极客时间训练营

系统架构设计师

第4章 信息安全技术基础知识

授课：王建平

目录

目录

信息安全的概念

1、信息安全属性（★★★）

- 机密性:确保信息不暴露给未授权的实体或进程。
- 完整性:只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改。
- 可用性:得到授权的实体在需要时可以访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。
- 可控性:可以控制授权范围内的信息流向及行为方式。
- 可审查性:对出现的信息安全问题提供调查的依据和手段。

2、信息安全的范围（★）

信息安全的范围包括：设备安全、数据安全、内容安全和行为安全。

1）设备安全

信息系统设备的安全是信息系统安全的首要问题，是信息系统安全的物质基础，包括3 个方面。

(1）设备的稳定性：指设备在一定时间内不出故障的概率。

(2）设备的可靠性：指设备在一定时间内正常执行任务的概率。

(3）设备的可用性：指设备可以正常使用的概率。

信息安全的概念

2 ）数据安全
数据信息可能泄露，可能被篡改，数据安全即采取措施确保数据免受未授权的泄露、篡改和毁坏，包括以下3 个方面。
(1 ）数据的秘密性：指数据不受未授权者知晓的属性。
(2 ）数据的完整性：指数据是正确的、真实的、未被篡改的、完整无缺的属性。
(3 ）数据的可用性：指数据可以随时正常使用的属性。

3 ）内容安全
内容安全是信息安全在政治、法律、道德层次上的要求。

4 ）行为安全
信息系统的服务功能是指最终通过行为提供给用户，确保信息系统的行为安全，才能最终确保系统的信息安全。

典型真题

61-62.在进行软件系统安全性分折时，（)保证信息不泄露给未授权的用户、实体或过程；完整性保证信息的完整和准确，防止信息被非法修改；（)保证对信息的传播及内容具有控制的能力，防止为非法者所用。

61、A.完整性　B.不可否认性　C.可控性　D.机密性.

62、A.完整性　B.安全审计　C.加密性　D.可控性.

参考答案：D D

信息存储安全

信息的存储安全包括信息使用的安全(如用户的标识与验证、用户存取权限限制、安全问题跟踪等)、系统安全监控、计算机病毒防治、数据的加密和防止非法的攻击等。

1.信息使用的安全（★）

1)用户的标识与验证

用户的标识与验证主要是限制访问系统的人员，对用户身份的合法性验证。方法有两种：

- 基于用户所拥有特殊安全物品的识别，如智能IC卡识别法、磁条卡识别法。
- 基于人的物理特征的识别，包括签名识别法、指纹识别法和语音识别法。

2)用户存取权限限制（★）

用户存取权限限制主要是限制进入系统的用户所能做的操作。一般有两种方法：

(1)隔离控制法。隔离控制法是在电子数据处理成分的周围建立屏障，以便在该环境中实施存取。主要实现方式包括物理隔离方式、时间隔离方式、逻辑隔离方式和密码技术隔离方式等。

(2)限制权限法。限制权限法是有效地限制进入系统的用户所进行的操作。即对用户进行分类管理，安全密级、授权不同的用户分在不同类别；对目录、文件的访问控制进行严格的权限控制，防止越权操作。

2.系统安全监控

安全监控系统+完善的审计系统+日志管理系统，利用日志和审计功能对系统进行安全监控。

信息存储安全

3.计算机病毒防治
计算机病毒具有隐蔽性、传染性、潜伏性、触发性和破坏性等点，所以需要建立计算机和病毒防治管理制度。
(1)经常从软件供应商网站下载、安装安全补丁程序和升级杀毒软件。
(2)定期检查敏感文件。
(3)使用高强度的口令。对不同的账号选用不同的口令。
(4)经常备份重要数据，要坚持做到每天备份。
(5)选择、安装经过公安部认证的防病毒软件，定期对整个硬盘进行病毒检测和清除工作。
(6)在计算机和因特网之间安装使用防火墙，提高系统的安全性。
(7)当计算机不使用时，不要接入因特网，一定要断掉网络连接。
(8)重要的计算机系统和网络一定要严格与因特网物理隔离。
(9)不要打开陌生人发来的电子邮件，无论它们有多么诱人的标题或者附件，同时要小心处理来自熟人的邮件附件。
(10)正确配置系统和使用病毒防治产品。

网络安全

1.网络安全隐患表现：物理安全、软件安全漏洞、不兼容使用安全漏洞、选择合适的安全哲理等。
2.网络存在的威胁主要表现在以下 5 个方面:（★）
(1)非授权访问。如假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。
(2)信息泄露或丢失。指敏感数据在有意或无意中被泄露或丢失，通常包括信息在传输中丢失或泄露、信息在存储介质中丢失或泄露以及通过建立隐蔽隧道等方式窃取敏感信息等。
(3)破坏数据完整性。非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。
(4)拒绝服务攻击。不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入网络系统或得不到相应的服务。
(5)利用网络传播病毒。

3.安全措施的目标（★）
(1)认证。确保会话对方的资源(人或计算机) 与它声称的一致。
(2)访问控制。确保会话对方 (人或计算机)有权做它所声称的事情。
(3)完整性。确保接收到的信息与发送的一致。
(4)审计。确保任何发生的交易在事后可以被证实，发信者和收信者都认为交换发生过，即所谓的不可抵赖性。
(5)保密。确保敏感信息不被窃听。

信息系统安全系统框架

信息安全系统框架由技术体系、组织机构体系和管理体系构建。（★★）

一、技术体系

从实现技术来看，信息安全系统涉及基础安全设备、计算机网络安全、操作系统安全、数据库安全、终端设备安全等多方面技术。

(1)基础安全设备。包括密码芯片、加密卡、身份识别卡等。

(2)计算机网络安全。指信息在网络传输过程中的安全防范，用于防止和监控未经授权破坏、更改和盗取数据的行为。

(3)操作系统安全。指操作系统的无错误配置、无漏洞、无后门、无特洛伊木马等，能防上非法用户对计算机资源的非法存取。

(4)数据库安全。分为数据库管理系统安全和数据库应用系统安全两部分，涉及物理数据库的完整性、逻辑数据库的完整性、元素安全性、可审计性、访问控制、身份认证、可用性、推理控制、多级保护以及消除隐通道等相关技术。

(5)终端设备安全。从电信网终端设备的角度分为电话密码机、传真密码机、异步数据密码机等。

二、组织机构体系

组织机构体系是信息系统安全的组织保障系统，由机构、岗位和人事机构三个模块构成一个体系。

三、管理体系

信息系统安全的管理体系由法律管理、制度管理和培训管理3个部分组成。

典型真题

完整的信息安全系统至少包含三类措施，即技术方面的安全措施、管理方面的安全措施和相应的(１)。其中，信息安全的技术措施主要有：信息加密、数字签名、身份鉴别、访问控制、网络控制技术、反病毒技术、（２)。

