04121100/信息安全概论	分散期末考试-0412	2024-06-17(19:00-20:25)	2106	无简称	临海校区	30	郭文平

笔试、闭卷

题型及分值：填空 20 个*2 分＝40 分，简答题 4 个*10 分＝40 分，综合题 1 个*20 分＝20 分

信息安全概述

1. 领导机构

中共中央网络安全和信息化领导小组组长：**习近平**

2. 信息安全的定义

网络安全是在分布网络环境中，对信息载体（处理载体、存储载体、传输载体）和信息的处理、传输、存储、访问提供安全保护，以防止数据、信息内容或能力拒绝服务或被非授权使用和篡改。（中国）

网络安全保护的总体思路：**“适度安全、保护重点”**

理解网络安全的重要性的三个层次：

- 从最高层次来讲，网络安全关系到国家的安全；
- 对组织机构来说，网络安全关系到组织机构的正常运作和持续发展；
- 就个人而言，网络安全是保护个人隐私和财产的必然要求；

3. 信息安全的属性

（1）机密性

机密性是指保证信息与信息系统不被非授权者所获取与使用，主要防范措施是密码技术。

（2）完整性

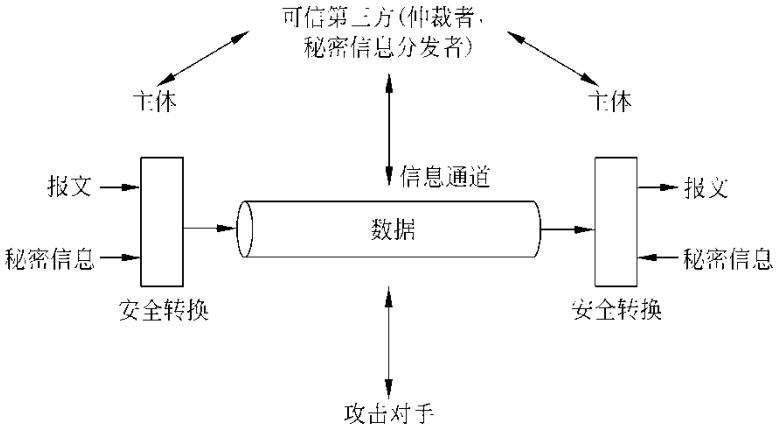
完整性是指信息是真实可信的，其发布者不被冒充，来源不被伪造，内容不被篡改，主要防范措施是校验与认证技术。

