第3章 物理安全

罗文坚

主要内容

3.1 概述

3.2 设备安全防护

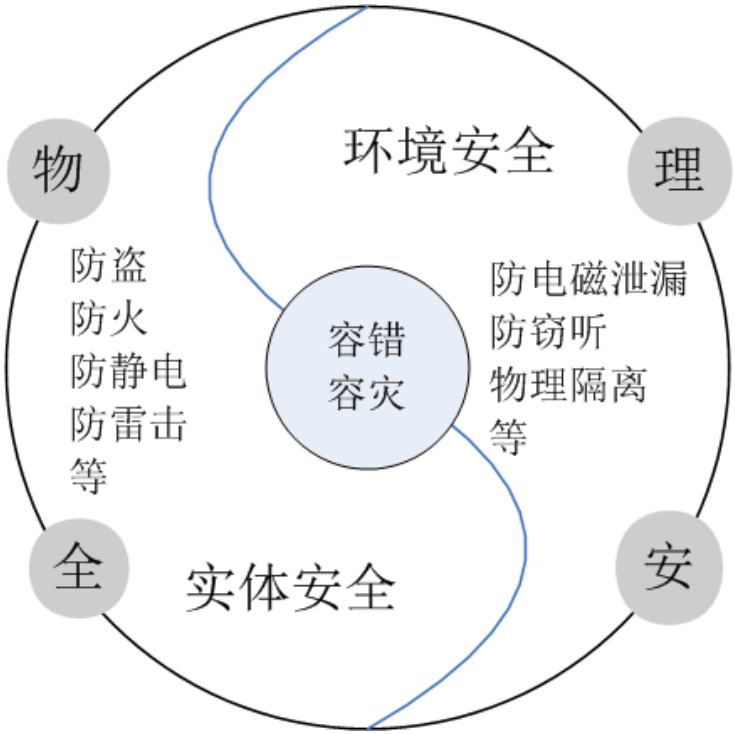
3.3 防信息泄露

3.4 物理隔离

3.5 容错与容灾

概述

- 物理安全：实体安全和环境安全。



- 物理安全技术主要解决两个方面的问题：
  - 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。

概述

- 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。

实际例子

- 某金融机构，机房没有24小时监控和值班巡检，导致机房空调出现异常后温度过高，导致多台服务器宕机。
- 某国企单位，机房在地下一层，门口竖了一块半米高的挡板，用来挡老鼠，防止老鼠咬坏线路的，☺。
- 某单位机房所在楼层的上层发生火灾，消防队灭火后，下层的机房被水给泡了。
- 某工厂车间，进出大门自动测量体重。体重波动超过五公斤就会报警。
- 某银行数据中心机房，采用双门禁系统。两道门禁不能同时打开。如果同时打开，会发出非常刺耳的报警声。
- 靠近ATM机的灌木丛太密，犯罪分子可以藏在它们后面，攻击前来取款的客户。

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

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。

- 对于保密程度要求高的计算机系统及其外部设备，应安装防盗报警装置，制定安全保护方法及夜间留人值守。

- 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。
- 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。

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

计算机机房的主要防火措施

1. 计算机中心应设置在远离散发有害气体及生产、储存腐蚀性物体和易燃易爆物品的地方，或建于其常年上风方向。
   - 不宜设在落雷区、矿区以及填杂土淤泥、流沙层、地层断裂、地址活动频繁区和低洼潮湿的地方；
   - 要避开有强电磁场、强振动源和强噪音源的地方。同时必须保证自然环境清洁、交通运输方便以及电力、水源充足。
2. 建筑物的耐火等级不应低于二级，要害部位应达到一级。
   - 五层以上房间内、地下室以及上下层或邻近有易燃易爆炸危险的房间内不得安装计算机。
   - 机房与其他房间要用防火墙分割封闭，装修、装饰材料要用不燃或阻燃材料。
   - 信息存储设备要安装在单独的房间，资料架和资料柜应采用不燃材料制作。

计算机机房的主要防火措施

3. 电缆竖井和管道竖井在穿过楼板时，必须用耐火极限不低于1h的不燃烧体隔板分开。电缆管道在穿过机房的墙壁处，也要设置耐火极限不低于0.75h的不燃烧体隔板，穿墙电缆应套金属管，缝隙应用不燃材料封堵。

