# 信息安全工程师考试考点明细

## 第1章：信息安全基础

### 考点1、信息安全概念

【考法分析】

本考点主要是对信息安全技术相关概念的考查。

【要点分析】

1．我国居民二代身份证正在使用256位的椭圆曲线新密码；国内外的许多电子商务系统正在使用1024位的RSA密码，与量子计算机类似，DNA计算机也是并行计算的，因此同样对现有密码构成严重的潜在威胁，目前可用于密码破译的量子计算算法主要有Grover算法和Shor算法。

2．在量子计算环境下，RSA，EIGamal，ECC公钥密码和DH密钥协商协议将不再安全；物理世界，人类社会和信息空间（Cyberspace）组成的三元世界。

3．信息空间突出了信息化的特征和核心内涵是信息，网络空间突出了网络互联的特征；网络空间安全的核心内涵仍是信息安全。没有信息安全，就没有网络空间安全。

4．信息安全的属性主要包含：

① 信息的保密性：信息不被未授权者知晓的属性；

② 信息的完整性：信息是正确的，真实的，未被篡改的，完整无缺的属性；

③ 信息的可用性：信息可以随时正常使用的属性。

5．能源，材料，信息是支撑现代社会大厦的三根支柱；信息系统安全可以划分为以下四个层次：设备安全，数据安全，内容安全，行为安全。其中数据安全即是传统的信息安全。

6．信息系统设备的安全是信息系统安全的首要问题；信息系统的设备安全是信息系统安全的物质基础，除了硬件设备外，软件系统也是一种设备。信息系统设备稳定可靠地工作是第一位的安全。

7．数据安全：采取措施确保数据免受未授权的泄露，篡改和毁坏；内容安全：信息安全在政治，法律，道德层次上的要求，还包括信息内容保密，知识产权保护，信息隐藏和隐私保护等诸多方面。行为安全：数据安全本质上是一种静态的安全，行为安全是一种动态安全。行为体现在过程和结果之中。程序的执行学列和相应的硬件动作构成了系统的行为，数据可以影响程序的执行走向。从而可以影响系统的行为。因此，信息系统的行为由硬件，软件和数据共同确定。所以，必须从硬件，软件和数据三方面来确保系统的行为安全。

8．网络空间安全学科是研究信息获取，信息存储，信息传输和信息处理领域中信息安全保障问题的一门新兴学科。

9．2015年6月，国务院学位委员会和教育部正式增设网络空间安全一级学科；网络空间安全学科的主要研究方向有：密码学，网络安全，信息系统安全，信息内容安全和信息对抗。

10．在这些众多的技术措施中，信息系统的硬件系统安全和操作系统安全是信息系统安全的基础，密码和网络安全等技术是关键技术。

11．密码学：由密码编码学和密码分析学组成；网络安全的基本思想是在网络的各个层次和范围内采取防护措施；信息系统安全的特点是从系统整体上考虑信息安全的威胁和防护；信息内容安全是信息安全在政治，法律，道德层次上的要求。也包括信息内容的保密，知识产权保护，信息隐藏，隐私保护等诸多方面。

12．信息对抗的实质是斗争双方利用电磁波和信息的作用来争夺电磁频谱和信息的有效使用和控制权。

13．数学是一切自然科学的理论基础，当然也是网络空间安全学科的理论基础；现代密码可以分为两类：基于数学的密码和基于非数学的密码；设计一个密码就是设计一个数学函数，而破译一个密码就是求解一个数学难题。

14．协议是网络的核心，因此协议安全是网络安全的核心。

15．博弈论便成为网络空间安全学科的理论基础之一；博弈论（Game Theory）是现代数学的一个分支；信息安全领域的斗争，本质上都是人与人之间的攻防斗争，因此博弈论便成为网络空间安全学科的理论基础之一，而且是网络空间安全学科所特有的理论基础。

16．信息论，控制论和系统论是现代科学的理论基础，因此也是网络空间安全学科的理论基础；信息论是商农为解决现代通信问题而创立的，控制论是维纳在解决自动控制技术问题中建立的，系统论是为了解决现代化大科学工程项目的组织管理问题而诞生的；信息论奠定了密码学的基础，信息论也奠定了信息隐藏的基础，因此，信息论构成了信息隐藏的理论基础；信息论的核心思想是整体观念。

17．控制论是研究机器，生命社会中控制和通信的一般规律的科学；控制的基础是信息。

18．保护，检测，响应（RDP）策略是确保信息系统和网络系统安全的基本策略；只有从信息系统的硬件和软件的低层做起，才能比较有效地确保信息系统的安全。

19．网络空间安全学科的许多问题是计算安全问题，因此计算理论也是网络空间安全学科的理论基础，其中包括可计算性理论和计算复杂性理论等；可计算理论是研究计算的一般性质的数学理论。它通过建立计算的数学模型，精确却分那些问题是可计算的，那些问题是不可计算的。

20．计算复杂性理论：研究现实的可计算性，如研究计算一个问题类需要多少时间，多少存储空间。

21．授权是信息系统访问控制的核心，信息系统是安全的，其授权系统必须是安全的；一般操作性的安全问题是1个不可判定问题，而具体的操作系统安全问题却是可判定问题。

22．本质上，密码破译就是求解一个数学难题，如果这个难题是理论不可计算的，则这个密码就是理论上安全的。

23．访问控制理论是网络空间安全学科所特有的理论基础；访问控制是信息系统安全的核心问题；访问控制理论包括各种访问控制模型与授权理论，例如，矩阵模型，BLP模型，BIBA模型，中国墙模型，基于角色的模型（RBAC），属性加密等，其中属性加密是密码技术与访问控制结合的新型访问控制；访问控制理论是网络空间安全学科的理论基础，而且是网络空间安全学科所特有的理论基础。

24．密码学理论是网络空间安全学科所特有的理论基础；数学，信息理论（信息论，系统论，控制论），计算理论（可计算理论，计算复杂性理论）是网络空间安全学科的理论基础，而博弈论，访问控制理论和密码学理论是网络空间安全学科所特有的理论基础。

25．笛卡尔方法分为4步：

① 永不接受任何我自己不清楚的真理。

② 将要研究的复杂问题，尽量分解为多个比较简单的小问题，一个一个地解决。

③ 将这些小问题从简单到复杂排序，先从容易解决的问题入手

④ 将所有问题解决后，再综合起来检验，看是否安全，是否将问题彻底解决了。

笛卡尔的方法论强调了把复杂问题分解成一些细小的问题分别解决，是一种分而治之的思想，是一种行之有效的方法；用整体的思想和方法来处理，由传统的方法论发展到系统性的方法论。

26．网络空间安全学科有自己的方法论，即包含分而治之的传统方法论，又包含综合治理的系统工程方法论，而且将这两者有机地融合为一体；网络空间安全学科具体概括为理论分析，逆向分析，实验验证，技术实现四个核心内容；必须强调指出的是，逆向分析是网络空间安全学科所特有的方法论。

27．网路空间安全学科的每一分支都具有攻和防两个方面：

① 在进行网络安全防护设计时，首先要进行安全威胁分析和风险评估；

② 认识系统的管理者和使用者，因此认识影响信息系统安全的重要因数。

以人为核心，运用定性分析和定量分析相结合，注意量变会引发质变，综合处理，追求整体效能，解决网络空间安全中的理论，技术和应用问题。

【备考点拨】

主要在上午题中涉及，了解并理解相关知识点内容。

### 考点2、信息安全法律法规

【考法分析】

本考点主要是对信息安全相关法律法规的考查。

【要点分析】

1．我国信息安全的法律体系可分为4个层面：

① 一般性法律规定；

② 规范和惩罚信息网络犯罪的法律；

③ 针对信息安全的特别规定；

④ 具体规范信息安全技术，信息安全管理等方面的法律法规。

2．计算机犯罪的明显特征：

① 隐秘性强；

② 高智能型；

③ 破坏性强；

④ 无传统犯罪现场；

⑤ 侦查和取证困难；

⑥ 公众对计算机犯罪认识不如传统犯罪清晰；

⑦ 计算机犯罪的诱惑性强：技术性强，富于挑战性；

⑧ 计算机犯罪经常是跨国犯罪。

3．计算机犯罪分为以下六类：

① 窃取和破坏计算机资产；

② 未经批准使用计算机信息系统资源；

③ 未批准或超越权限接受计算机服务；

④ 篡改或窃取计算机中保存的信息或文件；

⑤ 计算机信息系统装入欺骗性数据和记录；

⑥ 窃取或诈骗系统中的电子钱财。

4．互联网安全的刑事责任：

① 威胁互联网运行安全的行为；

② 威胁国家安全和社会稳定的行为；

③ 威胁社会主义市场经济秩序和社会管理秩序的行为；

④ 威胁个人，法人和其他组织的人身，财产等合法权利的行为。

5．网络安全问题日益凸显。一是，网络入侵，二是非法获取，三是，宣扬恐怖主义，极端主义，煽动颠覆国家政权，推翻社会主义制度，以及淫秽色情等违法信息。

6．网络运营者应履行下列安全保护义务：

① 制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

② 采取防范计算机病毒和网络攻击，网络入侵等危害网络安全行为的技术措施；

③ 采取记录，跟踪网络运行状态，监测，记录网络安全事件的技术措施，并按照规定留存网络日志；

④ 采取数据分类，重要数据备份和加密等措施；

⑤ 法律，行政法规规定的其他义务。

7．对关键信息基础设施，应实行重点保护；网络安全，是指通过采取必要措施，防范对网络的攻击，入侵，干扰，破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络存储，传输，处理信息的完整性，保密性可用性的能力。

8．中国计算机信息系统安全保护条例中计算机信息系统的概念，是指由计算机及其相关的和配套的设备，设施和网络构成的，按照一定的应用目标和规则对信息进行采集，加工，存储，传输，检索等处理的人机系统。

9．计算机病毒：是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

10．计算机信息系统安全专用产品：是指用于保护计算机i信息系统安全的专用硬件和软件产品；知识产权包括著作权（也称版权），工业产权（包括专利权和商标权），技术秘密和商业秘密。

11．2002年，国务院《计算机软件保护条例》正式施行。该条例称软件是指计算机程序及其有关文档。同一计算机程序的源程序和目标程序为同一作品。对软件著作权的保护不延及开发软件所用的思想，处理过程，操作方法或者数学概念等。

12．计算机软件受保护的条件有三个：原创性，可感知性，可再现性；计算机软件著作权人享有人身权和财产权。

### 考点3、信息安全管理基础

【考法分析】

本考点主要是对信息安全管理相关内容的考查。

【要点分析】

1．信息安全的定义：保护信息系统的硬件，软件及相关数据，使之不因为偶然或恶意的侵犯而遭受破坏，更改和泄露；保证信息系统中信息的机密性（Confidentiality），完整性（Integrity）和可用性（Availability）。

2．信息安全管理体系是信息安全管理活动的直结果，可表示为策略，原则，目标，方法，程序和资源等总的集合。

3．密码管理，密码除了用于信息加密外，也用于数据信息签名和安全认证。我国的商用密码管理原则：统一领导，集中管理，定点研制，专控经营，满足使用。

4．商用密码的应用领域十分广泛，主要用于对不涉及国家密秘码内容但又具有敏感性的内部信息，行政事物信息，经济信息等进行加密保护。

5．《商用密码管理条例》中所称商用密码，是指对不涉及国家密码内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。

6．商用密码技术是商用密码的核心，国家将商用密码技术列入国家秘密，任何单位和个人都有责任和义务保护商用密码技术的秘密。

7．国家密码管理局公布了无线局域网产品须使用的系列密码算法，包括：

① 对称密码算法：SMS4；

② 签名算法：ECDSA；

③ 密钥协商算法：ECDH；

④ 杂凑算法：SHA-256；

⑤ 随机数生成算法；自行选择。

其中ECDSA和ECDH密码算法须采用国家密码管理制定的椭圆曲线和参数；这是国内官方公布的第一个商用密码算法系列。

8．网络管理从功能上讲一般包括配置管理，性能管理，安全管理，故障管理等；网络管理最突出的特点是对网络组成成分管理的统一性和远程性。是以保证网络传输的性能和安全性为前提的。

9．网络管理体系结构包括以下四个方面：

协议：因为SNMP属于应用层

表示：适用面向对象式的表示方法

安全：管理者和被管理者之间要有认证和加密协议

对象：包括设备，各种协议，业务和交易过程

总体而言，网络管理的4个确定性特征是：统一化，智能化，安全化和主动化。

10．网络管理的几个主要开发方向：网管系统，应用性能管理，桌面管理，员工行为管理，安全管理。

11．网管系统：主要针对网络设备进行监测，配置和故障诊断；通用软件供应商开发的NMS系统试针对各个厂商网络设备的通用网管系统。

12．应用性能管理：

① 应用性能管理师一个比较新的网络管理方向，主要指对企业的关键业务应用进行监测，优化，提高企业应用的可靠性和质量，保证用户得到良好的服务，降低IT总拥有成本。

② 应用性能管理主要功能如下：监测企业关键应用性能；快速定位应用系统性能故障；优化系统性能。

13．桌面管理系统：由最终用户的电脑组成，这些电脑运行Windows，MAC系统。

14．员工行为管理：一部分是员工网上行为管理（EIM），另一部是员工桌面行为监测。

15．安全管理：保障合法用户对资源安全访问，防止病杜绝黑客蓄意攻击和破坏。

16．设备安全管理包括设备的选型，检测，安装，等级，使用，维护和存储管理等多方面的内容。

17．《信息安全等级保护管理办法》将信息系统的安全保护等级分为以下五级：

第一级：信息系统受到破坏后，会对公民，法人和其他组织的合法权益造成损害，但不损害国家安全，社会秩序和公共利益。

第二级：信息系统受到破坏后，会对公民，法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级：信息系统受到破坏后，会对国家安全造成特别严重损害。

《信息安全等级保护管理办法》明确规定，在信息系统建设过程中，运营，使用单位应当按照《计算机信息系统安全保护等级划分准则》。

18．GB17859-1999标准规定了计算机系统安全保护能力的五个等级：

第一级：用户自主保护级，通过隔离用户与数据，使用户具备自主安全保护的能力。

第二级：系统审计保护级，通过登录规程，审计安全性相关事件和隔离资源，使用户对自己的行为负责。

第三级：安全标记保护级，具有系统审计保护级所有功能，还提供有关安全策略模型，数据标记以及祖逖对客体强制性访问控制的非形式化描述，具有准确地标记输出信息的能力，消除通过测试发现的任何错误。

第四级：结构化保护级，要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。

第五级：访问验证保护级，满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。

19．涉密信息系统安全分级保护可以划分为秘密级，机密级和机密级（增强），绝密级三个等级：

① 秘密级：不低于国家信息安全等级保护三级的要求

② 机密级：不低于国家信息安全等级保护四级的要求

属于下列情况之一的机密级信息系统应选择机密级（增强）的要求：副省级以上的党政首脑机关，以及国防，外交，国家安全，军工等要害部门；机密级信息含量较高或数量较多；使用单位对信息系统的依赖程度较高。

③ 绝密级：信息系统中包含有最高为绝密级的国家秘密，不低于国家信息安安等级保护五级的要求。

20．涉密信息系统分级保护的管理过程分为八个阶段，即系统定级阶段，安全规划方案设计阶段，安全工程实施阶段，信息系统测评阶段，系统审批阶段，安全运行及维护阶段，定期评测与检查阶段和系统隐退终止阶段等。

21．涉密信息系统定级遵循“谁建设，谁定级”的原则。

22．目前国内外的趋势都是用网络隔离这个概念来代替物理隔离或安全隔离等；隔离技术的发展：

第一代隔离技术：完全地隔离

第二代隔离技术：硬件卡隔离

第三代隔离技术：数据传播隔离

第四代隔离技术：空气开关隔离

第五代隔离技术：安全通道隔离

23．防火墙是最常用的网络隔离手段；防火墙有一个很显著的缺点：就是防火墙只能做网络四层以下的控制，对于应用层内的病毒、蠕虫都没有办法。对于安全要求初级的隔离是可以的。

24．网闸的设计形象的借鉴了船闸的概念，设计采用“代理+摆渡”。不在河上架桥，可以设摆渡船，摆渡船不直接连接两岸，安全性当然要比桥好，即使是攻击，也不可能一下就进入，在船上总要收到管理者的各种控制。

25．网络隔离技术的安全要点：

① 要具有高度的自身安全性；

② 要确保网络之间是隔离的；

③ 要保证网间交换的只是应用数据；

④ 要对网闸的访问进行严格的控制和检查；

⑤ 要在坚持隔离的前提下保证网络畅通和应用透明。

网络隔离的关键是在于系统对通信数据的控制，即通过不可路由的协议来完成网闸的数据交换。

26．安全监控可以分为网络安全监控和主机安全监控两大类。

27．信息安全风险评估，则是指依据有关信息安全技术标准，对信息系统及由其处理，传输和存储的信息的保密性，完整性和可用性等安全属性进行科学评价的过程，它要评估信息系统的脆弱性，信息系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响，并根据安全事件发生的可能性和负面影响的程度来识别信息系统的安全风险；任何系统的安全性都可以通过风险的大小来衡量。

28．风险评估：指确定在计算机系统和网络中每一种资源缺失或遭到破坏对整个系统造成的预计损失数量。

29．风险评估的过程：

① 确定资产

② 脆弱性和威胁分析

③ 制定及评估控制措施

④ 决策

⑤ 沟通与交流

⑥ 监督实施

30．风险评估的方法：

① 典型的定量分析方法有因子分析法，聚类分析法，时序模型，回归模型，等风险图发，决策树法等

② 典型的定性分析方法有因素分析法，逻辑分析法，历史比较法，德尔菲法。

③ 定性与定量相结合的综合评估方法。

④ 典型的风险评估方法：层次分析法，它的基本步骤是：系统分解→构造判断矩阵→层次总排序。

31．风险管理就是以可以接受的费用识别，控制，降低或消除可能影响信息系统的安全风险的过程。

32．降低风险的途经：

① 避免风险

② 转移风险

③ 减少威胁

④ 减少脆弱性

⑤ 减少威胁可能的影响

⑥ 检测意外事件

风险接受是一个对残留风险进行确认和评价的过程。

### 考点4、信息安全标准化知识

【考法分析】

本考点主要是对信息安全标准化相关内容的考查。

【要点分析】

1．标准是人们以某种目的和需要而提出的统一性要求，是对一定范围内的重复性事物和概念所做的同意规定。

2．标准化则是制定标准并使其在社会一定范围内得到推广应用的一系列活动。

① 强制性标准：由法律规定必须遵照执行的标准。代号：GB

② 推荐性标准：非强制性标准，代号：GB/T

3．信安标委的成立标志着我国信息安全标准化工作步入了“统一领导，协调发展”的新时期。

4．信息安全管理的国际标准，主要可分为信息安全管理与控制类标准和技术与工程类标准；BS7799标准是英国标准协会（Birtishu Standards Institution,BSI）制定的信息安全管理体系标准。

5．《信息技术，安全技术，信息技术安全性评估准则》（简称CC）相当于最后的集大成者，是目前国际上最通行的信息技术产品及系统安全性评估准则，也是信息技术安全性评估结果国际互认的基础。

6．CC标准分为3个部分：

第1部分：简介和一般模型；

第2部分：安全功能要求；

第3部分：安全保证要求。

CC标准的核心思想有两点：一是信息安全技术提供的安全功能本身和对信息安全技术的保证承诺之间独立；二是安全工程的思想，即通过对信息安全产品的开发，评价，使用全过程的各个环节实施安全工程来确保产品的安全性。

7．2001年参照国际标准ISO/IEC15408,制定了国家标准GB/T18336《信息技术安全性评估准则》，作为评估信息技术产品与信息安全特性的基础准则。

【备考点拨】

主要在上午题中涉及，了解并理解相关知识点内容。

## 第2章：密码学基础与应用

### 考点1、密码学的基本概念

【考法分析】

本考点主要是对密码学基本概念的考查。

【要点分析】

1．研究密码编制的科学称为密码编制学(Cryptography)，研究密码破译的科学称为密码分析学(Cryptanalysis)，密码编制学和密码分析学共同组成密码学(Cryptology)。密码学作为信息安全的基础，其安全目标主要包括三个非常重要的方面：保密性（confidentiality）、完整性（integrity）和可用性（availability）。

