1. 猪毒问题

1000桶水，其中一桶有毒，猪喝毒水后会在15分钟内死去，想用一个小时找到这桶毒水，至少需要几头猪？限制条件：

1.一滴毒水足以导致一头猪的死亡。死亡时间为15分钟内不确定的某个时间点。

2.其死亡只是毒水导致的，不会有其他因素导致死亡。

3.猪的承水量无穷大，且假设饮一桶花费时间为零。

<https://www.zhihu.com/question/60227816>

文本

中度可信度描述已自动生成

1. 数字签名

**可以先使用私钥对原数据签名，再对签名进行摘要吗？**

不可以，主要有两个原因：

1、可行性： 接收方需要通过摘要验证数据完整性，然而接收方无法对数据进行签名，因此无法验证数据摘要一致性；

2、时间效率： 对原始数据进行签名（加密）时间太长，而摘要算法本身是压缩映射，可以缩短签名消耗的时间。

1. 假如你是单位WEB服务器管理员，试述你会采取哪些主要措施来保障WEB服务器安全。

访问控制（IP地址限制、Windows帐户、请求资源的Web权限、资源的NTFS权限）

用虚拟目录隐藏真实的网站结构；

设置基于SSL的加密和证书服务，以保证传输安全；

完善定期审核机制和入侵检测系统；

安装防火墙及杀毒软件；

及时安装操作系统补丁，减少操作系统漏洞等等。

1. 试述你是如何理解信息安全领域"三分技术，七分管理”这名话的

虽然目前有众多的安全产品，但没有任何一种能提供全方位的解决方案。

1)防病毒软件:不能保护机构免受使用合法程序对系统进行访问的入侵者进行的恶意破坏，也不能保护机构免受另一类合法用户的破坏。

2)访问控制:不会阻止人们利用系统脆弱点以管理员身份获得对系统的访问并查看系统文件

3)防火墙:不会阻止攻击者使用一个允许的连接进行攻击。也不能防止内部攻击。

4)入侵检测:不能检测出合法用户对信息的非正常访问。支持自动保护功能的入侵检测系统还可以带来附加的安全问题。如系统配置为阻止某个攻击地址的访问，之后会发现某用户的通信被错误识别为攻击通信，则其再无法与你通信了。

5)策略管理:可能没有考虑系统的薄弱点或应用软件中的错误配置。这有可能导致侵入。计算机上的策略管理也不能保证用户不写下他们的密码或将密码提供给未经授权的人。

6)薄弱点扫描:本身并不会保护计算机系统，需在找出薄弱点后采取安全措施。该方法也不会发现合法用户进行的不正当访问，也不能发现已经进入系统、查找配置文件或补丁程序的弱点的入侵者。

7)加密:加密系统并不能分辨提交了同样加密算法密钥的用户是合法还是非法用户。加密本身不能提供安全保障，还必须对加密密钥和系统有一个整体控制。

8)物理安全机制:不能保护系统不受到合法访问进行的攻击或通过网络实施的攻击。

所以安全技术和产品只是安全实践活动的一部分，是实现安全需求的手段，还应包括：制定完备的安全策略，通过风险评估来确定需求，根据需求选择安全技术和产品，按照既定安全策略和流程规范来实施、维护和审查安全措施。信息安全并不是技术过程，而是管理过程。

1. 假如你是一个网络管理员，请假定网络场景，说明你会采取哪些措施来构建网络安全体系，这些措施各有什么作用。

1. 将重要设备放入专门房间，保持良好环境，有专入制度，保证物理安全；

2. 在网关出口使用防火墙，如果对网络安全要求较高，可以使用状态检测型防火墙，如果对速度要求高可以使用硬件防火墙。

3. 在防火墙后面使用IDS，与防火墙配合使用，以加强内网安全。

4. 将所有服务器放置在专门的DMZ区域。

5. 对于内网安全，可以使用域环境，由DC统一管理帐号和密码，针对不同的用户和组设置不同的权限。

6. 做好操作系统、数据库系统、应用软件升级维护，做好数据备份，保障数据安全；购买正版杀毒软件并及时升级；

7. 对外通信采用IPSec或SSL等VPN加密技术，保障通信安全；

8. 为系统设置安全口令，做好访问控制，保障系统使用安全；

9. 建立完善的安全管理制度、审计制度、建立应急响应机构和机制；

10. 做好内部安全监管、安全培训等。

1. 试论述目前造成计算机网络不安全的原因是什么?可采取哪些相应的安全措施？

不安全原因1.网络自身的特性2.网络技术的开放3．网络协议的漏洞4. 通信系统和信息系统的自身缺陷5.系统"后门”6.黑客及病毒等恶意程序的攻击。

措施:制定安全策略：如采用什么样的安全保障体系、确定网络资源职责划分、制定使用规则、制定日常维护规程、确定在遇到安全问题时采取的措施；采取加密、数字签名、访问控制、数据完整性、鉴别、业务填充、路由控制、公证仲裁等机制。具体技术措施如：1）设置IP限制，屏蔽有威胁的IP地址2）设置身份验证，确保只有合法用户才能访问授权范围内的资源3）设置资源的WEB权限4）设置文件或目录的NTFS权限5）用虚拟目录隐藏真实的网站结构6）设置基于SSL的加密和证书服务，保证传输安全7）完善定期审核机制8）安装防火墙软件9）安装杀毒软件10）及时安装操作系统补丁，减少操作系统漏洞

