第一章

1：信息安全威胁的基本类型：信息泄露，信息伪造，完整性破坏，业务否决或拒绝服务，未经授权访问。

2：信息的安全属性主要包括：机密性，完整性，可用性，可控性，不可否认行。

3：信息安全威胁的主要表现形式：攻击原始资料（人员泄露，废弃的介质，窃取），破坏基础设施（电力系统，通信网络，信息系统场所），攻击信息系统（物理侵入，木马，恶意访问，服务干扰，旁路控制，计算机病毒），攻击信息传输（窃听，业务流分析，重放），恶意伪造（业务欺骗，假冒，抵赖），自身失误，内部攻击，社会工程学攻击。

4：面向应用的层次型技术体系结构：物理安全，运行安全，数据安全，内容安全，管理安全。

5：面向目标的知识体系结构：机密性，完整性，可用性。

6：面向过程的信息安全保障体系：保护，检测，反应，恢复。

7：OSI开放系统互联安全体系结构：安全服务（鉴别，访问控制，数据机密性，数据完整性，抗抵赖性），安全机制（加密，数字签名，访问控制，数据完整性，鉴别交换，业务流填充，路由控制，公证机制）。

第三章

1:设备安全防护:防盗，防火，防静电，防雷击。

2:防信息泄露:电磁泄露(屏蔽法，频域法，时域法)，窃听。

3: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。他是不安全就不联网，绝对保证安全。

4:逻辑隔离也是一种不同网络间的隔离部件，被隔离的两端仍然存在物理上数据通道连线，但通过技术手段保证被隔离的两端没有数据通道，即逻辑上隔离。在保证网络正常使用的情况下，尽可能安全。

5:物理安全:指为了保证计算机系统安全、可靠地运行，确保系统在对信息进行采集、传输、存储、处理、显示、分发和利用的过程中不会受到人为或自然因素的危害而使信息丢失、泄漏和破坏，对计算机系统设备、通信与网络设备、存储媒体设备和人员所采取的安全技术措施。主要包括实体安全和环境安全，涉及到网络与信息系统的机密性，可用性，完整性等属性。

6:电磁泄露:就是说你用的电脑，显示器，手机等，都是能产生电子辐射的，而且都有固定的特征，通过技术手段可以分析你电脑的使用内容，或者还原画面，造成秘密泄露！

7:物理隔离与逻辑隔离的区别:物理隔离部件的安全功能应保证被隔离的计算机资源不被访问，计算机数据不能被重用。  逻辑隔离应保证被隔离的计算机资源不被访问，只能进行隔离器内，外的原始应用数据交换，保证在进行数据交换时的数据完整性，以及保证隔离措施的可控性。

第四章

1:身份认证:是证实用户的真实身份与其所声称的身份是否相符的过程。实现身份认证的技术主要包括基于口令的认证技术，基于密码学的认证技术和生物特征的认证技术。

2:数字证书:是一种权威性的电子文档。它提供了一种在Internet上验证您身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个由权威机构----CA证书授权(Certificate Authority)中心发行的，人们可以在互联网交往中用它来识别对方的身份。当然在数字证书认证的过程中，证书认证中心（CA）作为权威的、公正的、可信赖的第三方，其作用是至关重要的。 数字证书也必须具有唯一性和可靠性。它采用公钥体制。

3:重放攻击:指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。它是一种攻击类型，这种攻击会不断恶意或欺诈性地重复一个有效的数据传输，重放攻击可以由发起者，也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据，之后再把它重新发给认证服务器。

4:Kerberos:他的设计目标是通过对称密钥系统为客户机服务器应用程序提供强大的第三方认证服务。包括一个AS和一个票据授予服务器。AS负责签发访问TGS服务器的票据，TGS负责签发访问其他应用服务器的票据。

5:CA:是负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。CA是证书的签发机构,它是PKI的核心。CA是负责签发证书、认证证书、管理已颁发证书的机关。它要制定政策和具体步骤来验证、识别用户身份，并对用户证书进行签名，以确保证书持有者的身份和公钥的拥有权。

6:PKI:是公钥基础设施，是一种遵循一定标准的密钥管理基础平台，它能够为所以网络应用提供加密和数字签名等密码服务所必须的密钥和证书管理。就是利用公钥理论和技术建立的提供安全服务的基础设施。

