- 练习**1.2** 在你使用的计算系统中，识别出潜在的、 可能包括安全机制的软件组件 。

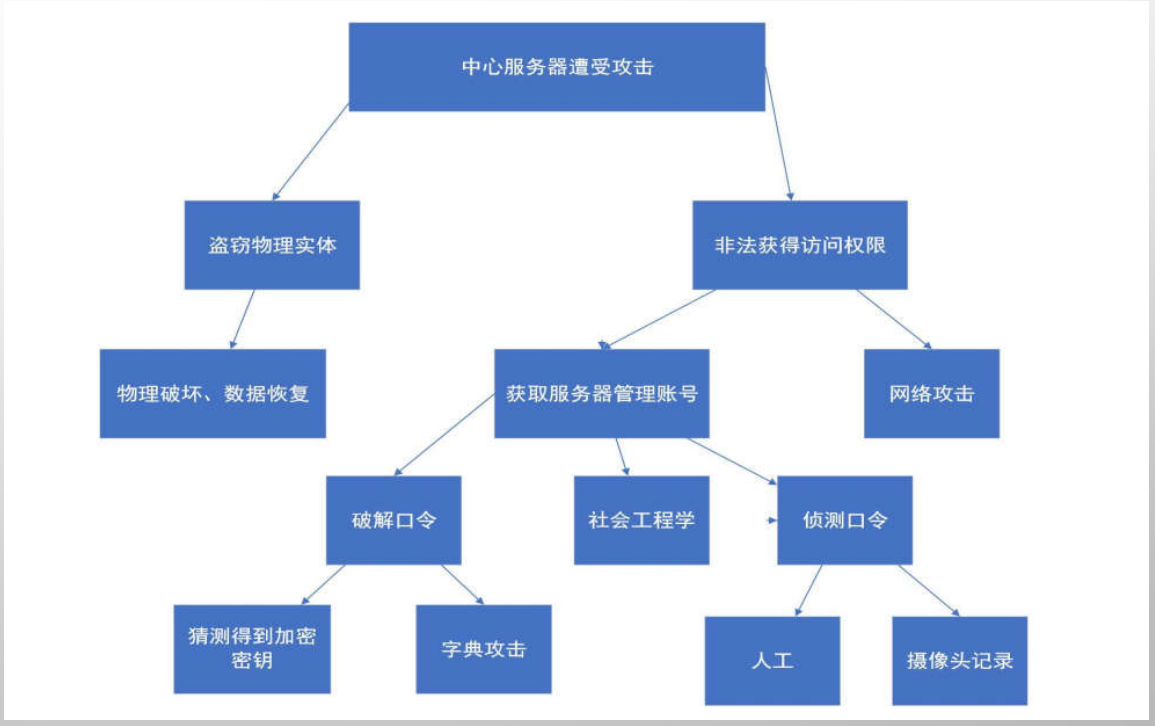
  ✓杀毒软件，可以对系统进行安全扫描，还可以对系统进行实时监控，有很强的安全保护能力。

  ✓浏览器:浏览器内置加密机制，有助于确保数据在传输过程中的私密性和安全性，其云端架构也可以对用户数据提供高效保护。

  ✓**FIREWALL**:及时发现并处理计算机网络运行时可能存在的安全风险、数据传输等问题，

- 练习1.6 考虑某校网安学院的中心服务器失窃的情况。如果发生这种情况，哪些资产可能被破坏？试对此威胁构建一棵攻击树。
- 可能被破坏的资产包括：其他非中心服务器的访问权限与口令；服务器存储的用户私人信息， 如电话号码、身份证号码、家庭住址等；服务器存储的的数据、代码等珍贵资料。

- 树根：一般类的攻击
- 树节点：达成攻击所需的子目标
- AND节点，OR节点
- 边：赋权值，估算攻击的成本、发生的可能性、成功的可能性等



- 练习2.3 写一篇短文讨论数据与信息之间的区别， 并用你自己的例子证明控制对数据的访问并不一定意味着就是控制对信息的访问。
- 数据是客观的，是指从物理世界或网络空间测量、感知、挖掘得到的原始资料，包括数字、文字、符号、图形、图像以及它们能够转换成的数据等形式。数据是信息的符号表示和载体，信息是数据的内涵和解释，也就是说，只有依照形式化规则处理数据之后才能产生信息。信息是经过意识概念化的，有一定的主观性，受人对客观事物变化规律的认识所制约，面对相同的数据，拥有不同知识和经验的人，可以理解出不相同的信息。
- 例子：加密内容

- 练习**2.5** 为维护存放在一个计算机系统中的考试结果，草拟一个安全策略。你的策略至少应考虑学生、讲师、行政人员的进入需求。

  (1) 学生应当被分配读取成绩的权限，以获取自己的考试情况，但不应该获得修改文件的权限；还应该分配提出成绩异议的权限，交予讲师处理。

  (2) 讲师有读取成绩的权限，也有提出修改成绩申请的权限，有权限有限次修改成绩，以防止账号失窃后发生恶意篡改行为。

  (3) 行政人员有读取成绩的权限，在收到讲师提出的成绩修改申请后，可以有修改成绩的权限，但是在未收到成绩修改申请时不能修改成绩，以防止账号失窃后发生恶意篡改行为。

