第 3 章

物 理 安 全

本章学习要点：

- 了解物理安全的意义、内容和基本防护方法；
- 了解物理隔离的基本思想及方法；
- 了解生物识别技术的基本原理；
- 了解物理安全管理的基本措施。

3.1 物理安全概述

物理安全(physical security)是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。特别是随着物联网(internet of things)和物理信息融合网络(cyber-physical systems)的发展，物理世界(物)与信息世界(机)、人类社会(人)能够无缝连接和有机融合，各种物理设备、车辆甚至建筑物，通过嵌入式计算、传感器监控、无线通信，以及大规模数据处理等技术，具备了感控能力、计算能力和通信能力，实现了物理设备的信息化和网络化，因此物理安全成为整个网络与信息系统安全当中非常重要且最基础的一环。

物理安全的概念如图 3.1 所示。传统意义的物理安全包括设备安全、环境安全/设施安全及介质安全；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。信息系统安全体现在信息系统的保密性、可用性、完整性三方面，从物理层面出发，系统物理安全技术应确保信息系统的保密性、可用性、完整性。例如：通过边界保护、配置管理、设备管理等措施保护信息系统的保密性，通过容错、故障恢复、系统灾难备份等措施确保信息系统的可用性，通过设备访问控制、边界保护、设备及网络资源管理等措施确保信息系统的完整性。

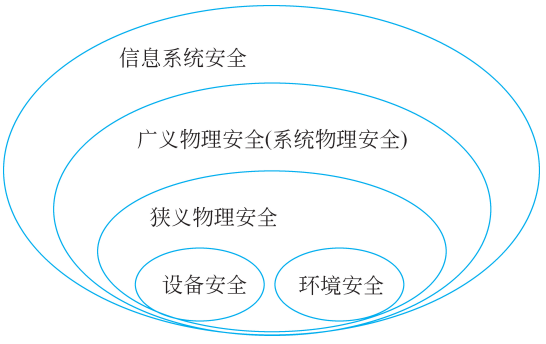

图 3.1 物理安全的概念

信息系统物理安全面临多种威胁，可能面临自然、环境和技术故障等非人为因素的威胁，也可能面临人员失误和恶意攻击等人为因素的威胁，这些威胁通过破坏信息系统的保密性（如电磁泄露类威胁）、完整性（如各种自然灾难类威胁）、可用性（如技术故障类威胁）进而威胁信息的安全。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。环境因素包括自然界不可抗的因素和其他物理因素。表 3.1 对信息系统面临的物理安全威胁种类进行了描述。

表 3.1 物理安全威胁分类表

种　类	描　述
自然灾害	地震、洪水、暴风、雷击等
物理环境影响	火灾、漏水、温度和湿度变化、有害气体等
电、磁环境影响	通信中断、电力中断、电磁泄露、静电等
软硬件故障	由于设备硬件故障、通信链路中断、系统本身或软件缺陷造成对信息系统安全可用的影响
物理攻击	物理接触、物理破坏、盗窃等
无作为或操作失误	由于应该执行而没有执行相应的操作，或无意执行了错误的操作，对信息系统造成的影响
管理不到位	物理安全管理无法落实、不到位，造成物理安全管理不规范，或者管理混乱，从而破坏信息系统正常有序运行
恶意代码和病毒	改变物理设备的配置，甚至破坏设备硬件电路，导致物理设备失效或损坏
网络攻击	利用工具和技术（如拒绝服务等）非法占用系统资源，降低系统可用性
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的职权，做出破坏信息系统的行为，如设备非法接入、设备非法外联
设计、配置缺陷	设计阶段存在明显的系统漏洞，系统未能正确有效配置，系统扩容和调整引起错误

物理安全主要用来解决两方面的问题：一方面是针对信息系统实体的保护；另一方面针对可能造成的信息泄露的物理问题进行防范。其主要内容包括以下几点。

1. 环境安全

应具备消防报警、安全照明、不间断供电、温湿度控制系统等。环境安全技术主要如下。

（1）安全保卫技术，主要的安全技术措施包括防盗报警、实时电子监控、安全门禁等，是环境安全技术的重要一环。

（2）计算机机房的温度、湿度等环境条件保持技术，可以通过加装通风设备、排烟设备、专业空调设备来实现。

（3）计算机机房的用电安全技术，主要包括不同用途的电源分离技术、电源和设备有效接地技术、电源过载保护技术和防雷击技术等。

（4）计算机机房安全管理技术，主要是制定严格的计算机机房工作管理制度，并要求所有进入机房的人员严格遵守管理制度，将制度落到实处。

2. 电源系统安全

电源安全主要包括电力能源供应、输电线路安全、保持电源的稳定性等。

3. 设备安全

要保证硬件设备随时处于良好的工作状态，建立健全使用管理规章制度，建立设备运行日

志。同时要注意保护存储媒体的安全性，包括存储媒体自身和数据的安全。设备安全防护技术主要包括防盗技术（报警、追踪系统等）、防火、防静电、防雷击等。

4. 通信线路安全

要防止电磁信息的泄露、线路截获（窃听），通信线路应有抗电磁干扰等安全技术。

此外，基于物理环境的容灾技术（灾难的预警、应急处理和恢复）和物理隔离技术，也属于物理安全技术的范畴。

物理安全涉及的主要技术标准包括以下方面。

（1）《信息安全技术 信息系统物理安全技术要求》（GB/T 21052—2007）是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。

（2）《计算机场地安全要求》（GB/T 9361—2011）和《计算机场地通用规范》（GB/T 2887—2011），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。

（3）《数据中心设计规范》（GB 50174—2017），适用于新建、改建和扩建建筑物中的数据中心设计，确保电子信息设备安全、稳定、可靠地运行。

（4）《信息安全技术 信息系统安全通用技术要求》（GB/T 20271—2006），在信息系统五个安全等级划分中，规定了对于物理安全技术的不同要求。

（5）《信息安全技术　网络安全等级保护基本要求》（GB/T 22239—2019），规定了不同安全保护等级信息系统的基本保护要求，基本技术要求从安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心几个层面提出，基本管理要求从安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理几方面提出。

（6）《信息技术设备用不间断电源通用规范》（GB/T 14715—2017），规定了信息技术设备用不间断电源的技术要求、试验方法、质量评定程序及标志、包装、运输、贮存等。

物理安全是整个网络与信息系统安全的必要前提，如果物理安全得不到保证，那么其他一切安全措施都将无济于事。即使是在云计算环境下，用户从云端获取网络基础设施服务，看起来用户不再需要考虑物理安全问题，但实际上对物理安全的控制转移到了云计算服务提供商手中，云服务提供商需要更强大的物理安全控制技术、更严密的管理措施来保证云端的物理安全。

3.2　物理安全技术

3.2.1　物理访问控制

物理访问控制（physical access control）主要指对进出办公楼、实验室、服务器机房、数据中心等关键资产运营相关场所的人员进行严格的访问控制。系统中线路连接所涉及的场所也需要进行严格控制，如电力供应房间、数据备份存储区、电话线和数据线的连接区等。此外，还可以利用闭路电视摄像机、运动探测器及其他设备进行监控，检测可能的入侵行为。

