8/1 简要说明毕巴模型中的低水标模型、毕巴环模型及严格模型之间的主要区别。

毕巴低水标模型立足于既防止直接的非法修改也防治简接的非法修改；
毕巴环模型不关心间接的非法修改问题，只关心直接的非法修改问题，环模型对写操作和执行操作进行控制，对“读”操作不实施任何控制；
毕巴模型的严格完整性形式根据主体和客体的完整性级别对“读”操作进行严格控制。

8/4 设 U1 是一个用户标识，TPJ 是一个转换过程，CDLk 是一个受保护的数据项，请问克-威模型如何判断用户 Ui 是否可以通过执行 TPJ 来对数据项 CDLK 进行操作？

用户 UI 通过执行 TPJ 对数据项 CDLK 进行操作，就必须由用户 UI 证明 TPJ 的有效性或 CDLK 的完整性；

如果用户 UI 有权证明 TPJ 的有效性，根据规则 E4（必须证明所有 TPJ 都向一个只能以附加的方法写的 CDLK 写入足够的信息，以便能够重视 TP 的操作过程），该用户就无权执行 TPJ，但已知条件说明用户 UI 能够执行 TPJ，这是矛盾的，所以不能由用户 UI 证明 TPJ 的有效性。

同样，如果用户 UI 有权证明 CDLK 的完整性，根据规则 E4，该用户就无权在 CDLK 上执行操作，但已知条件说明用户 UI 可执行 TPJ 在 CDLK 上的操作，这也是矛盾的，所以不能由用户 UI 证明 CDLK 的完整性。

8/11 MIT 的 AEGIS 模型在安全中央处理器中配备了哪些安全专用硬件单元？它们分别提供什么功能？

系统的可信计算基计算并检查进程对应的程序的哈希值，初始的进程的运行环境没有被非安全因素污染过。

AEGIS 模型通过保护进程的寄存器信息来保护进程环境信息的完整性。

这里涉及的存储介质的类型包括中央处理器中的 CACHE 高速缓存、中央处理器外的内存和磁盘等。系统需要用到进程的代码或数据时，首先把它们装入到内存中，进而装到 CACHE 高速缓存中，然后执行相应的代码并处理相应的数据。

在虚拟内存管理中，内存中的页面有可能被唤出到交换区中，交换区位于磁盘上，此时，在被唤出的页面上的代码或数据驻留被放置到磁盘上。

8/13 简要说明 MIT 的 AEGIS 完整性支持体系通过硬件单元实现莫科尔树模型的基本方法。

（1）一个进程的整个虚拟内存空间可以按照一定方式划分成一些列存储块，这些存储块为树叶，可以构造出一棵莫科尔树。利用这棵莫科尔树，完整性验证单元可以方便的对进程的虚拟内存空间中的存储块进行完整性验证。（2）当处理器从进程的虚拟内存空间中把信息读到 Cache 高速缓存中时，完整性验证单元验证指定虚拟地址对应的存储块的完整性，验证通过后，处理器才把相应的存储块中的信息存入到 Cache 高速缓存中。

8/14 简要说明内核主导的 IMA 模型进行完整性度量的基本方法。

（1）设计一个 measure 内核函数，用于对指定的内容进行完整性度量；（2）用于启动 measure 内核函数的完整性度量工作。

8/16 Tripwrite 文件完整性检查系统主要由哪些成分组成，结合这些成分，简要说明该系统的基本工作原理。

主要成分：控制策略、Tripewrite 基准数据库、及时数据库、Tripewrite 可执行程序、Tripewrite 需要使用配置信息。

原理：首先，根据完整性检查控制策略，为每个需要监控的文件生成一个指纹，并将它们存储到 Tripewrite 数据库中；必要时，重新为每个需要监控的文件生成新的指纹，并将新指纹与 Tripewrite 数据库中存储的指纹进行对比，由此可以确定需呀监控的文件是否已经被改动过。

5/1 简要说明 TE 模型的基本思想，并分析该思想与访问控制矩阵思想的相似之处和不同之处。

基本思想：它是一个强制访问控制模型，在 TE 模型中，把系统中所有主体划分成若干个组，每个组称为一个域，把系统中所有客体划分成若干个组，每个组称为一个类型。用 DDT 表定义域与类型的授权关系，以表中的行描述域，以表中的列描述类型，以行列交点描述访问权限。

