安全概念

8个安全机制：加密、数字签名、访问控制、信息完整性、鉴别交换、业务量填充、路由控制、公证

（鉴公路业签完加访）

5个安全服务：认证、访问控制、机密性、完整性、不可否认性（访不认完机）

安全体系：安全管理：安全运维中心、安全测评

安全技术：身份认证、访问控制、PKI、VPN、数据安全、防火墙、入侵检测

安全属性：机密性、完整性、可用性、可控性、不可否认性、可认证、可追溯、真实、可靠、匿名、隐私

（不用完机控）

安全威胁：对安全的一种潜在的危害（信息泄露、信息破坏、拒绝服务）

安全风险：安全事件发生的可能性

安全模型：P2DR：策略、保护、检测、响应

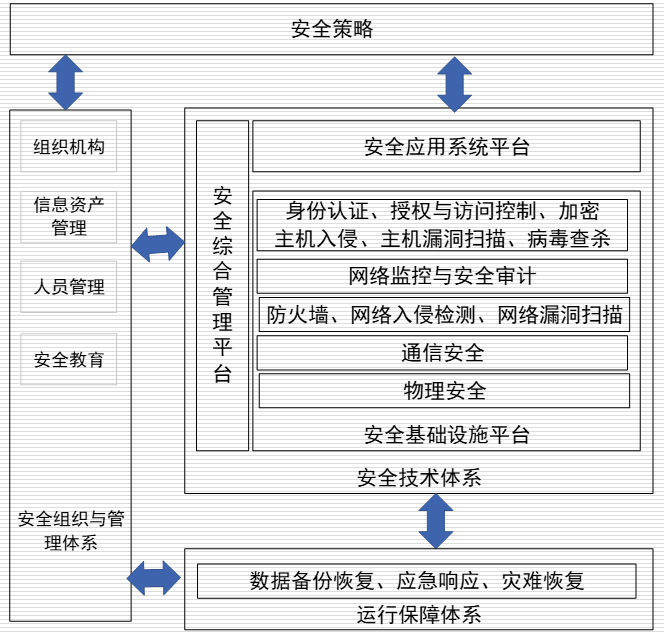
PDRR：保护、检测、响应、恢复

P2DR2：策略、保护、检测、响应、恢复

WPDRRC：预警、PDRR、反击

安全防御的原则：1、分层性原则 2、最小授权 3、简单性

信息安全保障体系：



安全管理

信息安全管理概念：是基于风险的安全管理，为了实现信息系统的安全目标，针对系统中需要保护的工作对象，通过技术和管理的手段，将系统潜在的风险控制在可接受的范围内

安全管理步骤：1、确定信息系统的安全目标 2、执行安全风险评估 3、选择合适的安全措施 4、编写计划和规程确保措施实施 5、检测实施过程

信息安全管理体系（ISMS）：组织在整体或特定范围内建立信息安全方针和目标，以及所用方法的体系

信息安全管理模型：PDCA 【计划、实施、检查、处理】

安全引用监控器（SRM）：负责对运行在用户模式代码的各种资源存取请求进行检查

DEP：数据执行保护，使指定内存页不具有可执行属性，堆栈不可执行

ASLR：地址空间布局随机化：随机排列程序的关键数据区域的位置

域：一批具有集中安全授权机构和若干工作站和成员服务器的计算机集合

AD：一个分布式的目录服务，信息可以分散在多台不同的计算机上

AD的关键机制：1、单点登录 2、全局目录 3、多主复制 4、组策略

站点：一个高速连接所形成的较快通信速率网络

组策略组成：分为GPC和GPT，GPC保存对象属性和版本信息，GPT保存组策略设置

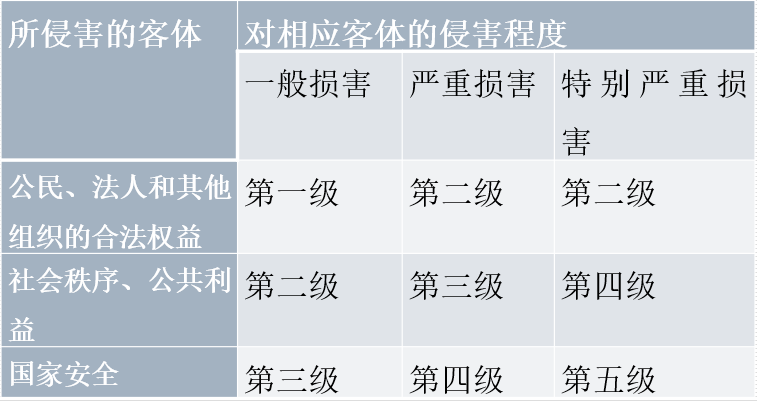
组策略优先级：本地策略🡪站点🡪域🡪OU策略

TCSEC：指导信息安全产品的制造和应用，为信安产品的测评提供准则和方法，是针对孤立的计算机系统，特别是小型机和主机系统。存在无保护级别、自主保护等级、强制保护等级、验证保护等级这四个安全级别。