A.用户需求　　B.政策法律.　　C.市场需求　　D.领域需求

A.数据备份和数据测试
B.数据迁移和数据备份
C.数据备份和灾难恢复.
D.数据迁移和数据测试

参考答案：B C

目录

信息安全技术-加密技术

◆**加密技术**

一个密码系统，通常简称为密码体制(Cryptosystem),由五部分组成：

(1)明文空间M,它是全体明文的集合。

(2)密文空间C,它是全体密文的集合。

(3)密钥空间K,它是全体密钥的集合。其中每一个密钥K均由加密密钥Ke和解密密钥Kd组成，即K=<Ke,Kd>。

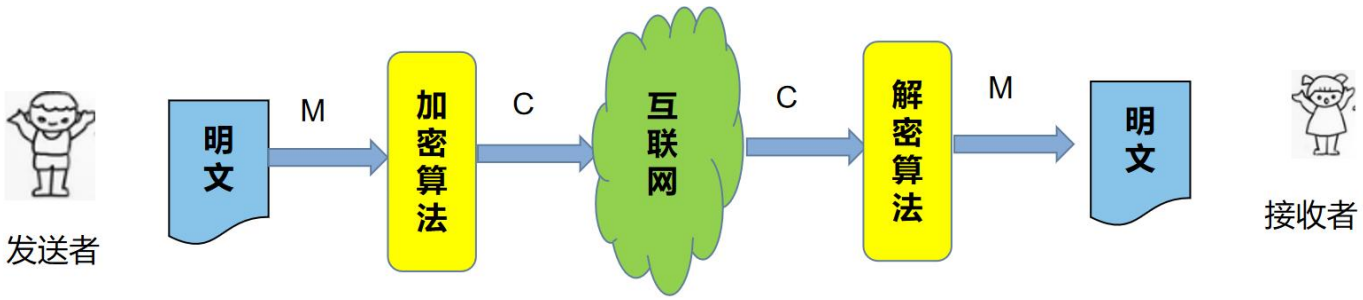
(4)加密算法E,它是一组由M至C的加密变换。

(5)解密算法D,它是一组由C到M的解密变换。

◆对于明文空间M中的每一个明文M,加密算法E在密钥Ke的控制下将明文M加密成密文C:C=E(M,Ke)

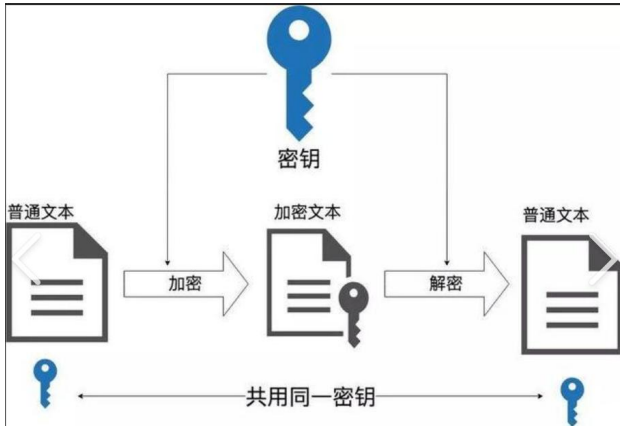
◆而解密算法D在密钥Kd的控制下将密文C解密出同一明文M:

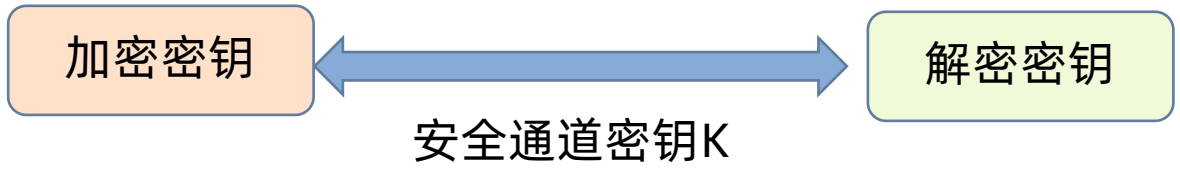
M=D(C,Kd)=D (E(M,Ke),Kd)



信息安全技术-对称加密算法

◆对称加密算法（★★★）
对称加密算法也称为私钥加密算法，是指加密密钥和解密密钥相同，或者虽然不同，但从其中的任意一个可以很容易地推导出另一个。





安全通道密钥K

对称加密：Ke=Kd，那么密钥K的安全传输是主要问题

信息安全技术-对称加密算法

◆对称加密：（★★★）

- 优点：加密速度快、效率高；
- 缺点：加密强度不高，且密钥分发困难其传输需要经过安全可靠的途径。
- 应用：大量数据的加密
- 实现方式：分别是分组密码和序列密码。分组密码是在明文分组和密文分组上进行运算，序列密码是对明文和密文数据流按位或字节进行运算。
- 常见算法：

（1）DES是一种迭代的分组密码，分组长度为64位，使用一个56位的密钥以及附加的8位奇偶校验位。攻击DES的主要技术是穷举法。

（2）3DES：用两个56位的密钥K1和K2。 加密：K1加密→K2解密→K1加密。解密：K1解密→K2加密→K1解密，所以密钥长度为112位。

（3）IDEA是在DES的基础上发展起来的，类似于3DES。分组长度为64位，密钥长度为128位。

（4）AES：代替-置换密码，是美国采用的加密标准用来代替DES，分组长度为128位，支持三种不同大小的密钥：128、192和256.

（5）RC-2、 RC-4、 RC-5

（6）SM1/SM4/SM7和ZUC（祖冲之密码）。

典型真题

DES 是一种( )，其密钥长度为 56 位，3DES 是利用 DES 的加密方式，对明文进行 3 次 加密，以提高加密强度，其密钥长度是 ( ) 位。

A.共享密钥.　B. 公开密钥　C. 报文摘要　D.访问控制

A.56　B.112.　C.128　D.168

试题分析

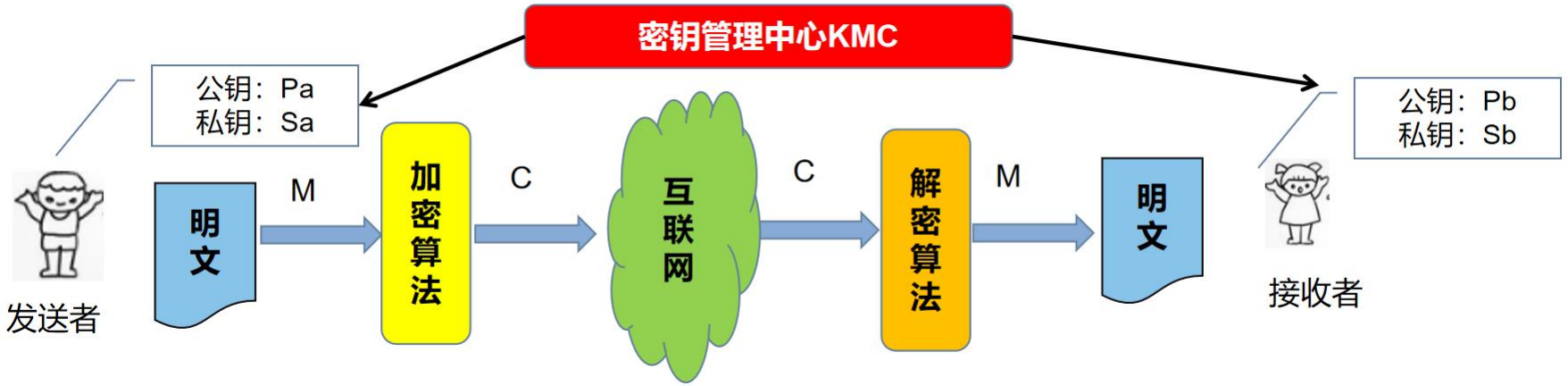
DES加密是一种对称加密算法，加密与解密秘钥相同。由于DES的密钥长度较短，为了提高安全性，就出现了使用112位密钥对数据进行三次加密的算法（3DES），即用两个56位的密钥K1和K2，发送方用K1加密，K2解密，再使用K1加密；接收方则使用K1解密，K2加密，再使用K1解密，其效果相当于将密钥长度加倍。

参考答案：（6）A　（7）B

信息安全技术-非对称密钥加密

◆非对称加密算法（★★★）

非对称加密算法也称为公钥加密算法，是指加密密钥和解密密钥完全不同，其中一个为公钥，另一个为私钥，并且不可能从任何一个推导出另一个。它的优点在于可以适应开放性的使用环境，可以实现数字签名与验证。



非对称加密

Ke ≠Kd，公钥是公开的，私钥是人们自己保存。二者配合使用。A的公钥加密必须用A的私钥解密。

信息安全技术-非对称密钥加密

◆非对称加密算法特点（★★★）

- 优点：加密强度高，密钥分发简单
- 缺点：加密速度慢，算法复杂
- 应用：少量数据的加密场合
- 常见算法：最常见的非对称加密算法是RSA，RSA算法的密钥长度为512位。RSA算法的保密性取决于数学上将一个数分解为两个素数的问题的难度，根据已有的数学方法，其计算量极大，破解很难。但是加密/解密时要进行大指数模运算，因此加密/解密速度很慢，主要用在数字签名中。加密速度慢。

Elgamal、ECC椭圆曲线算法、背包算法、Rabin、D-H、SM2/SM9.