① 保密性：确保信息仅被合法用户访问，而不被泄露给非授权的用户、实体或过程。

② 完整性：是指所有资源只能由授权方或以授权的方式进行修改，即信息未经授权不能进行改变的特性。

③ 可用性：是指所有资源在适当的时候可以由授权方访问，即信息可被授权实体访问并按需求使用的特性。

2．如果能够根据密文系统地确定出明文或密钥，或者能够根据明文—密文对系统地确定出密钥，则我们说这个密码是可破译的。密码分析者攻击密码的方法主要有以下三种。

① 穷举攻击：密码分析者采用依次试遍所有可能的密钥对所获密文进行解密，直至得到正确的明文。

② 统计分析攻击：就是指密码分析者通过分析密文和明文的统计规律来破译密码。

③ 数学分析攻击：是指密码分析者针对加密算法的数学依据通过数学求解的方法来破译密码。

3．根据密码分析者可利用的数据资源来分类，可将攻击密码的类型分为以下四种：

① 仅知密文攻击（Ciphertext-only attack）：是指密码分析者仅根据截获的密文来破译密码。

② 明文攻击（Known-plaintext attack）：是指密码分析者根据已经知道的某些明文-密文对来破译密码。

③ 选择明文攻击（Chosen-plaintext attack）：是指密码分析者能够选择明文并获得相应的密文。

④ 选择密文攻击（Chosen-ciphertext attack）：是指密码分析者能够选择密文并获得相应的明文。

一个密码，如果无论密码分析者截获了多少密文和用什么技术方法进行攻击都不能被攻破，则称为是绝对不可破译的。绝对不可破译的密码在理论上是存在的，这就是著名的“一次一密”密码。如果一个密码，不能被密码分析者根据可利用的资源所破译，则称为是计算上不可破译的。

4．置换密码：把明文中的字母重新排列，字母本身不变，但其位置改变了，这样编成的密码称为置换密码。

5．代替密码：构造一个或多个密文字母表，然后用密文字母表中的字母或字母组来代替明文字母或字母组，这样编成的密码称为代替密码。代替密码的目标就是加密文本，其思路非常简单：将字母表中的一个字符用另一个字符代替。

6．按代替所使用的密文字母表的个数可将代替密码分为单表代替密码、多表代替密码和多名代替密码。单表代替密码又称为简单代替密码。它只使用一个密文字母表，并且用密文字母表中的一个字母来代替一个明文字母表中的一个字母。典型的简单代替密码有加法密码、乘法密码、仿射密码等。

7．古典密码破译方法：

① 穷举分析：对于加法密码，密钥整数K只有n-1个不同的取值。对于明文字母表为英文字母表的情况，K只有25种可能的取值。即使是对于明文字母表为8位扩展ASCII码而言，K也只有255种可能的取值。因此，只要对K的可能取值逐一穷举就可破译加法密码。

② 统计分析：任何自然语言都有许多固有的统计特性。如果自然语言的这种统计特性在密文中有所反应，则密码分析者便可以通过分析明文和密文的统计规律而将密码破译。许多古典密码都可以用统计分析的方法破译。

【备考点拨】

了解并掌握相关知识点内容。

### 考点2、分组密码

【考法分析】

本考点主要是对分组密码算法的考查。

【要点分析】

1．根据明密文的划分和密钥的使用不同，可将密码体制分为分组密码和序列密码体制。

2．分组密码每一次加密一个明文块，而序列密码每一次加密一位或一个字符。分组密码和序列密码在计算机系统中都有广泛的应用。序列密码是要害部门使用的主流密码，而商用领域则多用分组密码。

3．理解DES算法P87表格。

4．S盒子的计算P90表2-8, 每个S有6位输入，有4位输出，会用8421的方法计算（91页前4行）。

5．DES的缺点P93页。

6．3DES的概念，长度168位（56\*3），如果是用2个密钥，长度112位（56\*2）P94页。

7．AES数据块的长度，密码的长度？P95页。

8．RIJNDAEL算法迭代圈数计算，已知Nk和Nb，求Nr，P96页。

9．乘法逆知识点，会求逆元：P97页。

10．SM4算法是一个分组算法，数据分组长度128比特，密钥长度128比特。加密算法与密钥扩展算法都采用32轮迭代结构，SM4密码算法是对合运算。

11．分组密码的工作模式：电子代码本模式、密码分组链接模式、输出反馈模式、密码反馈模式、CTR模式。了解其特点。P108-112页。

【备考点拨】

了解并掌握相关知识点内容。

### 考点3、序列密码

【考法分析】

本考点主要是对序列密码算法的考查。

【要点分析】

1．序列密码单独加密每个位。它是通过将密钥序列中的每个位与每个明文位相加实现的。

2．线性移位寄存器序列特点P115页。

3．RC4序列密码，了解安全性P117页。

4．ZUC算法采用哪三层结构设计P117页。

【备考点拨】

了解并掌握相关知识点内容。

### 考点4、Hash函数

【考法分析】

本考点主要是对Hash函数相关内容的考查。

【要点分析】

1．HASH函数应满足的性质。P119页。

2．SHA算法流程。P122页。

【备考点拨】

了解并掌握相关知识点内容。

### 考点5、公钥密码体制

【考法分析】

本考点主要是对公钥密码体制相关内容的考查。

【要点分析】

1．单向陷门函数概念。P131页。

2．RSA密码的计算及安全性。P134—P135页。

3．ELGamal密码体制：参数，加密算法，解密算法。P137页。

4．椭圆曲线密码的概念、安全性。P143页。

【备考点拨】

了解并掌握相关知识点内容。

### 考点6、数字签名

【考法分析】

本考点主要是对数字签名相关内容的考查。

【要点分析】

1．数字签名的基本模式。P146页。

2．数字签名的安全性。P146页。

3．基本的RSA签名体制算法的安全要素。P148页。

4．基本的ELGamal签名体制算法与安全性；不要随便给别人签名。P149页。

5．基本的ECC签名体制算法与安全性。

【备考点拨】

了解并掌握相关知识点内容。

### 考点7、认证

【考法分析】

本考点主要是对身份认证相关内容的考查。

【要点分析】

1．认证和加密的区别。P153页。

2．认证和数字签名的区别。P153页。

3．如何改进口令验证机制。P154页。

4．一个好的口令应当具备什么。P156页。

【备考点拨】

了解并掌握相关知识点内容。

### 考点8、密钥管理

【考法分析】

本考点主要是对密钥管理相关内容的考查。

【要点分析】

1．密钥的三级管理。P161页。

2．非对称密钥的生成。了解其特点。P165页。

3．公钥基础设施PKI包括的内容。P166页。

【备考点拨】

了解并掌握相关知识点内容。

## 第3章：网络安全基础

### 考点1、计算机网络基本知识

【考法分析】

本考点主要是对计算机网络基础技术的考查。

【要点分析】

1．网络协议：为进行网络中的数据交换而建立的规则、标准或约定就是网络协议(Protocol)。

2．计算机网络的体系结构：将计算机网络的各层及其协议的集合，称为计算机网络的体系结构( Architecture )。

3．几种典型的计算机网络体系结构：

① OSI/ISO 体系结构；

② TCP/IP 体系结构。

4．IP 地址：

① 概述：IP 地址的划分经过了三个阶段:分类的IP 地址:子网的划分:无分类编址(CIDR) 。

② 分类E 地址结构及类射

分类IP地址结构及类别：IP地址是由32 位二进制数，即4 个字节组成的，它与硬件没有任何关系，所以也称为逻辑地址。

5．Internet 路由协议

常见的内部网关协议：有RIP 协议和OSPF 协议；外部网关协议：有BGP 协议。

① 路由信息协议RIP：RIP 是一种分布式的基于距离向量的路由选择胁议，它位于应用层，考虑到和上下协议的相关性放在这里进行讨论。它允许一条路径最多只能包含15 个路由器。

② 开放最短路径优先协议OSPF（适用于大型网络）。

③ 外部网关协议BGP：BGP 是不同自治系统的路由器之间交换路由信息的协议。

④ 因特网组管理协议（IGMP）：IGMP 是在多播环境下使用的协议。

6．地址解析协议ARP 与反向地址解析协议RARP；网络中的一个机器具有逻辑地址和物理地址两种地址。逻辑地址是网络层的协议数据单元使用的地址，物理地址是数据链路层的协议数据单元MAC。

① ARP 协议：不知道物理地址那么就不能把网络层的数据包封装成MAC 帧，完不成通信。ARP 协议正是为了解决这个问题而设置的。

② RARP 协议：RARP 协议往往用于无盘工作站环境。

7．Internet 控制报文协议ICMP：ICMP协议允许路由器报告差错情况和提供有关异常情况的报告。

8．BGP 的结构和功能：BGP 用于在不同的自治系统(AS) 之间交换路由信息。

9．传输层协议TCP 协议特点：TCP 是面向连接的协议，提供可靠的、全双工的、面向字节流的，端到端的服务。

10．TCP 建立与释放连接机制：

① TCP 连接建立机制：TCP 使用三次握手来建立连接，大大增强了可靠性。

② TCP 连接释放机制：TCP 的释放分为半关闭和全关闭两个阶段。

11．TCP 定时管理机制：重传机制是保证TCP 可靠性的重要措施。TCP 每发送一个报文段，就对这个报文段设置一次计时器。只要计时器设置的重传时间到但还没有收到确认，就要重传这一报文段。

12．TCP 拥塞控制策略

TCP 的拥塞控制主要有以下四种方法:慢开始、拥塞避免、快重传和快恢复。

① 慢开始和拥塞避免：由小到大逐渐增大发送端的拥塞窗口数值，就是所谓的慢开始算法。

② 快重传和快恢复：快重传算法规定，发送端只要一连收到三个重复的ACK 即可断定有分组丢失了，就应立即重传丢失的报文段而不必继续等待为该报文段设置的重传计时器的超时。

13．UDP 协议的特点：发送数据之前不需要建立连接；UDP 的主机不需要维持复杂的连接状态表；UDP 用户数据报只有8 个字节的首部开销；网络出现的拥塞不会使源主机的发送速率降低，这对某些实时应用是很重要的。

14．域名系统DNS：功能是把Intemet 中的主机域名解析为对应的IP 地址。

15．电子邮件协议：邮件协议有发送协议SMTP 、接收协议POP3/IMAP4。

16．文件传输协议FTP的工作过程：FTP 是一个交互会话的系统，在进行文件传输时， FTP 的客户和服务器之间需要建立两个TCP 连接，一个控制连接，一个数据连接；FTP 的服务器进程由两大部分组成:一个主进程，负责接受新的请求:另外有若干个从属进程，负责处理单个请求。

17．远程登录协议Telnet：Telnet 有时也被称为虚拟终端协议。

18．动态主机配置协议DHCP：DHCP 是一种集中管理和自动分配IP地址的协议。

DHCP 支持三种类型的IP地址分配方式：

第一种人工分配，也称静态分配， DHCP为设备分配一个固定的IP 地址；

第二种动态分配，DHCP 从地址池中分配一个IP 地址给申请者，该地址有时间限制，在租约结束后收回；

第三种自动分配，从可用地址池中选择一个地址，自动地将其永久地分配给一台设备。

19．P2P (PeertoPeer) 应用协议：另一种模式应用模式叫点对点的应用，即 "peer-to-peer"，缩写为P2P 。这种模式不同于C/S 以服务器为中心，它没有客户机和服务器的区别，每个主机既是服务器也是客户机，既从其他主机获取资源，同时又为其他主机提供资源。

20．网络地址转换NAT：因特网的IP地址有本地地址和全球地址两类。但因特网中的所有路由器对目的地址是本地地址的数据报一律不进行转发。这就需要使用网络地址转换NAT，通常由路由器或专用NAT设备担任IP转换的功能。

【备考点拨】

了解并理解相关知识点内容。

### 考点2、网络安全的基本概念

【考法分析】

本考点主要是对网络安全相关内容的考查。

【要点分析】

1．网络安全法，涉及网络设备设施安全、网络运行安全、网络数据安全、网络信息安全等方面。

2．网络安全法有4大亮点：① 用户不实名禁提供服务；② 阻断违法信息传播；③ 重大事件时可限制网络；④ 出售公民个人信息最高10 倍违法所得罚款。

3．APT 攻击是一种以商业或者政治目的为前提的特定攻击；APT 攻击过程可概括为3 个阶段：攻击前准备阶段、攻击入侵阶段和持续攻击阶段。共分为5 个步骤：情报收集、防线突破、通道建立、横向渗透、信息收集及外传。

4．暗网(深网，不可见网，隐藏网)是指那些存储在网络数据库里、不能通过超链接访问而需要通过动态网页技术访问的资源集合，不属于那些可以被标准搜索引擎索引的表面网络。

5．网络其实有三层：① 表层网络：表层网就是人们所熟知的可见网络。② 深网：表层网之外的所有网络都称之为深网。③ 暗网：暗网是深网的一部分，但被人为地隐藏了起来。比特币成为暗网市场的主要流通货币。

【备考点拨】

了解并理解相关知识点内容。

### 考点3、网络安全威胁

【考法分析】

本考点主要是对网络安全防御技术相关内容的考查。

【要点分析】

1．网络安全是信息安全的核心。网络作为信息的主要收集、存储、分配、传输、应用的载体，其安全对整个信息的安全起着至关重要甚至是决定性的作用。

2、我国网络安全问题日益突出的主要标志是：

① 计算机系统遭受病毒感染和破坏的情况相当严重；

② 电脑黑客活动已形成重要威胁；

③ 信息基础设施面临网络安全的挑战；

④ 网络政治颠覆活动频繁。

3、制约提高我国网络安全防范能力的因素：

① 缺乏自主的计算机网络和软件核心技术；

② 安全意识淡薄是网络安全的瓶颈；

③ 运行管理机制的缺陷和不足制约了安全防范的力度；

④ 缺乏制度化的防范机制。

4．Sniffer 正当用处主要是分析网络的流量，由于Sniffer 可以捕获网络报文，因此它对网络也存在着极大的危害。

5．Sniffer 工作前提：① 网络必须是共享以太网；② 把本机上的网卡设置为混杂模式。

6．网络监听的防范方法：第一步工作就是要确保以太网的整体安全性；其次，采用加密技术；此外，对安全性要求比较高的公司可以考虑Kerberos（可信第三方认证机制）。

7．检测网络监听的手段：

① 反应时间；

② DNS 测试；

③ 利用ping 进行监测；

④ 利用ARP 数据包进行监测。

8．口令攻击类型：

① 字典攻击；② 强行攻击；③ 组合攻击。

口令破解器是一个程序，它能将口令解译出来，或者让口令保护失效。口令破解器一般并不是真正地去解码，因为事实上很多加密算法是不可逆的。

9．Email 口令破解：

① 利用邮件服务器操作系统的漏洞；

② 利用邮件服务器软件本身的漏洞；

③ 在邮件的传输过程中窃听。

10．拒绝服务攻击的主要企图是借助于两络系统或网络协议的缺陷和配置漏洞进行网络攻击，使网络拥塞、系统资源耗尽或者系统应用死锁，妨碍目标主机和网络系统对正常用户服务请求的及时响应，造成服务的性能受损甚至导致服务中断。

11．拒绝服务攻击DoS （DenialofService) 是阻止或拒绝合法使用者存取网络服务器（一般为Web 、FTP 或邮件服务器)的一种破坏性攻击方式。

12．拒绝服务攻击类型：

① 消耗资源；

② 破坏或更改配置信息；

③ 物理破坏或改变网络部件；

④ 利用服务程序中的处理错误便服务失效。

13．服务端口攻击：

① 同步包凤暴C SYNFlooding)：它是通过创建大量"半连接"来进行攻击。

② Smurf 攻击：这种攻击方法结合使用了IP 欺骗和ICMP 回复方法使大量网络数据充斥目标系统，引起目标系统拒绝为正常请求进行服务。

③ 利用处理程序错误的拒绝服务攻击：这种攻击方法主要是利用TCP/IP 协议实现中的处理程序错误实施拒绝服务攻击。包括PingofDeath 攻击、 Teardrop 攻击、Winnuke 攻击和Land 攻击等。

14．电子邮件轰炸：电子邮件轰炸是最早的一种拒绝服务攻击。电子邮件轰炸实质上也是一种针对服务端口(SMTP 端口，即25 端口)的攻击方式，它的原理是:连接到邮件服务器的SMTP (25) 端口，按照SMTP 协议发送几仔头信息加上一堆文字垃圾，就算只发送了一封邮件，反复多次，就形成了邮件炸弹。

15．分布式拒绝服务攻击DDoS：攻击者首先侵入并控制一些计算机，然后控制这些计算机同时向一个特定的目标发起拒绝服务攻击。

16．漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

17．缓冲区溢出攻击是一种通过往程序的缓冲区写超出其长度的内容，造成缓冲区溢出，从雨破坏程序的堆枝，使程序转而执行其他预设指令，以达到攻击目的的攻击方法。

18．僵尸网络(Botnet) 是指采用一种或多种传播手段，将大量主机感染bot 程序(僵尸程序)，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。Botnet 首先是一个可控制的网络，这个网络并不是指物理意义上具有拓扑结构的网络，它具有一定的分布性，随着bot 程序的不断传播雨不断有新位置的僵尸计算机添加到这个网络中来。

19．僵尸网络的防御方法：基于IRC 协议的BotNet 防御方法，主要有使用蜜网技术、网络流量研究以及IRCserver 识别技术。

① 使用蜜网技术：蜜罐技术是一种欺骗入侵者以达到采集黑客攻击方法和保护真实主机目标的诱骗技术。

② 网络流量研究：网络流量的研究是通过分析BotNet 中僵尸主机的行为特征，将僵尸主机划分为长期发呆型和快速加入型。

20．网络钓鱼是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息的一种攻击方式。

21．网络钓鱼防范措施：

① 申请并安装数字证书；

② 规范使用操作。

22．ARP 原理:某机器A 要向主机C 发送报文，会查询本地的ARP 缓存表，找到C 的IP 地址对应的MAC 地址后，就会进行数据传输。

23．ARP 欺骗的防范措施：

① 在wmxp 下输入命令: arp-s 网关IP 网关mac 固化arp表， 阻止arp欺骗。

② 使用ARP服务器。通过该服务器查找自己的ARP 转换表来响应其他机器的ARP广播。确保这台ARP 服务器不被黑。

③ 采用双向绑定的方法解决并且防止ARP 欺骗。

④ ARP 防护软件（ARPGuardo）

24．DNS 欺骗原理：首先是冒充域名服务器，然后把查询的IP 地址设为攻击者的IP 地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了，这就是DNS 欺骗的基本原理。

25．IP 欺骗的原理：通过编程的方法可以随意改变发出的包的IP 地址，但工作在传输层的TCP 协议是一种相对可靠的协议，不会让黑客轻易得逞。由于TCP 是面向连接的协议，所以在双方正式传输数据之前，需要用"三次握手"来建立一个值得信赖的连接。

26．IP 欺骗的防范：预防这种攻击可以删除UNIX 中所有的/etc/hosts.equiv 、$HOME!.rhosts 文件，修改/etc/inetd.conf 文件，使得RPC机制无法应用。另外，还可以通过设置防火墙过滤来自外部而信源地址却是内部目的报文。

27．Web 欺骗的原理：Web 欺骗的原理是攻击者通过伪造某个www 站点的影像拷贝，使该影像Web 的入口进入到攻击者的Web 服务器，并经过攻击者机器的过滤作用，从而达到攻击者监控受攻击者的任何活动以获取有用信息的目的，这些信息当然包括用户的账户和口令。