现有的物理访问控制技术和措施主要包括如下几方面。

（1）门卫。在每个出入口配备门卫，能够对非授权的进入者产生威慑，在某些情况下，能够阻止非授权进入。

（2）ID卡。为企业或机构的所有员工、合作人员配备ID卡。常见的方式主要包括两种，一种是带照片的证件，另一种是智能卡。智能卡具有较高的安全性和便携性：①能够存储人员信息，并具备防篡改机制；②能够在卡内进行高安全度的信息处理，如电子签名、加密等；③使用加密系统存储密钥；④能够提供安全的授权级别，对不同级别的人员进行访问控制。

（3）电子门禁卡。

① RFID感应卡，也称为EM卡，工作频率是125 kHz，通过射频无线发射技术；成本较低，有开门记录，但安全性一般，容易复制，不易双向控制，卡片信息容易因外界磁场丢失而导致卡片无效。

② IC卡，也称M1卡，工作频率为13.56MHz，是目前应用比较广泛的一种卡类型，如我国二代身份证。IC卡的优点是卡片与设备无接触，开门方便安全；安全性高，有开门记录，可以实现双向控制，卡片很难被复制。

③ CPU卡，芯片内含有一个微处理器。通常CPU卡内含有随机数发生器、硬件DES、3DES加密算法等，配合操作系统即片上OS，可以达到金融级别的安全等级，比传统的M1卡有着更强的安全性。

④ NFC手机代替门禁卡。近场无线射频通信（Near Field Communication，NFC）是基于RFID无线射频通信技术发展起来的一种近距离高频无线通信技术，工作在13.56MHz频段，可在短距离内实现电子身份识别或数据传输功能。内置NFC的手机可以与门禁交换控制数据，只需要将手机对准读卡器，便能打开门禁。NFC手机还可以作为虚拟凭证卡，代替公交卡、银行卡、门禁卡、医疗卡、图书借阅卡、工卡等多种智能卡。

（4）电子监控和监控摄像机。电子监控技术主要是指利用光电（photoelectric）、超声（ultrasonic）、微波（microwave）、红外（passive infrared）、压感（pressure-sensitive）等传感器，来检测区域访问并报警。闭路电视（Closed Circuit Television，CCTV）使用照相机通过传输媒介将图像传送到连接显示器的电视传输系统，传输媒介可以使用光缆、微波、无线电波或红外光束。

（5）金属探测器。利用电磁感应、X射线检测、微波检测等技术，可以探测随身携带或隐藏的武器与作案工具。

（6）电围栏。

（7）报警系统。报警系统经常与监控系统协同使用，类似于IDS，检测物理入侵行为，以及进行火灾报警、烟雾报警、地震报警、防盗报警等。

（8）生物识别。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（如指纹、脸像、虹膜等）和行为特征（如笔迹、声音、步态等）来进行个人身份的鉴定。

（9）密码锁。密码锁包括传统密码锁和可编程电子密码锁两类。电子密码锁通过密码输入来控制电路或是芯片工作，从而控制机械开关的闭合，完成开锁、闭锁任务。

常见物理访问控制技术和措施如图3.2所示。

3.2.2 生物识别技术

生物识别技术（biometric technology），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。由于人体特征具有人体所固有的不可复制的唯一性，这一生物密钥难以复制、失窃或被遗

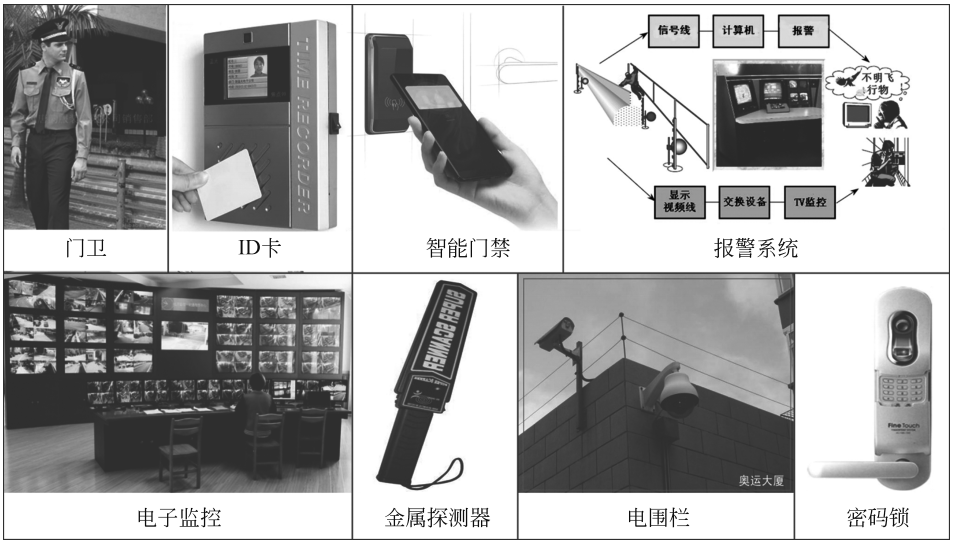

图 3.2　常见物理访问控制技术和措施

忘，利用生物识别技术进行身份认定十分安全、可靠、准确。

身份鉴别可利用的生物特征必须满足以下几个条件。

（1）普遍性，即必须每个人都具备这种特征。

（2）唯一性，即任何两个人的特征是不一样的。

（3）可测量性，即特征可测量。

（4）稳定性，即特征在一段时间内不改变。

在应用过程中，还要考虑其他的实际因素，如识别精度、识别速度、对人体无伤害、被识别者的接受性等。现在常用的生物特征识别如下。

（1）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。

（2）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。

3.2.2.1　常见生物识别技术

1. 指纹识别

指纹识别(fingerprint biometrics)技术是通过取像设备读取指纹图像，然后用计算机识别软件分析指纹的全局特征和指纹的局部特征，特征包括指纹的嵴、谷、终点、分叉点和分歧点等，从指纹中抽取特征值并加密存储。用户需要认证时，在指纹采集头重新按压手指，与已经登记好的指纹进行比对，就可以非常可靠地通过指纹来确认一个人的身份。其原理如图 3.3 所示。

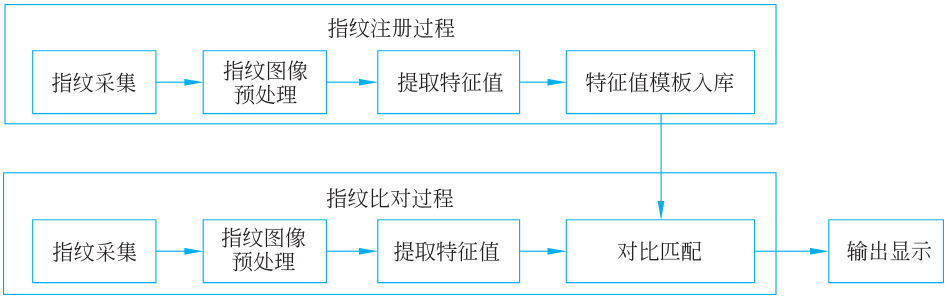

图 3.3　指纹识别基本原理

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。指纹识别的缺点在于，它是物理接触式的，指纹采集头上留下的印痕存在被用来复制指纹的可能性。

