极客时间训练营

系统架构设计师

第18章 安全架构设计理论与实践

授课：王建平

目录

目录

信息系统安全威胁

◆信息系统可能遭受到的威胁可总结为以下4 个方面：（★★）

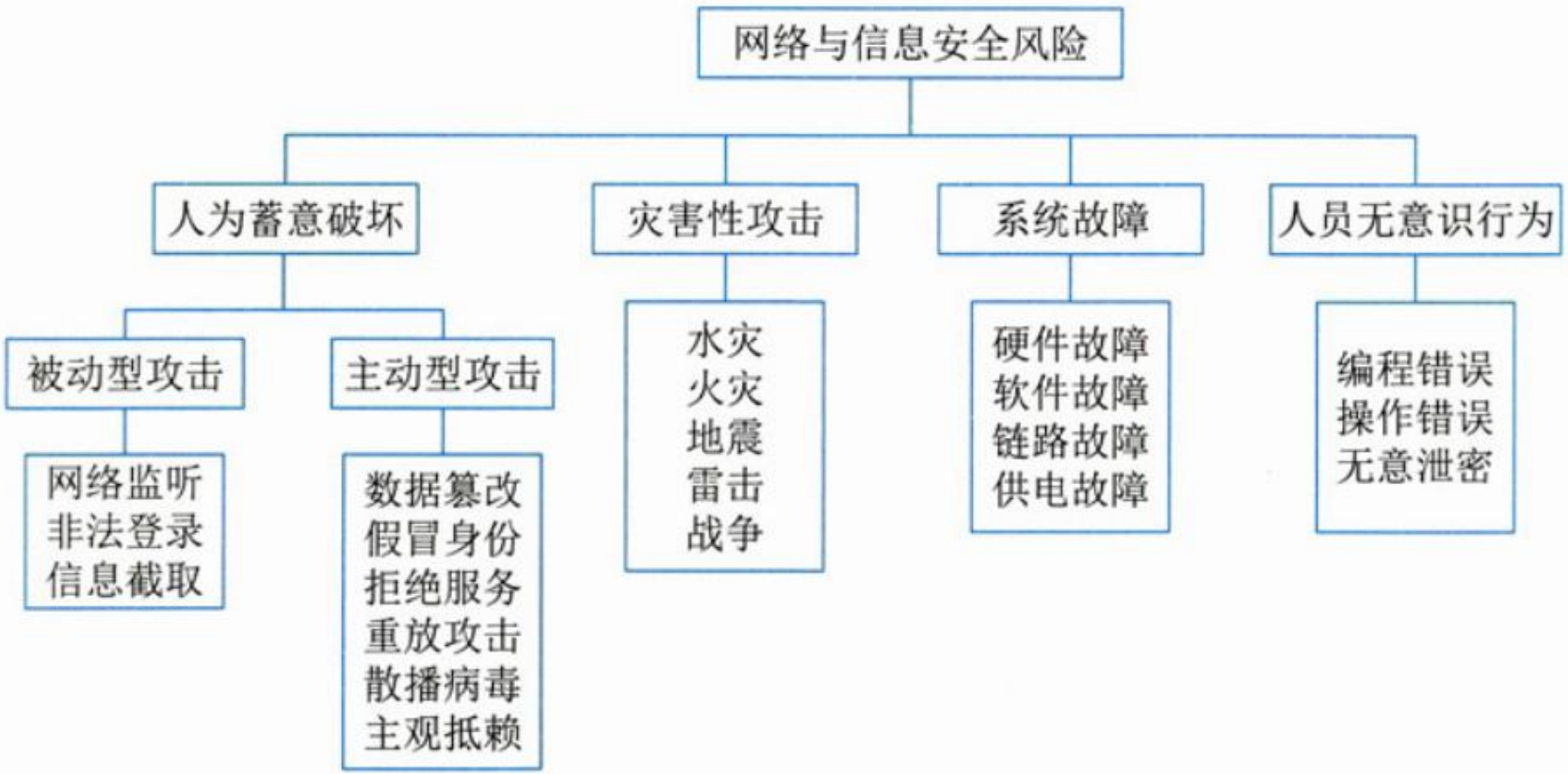


图 18-1　信息系统受到的安全威胁

安全架构概述

◆对于信息系统来说，威胁可以是针对物理环境、通信链路、网络系统、操作系统、应用系统以及管理系统等方面。

1）物理安全威胁是指对系统所用设备的威胁，如自然灾害、电源故障等；

2）通信链路安全威胁是指在传输线路上安装窃听装置或对通信链路进行干扰；

3）网络安全威胁是指通过技术手段窃取互联网信息，对网络形成严重的安全威胁；

4）操作系统安全威胁是指对系统平台中的软件或硬件芯片中植入威胁，如“木马”和“陷阱门”、BIOS的万能密码；

5）应用系统安全威胁是指对于网络服务或用户业务系统安全的威胁；

6）管理系统安全威胁是指由于人员管理上疏忽而引发人为的安全漏洞，如人为的通过拷贝、拍照、抄录等手段盗取计算机信息。

安全架构概述

◆具体来讲，常见的安全威胁有以下几种。（★★★）
(1)信息泄露：信息被泄露或透露给某个非授权的实体。
(2)破坏信息的完整性：数据被非授权地进行增删、修改或破坏而受到损失。
(3)拒绝服务：对信息或其他资源的合法访问被无条件地阻止。
(4)非法使用(非授权访问):某一资源被某个非授权的人或以非授权的方式使用。
(5)窃听：用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。
(6)业务流分析：通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等态势进行研究，从而发现有价值的信息和规律。
(7)假冒： 通过欺骗通信系统(或用户)达到非法用户冒充成为合法用户， 或者特权小的用户冒充成为特权大的用户的目的。黑客大多是采用假冒进行攻击。
(8)旁路控制：攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。
(9)授权侵犯：被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权的目的，也称作“内部攻击”。

安全架构概述

(10)特洛伊木马：软件中含有一个察觉不出的或者无害的程序段，当它被执行时，会破坏用户的安全。