典型真题

非对称加密算法中，加密和解密使用不同的密钥，下面的加密算法中（6）属于非对称加密算法。若甲、乙采用非对称密钥体系进行保密通信，甲用乙的公钥加密数据文件，乙使用（7）来对数据文件进行解密。

（6）A、AES　　B、RSA.　　C、IDEA　　D、DES

（7）A、甲的公钥　　B、甲的私钥　　C、乙的公钥　　D、乙的私钥.

答案：6、B　　7、D

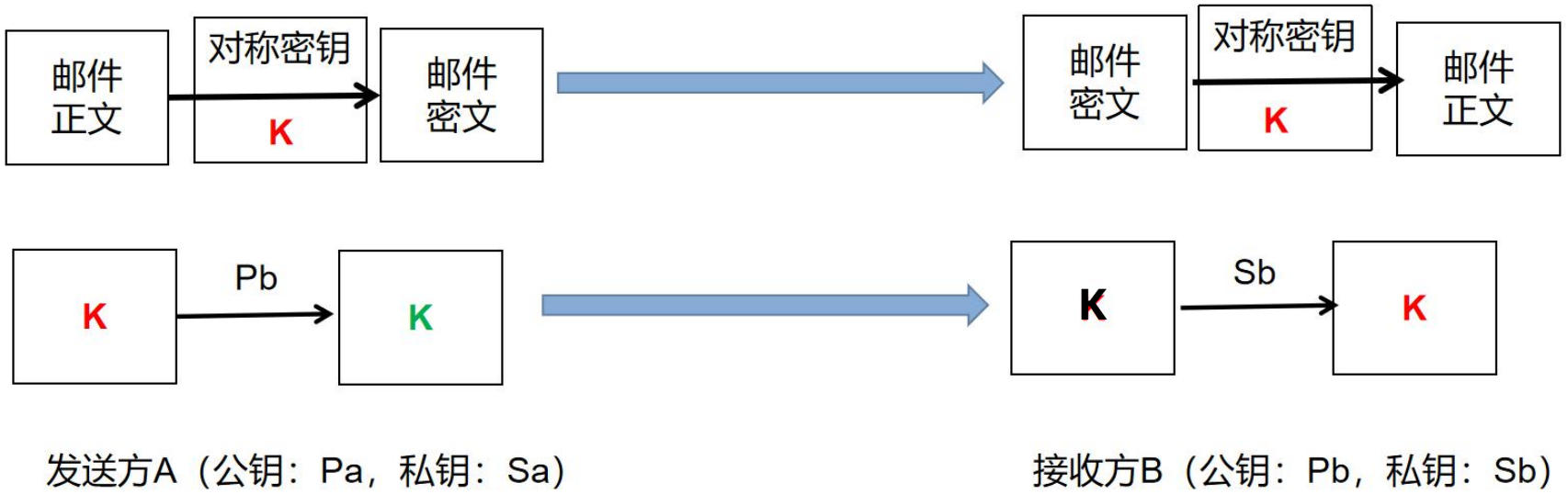
解析：RSA是非对称加密算法；

公钥和私钥是对称的，互相加解密，使用乙的公钥加密，只能用乙的私钥解密。

信息安全技术-电子信封

◆电子信封（★）

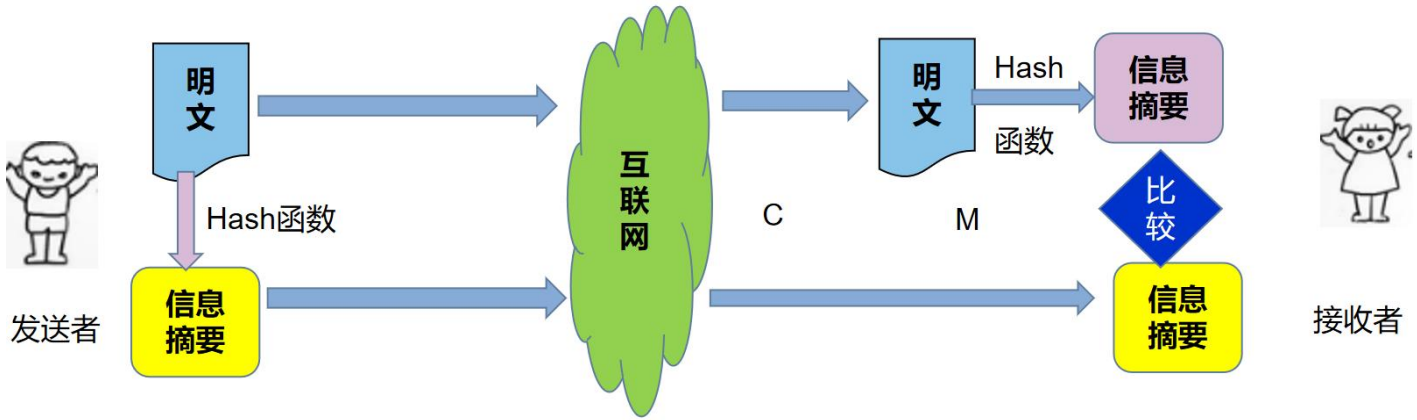
采用了私钥密码体制和公钥密码体制。原理：原文用对称密钥（随机密钥）加密传输，对称密钥的对称密钥用接收方公钥加密发送给对方，对方接收到电子信封，用私钥解密信封，取出对称密钥解密原文。



信息安全技术-数字摘要

◆数字摘要技术（★★★）

数字摘要又称杂凑算法又叫单向散列函数是主要的数字签名算法，它是利用散列（Hash）函数（哈希函数、杂凑函数）进行数据的加密。单向Hash函数提供了这样一种计算过程：输入一个长度不固定的字符串，返回一串定长的字符串，这个返回的字符串称为消息摘要（Message Digest, MD），也称为Hash值或散列值。



数字摘要三个特性：单向性、抗弱碰撞性（很难找到另外明文块相同的加密后生成相同的数字摘要）可以防伪造、抗强碰撞性、不管明文有多长都会生成相同长度的数字摘要。

信息安全技术-数字摘要

（1）消息摘要算法。消息摘要算法（Message Digest algorithm 5, MD5）用于确保信息传输完整一致，它的作用是让大容量信息在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式，即将一个任意长度的字节串变换成一个定长的大数）。

（2）安全散列算法。安全散列算法（Secure Hash Algorithm, SHA）MD5和SHA的散列值分别为128、160位。通常认为由于SHA采用的密钥长度较长，因此安全性高于MD5。SM3（国密算法）：256位。

思考？

数字摘要能保证完整性但是却不能保证机密性，因为明文在“裸奔”！

所以经常是结合使用。

典型真题

在我国商用密码算法体系中：（ ）属于摘要算法。
A.SM2　　B.SM3.　　C.SM4　　D.SM9

国密 SSL 证书采用(　)公钥算法体系，支持SM2，SM3，SM4等国密算法安全协拟，国密 SSL 证书可以满足政府机构、事业单位、大型国企、金融银行等行业客户的国产化改造和国密算法合规需求。
A.SM1　　B.SM2.　　C.SM3　　D.SM4

参考答案：B、B

数字签名

◆数字签名

数字签名是指通过一个单向函数对要传送的报文进行处理，得到用以认证报文来源并核实报文是否发生变化的一个字母数字串。它与数据加密技术一起，构建起了安全的商业加密体系。

传统的数据加密是保护数据的最基本方法，它只能够防止第三者获得真实的数据(数据的机密性)，而数字签名则可以解决否认、伪造、篡改和冒充的问题(数据的完整性和不可抵赖性)。