CC：适于硬件、固件和软件实现的信息技术安全措施，不包括与技术没有直接关联的属于行政性管理安全措施的安全评估标准。CC有七个等级，EAL1到EAL7,包括：安全功能需求，安全保障需求，和评估模型。

EAL1:功能测试、EAL2:结构测试、EAL3:系统测试和检查、EAL4:系统设计、测试和复查、EAL5:半形式化设计和测试、EAL6:半形式化验证半的设计和测试、EAL7:形式化验证的设计和测试

等保：客体，保护对象定级: 5个安全保护等级划分，分别是自主保护、指导保护、监督保护、强制保护、专控保护



主体，5个安全保护能力等级划分

第一级：应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难， 及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

第二级：应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难以及其他相当危害程度的威胁，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

第三级：应能够在统一安全策略下防护系统免受来自外部有组织的团体,拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

第四级：应能够在统一安全策略下防护系统免受来自国家级的、敌对组织的**、**拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件， 在系统遭到损害后，能够迅速恢复所有功能

PKI

PKI的概念：公钥基础架构PKI是一个安全基础设施，用来实现基于公钥密码体制的密钥和

证书的产生、管理、存储、分发和撤销等功能。

X.509证书：X.509是密码学里公钥证书的格式标准。含有公钥、身份信息、签名信息。

认证机构CA：是公钥基础设施中受信任的第三方实体，是信任的起点，向主体颁发证书， 证书吊销列表CRL，续借和更新证书。

职责： ▪ 验证并标识证书申请者的身份；

▪ 确保CA用于签名证书的公钥的质量；

▪ 证书材料信息（包括公钥证书序列号、CA标识等）的管理；

▪ 确定并检查证书的有效期限；

▪ 确保证书主体标识的唯一性，防止重名；

▪ 发布并维护作废证书表，对整个证书签发过程作日志记录；

▪ 向申请人发通知

分类：单个CA、分级结构、网状结构、桥式CA

证书的验证步骤：第一步：验证真实性。证书是否为可信任的CA认证中心签发？

 第二步：验证有效性。证书是否在证书的有效使用期之内。

 第三步：验证可用性。证书是否已废除。

 第四步：验证证书结构中的证书用途。

证书结构：颁发者Issuer、主体Subject、证书公钥信息、签名算法、有效期、序列号、拓展项

证书吊销：周期发布机制、在线查询机制

MITM攻击：即中间人攻击，发送自己的密文给A，发送自己的公钥给B。

PKI的安全性：对证书传输过程的攻击、对CA认证过程的攻击、对CA签名过程的攻击、对算法的攻击、对用户确认的攻击。

抵御中间人攻击：3种情况，(1)攻击者转发真实证书—直接失败 (2) 攻击者创建一个伪造证书—浏览器会警告 (3) 攻击者发送自己的证书—直接失败

交叉认证：独立的CA双方交叉认证(也就是互相发放证书)，结果是在对等的CA中产生了信任关系网。信任仅存在于这两个CA及其下面的子CA之间。

PKI能力：认证(数据源认证，身份认证）、完整性(数字签名)、不可否认性(数字签名)、保密性(公钥加密)