（3）可用性

可用性是指保证信息与信息系统可被授权人正常使用，主要防范措施是确保信息与信息系统处于一个可靠的运行状态之下。

4. 网络安全模型

报文从源站经网络（Internet）送至目的站，源站和目的站是处理的两个主体，它们必须协同处理这个交换。



在设计网络安全系统时，该网络安全模型应完成 4 个基本任务：

（1） 设计一个算法以实现和安全有关的转换。

（2） 产生一个秘密信息用于设计的算法。

（3） 开发一个分发和共享秘密信息的方法。

（4） 确定两个主体使用的协议，用于使用秘密算法与秘密信息以得到特定的安全服务。

信息安全风险评估

1. 信息资产的类型一般可分成以下 4 类。

（1） 物理资源

（2） 知识资源

（3） 时间资源

（4） 信誉（感觉）资源

信息资产一旦受到威胁和破坏，就会带来两类损失，一类是**即时的损失**；另一类是**长期的恢复所需花费**；

2. 攻击类型

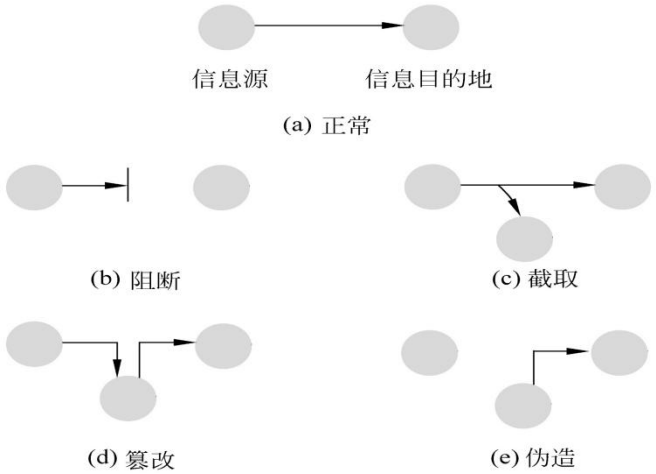
从安全属性来看，攻击类型可分为以下 4 类，要会画出示意图：

（1） 阻断攻击

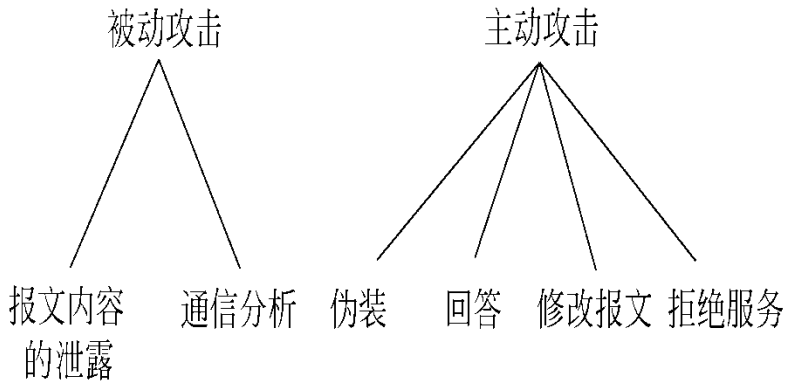
（2） 截取攻击

（3） 篡改攻击

（4） 伪造攻击



从攻击的发起方来区分，分为被动攻击和主动攻击。



被动攻击企图了解或利用系统信息但是不影响系统资源；

对付被动攻击的重点是**防范而不是检测；**

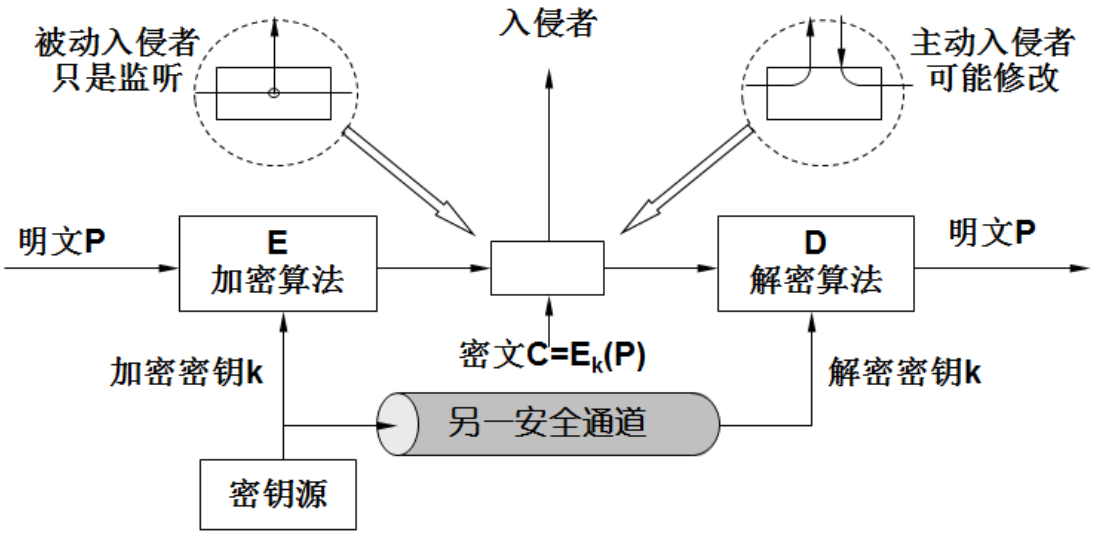
主动攻击则试图改变系统资源或影响系统操作。

对付主动攻击的重点在于检测**主动攻击并从导致的破坏或延迟中恢复过来。**