28．Web 欺骗的手段和方法：

① 改写URL；

② 特殊的网页假象。

29．Email 欺骗：电子邮件欺骗是在电子邮件中改变名字使之看起来是从某地或某人发来的实际行为。

30．电子邮件欺骗有三种基本方法：

① 相似的电子邮件地址；

② 修改邮件客户；

③ 远程联系，登录到端口25。

31．网站安全威胁：

① SQL注入攻击；

② 跨站攻击；

③ 旁注攻击。

32．旁注攻击，有两种抵御方法:

① 设置IIS 单用户权限/禁止，来阻止非法用户运仔任意的CMD 命令，从而使入侵者的旁注入侵在无法提升权限下导致失败；

② 利用端口转发技术。

33．社会工程学就是使人们眼从你的意愿、满足你的欲望的一门艺术与学问。社会工程学运用是否能成功也有取决于目标个体与你的目的有多大关联的因素的。

34．WEB安全漏洞：

① 加密算法中存在的漏洞

② 密钥管理中存在的漏洞

③ 身份认证机制中存在的漏洞

35．OpenSSL 安全漏洞：

① 计时攻击缺陷；② 分支预测缺陷；③ 故障分析缺陷；④ 单/双字节偏差缺陷；⑤ 伪随机数生成器缺陷；⑥ PaddingOracle 缺陷；⑦ Heartbleed 缺陷；⑧ 中间人攻击缺陷；⑨ 拒绝服务缺陷。

【备考点拨】

了解并理解相关知识点内容。

### 考点4、网络安全防御

【考法分析】

本考点主要是对网络安全防御相关内容的考查。

【要点分析】

1．防火墙主要是实现网络安全的安全策略，而这种策略是预先定义好的，所以是一种静态安全技术。

2．大多数防火墙规则中的处理方式主要包括以下几种：

Accept: 允许数据包或信息通过。

Reject: 拒绝数据包或信息通过，并且通知信息源该信息被禁止。

Drop: 直接将数据包或信息丢弃，并且不通知信息源。

缺省规则有两种选择:默认拒绝或者默认允许。

3．TCP/IP 协议族具有明显的层次特性，由物理接口层、网络层、传输层、应用层四层协议构成，每个层次的作用都不相同，防火墙产品在不同层次上实现信息过滤与控制所采用的策略也不相同。

4．包过滤技术的优点是简单，处理速度也很快。包过滤技术可能存在的攻击有:

① IP 地址欺骗；

② 源路由攻击；

③ 微分片攻击。

5．应用层网关也叫做代理服务器。它在应用层的通信中扮演着一个消息传递者的角色。

第三种防火墙技术是电路层网关。它是负责数据转发的独立系统，类似于网络渡船。电路层网关不允许一个端到端的直接的TCP 连接，它自网关建立两个TCP 连接，一个连接网关与网络内部的TCP 用户，一个连接网关与网络外部的TCP 用户。

6．防火墙的经典体系结构主要有三种形式：双重宿主主机体系结构、被屏蔽主机体系结构和被屏蔽子网体系结构。

7．入侵检测与防护的技术主要有两种:入侵检测系统(IntrusionDetectionSystem ， IDS)和入侵防护系统(IntrusionPreventionSystem ， IPS) ；入侵检测技术主要分成两大类：异常入侵检测和误用入侵检测；入侵检测系统的体系结构大致可以分为基于主机型(Host-Based) 、基于网络型(Network-Based) 和基于主体型(Agent-Based) 三种。

8．VPN 即虚拟专用网，它是依靠ISP和其他NSP，在公用网络中建立专用的、安全的数据通信通道的技术。VPN 可以认为是加密和认证技术在网络传输中的应用。

9．VPN 的数据加密技术：隧道技术、加解密技术、密钥管理技术、身份认证技术等。

10．隧道协议：三种最常见的也是最为广泛实现的隧道技术是:点对点隧道协议PPTP，第2 层隧道协议L2TP, IP安全协议（IPSec )。除了这三种技术以外还有通用路由封装GRE、L2F 以及SOCK 协议等。

① 点对点隧道协议CPPTP)；

② 第2层隧道悔议(L2TP)；

③ IP 安全协议(IPSec)。

11．扫描器是一种自动检测远程或本地主机、网络系统安全性弱点的程序。漏洞是在暖件、软件、协议的具体实现或系统安全策略上存在的缺陷。

12．端口扫描：互联网上通信的双方不仅需要知道对方的地址，也需要知道通信程序的端口号。

13．密码类探测扫描技术(即口令攻击)是黑客进行网络攻击时最常用、最基本的一种形式。

14．我国也提出了自己的动态安全模型——WPDRRC 模型★。该模型有6 个环节和3 大要素。6 个环节是W、P 、D 、R、R、C ，它们具有动态反馈关系。其中， p, D 、R、R与PDRR 模型中出现的保护、检测、反应、恢复等4 个环节相同;W 即预警(waming) ，就是根据己掌握的系统脆弱性以及当前的计算机犯罪趋势，去预测未来可能受到的攻击与危害C (counterattack) 则是反击一一一采用一切可能的高新技术手段，侦察、提取计算机犯罪分子的作案线索与犯罪证据，形成强有力的取证能力和依法打击手段。

15．WPDRRC 模型中具有层次关系的三大要素分别是人员、政策和技术。

16．风险分析中要涉及资产、威胁、脆弱性等基本要素。每个要素有各自的属性。资产的属性是资产价值:威胁的属性是威胁出现的频率;脆弱性的属性是资产弱点的严重程度。最终，计算出-个量化的风险值。

17．SSL 协议以对称密码技术和公开密码技术相结合，提供了如下三种基本安全服务:

① 秘密性SSL：协议能够在客户端和服务器之间建立起一个安全通道，所有消息都经过加密处理以后进行传输，网络中的非法黑客无法窃取。

② 完整性SSL：利用密码算法和散列(HASH) 函数，通过对传输信息特征值的提取来保证信息的完整性，确保要传输的信息全部到达目的地，可以避免服务器和客户端之间的信息受到破坏。

③ 认证性：利用证书技术和可信的第三方认证，可以让客户端和服务器相互识别对方的身份。

SSL 协议位于应用层和传输层之间，独立于应用层协议，即建立在SSL 之上的应用层协议可以透明地传输数据。

18．PGP 可以在电子邮件和文件储存应用中提供保密和认证服务，防止非授权者阅读，还能对邮件和文件加上数字签名，从而使收件人确信发送者是谁。

19．IEEE802.1x 是IEEE (美国电气电子工程师学会) 802 委员会制定的LAN标准中的一个，是一种应用于LAN 交换机和无线LAN 接入点的用户认证技术。

20．WEP 协议原理：WEP 基于RC4 算法用相同的密钥加密和解密，用开放系统认证和共享密钥认证进行认证。

21．WEP 是数据加密算法，它不是一个用户认证机制。

22．ADIUS 协议是一种提供在网络接入服务器和共享认证服务器间传送认证、授权和配置信息等服务的褂议。

23．Kerberos 是一种应用于分布式网络环境、以对称密码体制为基础，对用户及网络连接进行认证的增强网络安全的服务。★

24．X.509 是由国际电信联盟CITU-T) 制定的数字证书标准；X. 509 是基于公钥密码体制和数字签名的服务；X.509 给出的鉴别框架是一种基于公开密钥体制的鉴别业务密钥管理。

25．SSH (SecureShell) 协议是在传输层与应用层之间的加密隧道应用协议，它从几个不同的方面来加强通信的完整性和安全性。

26．蜜罐(Honeypot) 技术是)种主动助御技术，是入侵检测技术的一个重要发展方向。

蜜罐的优点有：① 使用简单；② 资源占用少；③ 数据价值高。

蜜罐的缺点有: ① 数据收集面狭窄；② 给使用者带来风险。

27．蜜罐有四种不同的配置方式：

① 诱骗服务（DeceptionService)；② 弱化系统（WeakenedSystem)；③ 强化系统（HardenedSystem)；④ 用户模式服务器（UserModeServer)。

28．用于备份的设备有硬盘、光盘、磁带三种；备份方式有三种：完全备份、增量备份、差异备份。完全备份就是对服务器上的所有文件完全进行归档；增量备份是指只把最近新生成的或者新修改的文件拷贝到备份设备上；差异备份与增量备份很相似。两者所不同的是，差异备份对上次备份后所有发生改变的文件都进行备份(包括删除文件的信息)，并且不是从上次备份的时间开始计算。

29．NAS （NetworkAttachedStorage) 通常译为"网络附加存储"或"网络连接存储"。意思是连接在网络上的存储设备。SAN （StorageAreaN etwork) 通常译为"存储区域网络"。它是使用光纤通道。

30．网络安全防范意识与策略：

① 保证通信安全：对链路、信息进行加密，实行访问控制。

② 保证信息安全：采取技术、管理等措施，保护信息，使信息的保密性、完整性和可用性得到保障。

31．加强安全保障：加强信息安全保障措施，协同加强信息安全。主要包括三个方面的措施：

①检测：对系统的脆弱性、外部入侵、内部入侵、滥用、误用进行检测，及时发现、修补漏洞。

② 响应：对各种安全事件及时晌应，把不安全因素消灭在萌芽状态。

③恢复：制定完整的恢复计划，使得在网络万一不能提供服务时，能够及时、完整地恢复。

32．局域网的安全风险主要有以下4个方面：

① 计算机病毒的破坏；② 恶意攻击；③ 人为失误；④ 软件本身的漏洞。

33．局域网的安全防范策略有：

① 物理安全策略；② 划分VLAN 防止网络侦听；③ 网络分段；④ 以交换机代替共享式集线器；⑤ 访问控制策略；⑥ 使用数字签名；⑦ 用户管理策略；⑧ 使用代理服务器；⑨ 防火墙控制；⑩ 入侵检测系统；⑪ 定期进行漏洞安全扫描；⑫ 建立完善的网络安全应急响应机制；⑬ 使用VPN。

【备考点拨】

了解并理解相关知识点内容。

### 考点5、无线网络安全

【考法分析】

本考点主要是对无线网络安全相关内容的考查。

【要点分析】

1．无线网络大体可分为无线广域网、无线城域网、无线局域网、无线个域网和无线体域网。

2．无线广域网（WWAN）：主要通过通信卫星把物理距离极为分散的局域网（LocalAreaNetwork ， LAN) 连接起来，它连接地理范围较大，常常是一个国家或是一个洲。

3．无线城域网(WirelessMetropolitanAreaNetwork ，WMAN)：主要通过移动电话或车载装置进行移动数据通信，可覆盖城市中的大部分地区。

4．无线局域网(WirelessLocalAreaNetwork, WLAN)：覆盖范围较小。

5．无线个域网C WirelessPersonalAreaNetwork, WPAN)：通常指近距离范围内的设备建立无线连接，WPAN 能够有效地解决"最后的几米电缆"的问题，进而将无线联网进行到底。

6．根据网络拓扑结构的不同，无线网络可分为集中式无线网络、分散式无线网络和分布式无线网络。

7．无线网络安全威胁：

① 无线窃听；② 假冒攻击；③ 信息篡改；④ 服务后抵赖；⑤ 重传攻击；⑥ 认证及密钙的攻击类型；⑦ 无线传感器网络节点劫持Sybil 攻击；⑧ 无线传感器网络虫涧攻击；⑨ 2G 伪基站攻击"伪基站"即假基站；⑩ NFC (NearFieldCommunication，近距离无线通信技术)面临特殊威胁攻击；⑪ RFID（RadioFrequencyIdentification ，射频识别) 面临特殊威胁攻击。

8．无线网络安全方案设计策略一般原则如下：

① 分析对系统的假设和约定。

② 分析网络的体系结构，明确网络的拓扑结构(星形、网状、分层树状、单跳还是多跳网络、拓扑结构是否变化、节点是否移动、节点移动的速度范围)、通信类型(单播、组播、广播等)、链路特征参数(带宽、吞吐率、延迟)、网络如模(节点数量、阿络覆盖面积〉、业务数据类型(语音、数据、多媒体、控制指令)等，~及网络的异拘性(多种形态网络的融合，有线网络和无线网络的融合)，网络的时效性(是临时存在的还是长期存在的)。它和上一条一起构成了设计安全方案时的客观约束条件。

③ 分析网络的业务构成(工作流程、操作过程)，涉及的实体(角色)、业务通信的基本内容等，思考这些实体和通信内容可能面临的安全威胁。

④ 分析网络和系统中的信任模型，明确方案涉及的相关实体和通信链路的信任程度，即追信链路或者实体是可信、半可信还是不可信的，思考并确定安全的边界.

⑤ 分析攻击网络和系统的敌手模型:

⑥ 从存在的威胁中归纳出共性的安全需求。

⑦ 根据前面步骤中归纳的安全需求、网络体系结构、系统假设确定设计需要达到的安全目标，以及实现该目标时要满足的特性，例如安全算法需要满足的计算量上限，存储空间上限，安全方案对容侵、容错的健壮性等。

针对以上原则，在设计无线网络安全方案时应综合采用以下策略:

① 安全策略(移动终端)；

② 效率策略；

③ 兼容性。

9．WPKI 即"无线公开密钥体系"它是将互联网电子商务中PKI安全机制引入到无线网络环境中的一套遵循既定标准的密钥及证书管理平台体系，用它来管理在移动向络环境中使用的公开密铝和数字证书，有效建立安全和值得信赖的无线网络环境。

10．使用RC4(RivestCipher) 串流加密技术达到机密性，并使用CRC-32 验和达到资料正确性。

11．Wi-Fi 网络安全接入(WPA/WPA2)：是一种保护无线电脑网络（Wi-FD） 安全的系统，它是应研究者在前一代的系统有线等效加密（WEP) 中找到的几个严重的弱点而产生的。

12．无线局域网鉴别与保密体系(WAPI)：无线局域网鉴别和保密体系WAPD ，是一种安全协议，同时也是中国无线局域网安全强制性标准。

13．802.11i：IEEE802.11 i 是802.11 工作组为新一代WLAN 制定的安全标准，主要包括加密技术:TKlP、AES 以及认证协议IEEE802.1x 。

14．移动通信系统安全：2G 伪基站攻击防御:改善GSM 网络安全可以从以下几个方面进行：

① 调整基站参数，在不改变GSM 网络鉴权协议的'情况下，各大移动运营高可以通过谓整各基站小区的参数来遏制伪基站的危害。

② 定位伪基站，目前伪基站经常被不法分子用来向移动用户群发垃圾短消息，这给用户带来很大的匾扰。

③ 运营商可以和公安机关等执法部门配合，加强对伪基站的查找和处罚力度，从行政和执法上加强对网络的保护。

15．无线传感器网络安全：

① 密钥管理、身份认证和数据加密：公开密钥加密由于加密安全性高、网络抗毁性强等优点，被广泛应用于传统网络。但是传感器网络资源(包括节点自身能量、存储容量、计算和通信能力等)严格受限的；对称密钥加密算法由于加密处理简单，加解密速度'快，密钥较短等特点，非常适合资源受限的传感器网络部署使用。

② 攻击检测与抵御：无线传感器网络容易受到各种恶意攻击，例如干扰服务、节点捕获等。

16．无线个域网安全：

① 蓝牙安全：蓝牙技术提供短距离的对等通信，它在应用层和链路层上都采取了保密措施以保证通信的安全性，所有蓝牙设备都采用相同的认证和加密方式。

② Zigbee 安全：ZigBee 是基于IEEE802.15 .4标准的低功耗局域网协议。根据国际标准规定， ZigBee技术是一种短距离、低功耗的无线通信技术。

③ NFC 安全：从NFC 芯片、安全单元、手机应用等方面来阐述相关安全对策。

④ RFID 安全：

针对RFID 设备的破坏和攻击。可以考虑使用"法拉第笼月使得攻击者对于RFID的标签信息主动欺骗攻击失效。

Hash-Lock 协议及一系列改进方法，核心思想是使用metaID 来代替真实的标签ID以避免信息泄露和被追踪。

【备考点拨】

了解并理解相关知识点内容。

## 第4章：信息系统安全基础

### 考点1、计算机设备安全

【考法分析】

本考点主要是对计算机设备安全的考查。

【要点分析】

1．一般认为，计算机安全的定义，要包括计算机试题及其信息的完整性，机密性，抗否认性，可用性，可审计性，可靠性等几个关键因数；

机密性：保证信息部被非授权访问；

完整性：维护信息和试题的人为或非人为的非授权篡改；

抗否认性：指保障用户无法再时候否认曾经对信息进行的生成，签发，接受等行为；

可用性：授权用户根据需要可以随时访问所需信息；

可审计性：保证计算机信息系统所处理的信息的完整性，准确性和可靠性，防止有意或无意地出现错误，乃至防止和发现计算机犯罪案件，除了采用其他安全措施之外，利用对计算机信息系统的审计的方法。利用审计跟踪的工具，可以记录用户的活动；审计跟踪可以监控和扑捉各种安全事件；审计跟踪的另一个主要功能是保存，维护和管理审计日志。

可靠性：指计算机在规定的条件下和给定的时间内完成预定功能的概率；所谓“失效率”是指计算机在某一瞬间失效元件数与元件总数的比率。

影响计算机可靠性的因数有内因和外因两个方面：

内因：机器本身的因数

外因：指环境条件对系统可靠性，稳定性和维护水平的影响

一般认为，在系统的可靠性工程中，元器件是基础，设计是关键，环境是保证。除了保证系统的正常工作条件及正确使用和维护外，还要采取容错技术和故障诊断技术。

容错技术：指用增加冗余资源的方法来掩盖故障造成的影响；故障诊断技术：通过检测和排除系统元器件或线路故障。

2．由于计算机系统本身的脆弱性以及硬件和软件的开放性，加之缺乏完善的安全措施，容易给犯罪分子以可乘之机。

3．计算机系统安全涉及到许多学科，因此它是一个综合性很强的问题。要想解决和计算机系统的安全，就必须首先从计算机的系统结构和基础出发，从计算机硬件环境出发，找到一条合理地解决问题的道路。

4．计算机系统安全是指：为了保证计算机信息系统安全可靠运行，确保计算机信息系统在对信息进行采集，处理，传输，存储过程中，不致收到人为（包括未授权使用计算机资源的人）或自然因数的危害，而使信息丢失，泄露或破坏，对计算机设备，设施（包括机房建筑，供电，空调等），环境人员等采取适当的安全措施。

5．对系统安全的研究大致可以分为基础理论研究，应用技术研究，安全管理研究等。基础理论研究：包括密码研究，安全理论研究；密码理论的研究重点是算法；安全理论的研究重点是单机环境，网络环境下信息防护的基本理论；应用技术研究包括安全实现技术，安全平台技术研究；安全技术的研究重点实在单机或网络环境下信息防护的应用技术；平台安全是指保障承载信息产生，存储，传输和处理的平台的安全和可控；安全管理研究包括安全标准，安全策略，安全测评等。

6．计算机系统外部设备在工作时能够通过地线，电源线，信号线，寄生电磁信号或谐波将游泳信息辐射的过程，叫计算机的电磁泄露。

7．计算机及其外部设备内的信息，可以通过两种途径泄露：一种是以电磁波的形式辐射，称为辐射泄露；另一种是通过各种线路和金属管道传导出去，称为传导泄露。

8．一般而言，传导泄露还伴随着辐射泄露。影响计算机电磁辐射强度的主要因素有：

① 功率和频率；

② 与辐射源的距离；

③ 屏蔽状况。

9．TEMPEST的电磁泄露是客观存在的。任何处于工作状态的电磁信息设备都存在不同程度的电磁泄露现象。TEMPEST泄露发射通过辐射和传导两种途径向外传播。

10．在实际中常用的电磁防护措施有：屏蔽，滤波，隔离，合理的接地与良好的搭接，选用低泄露设备，合理的布局和使用干扰器，传输信息加密等。

11．电磁泄露的解决方法有以下几种：

① 低辐射产品；

② 电磁干扰器；

③ 处理涉密信息的电磁屏蔽室的技术；

④ TEMPEST屏蔽室单纯使用屏蔽法，结合滤波的手段其中屏蔽室的门屏蔽性能抗老化是关键。

12．其他的防泄露技术：

① 滤波是抑制传导泄露的主要方法之一；

② 接地和搭接也是抑制传导泄露的有效方法；

③ 隔离和合理布局均为降低电磁泄露的有效手段；

④ 选用低泄露设别也是降低电磁泄露的有效手段之一；

⑤ 配置低辐射设备。

13．物理安全主要包括三个方面：① 场地安全（环境安全）；② 设备安全；（媒体安全）

14．计算机机房的安全等级分为A类，B类，C类三个基本来别：

① A级机房：对计算机机房的安全有杨哥的要求；

② C级机房：对计算机机房的安全有基本的要求。

15．同一机房也可以对不同的设备（如电源，主机）设置不同的级别；为了保证计算机中心有效地开展信息处理工作，基本工作房间和维修室，仪器室，备品室，磁介质存放室，人员工作室等房间所占面积的总和应不小于计算机机房面积的1.5倍，而且还应考虑到计算机信息系统设备的扩充。通常计算机机房的面积还应留有15%~30%的富裕空间。