身份认证

AAA：1、认证。在做任何动作之前必须要识别动作执行者的真实身份

2、授权。当用户身份被确认合法后，赋予该用户进行文件和数据等的操作权限，包括读、写、执行及从属权

3、审计。每一个人都应该为自己所做的操作负责，所以在做完事情之后都要留下记录，以便核查责任

3种凭证信息：◼ 主体所知道的，如要求输入用户的口令、密钥或记忆的图形图像等

◼ 主体所拥有的，如 智能卡、USB Key等。

◼ 主体自身的特征，如用户的指纹、声音、视网膜等生理特征以及签字、击键等行为特征。

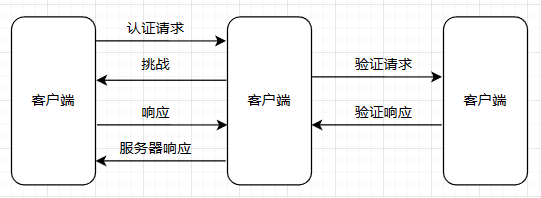
多因子认证：提高认证系统的强度，认证系统可以使用多个因子的认证方式

攻击：文本口令攻击：字典或穷举攻击、社交工程、窥探、垃圾收集、污迹攻击、网络数据流窃听、截取/重放攻击

文本口令防御：基于单向函数的口令存放、加盐Hash散列存储、强口令设置

密码学认证的攻击：中间人、窃听、重放

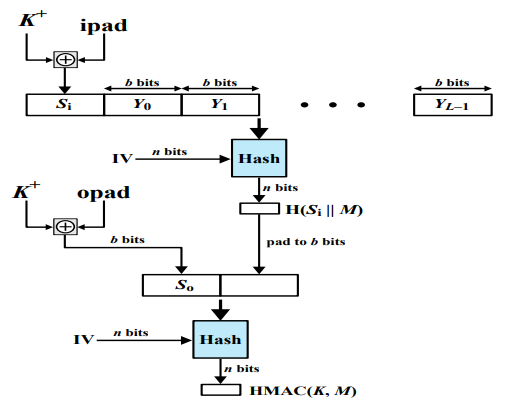
挑战应答模式：



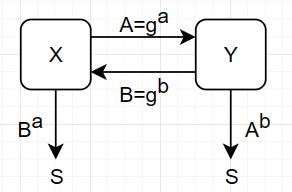
对称密钥的交换：A和B是要通信的用户，KDC是密钥分发中心，Ka和Kb是各自的密钥，Ks是通信用密钥

1. A🡪KDC : A||B||C
2. KDC🡪A : EKa[ Ra||B||Ks||EKb[ Ks||A ] ]
3. A🡪B : EKb[ Ks||A ]
4. B🡪A : EKs[ Rb ]
5. A🡪B : EKs[ Rb-1 ]

HMAC：HMAC(K,M)= H[(K+⊕opad)||H[(K+⊕ ipad )||M]]



Diffie-Hellman算法：p和g是公开的，X发送A给Y，Y发送B给X，然后各自计算出通信密钥S



Kerberos协议：(1)C向AS请求票据许可票据【发送的是C的ID和TGS的ID】

(2)AS发放票据许可票据和会话密钥【发送用C的密钥加密的Kc,tgs和TGS的票据】

(3)C请求服务授予票据【发送TGS的票据和S的ID】

(4)TGS发放服务授予票据和会话密钥【发送用Kc,tgs加密的Kc,s与S的票据】

(5)C请求服务【发送S的票据】

(6)S提供服务器认证信息【发送用Kc,s加密的时间戳】

NTLM：在工作组网络环境中的认证：服务器存储口令的散列值，用户输入口令，散列后对一个挑战进行运算，得到HMAC-MD5值，同时服务器也如此操作，最后比对这两个值是否一致。

访问控制

访问控制三要素：

1）主体（Subject）主体是对客体提出请求访问的主动实体，通常指用户或代表用户执行的程序。

2）客体（Object）客体是接受主体访问的被动实体，是需要保护的资源。主体有时也会成为访问或受控的对象，如一个主体可以向另一个主体授权，一个进程可能控制几个子进程等情况，这时受控的主体或子进程也是一种客体。

3）权限（Right/Permission）权限是主体可对客体执行的动作，也称为对客体的访问模式。

访问控制策略：也称安全策略，是为了满足应用的安全需求制定的主体对客体访问的一系列规则集，它反映信息系统对安全的需求。是对访问如何控制，如何做出访问决定的高层指南。

访问控制机制：访问控制机制是访问控制策略的软硬件底层实现。常见访问控制机制有 访问控制表、能力表、标签、密码学方案、上下文方案

访问控制模型：访问控制模型是对访问控制策略所表达的安全需求的简单、抽象、无歧义的描述，并为开发安全系统提供方案。它为安全策略和它的实现机制之间的关联提供了一种框架。

访问控制基本原则：

（1）最小特权原则 最小特权指的是“在完成某种操作时所赋予主体必不可少的特权”。最小特权原则按照主体所需权限的最小化原则分配主体权限，赋予主体权限不能超过主体执行操作时所需的权限。