数字签名使用的是公钥算法（非对称密钥技术）。

数字签名的过程：（★★★）

(1)发送者A先通过散列函数对要发送的信息(M)计算消息摘要(MD)，也就是提取原文的特征。

(2)发送者A将原文(M)和消息摘要(MD)用自己的私钥(PrA)进行加密，就是完成签名动作，其信息可以表示为PrA (M+MD)。

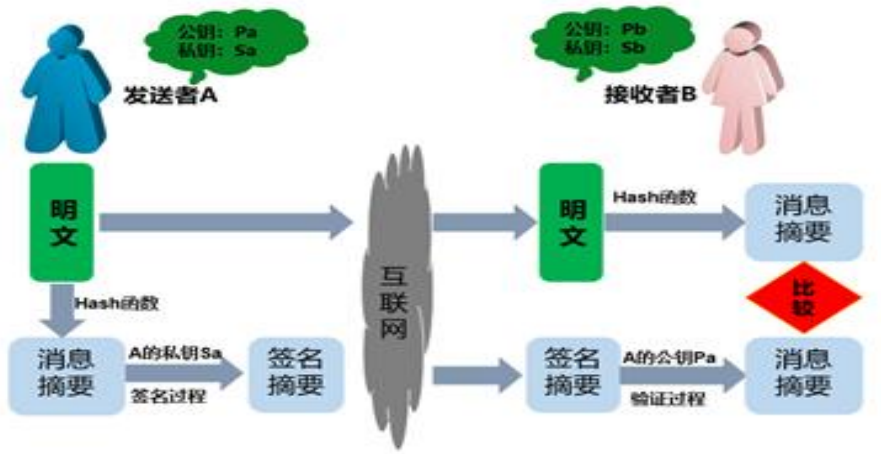
(3)然后以接收者B的公钥(PB)作为密钥，对这个信息包进行再次加密，得到PB(PrA(M+MD))。

(4)当接收者收到后，首先用自己的私钥PrB进行解密，从而得到PrA(M+MD)。

(5)再利用A的公钥(PA)进行解密，如果能够解密，显然说明该数据是A发送的，同时也就将得到原文M和消息摘要MD。

(6)然后对原文M计算消息摘要，得到新的MD，与收到MD进行比较，如果一致，说明该数据在传输时未被篡改。

数字签名



数字加密和数字签名的区别：（★★★）

- ✓ 数字加密是用接收者的公钥加密，接收者用自己的私钥解密。
- ✓ 数字签名是：将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用HASH函数对收到的原文产生一个新摘要信息，与解密的摘要信息对比

数字签名

◆数字签名的条件（★）

可用的数字签名应保证以下几个条件：

- 签名是可信的。签名使文件的接收者相信签名者是慎重地在文件上签字的。
- 签名不可伪造。签名证明是签字者而不是其他人在文件上签字。
- 签名不可重用。签名是文件的一部分，不可能将签名移到不同的文件上。
- 签名的文件是不可改变的。在文件上签名后，文件不能再改变。
- 签名是不可抵赖的。签名和文件是物理的东西，签名者事后不能声称他没有签过名。

数字证书

◆数字证书（★★）

数字证书又称为数字标识，是由认证中心（Certificate Authority, CA）签发的对用户的公钥的认证。是标识网络用户身份的电子文档，该文档由第三方认证机构CA负责发放。包含用户基本数据信息及公钥信息、由CA进行数字签名的CA的相关信息。

国际上对证书的格式和认证方法遵从X.509体系标准。

数字证书的内容：

✓数字证书的版本信息；
✓序列号（每个证书都有一个唯一的证书序列号）；
✓证书所使用的签名算法；
✓证书发行机构名称，命名规则一般采用X.500格式；
✓证书有效期；
✓证书所有者的名称；
✓证书所有者的公钥信息；
✓证书发行者对证书的签名。

典型真题

用户乙收到甲数字签名后的消息M，为验证消息的真实性，首先需要从CA获取用户甲的数字证书，该数字证书中包含（ ），并利用（ ）验证该证书的真伪，然后利用（ ）验证M的真实性.

A.甲的公钥　B.甲的私钥　C.乙的公钥　D.乙的私钥

A.CA的公钥　B.乙的私钥　C.甲的公钥　D.乙的公钥

A.CA的公钥　B.乙的私钥　C.甲的公钥　D.乙的公钥

参考答案：A、A、C

典型真题

用户A从CA获取了自己的数字证书，该数字证书中包含为证书进行数字签名的（ ）。

A、CA的私钥和A的公钥.　　B、CA的私钥和A的私钥

C、CA的公钥和A的公钥　　D、CA的公钥和A的私钥

数字签名是对以数字形式存储的消息进行某种处理，产生一种类似于传统手书签名功效的信息处理过程。数字签名标准DSS中使用的签名算法DSA是基于ElGamal和Schnorr两个方案而设计的。当DSA对消息m的签名验证结果为True，也不能说明（ ）

A、接收的消息m无伪造　　B、接收的消息m无篡改

C、接收的消息m无错误　　D、接收的消息m无泄密.

答案：A、D

典型真题

根据国际标准ITUT X.509规定，数字证书的一般格式中会包含认证机构的签名，该数据域的作用是（）。
A.用于标识颁发证书的权威机构CA
B.用于指示建立和签署证书的CA的X.509名字
C.用于防止证书伪造
D.用于传递CA的公钥

参考答案：C

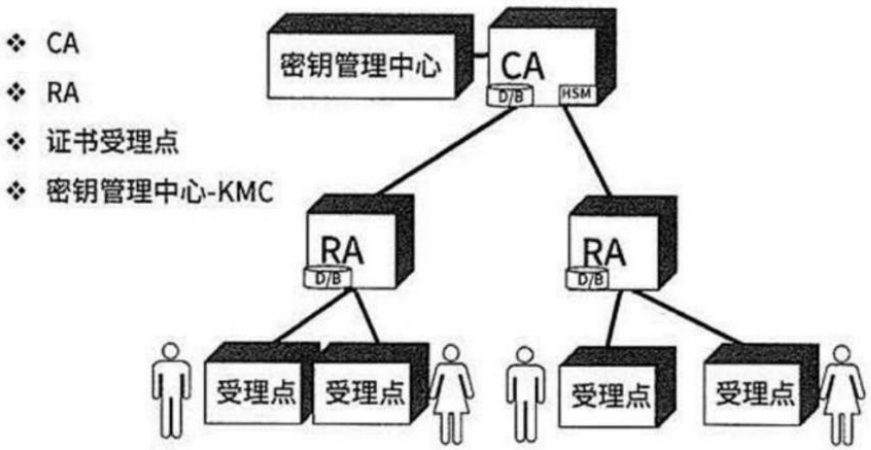
密钥管理技术-PKI公钥体系

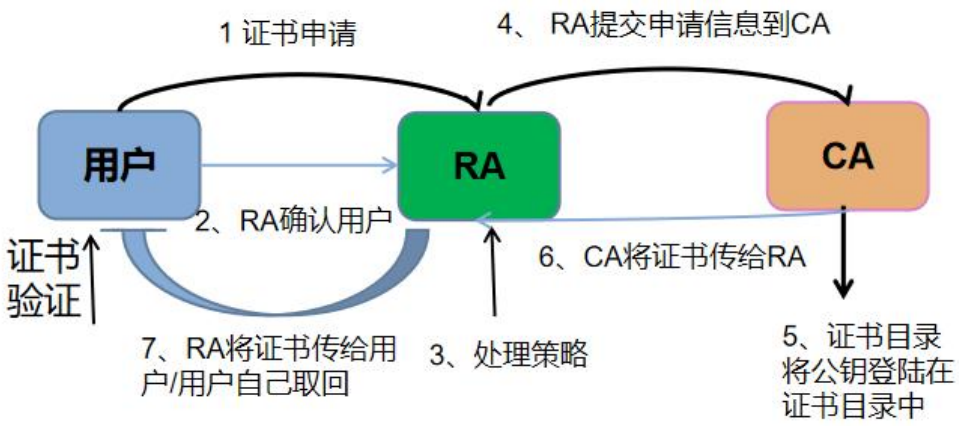
✓PKI是CA安全认证体系的基础，为安全认证体系进行密钥管理提供一个平台，它是一种新的我那网络安全技术和安全规范。