(11)陷阱门：在某个系统或某个部件中设置了“机关”,使得当提供特定的输入数据时，允许违反安全策略。
(12)抵赖：这是一种来自用户的攻击，例如，否认自己曾经发布过的某条消息、伪造一份对方来信等。
(13)重放：所截获的某次合法的通信数据备份，出于非法的目的而被重新发送。
(14)计算机病毒：所谓计算机病毒，是一种在计算机系统运行过程中能够实现传染和侵害的功能程序。一种病毒通常含有两个功能：一种功能是对其他程序产生“感染”;另外一种或者是引发损坏功能或者是一种植入攻击的能力。

安全架构概述

(15)人员渎职：一个授权的人为了钱或利益、或由于粗心，将信息泄露给一个非授权的人。
(16)媒体废弃：信息被从废弃的磁盘或打印过的存储介质中获得。
(17)物理侵入：侵入者通过绕过物理控制而获得对系统的访问。
(18)窃取：重要的安全物品，如令牌或身份卡被盗。
(19)业务欺骗：某一伪系统或系统部件欺骗合法的用户或系统自愿地放弃敏感信息。

安全架构概述

◆安全架构是架构面向安全性方向上的一种细分，通常的产品安全架构、安全技术体系架构和审计架构可组成三道安全防线。（★）
(1)产品安全架构：构建产品安全质量属性的主要组成部分以及它们之间的关系。产品安全架构的目标是如何在不依赖外部防御系统的情况下，从源头打造自身安全的产品。

(2)安全技术体系架构：构建安全技术体系的主要组成部分以及它们之间的关系。安全技术体系架构的任务是构建通用的安全技术基础设施，包括安全基础设施、安全工具和技术、安全组件与支持系统等，系统性地增强各产品的安全防御能力。

(3)审计架构：独立的审计部门或其所能提供的风险发现能力，审计的范围主要包括安全风险在内的所有风险。

典型真题

以下网络攻击中，（）属于被动攻击。
A.拒绝服务攻击
B.重放
C.假冒
D.网络监听
参考答案：D

软件中含有一个察觉不出的或者无害的程序段，当它被执行时，会破坏用户的安全属于（）。
A.拒绝服务攻击
B.重放
C.病毒
D.木马
参考答案：D

目录

安全模型

◆信息系统的安全目标是控制和管理主体(含用户和进程)对客体(含数据和程序)的访问。
◆安全模型是准确地描述安全的重要方面及其与系统行为的关系，安全策略是从安全角度为系统整体和构成它的组件提出基本的目标。安全模型提供了实现目标应该做什么，不应该做什么，具有实践指导意义，它给出了策略的形式。
◆如下图是模型的分类：（★★）

