第一章　绪论

考点一：了解计算机网络系统典型的安全威胁

威胁	描述
窃听	网络中传输的敏感信息被窃听
重传	攻击者事先获得部分或全部信息，以后将其发送给接收者
伪造	攻击者将伪造的信息发送给接收者
篡改	攻击者对合法用户之间的通信信息进行修改、删除或插入，再发送给接收者
非授权访问	攻击者通过假冒、身份攻击、系统漏洞等手段，获取系统访问权，从而使非法用户进入网络系统读取、修改、删除或插入信息等
拒绝服务攻击	攻击者通过某种方法使系统响应速度减慢甚至瘫痪，阻止合法用户获得服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
电磁、射频截获	攻击者从电子或机电设备发出的无线射频或其他电磁辐射中提取信息
人员疏忽	授权的人为了利益或疏忽将信息泄漏给未授权的人

考点二：计算机网络的不安全因素

1、不安全的主要因素：（1）偶发因素；（2）自然灾害；（3）人为因素

2、人为因素的分类：

名称	攻击	
被动攻击	（1）监视明文；（2）解密通信数据；（3）口令嗅探；（4）通信量分析	
主动攻击	（1）修改传输中的数据；（2）重放；（3）回话拦截；（4）伪装成授权的用户或服务器；（5）利用系统软件的漏洞；（6）利用主机或网络的信任；（7）利用恶意代码；（8）利用协议或基础设施的系统缺陷；（9）拒绝服务	
邻近攻击	（1）修改数据或收集信息；（2）系统干涉；（3）物理破坏	
内部人员攻击	恶意	（1）修改数据或安全机制；（2）擅自连接网络；（3）隐通道；（4）物理损坏或破坏
	非恶意	（1）修改数据；（2）物理损坏或破坏
分发攻击	（1）在设备生产时修改软硬件；（2）在产品分发时修改软硬件	

考点三：计算机网络安全的定义

1、计算机网络安全是指利用管理控制和技术措施，保证在一个网络环境里，信息数据的机密性、完整性及可使用性受到保护。

考点四：计算机网络安全的目标

1、计算机网络安全的目标：① 保密性；② 完整性；③ 可用性；④ 不可否认性；⑤ 可控性。

考点五：计算机网络安全的层次

1、根据网络安全措施作用位置的不同，可以将网络完全划分为四个层次，分别是物理安全、逻辑安全、操作系统安全和联网安全。

考点六：PPDR 模型

1、PPDR 模型是一种常用的网络安全模型，包含四个主要部分：

（1）Policy（安全策略）：是整个网络安全的依据。不同网络需要不同的策略，制定策略需要全面考虑局域网中如何在网络层实现安全性，如何控制远程用户访问等问题。策略一旦制定，应当作为整个网络系统安全行为的准则。

（2）Protection（防护）：通常是通过采用一些传统的静态安全技术及方法来实现的，主要有防火墙、加密和认证等方法。

（3）Detection（检测）：在 PPDR 模型中，检测是非常重要的一个环节，检测是动态响应和加强防护的依据也是强制落实安全策略的有力工具，通过不断地检测和监控网络和系统，来发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。

（4）Response（响应）：响应在安全系统中占有最重要的地位，是解决潜在安全问题的最有效办法。

2、PPDR 模型有一套完整的理论体系，以数学模型作为其理论基础——基于时间的安全理论。

考点七：OSI 安全体系结构

1、OSI 安全体系结构中定义了五大类安全服务，也称为安全防护措施。

（1）鉴别服务：提供对通信中对等实体和数据来源的鉴别；

（2）访问控制服务：对资源鉴别提供数据项是否来自于某个特定实体进行鉴别；

（3）数据机密性服务：保护信息不被泄露或暴露给未授权的实体；

（4）数据完整性服务：对数据提供保护，以对抗未授权的改变、删除或替代；

（5）抗抵赖性服务：防止参与通信的任何一方事后否认本次通信或通信内容。

2、OSI 参考模型从下层到上层依次是：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。

3、OSI 安全体系结构最基本的安全机制有八种：

① 加密机制；② 数字签名机制；③ 访问控制机制；④ 数据完整性机制；⑤ 鉴别交换机制；⑥ 通信业务流填充机制；⑦ 路由控制；⑧ 公证机制。

考点八：网络安全技术

1、网络安全的主要技术：

① 物理安全措施；② 数据传输安全技术；③ 内外网隔离技术；④ 入侵检测技术；⑤ 访问控制技术；⑥ 审计技术；⑦ 安全性检测技术；⑧ 防病毒技术；⑨ 备份技术；⑩ 终端安全技术。

2、物理安全措施主要包括环境安全、设备安全和媒体安全三个方面。

3、数据传输加密技术、数据完整性鉴别技术和防抵赖技术属于数据传输安全技术。防抵赖技术常用的方法是数字签名。

4、网络反病毒技术包括预防病毒、检测病毒和消除病毒三种技术。

考点九：计算机网络安全管理

1、计算机网络安全管理的主要内容有以下两方面：

（1）网络安全管理的法律法规。网络（信息）安全标准是信息安全保障体系的重要组成部分，是政府进行宏观管理的重要依据。信息安全标准关系到国家安全，是保护国家利益的重要手段，有利于保证产品的可信性，实现产品互联和互操作性，支持系统安全的测试和评估，保障计算机网络系统的安全可靠。