7:PKI的构成及每部分功能:认证机构CA(是PKI的核心执行机构，功能包括数字证书的申请注册，证书签发和管理)，证书库(是CA颁发证书和撤销证书的集中存放地，是网上的公共信息库，可提供公众进行开放式查询)，密钥备份及恢复(是密钥管理的主要内容)，证书撤销处理(撤销原CA证书，然后放入黑名单，用于公众核实证书的有效性)，PKI应用接口(使用者与PKI交互的唯一途径)。

8:RA服务器:主要面向业务受理操作员，负责登机，审核用户申请信息，包括注册申请和证书撤销申请，并将相关信息传给CA服务器和LDAP。

第五章

1:访问控制:是针对越权使用资源的防御措施，从而使系统资源在合法范围内使用。主要包括:主体，客体和控制策略。

2:访问控制模型:自主访问控制，强制访问控制，基于角色的访问控制。

3:自主访问控制:(DAC)是根据自主访问控制建立的一种模型，允许合法用户以用户或用户组的身份来访问控制策略许可的客体，同时阻止非授权用户访问客体。

4:强制访问控制:(MAC)是为了实现比DAC更为严峻的访问控制策略。它是一种多级访问控制策略，系统事先给访问主体和受控客体分配不同的安全级别属性，在实施访问控制时，系统先对访问主体和受控客体的安全级别属性进行比较，再决定访问主体能否访问该受控客体。

5:基于角色的访问控制:(RBAC)实施面向企业安全策略的一种有效的访问控制方式。其基本思想是，对系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。一旦用户被分配了适当的角色后，该用户就拥有此角色的所有操作权限。结构上有很多优势，更加灵活，方便和安全。

6:访问控制的基本原则:最小特权原则，最小泄露原则，多级安全策略。

7:MAC和DAC的区别:MAC的授权形式相对简单，工作量较小，但根据其特点不适合访问控制规则比较复杂的系统。DAC支持用户自主地把自己所拥有的客体的访问权限授予其他用户，但当企业的组织结构或是系统的安全需求发生较大变化时，就需要进行大量繁琐的授权工作，这样容易发生错误造成一些意想不到的安全漏洞。

8:角色和组的区别:组是具有某些相同特质的用户集合，而一个角色是一个与特定工作活动想关联的行为与责任的集合，角色不是用户的集合，也就与组不同了。组和用户都可以看成是角色分配的单位和载体，而一个角色可以看成是具有某种能力或某些属性的主体的一个抽象。

9:访问令牌:访问令牌说简单了就是个访问权限的数据集合,令牌中包含用户所有的权限,校验令牌可以识别用户是否有权限访问他要访问的位置

第六章

1:蠕虫病毒:一种常见的计算机病毒。它是利用网络进行复制和传播，传染途径是通过网络和电子邮件。是自包含的程序(或是一套程序),它能传播它自身功能的拷贝或它的某些部分到其他的计算机系统中。

2:蠕虫病毒与传统病毒的区别:蠕虫具有病毒的共同特征，但与传统病毒有一定的区别。传统病毒是需要寄生的，通过感染其他文件进行传播。蠕虫病毒一般不需要寄生在宿主文件中。蠕虫病毒往往能够利用漏洞进行攻击和传播。蠕虫病毒具有传染性，他是通过在互联网环境下复制自身进行传播，它的传染目标是互联网内的所以计算机。

3:木马:是一种伪装潜伏的网络病毒。木马是具有隐藏性，传播性的，可被用来进行恶意行为的程序。它一般不会直接对计算机产生危害，主要以控制计算机为目的。它的传播方式主要通过电子邮件，被挂载木马的网页以及捆绑了木马程序的应用软件。

4:病毒防治:检测，清除，预防，免疫。

5:拒绝服务攻击:是一种最悠久也是最常见的攻击形式，也称为业务否决攻击。严格说它不是一种具体的攻击方式，而是攻击所表现出来的结果最终使得目标系统因遭受某种程度的破坏而不能继续提供正常的服务。有两种攻击类型:一是利用网络协议的缺陷，通过发送一些非法数据包致使主机系统瘫痪。二是通过构造大量网络流量致使主机通信或网络堵塞，使系统或网络不能响应正常的服务。

6:Smurf攻击的原理:是以最初发动这种攻击的程序来命名的，这种攻击方法结合使用了IP地址欺骗和ICMP协议。它构造并发送源地址为受害主机地址，目的地址为广播地址的ICMP ECHO请求包，收到请求包的网络主机会同时响应并发送大量的信息给受害主机，致使受害主机崩溃。如果它攻击将回复地址设置成受害网络的广播地址，则网络中会充斥大量的ICMP ECHO响应包，导致网络阻塞。