3. 风险是丢失需要保护的资产的可能性。威胁＋漏洞＝风险

密码学基础

1. 传统的基于对称密钥的加密模型

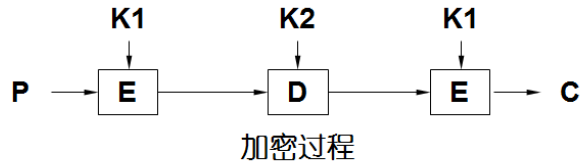


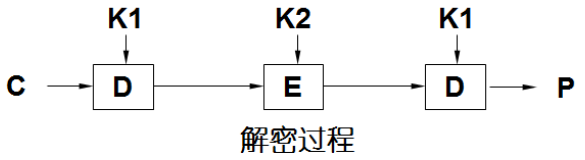
一个对称加密方案由 5 部分组成：
（明文、加密算法、密钥、密文、解密算法）
对称加密的安全使用有两个要求：
（1）需要一个强加密算法；
（2）发送者和接收者必须通过一个安全的方式获得密钥并且保证密钥安全。
对称加密的安全取决于**密钥**的保密性而非**算法**的保密性（**Kerckhoff 法则**）

2. 密码体制
（1）明文转换成密文的操作类型（**替换和换位**）；
（2）使用的密钥数（[对称、单钥、秘密密钥、传统加密]、[不对称、双钥、公开密钥]）
（3）明文的处理方式（分组密码和流密码）
3. 加密方案的计算安全性
（1）破解密文的代价超出被加密信息的价值；
（2）破解密文需要的时间超出信息的有用寿命；
4. 对称加密算法—**DES（Data Encryption Standard）数据加密标准**
明文按 64 bit 块加密，生成 64 bit 的密文，此算法有一个 56 bit 的密钥作为参数（另加 8 bit 的奇偶位）

解决 DES 算法中密钥太短的问题，由 IBM 公司提出 **3 重 DES （Triple DES）**

- **具体方法：用两个 DES 密钥、三个 DES 阶段来完成加密，首先，用 K1 对明文进行 DES 加密，然后用 K2 进行 DES 解密，最后再用 K1 进行 DES 加密，产生最终的密文**
- **解密的方法正好相反**