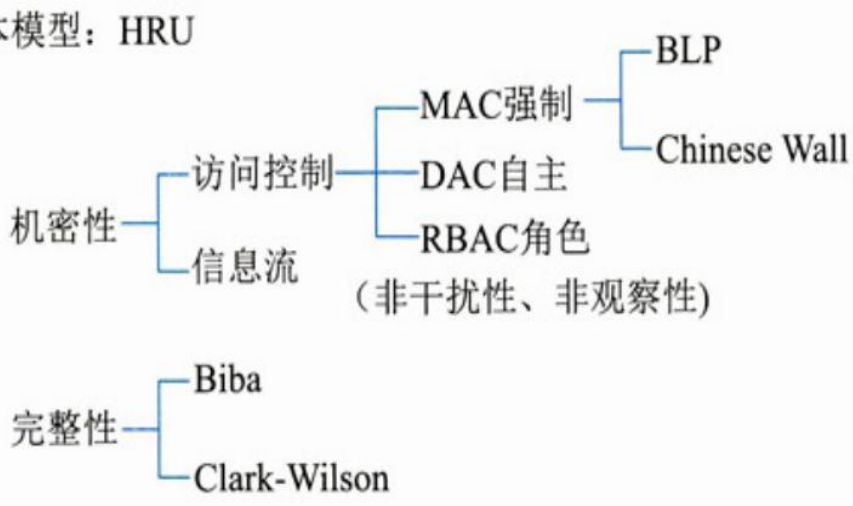


图 18-3　安全模型的分类方法

- ✓ HRU：访问控制矩阵模型（Harrison、 Ruzzo、Ullman)；
- ✓ MAC：强制访问控制模型（Mandatory Access Control)；
- ✓ DAC： 自主访问控制模型（Discretionary Access Control)；
- ✓ RBAC： 基于角色的访问控制模型（Role-Based Access Control)。

安全模型-状态机模型

◆状态机模型（★）
状态机模型描述了一种无论处于何种状态都是安全的系统。它是用状态语言将安全系统描述成抽象的状态机，用状态变量表述系统的状态，用转换规则描述变量变化的过程。一个状态是处于系统在特定时刻的一个快照。如果该状态所有方面满足安全策略的要求，则称此状态是安全的；一个安全状态模型系统，总是从一个安全状态启动，并且在所有迁移中保持安全状态，只允许主体以和安全策略相一致的安全方式访问资源访问。

◆状态机模型工作原理具体步骤描述如下：
(1)状态变量的默认值必须安全；
(2)用户试图使用变量的默认值；
(3)系统检查主体的身份验证；
(4)系统确保变更不会使系统置于不安全状态；
(5)系统允许变量值变更，发生状态改变(STATE CHANGE)；
(6)再重复执行(1)~(5)步，会导致另一次
状态变化。

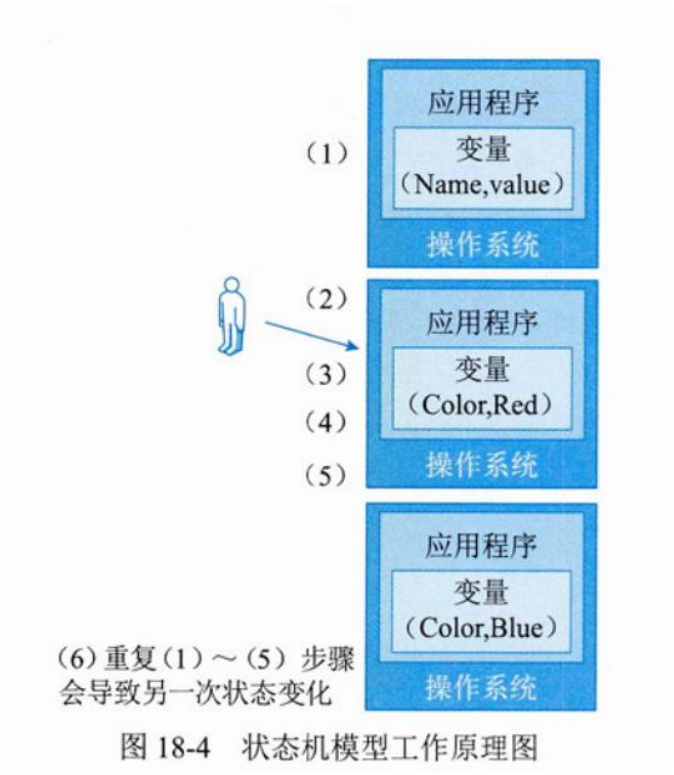
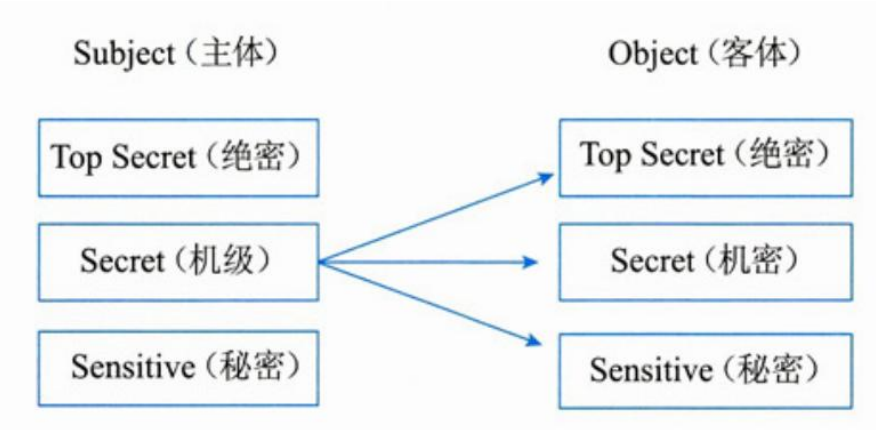


