

信息化素养提纲总结

一、无处不在的计算机

1. 电子数字计算机的四个时代是什么？分别具有哪些特征？

时间	元器件	数据处理方式	计算速度	整体特点
第一代 1946~1957	电子管	定点运算、 机器、汇编 语言	5000~1万次/ 秒	体积大、 功耗大、 速度慢
第二代 1958~1964	晶体管	浮点运算、高 级语言	几万~十几万 次/秒	体积小、 功耗减小 速度提高
第三代 1965~1970	中/小规模 集成电路	结构化、模块 化程序设计、 实时处理	十几万~几百 万次/秒	体积小、功 耗减小运行 速度提高
第四代1971~ 今	大、超 大规模 集成电 路	分时、实时 数据处理、 计算机网络	几千万 次到 百 亿条指 令/秒	性能大幅 度提高， 价格下 降，应用 到社会各 个领域

2. 第一台电子管计算机是什么？

第一台计算机 ENIAC : (electronic numerical integrator and Calculator) 诞生于美国宾西法尼亚大学，用于计算弹道。

元器件：电子管，耗电量大，不稳定，成本高，计算速度慢内存容量小，读写速度慢

无操作系统，只采用机器语言或汇编语言

3. 计算机的基本结构是什么？计算机系统的组成包括哪些部分？

计算机 = 硬件（主机+外设） + 软件（系统软件+应用软件）

4. 计算机**硬件系统**的组成是什么？
5. 计算机**主机**的组成是什么？
6. 计算机**中央处理器CPU**的组成是什么？
7. **内部存储器**包括哪些种类，分别有什么特点？
8. **外部存储器**包括哪些种类，分别有什么特点？

1. 主机

a) 中央处理器CPU

- i. 运算器（运算器完成各种算术运算和逻辑运算）
- ii. 控制器（控制器用来协调和指挥整个计算机系统的操作）

a) 内存储器

- i. RAM（随机存取存储器，俗称内存，随时使用，断电消失）
- ii. ROM（只读存储器，不能删改，出厂时固化，断电依旧保存）
- iii. Cache（高速缓冲存储器，远快于内存，用于提升效率）

2. 外设

- a) 外存储器（速度慢，容量大，价格低）（磁盘、闪存、光盘……）
- b) 输入设备
- c) 输出设备

9. 主板上的**总线**有哪些种类？

主板是计算机中最大的一块电路板，由多层印刷电路板和焊接在其上的 CPU 插槽、内存槽、高速缓存、控制芯片组、总线扩展、外设接口、鼠标口、CMOS 和 BIOS 控制芯片等构成

总线是一组连接各个部件的公共通信线，每一条线路都能够传输二进制数“0”和“1”

- a) 内部总线是各内部芯片与CPU之间的连线，用于芯片一级的互联
- b) 系统总线是各插件板与主板之间的连线，用于插件板一级的互联
- c) 外部总线是微机和外部设备之间的连线，用于设备一级的互联
- d) I/O总线就是CPU互联输入输出设备，并提供外设访问存储器和CPU的通道；I/O总线上通常传输数据、地址和控制信号三种信号

10. 常见的计算机**输入输出**设备有哪些？

键盘、鼠标、扫描仪、显示器、打印机、绘图仪、条形码阅读器……

11. **软件系统**指的是什么？计算机的软件系统的种类有哪些？

计算机软件是指计算机硬件上运行的各种程序、数据和一些

相关的文档、资料等

系统软件（操作系统）是用来控制和管理计算机资源，方便用户使用计算机的程序集合，是人机交互的接口，如 Windows、Linux 等

应用软件是专门为解决某个或某些应用领域中的具体任务而编写的功能软件，如 Office、Games 等

12. 操作系统的功能和种类有哪些？

1. 操作系统功能：
 - a) CPU的控制与管理
 - b) 内存的分配与管理
 - c) 外部设备的控制与管理
 - d) 文件管理
 - e) 作业管理和控制
2. 操作系统界面：
 - a) 命令行
 - b) 图形化