✓PKI包括公钥证书、证书管理机构、证书管理系统、围绕证书服务的各种软硬件设备及相应法律基础共同组成公开密钥基础设施PKI，公钥证书是最重要的组成部分

✓PKI包括签发证书的机构（CA），CA的任务：签发证书、管理和撤销证书（★）

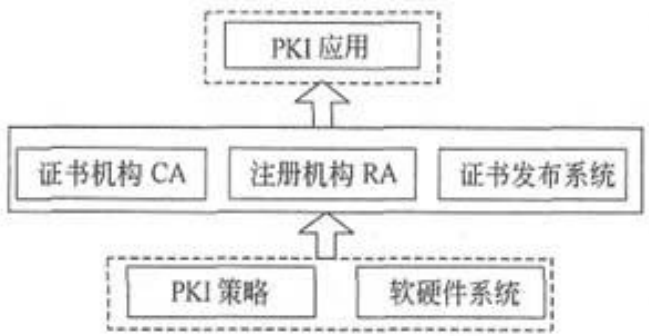
✓注册登记证书（RA）：接收证书申请人的注册信息，批准或拒绝证书申请、批准或拒绝恢复密钥申请、批准或拒绝恢复证书申请。（★）





典型真题

- 下图所示PKI系统结构中，负责生成和签署数字证书的是（1），负责验证用户身份的是（2）。



（1）A．证书机构CA　B．注册机构RA　C．证书发布系统　D．PKI策略

（2）A．证书机构CA　B．注册机构RA　C．证书发布系统　D．PKI策略

参考答案：（1）A （2）B

解析：在PKI系统体系中，证书机构CA负责生成和签署数字证书，注册机构RA负责验证申请数字证书用户的身份。

密钥管理技术-密钥分配

密钥分配一般要解决两个问题：
一是引进自动分配密钥机制，以提高系统的效率；二是尽可能减少系统中驻留的密钥量。

一、对称密钥的分配与管理（★★）
1.对称密钥的分配
两个用户A和B在获得共享密钥时有4种方式：
(1)经过A选取的密钥通过物理手段发送给另一方B。（快递等）
(2)由第三方选取密钥，通过物理手段分别发送给A和B。（中间人C）
(3)A、B 事先已有一个密钥，其中一方选取新密钥后，用已有密钥加密该新密钥后发送给另一方。
(4)三方 A、B、C各有一保密信道，C 选取密钥后，分别通过 A、B 各自的保密信道发送。（专用线路、无线电扩频通信等）

二、公钥(非对称密钥)加密体制的密钥管理（★★）
1.公开发布（本质--个人发布自己公钥）
用户将自己的公钥发送给每一位其他用户，或向某一团体广播。方法简单，但缺点是任何人都可以伪造密钥公开发布。如伪装成用户 A，以A 的名义向另一用户发送自己的公钥，则在 A 发现假冒者以前，假冒者可解读所有发向 A 的加密消息，甚至还能用伪造的密钥获得认证。

密钥管理技术-密钥分配

2.公用目录表--（可信组织发布公钥）
一个可信的实体或组织公用的公钥动态目录表，管理员为每个用户在目录表中建立一个条目，包括用户名和用户的公开密钥两个数据项。每个用户都亲自或以某种安全的认证通信在管理者那里注册自己的公钥。缺点是如果攻击者成功地获取管理员的密钥，就可以伪造一个公钥目录表，以后既可假冒任一用户又能监听发往任一用户的消息，且公用目录表还容易受到攻击者的攻击。
3.公钥管理机构
由公钥管理机构来为各用户建立、维护动态的公钥目录，采取更加严密的控制措施增强其安全性。用户都知道管理机构的公钥，当用户A 向公钥管理机构发送请求时，该机构对请求作出应答，并用自己的私钥加密后发送给A，A 再用机构的公钥解密。
缺点：因为每一用户要想和他人联系都须求助于管理机构，所以管理机构容易成为系统的瓶颈，并且管理机构维护的公钥目录表也容易被攻击篡改。
4.公钥证书
公钥证书是由证书管理机构 (CA) 为用户建立的，其中的数据项有与该用户的私钥相匹配的公钥及用户的身份和时间戳等，所有的数据项由 CA 用自己的私钥签字后就形成证书，即证书的形式为$CA_A=ESK_{CA}[T，ID_A，PK_A]$。T是当前的时间戳，$ID_A$是用户A的身份，$PK_A$是A的公钥，$ESK_{CA}$是CA的私钥，$CA_A$是为用户A 产生的证书。用户将自己证书发给另一用户B，而接收方B可用CA 的公钥 PK_{CA}对证书进行验证。这样通过证书交换用户间的公钥而无须再与公钥管理机构联系，避免了由统一机构管理带来的不便和安全隐患。

访问控制技术

◆访问控制技术

访问控制是指主体依据某些控制策略或权限对客体本身或是其资源进行的不同授权的访问。

1.访问控制的基本模型。（★）

访问控制包括3 个要素，即主体、客体和控制策略。

- ✓ 主体(Subject):是可以对其他实体施加动作的主动实体，简记为S。可以是用户所在的组织(用户组)、用户本身，也可是用户使用的计算机终端、卡机、手持终端(无线)等，甚至可以是应用服务程序或进程。
- ✓ 客体(Object):是接受其他实体访问的被动实体，简记为O。凡是可以被操作的信息、资源、对象都可以认为是客体。
- ✓ 控制策略:是主体对客体的操作行为集和约束条件集，简记为KS。控制策略是主体对客体的访问规则集，这个规则集直接定义了主体对客体的作用行为和客体对主体的条件约束。访问策略是一种授权行为。

访问控制包括认证、控制策略和审计三个方面的内容。

2.访问控制的实现技术（★★★）

1)访问控制矩阵

2)访问控制表

3)能力表

4)授权关系表

访问控制技术

1)访问控制矩阵

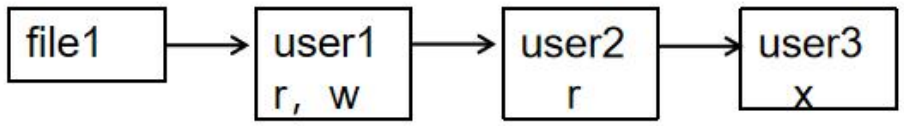
访问控制矩阵(ACM)以主体为行索引，以客体为列索引的矩阵，矩阵中的每一个元素表示一组访问方式，是若干访问方式的集合。即每个主体对哪些客体有哪些访问权限。查找、实现不方便。

用户	file1	file2	file3
User1	rw		rw
User2	r	rwx	x
User3	x	r	

2)访问控制表

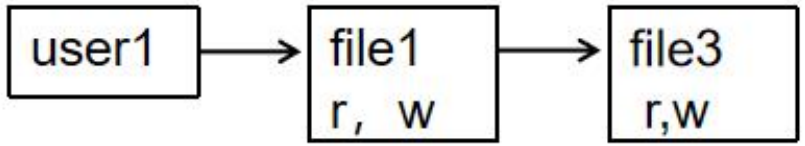
每个客体有一个访问控制表，是系统中每一个有权访问这个客体的主体的信息。实际上是按列保存访问矩阵。

访问控制表提供了针对客体的方便的查询方法，但是用访问控制表来查询一个主体对所有客体的所有访问权限是很困难。



访问控制技术

3)能力表
能力表(Capabilities)实际上是按行保存访问矩阵。每个主体有一个能力表，是该主体对系统中每一个客体的访问权限信息。使用能力表可以很方便地查询某一个主体的所有访问权限，只需要遍历这个主体的能力表即可。但查询对某一个客体具有访问权限的主体信息就很困难了，必须查询系统中所有主体的能力表。