DES的三重加密和解密

对称密钥加密模式（其目的是希望同一明文，同一加密方式，同一密钥，产生的密文不同）

（1）电子代码本模式

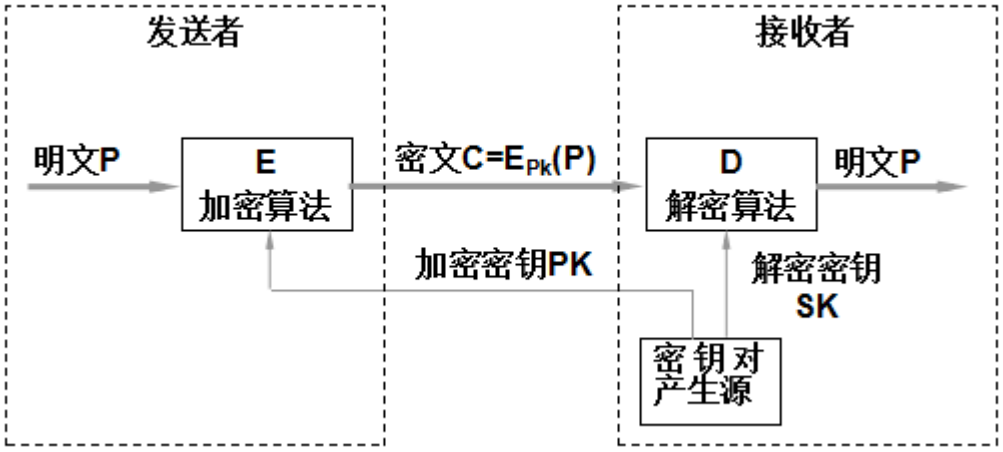
（2）密码块连接模式

（3）密码反馈模式

（4）流加密模式

（5）计数器模式

5. 公开密钥加密模型（最典型的算法是 RSA，基于数论）



密钥的选取

- 选择两个大质数，p和q（典型地为1024 bit）
- 计算n = p * q和z =（p - 1）*（q - 1）
- 选择一个与z互质的数d , (d, n)为解密密钥
- 找出e, 使e * d（mod z）= 1 (e,n)为加密密钥

公开密钥（加密密钥 ）为（e、n）

私有密钥（解密密钥 ）为（d、n）

加密密钥和解密密钥可互换

n为可编码的最大数

加密和解密算法

- 把明文看成一个bit串，并划分成每块k个bit，满足$2^k < n$，$P = 2^k$
  - 对原始信息P加密：

    使用公开密钥为（e、n），计算密文$C = P^e$（mod n）
  - 对加密信息C解密：

    使用私有密钥为（d、n），计算明文$P = C^d$（mod n）

加密和解密算法举例

- 选择p = 3，q = 11（实际中p、q为大质数）（Tnbm P754）

  n = p * q = 33，z =（p - 1）*（q - 1）= 20

  因为7与20互质，所以选择d = 7

  7e（mod 20）= 1的数有21、41、61、81、101……

  可选e = 3

  对原始信息P加密：

  即计算密文$C = P^3$（mod 33）使用的公开密钥为（3、33）

  对加密信息C解密：

  即计算明文$P = C^7$（mod 33）使用的私有密钥为（7、33）

《Computer Networks V4》 cs.sjtu 2022/5/24

加密和解密算法举例

- $P = 2^k < 33$，k = 5即用5bit表示一个信息，有32种表示
- 分别用其中的1 – 26表示26个英文字母A - Z

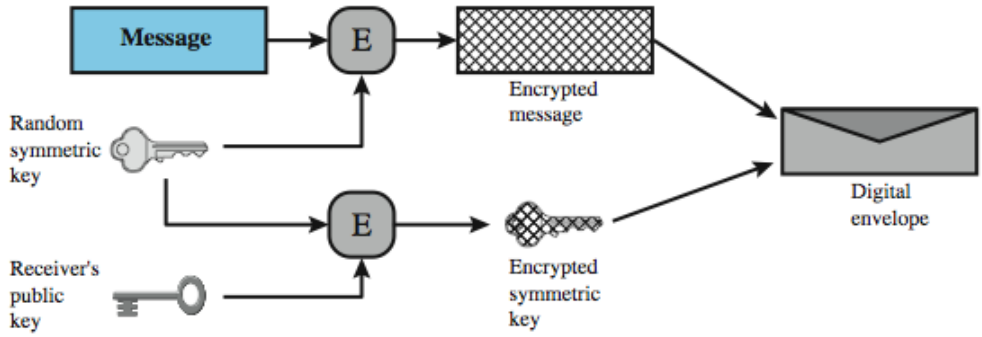
  如明文为SUZANNE可表示为19 21 26 01 14 14 05

明文(P)			密文(C)		解密后	
符号	数值	P^3	P^3(mod 33)	C^7	C^7(mod 33)	符号
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	1	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	5	E