（2）职责分离原则 是指遵循不相容职责相分离的原则，实现合理的组织分工。

（3）多人负责原则 即授权分散化，对于关键任务必须在功能上进行划分，由多人来共同承担，保证没有任何个人具有完成任务的全部授权或信息。

控制策略

自主访问控制DAC：自主访问控制DAC也称为基于身份的访问控制，其特点是根据主体的身份及允许访问的权限进行决策。自主是指主体能够自主地将自身具有的访问权限或其子集授予其他主体。

基于列（客体）（多数）访问控制表、基于保护位、基于环的

基于行（主体）能力表

特点：灵活易行、权限的授予是可传递的、信息在移动过程中访问权限关系会被改变



强制访问控制MAC：强制访问控制是一种基于规则的访问控制。它的特点是只有系统才能控制对客体的访问。所谓“强制”是用户不能任意改变实体（主体和客体）安全属性。安全属性和访问控制策略由系统或由安全管理员分配。通过比较主体与客体的安全属性来决定是否允许主体访问客体。

特点：配置粒度大，不灵活，但安全。片面强调保密性或完整性，适用场合较少。

涉及三个模型

基于角色的访问控制RBAC：权限通常由用户在一个组织中担当的角色来确定。权限/许可被授权给角色，角色被授权给用户，用户不直接与许可关联。对访问权限的授权由管理员统一管理。比如说A担任了教师一职就可以发试卷。

基于属性的访问控制ABAC：基于属性的访问控制规则都是通过用户、资源、操作、上下文 环境的属性来表达。

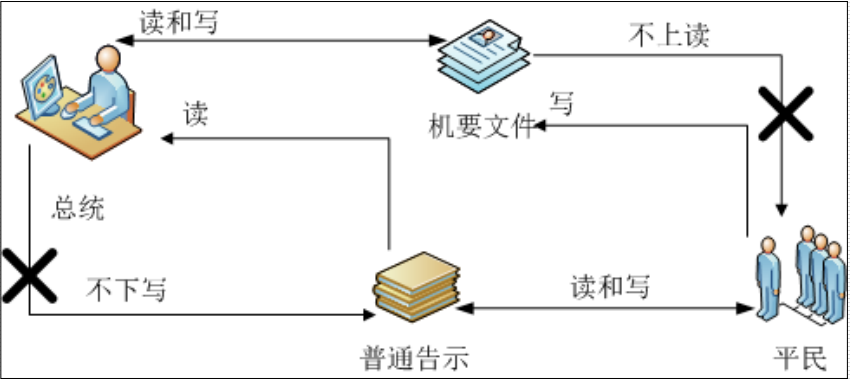
ABAC模型的主要优势是其灵活性和表达能力，最大 的障碍是每次的属性评价对系统性能的影响。

访问控制模型

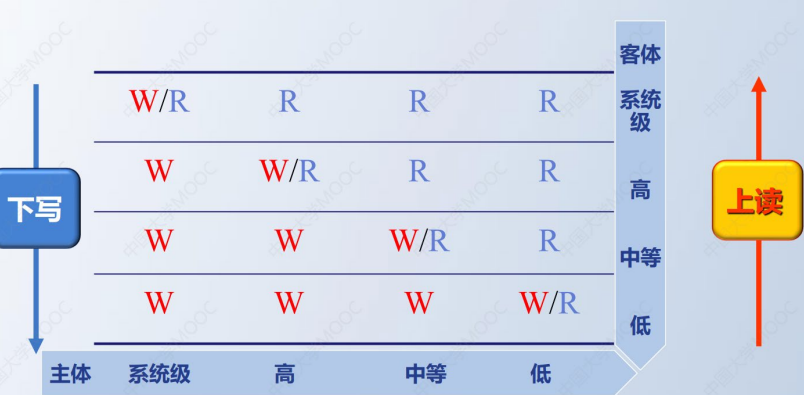
Bell-LaPadula模型（BLP贝拉模型）：不上读，不下写

读：允许信息从被读的客体流向读它的主体

写：允许信息从主体流向被写的客体。



Biba模型：不下读，不上写，信息在系统中只能自上而下进行流动



中国墙模型（BN）：此模型根据主体的访问历史来判断数据是否可以被访问。其本质是将全体数据划分为“利益冲突类”，根据强制约束，主体至多访问每个“利益冲突类”中的一个数据集。