16．机房的安全可以从以下几个方面来考虑：

① 供配电系统；② 防雷接地系统；③ 消防报警及自动灭火器系统功能；④ 门禁系统；⑤ 保安监控系统。

17．引起场地安全的自然原因的威胁有如下几种：

① 场地湿度对计算机设别所使用电子元器件，绝缘材料，金属构件以及记录介质等都将产生一定的影响；

② 场地湿度对计算机信息系统的影响；

③ 灰尘对计算机信息系统安全的影响；

④ 有害气体对计算机信息系统安全的影响；

⑤ 地震对计算机信息系统安全的影响。

18．引起场地安全的还有人为原因，其主要威胁有如下几种：

① 火灾；② 防水；③ 电源；④ 防物理，化学和生物灾害。

19．设备安全：包括设备的防盗和防毁，防止电磁信息泄露，防止线路截获，抗电磁干扰一级电源的保护。

20．工业电气设备产生的干扰，是计算机电磁干扰的主要来源。这种干扰源暗器干扰性质可分为：工频干扰，开关干扰，放点干扰和射频干扰。

21．计算机信息系统设备的可靠运行提供能源保障，可归纳为两个方面：对工作电源的工作连续性的保护（如使用不间断电源）和对工作电源的工作稳定的保护。

22．目前应用的UPS电源是一种比较理想的供电设备。介质安全是指介质数据和介质本身的安全。

23．计算机的可靠性工作，一般采用容错系统实现。容错主要依靠冗余设计来实现。

24．由于资源的不同，冗余技术分为硬件冗余，软件冗余，时间冗余和信息冗余。

25．容错系统工作方式分为：① 自动侦测；② 自动切换；③ 自动恢复。

26．容错是指一个系统在运行中其任何一个子系统发生故障时，系统仍然能够继续操作的能力。容错系统的实现应该遵守下列3个设计策略：① 冗余性：提供备份子系统；② 预防性；③ 恢复性。

27．具体的冗余技术可以分为如下的4种：① 硬件冗余；② 堆积冗余；③ 待命储备冗余：该系统中多个模块，其中只有一块处于工作状态；④ 混合冗余：堆积冗余和代码储备容易的结合。

28．计算机系统的硬件容错技术主要采取两个措施：一是每块模板上装有两套相同的逻辑处理部件，二是每一种模块都一式两份。

29．硬件容错具体的应用技术：

① 双CPU容错系统；② 双机热备份；③ 三机表决系统：三台主机同时运行，由表决器（Voter）根据三台机器的运行结果进行表决，有两个以上的机器运行结果相同，则认为该结果为正确。通常可靠性比双机系统要高，成本也高。④ 集群系统（Clusting）：指均衡负载的双机或多级系统。

30．软件容错本身有两层含义：一是对软件自身故障的处理；二是使用软件对系统中出现的其他故障进行处理。

31．研究表明，对于软件本身的设计故障，简单的冗余是不够的，需要辅以设计和数据表示的多样性才能达到较好的容错效果。

32．设计多样性（Design Diversity）技术的核心思想：完成某个功能有多种可能的不同方法，现将每种可能的方法都实现（每种实现称为一个变体），以尽可能保证至少有一个变体能可靠地运行。

33．设计多样性主要有三种经典的实现：

① 恢复块（Recoery Blocks，RcB）：通过建立还原点并使用可接受测试和后向恢复实现容错；

② N版本程序设计（N2Version progaramming,NVP）:使用多个不同的软件版本利用决策机制和前向恢复实现容错；

③ N自检程序设计（N Self Checking Programming，NSCP） ：利用程序冗余在执行过程中检测自身的行为。

34．数据容错的策略就是数据备份和恢复策略，以及容灾技术，数据纠错等技术。

35．数据备份通常可以分为完全备份，增量备份，差分备份和渐进式备份

完全备份（Fullbackup）：指将系统中所有选择的数据对象进行一次全面的备份。是最基本也是最简单的备份方式；

增量备份：只对上次备份后系统中变化过的数据对象的备份；

差分备份：只对上次完全备份i来系统中所偶变化过的数据对象的备份；

渐进式备份：也称为“只有增量备份”或“连续增量备份”；它是指系统排出完全备份，数据对象只有当放生改变时才被写入到存储介质上；渐进式备份只在初始时做所有数据文件的全部备份，以后只备份新建或改动过的文件，比上述三种备份方式有更少的数据移动；减少了备份时间和所需的存储容量，减轻了网络负担；降低潜在的人为错误。

36．数据恢复：通常分为全盘恢复，数据库和邮件系统恢复，个别文件恢复和重定向恢复。

37．容灾可以分为数据容灾和因公容灾两类：

数据容灾：在异地建立一个数据容灾系统；

应用容灾：建立在数据容灾的基础之上，在移动容灾中心建立和本地应用服务系统相当的应用系统。

38．数据备份和数据容灾存在本质的区别：备份数据从逻辑上来讲施离线的，一旦灾难发生，数据备份只能保证在一定时间内将数据恢复到某个时间点上的完整正确的状态。而数据容灾的关键在于保护数据的在线状态，保证数据在发生灾难时能从容灾中心及时恢复并且无缝地想歪提供数据服务。

39．存储器的主要错误是是单个电路故障所引起的以为错或者相关多位错，而随机独立的多位错误极少。在按字节组织的内存储器中，主要错误模式为单字节错；而在位组织的内存储器中，主要错误模式为单位错。

40．半导体存储器的错误大体上分为硬错误和软错误，其中主要为软错误。硬错误所表现的现象是在某个或某些位置上，存取数据重复地出现错误，出现这种现象的原因是一个或几个存储单元出现故障。软错误主要是由a粒子引起的，引起软错误的另一原因是噪声干扰。

41．存储技术中常用的纠检错码有奇偶校验码，海明码及其改进码。

① 一维奇偶校验码是最简单的一种纠错码，它能发现所有的奇数位错，但它不能用来纠正错误。二维奇偶校验码可以纠正一位错。

② 海明码是一种能纠一维错的线性分组码。常用的能检测两位错同事能纠正一位错的纠错码有扩展海明码和最佳奇权码，它们的最小码距都为4，两者有相似之处，比如冗余度一样。

③ 利用纠错码技术，可以保证计算机存储设备数据安全。

【备考点拨】

了解并理解相关知识点内容。

### 考点2、操作系统安全

【考法分析】

本考点主要是对操作系统安全相关内容的考查。

【要点分析】

1．操作系统实质是一个资源管理系统，管理计算机系统的各种资源，用户通过它获得对资源的访问权限。安全操作系统出了要实现普通操作系统的功能外，还要保证它所管理资源的安全性，包括保密性（Secrecy），完整性（Integrity）和可用性（Availability）。

2．安全威胁可以分为如下6类：① 不合理的授权机制；② 不恰当的代码执行；③ 不恰当的主体控制；④ 不安全的进程间通信（IPC）；⑤ 网络协议的安全漏洞；⑥ 服务的不当配置。

3．按照威胁的行为方式划分，通常有下面4种：① 切断；② 截取；③ 篡改；④ 伪造。

4．按照安全威胁的表现形式来分，操作系统面临的安全威胁有以下5种：① 计算机病毒；② 逻辑炸弹；③ 特洛伊木马；④ 后门；⑤ 隐蔽通道。

5．安全模型包括状态机模型，信息流模型，无干扰模型，不可推断模型，完整性模型等类型。

① 状态机模型：欧诺个状态语言将安全系统描绘成抽象的状态机，用状态变量表示系统的状态，用转换规则描述变量变化的过程。状态机模型用于描述通用操作系统的所有状态变量几乎是不可能的 ，通常只能描述安全操作系统中若干个与安全相关的主要状态变量。

② 信息流模型：用户描述系统中客体间信息传输的安全需求。信息流模型不是检查主体对客体的存取，二十试图控制从一个客体到另一个客体的信息传输过程。

③ 无干扰模型：将系统的安全需求描述成一系列主体间操作互不影响的断言

④ 不可推断模型：这个模型提出了不可推断性的概念，要求低安全级用户不能推断出高安全级用户的行为。

⑤ 完整性模型：目前公认的两个完整性模型是BIha模型和Clark-Wilson模型。

6．Biba模型通过完整级的概念，控制主体“写”访问操作的客体范围。Clark-Wilson模型针对完整性问题，对系统进行功能分割和管理。

7．BLP模型是最早的一种计算机多级安全模型，也是受到公认最著名的状态机模型。

8．操作系统的安全机制就是指在操作系统中利用某种技术，某些软件来实施一个或多个安全服务的过程。

9．身份鉴别是计算机系统正确识别用户个人身份的重要途径。

10．访问是使信息在主体和对象间流动的一种交互方式。访问控制是对信息系统资源进行保护的重要措施，适当的访问控制能够阻止未经允许的用户有意或无意地获取数据。

11．访问控制的手段包括用户识别代码，口令，登陆控制，资源授权（例如用户配置文件，资源配置文件和控制列表），授权核查，日志和审计。

12．最小特权原则应限定系统中每个主体所必需的最小特权，确保可能的事故，错误，网络部件的篡改等原因造成的损失最小。

13**．**最小特权原则要求每个主体在操作时应当使用尽可能少的特权。

14．可信通路（Trusted Paht，TP）也称为可信路径，是指用户能跳过应用层而直接同可信计算基之间通信的一种机制。

15．安全操作系统很重要的一点是进行分层设计，而运行域正是一种基于保护环的层次等级式结构。

16．存储器是操作系统管理的重要资源之一，也是被攻击的主要目标。存储器保护主要是指保护用户在存储器中的数据，防止存储器中的数据泄露或被篡改。

17．在操作系统中，所有的数据都是以文件形式存在的。文件保护就是防止文件被非法窃取，篡改或丢失，同时又保证合法用户能正确使用文件。

18．进行文件保护的方法主要有文件的备份，文件的恢复，文件的加密。

19．操作系统的安全审计是指对系统中有关安全的活动进行记录，检查和审核。

20．安全操作系统的设计原则：

① 最小特权；② 机制的经济性；③ 开放系统设计；④ 完整的存储控制机制；⑤ 基于“允许”的设计原则；⑥ 权限分离；⑦ 避免信息流的潜在通道；⑧ 方便使用。

21．在现有操作系统上实现安全增强是目前提高操作系统安全性普遍采用的方式，一般有三种具体方法：

① 虚拟机法。在现有操作系统与硬件之间增加一个新的分层作为安全内核，操作系统几乎不变地作为虚拟机来运行。

② 改进、增强法。在现有操作系统的基础上对其内核和应用陈旭进行面向安全策略的分析，然后加入安全机制，经改造，开发后的安全操作系统基本上保持了原来操作系统的用户接口界面。

③ 仿真法。对现有操作系统的内核进行面向安全策略的分析和修改以形成安全内核。然后在安全内核与原来操作系统用户接口界面中间再编写一层仿真程序。

22．安全操作系统的一般开发过程：

首先建立一个安全模型；然后是安全机制的设计与实现；最后是安全操作系统的可信度认证。

23．操作系统近年来受到重视的安全增强技术：

① 增强对用户身份的识别；② 增加对访问的控制；③ 审计增强；④ 安全管理增强；⑤ 多管理员增强：改进原有操作系统中管理方面的缺陷和开发自动化或半自动化的辅助管理技术或工具；⑥ 自动化辅助管理。

除了缓冲区溢出的安全增强，网络协议栈安全增强，系统完整性保护等近年来也有一定的研究。

【备考点拨】

了解并理解相关知识点内容。

### 考点3、数据库系统的安全

【考法分析】

本考点主要是对数据库系统安全相关内容的考查。

【要点分析】

1．数据库安全就是保证数据库信息的保密性，完整性，一致性和可用性；一般而言，数据库安全涉及以下这些问题：

① 问题数据库的完整性；② 逻辑数据库的完整性；③ 元素安全性；④ 可审计性；⑤ 访问控制；⑥ 身份认证；⑦ 可用性；⑧ 推理控制；⑨ 多级保护；⑩ 消除隐通道。

2．数据库安全的发展可分为4个阶段：萌芽阶段，军事主导阶段，标准化阶段，多样化阶段。

3．访问控制技术提供了一种控制用户访问数据的机制。

4．安全策略表达模型一般分为两大类，即自主访问控制（DAC）和强制访问控制（MAC）。自主访问控制中，用户对信息的访问是基于用于的鉴别和访问控制规则的确定，每个用户都要给予系统中每个访问对象的访问权限。在强制访问控制中，系统给主体和客体分配了不同的安全标记，通过比较主体和客体的安全标记是否匹配，来决定是否允许访问。

5．数据中需要满足的安全策略应该满足以下一些原则：

① 最小特权原则；② 最大共享原则；③ 开放系统原则和封闭系统原则。

6．在开发系统中，存储规则规定的是哪些访问操作是不被允许的；在设计文芳控制策略时，还有一些特殊的规则约束。

7．数据库安全策略的实施：

① 子模式法：对于用户而言，他所能访问到的信息是数据库中模式的一部分，并且是模式的i中对外体现形式，而不能访问到或了解到整个模式。用户所能了解的那部分模式，称为子模式。

② SQL修改查询法：该方法的核心思想是当用户进行SQL查询时，数据库系统对用户提交的SQL查询语句自动附加上更多的安全约束限制。

③ 集合法。

④ 请求排序法。

8．数据库加密技术是一种对计算机系统外存储器中数据进行保护的有效手段。数据库加密技术还有其更为特殊的要求。

① 数据库中的数据保存的时间相对更长，因此对加密强度的要求也更高；

② 数据库中数据量很大，对加密熟读要求更高；

③ 数据库中数据通常是多用户共享的，对加密和解密的性能要求也会更高

④ 数据库中的数据规律性教强，某一个列的数据项往往取值于某一个限定范围，往往呈现一定的概率分布。引出数据库的加密技术需要消除密文之间的关联性。确保相同或雷士的明文在加密后的密文无规律性。

9．多级安全数据库是数据库在具体设计，实现方面中药的研究领域。它将数据库中的重要数据进行安全等级划分，通过融合访问控制，数据库加密等技术实施的综合保障技术来实现符合标准规范的安全数据库。

10．推理通道通常分为三大类：

① 演绎推理通道：在这类推理通道中，高级数据可以完全从低级数据中形式化的推理得出。

② 不明推理通道：在这类推理通道中，如果确定一些低级别上的推理依据公里，由低级数据就可以推理出高级数据，完成演绎推理及其证明这类推理通道相比于演绎推理通道，需要一些推理假设，因此其完备性相对较弱。

③ 概率推理通道：在这类推理通道中，由低等级数据可以降低高等级数据的不确定性。

11．数据库备份分为物理备份和逻辑备份，其中文理备份又分为：冷备份和热备份。

① 冷备份：通过定期的对系统数据库进行备份，并将备份数据存储在磁带，磁盘等介质上。在冷备份过程中，数据库必须是关闭状态。

② 热备份：热备份是指当数据库正在运行时进行的备份，又称联机备份。热备份的实现通常徐璈一个备用的数据库系统。

③ 逻辑备份：物理备份的一种补充，它使用软件技术，利用到处工具执行SQL语句方式，从数据库中读取数据，将其到处到一个数据文件中。该文件的格式一般与原数据库的文件格式不同，而是原数据库中数据内容的一个映像。因此，逻辑备份文件只能用来对数据库进行逻辑恢复，即数据导入，而不能按数据库原来的存储特征进行物理恢复。逻辑备份一般用于增量备份。

【备考点拨】

了解并理解相关知识点内容。

### 考点4、恶意代码

【考法分析】

本考点主要是对恶意代码相关内容的考查。

【要点分析】

1．恶意代码，指为达到恶意的目的而专门设计的程序或代码，是指一切旨在破坏计算机或者网络系统可靠性，可用性，安全性和数据完整性或者消耗系统资源的恶意程序。

恶意代码的主要的存在形态有：恶意数据文档，恶意网页，内存代码，可执行程序和动态链接库等。

2．恶意代码=广义的计算机病毒；恶意代码的一般命名格式为：<恶意代码前缀>.<恶意代码名称>.<恶意代码后缀>；恶意代码后缀的数量可以有1到多个，如果只有1个，通知是指一个恶意代码的变种特征。

3．常用恶意代码前缀解释：

① 系统病毒：前缀为：Win32，PE，Win95，W32，W95等，这些病毒是可以感染Windows操作系统的\*.exe和\*.dll文件。

② 网络蠕虫：前缀为Worm

③ 特洛伊木马：前缀为Trojam

④ 脚本病毒：前缀为Script

⑤ 宏病毒：前缀为Macro

⑥ 后门程序：前缀是Backdoor

⑦ 病毒种植程序病毒

⑧ 破坏程序病毒：前缀是Harm

⑨ 玩笑病毒：前缀是Joke

⑩ 捆绑机病毒：前缀是Binder

4．恶意代码命名的形式，每个组成部分介绍如下：

① 恶意代码类型（malware\_type）；② 平台（platform）；③ 家族名（family\_name）；④ 组名（group\_name)；⑤ 感染程度（infective\_length）；⑥ 变种名（variant）；⑦ 退化标识（devolution）；⑧ 修饰符（modifiers）。

5．计算机病毒的特征可以归纳为传染性，程序性，破坏性，非授权性，隐蔽性，潜伏性，可触发性和不可预见性。

6．计算机病毒的生命周期：潜伏阶段，传播阶段，出发阶段，发作阶段。

7．计算机病毒传播途径：

① 通过软盘，光盘传播；② 通过移动存储设备传播；③ 通过网络传播。

8．蠕虫最重要的两个特征：“可以从一台计算机移动到另一台计算机”，以及“可以自我复制”。

9．木马与病毒不同，它不以破坏目标计算机系统为主要目的，同时在主机间没有感染性。木马的危害早已超过病毒。

10．特洛伊木马又可以分为多种，如远程控制型木马，信息窃取木马，破坏型木马等。

11．后门：指绕过系统中常规安全控制机制而获取对特定软件或系统的访问权限的程序。一般是指攻击者在获得目标主机控制权之后为了今后能方便地进入该计算机而安装的一类软件，它不仅绕过系统已有的安全设置，而且还能挫败系统上各种增强的安全设置。

12．其他恶意代码：① DDos程序；② 僵尸程序（Bot）；③ Rootkit：最初被定义为由有用的小程序组成的工具包，可是的攻击者能够获得计算机用户“Root”的最高系统权限。Rootkit技术的关键在于“是的髠对象无法被检测”，因此Rootkit所采用的大部分技术和技巧都用于在计算机上隐藏代码和数据。④ Exploit：漏洞利用程序。针对某一特定漏洞或一组漏洞而精心编写的漏洞利用程序。目前比较常见的Exploit有：主机系统漏洞Exploit、文档类漏洞Exploit和网页挂马类Exploit等。