7:嗅探攻击:也称为网络嗅探，是指利用计算机的网络接口截获目的地为其他计算机中的数据包的一种手段。黑客利用嗅探器获取网络传输中的重要数据。

8:IP欺骗:就是一台主机设备冒充另外一台主机的IP地址，与其他设备通信。主要是基于远程过程调用RPC的命令，这些命令仅仅根据信源IP地址进行用户身份确认，以便允许或拒绝用户RPC，获得远程主机的信任及访问特权。

9:DNS欺骗:DNS是一个可以将域名和IP地址相互映射的分布式数据库，DNS欺骗的目的是冒充域名服务器，把受害者要查询的域名对应的IP地址伪造成欺骗着希望的IP地址，这样受害者就只能看到攻击者希望的网站页面。有两种形式，即监听式主机欺骗和DNS服务器污染。

10:僵尸病毒:也称为僵尸程序，是通过特定协议的信道连接僵尸网络服务器的客户端程序，被安装了僵尸程序的机器称为僵尸主机，而僵尸网络是由这些受控的僵尸主机依据特定协议所组成的网络。  僵尸病毒的程序结构与木马程序基本一致，主要区别在于多数木马程序是被控制端连接的服务器端程序，而僵尸程序是向控制服务器发起连接的客户端程序。传播与木马相似，主要途径包括电子邮件，含有病毒的web网页，捆绑了僵尸程序的应用软件以及利用系统漏洞攻击加载等。

11:缓冲区溢出:是指当计算机向缓冲区内填充数据位数是超过了缓冲区本身的容量，溢出的数据覆盖了合法数据。它是一种非常普遍，非常危险的程序漏洞，在各种操作系统，应用软件中广泛存在。一般是由程序员写程序时的马虎所致。

12:网络钓鱼:是指攻击者通过伪造以假乱真的网站和发送诱惑受害者按攻击者意图执行某些操作的电子邮件等方法，使得受害者自愿交出重要信息的手段。

第七章

1:防火墙:是一个软件和硬件设备组合而成的，在内部网络和外部网络之间构造的安全保护屏障，从而保护内部网络免受外部非法用户的侵入。是位于两个或多个网络之间，执行访问控制策略的一个或一组系统，是一类防范措施的总称。

2:防火墙的作用:网络流量过滤，网络监控审计，支持NAT部署，支持DMZ，支持VPN。

3:包过滤防火墙:面向网络底层数据流进行审计和控管，因此其安全策略主要根据数据包头的源地址，目的地址，端口号和协议类型等标志来制定，可见其主要工作在网络层和传输层。

4:VPN:虚拟专用网，它是通过一个公用网络建立一个临时的，安全的选择，也可以理解为一条穿过公用网络的安全，稳定的隧道。VPN的实现主要依赖于隧道技术(一种协议完成对另一种协议的数据报文封装，传输和解封三个过程)。

5:入侵检测系统:以数据源为标准分为主机入侵检测系统和网络型入侵检测系统。以检测技术分为基于误用检测的IDS和基于异常检测的IDS。

6:Snort系统:是一个开放源代码的轻量级网络入侵检测系统，高效稳定，在全世界范围内被广泛安装和使用，它遵循CIDF模型，使用误用检测的方法来识别发现违反系统的网络安全策略的网络行为。

第八章

1:SSL:是一种用于保护客户端与服务器之间数据传输安全的加密协议，其目的是确保数据在网络传输过程中不被窃听及泄密，维护数据的完整性。SSL协议族是由四个协议组成的，分别是SSL记录协议，SSL握手协议，SSL转换密码规范协议和SSL报警协议。其中，SSL记录协议被定义为在传输层与应用层之间，其他协议为应用层协议。

2:HTTPS:是Web服务数据的主要传输规范。HTTPS是以安全为目标的HTTP通道，即在HTTP下加入SSL协议。

3:HTTPS的安全实现:他的思想很简单，就是客户端向服务器发送一个连接请求，然后双方协商一个SSL回话，并启动SSL连接，接着就可以在SSL的应用通道上传送HTTPS数据。

4:SET:是国际上最早应用于电子商务的一种网络协议，它依据网络电子交易的特点，专门用于解决交易的安全问题。SET的六组件分别是持卡人，商家，发卡机构，清算机构，支付网关和认证中心。SET协议安全性主要依靠其采用的多种安全机制，包括对称密钥密码，公开密钥密码，数字签名，消息摘要，电子信封，数字证书以及双重签名等。