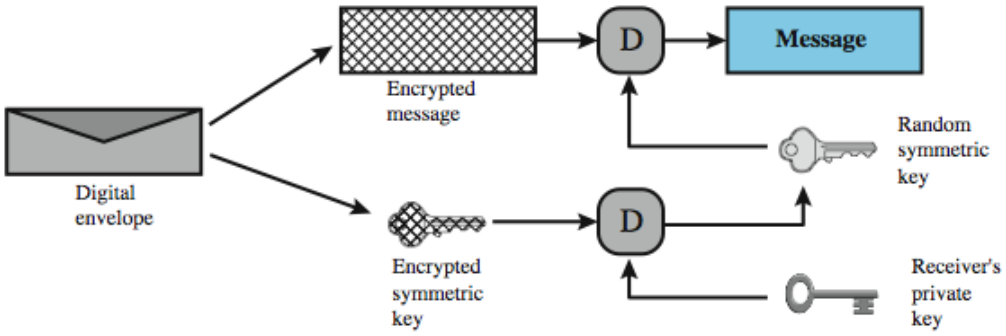
发送者的计算　　接收者的计算

- **对称密码体系的最大特点是加密速度快，适合加密大数据量，但是密钥分发困难；**
- **非对称密码体系很适合加密和认证，但是速度慢，不适合大数据量的加密；**

利用对称加密体制和公开密钥体制的优点进行综合设计，即所谓的数字信封技术



(a) Creation of a digital envelope



(b) Opening a digital envelope

画出示意图（a）是加密过程；（b）是解密过程；

加密工作过程：

对于一段明文（message），随机选择一个对称密钥进行加密变成密文。再选择接收方的公钥对这个对称密钥进行加密，和密文一起组成一个数字信封发送给接收者。

解密工作过程：

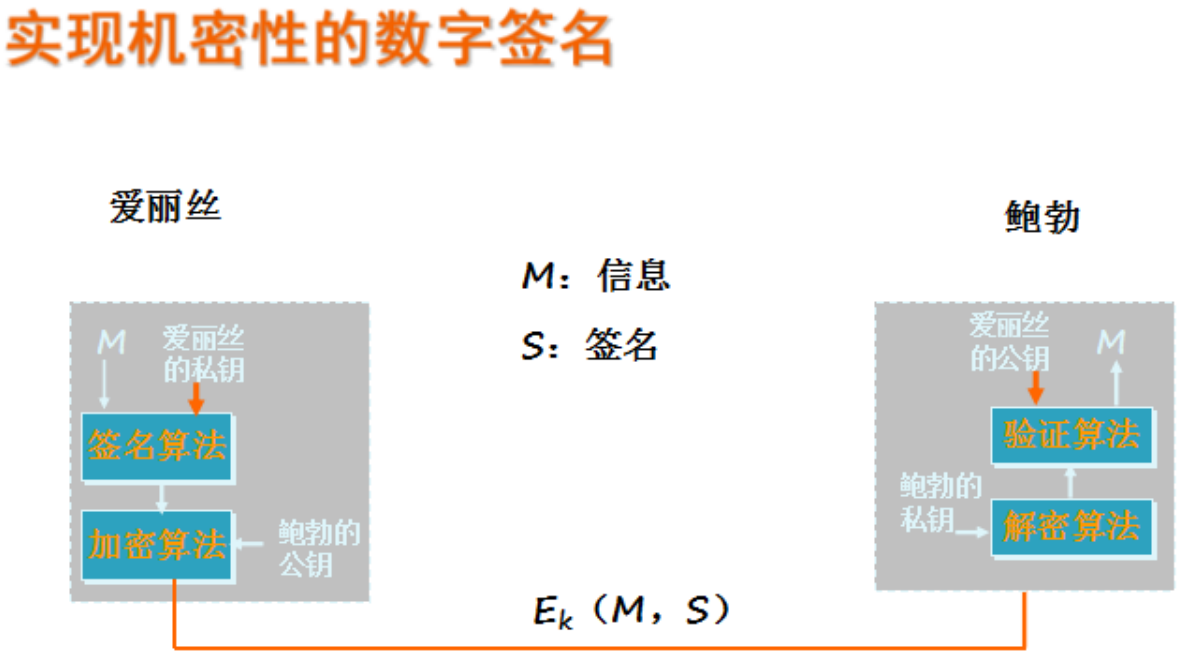
接收文收到数字信封后，分离出密文和加密的对称密钥，用自己的私钥来解密这个对称密钥，然后用解密后的对称密钥对密文进行解密，得到明文，这样完成解密过程。

