网络工程师学习笔记第8章 网络安全与信息安全思科认证
PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/633/2021_2022__E7_BD_91_E7_BB_9C_E5_B7_A5_E7_c101_633705.htm 第8章 网络安全与信息安全 主要内容:1、密码学、鉴别 2、访问控制、计算机病毒 3、网络安全技术 4、安全服务与安全机制 5、信息系统安全体系结构框架 6、信息系统安全评估准则 一、密码学 1、密码学是以研究数据保密为目的，对存储或者传输的信息采取秘密的交换以防止第三者对信息的窃取的技术。 2、对称密钥密码系统(私钥密码系统):在传统密码体制中加密和解密采用的是同一密钥。常见的算法有:DES、IDEA 3、加密模式分类: (1)序列密码:通过有限状态机产生性能优良的伪随机序列，使用该序列加密信息流逐位加密得到密文。 (2)分组密码:在相信复杂函数可以通过简单函数迭代若干圈得到的原则，利用简单圈函数及对合等运算，充分利用非线性运算。 4、非对称密钥密码系统(公钥密码系统):现代密码体制中加密和解密采用不同的密钥。 实现的过程:每个通信双方有两个密钥，K和K ’，在进行保密通信时通常将加密密钥K公开(称为公钥)，而保留解密密钥K ’(称为私钥)，常见的算法有:RSA 二、鉴别 鉴别是指可靠地验证某个通信参与方的身份是否与他所声称的身份一致的过程，一般通过某种复杂的身份认证协议来实现。 1、口令技术 身份认证标记:PIN保护记忆卡和挑战响应卡 分类:共享密钥认证、公钥认证和零知识认证 (1)共享密钥认证的思想是从通过口令认证用户发展来了。 (2)公开密钥算法的出现为 2、会话密钥:是指在一次会话过程中使用的密钥，一般都是由机器随机生成的，会话密钥在实际使用

时往往是在一定时间内都有效，并不真正限制在一次会话过程中。 签名:利用私钥对明文信息进行的变换称为签名 封装:利用公钥对明文信息进行的变换称为封装 3、Kerberos鉴别:是一种使用对称密钥加密算法来实现通过可信第三方密钥分发中心的身份认证系统。客户方需要向服务器方递交自己的凭据来证明自己的身份，该凭据是由KDC专门为客户和服务器方在某一阶段内通信而生成的。凭据中包括客户和服务器方的身份信息和在下一阶段双方使用的临时加密密钥，还有证明客户方拥有会话密钥的身份认证者信息。身份认证信息的作用是防止攻击者在将来将同样的凭据再次使用。时间标记是检测重放攻击。 4、数字签名: 加密过程为C=EB(DA(m)) 用户A先用自己的保密算法(解密算法DA)对数据进行加密DA(m)，再用B的公开算法(加密算法EB)进行一次加密EB(DA(m))。 解密的过程为m= EA (DB (C)) 用户B先用自己的保密算法(解密算DB)对密文C进行解密DB (C)，再用A的公开算法(加密算法EA)进行一次解密EA (DB (C))。只有A才能产生密文C，B是无法依靠或修改的，所以A是不得抵赖的DA(m)被称为签名。 三、访问控制 访问控制是指确定可给予哪些主体访问的权力、确定以及实施访问权限的过程。被访问的数据统称为客体。 1、访问矩阵是表示安全政策的最常用的访问控制安全模型。访问者对访问对象的权限就存放在矩阵中对应的交叉点上。 2、访问控制表(ACL)每个访问者存储有访问权力表，该表包括了他能够访问的特定对象和操作权限。引用监视器根据验证访问表提供的权力表和访问者的身份来决定是否授予访问者相应的操作权限。 3、粗粒度访问控制:能够控制到主机对象的访问控制 细粒度访问控制:

能够控制到文件甚至记录的访问控制 4、防火墙作用:防止不希望、未经授权的通信进出被保护的内部网络，通过边界控制强化内部网络的安全政策。 防火墙的分类:IP过滤、线过滤和应用层代理 路由器过滤方式防火墙、双穴信关方式防火墙、主机过滤式防火墙、子网过滤方式防火墙 5、过滤路由器的优点:结构简单，使用硬件来降低成本.对上层协议和应用透明，无需要修改已经有的应用。缺点:在认证和控制方面粒度太粗，无法做到用户级别的身份认证，只有针对主机IP地址，存在着假冒IP攻击的隐患.访问控制也只有控制到IP地址端口一级，不能细化到文件等具体对象.从系统管理角度来看人工负担很重。 6、代理服务器的优点:是其用户级身份认证、日志记录和帐号管理。缺点:要想提供全面的安全保证，就要对每一项服务都建立对应的应用层网关，这就极大限制了新应用的采纳。 7、VPN:虚拟专用网，是将物理分布在不同地点的网络通过公共骨干网，尤其是internet联接而成的逻辑上的虚拟子网。 8、VPN的模式:直接模式VPN使用IP和编址来建立对VPN上传输数据的直接控制。对数据加密，采用基于用户身份的鉴别，而不是基于IP地址。隧道模式VPN是使用IP帧作为隧道的发送分组。 9、IPSEC是由IETF制订的用于VPN的协议。由三个部分组成:封装安全负载ESP主要用来处理对IP数据包的加密并对鉴别提供某种程序的支持。，鉴别报头(AP)只涉及到鉴别不涉及到加密，internet密钥交换IKE主要是对密钥交换进行管理。 四、计算机病毒 1、计算机病毒分类:操作系统型、外壳型、入侵型、源码型 2、计算机病毒破坏过程:最初病毒程序寄生在介质上的某个程序中，处于静止状态，一旦程序被引导或调用，它就被激活，变成有传

染能力的动态病毒，当传染条件满足时，病毒就侵入内存，随着作业进程的发展，它逐步向其他作业模块扩散，并传染给其他软件。在破坏条件满足时，它就由表现模块或破坏模块把病毒以特定的方针表现出来。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com