（1）简单安全性 允许一个用户访问与他曾经访问过的公司没有利益冲突的公司信息。即，初始时可自由访问，一旦访问了数据，即进入强制性限制。

（2）清洁信息 清洁信息不存在公司敏感信息，所以，可以不用限制对清洁信息的读访问请求。

（3）\* 特性 非清洁的信息只局限在本公司数据集内部，不能随意流动，清洁后的信息可以在系统中自由的流动。

数据安全

存储加密：加密是防止原始数据被窃取之后导致里面的敏感信息泄露的典型手段。

根据加密的粒度，可分：◼ 整盘数据加密 ◼ 文件、目录、程序加密 ◼ 数据库加密

字段加密：指应用层的结构化数据（数据库、keyvalue等），加密后再直接将字段密文写入数据库。

透明加密：或称静态加密，加密在存储系统内部自动完成，应用层看到的是明文，应用层开发人员不用关注底层加密细节。

透明加密EFS：

加密过程 ◼ 文件被拷贝到临时文本文件

◼ 文件被一个随机产生的Key (FEK： file encryption key)所加密（DESX, 3DES AES）。

◼ 使用用户的公钥对FEK加密，数据解密区域（DDF: data decryption Field ）产生。

◼ 使用恢复代理的公钥对FEK加密，数据恢复区域（DRF data recover field）产生。

◼ 包含加密数据、DDF及所有DRF的加密文件被写入磁盘。

◼ 在第一步中创建的文本文件被删除。

解密过程 ◼ 使用DDF以及用户的私钥（或者恢复代理的私钥）解密 FEK .

◼ 使用FEK解密文件。

数据容错系统：是指建立一个本地或异地的数据系统，该系统是对本地系统关键应用数据的实时复制，当出现灾难时，可迅速接替本地系统以保证业务的连续性。

应用容错系统：比数据容错系统层次更高，即建立一套完整的，与本地数据系统相当的备份应用系统，在灾难出现后，能迅速接管或承担本地应用系统的业务运行。

数据备份：

备份策略：完全备份、增量备份、差异备份、按需备份

完全备份：是对某一个时间点上的所有数据或应用进行的一个完全拷贝。

增量备份：是备份自上一次备份之后有变化的数据。增量备份过程中，只备份有标记的文件/夹，备份后清除标记。这就意味着，第一次增量备份的对象是进行全备后所产生的增加和修改的文件；第二次增量备份的对象是进行第一次增量备份后所产生的增加和修改的文件，如此类推。

差异备份：只备份自上次备份后有变化标记的文件。差异备份过程中，只备份有标记的那些选中的文件和文件夹。它不清除标记（存档属性），也即备份后不标记为已备份文件。在进行恢复时，只需对上次全备份和最后一次差异备份 进行恢复。

NAS：网络附属存储NAS是一种带有服务器和内嵌操作系统的网络文件服务器。NAS设备直接连接到TCP/IP网络上,可提供跨平台文件共享。可将分布独立的数据整合为大型、集中化管理的数据中心，便于对不同主机和应用服务器进行访问的技术。

优点：◼ 独立于应用服务器（即使应用服务器不工作，仍然可以从NAS中读取数据）

缺点：◼ 由于存储数据通过普通数据网络传输，因此易受网络上其它流量的影响。影响系统性能。

云存储：是一个以数据存储和管理为核心的云计算系统服务。

RAID：将多块磁盘通过一定的技术手段组成一个单一的虚拟磁盘 使用。利用数组方式制作磁盘组，配合数据分散排列的设 计，以冗余技术增加可靠性。

RAID 0：又称带区/条带阵列。将数据分割存储到多块硬盘上，磁盘读写时负载平均分配到多块磁盘；由于多块磁盘可同时读写，所以速度明显提升

RAID 1：又称镜像阵列。至少由2块磁盘实现；将同样的数据写入2块硬盘（互为镜像），一块磁盘发生故障时 ，另一块硬盘可继续工作，并可在更换硬盘后重新创建镜像。

RAID 5：由至少3块磁盘实现的磁盘冗余阵列；将数据分布在不同磁盘上，并在所有磁盘上交叉的存取数据及奇偶校验信息（RAID5布局有左结构和右结构之分）

RAID 2：采用海明冗余纠错码、跨接技术和存储纠错数据方法，数据按位分布到磁盘上。磁盘台数由纠错码和数据盘数决定。（很少使用）

RAID 3：结合跨接技术、存储纠错数据方式，采用数据校验和校正。利用单独奇偶校验磁盘进行。一个盘故障，可根据读出数据内容和奇偶校验位确定出错位置，对数据进行修正和重组，校验方式可采用位交错或字节交错。