5:CA证书:就是一份文档，它记录了用户的公开密钥和其他身份信息。

第二章

1:密码学:包括密码编码学和密码分析学。一个完整的密码体制包括五个要素:M,C,K,E,D。M是可能明文的有限集，称为明文空间。S是可能密文的有限集，称为密文空间。K是一切可能密钥构成的有限集，称为密钥空间。E是加密算法。D是解密算法。 密码学的目的就是发送者和接收者两个人在不安全的信道上进行通信，而破译者不能理解他们信道的内容。

2:古典替换密码:它的加密方法一般是文字替换。使用手工或机械变换的方式实现基于文字替换的密码。主要包括单表代替密码，多表代替密码以及转轮密码等。

3:常见的密码分析攻击形式:唯密文攻击，已知明文攻击，选择明文攻击，自适应选择明文攻击，选择密文攻击，选择密钥攻击。

4:简单代替密码:是指将明文字母表M中的每个字母用密文字母表C中的相应字母来代替，包括移位密码，乘数密码，仿射密码。

5:多表代替密码:是以一系列代替表依次对明文消息的字母进行代替的加密方法。这类密码，对每个明文字母都采用不同的代替表进行加密，称作一次一密密码。经典的多表代替密码:维吉尼亚密码和轮转机等密码。

6:对称密钥密码:又称为单密钥密码，建立在通信双方共享密钥的基础上，是加密密钥和解密密钥为同一个密钥的密码系统。

7:DES算法:是一种对二进制数据进行分组加密的算法，它以64位为分组对数据加密，DES的密钥也是长度为64位的二进制数，其中有效位数为56位。

8:分组密码:是将明文消息编码表示后的数字（简称明文数字）序列，划分成长度为n的组（可看成长度为n的矢量），每组分别在密钥的控制下变换成等长的输出数字（简称密文数字）序列。

9:流密码:它是对称密码算法的一种。序列密码具有实现简单、便于硬件实施、加解密处理速度快、没有或只有有限的错误传播等特点，因此在实际应用中，特别是专用或机密机构中保持着优势，典型的应用领域包括无线通信、外交通信。

10:公开密钥密码:又称为非对称密钥密码或双密钥密码，是加密密钥和解密密钥为两个独立密钥的密码系统。

11:单向陷门函数:是有一个陷门的一类特殊单向函数。它首先是一个单向函数，在一个方向上易于计算而反方向却难于计算。但是，如果知道那个秘密陷门，则也能很容易在另一个方向计算这个函数。即已知x，易于计算f（x），而已知f（x），却难于计算x。然而，一旦给出f（x）和一些秘密信息y，就很容易计算x。在公开密钥密码中，计算f（x）相当于加密，陷门y相当于私有密钥，而利用陷门y求f（x）中的x则相当于解密

12:消息认证:作为信息安全的三个基本目标之一，信息完整性的目的是确保信息在存储，使用，传输过程中不会被非授权用户篡改或防止授权用户对信息进行不恰当的修改。 违反安全规则的行为主要是:伪造，内容修改，顺序修改，时间修改，否认。

13:MAC:是一种重要的认证技术，基本思想是利用事先约定的密码，加密生成一个固定长度的短数据块MAC，并将MAC附加到消息后，一起发送给接收者，接收者使用相同密码对消息原文进行加密得到新的MAC，比较新的MAC和随消息一同发来的MAC，如果相同则未受到篡改。生成消息认证码的方法主要包括基于加密函数的认证码和消息摘要。(基于加密函数的认证码是指使用加密函数生成固定长度的认证码)

14:消息摘要:是以单向散列计算为核心，将任意长度的消息全文作为单向散列函数的输入，进行散列计算，得到的被压缩到某一固定长度的散列值作为认证符。

15:散列函数:是把任意长的输入消息串变化成固定长的输出串的一种函数。这个输出串称为该消息的杂凑值。一般用于产生消息摘要，密钥加密等.作用是:文件校验，数字签名，鉴权协议。

16:数字签名:是一种认证技术，主要用来防止信源抵赖。通过某种密码运算生成一系列符号及代码，构成可以用来进行数据来源验证的数字信息。数字签名主要采用公钥加密技术实现。

(1)A和B都将自己的公开密钥Ke公开登记并存入管理中心的共享的公开密钥数据库PKDB,以此作为对方及仲裁者验证签名的数据之一。

（2）A用自己的保密的解密密钥Kda对明文数据M进行签名得到签名S，然后A查询PKDB查到B的公开的加密钥Kea，并对用Kea对S再加密，得到密文C

（3）最后A把C发送给B，并将S和C留底。