- 练习**2.A** 计算机安全的五个设计原则是什么？

  (1) 在一个给定的应用中，一个计算机系统中的保护机制应该集中在数据、操作还是用户上？

  (2) 一个安全机制应该被放置在计算机系统的哪一个层次上？

  (3) 与富有特色的安全环境相比，你是否偏爱简单性和更高的保证？

  (4) 定义和实施安全的任务是应该交给一个中央实体，还是应该托付给系统中的各个成员？

  (5) 如何防止攻击者访问位于保护机制下面的层？

第二次作业：作业内容 3.3、3.4、3.6、3.a、3.b、4.1

练习3.3 假定口令长度为6个字符，可以使用字母和数字，区分大小写。在以下条件下，蛮力攻击平均所需要的时间分别为多少？

① 检查一个口令需要1/10秒？
26+26+10=62
平均时间为1/2*1/10*62^6=2.84*10^9秒，约90年

② 检查一个口令需要1微秒？
检查单个口令的时间变为原来的十万分之一， 则平均时间变为2.84*10^4秒，约0.328天

练习3.4 假定你只允许使用26个字符来构造长为n的口令。进一步假设你在区分大小写和不区分大小写的两个系统中使用了此相同的口令，试给出猜测出大小写区分的口令所需要的最大尝试次数。

① 先从不区分大小写的系统入手， 最大的尝试的次数为26^n次。再对每个位置大小写上尝试，所需要的最大尝试次数为2^n。所以总的最大尝试次数为2^n+26^n。

练习3.6 口令由用户输入并由计算机检查。因此，在用户和计算机之间一定有通信的通道。到目前为止，我们一直非常抽象地看待这个通道，假设他们存在并且足够安全。什么时候这种假设是合理的？什么时候是不合理的？

① 当用户输入口令并由计算机检查，在之间的通信过程中可能遭遇的攻击有：用户输入口令被攻击者直接观察到，使用摄像头或窃听器间接获取，使用恶意软件获取得到， 通过键盘声音推测口令（一些特殊情况）等（即物理安全和软件安全）

② 所以当用户处于一个规避上述风险的良好的私人环境（外界不可见，没有恶意软件）时，可以认为用户输入口令的信道是安全的。反之，则不合理。

练习3. a用户身份认证可以基于哪些信息？

① 你知道的事情： 口令、个人身份识别号码（PIN）、令牌(tokens)、信用卡电话等你拥有的东西如：物理令牌、智能卡、USB key所以当用户处于一个规避上述风险的良好的私人环境（外界不可见，没有恶意软件）时，可以认为用户输入口令的信道是安全的。反之，则不合理。

② 你是谁： 掌纹、指纹、虹膜图案或视网膜图案、人脸等生物识别技术

③ 你做什么： 手写签名，银行支票，信用记录，法律执法，手势密码等

④ 你在哪里： IP认证， GPS定位认证

练习3. b描述口令认证机制面临的三种威胁

① 用户长期使用同样的口令，没有妥善保管自己的口令，使用弱口令，使用长度较短的口令，在不同的地方使用同样的口令，使得攻击者可以通过穷举或者猜测攻击猜出口令

② 欺骗攻击与重放攻击。攻击者可以伪造一个页面骗取用户输入自己的密码口令，或者监听用户与服务器之间的通信信道来获取通信内容，并重放通信内容以达到冒充用户的目的。

③ 未加密的口令文件内容泄漏或者是文件内容的修改可能导致口令认证机制遭到威胁，攻击者通过窃取未加密的口令文件或进行篡改，可以方便的对许多用户开展攻击。

练习4.1给定两个比特位来控制一个目录上的访问操作，怎样才能使拥有4种操作？怎样控制文件的创建与删除？怎样用这些操作来实现文件的隐藏？

① 两个比特位有4中0， 1组合，所以可以对4种操作的每一种都用一种组合来编码。比如用00来编码读，01来编码写， 10来编码附加， 11来编码执行。

② 控制文件创建和删除的方法：可以预先写一个创建文件和删除文件的程序，所有人禁止读、写和附加，只有获取了指定的权限才可以执行该程序创建或删除文件。

③ 实现文件隐藏的方法：对于需要隐藏的文件，将不被允许看到文件的人的权限设置为禁止读、写、附加和执行，只有部分人被设置为允许读文件，这样就实现了文件的隐藏。。

- 练习**4.5** 讨论：组和角色的不同点是什么，它们是否有本质的区别?