单用户单任务：DOS

单用户多任务：Windows

（注：Linux 应该是多用户多任务）

多用户多任务分时：UNIX

+网络功能：Netware、windows NT

13. 常用的计算机应用程序有哪些？

应用程序 APP (Application Program) 是为了某种特定的用途而开发的软件，一般只适用于一种或少数几种操作系统

常用应用程序：

- a) 文档处理软件
- b) 互联网与多媒体（浏览器、电子邮件、即时通信、网络下载等）
- c) 计算、分析、设计专用软件
- d) 程序设计、数据库软件
- e) 网络信息安全（病毒和木马防范、网络防火墙等）
- f) 专用程序及其他

14. BIOS程序是什么？

基本输入输出系 BIOS (Basic Input Output System) 是一组固化到计算机内主板上一个 ROM 芯片上的程序，它保存着计算机最重要的基本输入输出的程序、开机后自检程序和系统自启动程序；其主要功能是为计算机提供最底层的、最直接的硬件设置和控制

计算机的启动过程中，系统 BIOS 对系统的几乎所有硬件进行检测，这个过程通常称为 POST 自检 (Power On Self Test)

1. 完整的POST自检包括

a) 关键部件的检测:

i. 加电—CPU—BIOS—System Clock—64KB RAM—IRQ—显卡等

b) 非关键部件的检测:

i. 检测完显卡后，计算机将对64KB以上内存、I/O、软硬盘驱动器、键盘、即插即用设备、CMOS设置等进行检测，并在屏幕上显示各种信息和出错报告

#在正常情况下，POST 过程进行得非常快；如果出现错误，对于严重致命性故障就停机，由于各种初始化操作还没完成，不能给出任何提示或信号；对于非严重故障则给出提示或声音报警信号，等待用户处理

2. 当自检完成后，系统转入BIOS的下一步骤:

a) 寻找操作系统进行启动，然后将控制权交给操作系统

15. 计算机的启动过程是怎样的？

- 1) CPU初始化
- 2) 关键设备的检测
- 3) 显卡初始化
- 4) 显示系统BIOS的启动画面
- 5) 检测和显示CPU参数
- 6) 检测和显示系统标准硬件
- 7) 检测和配置即插即用设备
- 8) 显示标准硬件设备列表
- 9) 更新扩展系统配置数据ESCD
- 10) 系统BIOS引导启动盘，Windows启动

16. 计算机的发展趋势有哪些

1) 巨型化:

发展高速、大存储容量和强大功能的超大型计算机，用于核反应、天文、气象、宇宙工程、生物工程等尖端科学及新兴科学

2) 微型化:

芯片的集成度越来越高，计算机的元器件越来越小，而使得计算机的计算速度快、功能强、体积小、价格低

3) 网络化:

在一定的地理区域内，将分布在不同地点的不同机型的计算机和外部设备由通信线路互联组成一个规模大、功能强的网络环境，在网络软件的协调下，可以共享信息、数据及系统资源

4) 智能化:

让计算机来模拟人的感觉、行为、思维过程，使计算机具备听、视、语言、行为、思维、推理，学习、证明等能力。包括模式识别、专家系统、智能机器人

5) 多媒体化:

多媒体是“以数字技术为核心的图象、声音与计算机、通信等融为一体的信息环境”的总称,使计算机以更接近人的自然方式与我们交换信息

17. 计算机的分类有哪些

a) 超级计算机(巨型机):

特点: 体积大, 运行速度快, 功能强, 存储容量大, 用于科研国防, 例如: 神威、银河、曙光

b) 大型机:

特点: 由主处理器以及其他若干计算机组成, 用大型企事业数据库系统或网络中心的主机

c) 小型机:

特点: 规模小, 成本低, 用途广泛, 用于网络服务器

d) 工作站(超级微机):

