操作系统安全复习

第一部分 引言

1、 操作系统安全威胁：病毒特征、蠕虫、逻辑炸弹、特洛伊木马、天窗、隐蔽通道

- 计算机病毒：指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者代码。 特点：隐蔽性、传染性、潜伏性、破坏性
- 蠕虫：类似计算机病毒，是一种能自我复制的计算机程序。蠕虫可能会执行垃圾代码发动DDOS攻击，还可以更改和破坏数据。不需要附在别的程序内，可能不用使用者介入操作也能自我复制或执行。
- 逻辑炸弹：附着在某些合法程序上的恶意代码，在特定的逻辑条件满足下会激活和执行。一般都被添加到被感染程序的起始处。不能复制自身，不能感染其他程序
- 木马：表面执行合法功能，实际上却运行非法功能。木马是一个独立的应用程序，不能自我复制，具有潜伏性。
- 隐蔽通道：系统中不受安全策略控制的、违反安全策略的信息泄露路径。分为隐蔽存储通道和隐蔽定时通道
- 天窗/后门：嵌在操作系统里的一段非法代码，渗透者利用该代码提供的方法侵入操作系统而不受检查

2、操作系统安全和信息系统安全

一个有效可靠的安全系统应具有很强的安全性，必须具有相应的保护措施，消除或限制如病毒等对系统构成的安全隐患。

一个安全的计算机信息系统应该满足机密性、完整性、可追究性和可用性的要求（P3~P6）

操作系统安全是信息系统安全的基础

3、术语

- 安全周界：用半径表示空间。该空间包围着用于处理敏感信息的设备，并在有效的物理和技术控制之下，防止未授权的进入或敏感信息的泄露
- 主体：系统能够发起行为的实体，如进程
- 客体：系统中被动的主体行为承担者。对一个客体的访问隐含着对其包含信息的访问。
- 标识与鉴别：用于保证只有合法用户才能进入系统，进而访问系统中的资源
- 访问控制：限制已授权的用户、程序、进程或计算机网路中其他系统访问本系统资源的过程
- 最小特权原则：系统中每一个主体只拥有与其操作系统相符所需要的、必需的、最小的特权集
- 隐蔽通道：允许进程以危害系统安全策略的方式传输信息的通信信道
- 审计：一个系统的审计就是对系统中有关安全的活动进行记录、检查及审核
- 授权：授予用户、程序或进程的访问权
- 操作系统安全：操作系统无错误配置、无漏洞、无后门、无木马等，能防止非法用户对计算机资源的非法访问，一般用来表达对操作系统的安全需求
- 操作系统的安全性：操作系统具有或应具有的安全功能，如存储保护、运行保护、标识与鉴别、安全审计等
- 安全操作系统：对所管理的数据与资源提供适当的保护级，有效控制硬件与软件功能的操作系统。通常，一个安全操作系统是从开始设计时，就充分考虑到系统的安全性。另一种是基于一个通用的操作系统，对其专门进行安全性改进或增强，并通过相应的安全性评估
- 多级安全操作系统：实现了多级安全策略的安全操作系统，如符合TECSEC-B1级以上的安全操作系统

4、构建安全的基本要素方面主要内容

第二部分 基本概念

1、系统边界与安全周界

- 系统边界：确定系统边界需要准确地规范系统和外界的接口。外部安全控制实施于这些接口，只要控制到位，内部控制就可以保护系统内部信息免受特定的威胁。
- 安全周界：系统内部组件有两种，负责维护系统安全（或安全相关）的部分和所有其他部分。用一种假象的边界分离两种类型的组件，该边界称为安全周界。

> 安全边界内的所有组件的属性必须被精确定义，因为任何一个组件发生故障，都可能导致安全背离；相反，安全周界外部的组件的属性是相当随意的，仅实施通过系统边界进入系统时的限制。

2、操作系统安全功能：操作系统的安全性是指操作系统具有或应具有的安全功能

3、软件可信类别：可信的、良性的、恶意的

- **可信软件：软件保证能安全运行，且以后系统的安全也依赖于该软件的无错操作**
- 良性的：软件并不确保安全运行，但由于使用了特权或对敏感信息的访问权，因而必须确信它不会有意地违反规则。良性软件的错误被视作偶然性的，这类错误不会影响系统安全
- 恶意的：软件来源不明，从安全角度出发，该软件必须被当作恶意的，认为其将对系统造成破坏