  从定义上来看，具有相同访问权限的用户集合形成组，然后再给授予访问对象的许可。而一组特定应用的操作（过程）称为角色，主体从它们履行的角色上获取访问权限。这两种本质上没有区别，都是结构化中间控制的实现方法，都有利于用一种简单的管理方式来实现访问控制。

- 练习**4.8** 给定一个用间隔的格作为安全标签的策略。 当且仅当主体的安全标签是对象安全标签的子集时才能授权访问。 假设有ADMIN、LECTURERS、 STUDENTS这几个类，标签为{STUDENT}的主体能访问以上哪几个对象？为什么标签为{ADMIN,STUDENTS}的主体比标签为{STUDENTS}有更多的限制？解释在这个策略中标签中∅ 和{ADMIN,LECTURERS, STUDENTS}的角色的意思。

  (1). 标签为**{STUDENT}**的主体可以访问的对象有**{STUDENT}, {STUDENT, LECTURERS},{STUDENT, LECTURERS, ADMIN}, {STUDENT, ADMIN}**。

  (2). 由于当且仅当主体的安全标签是对象安全标签的子集时才能授权访问，所以与标签为**{ADMIN, STUDENTS}**的主体相比，标签为**{STUDENTS}**的主体可以额外访问**{STUDENT}, {STUDENT, LECTURERS}**。也就是标签为**{ADMIN,STUDENTS}**的主体有更多的限制。

  (3). 标签为∅的主体可以访问任意标签的客体；标签为**{ADMIN, LECTURERS,STUDENTS}**的主体只能访问标签为**{ADMIN, LECTURERS, STUDENTS}**的客体。

- 练习**4.9** 给定一组种类，实现基于格的需要停止(NEED-TOWITHHOLD)策略，该策略可以有选择地从主体收回访问权限。

令**H**为一个密级集合，具有分等级（线性）的排序$\leq_H$；

令**C**是一个种类集合，如工程名字、公司部门、学院的系等，一个间隔就是一个种类集；

令**D**是一个用户集合，用来完成收回访问权限操作，简单理解为禁止访问名单。

安全标签是一个三元组（**h, c, D**），其中$h \in H$是一个安全级别，而$c \subseteq C$是一个间隔，**D**是用户的集合。安全标签的偏序$\leq_H$定义为：
$(h_1, c_1, D_1) \leq (h_2, c_2, D_2)$ 当且仅当$h_1 \leq_H h_2$, $c_1 \subseteq c_2$, $D_2 \notin D_1$。

如主体$user1$的安全标签为**{private, {personnel}, {user1}}**，那么他可以访问安全标签为**{private, {personnel}, $\emptyset$ }, {private, {personnel}, {user2, user3}}**的客体，不可以访问标签为**{private, {personnel}, {user1, user3}}**的客体。管理员对客体的安全标签项D中加入某主体即可收回该主体对此客体的访问权限。

- 练习**1.** 用ABC模型描述RBAC0模型。
  先来看用ABC模型描述RBAC1

- RBAC1引入了角色的等级和角色间的继承关系
- 角色间的继承关系可分为一般继承关系和受限继承关系
  - 一般继承关系仅要求角色继承关系是一个绝对偏序关系，允许角色间的多继承
  - 受限继承关系则进一步要求角色继承关系是一个树结构，要求角色间单继承

- (1) P = {(o，r)}，P表示授权集合，(o，r)为客体-权限对
- (2) ROLE表示角色层次的偏序关系
- (3) actRole表示激活角色，实现“用户-角色”分配
- (4) pRole表示授权角色，实现“角色-权限”分配
- (5) ATT(S) = {actRole}；
- (6) ATT(O) = {pRole}
- (7) allowed(s，o，r) = role ∈ actRole(s) ∧ role' ∈ pRole(o，r) ∧ role≥role'，即如果存在授权角色(pRole(o，r))，其偏序关系≤激活角色(actRole(s))，则访问请求被允许

答：①P = {(o，r)}，P 表示授权集合，(o，r)为客体-权限对
②ROLE 表示角色
③actRole 表示激活角色，实现“用户-角色”分配
④pRole 表示授权角色，实现“角色-权限”分配
⑤ATT(S) = {actRole}
⑥ATT(O) = {pRole}
⑦allowed(s，o，r)= role ∈actRole(s) ∧ role ∈ pRole(o，r) 即一个用户被分配了一个角色且该角色拥有该权限，则访问请求被允许

- 练习**2** 针对你日常生活/学习中的一个访问/使用控制例子，试用ABC模型形式化地描述它。

¤ (1) P = {(o，r)}，P表示授权集合，(o，r)为客体-权限对
¤ (2) ROLE表示角色层次的偏序关系
¤ (3) actRole表示激活角色，实现“用户-角色”分配
¤ (4) pRole表示授权角色，实现“角色-权限”分配
¤ (5) ATT(S) = {actRole}；
¤ (6) ATT(O) = {pRole}
¤ (7) allowed(s，o，r) = role ∈ actRole(s) ∧ role' ∈ pRole(o，r) ∧ role≥role'，即如果存在授权角色(pRole(o，r))，其偏序关系≤激活角色(actRole(s))，则访问请求被允许

答：①P = {(o，r)}，P 表示授权集合，(o，r)为客体-权限对
②ROLE 表示角色
③actRole 表示激活角色，实现“用户-角色”分配
④pRole 表示授权角色，实现“角色-权限”分配
⑤ATT(S) = {actRole}
⑥ATT(O) = {pRole}
⑦allowed(s，o，r)= role ∈actRole(s) ∧ role ∈ pRole(o，r) 即一个用户被分配了一个角色且该角色拥有该权限，则访问请求被允许