4. 要建立不间断供电系统或自备供电系统，并在靠近机房部位设置紧急断电装置。计算机系统的电源线上，不得接有负荷变化的空调系统、电动机等电气设备，并做好屏蔽接地。消防用电设备的配电线路明敷时应穿金属管，暗敷时应敷设在不燃结构内。电气设备的安装和检修、改线和临时用线等应符合电气防火的要求。

5. 机房外面应有良好的防雷设施。设施、设备的接地电阻应符合国家规定的有关标准要求。机房内宜选用具有防火性能的抗静电地板。

计算机机房的主要防火措施

6. 可视情况设置火灾自动报警、自动灭火系统，并尽量避开可能招致电磁干扰的区域或设备，同时配套设置消防控制室。

7. 计算机中心应严禁存放腐蚀性物品和易燃易爆物品。检修时必须先关闭设备电源，再进行作业，并尽量避免使用易燃溶剂。

8. 所有工作场所应禁止吸烟和随意动火。工作人员应掌握必要的防火常识和灭火技能，值班人员每日要定时做好防火安全巡回检查，应配备轻便的气体灭火器。

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。
  - 设备或人体上的静电最高可达数万伏甚至数十万伏；在正常操作下，常达数百至数千伏。
- 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”。

计算机机房的静电防范措施

1. 温度、湿度要求：温度18~28度，湿度40%~65%。

2. 空气含尘要求：每升直径大于0.5μm的含尘浓度粒应小于3500个，每升直径大于5μm的含尘浓度粒应小于30个。含尘粒子为非导电、非导磁性和非腐蚀性的。

3. 地面要求：当采用地板下布线方式时，可铺设防静电活动地板；当采用架空布线方式时，应采用静电耗散材料作为铺垫材料。

4. 墙壁、顶棚、工作台和座椅的要求：墙壁和顶棚表明应光滑平整，减少积尘，避免炫光。允许采用具有防静电性能的墙纸及防静电涂料。可选用铝合金箔材做表面装饰材料。工作台、椅、终端台应是防静电的。

计算机机房的静电防范措施

5. 静电保护接地要求：静电保护接地电阻应不大于10欧姆，防静电活动地板金属支架、墙壁、顶棚的金属层都应接静电地，整个通信机房形成一个屏蔽罩。通信设备的静电地、终端操作台地线应分别接到总地线母体汇流排上。

6. 人员和操作要求：操作者必须进行静电防护培训后才能操作。

7. 其它防静电措施：必要时装设离子静电消除器，以消除绝缘材料上的静电和降低机房内的静电电压。机房内的空气过于干燥时，应使用加湿器或其他办法用以满足机房对湿度的要求。

8. 设施维护：定期（如一周）对防静电设施进行维护和检验。

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。接闪装置包括避雷针、避雷线和避雷带等。
  - 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，当直接雷或感应雷在线路上产生的过电压波沿着导线进入室内或设备时，避雷器的电阻突然降到低值，近于短路状态，将闪电电流分流入地。
  - 屏蔽：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。

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

电磁泄露

- 电子计算机和其他电子设备一样，工作时产生电磁发射，电磁发射包括辐射发射和传导发射。

- 电磁发射可能产生两个问题：
  1. 电磁干扰；
  2. 信息泄露。

电磁干扰

- 电磁干扰EMI（Electro Magnetic Interference）
  - 是指一切与有用信号无关的、不希望有的，或对电器及电子设备产生不良影响的电磁发射。
- 防止EMI要从两个方面来考虑：
  - 减少电子设备的电磁发射；
  - 提高电子设备的电磁兼容性EMC。
- 电磁兼容性EMC（Electro Magnetic Compatibility）：
  - 电子设备在自己正常工作时产生的电磁环境，与其它电子设备之间相互不影响的电磁特性。

TEMPEST

- 电磁发射还可能被高灵敏的接收设备接收并进行分析、还原，造成了计算机的信息泄露。
  - 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**技术又称为计算机信息泄漏安全防护技术，是一项综合性的技术，包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等项技术，涉及到多个学科领域。