> 日常软件大多是良性的

4、安全策略和安全模型

- 安全策略是针对系统面临的安全威胁所采取的应对方法，包括有关管理、保护和发布敏感信息的法律、规定和实施细则。
- 安全模型是对安全策略所表达的安全需求的简单、抽象、无歧义的描述，它为安全策略和安全策略实现机制的关联提供了一种框架。

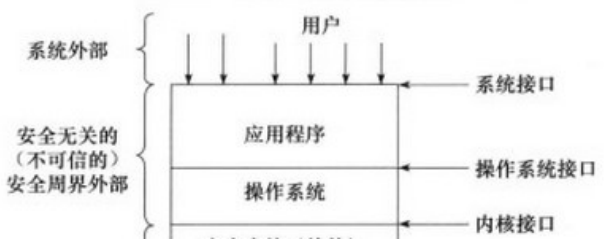
安全模型描述了对于某个安全策略需要用哪种机制来满足；而模型的实现则描述了如何把特定的机制应用与系统中，从而实现某一特定安全策略所需的安全保护。

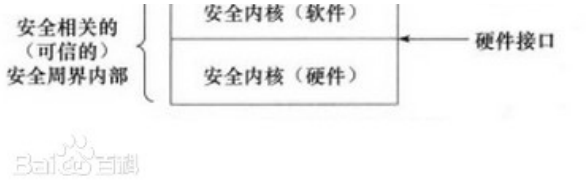
5、引用验证机制满足的原则

1. 必须具有自我保护能力。 保证引用验证机制即使受到攻击也能保持自身的完整性。
2. 必须总是处于活跃状态。 保证程序对资源的所有引用都应得到引用验证机制的仲裁。
3. 必须设计得足够小，以利于分析和测试，从而能够证明它的实现是正确的。 保证引用验证机制的实现是正确和符合要求的

6、安全内核的设计和实现的基本原则（P35）

安全内核是指系统中与安全性实现有关的部分，包括访问控制机制、授权机制和授权管理机制等部分。安全内核是实现引用监控器概念的一种技术。





安全内核的设计和实现应当符合一下三个基本原则：

1. 完整性原则：要求主体引用客体时必须通过安全内核，即所有信息的访问必须经过安全内核。
2. 隔离性原则：要求安全内核具有防篡改的能力，既可以保护自己，防止偶然破坏
3. 可验证性原则：
    - 利用最新的软件工程技术，包括结构设计、模块化、信息隐藏、分层、抽象说明以及合适的高级语言；
    - 内核接口简单化；
    - 内核小型化；
    - 代码检查；
    - 完全测试；
    - 形式化数学描述与验证。

7、TCB (Trusted Computing Base,可信计算基) 的组成部分

1. 操作系统的安全内核
2. 具有特权的程序和命令
3. 处理敏感信息的程序，如系统管理命令等
4. 与TCB实施安全策略有关的文件
5. 其他有关的固件、硬件和设备
6. 负责系统管理的人员
7. 保障固件和硬件正确的程序和诊断软件

8、隐蔽通道的概念及类型（P64）

隐蔽通道：允许进程以危害系统安全策略的方式传输信息的通信信道(TCSEC,1985)
可分为 隐蔽存储通道 和 隐蔽定时通道 ， 或者分类为 噪音通道 和 无噪通道

9、隐蔽通道与MAC策略关系（P65）

隐蔽通道只与强制安全策略（MAC）有关，与自主安全策略（DAC）无关。

10、隐蔽通道的分类（P65）

- 隐蔽存储通道
  发生条件：如果使用这种通道涉及一个进程直接或间接写入一个存储位置，此时便有另外一个进程直接或间接读这个存储位置。一般来说隐蔽存储通道涉及不同安全级主体可以共享的某种有限的资源（如硬盘）
- 隐蔽定时通道
  发生条件：通过一个进程采用调节自己对系统资源（如CPU）的使用，从而影响另外一个进程观察到的真实响应时间。

隐蔽通道可能是有噪音的，也可能是无噪音的。无噪通道是指发送者发送的信号与接收者接受的信号百分百相同。

11、如何判定存储通道与定时通道

- 隐蔽存储通道：

1. 发送方和接收方进程必须有权存取共享资源的同一属性
2. 发送方进程必须有办法改变（如写）该共享资源

3. 接收方进程必须有办法侦察（如读）该共享资源的改变
4. 必须存在某种机制，是发送方和接收方进程能启动隐蔽通信并正确给事件排序。该机制可能是另外一条较小带宽的隐藏通道