- 具体化即可。例如：戴口罩、售票系统、教务系统等。

- 练习5.2没有安全内核是否安全？讨论有一个可信计算基的安全内核（如TCB）的优点和缺点。

  • 安全内核是实现引用监控器的可信计算基的硬件、固件和软件的总和，处理所有的访问控制，安全内核是实现引用监控器概念的一种技术，并不一定非要采用设置安全内核的方式来保证安全。

  • A. 优点方面，TCB中的操作系统安全内核包括验证机制的实现、对系统自身的访问控制，以及组成管理用户和程序的安全属性组件，代表着底层的安全机制，因而能提供更多等级的安全保护（相比于应用软件实现的安全保护机制）。

  B. 对应地，TCB中的操作系统安全内核也有其本身的缺点，作为底层的安全机制，TCB中的操作系统安全内核实现的复杂程度高，也因此有更多自身实现上的隐患（安全内核代码**BUG**），所以需要经常进行补丁更新；另外，由于操作系统安全内核使用的广泛性，一旦发生问题可能导致受到安全威胁的用户会更多。

- 练习5.5 一些缓冲区溢出攻击会把他们希望执行的代码放入调用栈中。通过区分程序和数据来帮助构建抵御这种特殊类型的缓冲溢出攻击的能力将如何实现？

  这些缓冲区溢出攻击的实现基于恶意代码作为函数的一部分存储在内存中，在发生缓冲区溢出时，恶意代码就可以被执行。为了抵御这种类型的攻击，我们要求系统底层有能力区分程序和数据，也就是当进行数据处理时拒绝函数执行。具体地，安全机制设计两种状态：数据处理模式和程序执行模式，在数据处理模式下，不允许代码执行，这样就可以防止缓冲区溢出时系统执行放在调用栈堆上的代码。

- 练习5.6反病毒软件扫描文件来对抗攻击。一个病毒如何截取对内存的读请求以及隐藏它的存在？

① 病毒将自己文件的访问权限设置高于反病毒软件的访问权限，反病毒软件将无法对病毒文件进行扫描。

② 病毒可以将自己嵌入一个已存在的合法的可执行文件中，当合法文件执行时，病毒也同时执行，这样不会被扫描文件的反病毒方式发现。

③ 一个病毒可以通过修改内存控制块来截取读请求并隐藏其存在。

- 练习1计算机正常工作的温度和湿度范围分别是多少？
  计算机正常工作的温度在10～35度，相对湿度为30％～80％
- 练习2计算机机房建设时，需要考虑的安全项目有哪些？
  场地选择、结构防火、机房内部装修、活动地板、供配电系统、空调系统、其它设备和辅助材料、火灾报警及消防设施、防水安全计算机房、防静电计算机房、防雷击、防鼠害、电磁波的防护等。

第五次作业：6.a、6.b、6.3、练习1、7.2、7.3

练习6.b 进程的真实UID和有效UID有什么区别？

真实 UID 和真实 GID：标识用户的身份，也就是登录用户的 UID 和 GID，可以用 id 命令查看。

有效 UID 和有效 GID：进程用来决定我们对资源的访问权限。一般情况下，有效 UID 等于实际 UID，有效 GID 等于实际 GID。当设置-用户-ID（SUID）位设置，则有效 UID 等于文件的所有者的 UID，而不是实际 UID；同样，如果设置了设置-用户组-ID（SGID）位，则有效 GID 等于文件所有者的 GID，而不是实际 GID。

文件	uid	gid	set uid 标志位	set gid 标志位	mode的 Bit 8-0
Program1	10	12	1	0	4551
File1	10	12	0	0	0600

练习6.a 在一个Unix系统中，几个文件的inode 信息摘要如下：
令用户Alice的uid=30和gid=22，问其能否运行程序Program1？如果能运行，运行进程的真实 uid、真实gid、有效uid和有效gid分别是什么？进程运行时是否可以读文件File1，为什么？

① 运行时，用户（进程）的真实 UID 为 30，真实 GID 为 22。而 program1 的SUID 为 1，说明会对用户进行置位。所以用户的有效 UID 会被改变为 10，有效 GID 仍然为 22。由于用户的有效 UID 已经变成了 10 和文件的属主 UID 相同。

② 权限为 6 表示属主拥有读和写的权限， 所以可以读文件 1。

作为选择，我们多数用三位八进制数字的形式来表示权限，第一位指定属主的权限，第二位指定组权限，第三位指定其他用户的权限，每位通过4(读)、2(写)、1(执行)三种数值的和来确定权限。

还可设置第四位，它位于三位权限序列的前面，第四位数字取值是4，2，1，代表意思如下：

4，执行时设置用户ID，用于授权给基于文件属主的进程，而不是给创建此进程的用户。
2，执行时设置用户组ID，用于授权给基于文件所在组的进程，而不是基于创建此进程的用户。
1，设置粘着位。