2. 人脸识别

人脸识别(facial biometrics)技术通过对面部特征和它们之间的关系(如眼睛、鼻子、嘴巴、下巴等的形状、大小、位置及它们之间的相对位置)来进行识别，如图 3.4 所示。基于面部特征的识别是十分复杂的，需要人工智能和机器知识学习系统。用于捕捉面部图像的两项技术为标准视频技术和热成像技术。

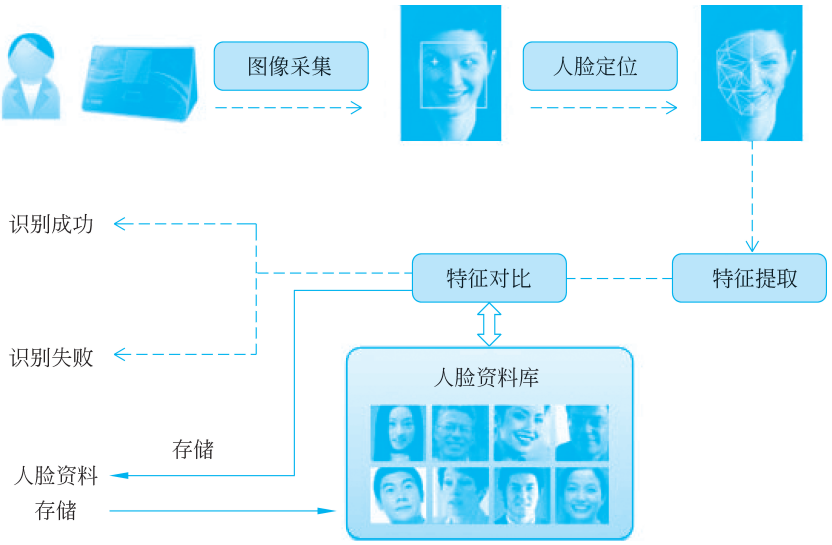

图 3.4　人脸识别系统

(1) 标准视频技术通过视频摄像头摄取面部的图像。

(2) 热成像技术通过分析由面部毛细血管的血液产生的热线来产生面部图像。热成像技术并不需要较好的光源，即使在黑暗情况下也可以使用。

人脸识别技术的优点是非接触性。缺点是：需要比较高级的摄像头才可有效高速地捕捉面部图像；由于使用者面部的位置与周围的光环境都可能影响系统的精确性，人们公认面部识别是最容易被欺骗的；采集图像的设备会比其他技术昂贵得多。另外，对于因头发、饰物、表情、姿态等引起的人体面部的遮挡或变化，以及创伤、年龄等其他变化，可能需要通过人工智能技术来得到补偿。人脸识别技术的改进依赖于提取特征与比对技术的提高。

人脸识别技术起步于 20 世纪 60 年代末至 70 年代初，当时主要是以人脸特征点的间距、比率等参数为特征，提取的信息是人脸主要器官特征信息及其之间的几何关系，但是对于视角、表情变化等情况下的识别能力差。20 世纪 90 年代以来，研究的重点是基于整体的识别方法，如特征脸方法、弹性图匹配方法等，充分利用人脸各个特征点之间的拓扑关系和各个器官自身的信息，避免提取面部局部特征，提高了识别稳健性。20 世纪 90 年代中期，整体识别和部分分析方法相互结合，融合人脸的形状拓扑结构特征、局部灰度特征和全局灰度特征等多种特征。20 世纪 90 年代后期，一些商业性的人脸识别系统逐渐进入市场。2000 年以来，人脸识别技术日趋成熟，取得了在一定约束条件下的较好的识别结果，然而，由光照、姿态、化妆、表情、年龄等因素引起的面部遮挡或变化，仍然令人脸识别算法的准确性面临很大的挑战。当前

在有遮挡人脸识别研究领域，主要采用子空间回归方法、鲁棒误差编码方法和鲁棒特征提取方法等，来解决由遮挡引发的特征损失、对准误差和局部混叠等问题。此外，由于图像是三维物体在二维空间的简约投影，因此利用脸部曲面的显式三维表达来进行人脸识别，能够解决二维人脸识别中姿态、光照变化稳健性差的问题，这也是近年来的研究热点。

2013 年 7 月，芬兰创业公司 Uniqul 和全球最大的在线支付公司 PayPal 测试推出了史上第一款基于脸部识别系统的支付平台，人脸识别技术进入了高速发展期。随后，我国中科院也开发出了人脸识别支付系统。2015 年，国内多家商业巨头也纷纷加入人脸识别产业，如阿里巴巴公司的“刷脸支付”、腾讯公司的“优图人脸识别”等。2017 年，iPhone X 引入 Face ID 人脸识别之后，人脸识别逐渐在智能手机中普及。2018 年，小米、OPPO、华为等的多款手机开始支持 3D 人脸识别技术。

3. 虹膜识别

虹膜识别(iris biometrics)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。虹膜是一种在眼睛瞳孔内的织物状的各色环状物，每个人的虹膜都包含一个独一无二的基于水晶体、细丝、斑点、凹点、皱纹和条纹等特征的结构。虹膜在眼球的内部，用外科手术很难改变其结构。由于瞳孔随光线的强弱变化，想用伪造的虹膜代替活的虹膜是不可能的。即使是接受了角膜移植手术，虹膜也不会改变。虹膜识别技术与相应的算法结合后，可以达到十分优异的准确度，即使全人类的虹膜信息都录入一个数据库中，出现错误拒绝和错误接收的可能性也相当小。

实验表明，到目前为止，虹膜识别是“最精确的”“处理速度最快的”“最难伪造的”生物识别技术，也是较为昂贵的识别方式之一。

4. 声音识别

声音识别(voice recognition)技术是一种依据人的行为特征进行识别的技术。声音识别设备不断地测量、记录声音的波形和变化。而声音识别基于将现场采集到的声音与登记过的声音模板进行精确的匹配。声音识别的优点：声音识别也是一种非接触的识别技术，用户可以很自然地接受。声音识别的缺点：和其他的识别技术一样，声音因为变化的范围太大，故而很难进行一些精确的匹配；声音会随着音量、速度和音质的变化(如感冒时的声音变化)而影响比对结果；目前来说，还很容易用录在磁带上的声音来欺骗声音识别系统。

5. 签名识别

签名识别(signature patterns)技术是通过计算机把手写签名的图像、笔顺、速度和压力等信息与真实签名样本进行比对，以鉴别手写签名真伪的技术。手写签名作为身份认证的手段已经用了几百年了，而且我们都很熟悉在银行的格式表单中签名作为我们身份的标志。签名形状和相对位置的相关参数包括：签名的整体倾斜角度、签名的宽高比、签名的笔迹长度、签名落笔的总时间、签名抬笔的总时间、书写平均速度、笔迹的压力变化信息和形状变化信息等。签名识别易被大众接受，是一种公认的身份识别技术。但事实表明人们的签名在不同的时期和不同的精神状态下是不一样的，这降低了签名识别系统的可靠性。

3.2.2.2　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：一是错误拒绝率(False Reject Rate，FRR)，也就是合法用户被拒绝通过的概率；二是错误接受率(False Accept Rate，FAR)，也就是假冒的人被通过的概率。