- 隐蔽定时通道：

1. 发送方和接收方进程必须有权存取共享资源的同一属性
2. 发送方和接收方进程必须有权存取一个时间参照，如实时时钟
3. 必须存在某种机制，是发送方和接收方进程能启动隐蔽通信并正确给事件排序。该机制可能是另外一条较小带宽的隐藏通道

12、隐蔽通道的特征

第三部分 安全机制

1、操作系统的安全性设计的方面：

物理上分离、时间上分离、逻辑上分离、密码上分离，设计过程考虑的安全策略

2、操作系统安全的主要目标、通用安全需求

- 主要目标：
  1. 按系统安全策略对用户的操作进行访问控制，防止用户对计算机资源的非法存取（窃取、篡改和破坏）
  2. 标识系统中的用户和身份鉴别
  3. 监督系统运行的安全性
  4. 保证系统自身的安全性和完整性、

3、硬件安全机制：存储保护、运行保护、I/O保护 （P42-P45）

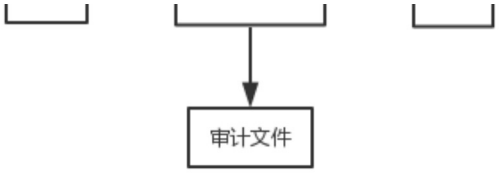
- 存储安全：最基本的要求，保护用户存储在存储器中的数据。保护单元为存储器中的最小数据范围，保护单元越小，存储安全精度越高
- 运行安全：等级域机制应该保护某一环不被其外层环侵入，并且允许在某一环内的进程能够有效的控制与利用该环以及低于该环特权的环
- I/O安全

4、安全操作系统的标识与鉴别机制：概念、注意的问题（P54）

标识与鉴别是涉及系统和用户的一个过程。标识是系统要求标识用户的身份，并为每个用户取一个名称——用户标识符。用户标识符必须唯一且不能伪造，防止其他用户冒充。将用户标识符与用户联系的动作称为鉴别，用以识别用户的真实身份，它总是需要用户具有能够证明他身份的特殊信息，这个信息是秘密的，任何其他用户都不能拥有它。

5、访问控制机制的引用监控器的基本原理及思想

访问控制机制的理论基础是引用监控器。引用监控器的具体实现称为引用验证机制，它是实现引用监控思想的软硬件的结合。



安全策略所要求的存取判定以抽象存取访问控制数据库中的信息为依据，存取判定是安全策略的具体体现，它随着主体和客体的产生或删除及其权限的修改而改变。引用监控器的关键作用是控制从主体到客体的每一次存取，并将重要的安全事件存入审计文件中。

6、自主访问控制（DAC）概念及实现方式

DAC是用来决定一个用户是否有权访问客体的一种访问约束机制。文件的拥有者可以按照自己的意愿精确指定系统中其他用户对其文件的访问权。
为了实现完备的自主访问控制机制，系统要将访问控制矩阵相应的信息以某种形式保存在系统中。实际的方法是基于矩阵的行或列表达访问控制信息。

7、基于行的自主访问控制机制明细表形式：能力表、前缀表、口令（P46）

8、基于列的自主访问控制机制明细表形式：保护位、访问控制表。（P47）

9、强制访问控制(MAC)基本概念及原理

MAC机制下，系统中的每个进程、文件、IPC客体（消息队列、信号量集合和共享存储区）都被赋予了相应的安全属性，这些安全属性是不能改变的，它由管理部门(如安全管理员)或由操作系统自动地按照严格的规则来设置，不像访问控制表那样，可由用户或他们的程序直接或间接修改。

10、自主访问控制与强制访问控制的区别

适用场合不同。
DAC 和 MAC 是两种不同类型的访问控制机制，它们常结合起来使用。用户用 DAC 防止其他用户非法入侵自己的文件，MAC 使用户不能通过意外事件和有意识的误操作逃避安全控制。MAC 用于将系统中的信息分密级和类进行管理。