- 常规的信息安全技术（如加密传输等）不能解决输入和输出端的电磁信息泄露问题，因为人机界面不能使用密码，而使用通用的信息表示方法，如**CRT**显示、打印机打印信息等。事实证明，这些设备电磁泄露造成的信息泄露十分严重。

TEMPEST

- 通常我们把输入、输出的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。

- 防电磁信息泄露，主要包括三个层面：
  1. 抑制电磁发射，采取各种措施减小“红区”电路电磁发射；
  2. 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；
  3. 相关干扰，采取各种措施使相关电磁发射信号即使被接收到也无法识别。

防电磁泄漏的常用方法

- 常用的防电磁泄漏的方法：
  - 屏蔽法（即空域法）
  - 频域法
  - 时域法

- 屏蔽法（即空域法）
  - 屏蔽法主要用来屏蔽辐射及干扰信号。
  - 采用各种屏蔽材料和结构，合理地将辐射电磁场与接收器隔离开，使辐射电磁场在到达接收器时强度降低到最低限度，从而达到控制辐射的目的。
  - 空域防护是对空间辐射电磁场控制的最有效和最基本的方法。机房屏蔽室就是这种方法的典型例子。

常用的防电磁泄漏的方法

- 频域法
  - 频域法主要解决正常的电磁发射受干扰问题。
  - 不论是辐射电磁场，还是传导的干扰电压和电流都具有一定的频谱，即由一定的频率成分组成。
  - 通过频域控制的方法来抑制电磁干扰辐射的影响，即利用系统的频率特性将需要的频率成分（信号、电源的工作交流频率）加以接收，而将干扰的频率加以剔除。
  - 频域法就是利用要接收的信号与干扰所占有的频域不同，对频域进行控制。

- 时域法
  - 与频域法相似，时域法也是用来回避干扰信号。
  - 当干扰非常强，不易受抑制、但又在一定时间内阵发存在时，通常采用时间回避方法，即信号的传输在时间上避开干扰。

窃听

- 窃听是指通过非法的手段获取未经授权的信息。
- 窃听的实现主要依赖于各种“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、电磁辐射以及计算机网络等。
- 窃听技术，是指窃听行动所使用的窃听设备和窃听方法的总称。
- 目前已经形成了有线、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从军事机密向商业活动甚至平民生活发展。

窃听

- 有线窃听：主要指针对他人之间的有线通信线路予以秘密侵入，以探知其通信内容。典型的是对固定电话的监听。
- 无线窃听：通过相关设备侵入他人间的无线通信线路以探知其通信内容，典型的是对移动电话的监听。
- 激光窃听：用激光发生器产生的一束极细的红外激光射在被窃听房间的玻璃上，房间内有人谈话时，窗玻璃会随声波发生轻微震动，从玻璃上反射回来的激光中包含了室内声波震动信息，经过接收器接收，解调放大，就能将声音还原。
- 辐射窃听：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：通过在网络的特殊位置按照窃听软件，接收能够收到的一切信息，并分析还原为原始信息。

窃听

- 防窃听：指搜索发现窃听装置及对原始信息进行特殊处理，以达到消除窃听行为或使窃听者无法获得特定原始信息。

- 防窃听技术主要分为两种：
  - 检测：主要指主动检查是否存在窃听器，可以采用电缆加压技术、电磁辐射检测技术以及激光探测技术等；
  - 防御：主要是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。
    - 另外，电磁信号屏蔽也属于窃听防御技术。

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

概述

- 物理隔离概念，最早出现在美国、以色列等国家的军方，用以解决涉密网络与公共网络连接时的安全。

- 在我国的政府涉密网络及军事涉密网络的建设中，也涉及了需要物理隔离的问题。

- 物理隔离，首先遇到的问题是安全域的问题。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：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、本部门或者本系统的工作秘密的网络空间。
  - 公共服务域：既不涉及国家秘密，也不涉及工作秘密。

物理隔离

- 物理隔离：
  - 较早时描述的单词Physical Disconnection。
  - 后来用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。