特点: 速度快, 存储容量大, 易联网, 用于图像处理和辅助设计

e) 个人计算机(PC机) 台式机、笔记本、掌上电脑

18. 常见的移动智能终端操作系统有哪些

IOS

Android

Windows Phone

19. 如何保障系统和软件安全

a) 使用正版的操作系统和软件

b) 使用系统防火墙

c) 安装防病毒软件

d) 及时安装补丁程序

e) 正规的渠道获取软件

f) 根据自己的使用习惯和系统的性能选择合适的杀毒软件

g) 杀毒软件一定要保持在工作状态, 并且及时更新最新的病毒库

h) 一台机器上原则上不要安装两种杀毒软件

i) 及时更新补丁

二、无处不在的通信

1. 什么是通信

信源变成可传输的信号后, 通过信道(媒介)传输给信宿的过程就叫通信。

2. 通信的基本要素是什么

信源、信道、信宿

3. 主流的**通信技术**包括哪些

电信网、计算机网络、有线电视网

4. 从有线电报发展为**无线电报**，哪项发明起了决定作用？

电磁波

5. **莫尔斯电码**的主要贡献是什么？基本原理是什么？

只用两种电符号就能表示所有英文和数字，简化电报设计与传输

6. 有线电话的发明过程中，**交换机**的作用是什么？

将原本固定一对一的电话扩展至一对多

7. 电话交换机的技术历程是什么？哪一个技术发明催生了**程控交换机**的出现？

程控交换机=计算机+交换机

交换机类型	接续方式	控制方式	接线器	交换信息
磁石交换机	人工	铃流	塞绳	模拟话音业务
供电制交换机	人工	环路电流	塞绳	模拟话音业务
步进制交换机	自动	拨号脉冲	升降和旋转部件	模拟话音业务
纵横制交换机	自动	布线逻辑	机电纵横接线器	模拟话音业务
模拟程控交换机	自动	存储程序	空分电子接线器	模拟话音业务
数字程控交换机	自动	存储程序	时分电子接线器	数字话音、非话音数据图文传真等

8. **我国的电信网结构**是什么？

三级结构：本地网、长途网、国际网

9. 使**无线电话**成为可能的技术是什么？

电磁波和无线电；技术准备——载波：由振荡器产生并在通讯信道上传输的电波，被调制后用来传送语音或其它信息

10. 简述**蜂窝移动**通信系统的组成和原理。

组成：交换网路子系统(NSS)、无线基站子系统(BSS)和移动台(MS)三大部分 / 原理：小区制、蜂窝组网的理论

11. 简述蜂窝移动电话中，**1G/2G/3G/4G**的发展历程和各自特点。

1G: 第一代移动无线网络是面向语音的模拟无线系统，使用 FDMA 技术实现。

2G: 第二代移动无线网络是面向语音的数字无线系统，使用 TDMA 或窄带 CDMA 技术实现。

3G: 第三代移动无线网络把蜂窝电话、语音业务以及移动数据业务用各种分组交换数据业务综合在一个高语音质量、高容量、高速率的网络系统中。

4G: 第四代移动无线网络最初目的就是提高蜂窝电话和其他移动装置无线访问 Internet 的速率，最重要的特征就是更快的无线通信速度

12. 什么是**计算机网络**？

计算机网络 — 将地理位置不同并且具有独立功能的多个计算机系统，通过通信设备和通信线路连接起来，在网络软件的支持下实现彼此之间的数据通信和资源共享的系统，称之为计算机网络。(A computer network is a collection of autonomous computers, interconnected by communication channels. 被操作对象: 一些独立自治的计算机系统; 互连的手段: 在各种各样的在协议(Protocol)支持下进行工作)

13. 计算机网络的**发展历程**是什么？

计算机孤岛→终端出现→计算机和计算机互联→网络与网络互联

14. **ARPANET**的技术特点有哪些，在网络发展历程的贡献是什么？

不采用传统电话网的集中式结构，提出了分组交换技术的概念；采用分组交换技术实现计算机与计算机之间的通信，使计算机网络的结构、概念都发生了变化，形成了通信子网和资源子网的网络结构

15. 计算机网络发展经过了哪些阶段？每个阶段的主要特点是什么？

阶段	20 世纪	特点
远程终端联机阶段	50-60 年代中	主机—通信线路—终端
计算机网络阶段	60 年代中-70 年代中	采用分组交换技术实现计算机与计算机之间的通信
计算机网络互联阶段	70 年代中-80 年代末	网络体系结构的形成 网络协议的标准化
互联网时代	80 年代末至今	开启各个领域的网络化进程

三、无处不在的互联网

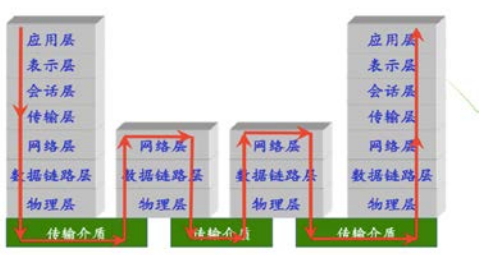
1. OSI 参考模型的基本结构是什么？各层的主要功能是什么？

1. 物理层(physical layer)：保证二进制位流的正确传输.
2. 数据链路层(data link layer)：保证信息帧的正确传输和流控、实现介质访问控制协议
3. 网络层(network layer)：报文分组和组装、路由选择
4. 传输层(transport layer)：保证端一端的信息的正确传输
5. 会话层(session layer)：建立、管理、结束主机间的会话
6. 表示层(presentation layer)：数据压缩和解压缩、数据加密和解密、文件格式的转换
7. 应用层(application layer)、为应用程序提供网络服务