练习6.3 哪条Unix命令可以列出你的目录下其他人可写的文件？

① 使用文件查找命令find

② /表示当前目录； 其他人可写权限应该为002。

③ find / -perm 002 （显示方便还可以加其他参数）

find -perm，根据文件的权限来查找文件。在linux中文件或目录有三者权限r,w,x，代表的含义分别是读、写、可执行。而一个文件或目录的属性中又包括所属用户u、所属组g、其他o三个部分的属性，分别表示所属用户、所属组、其他用户对这个文件所拥有的权限。用户在其拥有权限的位上设置1，没有权限的位设置0。

-perm mode　　文件的权限正好是mode就匹配
-perm -mode　　文件的权限包括mode就匹配（该文件还可以拥有额外的权限属性）
-perm +mode　　文件的权限部分满足mode就匹配（已弃用，find新版使用-perm /mode）

练习1 Android系统的安全机制主要有哪些？

① 进程沙箱隔离机制

② 用户ID机制

③ 权限机制

④ 签名机制

⑤ SEAndroid机制

练习7.2在Unix和Windows中，访问权限是为用户和组定义的。为了便于更好的安全管理，用户被放到不同的组中。当用户拥有的权限少于用户所在组的权限时，两个操作系统会如何决定访问权限呢？如何拒绝给予用户那些已经给予用户所在组的访问权限？

① 当用户拥有的权限少于用户所在组的权限时：

a）UNIX中，属主按照属主权限算， 若不是属主，但属于所在组，按照组权限算。

b）Windows， 决策将根据访问掩码、主体的令牌、对象的ACL来决定。大体来说，如果存在DACL，那么系统将检查访问对象的属主，如果属主是用户且访问掩码包括Read_Control和Write_DAC请求，则允许。

练习7.2在Unix和Windows中，访问权限是为用户和组定义的。为了便于更好的安全管理，用户被放到不同的组中。当用户拥有的权限少于用户所在组的权限时，两个操作系统会如何决定访问权限呢？如何拒绝给予用户那些已经给予用户所在组的访问权限？

② 拒绝给予用户那些已经给予用户所在组的权限：

a）Unix中通过更改属主、属主所在组和其他组对文件的权限， 即可拒绝。。

b）Windows中，在对象的DACL中添加一个Access-denied ACE，该ACE的SID和用户线程令牌SID匹配，即直接对用户申明放弃/拒绝某一权限， 从而实现限制组中用户权限的目的。。

DACL自由访问控制列表：对对象持有者控制访问对象，并标明特定的用户，特定的组是否能持有对象。简单一句话就是说，定义哪个用户，或哪个用户所属的组访问该对象的权限。

ACL访问控制列表：DACL和SACL构成了整个存取控制列表Access Control List

ACE访问控制项：ACL中的每一项，我们叫做ACE（Access Control Entry）

访问掩码的功能是以压缩形式描述访问权限。 为简化访问管理，访问掩码包含一组四位（ 一般权限），这些权限通过使用函数RtlMapGenericMask转换为一组更详细的权限。

练习7.3讨论“ 中间层控制” 是如何在Windows中使用的?

① 使用域来实现一次签到以及集中式的安全管理。域是共享公用用户账户数据库和安全策略的计算机集合，可以构成层次结构。域管理员在域控制器上创建并管理域用户和组。

② 对象被组织在活动目录中。活动目录使用了一种结构化的数据存储方式，并以此作为基础对目录信息进行合乎逻辑的分层组织。

③ 每一种对象类型都有一个特定的属性以及一个唯一的GUID（globally unique identifier），每一种属性都有自己的GUID。对象类型的属性可以被组织到属性集中；一个属性集合通过GUID来识别。

练习7.3讨论“ 中间层控制” 是如何在Windows中使用的?

④ 使用别名来实现逻辑角色：应用程序开发者指派一个别名student，在部署时，适当的SID会分配给这个别名。

⑤ 使用访问许可来描述可以施加于对象的操作，可以为每一类对象制定特定的访问权限，每一类对象都具有从通用访问权限到真实访问权限的映射。

第六次作业：练习1、练习2、练习8.1、练习8.5、练习9.8、练习9.a

练习1 Windows系统中，LSA、SAM指什么？DEP、ASLR又是指什么技术？

- LSA指Local Security Authority，也就是本地安全权威，作用是在用户登陆时，检查用户账户并创建访问令牌(access token)， LSA还负责审计工作。
- SAM指Security Account Manager，也就是安全账户管理员，作用是维护用户数据库，在本地用户认证期间， LSA将使用该数据库。
- DEP指Data Execution Prevention ，也就是数据执行保护，是一套软硬件技术，能够在内存上执行额外检查以帮助防止在系统上运行恶意代码。
- ASLR指Address Space Layout Randomization，也就是地址空间配置随机加载，是一种防范内存损坏漏洞被利用的技术，目的是为了防止栈溢出，保护用户程序的安全。