相似点：都是采用矩阵思想

不同之处在于 TE 模型是强制访问控制，控制策略需要从 0 开始。

5/4 以进程对文件的访问为例，简要说明 DTE 模型的 DTEL 主要是从哪几个方面描述访问控制规则的。

DTE 模型是通过 DTEL 描述访问控制策略的配置而实现访问控制，DTEL 类型描述功能定义类型，类型赋值功能把类型赋值给客体；域描述功能定义域，域权限，域与主体关系以及主体的域切换方法，初始域设定功能设定第一个进程的工作域，从而使整个系统的进程的工作域的确定基础。

5/9 在 SETE 模型中，进程为实现工作域切换必须满足哪些条件？简要说明授权进程进行工作域切换的基本方法。

进程新的工作域必须拥有对可执行文件的类型的 entrypoint 的权限；

进程旧的工作域必须拥有对入口点程序的类型的 execute 访问权限；

进程旧的工作域必须拥有对进程的新的工作域的 transition 访问权限

5/11 在 SELinux 系统中，什么是访问判定？什么是访问向量？简要说明访问判定的基本方法。

用（source-type target-type，object-class,perm-list）四元组描述访问控制权，表示判定结果的位图称为访问向量。

判定方法：首先，除非在访问控制策略中有匹配的访问控制规则，明确授权主体，在客体上实施找定的操作，否则操作申请被拒绝。

其次，一旦操作申请被拒绝，系统将审计该操作被拒绝事件，除非系统明确说明无需审计。最后，如果系统对已授权的操作有明确的审计要求，就进行审计。

5/12 在 SELinux 系统中，什么是切换判定？简要说明切换判定的基本方法。

在 SELinux 系统中，为的是否需要切换新创建的进程和文件的类型标签做出结论的过程称为切换判定。

创建新进程时，将父进程的域标签作为新进程的域标签，创建新文件或新目录

时，将父目录的类型标签作为新文件或目录的类型标签。但有时需要给新的主体或新的客体分配新的标签。

5/15 SELinux 系统的内核体系结构主要由哪几部分组成？各部分主要分别负责承担什么任务？

由安全服务器、内核客体管理器、访问向量缓存 AVC

安全服务器提供安全策略判定；客体服务器在它所管理的资源上实施安全服务器所提供的安全策略判定结果；AVC 缓存安全服务器生成的访问判定结果供以后在进行访问权限检查时使用，也是内核客体管理器与安全服务之间的接口。

5/16 在 SELinux 系统的体系结构设计中，为什么需要用户控件的客体服务器？引入用户空间的安全服务期有什么好处？引入用户空间的策略管理服务器有什么好处？

（1）在 SELinux 系统体系结构中，它的突出特点是既支持对内核资源实施访问控制也支持对用户资源空间的资源实施访问控制；该体系结构源自 FLASK 体系结构，而 FLASK 体系结构是面向微内核的，在微内核系统中，大部分的资源管理是由用户空间服务器实现的

（2）用户空间的安全服务器可以便于用户空间的客体管理器提供访问控制判定，增设用户空间安全服器后，就可以把系统中的安全策略划分为内核策略和用户策略。

（3）在用户空间设定策略服务器，用户对 SELinux 系统中的所有安全策略进行总体处理，从中区分出内核策略和用户策略，把内核策略装入到内核安全服务器中，把用户策略安装到用户空间的安装服务器中。

4/2 什么是自主安全性？什么是强制安全性？自主安全性与自主访问控制之间，强制安全性与强制访问控制之间分别是什么关系？

强制安全性是指能够实现整个组织全范围的安全性策略，也称为非自主安全性；自主安全性是指体现普通用户在策略逻辑定义和安全属性分配方面的自主特点。

一个操作系统的强制安全性策略可以分解为多种具体的安全策略，如强制访问

控制策略、强制认证支持策略、强制加密支持策略。

4/5　在文件中保存口令相关信息的常见方法有哪些？试分析他们的安全性。

法一：在口令字段中保存明文，身份认证时，直接取其值与用户输入的口令进行对比；法二：用确定的算法借助口令进行加密，在口令字段中保存口令的密文，身份认证时，将口令的密文解密，将解密后的口令与用户输入的口令进行对比；法三：用确定的算法借助口令进行某种运算，在口令字段中保存运行的结果，身份认证时，借助用户输入的口令进行相同的运算，将口令字段中保存的结果与运算结果进行对比。

法一和法二分别保存明文和密文形式的口令。法一很难保证口令的安全，攻击者只需要得到账户信息数据库文件，就得到了所有账户的口令。法二难以抵御口令猜解攻击，攻击者可能采取已知密文猜解明文的方法去破解口令。法三在整个系统中不保存任何形式的 k 口令。