11、强制访问控制防止特洛伊木马（P53）

防止木马侵入系统是极端困难的，如果不依赖与一些强制手段，想避免木马的破坏是不可能的。使用 MAC 机制，对于违反强制访问控制的木马，可以防止它取走信息。

12、最小特权管理基本思想

系统不应给用户超过执行任务所需特权以外的特权，如应将超级用户的特权划分为一组细粒度的特权，分别授予不同的系统操作员/管理员，使各种系统操作员/管理员只具有完成其任务所需的特权，从而减少由于特权用户口令丢失或错误软件、恶意软件、误操作所引起的损失。

13、可信路径 / 可信通路的概念及一般过程（P59）

可信通路提供保障用户和内核通信的机制。

14、安全审计概念及目的

一个系统的安全审计就是对系统中有关安全的活动进行记录、检查和审核。
目的是检测和阻止非法用户对计算机系统的入侵，并显示合法用户的误操作。

15、安全操作系统一般要审计的事件：注册事件、使用系统事件和利用隐蔽通道事件

亦即标识和鉴别机制的使用、把客体引入到用户的地址空间（如创建文件、启动程序）、从地址空间删除客体、特权用户所发生的动作，以及利用隐蔽存储通道的事件等。第1类属于系统外部事件，即准备进入系统的用户产生的事件；后两类属于系统内部的事件，即已经进入系统的用户产生的事件。

第四部分 通用操作系统安全机制

1、Unix操作系统提供系统功能的方式

- 系统调用
- 异常
- 中断
- 系统进程

2、标识与鉴别机制概念与原理(P86)

UNIX的各种管理功能都被限制在一个超级用户（ROOT）的权限中。超级用户可以控制系统中的所有资源。它能够管理所有资源的各类变化情况，或者只管理很小范围的重大变化。

3、自主存取控制机制（DAC）和强制存取控制（MAC）的原理

4、最小特权管理概念

UNIX 将敏感操作分成26个特权，由一些特权用户分别掌握这些特权，每个特权用户都无法独立完成所有的敏感操作。系统的特权管理机制维护一个管理员数据库，提供执行特权命令的方法。所有用户进程一开始都不具有特权，通过特权管理机制，非特权的父进程可以创建具有特权的子进程，非特权用户可以执行特权命令。系统定义了许多职责，一个用户与一个职责关联。职责中又定义了与之相关的特权命令，即完成这个职责需要执行哪些特权命令。

5、Windows安全模型及其组成部分（P96）

安全模型由本地安全认证、安全帐号管理器、安全资源引用监控器构成，还包括注册、访问控制和对象安全服务等。

6、Windows安全登录过程以及远程安全登录（P102）

第五部分 安全策略与安全模型

1、安全策略概念及其表达语言、信息系统的安全需求主要方面

- 安全策略是一种声明，它将系统的状态划分为两个集合：一个是已授权的集合，即安全状态集合，另一个是未授权状态的集合，即不安全状态集合。
- 安全策略表达语言主要分为高层策略语言和低层策略语言。高层策略语言用于表达对系统中抽象实体的策略限制，低层次语言用于表达对系统中程序的输入或调用选项的限制。

2、安全策略的类型及对应的安全需求

- 机密性策略：保护信息机密性的安全策略
- 完整性策略：保护信息完整性的安全策略
- 混合型：同时着眼与两个方面
- 中立型：可以适用多样性安全目标的安全策略，可以用于表达机密性策略、完整性策略、混合策略甚至其他安全目标策略。

3、安全模型的特点、目的及基本要求

安全模型特点：

- 精确、无歧义的
- 简易和抽象的，容易理解
- 它是安全相关的，即只涉及安全性质，而不限制系统的功能极其实现
- 它是安全策略的清晰表达

目的：安全模型的目的在于明确表达安全需求，为设计开发安全系统提供方针。

基本要求：

- 完备性
- 正确性
- 一致性
- 简明性

4、状态机模型原理和开发一个状态机的步骤

用模仿操作系统和硬件执行过程的方法描述计算机系统，它将一个系统描述为一个抽象的数学状态机器。在这样的模型里，状态变量表示机器的状态，转换函数或者操作规则用以描述状态变量的变化过程，它是对系统应用通过请求系统调用从而影响操作系统状态的这一方式的抽象。这个抽象的操作系统具有正确描述状态可以怎样变化和不可以怎样变化的能力。

