信息安全答案

信息安全——关注信息本身的安全，以防止偶然的或

未授权者对信息的恶意泄露、修改和破坏，从而导致

信息的不可靠或无法处理等问题，使得我们在最大限

度地利用信息为我们服务的同时而不招致损失或使损

失最小。（定义1）

? 信息安全——防止任何对数据进行未授权访问的措

施，或者防止造成信息有意无意泄漏、破坏、丢失等

问题的发生，让数据处于远离危险、免于威胁的状态

和特性。（定义2）

? 网络安全——计算机网络环境下的信息安全。

信息安全的属性：? 保密性（Confidentiality）：

—保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

—信息不被泄露给未经授权者的特性。

? 完整性（Integrity）：

—保证数据的一致性，防止数据被非法用户篡改。

—信息在存储或传输的过程中保持未经授权不能改变的特性。

? 可用性（Availability）：

—保证合法用户对信息和资源的使用不会被不正当地拒绝。

—信息可被授权者访问并按需求使用的特性。

? 不可抵赖性（Non-repudiation）（又称：抗抵赖性或不可否认性）

---所有参与者都不可能否认或抵赖曾经完成的操作和承诺。

---建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。

? 可控制性（Controllability）：

---对信息的传播及内容具有控制能力

3. 常见的安全威胁有哪些？

安全威胁有时可以被分为故意的和偶然的：

故意的威胁如假冒、篡改等。（可以进一步分为主动攻击和被动攻击。被动攻击不会导致对系统中所含信息的任何改动，而且系统的操作和状态也不会改变。因此被动攻击主要威胁信息的保密性；主动攻击则意在篡改系统中所含信息、或者改变系统的状态和操作，因此主动攻击主要威胁信息的完整性、可用性和真实性。）

偶然的威胁如信息被发往错误的地址、误操作等。

非法访问

1）口令破解

2）IP欺骗

3）DNS欺骗

4）重放攻击

5）非法使用

6）特洛伊木马

4.“信息保障”(informationassurance，IA)概念是美国国防部于20世纪90年代率先提出的，后经多次修改、完善，已得到世界范围的广泛认可。就其本质来说，信息保障是一种保证信息和信息系统能够安全运行的防护性行为，是信息安全在当前信息时代的新发展。信息保障的对象是信息以及处理、管理、存储、传输信息的信息系统；目的是采取技术、管理等综合性手段，使信息和信息系统具备机密性、完整性、可用性、可认证性、不可否认性，以及在遭受攻击后的可恢复性。

5.信息安全保障发展历史：20世纪40、50年代，信息安全以通信保密为主体，要

求实现信息的机密性。20世纪60、70年代，随着小规模计算机组成的简单网络系统的出现，网络中多点传输、处理以及存储的保密性、完整性、可用性问题成为关注焦点；进入20世纪90年代，随着网络技术的进一步发展，超大型网络迫使人们必须从整体安全的角度去考虑信息安全问题。

6.按照密钥的特点对密码算法的分类：对称密码算法；非对称密码算法；

7.对称密码算法的优缺点；一个密钥

8.非对称密码算法的优缺点；两个密钥

9.公钥密码加密和鉴别过程（PKI体系）

用户向RA提交证书申请，RA审查后由CA颁发证书给用户

发送方计算信息摘要值

发送方将信息摘要值发送给时间戳服务器，获取带有服务器签名的时间戳

发送方将信息摘要值、时间戳用自己的私钥加密，得到签名数据

发送方随机产生一个对称密钥，用此密钥和某种算法对信息进行对称加密，得到密文

发送方将上一步使用的对称密钥和算法代号用接收方的公钥加密，和密文保存在一起

发送方将签名数据和密文通过不安全信道发送给接收方

接收方用自己的私钥解密密文的对称密钥和算法代号部分

接收方用上一步得到的算法和对称密钥对密文正文进行解密，得到明文信息

接收方用发送方的公钥对签名数据进行解密

接收方计算信息摘要值，与签名数据解密结果中的摘要值进行比较，如果一致则信息没有被篡改

接收方检查时间戳，确认没有遭受重放攻击

10.PKI （ Public Key Infrastructure ）指的是公钥基础设施。 CA （ Certificate Authority ）指的是认证中心。 PKI 从技术上解决了网络通信安全的种种障碍。 CA
从运营、管理、规范、法律、人员等多个角度来解决了网络信任问题。由此，人们统称为 “ PKI/CA ” 。从总体构架来看， PKI/CA
主要由最终用户、认证中心和注册机构来组成。