FRR 的含义是，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得越高，FRR 的数值也越高。FAR 的含义是，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。

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，如图 3.5 所示，CER 为 FRR 与 FAR 的交叉点。

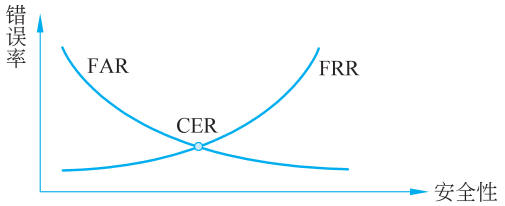

图 3.5　生物特征识别系统的准确度

生物特征识别系统在利用个人特征来鉴别或验证用户身份时，如果检测“有噪声”，当指纹中带有疤痕或因感冒而改变声音，识别的准确度就会下降。如果能够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，那么生物识别技术将更加完善。这也被称为多生物识别技术，或多模态生物特征识别技术。

对多特征的融合常用的方法有两种，一种是并行融合，另一种是串行融合。并行融合是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。串行融合是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。

多生物特征融合识别的优点在于：首先，已经证明利用多个生物特征融合可以提高身份鉴别的正确率；其次，利用多个生物特征显然可以拓宽生物特征识别系统的应用人群范围；最后，从防伪的角度，伪造多个生物特征的难度远远大于伪造单一的生物特征。

多生物特征识别技术发展的核心在于构建准确而快速的融合算法，就是对两种或多种生物识别的标准都加以计算和选择，最后形成一个统一的、整体的判断标准，这也是多生物特征识别技术未来的发展方向。

3.2.3　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”。

3.2.3.1　检测技术

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。窃听主要依赖于各种“窃听器”，不同的窃听器针对的对象不同，主要包括会议谈话、有线电话、无线信号、电磁辐射及计算机网络等。随着技术发展的日新月异，窃听已经形成了有线、无线、激光、红外、卫星和遥感等种类齐全的庞大窃听家族，而且被窃听的对象也已从军事机密向商业活动甚至平民生活发展。

有线窃听指秘密侵入他人之间的有线通信线路，探知其通信内容，如对固定电话的监听。无线窃听指对无线通信线路的秘密侵入，如对移动电话的监听。激光窃听就是用激光发生器产生一束极细的红外激光，射到被窃听房间的玻璃上，当房间里有人谈话的时候，玻璃因受室

内声音变化的影响而发生轻微的振动，从玻璃上反射回来的激光包含了室内声波振动信息，这些信息可以还原成为音频信息。辐射窃听是利用各种电子设备存在的电磁泄露，收集电磁信号并还原，得到相应信息。计算机网络窃听主要是通过在网络的特殊位置安装窃听软件，接收能够收到的一切信息，并分析还原为原始信息。

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。

3.2.3.2　监控技术

监控技术主要是利用光电、超声、微波、红外、压感等传感器，来检测区域访问并报警。监控系统是安防系统中应用较多的系统之一，它是一种被动的设备，但可以与其他的控制措施配合使用（如围墙、巡逻、报警系统等）来阻止入侵。视频监控系统的发展可以划分为三个阶段：第一代，模拟视频监控系统，即闭路电视；第二代，数字视频监控系统；第三代，智能视频监控系统。

1. 第一代：模拟视频监控系统

20 世纪 70 年代，电子监控系统开始普及，这个时期以闭路电视（CCTV）为主。闭路电视中使用照相机通过传输媒介将图片传送到连接显示器的电视传输系统，传输媒介可以使用光缆、微波、无线电波或红外光束，模拟视频设备包括视频画面分割器、矩阵、切换器、卡带式录像机（Video Cassette Recorder，VCR）及视频监视器等。CCTV 根据图像信号的清晰度，分为下面三个等级。

（1）检测级：能够检测到对象的存在。

（2）识别级：能够检测到对象的类型。

（3）确认级：能够分辨对象的细节。

部署 CCTV 的关键在于：充分理解设施的整个监控需求；确定需要监控的区域大小，深度、宽度来决定照相机镜头的尺寸；明确照明条件，不同的灯光和照明将提供不同的效果等级。照明设备应该在黑暗中能够提供持续的覆盖程度，对象与背景的对比度也非常重要。CCTV 技术价格低廉，安装简单，适合小规模的安全防范系统。

2. 第二代：数字视频监控系统

20 世纪 90 年代中期，随着数字编码技术和芯片技术的进步，出现了数字视频监控系统，解决了磁带录像机存储容量太小、线缆式传输限制了监控范围等缺点。初期采用模拟摄像机和嵌入式硬盘录像机（Digital Video Recorder，DVR）的“半模拟-半数字”方案，从摄像机到 DVR 仍采用同轴线缆输出视频信号，通过 DVR 同时支持录像和回放，并可支持有限 IP 网络访问。后期发展成为利用数字摄像机和视频服务器（Digital Video Server，DVS），成为真正的全数字化视频监控系统。数字视频监控系统时代，可容纳的摄像机数量得到了海量的提升，监控规模空前扩大的同时，带来了对视频内容理解的需求。

3. 第三代：智能视频监控系统

随着数字视频监控技术的进步，人们对安全性要求的提高，以及经济条件的改善，当今社会中监控摄像头的个数增长越来越快，覆盖范围也越来越广。但是传统的视频监控仅提供视频的捕获、存储和回放等简单的功能，记录发生的事情用于事后查询，很难起到预警和实时报警的作用。为了从海量监控视频数据中，实时地发现异常行为并及时采取有效措施，智能视频监控技术应运而生。智能视频监控的核心是基于计算机视觉的视频内容理解技术，在底层上

对动态场景中的感兴趣目标进行检测、分类、跟踪和识别，在高层上对感兴趣目标的行为进行识别、分析和理解。智能视频监控技术广泛应用于公共安全监控、工业现场监控、居民小区监控、交通状态监控等各种监控场景中，实现犯罪预防、交通管制、意外防范和检测、老幼病残监护等功能。作为最早应用于物联网的重要技术之一，其发展也受到了物联网大数据的巨大影响，在不久的将来，依靠视频大数据的智能视频监控技术一定会具有更高的智能，甚至具有人类一样的智慧。

3.2.4 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信息泄露事件，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。有鉴于此，我国国家保密局2000年1月1日起实施的《计算机信息系统国际互联网保密管理规定》的第二章第六条要求："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。"包括美国在内的许多国家也都利用物理隔离来解决政府和军事涉密网络与公共网络连接时的安全问题。

3.2.4.1 什么是物理隔离

物理隔离到目前为止没有一个十分严格的定义，较早时用于描述的英文单词为physical disconnection，后来使用词汇physical separation和physical isolation。这些词汇共有的含义都是与公用网络彻底地断开连接，但这样背离了网络的初衷，同时会给工作带来不便。后来，很多人开始使用physical gap来描述它，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。

物理隔离首先要考虑的是安全域的问题。国家的安全域一般以信息涉密程度划分为涉密域和非涉密域。涉密域就是涉及国家秘密的网络空间；非涉密域不涉及国家的秘密，但是涉及本单位、本部门或本系统的工作秘密。公共服务域是不涉及国家秘密，也不涉及工作秘密，向互联网完全开放的公共信息交换空间。类似地，企业的安全域一般分为企业内网、企业外网和公网（如Internet）。