6. 消息认证和数字签名

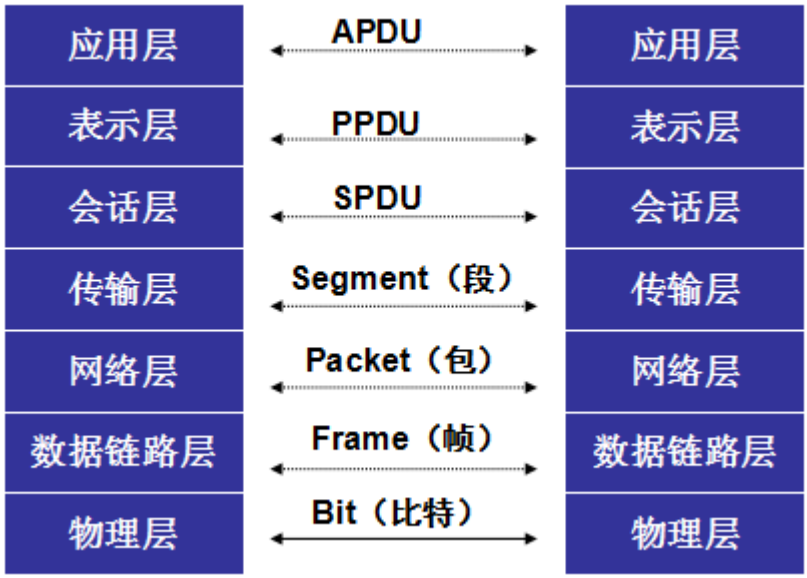
信息的完整性和抗否认性也是信息安全的重要内容，保证信息的完整性和抗否认性主要通过消息认证和数字签名来实现。

一般说来产生认证符的方法可以分为以下三类：
信息加密：将明文加密后以密文作为认证符。
消息认证码（MAC）： 用一个密钥控制的公开函数作用后产生的固定长度的数值，也称为密码校验和。
散列函数：一个将任意长度的消息映射为定长的散列值的函数，散列值作为认证符。

思考：若需要既提供保密同时也提供认证和签名可用什么方案（画出示意图，并说出整个工作过程）？



OSI 参考模型与 TCP IP 模型



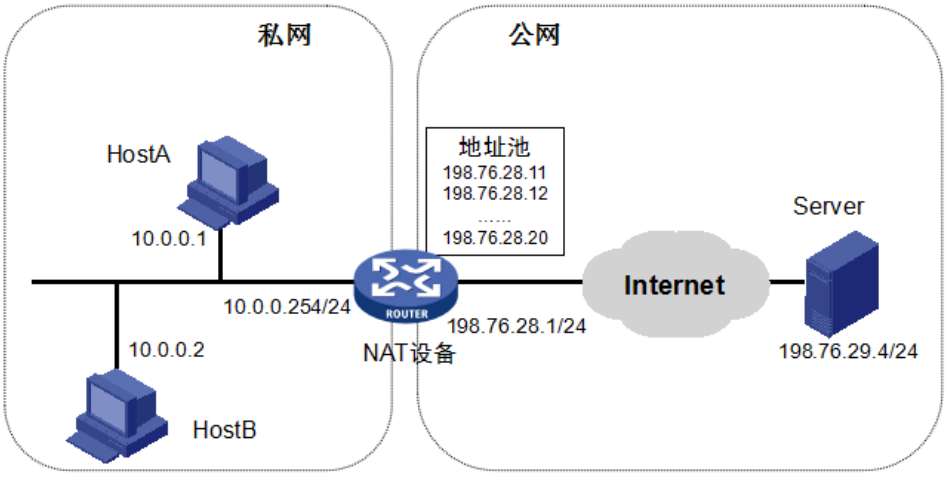
网络层的主要协议：IP、ICMP、IGMP
传输层的主要协议：TCP、UDP
应用层的主要协议：Telnet、FTP/TFTP、SMTP/POP3、SNMP/HTTP

