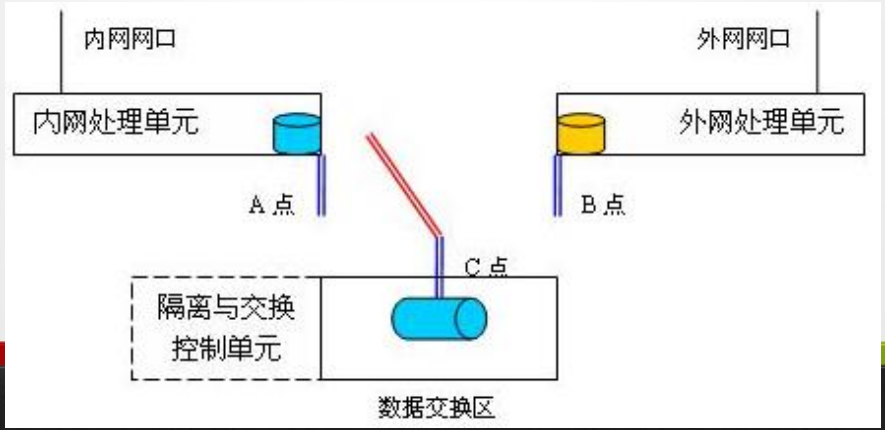
网络物理隔离技术

- 第四代物理隔离技术：空气开关隔离
  - ✓ 空气开关隔离通过使用单刀双掷开关，使得内外部网络分时访问临时缓冲器来完成数据交换



网络物理隔离技术

- 第五代物理隔离技术：安全通道隔离
  - ✓ 安全通道隔离，通过专用通信设备、专有安全协议和加密验证机制及应用层数据提取和鉴别认证技术，进行不同安全级别网络之间的数据交换，彻底阻断了网络间的直接TCP/IP连接
  - ✓ 同时对网间通信的双方、内容、过程施以严格的身份认证、内容过滤、安全审计等多种安全防护机制，从而保证了网间数据交换的安全、可控，杜绝由于操作系统和网络协议自身漏洞带来的安全风险，成为当前隔离技术的发展方向。



6.2.5 防信息泄漏技术

- 信息泄露
  - ✓ 计算机主机及其附属电子设备，如**视频显示终端**、**打印机**等，在工作时不可避免地会产生**电磁辐射**，这些辐射中携带有计算机正在进行处理的数据信息。
  - ✓ 加解密等常规信息安全技术，并不能解决输入、输出端的电磁信息泄露问题
  - ✓ 使用专门的高灵敏设备接收这些电磁辐射，经过分析还原，即可恢复出原信息。
- 美国国家安全局：TEMPEST（Transient Electromagnetic Pulse Emanation Standard），包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等多项技术

屏蔽隔离：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

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。

抑制电磁发射：采取各种措施减小“红区”电路电磁发射；

6.3 物理安全管理

环境安全管理

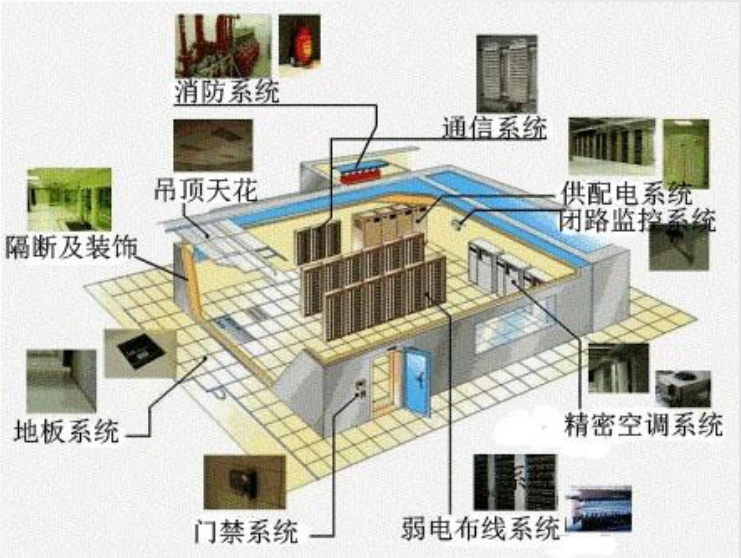
设备安全管理

数据安全管理

人员安全管理

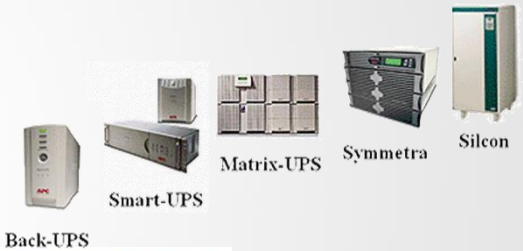
6.3.1 环境安全管理

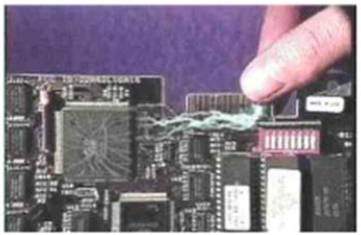
- 机房安全要求
- 机房防盗要求
- 机房三度要求
- 防水、防火等要求



6.3.2 设备安全管理

- 设备的使用管理
- 设备的维护与保养
- 防盗
- 供电系统安全
- *防静电*
- 防雷击





6.3.3 数据安全管理

- 数据存储介质，如硬盘、磁盘、磁带、打印纸、光盘等的安全控制

6.3.4 人员安全管理

- 《信息安全技术 信息系统物理安全技术要求》（GB/T 21052-2007）将物理安全技术等级分为五个不同级别
  - ✓ 第二级“人员要求”：安全管理机构及人员
  - ✓ 第三级“人员与职责要求”：明确分工责任、编制正式文件、实施等级标记管理制度
  - ✓ 第四级“人员与职责要求”：实施物理安全管理质量控制、评估和评审，建立质量管理体系文件，隔离不同安全域，建立出入安全检测制度

小结

- 物理安全的内涵、主要威胁、主要技术及相关标准
- 物理访问控制技术、生物识别技术、检测和监控技术、物理隔离技术、防信息泄露技术等的基本原理、思想及方法
- 物理安全管理的基本措施