13．为了彻底清除恶意代码，需要按照以下步骤进行：

① 停止恶意代码的所有活动行为（包括停止进程，服务，卸载DLL等）；

② 删除恶意代码新建的所有文件备份（包括可执行文件，DLL文件，驱动程序等）；

③ 清除恶意代码写入的所有启动选项；

④ 对被计算机病毒感染的文件，还需要对被感染文件进行病毒清除等。

需要注意的是，并不是所有恶意代码对系统进行的修改都可以被恢复。

14．典型反病毒技术：

① 特征值查毒法：前提是需要从病毒体中提取病毒特征值构成病毒特征库；

② 校验和技术；

③ 启发式扫描技术：一个熟练的程序员在调试状态下只需要一看便可一目了然。启发式代码扫描技术实际上就是把这种经验和知识移植到反病毒软件中，从而有可能找到未知的病毒。

④ 虚拟机技术：软件模拟法，它是一种软件分析器，用软件方法来模拟和分析程序的运行，而且程序的运行不会对系统起实际的作用

⑤ 行为监控技术：通过审查应用程序的操作来判断是否有恶意（病毒）倾向并向用户发出警告。

⑥ 主动防御技术：并不是一项全新的技术，集成了启发式扫描技术和行为监控及行为阻断等技术。

【备考点拨】

了解并理解相关知识点内容。

### 考点5、计算机取证

【考法分析】

本考点主要是对计算机取证技术相关内容的考查。

【要点分析】

1．计算机取证是将计算机调查和分析技术应用与对潜在的，有法律效力的证据的确定与提取上。

2．计算机取证包括了对以磁介质编码信息方式存储的计算机证据的保护，确认，提取和归档。与传统证据一样，电子证据必须是可信，准备，完整，符合法律法规的，是法庭所能够接受的。同时，电子证据与传统证据不同，具有高科技性，无形性和易破坏性等特点

3．计算机取证主要是对电子证据的获取，分析，归档，保存和描述的过程；计算机取证的通常步骤包括：保护目标计算机系统，确定电子证据，收集电子证据，保全电子证据。

4．分析电子证据的信息需要很深的专业知识，应依靠专业的取证专家。通常取证分析工作中用到的技术包括：① 对比分析和关键字查询；② 文件特征分析技术；③ 密码破译；④ 数据恢复与残留数据分析；⑤ 磁盘备份文件，镜像文件，交换文件，临时文件分析技术；⑥ 日志记录文件分析；⑦ 相关性分析等。

【备考点拨】

了解并理解相关知识点内容。

### 考点6、嵌入式系统安全

【考法分析】

本考点主要是对嵌入式系统安全相关内容的考查。

【要点分析】

1．广义地讲，凡是不用于通用目的的可编程计算机设备，就可以算是嵌入式计算机系统。最典型的嵌入式系统如手机，可视电话等，如传真机，打印机等；狭义上讲：嵌入式系统是指以应用为核心，以计算机技术为基础，软硬件可裁剪，适用应用系统对功能，可靠性，成本，体积和功耗严格妖气的专用计算机系统。

2．嵌入式系统具有如下特点：① 嵌入式系统具有应用针对性；② 嵌入式系统硬件一般对扩展能力要求不高；③ 嵌入式系统一般采用专门针对嵌入式应用设计的中央处理器；④ 嵌入式系统中操作系统可能有也可能没有，且嵌入式操作系统与桌面计算机操作系统有较大差别；⑤ 嵌入式系统一般有实时性要求；⑥ 嵌入式系统一般有较高的成本控制要求；⑦ 嵌入式系统软件一般有固化的要求；⑧ 嵌入式系统一般采用交叉开发的模式；⑨ 嵌入式系统在体积，功耗，可靠性，环境适应性上一般有特殊要求；⑩ 嵌入式系统技术标准化程度不高，也存在一定程度的标准化。

3．常见的嵌入式系统设备，包括智能卡，USB-key和智能手机等。

4．智能卡的用途可归为如下四点：① 身份识别；② 支付工具；③ 加密解密；④ 信息存储。

5．从本质上说，片内操作系统（COS）是智能卡芯片内的一个监控软件，它在智能卡中的概念和地位类似与DOS在个人计算机PC中的概念和地位。与DOS不一样的地方在于：COS更加注意安全；COS一般由四部分组成★：通讯管理模块和安全管理模块，应用管理模块和文件管理模块。

6．针对智能卡，有以下几种常见的攻击手段：① 物理篡改；② 时钟抖动；③ 超范围电压探测。

7．USB Key是一种USB接口的硬件设备；USB Key身份认证的特点：

① 双因子认证：每一个USB key都具有硬件PIN码保护，PIN码和硬件构成了用户使用USB Key的两个必要因数。即所谓“双因子认证”。用户只有同时取得了USB Key和用户PIN码，才可以登录系统。

② 带有安全存储空间。

③ 硬件实现加密算法。

④ 便于携带，安全可靠

⑤ 身份认证模式

8．USB Key目前来说并不是绝对安全的，实际存在两大安全漏洞：

① 交互操作存在漏洞，黑客可以远程控制；

② 无法防止数据被篡改。

解决这些漏洞的方法是通过在USB设备上增加新的硬件，革新认证策略。

9．由于USB Key具有安全可靠，便于携带，使用方便，成本低廉的优点，使用USB key存储数字证书的认证方式已经成为目前主要的认证模式。

10．智能手机的诞生，是PDA演变而来的。PDA，英文全称Personal Digital Assistant，即个人数码助理，一般是指掌上电脑。

11．智能手机的操作系统有：Windows CE，Palm OS，Pocket PC，WindowsPhone和IOS，安卓等。

Windows CE：微软开发的嵌入式操作系统；

Palm OS：Palm公司开发的32位嵌入式操作系统；

Pocket PC：在Windows CE的基础上改进的；

WindowsPhone：简称WP；

Android：是一种以Linux为基础的开放源代码操作系统。Android 分为4个层，从高层到低层分别是应用程序层，应用程序框架层，系统运行库层和Linux核心层。Android是以Linux为核心的手机操作平台；

iOS：由苹果公司开发的移动操作系统，也是闭源的操作系统，所有的开发软件必须苹果的审核才能开放使用，并且只能在苹果的硬件设备上使用。

12．智能手机安全隐患有如下的几个方面：

① 目前我国软件应用平台以谷歌的安卓为主；

② 黑客们就电商APP进行二次打包伪装知名应用混淆用户；

③ 手机病毒感染率非常严峻；

④ 短信信息常含有一些恶意软件，网站的链接，扫面二维码染毒的分先日益增多。

13．可信智能手机应该具有无线保密通信，GPS等典型的功能应用，其具体方法如下：

① 可信智能终端系统的体系结构；

② 可信智能终端的操作系统安全增强；

③ 可信智能终端的信任链结构；

④ 可信只能终端的保密通信与可信网络连接。

14．现代工业控制系统包括过程控制，数据采集系统（SCADA），分布式控制系统（DCS），程序逻辑控制（PLC）以及其他控制系统等。

15．在中国，与传统的网络语信息系统安全相比，工业控制系统信息安全保护水平明显偏低，长期以来没有得到关注，大多数的工业控制系统在开发设计时，只考虑了效率和实时等特性，并未将信息安全纳入主要考虑的指标。

16．工业控制系统面临的威胁是多样化的，一方面敌对政府，恐怖组织，商业间谍，内部不法人员，外部非法入侵者等对系统虎视眈眈；另一方面，系统复杂性，认为事故，操作系统，设备故障和自然灾害等也会对工业控制系统造成破坏。

17．电力工控系统面临的主要威胁：① 内部人为风险；② 黑客攻击；③ 病毒破坏；④ 预置陷阱；⑤ 电力工控系统采用对策：加强制度建设和人员管理；加强技术防范；加强整体防护。

18．工控系统信息安全不是一个单纯的技术问题，而是涉及到技术，管理，流程，人员意识等各方面的系统工程，徐璈组件包括控制工程师，工控设备供应商，系统集成商，信息安全专家等成员的工控系统信息安全队伍。

19．在监控级(如：工程师站、操作员站、历史站等)和网络层面可采取现有等级保护的相关标准和规范开展等级测评；在控制级，应加强对 Modbus、 OPC 等通信协议 的使用管理，对其用户身份进行鉴别和认证；在现场级，应实现对设备、控制元件的准入检测，加快建立工控设备的检测标准和规范；在管理上，应建立完善的工控系统安全运维方案、策略和计划，加强日常安全培训，严控处理流程，防止内部攻击，实现终端安全防护，操作使用安全，针对现阶段难议解决的技术问题应通过管理手段进行弥补，切实提高工控系统的安全防护能力。

【备考点拨】

了解并理解相关知识点内容。

## 第5章：应用系统安全基础

### 考点1、Web安全

【考法分析】

本考点主要是对Web安全相关内容的考查。

【要点分析】

1．Web 安全威胁：从其来源说Web 威胁还可以分为内部攻击和外部攻击两类。前者主要来自信任网络，可能是用户执行了未授权访问或是无意中定制了恶意攻击；后者主要是由于网络漏洞被利用或者用户受到恶意程序制定者的专一攻击。

2．最具危险性的Web 威胁：① 可信任站点的漏洞；② 浏览器和浏览器插件的漏洞；③终端用户；④ 可移动的存储设备；⑤ 网络钓鱼；⑥ 僵尸网络；⑦ 键盘记录程序；⑧ 多重攻击；以上这些威胁并不代表全部。

3．Web 访问控制技术：访问控制是Web 站点安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法访问者访问。访问Web 站点要进行用户名、用户口令的识别与验证、用户账号的缺省限制检查。只要其中任何一关未过，该用户便不能进人某站点进行访问。

4．Web 服务器一般提供了如下三种类型的访问控制方法。

① 通过IP地址、子网或域名来进行控制；

② 通过用户名/口令来进行访问控制；

③ 通过公钥加密体系PKI-智能认证卡来进行访问控制。

5．单点登录技术：单点登录系统的目的就是为这样的应用系统提供集中统一的身份认证，实现"一点登录、多点漫游"的目标，方便用户使用。

6．单点登录系统采用基于数字证书的加密和数字签名技术，基于统一的策略的用户身份认证和授权控制功能，从而实现"一点登录、多点漫游"。但是在实际应用中，一些理论上不错的方案却在实际中无法实现，这里总结三个主要的方面：计算环境相关的问题；组织结构的问题和电子身份认证方法的问题。

7．几种常用的单点登录模型：

① 基于网关的SSO 模型；

② 基于验证代理的SSO 模型；

③ 基于Kerberos 的sso 模型。

8．常见的网页防篡改技术有以下三种:

① 时间轮询技术：时间轮询技术是利用一个两页检测程序，以轮询方式读出要监控的网页，与真实网页相比较，来判断网页内容的完整性，对于被篡改的网页进行报警和恢复。

② 核心内嵌技术+事件触发技术：所谓事件触发技术就是利用操作系统的文件系统或驱动程序接口，在网页文件的被修改时进行合法性检查，对于非法操作进仔报警和恢复。

所谓核心内嵌技术即密码水印技术。该技术将篡改检测模块内嵌在Web 服务器软件里，它在每一个网页流出时都进行完整性检查，对于篡改网页进行实时访问阻断，井予以报警和恢复。

③ 文件过滤驱动技术十事件触发技术：其原理是将篡改监测的核心程序通过微软文件底层驱动技术应用到Web 服务器中，通过事件触发方式进行自动监测，对文件夹的所有文件内容，对照其底层文件属性，经过内置散列快速算法，实时进行监测，若发现属性变更，通过非协议方式，纯文件安全拷贝方式将备份路径文件夹内容拷贝到监测文件夹相应文件位置，通过底层文件驱动技术，整个文件复制过程毫秒级，使得公众无法看到被篡改页面，其运行性能和检测实时性都达到最高的水准。

9．内容安全管理技术可以细分为电子邮件过滤、网页过滤、反间谍软件三大技术。针对反间谍软件危害性，应从三方面加以防范。一是预防，二是设置障碍，三是杀毒。

【备考点拨】

了解并理解相关知识点内容。

### 考点2、电子商务安全

【考法分析】

本考点主要是对电子商务安全相关内容的考查。

【要点分析】

1．电子商务安全概念、特点：电子商务安全从整体上可分为两大部分：网络安全和商务交易安全。

2．网络安全的内容包括：网络设备安全、网络系统安全、数据库安全等。

3．电子商务安全是以网络安全为基础的。电子商务安全与肉络安全又是有区别的：首先，网络不可能绝对安全，在这种情况下，还需要运行安全的电子商务。其次，即使网络绝对安全，也不能保障电子离务的安全。

4．电子商务安全具有如下四大特性：

① 电子离务安全是一个系统概念；

② 电子商务安全是柏对的；

③ 电子商务安全是有代价的；

④ 电子商务安全是发展的、动态的。

5．安全需求：

① 交易实体身份可认证性需求；

② 信息保密性的需求；

③ 信息完整性的需求；

④ 交易信息的不可抵赖性需求；

⑤ 商务服务的有效性需求；

⑥ 访问控制性需求。

电子商务要安全地展开，以上几个最基本的安全要素必须实现。也就是说，数据和信息的隐私必须受到保护，交易者身份必须得到认证，并且具有可认证性，未被授权的进入应该进行控制和拒绝。

6．身份认证过程指的是当用户试匮访问资源的时候，系统确定用户的身份是否真实的过程。认证对所有需要安全的服务来说是至关重要的，因为认证是访问控制执行的前提，是判断用户是否有权访问信息的先决条件，同时也为日后追究责任提供不可抵赖的证据。

7．通常可以根据以下5 种信息进行认证：

① 用户所知道的。

② 用户所拥有的。

③ 用户本身的特征。

④ 根据特定地点(或特定时间)。

⑤ 通过信任的第三方。

认证技术决定了系统的安全程度。

8．所谓数字证书就是在互联网通信中标志通信各方身份信息的一系列数据，提供了一种在Intemet 上验证用户身份的方式，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一CA机构，又称为证书授权中心发行的，人们可以在网上用它来识别彼此的身份。

9．CA机构，又称为证书授权中心，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。

10．数字证书采用公钥体制，即利用一对互相匹配的密铝进行加密、解密。

11．数字证书与传输密钥和签名密钥对的产生相对应。对每一个公钥做一张数字证书，私钥用最安全的方式交给用户或用户自己生产密钥对。在公开密钥密码体制中，常用的一种是RSA体制。

12．目前有两种安全在线支付协议被广泛采用，分别为安全电子交易协议(SET) 和安全套接字协议(SSL) ，二者均是成熟和实用的安全协议。

13．SET 协议是应用层的协议，是一种基于消息流的协议，它是面向B2C (企业对消费者)模式的，完全针对信用卡来制定，涵盖了信用卡在电子商务交易中的交易协议信息保密、资料完整等各个方面。

14．SET 协议主要使用的技术包括：对称密钥加密、公钥加密、Hash 算法、数字签名、数字信封以及数字证书等技术。

15．SET 协议是一个基于可信的第三方认证中心的方案，其主要的实现目标是：

① 保证电子离务参与者信息的相互隔离；

② 保证信息在Internet 上安全传输；

③ 解决多方认证问题；

④ 保证网上交易的实时性；

⑤ 提供一个开放式的标准。

16．SET交易的参与方包括持卡人、发卡机构、离家、收单银行、支付网关和数字证书认证中心CA。

17．SET 协议分为三个部分：

① 商业描述；② 程序员指导；③ 正式的协议定义。

18．SET 协议是一种电子支付系统的安全协议，因此它涉及加密、认证等多种技术。

① 加密技术：加密技术是SET 协议中的核心技术，在SET 中使用的主要包括对称加密、非对称加密、数字签名、消息摘要、数字信封、双重签名等。

② 认证技术：网上交易的买卖双方在进行每一笔交易时，为了保证交易的可靠性，买方和卖方都要鉴别对方的身份。

19．CA的主要功能有：收注册请求处理、批准/拒绝请求、发行证书。

20．认证技术具体涉及以下一些内容：

① 证书信息：

持卡人证书：持卡人证书表明持卡人拥有的支付卡是合法的，它是由权威的金融机构数字签署的，不能由其他非法第三方产生。

商家证书：商家证书与持卡人证书基本一样。

支付网关证书：支付网关证书由收单行或收单行的处理系统拥有。

收单行证书：一个收单银行必须拥有证书，才能使一个CA 接收和处理商家从公共和专用网络发出的证书请求。

发卡行证书：一个发卡银行必须拥有证书， CA 才能接收和处理来自持卡人的证书请求(通过公共或专用网络)，那些选择支付卡品牌来代理处理证书请求的发卡行不需要证书。

② 证书的发行。

③ 认证信息和验证结构：

认证信息：在SET 中，交易双方的身份必须要验证， CA 是提供身份验证的第三方机构。

21．SET协议主要是通过使用密码技术和数字证书方式来保证信息的机密性和安全性，它实现了电子交易的机密性、数据完整性、身份的合法性和不可否认性。

22．SSL 安全套接层协议是安全通信协议。在SSL中，采用了公开密钥和私有密钥两种加密方式，它对计算机之间整个会话进行加密，从而保证了安全传输。SSL 的安全服务位于TCP 和应用层之间，可为应用层(如HTTP 、FTP 、SMTP) 提供安全业务，服务对象主要是Web 应用，即客户浏览器和服务器。

23．SSL 服务器认证允许用户确认服务器身份。SSL 客户机认证允许服务器确认用户身份。

24．一个加密的SSL 连接要求所有在客户机与服务器之间发送的信息由发送方软件加密和由接受方软件解密，对称加密法用于数据如密(如用DES 和RC4 等)，从而连接是保密的。

25．SSL主要工作流程包括：网络连接建立；与该连接柜关的加密方式和压缩方式选择；双方的身份识别；本次传输密钙的确定；加密的数据传输；网络连接的关闭。

26．SSL是一个两层协议，包括SSL 握手层协议和SSL 记录层协议。

27．SSL协议提供的服务可以归纳为如下三个方面：

① 用户和服务器的合法性认证；

② 加密数据以隐藏被传送的数据；

③ 维护数据的完整性。

28．SSL 协议自身的缺陷：

① 客户端假冒；

② SSL 协议无法提供基于四P 应用的安全保护；

③ SSL 协议不能对抗通信流量分析；

④ 可能受到针对基于公钥加密标准（PKCS) 的协议的自适应选择密文攻击；

⑤ 进程中的主密钥泄漏；

⑥ 磁盘上的临时文件可能遭受攻击。

29．SSL 加密算法和会话密钥是在握手协议中协商并由Cipher-Choice 指定的。现有的SSL 版本中所用到的加密算法包括：RC4、RC2、IDEA、DES 和3DES ，而加密算法所用的密钥由消息散列函数MD5 产生。

30．SSL 协议中对称加密用于加密应用数据，非对称加密用于验证实体和交换密钥。非对称加密算法按用途分为密钥交换算法和数字签名算法。

【备考点拨】

了解并理解相关知识点内容。

### 考点3、信息隐藏

【考法分析】

本考点主要是对信息隐藏技术相关内容的考查。

【要点分析】

1．信息隐藏是把一个有意义的信息隐藏在另一个称为载体(Cover) 的信息中得到隐蔽载体(Stego Cover) S。非法者不知道这个普通信息中是否隐藏了其他的信息，而且即使知道也难以提取或去除隐藏的信息。为增加攻击的难度，也可以把加密与信息隐藏技术结合起来，即先对消息M 加密得到密文消息M' ，再把M' 隐藏到载体C 中。这样攻击者要想获得消息，就首先要检测到消息的存在，并知道如何从隐蔽的载体S 中提取M'及如何对M'解密以恢复消息M 。

2．信息隐藏不同于传统的密码学技术。信息隐藏则主要研究如何将某一机密信息秘密隐藏于另一公开的信息中，然后通过公开信息的传输来传递机密信息。

3．信息之所以能够隐藏在多媒体数据中是因为：

① 多媒体信息本身存在很大的冗余性，从信息论的角度看，未压缩的多媒体信息的编码效率是很低的，所以将某些信息嵌入到多媒体信息中进行秘密传送是完全可行的，并不会影响多媒体本身的传送和使用。

② 人眼或人耳本身对某些信息都有一定的掩蔽效应，比如人眼对灰度的分辨率只有几十个灰度级：对边沿附近的信息不敏感等。利用人的这些特点，可以很好的将信息隐藏雨不被察觉。