2. OSI 参考模型的基本思想？网络中各节点具有相同的层次；不同节点的同等层具有相同的功能；同一节点内相邻层之间通过接口通信；每一层可以使用下层提供的服务，并向其上层提供服务；不同节点的同等层按照协议实现对等层之间的通信

3. 互联网中的数据是如何流动的？

OSI参考模型：数据流向



4. TCP/IP 体系结构的主要特点是什么？不同层主要包含哪些协议？

主要特点：

- a) 开放的协议标准，可以免费使用；
- b) 可运行于局域网、广域网和互联网中；
- c) 统一的网络地址分配方案；
- d) 标准化的高层协议。

TCP/IP协议栈

@ 网络层协议主要包括：

	OSI模型	TCP/IP 协议					TCP/IP 模型
@ 互联网协议IP	应用层	文件传输	远程登录	电子邮件	网络文件	网络管理	应用层
@ 互联网控制报文协议 ICMP	表示层	协议 FTP	协议 Telnet	协议 SMTP	服务 协议 NFS	协议 SNMP	
	会话层						
@ 传输层协议包括：	传输层	TCP UDP					传输层
@ 传输控制协议TCP	网络层	IP	ICMP	ARP	RARP		网际层
@ 用户数据报协议UDP	数据链路层	Ethernet IEEE 802.3	FDDI	Token-Ring/ IEEE 802.5	ARCnet	PPP/SLIP	网络接口层
@ 应用层包括所有的高层协议	物理层						硬件层

5. 互联网主要的设备有哪些？分别有什么特点？

- a) 物理层:集线器，中继器 @ 广播式转发 @ 所有设备属于一个网段(冲突域)
- b) 数据链路层:网桥，交换机 @ 可以划分多个网段(冲突域) @ 所有同属于一个广播域

c) 网络层: 路由器 @ 多个广播域

6. IP 地址的格式和分类是什么?

IP 地址是一种层次型地址结构, IP 地址长度为四字节(32bit), 分为两部分, 即网络号(Network ID) 和主机号(Host ID); IP 地址是 32 位二进制, 分为 4 个字节, 每个字节 8 位, 中间用小圆点隔开, 然后将每八位二进制转换成一个十进制数; 分为 A/B/C/D/E 五类 (A、B、C 类网络数递增, 主机数递减; D 类为组播; E 类为未来使用)

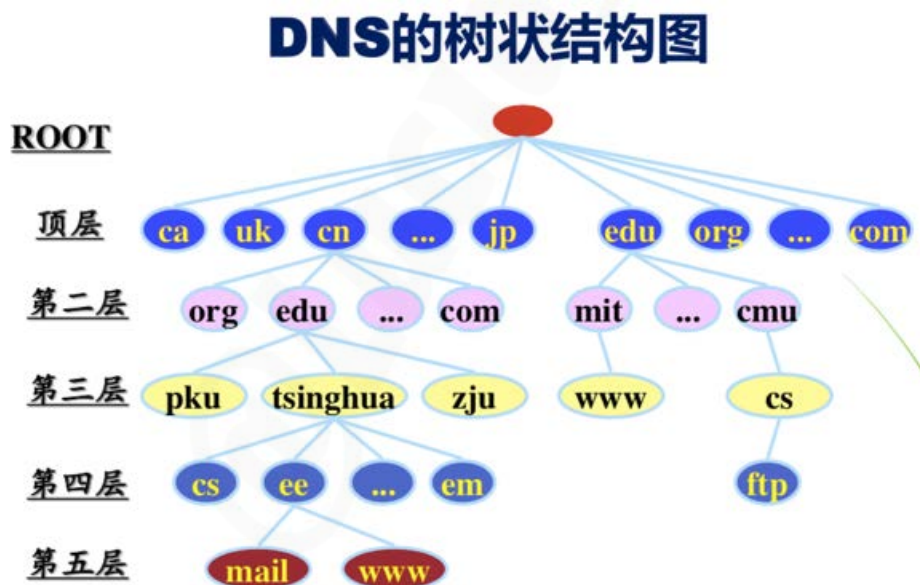
7. 什么是域名系统 DNS? 域名系统 DNS 中域名的结构是什么?