4)授权关系表
每一行表示主体和客体的一个授权关系。对应访问矩阵中每一个非空元素的实现技术。
对表按主体进行排序，可以得到能力表的效率。
对表按客体进行排序，可以得到访问控制表的效率。
适合采用关系数据库来实现。

典型真题

以主体为行索引，以客体为列索引的矩阵，矩阵中的每一个元素表示一组访问方式，是若干访问方式的集合，属于（）。
A.访问控制矩阵.
B.访问控制表
C.能力表
D.授权关系表

参考答案：A

目录

信息安全的抗攻击技术

一、密钥的选择
密钥在概念上被分成两大类：数据加密密钥(DK)和密钥加密密钥(KK)。前者直接对数据进行加密，后者用于保护密钥，使之通过加密而安全传递。
算法的安全性在于密钥。（★）
为对抗攻击者的攻击，密钥的生成需要考虑 3 个方面的因素：（★）
1.增大密钥空间（更长的密钥长度） 2.选择强钥 3.密钥的随机性（密码不要有规律）

二、拒绝服务攻击与防御（★★★）
拒绝服务攻击(DoS)是借助于网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。
目前常见的拒绝服务攻击为分布式拒绝服务攻击(DDoS)。
1)拒绝服务攻击的分类
拒绝服务攻击主要有以下几种模式:
(1)消耗资源。攻击者利用系统资源有限这一特征，或者是大量地申请系统资源，并长时间地占用；或是不断地向服务程序发出请求，使系统忙于处理攻击者的请求，而无暇为其他用户提供服务。
攻击者可以针对以下几种资源发起拒绝服务攻击:
①针对网络连接的拒绝服务攻击。②消耗磁盘空间。③消耗CPU资源和内存资源。

信息安全的抗攻击技术

(2)破坏或更改配置信息。计算机系统配置上的错误也可能造成拒绝服务攻击，尤其是服务程序的配置文件以及系统、用户的启动文件。攻击者修改配置文件，从而改变系统向外提供服务的方式。
(3)物理破坏或改变网络部件。这种拒绝服务针对的是物理安全，其通过物理破坏或改变网络部件以达到拒绝服务的目的。其攻击的目标有计算机、路由器、网络配线室、网络主干段、电源、冷却设备，及其他的网络关键设备。
(4)利用服务程序中的处理错误使服务失效。

2)分布式拒绝服务攻击（★）
分布式拒绝服务攻击的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。分布式拒绝服务攻击克服了传统拒绝服务攻击的受网络资源限制和隐蔽性差两大缺点，危害性更大。
分布式拒绝服务攻击工具一般采用三级控制结构：

- ✓ Client (客户端)运行在攻击者的主机上，用来发起和控制分布式拒绝服务攻击。
- ✓ Handler(主控端)运行在已被攻击者侵入并获得控制的主机上，用来控制代理端。
- ✓ Agent(代理端)运行在已被攻击者侵入并获得控制的主机上，从主控端接收命令，负责对目标实施实际的攻击。

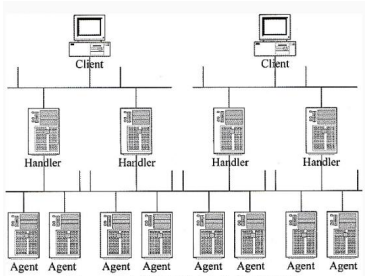


图 5-2　分布式拒绝服务攻击的三级控制结构

信息安全的抗攻击技术

3)拒绝服务攻击的防御方法（★★）
使用下面的方法尽量阻止拒绝服务攻击：
(1)加强对数据包的特征识别，通过搜寻特征字符串，就可以确定攻击服务器和攻击者的位置。
(2)设置防火墙监视本地主机端口的使用情况。对本地主机中的敏感端口进行监视，如UDP 31335、 UDP 27444、 TCP 27665。如果外部主机主动向网络内部高标号端口发起连接请求,则系统也很可能受到侵入。
(3)对通信数据量进行统计也可获得有关攻击系统的位置和数量信息。例如，在攻击之前，目标网络的域名服务器往往会接收到远远超过正常数量的反向和正向的地址查询。在攻击时，攻击数据的来源地址会发出超出正常极限的数据量。
(4)尽可能地修正已经发现的问题和系统漏洞。

信息安全的抗攻击技术

欺骗攻击与防御（★★★）
1.ARP欺骗
2.DNS欺骗
3.IP欺骗

信息安全的抗攻击技术

◆ARP欺骗（★★★）

又称ARP毒化或ARP攻击，是针对以太网地址解析协议(ARP)的一种攻击技术，通过欺骗局域网内访问者PC的网关MAC地址，使访问者PC错以为攻击者更改后的MAC地址是网关的MAC，导致网络不通。此种攻击可让攻击者获取局域网上的数据包甚至可篡改数据包，且可让网络上特定计算机或所有计算机无法正常连线。

ARP欺骗的防范措施：

(1)在WinXP下输入命令 arp -s gate-way-ip gate-way-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)使用ARP防护软件--ARP Guard。

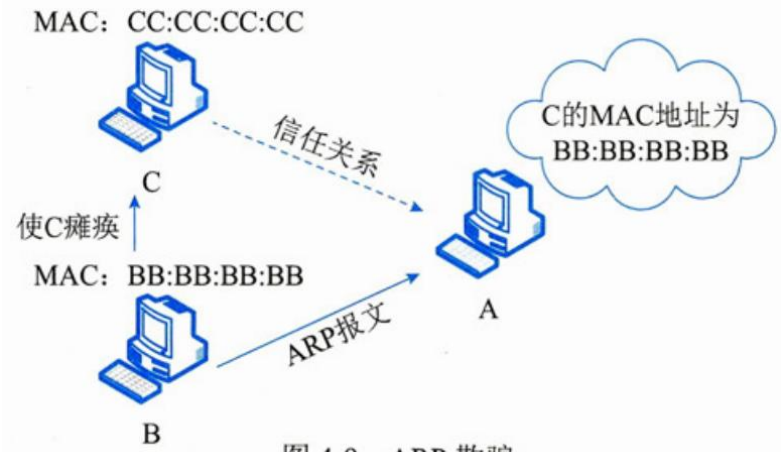


图 4-9　ARP 欺骗

信息安全的抗攻击技术

◆DNS欺骗（域名解析IP地址）（★★★）

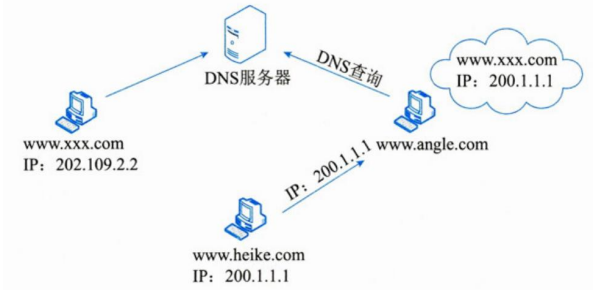
DNS欺骗首先是冒充域名服务器，然后把查询的IP地址设为攻击者的IP地址，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了。DNS欺骗其实并不是真的"黑掉"了对方的网站，而是冒名顶替、招摇撞骗罢了。

DNS欺骗的检测：根据检测手段的不同，将其分为被动监听检测、虚假报文探测和交叉检查查询三种。

①被动监听检测:该检测手段是通过旁路监听的方式，捕获所有DNS请求和应答数据包，并为其建立一个请求应答映射表。如果在一定的时间间隔内，一个请求对应两个或两个以上结果不同的应答包，则怀疑受到了DNS欺骗攻击，因为DNS服务器不会给出多个结果不同的应答包。