RAID 4：与RAID3类似，但数据是以扇区交错方式存储于各台磁盘，也称块间插入校验。采用单独奇偶校验盘。

RAID 6：将整个磁盘阵列看成一个二维阵列。RAID5只在一组（相当于行）上有奇偶校验盘，而RAID6在各组的同一位置的盘组成的列上也加上了奇偶校验盘。同时可支持两块盘出错。

隐私保护：是对隐私数据采取一系列的安全手段防止其泄露和被滥用的行为，同时用户还能享受各种服务。旨在实现数据安全和共享的某种平衡。

数据库推理：求和，记录数，平均值，智能填充，线性特性。

阻止用户根据非敏感信息推导出敏感信息：

滤除法：当查询可能涉及敏感信息时，默默拒绝提供查询结果，不给出任何反馈。

隐藏法：当查询可能涉及敏感信息时，隐藏掉部分与查询相关信息，只提供近似查询结果。

匿名技术

◼ 通过限制数据发布的技术，数据集对外发布的隐私保护技术主要包括：

匿名化、假名化（使用假名替换真名）等去标识化手段，将数据集清洗后提供给第三方。让攻击者无法从处理后的数据记录定位到自然人。

◼ 匿名隐私保护技术是在隐去标识属性的基础上，为了更好地保护发布数据中的隐私信息不被泄露，对用户的准标识符进行数据发布限制的技术。

主要的匿名技术：

K-匿名

是指以一个泛化值代替一个具体值的形式，完成匿名处理，本质上是对原始信息的一个泛化处理。

◼ 目的是保证公开数据中包含的个人信息至少有k-1条记录不可区分（k条记录称为一个等价类）。即，公开数据中的任意准标识信息相同的组合都要出现至少K次。

K值越大，保护强度越强。K值越大，丢失的信息更多，可用性越低（一些样本如 果无法凑成一个等价类就不能用） 存在缺陷：◼ 如果一个等价类里多个样本敏感数据一致，隐私就泄露了（一致性攻击）

L-Diversity(L-多样性)

每个k-匿名组至少包含L个不同的敏感属性值，在K-匿名的基础上，要求保证任意一个等价类中的敏感属性至少有L个不同的值。

t-邻近匿名

在相同的准标识类型组中，敏感信息的分布情况与整个数据敏感信息分布情况临近，不超过阈值t

差分隐私：为了防止攻击者利用减法思维实施差分攻击获取到个人隐私，提出了差分隐私保护技术。

差分隐私思路：当对有限数据集D 进行一组查询函数操作 F={f 1， f 2…. f n }(如计数、求和、平均值、中位数或其他范围查询）所得到的查询结果F(D), 算法M对查询结果进行处理，使之满足隐私保护条件，此过程称为隐私保护机制。

隐私保护条件：数据集D中增加或减少一条记录，形成的数据集D’，D和D’称为邻近数据集, 对任意两个邻近数 据集D和D’, 其差分隐私处理后输出结果几乎相同。

安全多方计算：为解决一组互不信任的参与方之间的隐私的协同计算问题， 它能使参与计算方，每一方都只知道自己的输入数据和所有数据计算后的最终结果，安全多方计算涉及的秘密共享、可验证秘密共享、门限密码学、零知识证明等多方面内容。其中应用的密码学算法包括：公钥密码体制、同态公钥加密体制。

TPM是一个微芯片，设计用于提供基本安全性相关功能，主要涉及加密密钥。TPM通常安装在台式计算机或者便携式计 算机的主板上，通过硬件总线与系统其余部分通信。

通信安全

VPN：VPN是利用不安全的公用互联网作为信息传输媒介，通过附加的安全隧道、用户认证等技术实现与专用网络相类似的安全性能，从而实现对重要信息的安全传输。

几种VPN协议比较

1. PPTP提供认证和加密功能，但安全强度低

2. L2TP提供认证和控制报文加密方式，但不对传输中的数据加密

3. IPSec提供了完整的安全解决方案, 但不支持组播，无法穿越NAT

4. TLS/SSL提供认证、加密、完整性验证,多用于web

5. GRE提出较早，是通用路由封装协议，支持全部的路由协议，通过GRE, 用户可利用公共IP网络连接非IP网络，GRE只封装，不提供加密，实际环境中经常与IPSec一起使用。PPTP：PPTP通过PPTP控制连接来创建、维护、终止一条隧道，并使用通用路由封装GRE对PPP帧进行封装。封装前，PPP帧的有效载荷必须经过加密、压缩或是两者的混合处理