域名系统采用层次结构, 按地理区域或机构区域进行分层。在书写时, 采用圆点(.)将各个层次域隔开。/ 域名系统 DNS 的核心是分级的、基于域的命名机制以及为了实行这个命名机制的分布式数据库系统。

8. 域名与 IP 地址之间的关系是什么?

域名系统用于将便于人们记忆的主机域名和电子邮件地址映射为计算机易于识别的 IP 地址。

9. 常用的域名怎么表示? (如下图)



10. 域名什么是 MAC 地址? MAC 地址的作用是什么? 每个计算机都需要有一个能够唯一标识自己的方式; 无论是否连接在网络上, 都会有一个物理地址, 而且是唯一的。在出厂之前, 生产网卡的厂商会为每一块网卡指定一个物理地址, 也被称为 MAC 地址。

11. IP 地址与 MAC 地址的对应关系是什么？

物理地址：MAC地址	逻辑地址：IP地址
<p>@物理地址是第二层地址</p> <p>@MAC地址固化在网卡的硬件结构</p> <p>@只要主机或设备的网卡不变，其MAC地址就是不变的</p> <p>@即使其从一个网络被移到另一个网络，从地球的一端移到另一端</p> <p>@一种平面化的地址，不能提供关于主机所处的网络位置信息</p> <p>@就类似人的姓名</p>	<p>@逻辑地址是第三层地址</p> <p>@IP地址是随着设备所处网络位置不同而变化的</p> <p>@设备从一个网络被移到另一个网络时，其IP地址也会相应地发生改变</p> <p>@IP地址是一种结构化的地址，可以提供关于主机所处的网络位置信息</p> <p>@就类似人的住址</p>

12. ARP 协议的工作流程是什么？

- 在主机启动加入网络时，首先主动广播自己的IP/MAC地址。建立一个ARP表，表中存放(IP地址，MAC地址)对。当源主机确定了目标的IP地址后，为了获得目标的MAC地址，开始查找ARP表。
- 若源与目的主机在同一子网内，用目的IP地址在ARP表中查找。若不再同一子网，用缺省网关的IP地址在ARP表中查找。如果ARP表中没有所需要的MAC地址。源主机就发出一个广播请求：“如果你的IP地址和这个目的IP地址相同，请告诉我你的物理地址。”
- 网络中的主机在接收到请求后，开始判别地址段是否和自己相符。不相符，信息丢弃；相符，则作出响应“我的物理地址为 aabb.ccdd.eeff”。源主机就将此信息储存到自己的ARP表中。
- ARP表中的表项有生存期，超时则删除。

四、无处不在的互联网应用

1. 应用层常用的协议有哪些？都有什么用途？

- 文件传输 - TFTP - FTP- NFS;
- 电子邮件 - SMTP;

- c) 远程登录- Telnet - rlogin;
- d) 网络管理- SNMP;
- e) 域名服务- DNS;
- f) 即时通讯- QQ -weChat

2. 应用程序的实现结构中，对等模式和客户/服务器模式有什么不同？

对称的对等模式-应用进程的地位和作用平等；

客户/服务器模式-@ 客户：一般为网络用户的主机 @ 处于主动地位，向服务器发出各种请求@ 服务器：为网络上能够提供特定服务的主机 @ 处于被动地位，根据客户的请求提供响应的服务-提出要求 返回结果

3. 客户/服务器模式中，客户机和服务器的地位和特点分别是怎么样的？
(见上题)

4. 万维网 WWW 的基础技术是什么？采用了哪种实现结构？哪种传输协议？

超文本(hypertext)是万维网的基础；WWW 系统是基于服务器/客户模式的，客户端和服务端之间的传输协议为超文本转换协议 HTTP(HyperText Translation Protocol)；