开发步骤：

1. 定义安全相关的状态变量
2. 定义安全状态的条件
3. 定义状态转换函数
4. 检验函数是否维持了安全状态
5. 定义初始状态
6. 依据安全状态的定义，证明初始状态安全

5、BLP模型概念（基本概念、机密性模型、适用于军事安全策略、最早的多级安全模型、状态机安全模型）（P114）

6、BLP模型的安全策略包括强制存取控制和自主存取控制，其分别对应于哪种安全策略

自主安全策略： 访问矩阵
强制访问控制： 简单安全特性 和 *特性

7、BLP模型的优点与不足

不足：

- 模型使用了与可信主体相关的安全规则，使得人们很难确定系统执行的安全规则的确定特性，也就是说系统真正执行的安全规则既有 BLP 的安全规则又有可信主体超越 BLP 安全规则的规则

- BLP 仅处理单级客体， 缺乏处理多级客体的相关机制， 但是一些信息系统的数据对象（如硬盘）只能按多级对象处理。
- 没有支持应用相关的安全规则。

8、Biba模型（基本概念、完整性模型、完整级别：密级和范畴），以及该模型控制下的隐蔽通道 (P123)

9、Biba模型基本原理及优点、不足（P126）

优势：

- 简单性
- 与 BLP 模型相结合的可能性

不足：

- 完整性标签确定的困难性
- 在有效保护数据一致性方面是不充分的
- 当机密性和完整性都受到充分的重视后，很容易出现进程不能存取任何数据的局面。

10、Clark-Wilson安全模型的基本原理（P127）

11、多策略安全模型：中国墙安全模型（机密性和完整性结合的商业安全模型、RBAC安全模型和DTE安全模型可以描述多种安全需求的中立安全模型）（P131）

12、RBAC安全模型（基本概念、基本要素构成）（P137——P140）

RBAC——基于角色的存取控制模型提供了一种强制存取控制机制。
角色类似于业务系统中的岗位、职位或分工。
要求明确区分权限和职责两个概念。

第六部分 安全体系结构

1、安全体系结构含义及主要内容

安全体系结构主要包含如下几个方面：

1. 详细描述系统中与安全相关的所有方面
2. 在一定的抽象层次上，描述各个安全相关模块之间的关系
3. 提出指导设计的基本原理
4. 提出开发过程的基本框架以及对于该框架体系的层次结构

2、安全体系结构类型、设计的基本原则

- 类型：
    1. 抽象体系
    2. 通用体系
    3. 逻辑体系
    4. 特殊体系
- 基本原则：
    1. 从系统设计之初就考虑安全性

2. 应尽量考虑未来可能面临的安全需求
3. 隔离安全控制，并使其最小化
4. 实施特权极小化
5. 结构化安全相关功能
6. 使安全相关的界面友好
7. 不要让安全依赖于一些隐藏的东西

3、权能体概念及优点

4、Flask体系结构支持策略可变通性的含义

把计算机系统抽象成一个状态机，它执行原子操作来完成从一个状态到另一个状态的转换，这对定义安全策略的可变通性更有用。在这种模型下，如果安全策略能够以原子粒度介入到系统执行的任意操作中，如允许操作的运行、拒绝操作，甚至介入自己的操作，一个系统就可以考虑提供整个安全策略的可变通性。在这样的系统中，如果当前系统状态包括了历史信息，则安全策略能利用整个当前系统状态知识来做决定。因为介入所有访问请求是可能的，所以修改现存的安全策略和撤销任何以前授予的访问权也是可能的。

第七部分 安全保证技术

1、安全保证与安全保障概念及其区别

- 安全保证：对系统满足安全需求的信任，基于保证技术提供了相关证据
  - 关心的是安全需求和安全机制的实现的正确性、一致性和完整性
- 安全保障：能够访问信息并保持信息质量的安全性
  - 关心的是信息面临的威胁，以及用来保护信息的安全机制

2、安全开发生命周期 (SDL) 过程

培训	要求	设计	实施
核心安全培训	分析安全和隐私风险；定义质量门	威胁建模；攻击点分析	安全工具；遵守禁止的功能；静态分析

验证/测试	发布/审查	维护/响应
动态/FUZZ 测试；验证威胁模块/攻击点	响应计划；最终安全审查；发布安装包	响应执行

3、形式化验证技术和形式化安全验证技术概念（P189-P196)