3．信息隐藏的分类：

隐写术：其目的是在不引起任何怀疑的情况下秘密传送消息。

数字水印：嵌在数字产品中的数字信号，其目的是进行版权保护、所有权证明、指纹(追踪发布多份拷贝)和完整性保护等。

对信息隐藏技术的不同应用，各自有着进一步不同的具体要求，并非都满足上述要求。

4. 根据信息隐藏的目的和技术要求，该技术存在以下特性：

① 透明性；

② 鲁棒性：鲁棒性(robustness )指不因图像文件的某种改动而导致隐藏信息丢失的能力；

③ 不可检测性；

④ 安全性：安全性(security) 指隐藏算法有较强的抗攻击能力，即它必须能够承受一定程度的人为攻击，而使隐藏信息不会被破坏。

⑤ 自恢复性；

⑥ 对称性；

⑦ 可纠错性。

5．信息隐藏模型：我们称待隐藏的信息为秘密信息，它可以是版权信息或秘密数据，也可以是一个序列号;而公开信息则称为载体信息 ，如视频、音频片段。这种信息隐藏过程一般由密钥(Key) 来控制，即通过嵌入算法将秘密信息隐藏于公开信息中，而隐蔽载体(隐藏有秘密信息的公开信息)则通过信道传递，然后检测器(Detector) 利用密钥从隐蔽载体中恢复/检测出秘密信息。

6．常用算法：信息隐藏及数字水印技术是近几年来国际学术界兴起的一个前沿研究领域。虽然其载体可以是文字、图像、语音等不再格式的文件，但是使用的方法没有本质的区别。

7．在图像中应用的信息隐藏技术基本上可以分为两大类空域法和频域法。空域法就是直接改变图像元素的值，一般是在图像元素的亮度和色带中加入隐藏的内容。频域法是利用某种数学变换，将自像用频域表示，通过更改图像的某些频域系数加入待隐消息，然后再利用反变换来生成隐藏有其他信息的图像。各种不同的数学变换都可以被使用，目前已有的方法，主要集中在小波变换，频率变换， DCT 变换等等。

① 空域算法：该类算法中典型的算法是将信息嵌入到随机选择的图像点中最不重要的像素位(LSB) 上，这可保证嵌入的水印是不可见的。

② Patchwork算法：该算法是随机选择N 对像素点（ai ， bi），然后将每个ai点的亮度值加1，每个bi 点的亮度值减1，这样整个图像的平均亮度保持不变。

③ 频域算法：采用了扩展频谱通信技术。另外，还可以将数字图像的空间域数据通过离散傅里叶变换（DFT) 或离散小波变换（DWT) 转化为相应的频域系数。

④ 压缩域算法：基于JPEG、MPEG 标准的压缩域数字水印系统不仅节省了大量的完全解码和重新编码过程。

⑤ NEC 算法：该算法由NEC 实验室的Cox 等人提出。其实现方法是，首先以密钥为种子来产生伪随机序列，该序列具有高斯N(0, 1)分布，密钥一般由作者的标识码和图像的哈希值组成，其次对图像做DCT 变换。

⑥ 生理模型算法：人的生理模型包括人类视觉系统HVS (Human Visual System)和人类听觉系统HAS。利用视觉模型来确定与周像相关的调制掩模，然后再利用其来插入水印。这一方法同时具有好的透明性和强健性。

8．第一篇关于图像数字水印的文章发表于1994年。经过多年的努力，信息隐藏技术的研究已经取得了很大进展，国际上先进的信息隐藏技术现己能做到:使隐藏有其他信息的信息不但能经受人的感觉检测和仪器设备的检测，而且还能抵抗各种人为的蓄意攻击。

9．信息隐藏技术的应用领域为五个方面：

① 数据保密；

② 数据的不可抵赖性；

③ 数字作品的版权保护；

④ 防伪；

⑤ 数据的完整性。

10．数字水印技术通过将数字、序列号、文字、图像标志等信息嵌入到媒体中，嵌入的过程中对载体尽量小的修改，以达到最强的鲁棒性，当嵌入水印后的媒体受到攻击仍然可以恢复水印或者检测出水印的存在。

11．数字图像的内嵌水印有下列特点：① 透明性；② 鲁棒性；③ 安全性。

12．所有嵌入水印的方法部包含两个基本的构造模块：水印嵌入系统和水印恢复系统。

① 水印嵌入系统的输入是水印；

② 水印恢复系统的输入是已经嵌入水印的数据。

13．水印系统根据输入输出的种类及其组合可分为三种：

① 秘密水印(非盲化水印)该类系统至少需要原始的数据；

② 半秘密水印(半盲化水印)该类系统并不使用原始数据来检测，但是需要水印的拷贝。

③ 公开水印(盲化或健忘水印。

14．目前提出的数字水印嵌入方法，基本分为两类：基于空间域和基于变换域的方法。

① 空间域数字水印是直接在声音、图像或视频等信号空间上叠加水印信息。常用的技术有最低有效位算法(LSB) 和扩展频谱方法；

② 变换域数字水印是指在DCT 变换域、时/频变换域(DFT)或小波变换域(DWT)上隐藏水印。

15．视频水印面向数字视频载体，是数字水印技术中的热点和难点。

16．同其他水印技术一样，视频水印应满足基本的水印性能要求，如透明性、鲁棒性、安全性等，也同时存在以下几种视频水印特殊要求。

① 经受各种非恶意的视频处理；

② 实时性：实时性要求是视频水印算法的特殊要求；

③ 共谋攻击：共谋攻击是在静态图像水印算法中己经考虑到的一种特殊水印攻击。

17．水印必须对一些无意的攻击具有鲁棒性，也就是对那些能保持感官相似性的数字处理操作具备鲁棒性，常见的操作有：① 剪切；② 亮度和对比度的修改；③ 增强、模糊和其他滤波算法；④ 放大、缩小和旋转；⑤ 有损压缩，如JPEG 压缩；⑥ 在图像中加噪声。

18．通常假定在检测水印时不能获得原始产品。下面是有意攻击一般分类：

① 伪造水印的抽取；

② 伪造的肯定检测；

③ 统计学上的水印抽取；

④ 多重水印。

19．应用中的典型攻击方式及对策：

① 鲁棒性攻击：在不损害图像使用价值的前提下减弱、移去或破坏水印，也就是各种信号处理操作，还有一种可能性是面向算法分析的。

② 表达攻击：这种攻击并不一定要移去水印，它的目标是对数据作一定的操作和处理，使得检测器不能检测到水印的存在。

③ 解释攻击：在一些水印方案中可能存在对捡测出的水印具有多种解释。解释攻击包括拷贝攻击、可逆攻击等，它使数字水印的版权保护受到了挑战。

④ 法律攻击：得益于关于版权及数字信息所有权的法律的漏洞和不健全，据此应健全相关法律条例和公证制度，把数字水印作为电子证据应用于版权的仲裁，其中涉及计算机取证和纳证。

20．解释攻击及其解决方案：

① 水印仲裁：在发生版权纠纷时第三方对水印真伪进行鉴别的过程；

② 解释攻击：属于协议层的攻击，它以设计出一种情况来阻止版权所有者对所有权的断言为攻击自的。最初的解释攻击是针对不可见和非盲(需原作品)水印的仲裁阶段进行的。这样的水印在仲裁时，仲裁者根据待仲裁作品与原作品的差别来对水印进行仲裁。

③ 抗解释攻击解决方案：通过对解释攻击成功的原因进行分析，发现大多数不可见、需原图的数字水印方案主要有以下三方面的不足：首先，大多数水印方案没有提供本质的方法来检测两个水印中哪一个是先加上去的；其次，由于水印注册时仅仅对水印序列进行了注册，而没有对原作品进行注册，使得攻击者可以伪造原作品；第三，由于水印嵌入方案具有可逆性，为伪造水印提供了条件。

21．由解释攻击所引起的无法仲裁的版权纠纷的解决方案主要有三种：第一种方法是引入时戳机制，从而确定两个水印被嵌入的先后顺序；第二种方法作者在注册水印序列的同时对原始作品加以注册，以便于增加对原始图像的检测；第三种方法是利用单向水印方案消除水印嵌入过程中的可逆性。

【备考点拨】

了解并理解相关知识点内容。

### 考点4、网络舆情

【考法分析】

本考点主要是网络舆情相关内容的考查。

【要点分析】

1．网络舆情是指在互联网上流行的对社会问题不同看法的网络舆论，是社会舆论的一种表现形式。

2．网络舆情其表现方式主要为:新闻评论、BBS 论坛、博客、播客、聚合新闻CRSS) 、新闻跟帖、转帖等等。

3．网络舆情的特点：① 直接性；② 随意性和多元化；③ 突发性；④ 隐蔽性；⑤ 偏差性。

4．网络舆情的诱发因素：① 社会突发公共事件；② 虚假信息和不良信息。

5．网络舆惰的关键性技术主要包含以下四个方面：

① 网络舆情采集与提取技术；

② 网络舆情话题发现与追踪技术；

③ 网络舆情倾向性分析技术；

④ 多文档自动文摘技术。

6．网络舆惰的预警措施：

① 制定应急预案；

② 加强监测力度，密切关注事态发展；

③ 建立并完善公共危机的信息通报机制；

④ 部门联动，分工协作。

【备考点拨】

了解并理解相关知识点内容。

### 考点5、隐私保护

【考法分析】

本考点主要是隐私保护相关内容的考查。

【要点分析】

1．从隐私所有者的角度，隐私可以分为以下三类：① 个人隐私；② 通信内容隐私；③ 行为隐私。

2．隐私泄露方式：① 互联网服务；② 智能终端；③ 黑客攻击；④ 管理者监听。

3．从数据挖掘的角度，目前的隐私保护技术主要可以分为三类：

① 基于数据失真的隐私保护技术；

② 基于数据加密的隐私保护技术；

③ 基于数据匿名化的隐私保护技术。

4．数据失真技术通过扰动原始数据来实现隐私保护。基于数据失真的技术通过添加噪音等方法，使敏感数据失真但同时保持某些数据或数据属性不变，仍然可以保持某些统计方面的性质。

① 随机化：数据随机化即是对原始数据加入随机噪声，然后发布扰动后数据的方法。

② 阻塞与凝聚：随机化技术一个无法避免的缺点是:针对不同的应用都需要设计特定的算法对转换后的数据进行处理，因为所有的应用都需要重建数据的分布。鉴于随机化技术存在的这个缺陷，研究人员提出了凝聚技术:它将原始数据记录分成组，每一组内存储着由k 条记录产生的统计信息，包捂每个属性的均值、协方差等。这样，只要是采用凝聚技术处理的数据，都可以用通用的重构算法进行处理。

③ 差分隐私保护：差分隐私保护可以保证，在数据集中添加或删除一条数据不会影响到查询输出结果，因此即使在最坏情况下，攻击者己知除一条记录之外的所有敏感数据，仍可以保证这一条记录的敏感信息不会被泄露。

5．基于数据加密的隐私保护技术所针对的数据对象往往是分布式的。在分布式环境下，根据应用的不同，数据会有不同的存储模式，站点也会有不雨的可信度及相应行为。

6．分布式应用普遍采用两种模式存储数据：垂直划分的数据模式和水平划分的数据模式。垂直划分数据是指分布式环境中每个站点只存储部分属性的数据，所有站点存锚的数据不重复；水平划分数据是将数据记录存储到分布式环境中的多个站点，所有站点存储的数据不重复。

7．对分布式环境下的站点(参与者)，根据其行为，可分为：① 准诚信攻击者；② 恶意攻击者。分布式环境下的四个常见应用：安全多方计算、分布式匿名化、分布式关联规则和分布式聚类入手，介绍相应的隐私保护技术。当前，解决上述问题的策略是假设有可信任的服务提供者或是假设存在可信任的第三方。大家把各自的输入秘密地交给这个可信方，由可信方来计算出结果，然后将相应的结果返回给参与计算的各方。但是在目前多变和充满恶意的环境中，这是极具风险的，很难找到这样的可信第二方。

8．安全多方计算( SMC) ，是解决→组互不信任的参与方之间保护隐私的协同计算问题。

现有的许多密码工具都是安全多方计算的基础，SMC 的关键技术涉及到秘密分享与可验证秘密分享、门限密码学、零知识证明等多方面的内容。

① 秘密分享是一种分发、保存和恢复秘密的方法，是实现安全多方计算的一种重要工具。早期的方案中均假设所有参与方是诚实的，即秘密分享者Pi(l 《i《n) 所提供的秘密分片都是正确的，因此不能够抵抗恶意攻击者的欺骗行为。能够对分发的秘密分片的正确性进行验证实现了可验证秘密分享(Verifiable Secret Sharing) 。如果系统中任何成员(包括外部成员)都可以验证秘密分片Si 的正确性，则称可公开验证秘密分享。

② 同态公钥密码体制：在SMC 技术所采用的各种密码算法中，一个重要的密码体制是具有同态性质的公钥密码体制。

③ 零知识证明：零知识证明是密码学中的一个基本方法，目的是使证明者P 向验证者V 证明自己拥有某个秘密，同时P 又不会向V 泄露该秘密的任何其他有用的信息。

④ 混合网协议：混合网(Mixnets/Mix Network) 是实现匿名发送的基本密码协议。

混合网由服务网的集合构成，原始信息输入混合同，通过多次秘密置换后再输出，隐藏了输出消息与发送方的关系，实现匿名消息发送。

9．在分布式环境下，数据匿名化的重点问题是:如何在通信时既能保证站点数据隐私不泄露，又可以收集得到足够的信息来满足数据挖掘规则的要求，从而使实现的数据匿名保护的利用率尽量高。

10．关联规则挖掘就是从大量的数据中挖掘出描述数据项之间相互联系的有价值的知识。关联规则挖掘可以发现存在于数据库中的项自或属性间的有意义的关系，这些关系是事先未知的且隐藏的，也就是说不能通过数据库的逻辑操作(如表的联接)或统计的方法得出。

① 水平分布下关联规则挖掘的隐私保护算法：数据水平分布的关联规则挖掘的目的是寻找全局关联规则。

② 垂直分布下关联规则挖掘的隐私保护算法：数据垂直分布下的关联规则挖掘的关键在于项集中的项分布在不同站点，需要在这样的情况下计算项集的支持度。

在数据垂直划分的分布式环境中，需要解决的问题是:如何利用分布在不同站点的数据计算项集（item set)计数，找出支持度大于阙值的频繁项集。

11．聚类是对记录进行分组，把相似的记录分在闰一个聚簇里，主要是使得属于同一聚簇的个体的差异尽可能小，而个体差异在不同聚簇之间尽可能大。

12．数据匿名化一般采用两种基本操作，一种是抑制(Suppression) ，即不发布某些数据项:另一种是泛化(Generalization) ，即对数据进行更概括、抽象的描述。

13．数据匿名化所处理的原始数据，如医疗数据、统计数据等，一般为数据表形式；几种常见的针对匿名化模型的攻击方式：链接攻击、同质攻击、相似性攻击、背景知识攻击。

链接攻击：某些数据集存在其自身的安全性，即孤立情况下不会泄露任何隐私信息，但是当恶意攻击者利用其他存在属性重叠的数据集进行链接操作，便可能唯一识别出特定的个体，从而获取该个体的隐私信息。

同质攻击：当通过链接攻击仍然无法唯一确认个体，但是却存在个体对应的多条记录拥有同一个敏感隐私信息，从而造成隐私的泄露，称这一过程为同质攻击。

相似性攻击：由于敏感信患往往存在敏感度类似的情况，攻击者虽然无法唯一确定个体，但如果个体对应的多条记录拥有相似敏感信息，便能够推测出个体的大概隐私情况。

背景知识攻击：如果攻击者掌握了某个体的某些具体信息，通过链接攻击后即使只能得到某个体对应的多条信息记录，并且记录间的敏感属性也完全不同或不相似，但攻击者却能够根据所掌握的背景知识，从多条信息记录中找出唯一对应的信息记录，从而获取到该个体的隐私信息。

14．目前提出的匿名化方法主要通过泛化和抑制操作来实现。

① 泛化：泛化的基本思想是用更一般的值来取代原始属性值。通常泛化可分为两种类型:域泛化和值泛化。

② 抑制：抑制又成隐匿，是指用最一般化的值取代原始属性值。

15．数据匿名化算法：

① 基于通用原则的匿名化算法；

② 面向特定应用的匿名化算法；

③ 基于聚类的匿名化算法。

16．隐私保护技术在保护隐私数据的同时，需要最大可能地保证数据的可用性，即保证数据对实际应用的价值。

17．隐私的度量方法：通常从披露风险和信息缺损两个角度对稳私保护的效果进行度量。

① 披露风险：现有的隐私度量都可以统一用"披露风险" (Disc1osure Risk) 来描述。披露风险表示为攻击者根据所发布的数据和其他背景知识(Background Knowledge) 可能披露隐私的概率。通常，关于隐私数据的背景知识越多，披露风险越大。

② 信息缺损：信息缺损表示经过隐私保护技术处理之后原始数据的信息丢失量，是针对发布数据集质量的一种度量方法。

18．隐私保护技术需要遵循最小信息缺损原则；信息缺损越小，说明发布的数据集有效性越高，数据越有价值。

19．隐私保护算法可以从下列方面进行评价和比较：

① 隐私保护度：隐私保护度是站在隐私保护的角度对隐私保护算法进行评估，该算法如何能够最大限度地防止入侵者非法获取隐私数据，对隐私进行有效的保护。

② 数据有效性：数据有效性是指隐私保护算法在处理数据的时候，对原始信息的修改使得挖掘结果，也即最终得出的全局关联规则，与原始数据之间关系的匹配程度。数据缺损的越多，信息丢失的越多，数据的有效性就会越差。

③ 算法复杂度：算法的复杂度一般指算法的时间复杂性和空间复杂性，即算法的执行时间和进行数据处理时消耗的系统资源，可以说算法复杂度是直接与计算效率相关的一条重要标准。

算法复杂性的高低主要体现在所需要的系统资源上。所需资源越多，该算法的复杂性就越高。

④ 算法扩展性：算法扩展性指隐私保护算法在处理海量数据集或者数据量急剧增大时的应变能力。算法扩展性的好坏直接反映在当所处理的数据量突然增多的时候，算法的处理效率是否受到剧烈的影响。显而易见，一个扩展性好的隐私保护算法在数据量增大的同时，其处理效率的变化应该是相对缓慢的。

【备考点拨】

了解并理解相关知识点内容。

## 第6章：网络安全技术与产品

### 考点1、网络安全需求分析与基本设计

【考法分析】

本考点主要是对网络安全需求分析与设计相关内容的考查。

【要点分析】

1．网络安全在维基百科的定义是，网络安全包括网络设备安全、网络信息安全、网络软件安全。

2．网络安全的目标就是要实现信息系统的基本安全特征（即网络安全基本属性），并达到网络通讯所需的保障级别。

3．网络安全的基本属性包括机密性、完整性、可用性、可追究性、抗否认性。

4．安全威胁分为网络基础设施威胁、网络主机（服务）威胁、网络客户的安全威胁。也可分为网络内部威胁、网络外部威胁。

5．网络安全需求包括：安全服务、安全机制、技术管理以及在系统上的合理部署和关系配置。

6．在ISO的安全体系结构中包含：安全服务（Security Service）、安全机制（Security Mechanism）、安全管理（Security Management）

7．网络安全体系结构包含：安全服务、协议层次、系统单元；安全服务包括：认证、访问控制、数据完整性、数据保密性、抗抵赖、审计、可用性；系统单元分为：物理环境、应用平台、系统平台、网络平台、通讯平台。

8．协议层次是互联网的TCP/IP协议的基础；物理层设计在物理通信道上传输原始比特； 链路层分为介质访问控制和逻辑链路控制；网络层负责将数据从物理链接的一端传递到另一端；传输层的主要目的在于弥补网络服务与用户需求之间的差距；应用层想用户提供最常用且通用的应用程序。