通配符掩码（或叫反掩码）和 IP 地址结合使用以描述一个地址范围
通配符掩码（或叫反掩码）和子网掩码相似，但含义不同
0 表示对应位须比较
1 表示对应位不比较

1. 什么是反掩码？
答：与 IP 地址结合，扫描一个地址范围。0 表示需要比较，1 表示不需要比较。
2. 禁止 192.168.1.45 这个地址访问网络，写出对应的反掩码
答：rule 1 deny 192.168.1.45 0.0.0.0
3. Rule1 deny source 192.168.1.67 0.0.0.15,请写出这些规则的含义
答：禁止 192.168.1.64~79 访问网络
Rule1 deny source 192.168.1.97 0.0.0.15,
Rule1 deny source 192.168.1.17 0.0.0.15,

192.168.1.01000011
00001111
4. Rule 2 deny source 192.168.1.13 0.0.255.255
Rule 3 permit source 192.168.1.13 0.0.0.63
（1） 如果 match-order config，则 rule2 和 rule3 两条规则的含义是什么？
match-order config 配置优先
有效：Rule 2 deny source 192.168.1.13 0.0.255.255
禁止：192.168.0.0~192.168.255.255 地址段访问网络
（2） 如果 match-order auto，则 rule2 和 rule3 两条规则的含义是什么？
match-order auto 深度优先（地址范围小的优先）
禁止：192.168.0.0~192.168.255.255 地址段访问网络
还允许：192.168.1.0~192.168.0.63 地址段访问网络

网络地址转换
私有地址范围：
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255



防火墙是隔离在内部网络与外部网络之间的一个防御系统。具有以下属性：

（1）防火墙是不同网络或者安全域之间信息流的唯一通道，所有双向数据流必须经过防火墙。

（2）只有经过授权的合法数据，即防火墙安全策略允许的数据才可以通过防火墙。

（3）防火墙系统应该具有很高的抗攻击能力，其自身可以不受各种攻击的影响。

简而言之，防火墙是位于两个(或多个)网络间，实施访问控制策略的一个或一组组件集合。

信息系统安全等级保护

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息、公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

“公安部为牵头单位”

信息安全等级保护流程，即五个环节：定级、备案、建设整改、等级测评、监督检查

开展等级保护工作的基本要求

（1）准确定级；（2）严格审批；（3）及时备案；（4）认真整改；（5）科学测评

定为三级的每年检查一次，四级的每半年检查一次

信息和信息系统安全保护等级

第一级为**自主保护级**，适用于一般的信息和信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益；

第二级为**指导保护级**，适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害；

第三级为**监督保护级**，适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害；

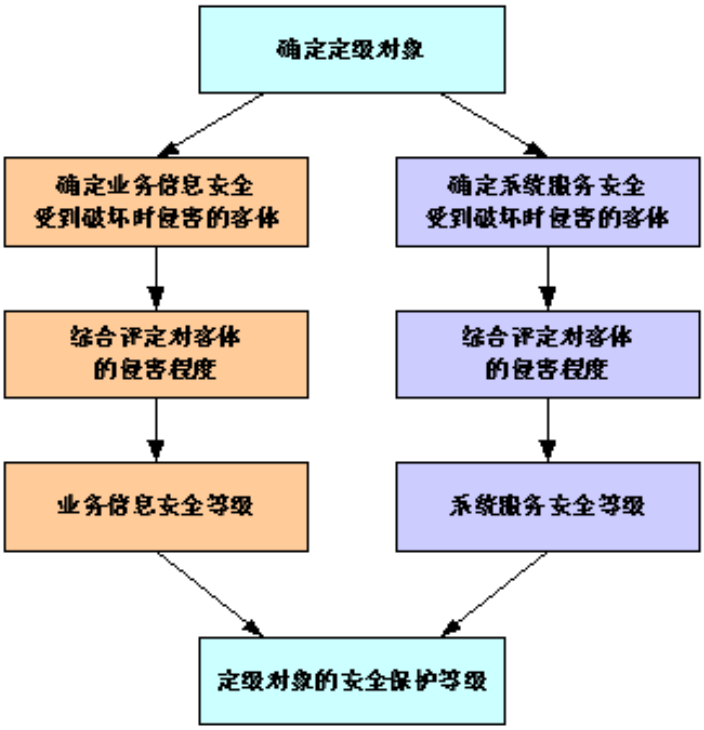
第四级为**强制保护级**，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成严重损害；
第五级为**专控保护级**，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害；