②虚假报文探测:该检测手段采用主动发送探测包的方式来检测网络内是否存在DNS欺骗攻击者。这种探测手段基于一个简单的假设:攻击者为了尽快地发出欺骗包，不会对域名服务器IP地址的有效性进行验证。如果向一个非DNS服务器发送请求包，正常来说不会收到任何应答，但是由于攻击者不会验证目标IP地址是否是合法DNS服务器，他会继续实施欺骗攻击，因此，如果收到了应答包，则说明受到了攻击。（比如诈骗电话，你虚拟个同学名字，这样你会知道受到欺骗）

③交叉检查查询:在客户端收到DNS应答包之后，向DNS服务器反向查询应答包中返回的IP地址所对应的DNS名字，如果二者一致说明没有受到攻击，否则说明被欺骗。



信息安全的抗攻击技术

◆IP欺骗（★★★）

指创建源地址经过修改的IP数据包，目的要么是隐藏发送方的身份，要么是冒充其他计算机系统。恶意用户往往采用这项技术对目标设备或周边基础设施发动 DDoS 攻击。虽然无法预防 IP 欺骗，但可以采取措施来阻止伪造数据包渗透网络。

入口过滤是防范欺骗的一种常见的防御措施，入口过滤是一种数据包过滤形式，通常在网络边缘设备上实施，用于检查传入的 IP 数据包并确定其源标头。如果这些数据包的源标头与其来源不匹配或者看上去很可疑，则拒绝这些数据包。

◆端口扫描（★★★）

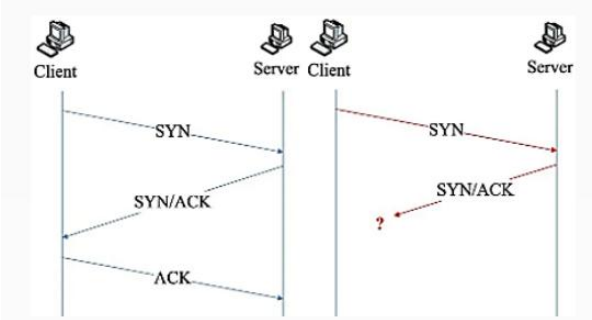
端口扫描就是尝试与目标主机的某些端口建立连接，如果目标主机该端口有回复，则说明该端口开放，即为"活动端口"。

通过端口扫描可以判断目标主机上开放了哪些服务，判断目标主机的操作系统。

例题：若一台服务器只开放了25和110两个端口，那么这台服务器可以提供（ ）服务。

A.E-Mail.　　B.WEB　　C.DNS　　D.FTP

信息安全的抗攻击技术



◆强化TCP/IP堆栈以抵御拒绝服务攻击（★★★）

1)同步风暴(SYN Flooding)

SYN Flood攻击中，利用TCP三次握手协议的缺陷，攻击者向目标主机发送大量伪造源地址的TCP SYN报文，目标主机分配必要的资源，然后向源地址返回SYN + ACK包，并等待源端返回ACK包。由于源地址是伪造的，所以源端永远都不会返回ACK报文，受害主机继续发送SYN + ACK包，并将半连接放入端口的积压队列中，虽然一般的主机都有超时机制和默认的重传次数，但由于端口的半连接队列的长度是有限的很快被填满，服务器拒绝新的连接，导致该端口无法响应其他机器的连接请求。

2)ICMP攻击

利用操作系统规定的ICMP数据包最大尺寸不超过64KB这一规定，向主机发起"Ping of Death"(死亡之Ping)攻击。"Ping of Death"攻击的原理是：如果ICMP数据包的尺寸超过64KB上限时，主机就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使主机死机。此外，向目标主机长时间、连续、大量地发送ICMP数据包，会形成"ICMP风暴"，使得目标主机耗费大量的CPU资源处理，最终使系统瘫痪。

3)SNMP攻击

SNMP是TCP/IP网络中标准的管理协议，它允许网络中的各种设备和软件，包括交换机、路由器、防火墙、集线器、甚至操作系统、服务器产品和部件等，能与管理软件通信，汇报其当前的行为和状态。但是,SNMP还能被用于控制这些设备和产品，重定向通信流，改变通信数据包的优先级，甚至断开通信连接。入侵者如果具备相应能力，就能完全接管你的网络。

信息安全的抗攻击技术

◆系统漏洞扫描（★）

系统漏洞扫描是对重要计算机信息系统进行检查，发现其中可能被黑客利用的漏洞。

系统漏洞扫描从底层技术来划分，可以分为：

- 基于网络的扫描
- 基于主机的扫描

1)基于网络的漏洞扫描

基于网络的漏洞扫描器是通过网络来扫描远程计算机中的漏洞。

基于网络的漏洞扫描器的优点:

(1)价格相对来说比较便宜。

(2)在操作过程中，不需要涉及目标系统的管理员。

(3)在检测过程中，不需要在目标系统上安装任何东西。

(4)维护简便。

2)基于主机的漏洞扫描

基于主机的漏洞扫描器通常在目标系统上安装一个代理(Agent)或者是服务(Services)，以便能够访问所有的文件与进程，这也使得基于主机的漏洞扫描器能够扫描更多的漏洞。

基于主机的漏洞扫描器具有如下优点:

(1)扫描的漏洞数量多。

(2)集中化管理。

(3)网络流量负载小。

典型真题

SYN Flooding攻击的原理是( )。
A.利用TCP三次握手，恶意造成大量TCP半连接，耗尽服务器资源，导致系统拒绝服务.
B.操作系统在实现TCP/IP协议栈时，不能很好地处理TCP报文的序列号紊乱问题，导致系统崩溃
C.操作系统在实现TCP/IP协议栈时，不能很好地处理IP分片包的重叠情况，导致系统崩溃
D.操作系统协议栈在处理IP分片时，对于重组后超大的IP数据包不能很好地处理，导致缓存溢出而系统崩溃
试题分析本题考查网络安全的知识。
SYN Flooding是一种常见的DOS(denial of service,拒绝服务)和DDoS(distributeddenial of service,分布式拒绝服务)攻击方式。它使用TCP协议缺陷，发送大量的伪造的TCP连接请求，使得被攻击方CPU或内存资源耗尽，最终导致被攻击方无法提供正常的服务。
参考答案(64)A

下列攻击方式中，( )不是利用TCP/IP漏洞发起的攻击。
A.SQL注入攻击.　　B.Land攻击　　C.Ping of Death　　D.Teardrop攻击
参考答案：A

目录

计算机信息系统安全保护等级

◆计算机系统安全保护等级（★★）

级别	名称	要点
第1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，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。
第2级	系统审计保护级	实施了粒度更细的自主访问控制，它通过登录规程、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3级	安全标记保护级	具有系统审计保护级所有功能+提供有关安全策略模型数据标记以及主体对客体强制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4级	结构化保护级	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+考虑隐蔽通道+加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。
第5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。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。排除了那些对实施安全策略来说并非必要的代码；在设计和实现时，将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

网络安全技术

◆**防火墙**是在内部网络和外部因特网之间增加的一道安全防护措施，分为网络级防火墙和应用级防火墙。（★★）

网络级防火墙层次低，但是效率高，因为其使用包过滤和状态监测手段，一般只检验网络包外在（起始地址、状态）属性是否异常，若异常，则过滤掉，不与内网通信，因此对应用和用户是透明的。