物理隔离实际上就是内部网不直接或间接地连接公共网。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，总有一个系统处于"空闲"状态，这样只要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。

最初的物理隔离是建立两套网络系统和计算机设备：一套用于内部办公，另一套用于与互联网连接。这样的两套互不连接的系统不仅成本高，而且极为不便。这一矛盾促进了物理隔离设备的开发，也迫切需要一套技术标准和方案。

如果将一个企业涉及的网络分为内网、外网和公网，其安全要求应该如下。

（1）在公网和外网之间实行逻辑隔离。

（2）在内网和外网之间实行物理隔离。

具体拓扑形式如图3.6所示。

图3.6 企业网络的划分

要实现内网与外网之间物理隔离的目的，必须保证做到以下几点。

（1）阻断网络的直接连接，即三个网络不会同时连在隔离设备上。

（2）阻断网络的 Internet 逻辑连接，即 TCP/IP 的协议必须被剥离，原始数据通过点到点协议而非 TCP/IP 协议透过隔离设备进行传输。

（3）隔离设备的传输机制具有不可编程的特性，因此不具有感染的特性。

（4）任何数据都通过两级移动代理的方式来完成，两级移动代理之间是物理隔离的。

（5）隔离设备具有审查功能。

（6）隔离设备传输的原始数据不具有攻击或对网络安全有害的特性（如 TXT 文本不会像病毒一样），也不会执行命令等。

（7）具有强大的管理和控制功能。

（8）从隔离的内容看，隔离分为数据隔离和网络隔离。数据隔离主要指存储设备的隔离，即一个存储设备不能被几个网络共享。网络隔离是把被保护的网络从公开的、无边界的、自由的环境中独立出来。只有实现了两种隔离，才是真正意义上的物理隔离。

此外，还应该在物理辐射上阻断内部网和外部网，确保内部网络信息不会通过电磁辐射或耦合方式泄露到外部网。

物理隔离技术主要应用于需要对内部重要数据进行安全保护的国家各级政府部门、军队系统、金融系统等。这些部门对网络安全有更高的要求，严格禁止信息泄露和被篡改，而且出于信息交换的需要，不能够完全隔离与外部网络的联系。

3.2.4.2　网络物理隔离的基本形式

物理隔离发展至今已有五代隔离技术，前两代为用户级，后三代为网络级。

1. 用户级物理隔离

用户级物理隔离的目的，是使一台计算机既连接内网又连接外网，可以在不同网络上分时地工作，在保证内、外网络隔离的同时节省资源、方便工作。用户级物理隔离自出现至今经过多次演变，不断发展成熟。

（1）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。

（2）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。

双硬盘物理隔离系统，如图 3.7，即客户端增加一块物理隔离卡，客户端的硬盘或其他的存储设备首先连接到该卡，然后再转接到主板上，隔离卡可以控制客户端的选择。选择不同的硬盘时，同时选择了该卡不同的网络接口。这种隔离产品有的仍然需要网络布线为双网线结构，存在较大的安全隐患。

单硬盘物理隔离系统，通过对单个硬盘上磁道的读写控制技术，在一个硬盘上分隔出两个独立的工作区间，其中一个为公共区（public），另一个为安全区（secure）。这两个区分别装有两个操作系统，用户可以在本地通过操作系统上的一个切换图标自由选择内外两个不同网络。用户在任意时间只能与其中一个网络相连，这两个区之间无法互相访问。

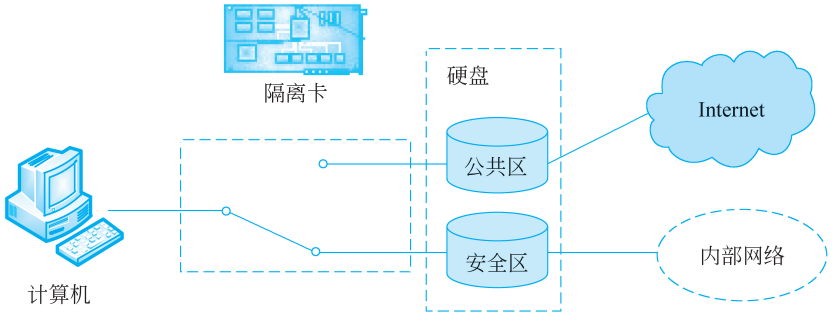

图 3.7　双硬盘物理隔离系统

2. 网络级物理隔离

网络级物理隔离技术最早采用隔离集线器的方式。隔离集线器相当于内网和外网两个集线器的集成，通过电子开关进行切换，从而连接到内网或外网两者之一。隔离集线器只有与其他隔离措施（如物理隔离卡等）相配合，才能实现真正的物理隔离。

（1）第三代物理隔离技术：数据转播隔离。数据转播隔离利用互联网信息传播服务器分时复制转播文件的途径实现隔离，是一种非实时的互联网访问方式。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。

（2）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，其基本功能框图如图 3.8 所示。

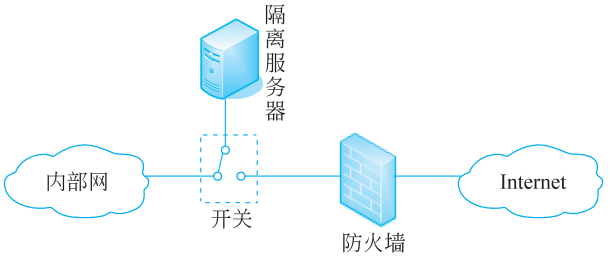

图 3.8　空气开关隔离技术

该隔离系统由隔离服务器和防火墙组成。隔离服务器有内部网络和外部网络两个接口，但不能同时连接两个网络，而是利用一个切换开关，使得服务器在连接内网时断开外网，连接外网时断开内网。内网用户要从外网下载数据时，隔离服务器首先连接外网，将数据暂存在服务器中，隔一定时间后断开外网，连接内网，将数据发送到内部网络中。内外网之间的切换非常快，用户基本感觉不到时延。为防止信息泄露及黑客入侵，外部数据进入内网前会经过防火墙的过滤。

（3）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。

这种信息隔离与交换系统俗称网闸，网闸的设计是“代理＋摆渡”，如图 3.9 所示。当外网需要有数据到达内网的时候(B 点)，外部的服务器立即发起对隔离设备的非 TCP/IP 协议的数据连接，一般是不可路由的私有协议，隔离设备将所有的协议剥离或重组，将原始的数据写入存储介质(C 点)。根据不同的应用，可能有必要对数据进行完整性和安全性检查，如网络协议检查、防病毒和恶意代码扫描等。一旦数据完全写入隔离设备的存储介质，隔离设备立即中断与外网的连接，转而发起对内网的非 TCP/IP 协议的数据连接。隔离设备将存储介质内的数据通过专用隔离硬件交换到内网处理单元(A 点)。内网收到数据后，立即进行 TCP/IP 的封装和应用协议的封装，并交给应用系统。在控制台收到完整的交换信号之后，隔离设备立即切断隔离设备与内网的直接连接。