L2TP：L2TP用PPP协议对数据进行封装，然后添加附加包头用于数据在互联网络上的传输

L2TP隧道可分为两种类型。强制性隧道：用户完全不知道L2TP连接表现形式；自发性隧道：用户知道L2TP连接表现形式

IPsec的封装模式：

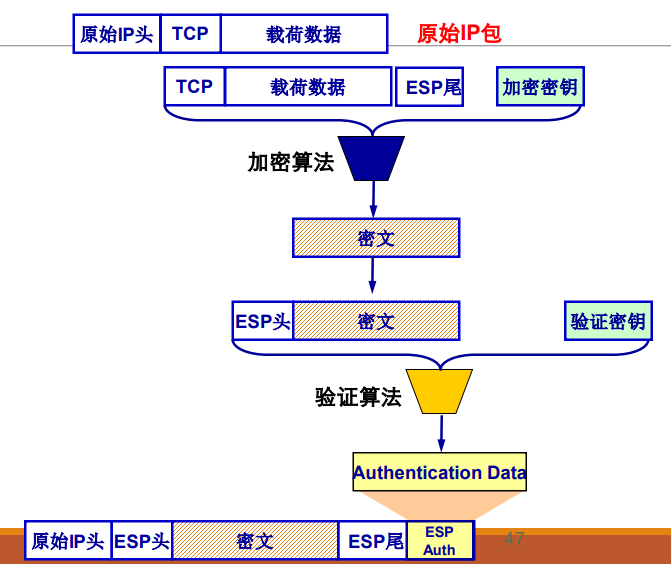
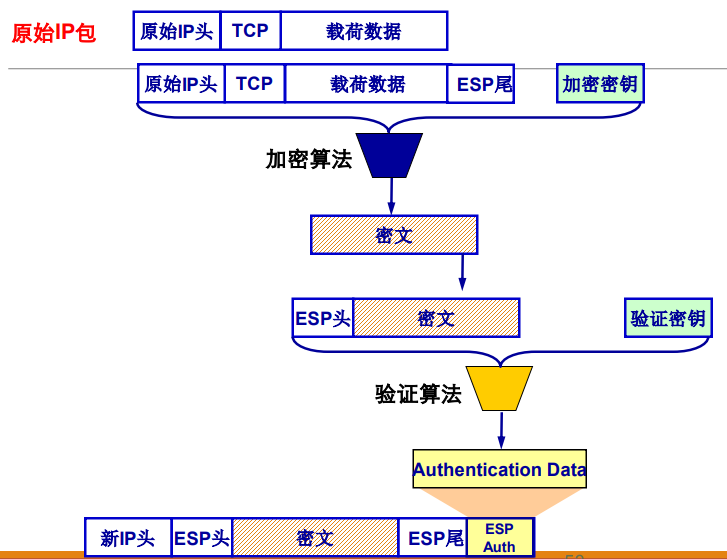
传输模式，IPsec VPN 保护的是IP包的有效载荷，或者说是上层协议。用于端到端的连接，两端的系统必须支持IPSec，而中间节点系统则不必支持，它们只是以普通的方式转发数据包。