（2）计算机网络安全评价标准。计算机网络安全评价标准是一种技术性法规，在信息安全这个特殊领域，没有这种标准，会带来相关立法、执法的偏颇，造成严重后果，因此各国都在积极制定本国的认证标准。

（3）概括起来，网络安全包括以下三个重要部分：① 先进的技术；② 严格的管理；③ 威严的法律。

考点十：网络安全技术的发展趋势

1、网络安全技术的发展是多维的、全方位的，主要有以下几种：

① 物理隔离；② 逻辑隔离；③ 防御来自网络的攻击；④ 防御网络上的病毒；⑤ 身份认证；⑥ 加密通信和虚拟专用网；⑦ 入侵检测和主动防卫；⑧ 网管、审计和取证。

考点十一：网络安全威胁的发展趋势

1、网络安全威胁的发展趋势：

（1）与 Internet 更加紧密地结合，利用一切可以利用的方式进行传播。

（2）所有的病毒都具有混合型特征，集文件传染、蠕虫、木马和黑客程序的特点于一身，破坏性大大增强。

（3）其扩散极快，而更加注重欺骗性。

（4）利用系统漏洞将成为病毒有力的传播方式。

（5）无线网络技术的发展，使远程网络攻击的可能性加大。

（6）各种境外情报、谍报人员将越来越多地通过信息网络渠道收集情报和窃取资料。

（7）各种病毒、蠕虫和后门技术越来越智能化，并出现整合趋势，形成混合性威胁。

（8）各种攻击技术的隐秘性增强，常规防范手段难以识别。

（9）分布式计算机技术用于攻击的趋势增强，威胁高强度密码的安全性。

（10）一些政府部门的超级计算机资源将成为攻击者利用的跳板。

（11）网络管理安全问题日益突出。

第二章　物理安全

考点一：物理安全

1、物理安全的地位：是整个计算机网络系统安全的前提，在整个网络信息系统安全中占有重要地位。

2、主要内容：① 机房环境安全；② 通信线路安全；③ 设备安全；④ 电源安全。

考点二：机房安全

1、机房安全等级分类：

① A 类：对计算机机房的安全有严格要求，有完善的计算机机房安全措施；

② B 类：对计算机房的安全有较严格要求，有较完善的计算机房安全措施；

③ C 类：对计算机房的安全有基本的要求，有基本的计算机机房安全措施。

2、计算机机房在设计时首先要考虑的问题是如何减少无关人员进入机房。

3、机房的三度要求：

温度	18～22℃、超过规定范围时，每升高 10℃，计算机的可靠性下降 25%
湿度	40%～60%为宜
洁净度	机房尘埃颗粒直径小于 0.5 纳米，平均每升空气含尘量小于 1 万颗
为使机房内的三度达到规定的要求，空调系统、去湿机和除尘器是必不可少的设备。	

4、静电对电子设备的损害具有以下特点：隐蔽性、潜在性、随机性和复杂性。

5、地线种类：直流地、屏蔽地、静电地、雷击地和保护地

6、机房避免火灾、水灾的措施：隔离、火灾报警系统和灭火设施。机房应配置适用于计算及机房的灭火器材所在楼层应有防火栓和必要的灭火器材和工具，这些设施需具有明显的标记且定期检查，一般每 4 ㎡至少应配置一个灭火器。

考点三：设备安全

1、设备安全是一个比较宽泛的概念，包括设备的维护与管理、设备的电磁兼容好电磁辐射防护，以及信息存储媒体的安全管理等内容。

考点四：硬件设备

1、硬件设备的使用管理：

① 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的操作使用规程，并严格按操作规程进行操作；

② 建立设备使用情况日志，并严格登记使用过程的情况；

③ 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；

④ 坚持对设备进行例行维护和保养，并指定专人负责。

考点五：通信线路安全

1、通信线路安全技术：

① 电缆加压技术

② 对光纤等通信线路的防窃听技术（距离大于最大长度限制的系统之间，不采用光纤线通信；加强复制器的安全，如用加压电缆、警报系统和加强警卫等措施）

考点六：电磁辐射的防护

1、电磁辐射的防护措施主要有两类：

（1）对传导发射的防护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合；

（2）对辐射的防护，这类防护措施又可以分为两种：

① 采用各种电磁屏蔽措施，如对设备的金属屏蔽和各种接插件的屏蔽，同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离；

② 干扰的防护措施，即在计算机系统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

2、为提高电子设备的抗电磁干扰能力，除提高芯片、部件的抗电磁干扰能力外，主要的措施有屏蔽、隔离、滤波、吸收及接地等，其中屏蔽是应用最多的方法。

考点七：机房供电

1、机房安全供电的方式分为三类：

一类供电	需建立不间断（UPS）供电系统
二类供电	需建立带备用的供电系统
三类供电	按一般用户供电考虑

2、电源对用电设备安全的潜在威胁：① 脉动与噪声；② 电磁干扰