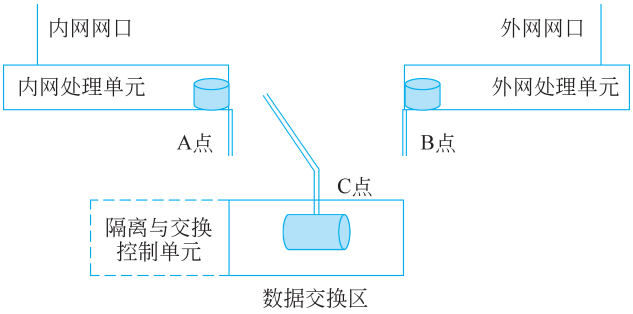

图 3.9　安全通道隔离技术原理

3.2.5　防信息泄露技术

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。尤其是显示器，由于显示的信息是供人阅读的，是不加任何保密措施的，所以其产生的辐射也最容易造成泄密。使用专门的高灵敏接收设备将这些电磁辐射接收下来，经过分析还原，就可以恢复原信息。

针对这一现象，美国国家安全局开展了一项绝密项目，后来产生了 TEMPEST(Transient Electromagnetic Pulse Emanation Standard)技术及相关产品。TEMPEST 技术又称计算机信息泄露安全防护技术，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，涉及多个学科领域。加解密等常规信息安全技术，并不能解决输入和输出端的电磁信息泄露问题，如 CRT 显示、打印机打印信息等。

TEMPEST 防电磁泄露的基本思想主要包括三个层面，如图 3.10 所示。

(1) 抑制电磁发射。采取各种措施想办法减少显示器、打印机等输入输出设备电路的电磁辐射。

(2) 屏蔽隔离。在其周围利用各种屏蔽材料使电磁发射场衰减到足够小，不易被接收，甚至接收不到。例如，对于需要高度保密的信息地点(如军、政首脑机关的信息中心和驻外使馆等地方)，应该将信息中心的机房整个屏蔽起来。屏蔽的方法是采用接地的金属网把整个房间屏蔽起来。小型系统可以把需要屏蔽的计算机和外部设备放在体积较小的屏蔽箱内。

(3) 相关干扰。在计算机旁边放置一个辐射带宽相近的干扰器，不断地向外辐射干扰电磁波，扰乱计算机发出的信息电磁波，使相关电磁泄露即使被接收也无法识别。

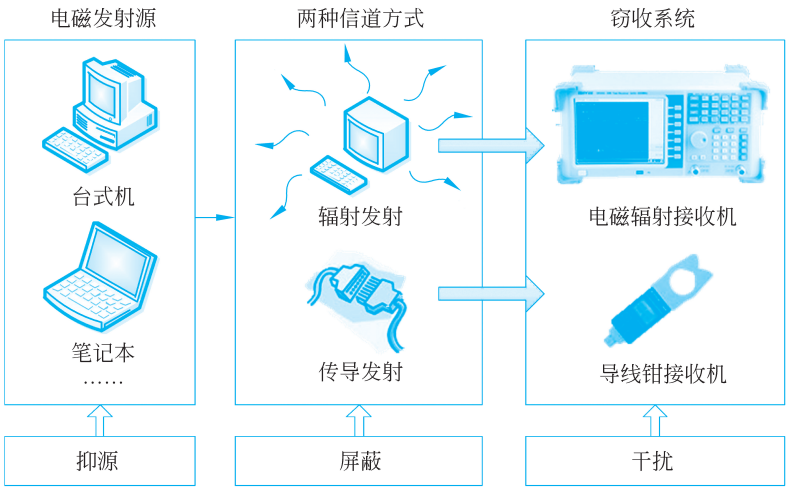

图 3.10　电磁泄露防护方式

3.3　物理安全管理

3.3.1　环境安全管理

计算机系统的技术复杂，电磁干扰、振动、温度和湿度变化都会影响计算机系统的可靠性、安全性。轻则造成工作不稳定、性能降低或出现故障；重则会使零部件寿命缩短，甚至是损坏。为了使计算机能够长期、稳定、可靠、安全地工作，应该选择合适的场地环境。

1. 机房安全要求

计算机机房应尽量建立在远离生产或存储具有腐蚀性、易燃易爆物品的场所周围；尽量避开污染区，以及容易产生粉尘、油烟和有毒气体的区域和雷区等。

机房应选用专用的建筑物，在建筑设计时考虑其结构安全。若机房设在办公大楼内，则最好不要安排在底层或顶层，这是因为底层一般较潮湿，而顶层有漏雨、雷击的危险。在较大的楼层内，计算机机房应靠近楼梯的一边。

此外，如何减少无关人员进入机房的机会也是计算机机房设计时首要考虑的问题。

2. 机房防盗要求

视频监视系统是一种较为可靠的防盗设备，能对计算机网络系统的外围环境、操作环境进行实时全程监控。对重要的机房，还应采取特别的防盗措施，如值班守卫、出入口安装金属探测装置等。

3. 机房“三度”要求

温度、湿度和洁净度并称为“三度”，为保证计算机网络系统的正常运行，对机房内的三度都有明确的要求。为使机房内的三度达到规定的要求，空调系统、去湿机、除尘器是必不可少的设备。重要的计算机系统安放处还应配备专用的空调系统，它比公用的空调系统在加湿、除尘等方面有更高的要求。

（1）温度：机房温度一般应控制在 18～22℃。

（2）湿度：相对湿度一般控制在 40%～60%为宜。

（3）洁净度：尘埃颗粒直径小于 0.5 μm，含尘量小于 1 万颗/升。

4. 防水与防火要求

计算机机房的火灾一般是由电气原因(电路破损、短路、超负荷)、人为事故(吸烟、防火、接线错误)或外部火灾蔓延引起的。计算机机房的水灾一般是由机房内有渗水、漏水等原因引起的。

为避免火灾、水灾,应采取如下具体措施。

(1) 隔离。

(2) 设置紧急断电装置。

(3) 设置火灾报警系统。

(4) 配备灭火设施。

(5) 加强防水、防火管理和操作规范。例如,计算机中心应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,检修时必须先关闭设备电源再进行作业等。

3.3.2　设备安全管理

1. 设备的使用管理

要根据硬件设备的具体配置情况,制定切实可行的硬件设备操作使用规程,并严格按操作规程进行操作。建立设备使用情况日志,并严格登记使用过程的情况。建立硬件设备故障情况登记表,详细记录故障性质和修复情况。坚持对设备进行例行维护和保养,并指定专人负责。

2. 设备的维护与保养

定期检查供电系统的各种保护装置及地线是否正常。对设备的物理访问权限限制在最小范围内。

3. 防盗

在需要保护的重要设备、存储媒体和硬件上贴上特殊标签(如磁性标签),当有人非法携带这些重要设备或物品外出时,检测器就会发出报警信号。将每台重要的设备通过光纤电缆串接起来,并使光束沿光纤传输,如果光束传输受阻,则自动报警。

4. 供电系统安全

电源是计算机网络系统的命脉,电源系统的稳定可靠是计算机网络系统正常运行的先决条件。电源系统电压的波动、浪涌电流和突然断电等意外情况的发生还可能引起计算机系统存储信息的丢失、存储设备的损坏等情况的发生,因此电源系统的安全是计算机系统物理安全的一个重要组成部分。