5. Web 网站系统的组成部分有哪些？常用的技术有哪些？

万维网 WWW 又称为网站 Web，完整的网站系统分成服务器端、客户机接收端和通信协议三部分@服务器端:Web Server @客户机接收端:浏览器 Browser、专用程序 @通信协议:HTTP(超文本传输协议)是基于 TCP/IP 的应用层协议，典型的 Client/Server 工作方式，简单快速，数据传输较少

6. WWW 代理服务的功能是什么？

对 WWW 代理服务器而言，其功能为：@ 代理访问、加快访问速度@ 内外网隔离，起到防火墙的保护作用@ 用户管理和用户行为监控；万维网高速缓存将最近的一些请求和响应暂存在本地磁盘中@ 当与暂时存放的请求相同的新请求到达时，高速缓存就把暂存的响应发送出去，而不需要按 URL 的地址再去因特网访问该资源

7. 电子邮件系统由哪些部分组成？

列举几个主要的即时通讯服务。电子邮件系统由两部分组成：

1. @ 用户代理——允许用户阅读/发送电子邮件，一般为用户进程。
 - a) @ 用户负责编写和阅读邮件，提供收件人的地址。
 - b) @ 邮件编辑器和阅读器负责邮件与处理程序之间的接口程序。
2. @ 邮件传输代理(也称邮件服务传输系统)——将消息从源端发送至目的端。
 - a) @ 由邮件服务器(mail server)、邮件主机(mail host)、中继主机(relay host)等组成

8. 电子邮件的格式是怎样的？RFC822 和 MIME 格式有什么不同？

电子邮件是由信封和消息两个部分构成的。

@ 信封：“用户名@主机名”

@ 消息：由信头(一些控制信息)和信体(由发信人自由撰写的内容) 构成。
/ RFC882: 由发信人填写的参数&由邮件系统填写的参数；MIME: @ 邮件信头和信体都采用了 7 位的 ASCII 码 @ 限制条件-每个字节的最高位置零 @ 使用条件-适用于无格式的英文文本信息传输 @ 不适用于 @ 包含了非 ASCII 码字符集的信息，例如中文。 @ 包含了格式的文本信息，例如 DOC 文件。 @ 包含了语音和图象等非文本信息。

9. 简要描述电子邮件的工作流程。

1. 用邮件处理软件撰写信件和收件人地址。
2. 客户程序将邮件通过 SMTP 发给服务提供者---邮件服务器。
3. 邮件服务器利用 Internet 使用 SMTP 协议在邮件主机之间传递邮件。
4. 邮件到达目的邮件服务器，目的邮件服务器将邮件放入接收者的信箱中。
5. 接收者利用 POP3 从他的邮件服务器中取信，并利用邮件处理软件阅读信件。

10. 简要描述 SMTP 协议的实现过程。(Simple Mail Transfer Protocol)

1. 寻址: 向 DNS 发送请求，得到接收方的 IP 地址。

2. 建立连接:源邮件主机向目的邮件主机 TCP 端口 25 请求建链, TCP 握手成功, 目的邮件主机回送确认(220)。
3. 传输邮件:完成邮件的传送。
4. 拆除连接:源邮件主机请求断链, 目的邮件主机回送确认(221)

11. POP3 协议和 IMAP 协议在功能上有什么异同?

都是电子邮件的接受协议; /IMAP 协议运行在 TCP/IP 协议之上, 使用的端口是 143。与 POP3 协议的主要区别是用户可以不用把所有的邮件全部下载, 可以通过客户端直接对服务器上的邮件进行操作。

12. 即时通讯(IM)的含义是什么? 列举几个主要的即时通讯服务。

即时通讯 IM(Instant messaging)是一个终端服务, 允许两人或多人使用网络上即时地传递文字讯息、档案、语音与视频交流。/ QQ, 微信, Skype, Telegram, 钉钉 etc.

13. 虚拟专用网 VPN 的功能是什么?优势有哪些?为什么会有对 VPN 的需求?