1. 至少分析、讨论5种信息系统所面临的安全威胁。

信息系统所面临的常见安全威胁如下所示：

1. 软硬件故障：由于设备硬件故障、通信链接中断、信息系统或软件Bug导致对业务、高效稳定运行的影响。

2. 物理环境威胁：断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件和自然灾害。

3. 无作为或操作失误：由于应该执行而没有执行相应的操作，或无意的执行了错误的操作，对系统造成影响。

4. 管理不到位：安全管理无法落实，不到位，造成安全管理不规范，或者管理混乱，从而破坏信息系统正常有序运行。

5. 恶意代码和病毒：具有自我复制、自我传播能力，对信息系统构成破坏的程序代码。

6. 越权或滥用：通过采用一些，超越自己的权限访问了本来无权访问的资源；或者滥用自己的职权，做出破坏信息系统的行为。

7. 黑客攻击技术：利用黑客工具和技术，例如，侦察、密码猜测攻击、缓冲区溢出攻击、安装后门、嗅探、伪造和欺骗、拒绝服务攻击等手段对信息系统进行攻击和入侵。

8. 物理攻击：物理接触、物理破坏

1. 试介绍VPN使用了哪些主要技术。

1）隧道（封装）技术是目前实现不同VPN用户业务区分的基本方式。一个VPN可抽象为一个没有自环的连通图，每个顶点代表一个VPN端点（用户数据进入或离开VPN的设备端口），相邻顶点之间的边表示连结这两对应端点的逻辑通道，即隧道。

隧道以叠加在IP主干网上的方式运行。需安全传输的数据分组经一定的封装处理，从信源的一个VPN端点进入VPN，经相关隧道穿越VPN（物理上穿越不安全的互联网），到达信宿的另一个VPN端点，再经过相应解封装处理，便得到原始数据。（不仅指定传送的路径，在中转节点也不会解析原始数据）

2）当用户数据需要跨越多个运营商的网络时，在连接两个独立网络的节点该用户的数据分组需要被解封装和再次封装，可能会造成数据泄露，这就需要用到加密技术和密钥管理技术。目前主要的密钥交换和管理标准有SKIP和ISAKMP（安全联盟和密钥管理协议）。

3）对于支持远程接入或动态建立隧道的VPN，在隧道建立之前需要确认访问者身份，是否可以建立要求的隧道，若可以，系统还需根据访问者身份实施资源访问控制。这需要访问者与设备的身份认证技术和访问控制技术。

1. 什么是数字签名？它在电子商务中起什么作用？

答：1）从技术上来讲，数字签名其实就是通过一个单向函数对要传送的报文(或消息)进行处理，产生别人无法识别的一段数字串，这个数字串用来证明报文的来源并核实报文是否发生了变化。在数字签名中，私有密钥是某个人知道的秘密值，与之配对的唯一公开密钥存放在数字证书或公共数据库中，用签名人掌握的秘密值签署文件，用对应的数字证书进行验证。

2）数字签名技术最早应用于用户登录过程。对于大多数用户来讲，用户名和口令已习以为常了，其中隐含的签名技术可能并不为人所知。 推动数字签名广泛应用的最大功臣应当是PKI技术。 在各国政府的积极支持下，PKI作为电子商务、电子政务的技术平台，使得技术应用、商业价值、生产力提高成为有机的整体，得到了长足的发展，数字证书的概念已逐渐被越来越多的人所接受，极大地促进了信息化建设的进程。到目前为止，全国各省市几乎都建立了自己的CA认证中心，这些CA中心的数字证书及相关应用方案被广泛应用于网上报关、网上报税、网上报检、网上办公、网上招投标、网上采购、数字工商等大型电子政务和电子商务工程。

1. Internet的安全解决方案是什么？

答：从整体上看，Internet网络安全问题可分为以下几个层次，即操作系统层、用户层、应用层、网络层（路由器）和数据链路层。这5个层次的网络系统安全体系理论已得到了国际网络安全界的广泛承认和支持。 （5分）

网络层的安全是Internet网络安全解决方案中最重要的部分。涉及到3个方面：

（1）IP协议本身的安全性。IP协议本身未经加密使人们非法信息和口令成为可能；

（2）网管协议的安全性。由于SNMP协议的认证机制非常简单，而且使用未加保密的明码传输，这就可能通过非法途径获得SNMP协议分组并分析破解有关网络管理信息；

（3）最重要的方面，就是网络交换设备的安全性。交换设备包括路由器和ATM设备。由于Internet普遍采用路由器方式的无连接转发技术，而且路由协议是动态更新的 OSPF和 RIP协议。这些协议动态更新都装有协议的路由器路由表。一旦某一个路由器发生故障或问题，将迅速波及到路由器相关的整个Internet自治域。（5分）

表格

描述已自动生成

1. 完整的保密通信方案设计

1）利用DH密钥交换协议，让发送方和接收方确定对称密钥。将嵌入的信息结合数字签名和时间戳信息，再利用密钥进行加密，再将加密结果通过LSB算法嵌入到图片中。

2）发送方和接收方共享同一个散列函数MD5，并利用基于事件同步的口令认证技术。发送方对步骤(1)中的图片数据，进行散列，将散列结果作为口令数据，与图片数据一并发送给接收方。

3）接收方收到信息后，先根据自己的散列函数MD5，对图片数据进行散列，将散列结果与口令数据进行对比，如果一致，说明源自可信的发送方，此时接收数据。否则，不予置理。

4）接受数据后，提取出图片数据中的水印信息。并利用密钥进行解密，解密后验证数字签名和时间戳，如果该时间戳超过发送方约定的时效，则该数据有误。否则，得到的嵌入信息即可得到完整的该隐藏信息。

1. DES解法

[信息安全密码学：DES算法的核心 E盒、S盒、P盒\_Lmars97的博客-CSDN博客\_des s盒](https://blog.csdn.net/qq_44131896/article/details/117573452)

白板上的文字

描述已自动生成