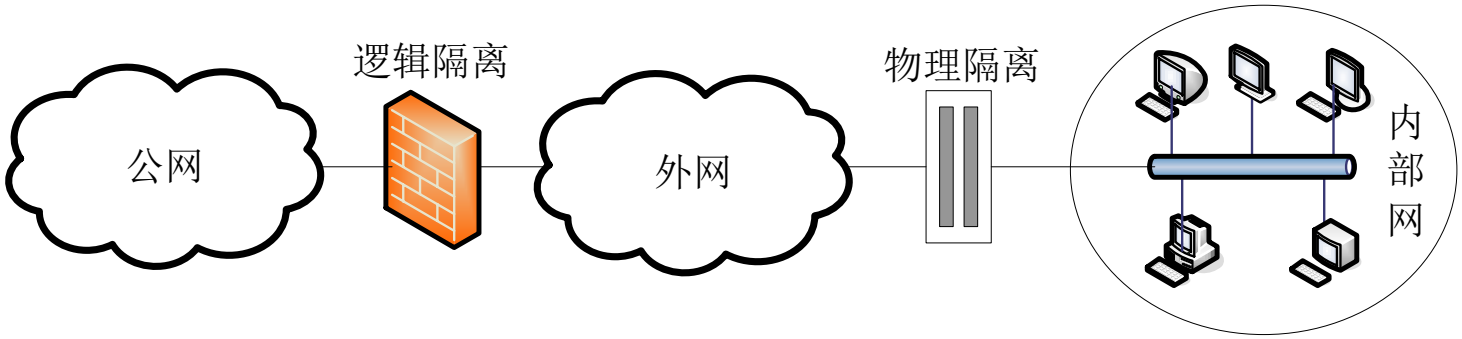
- 最初的物理隔离方法：建立两套网络系统和计算机设备。
  - 一套用于内部办公，另一套用于与互联网连接。
  - 采用两套互不相连的系统，不仅成本高，而且极为不便。
  - 这一矛盾促进了物理隔离设备的开发。

对物理隔离的理解表现

1. 阻断网络的直接连接。
2. 阻断网络的Internet逻辑连接。
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. 任何数据都是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. 隔离设备具有审查的功能。
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文件不会有病毒一样，也不会执行命令。
7. 强大的管理和控制功能。
8. 从隔离的内容看，隔离分为网络隔离和数据隔离。
   - 数据隔离：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：把被保护的网络从公开的、无边界的、自有的环境中独立出来。

物理隔离与逻辑隔离

- 物理隔离与逻辑隔离有很大的区别。
  - 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。



企业网络的划分

网络物理隔离的基本形式

1. 内外网络无连接，内网与外网之间任何时刻均不存在连接，是最安全的物理隔离形式。

2. 客户端物理隔离，采用隔离卡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。

3. 网络设备端物理隔离，在网络设备处的物理隔离常常要与客户端的物理隔离相结合，它可以使客户端通过一条网线由远端切换器连接双网，实现一台工作站连接两个网络的目的。

4. 服务器端物理隔离，实现在服务器端的数据过滤和传输，使内外网之间同一时刻没有连线，能快速、分时地传递数据。

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

容错

- 任何信息系统都存在脆弱性问题。

- 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：也称双件设备，就是备份两套相同的部件。正常情况下，一套运行，一套空闲。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。当原系统出现故障时，辅助系统只能在接近故障点的地方开始工作。

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。

容灾

- 容灾是针对灾害而言。灾害对于系统来说，危害性比错误要大、要严重。从保护系统的安全性出发，备份是容错、容灾以及数据恢复的重要保障。
  - 地震、火灾、水灾、暴乱、恐怖活动等。

- 容灾的真正含义是对偶然事故的预防和恢复。

- 解决方案有两类：
  1. 对服务的维护和恢复；
  2. 保护或恢复丢失的、被破坏的或被删除的信息。
  - 只有将两者结合起来，才能提供完整的灾难恢复方案。

容灾

- 灾难恢复策略：
  （1）做最坏的打算；对于可能遭受的破坏情况，尽量考虑周全。
  （2）充分利用现有资源；例如，利用磁盘、光盘等备份系统的信息和数据，直接用于灾难恢复。
  （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。
  - 例如，每天进行增量备份，每周进行一次完整备份。
  - 对于特别重要的部门，必须异地备份。

作业

- 习题2（1）。物理安全主要包括哪些内容？
- 习题2（4）。物理隔离和逻辑隔离的区别是什么？

- 思考题：假设某互联网企业需要建设一个数据中心，请提供一个物理安全解决方案。