《计算机场地通用规范》(GB/T 2887—2011)将供电方式分为三类:一类供电,需要建立不间断供电系统;二类供电,需要建立带备用的供电系统;三类供电,按一般用户供电考虑。

5. 防静电

不同物体间的相互摩擦、接触会产生能量不大但电压非常高的静电。如果静电不能及时释放,就可能产生火花,容易造成火灾或损坏芯片等意外事故。计算机系统的 CPU、ROM、RAM 等关键部件大都是采用 MOS 工艺的大规模集成电路,对静电极为敏感,容易因静电而损坏。

机房的内装修材料一般应避免使用挂毯、地毯等吸尘、容易产生静电的材料,而应采用乙烯材料。为了防静电,机房一般要安装防静电地板。机房内应保持一定湿度,特别是在干燥季节应适当增加空气湿度,以免因干燥而产生静电。

6. 防雷击

接地与防雷是保护计算机网络系统和工作场所安全的重要措施。接地指整个计算机系统中各处电位均以大地电位为零参考电位。接地可以为计算机系统的数字电路提供一个稳定的0V参考电位，从而可以保证设备和人身的安全，同时也是防止电磁信息泄露的有效手段。

要求良好接地的设备有：各种计算机外围设备、多相位变压器的中性线、电缆外套管、电子报警系统、隔离变压器、电源和信号滤波器、通信设备等。

3.3.3 数据安全管理

计算机网络系统的数据要存储在某种媒体上，常用的存储媒体有：硬盘、磁盘、磁带、打印纸、光盘等。数据安全管理的内容主要包括以下几方面。

（1）存放有业务数据或程序的磁盘、磁带或光盘，必须注意防磁、防潮、防火、防盗。

（2）对硬盘上的数据，要建立有效的级别、权限，并严格管理，必要时要对数据进行加密，以确保硬盘数据的安全。

（3）存放业务数据或程序的磁盘、磁带或光盘，管理必须落实到人，并分类建立登记簿。

（4）对存放有重要信息的磁盘、磁带、光盘，要复制两份并分两处保管。

（5）打印有业务数据或程序的打印纸，要视同档案进行管理。

（6）凡超过数据保存期的磁盘、磁带、光盘，必须经过特殊的数据清除处理，视同空白磁盘、磁带、光盘。

（7）凡不能正常记录数据的磁盘、磁带、光盘，必须经过测试确认后销毁。

（8）对需要长期保存的有效数据，应在磁盘、磁带、光盘的质量保证期内进行转储，转储时应确保内容正确。

3.3.4 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。

第二级物理安全技术要求中设立了“人员要求”：要求建立正式的安全管理组织机构，委任并授权安全管理机构负责人负责安全管理的权力，负责安全管理工作的组织和实施。

第三级物理安全技术要求中规定了“人员与职责要求”：在满足第二级要求的基础上，要求对信息系统物理安全风险控制、管理过程的安全事务明确分工责任。对系统物理安全风险分析与评估、安全策略的制定、安全技术和管理的实施、安全意识培养与教育、安全事件和事故响应等工作应制定管理负责人，制定明确的职责和权力范围。编制工作岗位和职责的正式文件，明确各个岗位的职责和技能要求。对不同岗位制定和实施不同的安全培训计划，并对安全培训计划进行定期修改。对信息系统的工作人员、资源实施等级标记管理制度。对安全区域实施分级标记管理，对出入安全区域的工作人员应验证标记，与安全标记不相符的人员不得入内。对安全区域内的活动进行监视和记录，所有物理设施应设置安全标记。

第四级物理安全技术要求中规定了“人员与职责要求”：在满足第三级要求的基础上，要求安全管理渗透到计算机信息系统各级应用部门，对物理安全管理活动实施质量控制，建立质量管理体系文件。要求独立的评估机构对使用的安全管理职责体系、计算机信息系统物理安全风险控制、管理过程的有效性进行评审，保证安全管理工作的有效性。对不同安全区域实施隔离，建立出入审查、登记管理制度，保证出入得到明确授权。对标记安全区域内的活动进行

不间断实时监视记录。建立出入安全检查制度，保证出入人员没有携带危及信息系统物理安全的物品。

第五级物理安全技术要求在标准中未进行描述。

3.4　本 章 小 结

物理安全在整个计算机网络信息系统安全体系中占有重要地位。物理安全涉及计算机设备、设施、环境、人员等应当采取的安全措施，确保信息系统安全可靠运行，防止人为或自然因素的危害而使信息丢失、泄露或破坏。本章首先对物理安全的内涵、主要威胁、主要技术及相关标准进行了概述；其次，对物理访问控制技术、生物识别技术、检测和监控技术、物理隔离技术、防信息泄露技术等进行了详细介绍；最后，对物理安全管理所涉及的环境安全管理、设备安全管理、数据安全管理、人员安全管理等内容进行了阐述。

思　考　题

1. 物理安全在计算机信息系统安全中的意义是什么？
2. 物理安全主要包含哪些方面的内容？
3. 生物识别系统常见的实现方式和实现过程是怎样的？
4. 物理隔离与逻辑隔离的区别是什么？
5. 防止电磁泄露的主要途径有哪些？

第 4 章 操作系统安全

本章学习要点：

- 了解安全操作系统的安全策略与模型；
- 了解安全操作系统的访问控制机制；
- 了解安全操作系统的评测方法与准则。

操作系统是整个计算机系统的基础，它管理着计算机资源、控制着整个系统的运行，直接和硬件打交道，并为用户提供接口。无论是数据库系统、应用软件还是网络环境，它们都是建立在操作系统之上的，通过操作系统来完成对信息的访问和处理。因此，可以认为操作系统安全是整个信息安全的必要条件，这就使得操作系统经常是被攻击的目标。

WannaCry（又称 Wanna Decryptor），是一种“蠕虫式”的勒索病毒软件，大小为 3.3MB，利用永恒之蓝（EternalBlue）进行传播。永恒之蓝是 2017 年 5 月全球范围内暴发的基于 Windows 网络共享协议进行攻击传播的蠕虫恶意代码。不法分子通过改造之前泄露的 NSA 黑客武器库中“永恒之蓝”攻击程序发起了此次网络攻击事件。

2017 年，WananCry 席卷全球，超过 100 个国家和地区因感染 WananCry 损失惨重，堪称一场科技恐怖袭击。WananCry 会扫描计算机上的 TCP 445 端口（Server Message Block/SMB），以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求用户以比特币的形式支付赎金，勒索金额为 300～600 美元。在此次事件中，多个国家的重要信息网络受到袭击，我国的大量企业和机构内网，包括教育、企业、医疗、电力、能源、银行、交通等多个行业均受到不同程度的影响，我国的校园网络更是成为重灾区，多所高校出现病毒感染，学生的毕业论文等重要资料被病毒加密，只有支付赎金才能恢复。之后，360 安全中心发布公告，此次勒索事件是不法分子利用微软操作系统中编号为 MS17-010 的一个漏洞所致。微软公司曾经发布了对应安全补丁，遗憾的是，许多用户并没有及时更新，最终导致了这次“史无前例级别”的网络勒索事件，其中的教训令人警醒。