在公共网络中建立专用网络, 数据通过安全的“加密隧道”在公共网络中传播。

VPN 的优势:

- 1) 节约成本:节省专线费用、设备费用、移动通讯费用等
- 2) 使用强有力的加密手段保证传输数据的机密性(数据机密性)
- 3) 保障传输数据的不被篡改(数据完整性)
- 4) 使用数字签名技术保障数字发送源的真实性(数据的真实性)
- 5) 提供不同用户不同权限的访问控制(访问控制)

因为:

- 1) 企业的收购与合并, 需要互连不同的网络
- 2) 企业的分支机构增多, 各分支机构需要网络互连
- 3) 动态的企业与客户之间的联系
- 4) 昂贵的专线费用
- 5) 企业数据的安全性保护

14. 简要描述虚拟专用网 VPN 的隧道技术原理

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据可以是不同协议的数据帧或包。隧道协议将这些

其它协议的数据帧或包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网络传递。

15. VPN 的使用模式有哪些？

- 6) Access VPN: 企业员工或小分支机构通过公网远程访问的方式，访问公司的虚拟网
- 7) Intranet VPN: 企业总部与分支机构通过VPN虚拟专用网进行的网络连接
- 8) Extranet VPN: 企业之间发生并购，兼并或企业间建立战略联盟后，使不同企业网通过公网来构筑的虚拟网

四、无处不在的网络安全

16. 互联网安全黑色产业链有哪些组成部分？

- 1) 最顶层——漏洞挖掘
- 2) 第二层——代码编写
- 3) 第三层——信息窃取
- 4) 第四层——信息贩卖
- 5) 第五层——窃取诈骗

17. 说明个人日常使用网络时需要保护的信息。

- 1) 网络账号
- 2) 个人身份信息
- 3) 隐私信息
- 4) 与现实财产有关的信息
- 5) 其他有用的数据信息

18. 网络攻击中窃取信息的主要途径有哪些？

- 1) 数据在网络传输过程中被窃取
- 2) 数据存储在自己系统上被恶意软件（木马病毒）窃取
- 3) 数据存储在网络系统上的数据被恶意攻击者通过攻击窃取

4) 用户被钓鱼，自己泄露的

19. 网络中常见的攻击技术有哪些？

- 1) 基于缺陷（漏洞）的攻击
- 2) 中间人攻击
- 3) 病毒木马
- 4) 蛮力破解
- 5) 社会工程学攻击
- 6) 拒绝服务攻击

20. 什么是(系统或软件的)漏洞?漏洞可能是在计算机系统的哪些阶段产生的?不同阶段产生的漏洞都有哪些弥补方式?

- 1) 漏洞：系统或软件程序在编写及实现过程中存在的问题
- 2) 产生及对应弥补方式：
 - a) ①设计阶段的缺陷——困难，往往需要推翻原有的设计框架才能修补；因此很多时候只能通过变通的方法来缓解风险，并不能完全杜绝
 - b) ②实现阶段的缺陷——通过安装“补丁程序”来解决问题
 - c) ③使用阶段的缺陷——只能靠用户改变自身习惯来杜绝。

21. 病毒的发展阶段有哪些?病毒具有哪些功能?

- 1) 传统病毒——蠕虫病毒——木马病毒
- 2) 漏洞利用、程序感染、自主传播、及远程控制的各种功能

22. 简要说明下列信息窃取方式:蛮力破解(字典、撞库)、中间人攻击、拒绝服务攻击、恶意软件。

- 1) 使用数字和字母的任意组合，猜出用户名和口令（字典）；
- 2) 用已经获取的用户名和密码去尝试登陆其他更大型的信息系统（撞库）；

- 3) 在两个受害人网络链路之间进行数据监听和数据篡改
- 4) 企图通过使你的计算机崩溃或把它压垮来阻止你提供服务
- 5) 伪装成正常程序欺骗用户来运行

23. 什么是**社会工程学攻击**?网络上的社会工程学攻击手段有哪些?

利用人的弱点（如本能反应，好奇心，信任，贪便宜等）进行恐吓、欺诈以获取利益的一种攻击行为

网页钓鱼、邮件欺诈、短信息欺诈

24. 什么是**防火墙**?有哪些常用技术?哪些事情是防火墙做不到的?

在两个网络（通常是用户内部网络和 Internet）之间实现访问控制政策的一个或一组系统（硬件、软件的组合）

常用技术：服务控制、方向控制、用户控制、行为控制

特点：

- 1) 自身不会正确的配置，需要用户定义访问控制规则
- 2) 不能防止内部恶意的攻击者
- 3) 无法控制没有经过他的连接
- 4) 不能很好地实现防病毒、信息扩散
- 5) 无法防范全新的威胁和攻击

25. 常见的**防病毒技术**有哪些?为什么不要在同一系统上装多个防病毒软件?