4/6 在口令中撒盐是什么意思？举例说明在 UNIX 系统实现口令撒盐的基本方法。

（1） 口令撒盐就是给口令拌入随机数的过程

（2） 生成一个随机数：Dsalt=Arandom();把随机数附加到口令上：Dtmp=Dpw||Dsalt;生成哈希值：Dhash=Ahash(Dtmp);把 Dhash 和 Dsalt 保存到系统中，作为用户的口令信息。

4/7　试举出操作系统支持的三种常见的网络化用户身份认证方法，并说明它们的基本原理和应用方法。

（1）基于客户机/服务器模式(简单模式、服务器认证、客户端认证)（2）认证消息的加密传输（客户机与服务器之间用密文传输）（3）面向服务的再度认证（KERVEROS 认证系统模式）

4/8　操作系统中的 PAM 身份认证框架是如何为具有身份认证需求的服务程序提供灵活的身份认证支持的？该框架由哪些主要成分构成？

为了使该框架发挥作用，系统管理员需要完成哪些工作？

PAM 的思想是实现服务程序与认证机制的分离，通过一个插拔式的接口，让服务程序插接到接口的一端，让认证机制插接到另一端，从而实现服务程序与认证机制的随意组合。PAM 框架定义了一个应用程序接口 API。一个 PAM 系统主要是由 API、动态装载的共享库和配置文件构成。在 PAM 框架中，每一种身份认证机制设置为一个 PAM 模块，实现为一个动态装载的共享库。PAM 模块遵循 PAM 的 API 规范。需要实施身份认证过程的服务程序按照 PAM 的 API 规范调用 PAM 系统中的身份认证功能。

4/15 简要说明 UNIX 操作系统中的 syslog 审计服务系统的基本结构和工作原理。

Syslog 审计服务系统由 syslog 的日志处理进程、配置文件、日志文件和 syslog 函数库构成；

工作原理：操作系统中的系统进程用户、进程及系统内核都有可能产生审计事件，它们可以调用 syslog 函数库中的函数把审计事件及相关的信息发送给 syslog 守护进程，由 syslog 为它们生成并处理日志信息。

1/2 信息安全攻击一般包含哪些主要环节？在各个环节中，攻击者主要想实现哪些目标？哪些环节与系统安全密切相关？为什么？

包含侦查、扫描、获取访问、维持访问、掩盖踪迹

侦查：收集尽量多的有关被攻击目标的信息，以便为实际的攻击做好准备；

扫描：以便进一步掌握有关的攻击目标的更多信息。

获取访问：闯入和访问目标系统

维持访问：在攻击成功之后为下一次攻击打开方便之门

掩盖踪迹：销毁攻击痕迹以便掩盖攻击行径

1/6 信息安全威胁可以划分为哪几种主要类型？它们分别有什么含义？什么样的行为可能产生这些威胁？

（1）威胁分为泄露、欺骗、破坏、篡夺。（2）泄露：对信息的非授权访问；欺骗：接受虚假数据；破坏：中断或妨碍正常工作；篡夺：对系统某些部分的非

授权控制。（3）泄露行为：嗅探；欺骗行为：篡夺或更改、伪装或电子欺骗、信源否认、信宿否认；篡夺行为：伪装或电子欺骗、拖延、拒绝服务

1/10 什么是控制访问矩阵？试说明它的结构和含义，并举例说明它在实际应用中的应用方法。

访问控制矩阵是对访问控制行为的一种抽象表示。（2）矩阵中的行与系统中的主体相对应，矩阵中的列与系统中的客体相对应，处于行与列的交叉点上的矩阵元素，描述主体对客体的访问权限。

3：**绑定：**用一个实体的公钥对一项信息进行加密的过程；绑定的情形是信息的发送方用信息的接收方的公钥对信息进行加密。

签名：签名把信息的完整性与用于产生签名的密钥关联在一起。TPM 把一些密钥标记为只用于签名的密钥。

封装：把一项信息与一个平台的的某个状态绑定在一起的过程称为信息在平台上的封装，平台的状态通常由平台的完整性度量值表示。

封装的签名：验证方要求一个签名必须包括一组特定的 PCR 寄存器。在签名操作期间，签名方采集特定寄存器的值，把它们组合到给定的信息之中，在计算待签名的摘要时，它们作为计算的输入信息的一部分，影响计算的输出结果。