9．网络安全防护系统的设计与实现应按照一下原则：最小权限原则；纵深防御原则；防御多样性原则：存在技术和防御两方面；网络安全的整体性原则；安全性评价与平衡原则；标准化与一致性原则。

10．校园网络安全构成威胁的因素很多，包括对网络硬件设备的破坏；窃取和干扰网络传输媒介上承载的信号；对邮件服务器进行攻击；针对应用服务器的攻击；管理者和使用者的威胁。

11．校园网络需要组合必要的安全设备和安全服务来构建网络安全系统，提供路由安全、路由过滤、防火墙、IDS、VPN、电子邮件安全、Web安全。

12．防火墙的设置应该满足如下原则：防火墙应该尽可能设置在网络最终出口和入口的校园网边界；除了网络防火墙设置在网络入口点之外，某些情况可能也需要将防火墙设置在校园网内部；防火墙不应该与其他的网络设备，比如路由器并行设置。

【备考点拨】

了解并理解相关知识点内容。

### 考点2、网络安全产品的配置与使用

【考法分析】

本考点主要是对网络安全产品的配置相关内容进行考查。

【要点分析】

1．网络流量状况是网络中的重要信息，可以实现如下目标：负载检测；性能分析；网络纠错；网络优化；业务质量监视；用户流量计费；入侵检测；协议调测。

2．流量监控对于网络性能分析、异常检测、链路状态检测、容量规划等发挥重要作用。

3．流量监控的内容：流量大小；吞吐量；带宽情况；时间计数；延迟情况；流量故障。

4．网络流量检测计数包括：基于数据采集探针的流量监控技术、基于SNMP/RMON的流量监控技术、基于Netflow/sFlow的流量监控技术、基于实时抓包的流量监控技术。

5．数据采集探针是专门用于获取网络链路流量数据的硬件设备。SNMP是TCP/IP的标准网络管理协议；RMON协议是对SNMP标准的扩展。NetFlow是基于Cisco提供的Netflow机制实现的网络流量信息采集；是Cisco专属协议，已经标准化。sFlow也是一种嵌入在路由器或交换机内的基于抽样的流量检测技术。

6．流量监控系统的评价标准：有效性、可靠性、实时性。网络流量监控分析的基础是协议行为解析分析，包含协议描述、协议行为解析。

7．Sniffer称为嗅探器，基于被动侦听原理的网络分析方式，能快速定位网络故障，并能捕获网络故障数据包，帮助网管人员分析和处理故障数据包。

8.Wireshark是一款免费开源的协议解析器，目前世界范围应用最广泛的网络协议解析软件

Wireshark能够在网康接口处捕捉数据包

9．NBAR是在CiscoISO12.0（5）XE2中引用的一个功能，它查看数据包的前512字节，可以检测识别各种应用协议，包括静态端口的、非TCP/IP的IP层协议、使用动态端口的、伪装其他端口的。

10．NRTG用户定义的定制应用程序分类，而多路由器流量图MRTG是基于SNMP的监控网络链路流量负载的工具软件，利用它可以从所有运行SNMP协议的设备上抓取信息，以非常直观的方式显示给用户，而且好用的系统资源较小。

【备考点拨】

了解并理解相关知识点内容。

### 考点3、网络安全风险评估实施

【考法分析】

本考点主要是对网络安全风险评估实施的相关内容进行考查。

【要点分析】

1．网络安全风险评估基本原则：标准性原则、可控性原则、最小影响原则。

2．识别阶段是风险评估工作的重要工作阶段，对组织和信息系统中资产、威胁、脆弱性等要素的识别，是进行信息系统安全风险分析的前提。

3．在风险评估工作中，风险的重要因素都已资产为中心，威胁、脆弱性以及风险都是针对资产而客观存在的。

4．威胁利用资产自身脆弱性，是的安全事件的发生成为可能，从而形成了安全风险。

5．把资产分为硬件、软件、数据、服务、人员、其他。

6．威胁分类方法：软硬件故障、物理环境影响、无作为或者操作实物、管理不到位、恶意代码、越权或滥用、网络共计、物理共计、泄密、篡改、抵赖。

7．根据威胁产生起因、表现、后果，分为：有害程序、网络攻击、信息破坏、信息内容攻击、设备设施故障、灾害性破坏、其他威胁。

8．威胁调查工作包括：威胁源动机及其能力、威胁途径、威胁可能性及其影响。

9．脆弱性是资产自身存在的，本身不会对资产造成损害；脆弱性可从技术、管理两个方面进行识别。

10．脆弱性识别所采用的方法：文档查阅、问卷调查、人工核查、工具检测、渗透测试。

11．风险评估是以围绕被评估组织核心业务开展为原则的，评估业务所面临的安全风险。

12．风险分析的主要方法是对业务相关的资产、威胁、脆弱性、其他各项属性的关联分析

13．风险分析模型：

威胁识别 → 威胁出现的频率 → 安全事件的可能性 → 风险值；

脆弱性识别 → 脆弱性的严重程度 → 安全事件的可能性、造成的损失 → 风险值；

资产识别 → 资产价值 → 安全事件造成的损失 → 风险值。

14．风险分析分为定性、定量，一般风险计算多采用定性计算方法。

15．风险处置方式一般包括接受、消减、转移、规避。

16．安全整改：非常严重、需立即降低且加固措施易于实施的安全风险，建议被评估组织立即采取安全整改措施；非常严重、需立即降低，但加固措施不便于实施的安全风险，建立被评估组织立即制定安全整改实施方案，尽快实施安全整改，整改前应对相关安全隐患进行严密监控，并做好应急预案。比较严重、需降低且加固措施不易于实施的安全风险，建议被评估组织指定限期实施的整改方案，整改前应对相关安全隐患进行监控。

【备考点拨】

了解并理解相关知识点内容。

### 考点4、网络安全防护技术的应用

【考法分析】

本考点主要是对网络安全防护技术的应用相关内容进行考查。

【要点分析】

1．安全漏洞扫描技术是一类重要的网络安全技术，与防火墙、入侵检测系统相互配合，能有效提高网络的安全性。

2．网络安全漏洞扫描技术基于Internet远程检测目标网络或本地主机安全性脆弱点的技术。

3．一次完整的网络安全漏洞扫描分为：

第一阶段：发现目标主机或网络；

第二阶段：发现目标后进一步搜集目标信息；

第三阶段：根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。

4．网络安全漏洞扫描技术包括有PING扫射、操作系统探测、如何探测访问控制规则、端口扫描、漏洞扫描。

5．PING扫描用于网络安全漏洞扫描的第一阶段；操作系统探测、如何探测访问控制规则和端口扫描用于第二阶段；网络安全漏洞扫描第三阶段。

6．Telnet到远程主机时三次握手机会：

第一步：一台计算机首先请求和另一台计算机建立连接；

第二步：接收到SYN请求的计算机响应发送来的序列号；

第三步：发起连接请求的计算机对收到的序列号做出应答。

7．从扫描器的探测功能分为：① 网络扫描器，基于Internet远程检测目标网络和主机系统漏洞的程序，如提供网络服务、后门程序、密码破解、阻断服务等的扫描测试；② 主机扫描器；③ 服务扫描器；④ 数据库扫描器；⑤ 专用扫描器。

8．网络安全漏洞的防御：采用网络防火墙抵御由于网络内存在的安全漏洞而存在的潜在网络攻击，通过防火墙过滤不安全的服务而降低风险；具体可体现在以下方面：强化网络安全策略；监控审计；防止内部信息泄露；数据包过滤；网络地址转换；虚拟专用网络。

9．VPN被定义为通过一个公用网络建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。

10．VPN四种技术保证安全：隧道技术、加解密技术、密钥管理技术、使用者与设备身份验证技术。

11．服务提供商提供虚拟电路来建立IPVPN服务。

18．高层安全协议可以提供应用层安全。

19．SOCKS是一个网络连接的代理协议，处于OSI模型的会话层，将连接请求进行鉴别和授权。

20．安全套接字属于高层安全机制，SSL是一个端到端协议，因而是在处于通讯通路通路端点的机器上实现，而不需要在通信通路的中间节点上实现。

21．S-HTTP是安全HTTP协议的安全扩展，它提供身份认证，也可以提供数据加密。

22．安全的多用途因特网邮件扩展可以被看作一个特殊的雷士SSL的协议。

23．第二隧道协议就是OSI模型中的数据链路层的安全协议，有PPTP 和 L2F 和L2TP，主要是为了组建远程访问VPN而提出。

24．IPSec是IETF正在完善的安全标准，它把几种安全技术结合在一起形成一个较为完整的体系，通过对数据加密、认证、完整性检查来保证数据传输的可靠性、私有性、保密性。

25．基于多协议标记交换的IPVPN是面向非连接的IP网络，可以像帧中继和提供IP服务级别一样具有保密性。

26．容灾备份系统指在相隔较远的异地，建立2套或多套功能相同的IT系统。

27．灾难恢复计划包括：数据保护、灾难防备、事后恢复

28．在建立容灾备份系统时会涉及到多种技术，如远程镜像技术、快照技术、基于IP的SAN互连技术。

29．远程镜像技术往往同快照技术结合起来实现远程备份，即通过镜像把数据备份到远程存储系统中，再用快照技术把远程存储系统中的信息备份到远程的磁带库、光盘库中。

30．快照是通过软件对要备份的磁盘子系统的数据快速扫描，建立一个要备份数据快照逻辑单元号LUN和快照cache。

31．互连技术即通过光钎通道FC，把2个SAN连接起来。

32．增量备份分为差别备份和累积备份；差别备份是从上次备份后修改过的文件的拷贝；累积备份是从上一个完全备份后被修改的全部文件拷贝。一周备份设计：周日完全备份，周1、2、3差别备份，周4累积备份，周5、6差别备份。恢复：首先恢复上周日完全备份，再恢复周4累积备份，再恢复周5/6。

33．异地备份“一个三”“三个不原则“：备份到300公里外；不能在同一地震带、不能在同地电网、不能在同一江河流域。

34．日志分析审计要求包括：记录与再现、入侵检测、记录入侵行为、威慑作用和系统本身的安全性。

35．日志分析方法包括：人工分析；计算机手工分析；处理审计记录并与分析人员最后决策相结合的半自动；依靠专家系统做出判断结果的自动化的智能分析。

36．正则表达式分析方法可以让用户通过一系列的特殊字符构建匹配模式。

37．关联规则挖掘问题就是通过用户指定最小支持度、最小可信度。

38．聚类分析也叫分类分析，基本思想是:我们所研究的样品之间存在程度不同的相似度。

【备考点拨】

了解并理解相关知识点内容。

## 第7章：信息系统安全工程

### 考点1、访问控制

【考法分析】

本考点主要是对访问控制相关内容的考查。

【要点分析】

1．基于角色的访问控制设计，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，以简化用户的权限管理，减少系统的开销。

2．Kerberos协议：在一个开放的分布式网络环境中，用户通过工作站访问服务器上提供的服务。服务器应该能够限制非授权用户的访问并能认证对服务的请求。工作站不能够被网络服务所信任其能够正确地认定用户，即工作站存在三种威胁：一个工作站上一个用户可能冒充另一个用户操作；一个用户可能改变一个工作站的网络地址，从而冒充另一台工作站工作；一个用户可能窃听他人的信息交换，并回放攻击获得对一个服务器的访问权或中断服务器的运行。上述问题可以归结为一个非授权用户能够获得其无权访问的服务或数据。Kerberos是标准网络身份认证协议，旨在给计算机网络提供“身份认证”。它是基于信任第三方，如同一个经纪人集中地进行用户认证和发放电子身份标识。

3．Kerberos系统应该满足的要求：① 安全；② 可靠；③ 透明；④ 可伸缩。

4．Kerberos设计思路及问题：使用一个（或一组）独立的认证服务器（Authentication Server，AS），来为网络中的用户（C）提供身份认证服务；认证服务器（AS），用户口令由AS保存在数据库中；AS与每个服务器（V）共享一个唯一保密密钥（Kv）（已被安全分发）。上述的协议问题就是：口令明文传送会被窃听。票据的有效性（多次使用）。访问多个服务器则需多次申请票据（即口令多次使用）。解决上述问题，Kerberos协议使用票据重用和引入票据许可服务器（Tickert Granting Server，TGS）。

5．口令猜测技术包括：① brute force（暴力攻击）；② 字符频率分析；③ 彩虹表；④Dictioingary Attack（字典攻击）；⑤ 基于概率的口令猜测；⑥ JTR：John the Ripper是目前最为流行的口令破解工具之一，是开源软件，可以在其官网上免费下载；⑦HASHCAT：HashCat是世界上最快的基于CPU的口令破解工具。

6．用户身份认证是信息系统的第一道安全防线，用户名—口令机制则是身份认证中最常用的方法。但是口令机制具有易懂、易用和易于实现的特点，这使得口令机制在今后一段时间依然是用户身份认证的一个重要方法。

【备考点拨】

了解并理解相关知识点内容。

### 考点2、信息系统安全的需求分析与设计准则

【考法分析】

本考点主要是对信息系统安全的需求分析及设计准则相关内容的考查。

【要点分析】

1．信息系统安全需求分析：设计源于需求，需求源于目标。

2．安全需求分类方法中，安全目标的关键就是实现安全的三大要素：机密性、完整性、可用性。

3．针对每一个安全属性，作为一个仅供参考的指导原则，潜在威胁影响可以进行适当地定级，并简单分为三个级别：① 低（Low，L）；② 中（Moderate，M）；③ 高（High，H）。

4．一般而言，大型网络信息系统面临着两方面的安全挑战：① 组织内的信息技术环境威胁；② 信息系统的系统安全管理问题。

5．一般而言，信息安全的理论研究设计一下基本属性：机密性、完整性、可用性、真实性、可审计性、抗抵赖性、可靠性等。安全需求的目标就要确保信息系统有足够的保护措施以达到这些基本属性，所以这些基本属性也称为安全目标。

6．组织体系结构（Enterprise Architecture，EA），也可译为“组织架构”或者“企业架构”。是用于帮助组织理解其自身的构造及运作方式的一种管理工具。通过EA的管理框架，组织可以合理有序地把安全考虑加入信息系统开发生命周期（System Development Life-Cycle，SDLC）里，在整个SDLC过程中进行组织内部信息系统的安全目标分析、安全风险评估、安全保护等级确认、安全保护措施选择、安全区域职责划分、安全事故处理、安全责任追究时，可以提供更全面、切实的参考。

7．安全信息系统的设计过程遵循信息系统开发生命周期（Information System Development Life Cycle,SDLC）进行。除此之外，还特别在设计过程中引入安全考虑，“信息系统安全开发生命周期”（Information Security Considerations of SDLC，TSC of SDLC）。

8．信息系统安全体系（Information Systems Security Architecture ，ISSA），包括信息系统安全技术体系、安全管理体系、安全标准体系和安全法律法规。

9．首先是安全法律法规与政策。解决系统安全第一步，要弄清楚系统可以提供什么样的服务，即业务需求。在设计安全系统之前，相关部门可对这个系统进行安全评估。

10．从技术角度而言，通用的安全技术体系包括以下模块：① 信息系统硬件安全；② 操作系统安全；③ 密码算法技术；④ 安全协议技术；⑤ 访问控制；⑥ 安全传输技术；⑦ 应用程序安全；⑧ 身份识别与权限管理技术；⑨ 入侵检测技术和防火墙技术。

同时，对于不同的信息系统，根据其应用场景与业务的不同，会对一部分的安全技术更为关注。

11．信息系统的安全管理体系，主要包括：① 安全目标确定；② 安全需求获取与分类；③ 风险分析与评估；④ 风险管理与控制；⑤ 安全计划制定；⑥ 安全策略与机制实现；⑦ 安全措施实施。

12．目前我国现有的信息系统安全标准体系可分为基础类、应用类、产品类。

13．《信息安全开发生命周期中的安全考虑指南》介绍了把安全纳入信息系统开发生命周期的所有阶段的框架：安全依据 → 初始阶段 → 设计阶段 → 实施阶段 → 运维阶段 → 最终处理阶段。

14．安全考法包括两部分内容，分别是控制开发和安全编码。安全控制是为了应对风险。

15．一般的信息系统的实际需求包括安全、方便、易操作、易维护和控制等，信息系统也不例外。在设计信息系统这类大型分布式系统时，通常会尽量避免过度使用基于密码的保护措施，因为使用密码难免导致数据处理速度变慢。

16．封闭式系统安全实现途径的特征主要有两点：一是由多个防火墙的组合来创建一个封闭的系统；二是使用入侵检测系统对封闭系统进行适时的威胁监视。

17．开放式系统的绝对安全保护很难实现。系统最容易出现的是软件漏洞，这往往也是最难进行检测的。从以往的经验看，攻击者一般都不会花时间去破解密码、攻击防火墙，而是找软件漏洞。软件漏洞有很多是编程者为了方便测试而留下的后门，但最后却没有删掉。操作系统的软件漏洞比较明显。

18．一般来说，需要综合应用密码保护、网络安全、操作系统保护以及编程语言系统保护这4种类型才能实现整个系统的安全。

19．要实现系统的安全，也不能仅从技术角度考虑，而是需要寻找一个平衡点，根据要保护的数据信息的价值来决定其平衡点，这个平衡包括安全、速度和成本等多方面的均衡。要寻找这一平衡点，要从以下3个方面进行综合考虑：① 风险分析；② 安全策略；③ 安全架构。

20．一般可以从以下6个方面来考虑企业信息系统安全：① 物理安全；② 网络安全；③主机安全；④ 数据安全；⑤ 独立评估；⑥ 安全应急机制。

【备考点拨】

了解并理解相关知识点内容。

### 考点3、信息系统安全产品的配置与使用

【考法分析】

本考点主要是对信息系统安全产品的配置与使用的考查。

【要点分析】

1．启用Windows自带防火墙。进入“控制面板 → 系统和安全 → Windows防火墙”。

2．在linux系统中，用户账号是用户的身份标志，它由用户名和用户口令组成。系统将用户名存放在/etc/passwd文件中，而将口令以加密的形式存放在/etc/shadow文件中。

3． /etc/passwd文件介绍：

一般/etc/passwd中一行记录对应着一个用户，每行记录又被冒号(:)分隔为7个字段，其格式和具体含义如下：

用户名:口令:用户标识号:组标识号:注释性描述:主目录:登录Shell；

用户名(login\_name)：是代表用户账号的字符串。通常长度不超过8个字符，并且由大小写字母和/或数字组成。登录名中不能有冒号(:)，因为冒号在这里是分隔符。为了兼容起见，登录名中最好不要包含点字符(.)，并且不使用连字符(-)和加号(+)打头。

口令(passwd)：一些系统中，存放着加密后的用户口令字。虽然这个字段存放的只是用户口令的加密串，不是明文，但是由于/etc/passwd文件对所有用户都可读，所以这仍是一个安全隐患。因此，现在许多Linux系统（如SVR4）都使用了shadow技术，把真正的加密后的用户口令字存放到/etc/shadow文件中，而在/etc/passwd文件的口令字段中只存放一个特殊的字符，例如“x”或者“\*”。

用户标识号(UID)：是一个整数，系统内部用它来标识用户。一般情况下它与用户名是一一对应的。如果几个用户名对应的用户标识号是一样的，系统内部将把它们视为同一个用户，但是它们可以有不同的口令、不同的主目录以及不同的登录Shell等。取值范围是0-65535。0是超级用户root的标识号，1-99由系统保留，作为管理账号，普通用户的标识号从100开始。在Linux系统中，这个界限是500。

组标识号(GID)：字段记录的是用户所属的用户组。它对应着/etc/group文件中的一条记录。

注释性描述(users)：字段记录着用户的一些个人情况，例如用户的真实姓名、电话、地址等，这个字段并没有什么实际的用途。在不同的Linux系统中，这个字段的格式并没有统一。在许多Linux系统中，这个字段存放的是一段任意的注释性描述文字，用做finger命令的输出。

主目录(home\_directory)：也就是用户的起始工作目录，它是用户在登录到系统之后所处的目录。在大多数系统中，各用户的主目录都被组织在同一个特定的目录下，而用户主目录的名称就是该用户的登录名。各用户对自己的主目录有读、写、执行（搜索）权限，其他用户对此目录的访问权限则根据具体情况设置。