练习2 Windows系统中，DACL和SACL有什么区别？

- DACL（Discretionary Access Control List），其指出了允许和拒绝某用户或用户组的存取控制列表。 当一个进程需要访问安全对象，系统就会检查DACL来决定进程的访问权。如果一个对象没有DACL，那么就是说这个对象是任何人都可以拥有完全的访问权限。其中ACE的类型是肯定(允许)或否定（拒绝） 。 DACL中的ACE格式包括： 类型：肯定(允许)或否定(拒绝) 标志；Object Type； Inherited Object Type；访问权限；主角SID： ACE应用的主角。
- SACL（System Access Control List），其指出了在该对象上的一组存取方式（如，读、写、运行等）的存取控制权限细节的列表。审计规则在SACL中定义， SACL中的ACE格式包括： Type：肯定的（审计允许的许可）或否定的(审计拒绝的许可)； Trustee：一个 SID（个人，组，别名）； Mask：许可(32-bit 掩码)。一个ACE可以同时是肯定的和否定的 。

练习8.1 用基本访问模式术语alter(修改)和observe(查看)描述*-property

- 如果对于每一个元素，均有$(s,o,a)\in b$，访问操作a是添加或写，主体s的当前级别受客体o的当前级别控制，即$f_C(s) \le f_O(o)$，那么状态(b, m, f)满足*-property
- 此外，如果存在一个元素，有$(s,o,a)\in b$，访问操作a是添加或写，那么对于所有的客体o'，$(s,o',a')\in b$，a'是读或写，必须有$f_O(o') \le f_O(o)$

- 如果主体可以对客体进行alter，那么主体s的当前级别受客体o的当前级别控制，也就是$f_C(s) \le f_O(o)$。

- 如果主体可以alter客体o，可以observe客体o'，那么$f_O(o') \le f_O(o)$。

练习8.5 改写针对Multics操作系统的ss-property

- 如果对于每一个元素都有$(s, o, a) \in b$，访问操作a是读或写，主体s的安全级别控制客体o的安全级别，即$f_s(s) \geq f_o(o)$，那么状态(b, m, f)满足ss-property

- Multics的主体就是进程。每个主体都有一个描述符段（descriptor segment）。对每一个客体，在每个主体的描述符段中都有一个段描述符字（segment descriptor word， SDW）。
- 对于一个活动进程的描述符段中的任何段描述符SDW，如果读或者写指示器处于开启状态，则进程的当前级别支配段级别。

练习9.a 描述BLP模型、 Biba模型、 Chinese Wall模型和Clark-Wilson模型的区别及主要应用场景。

- BLP模型： BLP模型描述的是多级安全（MLS）策略： 描述访问控制的保密性问题的状态机模型； 访问许可通过访问控制矩阵和安全级别来定义；安全策略防止信息从高安全级别流向低安全级别。模型是基于系统元素密级的，密级用安全级别（security level）来表示。BLP只考虑主体在查看或改变一个客体时发生的信息流动。主要应用场景是军事安全模型
- Biba模型：类似于BLP的状态模型，与BLP模型相比增加了完整性策略，使用一个完整性级别格的元素标注主体和对象的完整性策略，赋予主体和对象的完整性级别由函数 和给定。可以规定完整性级别不变的策略来阻止干净的主体和对象被脏的信息污染，在完整性的格中， 信息只能向下流动。
- Chinese Wall模型： 模拟了咨询公司的访问规则，主要的应用场景是商业和咨询业。与访问权限通常假设为静态的BLP模型相比， Chinese Wall模型在每次状态迁移中访问权限都要重新赋值。

练习9.a 描述BLP模型、 Biba模型、 Chinese Wall模型和Clark-Wilson模型的区别及主要应用场景。

- Clark-Wilson模型：主要研究了商务应用的安全性需求，这些需求主要是关于数据完整性的，即防止未授权的数据修改、欺骗和错误。与BLP模型不同的是， Clark-Wilson模型用程序作为主体和对象之间的中间控制层，主体被授权执行某些程序，数据项可通过特定的程序访问，定义可以访问某个特定类型数据的程序集是软件工程的一种常见机制，这种机制可以被卓有成效地运用到构造安全的系统中。

练习9.8在一个控制对病历和处方访问的医疗信息系统中： 医生可以读写病历和处方。护士只能读写处方，但是不应当知道病历的内容。 你如何在格模型中得到这个策略，阻止信息从病历流到处方？依你看，哪一种安全模型最适合这种策略？为什么？

- 将医生作为可信主体，最高安全等级为{High,{病历,处方}}，当前安全等级为{Low,{病历,处方}}，护士的安全等级为{Low,{处方}}，病历的安全等级为{High,{病历}}，处方的安全等级为{Low,{处方}}这样设置可以实现护士对处方的读写，对病历的不可见;医生当前安全等级可以对处方进行读写，最高安全等级可以对病历进行读写。