WananCry 感染原理：WananCry 感染的过程可分为两个阶段。

（1）感染阶段：病毒母体 mssecsvc.exe 运行，扫描随机 IP 的计算机进行感染，在感染后释放勒索程序 tasksche.exe。

病毒在网络上设置了开关，整个程序会先试图连接 szUrl 这个域名，连接成功就关闭线程，终止感染。szUrl 是个未经注册的地址：

```
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
```

这个域名显然是无效的。病毒被“启动”之后，会根据检测传给它的参数数量，安装 mssecsvc.exe，执行蠕虫函数。

蠕虫函数有三个主要作用：初始化网络、生成密码学相关的 API 和复制蠕虫的 payload

动态链接库(DLL)。payload 动态链接库的作用是把蠕虫病毒的二进制机器码复制到 C:\WINDOWS\mssecsvc.exe 并执行。初始化网络部分,蠕虫函数会生成两个线程,第一个线程用来扫描局域网内的主机,第二个线程用来扫描互联网里的主机。第一个线程通过 GetAdaptersInfo() 来获取局域网内的 IP 地址,然后用一个数组把这些 IP 地址存下来逐个扫描。这个线程会尝试连接 445 端口,如果连接成功就发起攻击感染。第二个线程会生成一个随机的 IP 地址,如果连接该随机 IP 地址的 445 端口成功,会对以 255.255.255.0 为掩码的整个地址段的计算机进行扫描,在这个地址段中开放 445 端口的计算机,都会被发起 MS17-010 漏洞攻击感染。

(2) 勒索阶段:勒索程序 tasksche.exe 运行,对磁盘文件进行加密,对感染 WananCry 的用户进行勒索。

勒索阶段主要是黑客利用 AES、RSA、比特币和洋葱路由等技术实现对感染 WananCry 的用户的匿名勒索。

洋葱网络是一种在计算机网络上进行匿名通信的技术。多层加密的通信数据在其传送到目的地的过程中,会通过由多个洋葱路由器组成的通信线路。在该过程中,每个洋葱路由器去掉一个加密层,并得到下一条路由信息,然后将数据继续发往下一个洋葱路由器,不断重复,直到数据到达目的地。

正是借助了比特币和洋葱路由技术,不法分子才能肆无忌惮地向感染 WananCry 的用户索取赎金。

WananCry 感染原因如下。

(1) 完全去中心化,没有特定的发行机构。

(2) 匿名性、无须交税及监管。

(3) 比特币依赖 P2P 网络,不会受发行机构的影响。

(4) 较方便、很简单就可以完成跨境交易。

EternalBlue(在微软的 MS17-010 中被修复)是在 Windows 的 SMB(server message block)服务处理 SMB v1 请求时发生的漏洞,这个漏洞导致攻击者在目标系统上可以执行任意代码。该漏洞出现的原因是 Windows SMB v1 中的内核态函数 srv!SrvOs2FeaListToNt 在处理 FEA(file extended attributes)转换时,会造成大非分页池(large non-paged kernel pool,一种内核的数据结构)上的缓冲区溢出。函数 srv!SrvOs2FeaListToNt 在将 FEA list 转换为 NTFEA(Windows NT FEA)list 前会调用 srv!SrvOs2FeaListSizeToNt 去计算转换后的 FEA lsit 的大小,然后会进行如下操作。

(1) srv!SrvOs2FeaListSizeToNt 会计算 FEA list 的大小并更新待转换的 FEA list 的大小。

(2) 由于错误地使用 Word 强制类型转换,最后计算出的待转换 FEA list 的大小比真正的 FEA list 大。

(3) 因为计算出的 FEA list 大小错误,当 FEA list 被转换为 NTFEA list 时,在大非分页池上就会出现缓冲区溢出问题。

攻击者利用缓冲区溢出漏洞就可以完成偷天换日,将原本应执行的程序代码操作转换为执行攻击代码。其详细的原理分析在 4.2.1 节给出。

4.1 操作系统安全概述

4.1.1 操作系统基础

操作系统(operating system,OS)是计算机系统中的一个系统软件,是计算机资源的直接管理者,操作系统为用户提供界面,是用户、应用程序和计算机硬件进行交互的“得力助手”。

操作系统在处理任务时,许多任务都与一些相关的安全问题有关,如图 4.1 所示,一个操作系统可以实现相关安全性的功能如下。

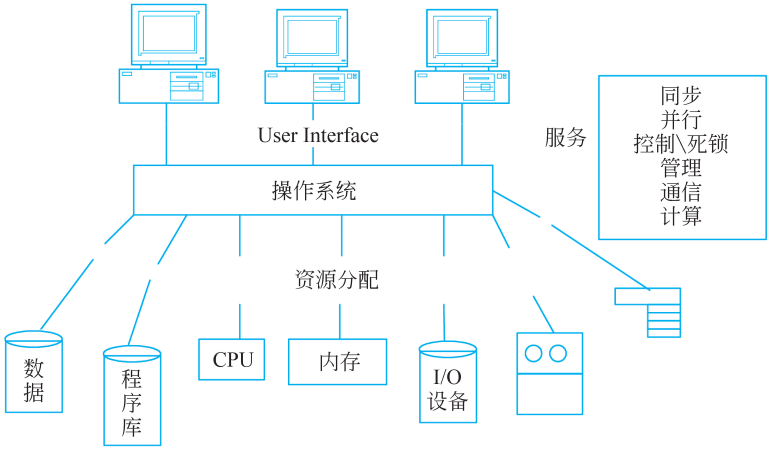

图 4.1 操作系统功能

(1) 用户鉴别。操作系统可以通过口令验证等机制对提出访问请求的用户识别并确定其身份。

(2) 内存保护。在一个系统中,所有的程序都是在受保护的内存中执行任务。这种保护可以防止外来的访问对内存造成的数据破坏,也可以控制一个用户对某一受限空间的访问权。例如,读、写、执行等不同的操作在内存中都是有不同的安全级别的。

(3) 文件及 I/O 设备访问控制。操作系统有保护 I/O 设备不受非法访问的能力。对于数据的保护通常是以查询表的形式利用访问控制矩阵来完成的。

(4) 对一般客体的资源分配与访问控制。用户在构造并发性许可并允许同步性时,要保证对客体的访问不会干扰到各个用户。通常会使用访问控制,它是由查询表实现的。

(5) 实现共享化。在系统中有些资源是分配给各用户专用的,而共享化则要求系统具有完整性和一致性。通常用带有完整性控制的查询表来实现共享。

(6) 公平服务。所有的用户都希望能最大限度地利用 CPU 得到尽可能多的服务。如不加控制,系统就会变得杂乱无章。操作系统通常使用硬件时钟控制和排序原则去保证服务公平性。

(7) 内部进程通信和同步。执行进程经常会与其他进程交换数据或保持同步性以实现资源的共享。操作系统的进程之间是相互联系的,用于交换需要处理的数据及同步信息。这些通信和同步由访问控制表实现。

(8) 操作系统数据保护。在操作系统中,重要的数据都是不能被随意更改的。很显然,如果数据没有受到保护而无法抵制非法访问,那么这个操作系统也就毫无安全性可言了。不同