隧道模式，只要IPsec双方有一方是安全网关或路由器，就使用隧道模式（典型应用VPN）

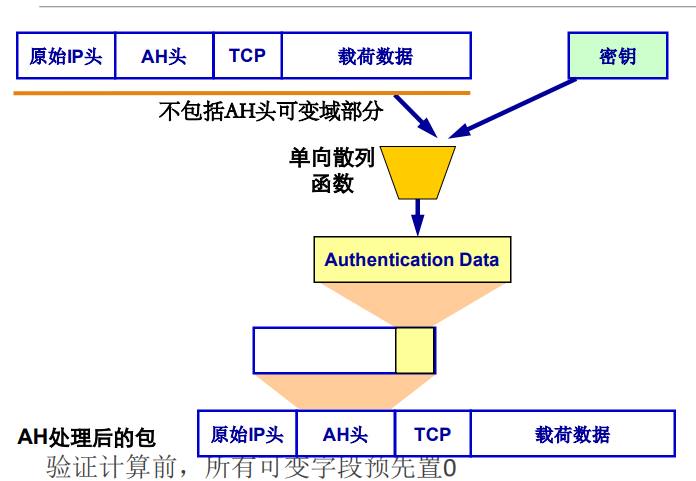
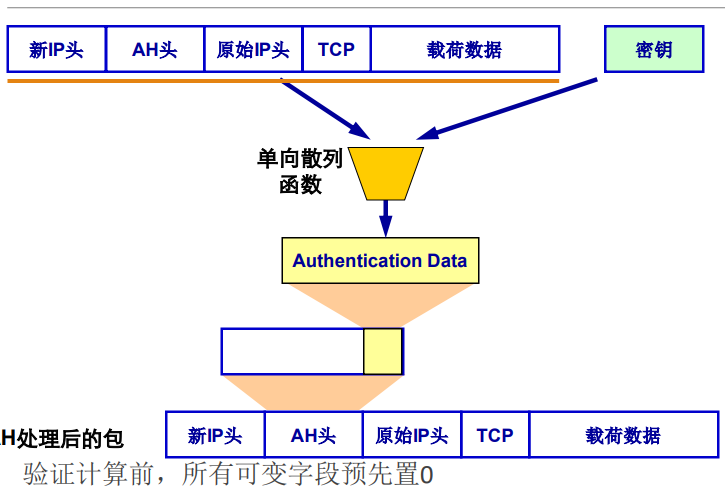
区别：数据包在传输过程中是否需要更改IP报头

IPsec封装协议：

负载安全封装（ESP）：提供对称加密、认证和完整性保护

传输模式：隧道模式：

认证报头协议（AH）：使用HMAC提供数据源认证和完整性保护

传输模式：隧道模式：

IKE（internet密钥交换）：

是通信双方用来协商封装形式、加/解密算法及其密钥、密钥的生命期、认证算法等共享安全参数的协议。主要负责协商协议的参数、交换公共密钥、对双方进行认证、在交换后对密钥进行管理。

安全参数SA：指通信对等方之间为了给需要受保护的数据流提供安全服务时而对某些要素的一种协定，如IPsec协议（AH或 ESP）、协议的操作模式（传输模式或隧道模式）、密码算法、密钥、密钥的生存期等SA被存放在安全关联数据库（SADB）。—个进来的SA可由三个参数惟一地表示为：<安全参数索引，目标IP地址，安全协议标识符>

安全策略数据库SPD：用来存放IPSec的规则，以定义哪些流量需要进行IPSec保护，并搜索与报文分组定义以及相关联的安全策略一致的SA。

IKE协商的两个阶段：

阶段一 在网络上建立一个IKE SA，为阶段二协商提供保护主模式（Main Mode）和激进模式（Aggressive Mode）

阶段二 在阶段一建立的IKE SA的保护下完成IPSec SA的协商快速模式（Quick Mode）

IKE的安全选项：

1. DH分组：Diffie-Hellman获得IKE信息加密的会话密钥

2. 完备前向安全性（PFS）：如果攻击者获得了某个会话密钥，不会对以前的会话产生任何影响

3. 加密协议选择：DES、3DES、AES

4. 认证/完整性协议选择：MD5、SHA-1

分割隧道：流向组织外部网络的任何流量不加密（明文）发送

NAT与IPSec/IKE的不兼容性：

静态NAT不可行，因为远程用户可能一直在改变位置需要多对一NAT。但是多对一NAT不能和IPSec一起工作。现有的解决办法：Cisco通过隧道将IPSec ESP数据包封装在UDP数据包中，允许数据包通过NAT设备

TLS作用：传输层安全协议TLS是一种在两个通信应用程序之间提供安全通道的协议。所有信息都是加密传播，第三方无法窃听。具有校验机制，一旦被篡改，通信双方会立刻发现。配备身份证书，防止身份被冒充。

TLS握手：握手协议是在客户端和服务器端进行安全通信前商定要使用的一些参数，并实现证书验证和密钥生成。其中主要参数为加密算法和密钥、MAC算法、密钥交换的算法等。

IPsec和TLS不同：

协商依赖的协议：IPSec用来保护IP层安全，使用UDP协议进行协商

 SSL用来保护基于TCP协议的应用层安全，使用TCP协议进行协商

保护对象： IPSec可以保护所有的IP报文，对于上层应用完全透明。如果要支持IPSec，应用层协议无需任何改动

 SSL/TLS无需修改操作系统，但是需要适配应用层协议，应用层很多种呀！

 SSL/TLS协议对NAT完全透明，因为它位于TCP协议之上