登录Shell(Shell)：用户登录后，要启动一个进程，负责将用户的操作传给内核，这个进程是用户登录到系统后运行的命令解释器或某个特定的程序，即Shell。Shell是用户与Linux系统之间的接口。Linux的Shell有许多种，每种都有不同的特点。常用的有sh(BourneShell),csh(CShell),ksh(KornShell),tcsh(TENEX/TOPS-20typeCShell),bash(BourneAgainShell)等。系统管理员可以根据系统情况和用户习惯为用户指定某个Shell。如果不指定Shell，那么系统使用sh为默认的登录Shell，即这个字段的值为/bin/sh。

4．/etc/shadow文件介绍：

  /etc/shadow文件格式与/etc/passwd文件格式类似，同样由若干个字段组成，字段之间用“:”隔开。

文件中字段主要含义为：登录名:加密口令:最后一次修改时间:最小时间间隔:最大时间间隔:警告时间:不活动时间:失效时间:标志 ；

“登录名”是与/etc/passwd文件中的登录名相一致的用户账号；

“口令”字段存放的是加密后的用户口令字：如果为空，则对应用户没有口令，登录时不需要口令；星号代表帐号被锁定；双叹号表示这个密码已经过期了；$6$开头的，表明是用SHA-512加密；$1$表明是用MD5加密；$2$ 是用Blowfish加密；$5$ 是用 SHA-256加密；

“最后一次修改时间”表示的是从某个时刻起，到用户最后一次修改口令时的天数。时间起点对不同的系统可能不一样。例如在SCOLinux中，这个时间起点是1970年1月1日；

“最小时间间隔”指的是两次修改口令之间所需的最小天数；

“最大时间间隔”指的是口令保持有效的最大天数；

“警告时间”字段表示的是从系统开始警告用户到用户密码正式失效之间的天数；

“不活动时间”表示的是用户没有登录活动但账号仍能保持有效的最大天数；

“失效时间”字段给出的是一个绝对的天数，如果使用了这个字段，那么就给出相应账号的生存期。期满后，该账号就不再是一个合法的账号，也就不能再用来登录了。

5．用户标识号(UID)是一个整数，系统内部用它来标识用户。其取值范围是0-65535。0是超级用户root的标识号，1-99由系统保留，作为管理账号，普通用户的标识号从100开始。在Linux系统中，这个界限是500。

6．MySQL具有的高性能、高可靠性、易用性及开源免费的特点。

【备考点拨】

了解并理解相关知识点内容。

### 考点4、信息系统安全测评

【考法分析】

本考点主要是对信息系统安全测评相关内容的考查。

【要点分析】

1．信息系统安全是指对信息系统及其处理的信息采取适当的安全保障措施，防止未授权的访问、使用、泄露、中断、修改、破坏，从而确保信息系统及其信息的机密性、完整性和可用性，保证信息系统功能的正确实现。

2．信息系统安全测评是依据信息安全测评的要求，在风险评估的基础上，对在信息系统生命周期中采取的技术类、管理类、过程类和人员类的安全保证措施进行测评和检查。

3．信息系统是由信息技术系统以及包含了人、管理、环境的运行环境组成。对信息系统的安全保障的评估，首先需要根据信息系统运行环境及相关的信息系统安全保障需求进行描述，信息系统安全测评准则提供了对安全保障需求描述的公共语音、结构和方法，这就是信息系统安全保障要求（ISPP）；然后就可以依据信息安全保障要求（ISPP）编制满足用户需求的信息系统安全保障方案（ISST）对信息系统安全保障要求（ISPP）的负荷情况进行评估，并在整个信息系统生命周期中对信息系统安全保障方案的执行情况和执行能力进行评估，最终确定组织机构的信息系统安全保障能力的级别。

4．信息系统安全测评的基本原则：① 标准型原则；② 关键业务原则；③ 可控性原则。

5．根据机密性、完整性和可用性特征以及信息和信息系统价值，可以将信息系统划分为5类；一般将信息系统的威胁分为7级。

6．模糊测试（Fuzzing）是一种黑盒测试技术，它将大量的畸形数据输入到目标程序中，通过监测程序的异常来发现被测试程序中可能存在安全漏洞。模糊测试的思想相对较简单直观，易于实现自动化，并且运用其发掘软件安全漏洞，从漏洞发现到重现和定位漏洞比较容易，不存在漏洞误报，目前正广泛应用于对文件格式、网络协议、Web程序、环境变量和COM对象等的安全测试中。模糊测试技术是一种发掘安全漏洞的有效方法。

7．模糊测试是一种基于去屑注入的自动化测试技术，没有具体的执行规则，旨在预测软件中可能存在的错误以及什么样的输入疯狗出发错误。与基于源代码的白盒测试相比，模糊测试的测试对象是二进制目标文件。

8．完整的模糊测试都要经历以下几个基本的阶段：识别目标 → 识别输入 → 生产模糊测试数据 → 执行模糊测试数据 → 监视异常 → 确定可利用性。

9．模糊器划分为随机模糊器、基于变异的模糊器和基于生成技术的模糊器。

10．为了避免产生大量的无效的测试数据，基于变异的模糊器使用样本文件来得到畸形数据集合。

11．基于生成技术的模糊器是当前应用范围最广的一类模糊器。

12．目前模糊测试对象主要有以下五类：① 环境变量和参数；② Web应用程序和服务器；③ 文件格式；④ 网络协议；⑤ Web浏览器。

13．模糊测试的优点：第一，模糊测试不需要程序的源代码即可发现问题。第二，模糊测试不受限于被测系统的内部实现细节和复杂程度。第三，使用模糊测试的可复用性较好，一个测试用例可适用于多种产品。

14．模糊测试有两个关键的操作：产生畸形数据和观察应用程序是否出现异常。但进行两个操作时存在如下问题：首先，目前理论上还未出现能成熟、优化生成畸形数据的方式。其次，需要有一个监控器观察应用程序是否出现异常。

15．代码审计工具帮助软件开发团队快速查找、定位、修复和管理软件代码安全问题。

16．静态代码★分析是软件缺陷检测的重要方法，是指在不执行程序的情况下，以程序源代码、可执行文件序列或高级语言中的中间代码等为对象，通过预先定义属性规约，自动地检查目标代码对属性规约的违反情况。

17．安全代码审计的第一步就是对每一个源代码文件的所有者分配权限、相关所有文件等建立一个数据库；下一步就是明确评审优先级。

18．从方法论的角度出发，宏观来看代码审计的主要方法可分为自顶向下、自底向上和两者结合的三种方法。

19．代码静态分析采用的方法★主要有模式匹配、定理证明、模型检测。

20．模式匹配主要步骤是依据统计及经验，定义和抽象缺陷及错误特征，对目标代码采用行走检查、模式匹配等方法过滤已知缺陷。

21．定理证明是代码形式化验证的重要技术，也属于静态代码分析的范畴。定理证明技术是将软件系统和性质都用逻辑方法来规约，通过基于公里和推理规则组成的形式系统，以定理证明的方法来证明软件系统是否具备所期望的关键性质。

22．模型检测是今年来研究的热点。该技术是通过搜索待验证软件系统模型的有穷状态空间来检验系统的行为是否具备预期性质的一种有穷状态系统自动验证技术。

23．信息系统安全评测由三个阶段组成：① 安全评估阶段；② 安全认证阶段；③ 持续监督阶段。

24．信息系统安全评估阶段按工作内容又划分几个子阶段：静态评估阶段、现场检测阶段、综合安全评估阶段。

25．在静态评估阶段信息系统资产所有者提出申请，与系统评估方签署协议，所有者提交文档，所有者为主提出评估对象的保护轮廓。

26．在现场检测阶段，评估项目组前往信息系统运行现场进行实地检测。

27．在综合安全评估阶段，现场检测工作结束后，项目组对检测数据和结果进行分析，完成《信息系统安全现场核查报告》及《信息系统安全测试报告》。

28．通过安全评估的信息系统将进入安全认证阶段，首先信息系统需要试运行6个月，评估机构将派出工作人员进行复审，并向认证委员会出示复审报告。认证委员会依据前面各个阶段报告做出认证决定，认证机构将对通过认证的信息系统签发认证证书。

29．认证监督阶段的三方面工作：① 配置管理和控制；② 对安全保证措施的监督检查；③ 认证监督决定。

【备考点拨】

了解并理解相关知识点内容。

## 第8章：应用安全工程

### 考点1、Web安全的需求分析与基本设计

【考法分析】

本考点主要是对web安全需求分析与基本设计的考查。

【要点分析】

1．2013年版本的OWASP（开源Web应用安全项目） TOP10包括的十大最有可能发生的应用漏洞：① 注入攻击：攻击者通过在应用程序预先定义好的查询语句结尾加上额外的查询语句元素，欺骗数据库服务器执行非授权的任意查询；② 失效的身份认证和会话管理；③ 跨站脚本(XSS)：当用户不小心单击这样带有恶意代码的链接时，其用户信息就有可能被攻击者盗取；④ 不安全的直接对象引用；⑤ 安全配置错误：许多设置的默认值并不是安全的；⑥ 敏感信息泄露；⑦ 功能级访问控制缺失；⑧ 跨站请求伪造(CSRF)：一个跨站请求伪造攻击迫使登录用户的浏览器将伪造的HTTP请求，包括该用户的会话cookie和其他认证信息，发送到一个存在漏洞的web应用程序。这就允许了攻击者迫使用户浏览器向存在漏洞的应用程序发送请求；⑨ 使用更含有已知漏洞的组件；⑩ 未验证的重定向和转发。

2．可以从以下几个方面来避免漏洞攻击：① 常使用自带的安全的API；② 如果没法使用一个参数化的API，那么你应该使用解释器具体的escape语法来避免特殊字符；③ 加强对用户输入的验证。

3．对于失效的身份认证和会话管理的防范，我们可以从以下方面来着手：① 一套单一的强大的认证和会话管理控制系统；② 区分公共区域和受限区域；③ 锁定账户和禁用帐户策略；④ 保护身份验证Cookie；⑤ 口令、会话时限。

【备考点拨】

了解并理解相关知识点内容。

### 考点2、电子商务安全的需求分析与基本设计

【考法分析】

本考点主要是对电子商务安全的需求分析与设计相关内容的考查。

【要点分析】

1．电子商务系统具有自身的特点：① 电子商务系统是支撑企业自身运营的基础平台；②电子商务系统是优化企业业务流程、降低经营成本的重要手段；③ 电子商务系统对实时性、安全性与可靠性要求较高；④ 电子商务系统大多是依托企业既有信息资源运行的系统。

2．电子商务系统是典型的三要素结构（业务系统、客户端展现、第三方支付）。

3．电子商务系统的设计开发的基本过程：传统软件开发设计过程遵循典型的瀑布模型，即需求分析、概要设计、详细设计、编码实现、测试分析、上线运维等阶段，这一模型对于电子商务系统而言同样适用。对于迭代开发、持续集成等敏捷软件开发模式而言，电子商务系统同样可以借鉴。电子商务系统的生命周期可以划分为立项规划、系统设计、开发集成、测试评估、运行维护五个阶段。

在电子商务系统规划阶段，首先需要确定企业未来的电子商务运作模式。

在电子商务系统设计阶段，需要在电子商务系统规划的基础上，确定整个电子商务系统体系结构中各个组成部分，重点是确定电子商务系统的功能、平台的基本功能和系统平台的构成。

需求需要哪些产品或者技术来构筑电子商务系统的平台，并完成应用软件系统的编码，最终将电子商务系统的应用软件和各种平台集成在一起。

在电子商务系统测试评估阶段，测试并分析系统的主要性能指标，优化系统的性能，提高系统的效率。

在电子商务系统运行维护阶段，包括电子商务系统的正常运转、维护和管理。

4．电子商务系统的基础设施安全需求包括如下方面：① 计算机硬件的安全性与可靠性；② 计算机网络的安全性；③ 操作系统的安全性；④ 数据库的安全性；⑤ 应用软件的安全性。

5．电子交易普遍存在着以下安全隐患：信息窃取；信息篡改；身份假冒；交易的否认。

6．电子商务系统中的电子交易安全需求包括以下几个方面：交易的真实性；交易的完整性；交易的保密性；交易的不可抵赖性。

7．电子商务系统安全架构从安全技术与安全管理两个层面为电子商务系统提供深度、多级、主动的安全防护，包括安全技术保障与安全管理运维两个部分。

安全技术保障包括交易安全、行为安全、数据安全、服务安全、网络安全和物理安全；安全管理运维包括安全治理、安全运维、安全评估和应急管理。

8．电子商务系统的安全技术包括物理环境安全、系统安全、网络安全、数据及支付安全等方面。

【备考点拨】

了解并理解相关知识点内容。

### 考点3、嵌入式系统的安全应用

【考法分析】

本考点主要是对嵌入式系统安全应用相关内容的考查。

【要点分析】

1．在一个嵌入式系统中使用Linux开发，经过如下过程：① 建立开发环境；② 配置开发主机；③ 建立引导装载程序。

2．磁卡是通过卡上磁条的磁场变化来存储信息的，而IC卡是通过嵌入卡中的电擦除式可编程只读存储器集成电路芯片来存储数据信息的。与磁卡相比较，IC卡具有明显优点。

3．基于智能卡的系统中可能存在很多潜在的功能要素。通常会有5~6个，包括持卡人、终端、数据持有者、发卡方、卡生产者以及卡软件开发方。

4．针对卡系统的各个功能要素，可以将攻击分为多种形式：① 终端对持卡人或数据拥有着的攻击；② 终端对发行商的攻击；③ 终端对卡生产商或卡系统软件的攻击；④ 持卡人对终端的攻击；⑤ 持卡人对数据拥有着的攻击；⑥ 持卡人对发行商的攻击；⑦ 持卡人对软件生产者的攻击；⑧ 发行商对持卡人的攻击；⑨ 发行商对终端的攻击；⑩ 多应用隔离。

5．增强对智能卡攻击的防范，可以通过加密硬件或采用更强的密码算法或协议。

① 加密硬件（发展趋势）；

② 功能合并（两个不同功能的合并，两者之间可能的攻击也就消失）。

6．现有智能终端操作系统主要包括Android、Windows Phone、iOS等。

7．Android是一种基于Linux的自由及开放源代码的操作系统，主要使用于移动设备。Android的系统架构采用了分层架构的思想，从上层到底层共包括四层，分别是：① 应用程序层；② 应用程序框架层；③ 系统库和Android运行时；④ Linux内核。

8． iOS系统是由苹果公司开发的移动操作系统。iOS的系统架构分为四个层次：① 核心操作系统层；② 核心服务层；③ 媒体层；④ 可触摸层。

9．Windows Phone 7架构基于Windows Embedded CE 6.0内核，主要包括三个组件区域：内核模式和用户模式组件（软件层）、硬件组件。

10．数据显示目前Android平台恶意软件主要有四种类型：① 远程控制木马；② 话费吸取类；③ 隐私窃取类；④系统破坏类。

11．手机系统的防范措施如下：① 不断增强手机安全防护意识；② 安装专业的安全防护软件；③ 不要随便安装不明的软件；④ 不要随便打开未知的链接；⑤ 二维码不要随便扫；⑥ 免费的Wifi有风险；⑦ 工作相关的文件资料不要存在手机中；⑧ 手机密码锁；⑨ 非必要不要Root手机。

【备考点拨】

了解并理解相关知识点内容。

### 考点4、数字水印在版权保护中的应用

【考法分析】

本考点主要是对数字水印技术相关内容的考查。

【要点分析】

1．数字水印技术是通过数字信号处理的方法，在数字化的多媒体数据中嵌入隐蔽的水印标记，可以应用于开放的网络环境下的多媒体数字作品的版权保护。

2．数据水印的应用领域包括以下几个方面：① 版权保护；② 加指纹；③ 标题与注释；④ 篡改提示；⑤ 使用控制。

3．数字版权保护系统必须满足以下基本应用需求：① 数字水印的隐蔽性；② 数字水印的鲁棒性；③ 数字水印的安全性。

4．基于数字水印的数字版权保护系统体系架构：任何一个数字水印算法都由水印、编码器（也称之为嵌入算法）及解码器和比较器（也称之为验证算法，还可以称之为提取算法或检测算法）这3部分组成。

5．数字水印的数字版权保护系统主要包括三部分：① 编码过程，通过在原始图像中嵌入具备版权标识的水印信息，生成可发布的水印图像；② 解码过程，通过对具体版权标识水印图像的检测，提取出嵌入的水印信息；③ 水印验证过程，通过对提取的水印信息和用户版权标识信息之间的对比分析，鉴定该作品的版权用户。

6．目前已有的数字水印算法主要包括以下几种：① 空域水印算法；② 变换域水印算法；③ 压缩域水印算法。

【备考点拨】

了解并理解相关知识点内容。

### 考点5、位置隐私保护技术的应用

【考法分析】

本考点主要是对位置隐私保护技术相关内容的考查。

【要点分析】

1．所谓个人位置隐私，是指由于服务或系统需要用户提供自身的“身份，位置、时间“三元组信息而导致的用户隐私泄露问题。目前，基于位置的服务LBS(Location-Based Services)吸引了众多的移动用户。

2．位置隐私保护体系可分为三种：集中式体系结构、客户—服务器体系结构和分布式体系结构。

集中式体系结构是指在移动用户和位置服务提供商之间设置一个可信第三方匿名服务器，因此也被称为可信第三方体系结构；

客户—服务器体系结构是指隐私保护操作直接在移动客户端进行，移动客户端将位置模糊化后的查询请求提交给位置服务提供商，位置服务提供商根据查询请求将候选结果集返回，移动客户端对候选结果集进行过滤以得到真实的查询结果；

分布式体系结构是指移动用户通过P2P方式与其他用户协作来实现位置隐私保护，无须依赖可信第三方。

3．通常情况下，被保护的属性主要包括用户的身份（ID）、空间信息（位置POS）和时态信息（时间Time）三类。

用户身份：用户的真实身份可以使姓名。

空间信息：空间信息指隐私保护的目标是移动用户的位置信息。

时态信息：在某些应用场景中，空间信息只有与当前的时间信息关联起来才是危险的。

4．位置隐私保护几种常见的保护方法：① 假名技术（位置假名和身份假名两个方向）；② 混合区（假名技术基础上）；③ k-匿名；④ 模糊空间和坐标变换；⑤ 信息加密：信息加密技术是最基本的安全防护方法；⑥ 位置分享：为了应对非可信位置服务提供商问题，位置分享将模糊化的位置信息分割成所谓的“份“，每“份”都有严格限制的位置精度。

取决于可访问的“份数”，客户端可以提供不同精度级别的位置信息。

5．基于k-匿名的位置隐私保护方案是当前的研究热点之一，在位置k-匿名模型下，每一个用户的位置以一个三元组表示（[x1,x2],[y1,y2],[t1,t2]）,其中（[x1,x2],[y1,y2]）表示移动用户所在的二维空间，[t1,t2]表示时间段。（[x1,x2],[y1,y2],[t1,t2]）描述了用户在[t1,t2]时间段的某一个时间点ti出现在（[x1,x2],[y1,y2]）所表示的二维空间的某一点。

所以攻击者只知道在此区域中有几个用户，具体哪个用户在那个位置无法确定。K值是由用户根据需求自己定义的。一般情况下，k值越大，匿名框也越大。

6．常用的三种位置k-匿名算法：

① 间隔匿名算法

基本思想为：可信第三方匿名服务器构建一个四叉树的数据结构，将二维空间用十字分成四个面积相等的正方形区区间，然后对每一个正方式再递归执行相同的操作。

② Hilbert匿名算法：也称为小集团算法(clique cloak)。

③ 连续查询匿名算法：在普通的匿名保护算法中，用户每次发起查询之后，第三方匿名服务器都通过匿名算法将用户泛化到有k个用户的匿名集AS中，使攻击者无法直接从匿名集AS中区分出真实用户。

【备考点拨】

了解并理解相关知识点内容。