4、形式化安全验证系统的组件：规范语言处理器、验证条件生成器和定理证明器

5、操作系统安全测评方法 (P197)

1. 形式化验证
2. 非形式化验证
3. 入侵分析

6、TCSEC对安全功能的4类7个安全级别的内容

- D类包含一个级别——D级，是安全性最低的等级。不满足任何高安全可信性的系统全部划入D类。该级别说明整个系统都是不可信任的。

- C类为自主保护类。该类的安全特定在于系统的对象（如文件、目录）可由其主体（如系统管理员、用户、应用程序）自定义访问权。自主保护类依据安全从低到高又可分为C1（自主安全保护级）、C2（受控制的访问控制级）两个安全级别。

- B类为强制保护类。该类的安全特点在于有系统强制的安全保护，在强制保护模式中，每个系统文件及主体都有自己的安全标签，系统则依据主体和对象的安全标签赋予它对访问对象的访问权限。强制保护类依据安全从低到高又分为B1（标记安全保护级）、B2（结构保护级）、B3（安全域级）三个安全等级。

- A类为验证设计类：A类是当前橘皮书中最高的安全级别，它包含了一个严格的设计、控制和验证过程。

第八部分 安全操作系统设计

1、安全操作系统设计的原则

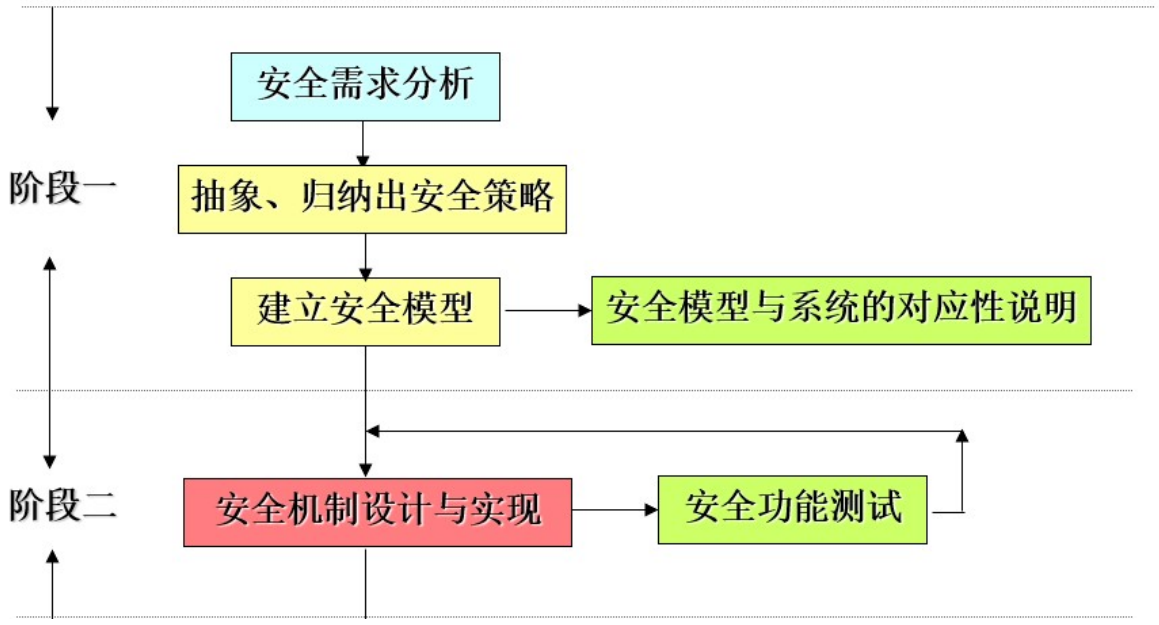
- 最小特权
- 机制的经济性
- 开放系统设计
- 完整的访问控制机制
- 基于“允许”的设计原则
- 权限分离
- 避免信息流的潜在通道
- 方便使用。友好的用户接口

2、安全操作系统的开发方法

- 虚拟机法
- 改进/增强法
- 仿真法

3、安全操作系统的开发过程

1. 系统需求分析
2. 系统功能描述
3. 系统实现



安全操作系统的一般开发过程

Book:《操作系统安全设计》. 沈晴霓 / 卿斯汉. 机械工业出版社. *2013-9. ISBN: 9787111432159.*