- 1) 通过病毒程序的特征匹配
- 2) 通过病毒程序的行为监控
- 3) 启发式扫描
- 4) 软件模拟操作系统，让病毒在虚拟的沙盒系统中运行

由于防病毒软件需要最高的系统权限，所以如果在一个系统上安装多个防病毒软件可能会出现权限控制导致错误

26. 访问控制技术的目的是什么?通过什么方式来发挥作用?

- 1) 能够保护系统和资源免受未经授权的访问
- 2) 防止非法用户进入系统
- 3) 方法合法用户对系统资源进行非法使用

27. 身份认证所使用的信息有哪些类型?分别就每种类型举出几个例子。

1. 基于你所知道的: 知识, 口令, 密码
2. 基于你所拥有的: 身份证, 钥匙,
3. 基于你的个人特征: 指纹, 笔迹, 声音
4. 双因素、多因素认证

28. 加密技术的应用环境和目的?熟练掌握 Playfair 密码算法。

1. 在不安全的环境中用来保护数据不被他人非法窃取
2. (见 PPT6 p43)

29. 信息安全意识包括哪三个方面?

使用环境安全、系统及软件安全、使用习惯的安全

30. 有线和无线网络环境中主要的安全风险是什么?

有线: 数据窃听——①控制网关设备进行数据窃听②局域网内使用 ARP 攻击网关进行数据窃听

无线: 数据窃听 (由于其扩散性使得无线网数据窃听要比有线网络容易)

31. 系统及软件面临的安全风险有哪些?哪些措施可以用来保护系统及软件安全?

系统:

1. 系统不可用: 被病毒感染后崩溃
2. 系统被别人控制: 入侵或是感染木马病毒

软件:

- a) 自身的安全隐患被人利用来控制系统

- b) 自身具有木马功能被用来控制系统

措施:

- a) 正规渠道获取操作系统和常用软件
- b) 使用防火墙和防病毒软件
- c) 及时安装补丁程序

32. 账号和密码使用的注意事项有哪些?如何设置安全的密码?

1. 记在脑海里、只能自己知道、设置强密码
2. 设立不同等级的账号用于处理不同安全需求, 为不同安全等级的账号设置不同的密码, 不要一个密码通用所有账号

33. 密码设置要求: 应该不少于八个字符, 一定要让自己记住, 可以采用联想法

1. 最好不要用名字生日电话号码等设置密码
2. 建议密码同时包含多种类型的字符

34. 银行卡的分类方式有哪些?目前银行卡的载体主要有哪些?

1. 按结算币种不同: 人民币卡和外币卡
2. 按使用对象不同: 单位卡和个人卡
3. 按信息载体不同: 磁条卡和智能卡 (IC 卡)
4. 按流通范围不同: 国际卡和地区卡啊
5. 按清偿方式: 信用卡和借记卡
6. 载体: 磁条卡、芯片卡 (接触式, 非接触式)、虚拟卡

35. 为什么芯片卡的安全性要比磁条卡的安全性要高?

磁条卡:

磁条卡离身、被盗后可复制, 标准比较简单, 磁条生产和写入的技术门槛低

POS 机终端单向读取磁条信息, POS 的合法身份完全无法确认

芯片卡：

外部认证：卡片可以验证终端合法性

内部认证：POS 机终端可以验证卡片合法性

36. 网上银行的安全保障由哪些环节组成？

- a) 银行身份认证
- b) 客户身份认证
- c) 通信安全

37. 支付平台发挥了怎样的作用？常见的支付平台有哪些类型？

- a) 网关型支付平台
- b) 账户型支付平台
- c) 移动支付

38. 简要描述网上支付的交易流程。（PPT6 p74）

网上支付的交易流程

1. The customer opens an account
2. The customer receives a certificate
3. Merchants have their own certificates
4. The customer places an order
5. The merchant is verified
6. The order and payment information are sent
7. The merchant requests payment authorizations
8. The merchant confirms the order
9. The merchant provides the goods or service
10. The merchant requests payments

39. 账户型支付平台和网关型支付平台有什么差别？

前者有内部交易功能，后者无内部交易功能。

40. 扫码支付中，条码发挥了什么作用？

信息载体，以图形方式表示特定编码的数据信息

41. NFC手机支付和银行卡支付之间是什么关系？

NFC手机支付本质是银行卡交易