11.SSL协议的工作流程：
服务器认证阶段：1）客户端向服务器发送一个开始信息“Hello”以便开始一个新的会话连接；2）服务器根据客户的信息确定是否需要生成新的主密钥，如需要则服务器在响应客户的“Hello”信息时将包含生成主密钥所需的信息；3）客户根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器；4）服务器恢复该主密钥，并返回给客户一个用主密钥认证的信息，以此让客户认证服务器。
用户认证阶段：在此之前，服务器已经通过了客户认证，这一阶段主要完成对客户的认证。经认证的服务器发送一个提问给客户，客户则返回（数字）签名后的提问和其公开密钥，从而向服务器提供认证。

12.在传统的企业网络配置中，要进行异地局域网

之间的互连，传统的方法是租用DDN(数字数据网)专线或帧中继。这样的通讯方案必然导致高昂的网络通讯/维护费用。对于移动用户(移动办公人员)与远端个人用户而言，一般通过拨号线路(Internet)进入企业的局域网，而这样必然带来安全上的隐患。

13.(1)使用VPN可降低成本(2)传输数据安全可靠(3)连接方便灵活(4)完全控制

14. VPN关键技术（隧道技术、密码技术、QoS技术）

15.VPN分类（Access VPN和网关-网关的VPN连接）

16.“Internet 协议安全性
(IPSec)”是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议 (IP) 网络上进行保密而安全的通讯。Microsoft® Windows® 2000、Windows XP 和 Windows Server 2003 家族实施 IPSec 是基于“Internet 工程任务组 (IETF)”IPSec 工作组开发的标准。

17.（1）自主访问控制模型（DAC Model）

访问控制的实现机制：访问控制表、访问控制矩阵、访问控制能力列表、访问控制安全标签列表

18.（2）强制访问控制模型（MAC Model）

-----Bell-LaPadula模型、 Biba模型

19.（3） 基于角色的访问控制模型

20.安全审计的内容：安全审计涉及四个基本要素:控制目标、安全漏洞、控制措施和控制测试。其中,控制目标是指企业根据具体的计算机应用,结合单位实际制定出的安全控制要求。安全漏洞是指系统的安全薄弱环节,容易被干扰或破坏的地方。控制措施是指企业为实现其安全控制目标所制定的安全控制技术、配置方法及各种规范制度。控制测试是将企业的各种安全控制措施与预定的安全标准进行一致性比较,确定各项控制措施是否存在、是否得到执行、对漏洞的防范是否有效,评价企业

安全措施的可依赖程度。显然,安全审计作为一个专门的审计项目,要求审计人员必须具有较强的专业技术知识与技能。
安全审计是审计的一个组成部分。由于计算机网络环境的安全将不仅涉及国家安危,更涉及到企业的经济利益。因此,我们认为必须迅速建立起国家、社会、企业三位一体的安全审计体系。其中,国家安全审计机关应依据国家法律,特别是针对计算机网络本身的各种安全技术要求,对广域网上企业的信息安全实施年审制。另外,应该发展社会中介机构,对计算机网络环境的安全提供审计服务,它与会计师事务所、律师事务所一样,是社会对企业的计算机网络系统的安全作出评价的机构。当企业管理当局权衡网络系统所带来的潜在损失时,他们需要通过中介机构对安全性作出检查和评价。此外财政、财务审计也离不开网络安全专家,他们对网络的安全控制作出评价,帮助注册会计师对相应的信息处理系统所披露信息的真实性、可靠性作出正确判

断。

21.防火墙的功能：(1)网络安全的屏障2)强化网络安全策略(3)对网络存取和访问进行监控审计由于所有的访问都必须经过防火墙，所以防火墙就不仅能够制作完整的日志记录，而且还能够提供网络使用的情况的统计数据。(4)防止内部信息的外泄

22.防火墙的局限性：

——

存在着一些防火墙不能防范的安全威胁，如防火墙不能防范不经过防火墙的攻击。例如，如果允许从受保护的网络内部向外拨号，一些用户就可能形成与Internet的直接连接。另外，防火墙很难防范来自于网络内部的攻击以及病毒的威胁