应用级防火墙，层次高，效率低，因为应用级防火墙会将网络包拆开，具体检查里面的数据是否有问题，会消耗大量时间，造成效率低下，但是安全强度高。

◆**入侵检测系统IDS**（★）

防火墙技术主要是分隔来自外网的威胁，却对来自内网的直接攻击无能为力，此时就要用到入侵检测IDS技术，位于防火墙之后的第二道屏障，作为防火墙技术的补充。

网络安全技术

◆入侵防御系统IPS

IDS和防火墙技术都是在入侵行为已经发生后所做的检测和分析，而IPS是能够提前发现入侵行为，在其还没有进入安全网络之前就防御。

在安全网络之前的链路上挂载入侵防御系统IPS，可以实时检测入侵行为，并直接进行阻断，这是与IDS的区别，要注意。

◆杀毒软件

用于检测和解决计算机病毒，与防火墙和IDS要区分，计算机病毒要靠杀毒软件，防火墙是处理网络上的非法攻击。

◆蜜罐系统（★）

伪造一个蜜罐网络引诱黑客攻击，蜜罐网络被攻击不影响安全网络，并且可以借此了解黑客攻击的手段和原理，从而对安全系统进行升级和优化。

信息安全风险管理

◆安全风险管理（★）
信息安全风险是指各类应用系统及其赖以运行的基础网络、处理的数据和信息，由于其可能存在的软硬件缺陷、系统集成缺陷等，以及信息安全管理中潜在的薄弱环节，而导致的不同程度的安全风险。

1.风险评估的实施流程（★）
- 确定风险评估的范围
- 确定风险评估的目标
- 建立适当的组织结构
- 建立系统的风险评估方法
- 获得最高管理者对风险评估策划的批准

2.风险评估
风险评估的基本要素：脆弱性、资产、威胁、风险和安全措施。（★）
风险评估是对信息资产存在的脆弱性，面临的威胁， 造成的影响，及三者综合作用所带来的风险的可能性评估。

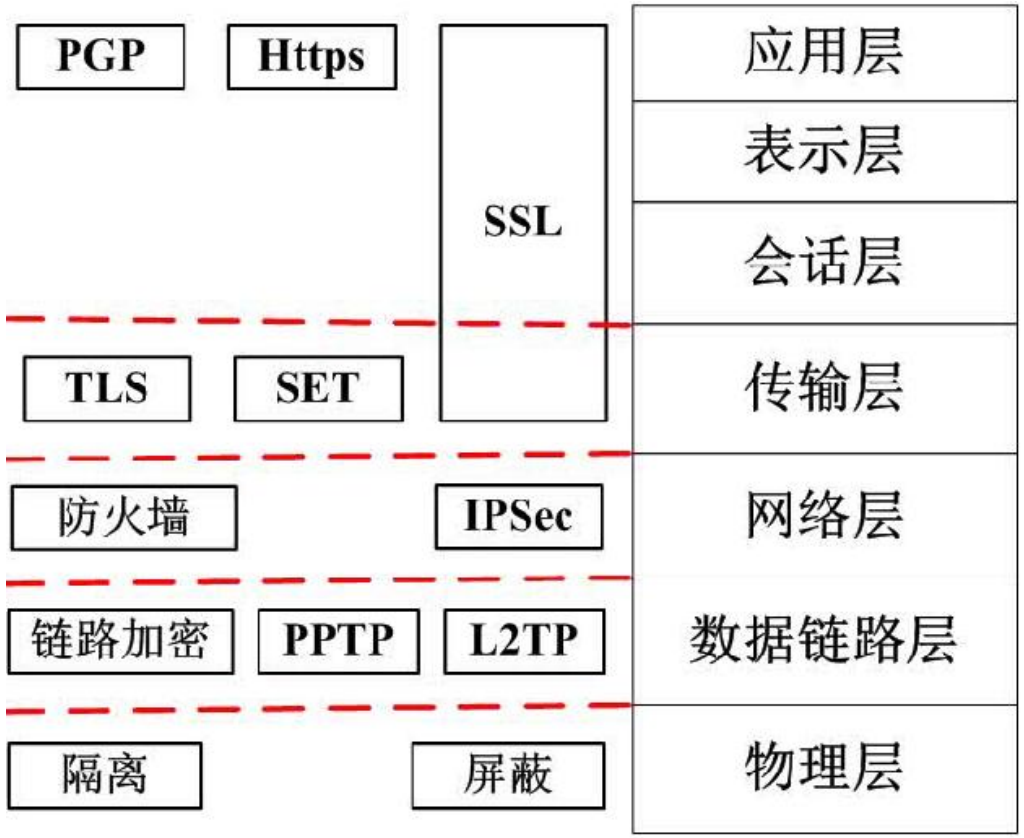
信息安全风险管理

风险计算模型包含信息资产、弱点／脆弱性、威胁等关键要素。每个要素有各自的属性， 信息资产的属性是资产价值，弱点的属性是弱点被威胁利用后对资产带来的影响的严重程度，威胁的属性是威胁发生的可能性。

风险计算的过程如下。：（★）
(1 ）对信息资产进行识别，并对资产赋值。
(2 ）对威胁进行分析，并对威胁发生的可能性赋值。
(3 ）识别信息资产的脆弱性，并对弱点的严重程度赋值。
(4 ）根据威胁和脆弱性计算安全事件发生的可能性。
(5 ）结合信息资产的重要性和发生安全事件的可能性，计算信息资产的风险值。

补充-网络安全协议

◆网络安全协议（★★）



- TLS：传输层安全协议
- IPSEC：安全协议在IP协议中增加了两个基于密码的安全机制-认证头（AH）和封装安全载荷（ESP）：认证头（AH）支持IP数据项的认证性和完整性和封装安全载荷（ESP）实现了通信的机密性。对IP包加密。
- PGP协议： PGP是一个基于RSA的邮件加密软件，还可用于文件存储的加密。PGP承认两种不同的证书格式：PGP证书和X.509证书，PGP证书包括PGP版本号、证书持有者公钥、证书持有者信息、证书拥有者的数字签名、证书的有效期、密钥的首选的对称加密算法。
- Https： HTTPS使用端口443，它的主要作用可以分为两种，一种是建立一个信息安全通道，来保证数据传输的安全；另一种就是确认网站的真实性。

补充-网络安全协议

◆Kerberos（★★）

Kerberos是一种网络身份认证协议，该协议的基础是基于信任第三方，它提供了在开放型网络中进行身份认证的方法，认证实体可以是用户也可以是用户服务。这种认证不依赖宿主机的操作系统或计算机的IP地址，不需要保证网络上所有计算机的物理安全性，并且假定数据包在传输中可被随机窃取和篡改。

Kerberos提供了一种单点登录(SSO)的方法。考虑这样一个场景，在一个网络中有不同的服务器，比如，打印服务器、邮件服务器和文件服务器。这些服务器都有认证的需求。 很自然的，让每个服务器自己实现一套认证系统是不合理的，而是提供一个中心认证服务器(AS-Authentication Server)供这些服务器使用。这样任何客户端就只需维护一个密码就能登录所有服务器。

因此，在Kerberos系统中至少有三个角色：认证服务器(AS),客户端(Client)和普通服务器(Server)。

客户端和服务器将在AS的帮助下完成相互认证。

在Kerberos系统中，客户端和服务器都有一个唯一的名字。同时，客户端和服务器都有自己的密码，并且它们的密码只有自己和认证服务器AS知道。

客户端在进行认证时，需首先向密钥分发中心来申请初始票据。

Kerberos使用时间戳来防止重放攻击

MIME(Multipurpose Internet Mail Extensions)中
文名为：多用途互联网邮件扩展类型。

典型真题

通常使用（ ）为IP数据报文进行加密。
A.IPSec.　　B.PP2P　C.HTTPS　　D.TLS

某电子商务网站为实现用户安全访问，应使用的协议是( ) .
A. HTTP　　B. WAP　　C. HTTPS.　　D. IMAP

以下用于在网络应用层和传输层之间提供加密方案的协议是（ ）。
A.PGP　　B.SSL.　　C.IPSec　　D.DES

下面可提供安全电子邮件服务的是()。
A.RSA　　B.SSL　　C.SET　　D.S/MIME.

采用Kerberos系统进行认证时，可以在报文中加入()来防止重放攻击。
A.会话密钥　B.时间戳　C.用户ID　D.私有密钥

参考答案：A、C、B、D、B

本章重点回顾

1、信息安全属性
2、对称加密、非对称加密、数字摘要、数字签名等
3、抗攻击技术

THANKS