- 这样设置可以实现护士对处方的读写，对病历的不可见;医生当前安全等级可以对处方进行读写，最高安全等级可以对病历进行读写。

- BLP只考虑主体在查看或改变一个客体时发生的信息流动，安全策略防止信息从高安全级别流向低安全级别。（其他模型当然也可以实现，只要能够满足题意就好）

- 练习9.6令X为一个4比特变量，可在0到15之间等概率地取值。给定条件“IF X>7 THEN Y:=1;”和初值“Y=0”，计算条件熵HY(X)。

- p（y=1）= p(y=0)=1/2
- 0<=i<=7 ,P(X=i|y=0)=1/8, P(X=i|y=1)=0
- 8<=i<=15 ,P(X=i|y=0)=0,P(X=i|y=1)=1/8

$$H_y(x) = H(X|Y) = \sum_y p(y)\,\mathrm{H}(\mathrm{X}|\mathrm{y})$$

- Hy(x)=-1/2*（1/8*log2（1/8）*8）*2=3bits

- 练习1 隐存储信道的必要条件是什么？隐定时信道的必要条件是什么？两者有什么区别？
  - 隐存储信道：资源共享。发送进程和接收进程必须能够对某一共享资源的同一个属性进行访问。发送信息。发送方必须能够改变共享资源的属性。接受消息。接收方必须能够探测访问到资源的属性。同步或者协同。必须存在一种机制来初始化发送进程和接收进程，并且对它们使用共享资源的次序进行同步或排序，以便告知接收者接收。
  - 隐定时信道：资源共享。发送进程和接收进程必须能够对某一共享资源的同一个属性进行访问。基准时间。发送进程和接收进程都必须按照同一个时间基准，比如实时时钟或者时间的顺序。接收者必须能够控制对发送者的属性变化进行检测的时机。同步或者协同。必须存在一种机制来初始化发送进程和接收进程，并且对它们使用共享资源的次序进行同步或排序。
  - 区别：隐存储信道是空间的共享，而隐定时信道是时间的共享，其中的存储单元只能在短时间内保留前一个进程发送的消息。不需要始终或者定时器的隐信道是隐存储信道，反之是隐定时信道。

- 练习**10.A** 简单描述TCSEC、 ITSEC、 CC的含义和安全级别的划分情况， 三者的安全级别有何区别和联系？

  TCSEC, 指TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, 也就是可信任计算机系统评估标准, 将计算机安全从高到低分为： A、 B、 C、 D四类七个级别, 共27条评估准则.

  ITSEC, 指INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA, 也就是信息技术安全评估标准, 吸取了TCSEC的经验教训；致力于提供一个安全评估的框架， 以便新的安全需要提出.评估准则分为7级: E0到E6七个评估级别表示了安全功能执行的正确性的保证级别.

  CC, 指COMMON CRITERIA, 也就是通用准则, 融合了各种以前的标准的思想, 放弃了ITSEC采用的对功能类和保证等级的严格分离, 在使用保护配置文件和预定义安全级别上追随了联邦标准. 有七个递增定义的EAL, 也就是七个安全等级.

  • ITSEC吸取了TCSEC的经验教训, 与TCSEC相比, 打破了功能性和保证性之间的联系; CC则是国际标准化组织统一现有多种准则的努力结果, 放弃了ITSEC采用的对功能类和保证等级的严格分离, 主要思想和框架取自ITSEC和FC, 仍然在不断发展和更新. 三者都有七个安全等级, 是不断吸取经验教训进行改善和标准化的结果。

- 练习**10.B** 根据TCSEC标准， WINDOWS 10 和LINUX 5.X的安全级别分别如何？ 试简述理由。

一、操作系统的安全级别有(TCSEC标准):

1、D级，最低安全性；

2、C1级，主存取控制；

3、C2级，较完善的自主存取控制（DAC)、审计；

4、B1级，强制存取控制（MAC）；

5、B2级，良好的结构化设计、形式化安全模型；

6、B3级，全面的访问控制、可信恢复；

7、A1级，形式化认证。

- C2级计算机系统比C1级具有更细粒度的自主访问控制
- C2级通过注册过程控制、审计安全相关事件以及资源隔离，使单个用户为其行为负责
- C2被认为对商业应用是最合理的安全级别；大多数厂商都提供经C2评估过的操作系统或数据库管理系统的版本

- B1级系统要求具有C2级系统的所有特性
- 在此基础上，还应提供安全策略模型的非形式化描述、数据标记以及命名主体和客体的强制访问控制
- 并消除测试中发现的所有缺陷

Windows 10是C2安全等级, Linux 5.x是C2安全等级 （linux系统安全级别一般不会低于Windows系统）

- **CHAP10B-练习1** 等级保护制度的主要内容有哪些?

  1. 对国家秘密信息、法人和其他组织及公民的专有信息、 公开信息分类分等级进行管理和保护;
  2. 对信息系统按业务安全应用域和区实行分等级保护;
  3. 对系统中使用的信息安全产品实行按分等级许可管理;
  4. 对等级系统的安全服务资质分等级许可管理;
  5. 对信息系统中发生的信息安全事件分等级响应、处置 。

- **CHAP10B-练习2** GB/T 22239-2019《网络安全等级保护基本要求》 中的十大安全类又有哪些?

GB/T 22239-2019《网络安全等级保护基本要求》的十大安全类

(1). 技术要求

安全物理环境

安全通信网络

安全区域边界

安全计算环境

安全管理中心

(2). 管理要求

安全管理制度

安全管理机构

安全人员管理

安全建设管理

安全运维管理

- **CHAP10B-练习3** 业务信息安全和系统服务安全有什么区别?