信息安全等级定级原则：
“自主定级、专家评审、主管部门审批、公安机关审核”
如何开展定级工作：
“谁主管谁负责、谁运营谁负责”
*运营、使用单位和主管部门是信息系统安全的第一责任人
信息系统的安全保护等级由**等级保护对象受到破坏时侵害的客体**和对**客体造成侵害的程度**两个定级要素决定。
受侵害客体
（1）公民、法人和其他组织的合法权益；
（2）社会秩序、公共利益；
（3）国家安全
对客体的侵害程度
（1）造成一般损害
（2）造成严重损害
（3）造成特别严重损害

表3-1 定级要素与安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

定级流程



业务信息安全和系统服务安全分别确定后，就高（取两者的高等级）确定信息系统安全等级。

微观思考题

结合自身经历和所学课程内容，你自身碰到过哪些计算机安全/网络安全问题，你是如何解决的？并谈谈目前计算机安全/网络安全面临的挑战？

宏观思考题

2013 年 6 月，前美国中央情报局雇员、现国家安全局防务承包商博斯艾伦公司(Booz Allen Hamilton Consulting Firm) 雇员爱德华·约瑟夫· 斯诺登(Edward Joseph Snowden) 揭露了美国政府的相关秘密监控工程和入侵行为，导致全球舆论震荡，被媒体称为“棱镜门”。

另外，在以思科为代表的美国 IT“八大金刚”思科（cisco）、IBM、谷歌（Google）、高通（Qualcomm）、英特尔（Intel）、苹果（Apple）、Oracle（甲骨文）、微软（Microsoft），主导了全球 IT 行业的发展。

还有近年来，我国出现了许多网络安全事件。

这些事件暴露出中国在网络与信息安全方面的弱点（或者说战略失误）是什么？我国在网络与信息安全方面应如何应对挑战？

可以围绕以下展开论述：
基础信息网络和重要信息系统在技术方面依赖进口；
网络安全保障工作方面的基础比较薄弱；
网络安全意识和安全防范能力薄弱；

信息系统安全建设和监管缺乏依据和标准；
安全保护措施和安全制度不落实；
监管措施不够到位。

网络安全处理流程

1.事件评估；2.事件上报；3.事件处理；4.事件监测；5.事后评估
（1）综合整个网络故障情况，确定应急事件类型（有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事故）和应急事件等级（特别重大事件、重大事件、较大事件、一般事件）；
（2）根据相关规定上报上级领导或上级主管部门；
（3）通知相关人员，启动应急预案，采取有效措施防止事件进一步扩大，尽可能减少负面影响；采用技术手段，尝试快速恢复网络系统；
（4）当应急事件成功处置后，还要持续监测，确认应急事件已根除，系统恢复到正常工作状况；
（5）事后评估，评估事件造成的损失，查找事件发生的原因。对存在的风险点进行整改，根据事件处理情况，进一步优化应急预案等。

相关的一些网络安全相关的法律法规。

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日通过，现予公布，自 2017 年 6 月 1 日起施行。

《中华人民共和国个人信息保护法》（2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过）本法自 2021 年 11 月 1 日起施行。