23.防火墙的分类（个人防火墙、软件防火墙、一般硬件防火墙和纯硬件防火墙的特点、典型应用）

——

防火墙技术可根据防范的方式和侧重点的不同而分为很多种类型，但总体来讲可分为二大类：分组过滤、应用代理。

——分组过滤（Packet filtering）：作用在网络层和传输层，它根据分组包头源地址，目的地址和端口号、协议类型等标志确定是否允许数据包通过。只有满足过滤逻辑的数据包才被转发到相应的目的地出口端，其余数据包则被从数据流中丢弃。

——应用代理（Application Proxy）：也叫应用网关（Application Gateway）,它作用在应用层，其特点是完全阻隔了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。实际中的应用网关通常由专用工作站实现。

24. IDS基本结构（事件产生器、事件分析器、事件数据库和响应单元）

25.基于异常的入侵方法检测:优点：可应用成熟的概率统计理论
缺点：①由于用户行为的复杂性，要想准确地匹配一个用户的历史行为非常困难，容易造成系统误报和漏报；
②定义入侵阈值比较困难，阈值高则误报率提高，阈值低则漏报率增高。

误用/滥用检测技术：原理：将入侵过程看作一个行为序列，该行为序列导致系统从初始状态转入被入侵状态。分析时，需要针对每一种入侵方法确定系统的初始状态和被入侵状态，以及导致状态转换的转换条件（导致系统进入被入侵状态必须执行的操作/特征事件）；然后用状态转换图来表示每一个状态和特征事件。
缺点：不善于分析过分复杂的事件，也不能检测与系统状态无关的入侵

26.安全威胁有时可以被分为故意的和偶然的：

故意的威胁如假冒、篡改等。（可以进一步分为主动攻击和

被动攻击。被动攻击不会导致对系统中所含信息的任何改动，而

且系统的操作和状态也不会改变。因此被动攻击主要威胁信息的

保密性；主动攻击则意在篡改系统中所含信息、或者改变系统的

状态和操作，因此主动攻

击主要威胁信息的完整性、可用性和真

实性。）

偶然的威胁如信息被发往错误的地址、误操作等。

26.计算机病毒广义定义：凡能够引起计算机故障，破坏计算机数据程序统称为计算机病毒。。

27.计算机病毒的内在特点如下：

（1）寄生性。

（2）传染性。

（3）潜伏性。

（4）隐蔽性。

（5）可触发性。

（5）破坏性。

28.计算机病毒传播途径

1）通过不可移动的计算机硬件设备进行传播，这些设备通常有计算机的专用ASIC芯片和硬盘等。

（2）通过移动存储设备来传播这些设备包括软盘、磁带等。

（3）通过计算机网络进行传播。

（4）通过点对点通信系统和无线通道传播

（4）通过点对点通信系统和无线通道传播

29.计算机病毒分类：按攻击的操作系统分类。按传播媒介分类。按链接方式分类。按危害程度分类。按寄生方式分类。按攻击机型分类。从广义病毒定义

30.宏病毒特点：只感染微软数据（文档）文件

机制：用VB高级语言编写的病毒代码，直接混杂在文件中，并加以传播。当打开受感染的文件执行触发宏病毒的操作时，病毒就会被激活，并存储到Normal。dot模板或Personal。xls文件中，以后保存的每个文档都会自动被病毒感染。

31.计算机病毒的逻辑结构：病毒的引导模块。病毒的传染模块。病毒的破坏模块。

32.网络病毒种类：根据攻击手段可分为蠕虫和木马两大类型

传播方式：电子邮件，网页，文件传输

33.寄生技术：病毒在感染的时候，将毒代码加入正常程序之中，原正常程序功能的全部或者部分被保留。

驻留技术：当被感染文件执行时，病毒的一部分功能模块进入内存，即使程序执行完毕，它们仍一直驻留在内存中。

加密变形技术：是一个具有里程碑意义的病毒技术。在加密病毒的基础改进，使解密子的代码对不同传染实例呈现多样性。

隐藏技术：病毒在进入用户系统之后，会采取种种方法隐藏自己的行踪，使病毒不易被用户和反病毒软件发现

34.反病毒技术

计算机病毒检测技术、计算机病毒的清除、计算机病毒的免疫、计算机病毒的预防

35.踩点-信息收集-目标探测

相关文档：

- 信息安全答案
- 信息安全面试题及答案
- 信息安全试题答案
- 信息安全试题及答案
- 信息安全数学基础答案
- 信息安全意识培训答案
- 信息安全导论答案
- 信息安全概论课后答案
- 信息安全管理答案
- 信息安全管理考试答案