  业务信息安全和系统服务安全是定级对象的安全保护等级时的两个不同的方面,保护侧重点不同. 保护数据在存储, 传输, 处理过程中不被泄漏, 破坏和免受未授权的修改的信息安全类要求(简记为S, SECURITY)是业务信息安全; 保护系统连续正常运行, 免受对系统的未授权修改, 破坏而导致系统不可用的服务保证类要求(简记为A , AVAILABLE)是系统服务安全.

  “业务信息”与“系统服务”相对应, 分别从静态和动态两个方面体现信息系统的重要作用 。

第八次作业：练习1、练习2、练习3、练习4、练习1、练习2

练习1假设有一个accounts数据库，他的记录是(customer_name, account_number, balance, credit_rating)以及以下一些用户类型：customer, clerk, manager。试定义一个访问结构，比如通过视图，来实现如下一些功能：

- customer可以读取他们自己的account信息
- clerk可以读取除了credit_rating以外所有的字段信息，也可以更新所有用户的
- balancemanager可以创建新的记录，读取所有的字段信息以及为所有用户更新他们的credit_rating

1、customer可以读取他们自己的account信息

- CREATE VIEW Customer_View AS SELECT * FROM Accounts where customer_name = current_user();
- GRANT SELECT ON Customer_View TO GROUP Customer;

2、clerk可以读取除了credit_rating以外所有的字段信息， 也可以更新所有用户的balance。

- CREATE VIEW Clerk_View AS SELECT customer_name, account_number, balance FROM Accounts;
- GRANT SELECT, UPDATE(balance) ON Clerk_View TO GROUP Clerk;

3、manager可以创建新的记录，读取所有的字段信息以及为所有用户更新他们的credit_rating。

- CREATE VIEW Manager_View AS SELECT * FROM Accounts;
- GRANT SELECT, INSERT, UPDATE(credit_rating) ON Manager_View TO GROUP Manager;

练习2 所有的在Students关系(见下页的表格)上的统计性查询在其查询结果中都至少要包含三个元组。只有在属性Grade Ave上的AVG查询才是允许的。试找出一个新的通用的追踪者，并且构建一个对Homer的平均分数的跟踪攻击

Name	Sex	Program	Units	Grade Ave.
Alma	F	MBA	8	63
Bill	M	CS	15	58
Carol	F	CS	16	70
Don	M	MIS	22	75
Errol	M	CS	8	66
Flora	F	MIS	16	81
Gala	F	MBA	23	68
Homer	M	CS	7	50
Igor	M	MIS	21	70

Q1: SELECT COUNT(*) FROM Students WHERE Program = ‘CS’

Q2: SELECT COUNT(*) FROM Students WHERE Program = ‘CS’ AND NOT Name =‘Homer’

Q3: SELECT AVG(Grade) FROM Students WHERE Program = ‘CS’

Q4: SELECT AVG(Grade) FROM Students WHERE Program = ‘CS’ AND NOT Name= ‘Homer’

由上述查询可以得到Q1=4、Q2=3、Q3=61、Q4=64.67
因此可得Homer的成绩为4*61-3*64.67=50
从Sex的角度也可以计算得到

练习3 增量备份和差分备份有什么区别？

- 增量备份：每次备份的数据只是相当于上一次备份后增加的和修改过的数据。

- 差分备份：每次备份的数据是相对于上一次全备份之后新增加的和修改过的数据。

练习4 RAID 5工作原理是什么？最少需要几块硬盘？

- 通过存储数据的奇偶校验值，借助其他完整的数据恢复缺失的数据。至少需要三块硬盘。

练习1 将当前浏览器的安全设置文档化，你的系统上的安全相关信息存放在什么地方？

- C:\Users\Username\AppData\Local\Google\Chrome\UserData

练习2 考虑一个调用它自己N次的递归函数。比较没有尾调用清除和有尾调用清除时堆栈遍历的性能

- 尾递归可以把堆栈中的数据清除，把空间留给最后的递归调用，因此没有尾递归调用的空间复杂度为O(N)，有尾递归的空间复杂度为O(1)，但是时间上他们均需要清除堆栈，传递参数，因此时间上性能均为O(N)，但是有尾递归可以直接返回结果，而不需要层层向上传递，因此可能要优于没有尾递归时调用。

- 练习1 云计算的三种服务模式分别是什么？
  - 软件即服务(SAAS)
  - 平台即服务(PAAS)
  - 基础设施即服务(IAAS)。
- 练习2 云计算的主要特征有哪些？
  - 按需自助服务
  - 泛在接入
  - 资源池化
  - 快速伸缩性
  - 服务可计量

- 练习1：三种入侵检测方法？
  - 基于主机：
  - 基于网络
  - 混合型
- 练习2：异常检测与误用检测？
  - 异常检测：入侵和滥用行为通常和正常的行为存在严重的差异，检查出这些差异就可以检测出入侵
  - 误用检测：是通过某种方式预先定义行为，然后见识系统的运行，从中找出符合预先定义规则的入侵行为。
  - 异常检测是指通过攻击行为的特征库,采用特征匹配的方法确定攻击事件.误用检测的优点是检测的误报率低,检测快,但误用检测通常不能发现攻击特征库中没有事先指定的攻击行为,所以无法检测层出不穷的新攻击。