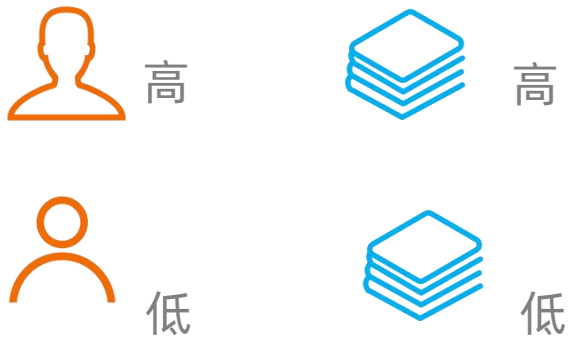
图 18-4　状态机模型工作原理图

安全模型-BLP模型

◆BLP模型（主要是下读上写保证机密性问题）（★★★）
◆ Bell-LaPadula 模型使用主体、客体、访问操作(读、写、读/写)以及安全级别这些概念，当主体和客体位于不同的安全级别时，主体对客体就存在一定的访问限制。通过该模型可保证信息不被不安全主体访问。Bell-LaPadula模型是符合军事安全策略的计算机安全模型，简称BLP模型。

◆ 其安全规则：
✓ 简单安全规则 ： 安全级别低的主体不能读取安全级别高的客体；（不能上读，只能下读）--对上只能提供数据但是不能获取数据。
✓ 星属性安全规则：安全级别高的主体不能往低级别的客体写。（不能下写，只能上写）--对下可以获取数据不能为下级提供数据）
✓ 强星属性安全规则：不允许对另一级别进行读写。（同一级别可读可写）
✓ 自主安全规则：使用访问控制矩阵来定义说明自由存取控制。

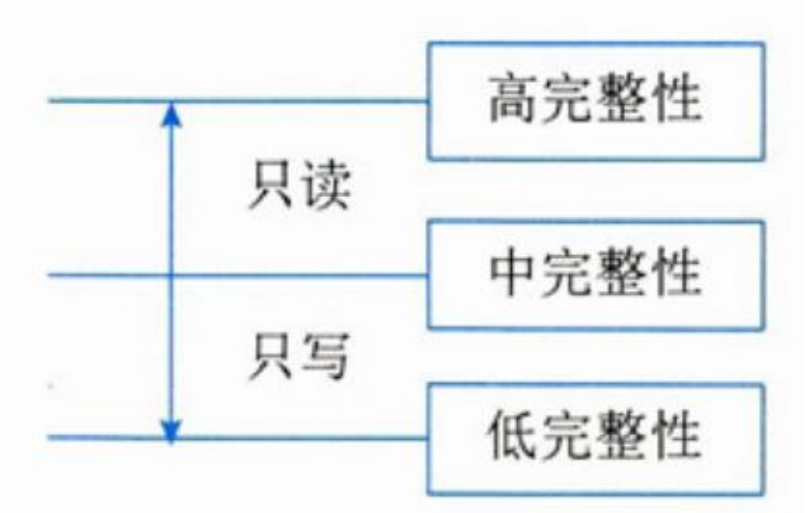




安全模型-BiBa模型

◆BiBa模型（总结：主要是上读下写保证完整性问题）（★★★）
此模型主要用于防止非授权修改系统信息，以保护系统的信息的完整性。模型也是采用主体、客体、完整性级别描述安全策略要求。

◆BiBa模型能够防止数据从低 完整性级别流向高完整性级别，其安全规则如下：（上读下写原则）
(1）星完整性规则：表示完整性级别低的主体不能对完整性级别高的客体写数据；（不能上写，只能下写）
(2）简单完整性规则：表示完整性级别高的主体不能从完整性级别低的客体读取数据；（不能下读，只能上读）
(3）调用属性规则：表示一个完整性级别低的主体不能从级别高的客体调用程序或服务。（主体级别≥客体级别）



安全模型-Clark-Wilson 模型

◆Clark-Wilson 模型型实现了成型的事务处理机制，常用于银行系统中以保证数据完整性。（★）

◆模型基本原理

CWM是一种将完整性目标、策略和机制融为一体的模型。为了体现用户完整性，CWM提出了职责隔离(Separation of Duty)目标；为了保证数据完整性，CWM提出了应用相关的完整性验证进程；为了建立过程完整性，CWM定义了对于变换过程的应用相关验证。

◆模型特征

CWM的主要特征是：

(1)采用Subject/Program/Object三元素的组成方式。Subject要访问Object只能通过Program进行；

(2)权限分离原则：将要害功能分为有2个或多个Subject完成，防止已授权用户进行未授权的修改；

(3)要求具有审计能力(Auditing)。

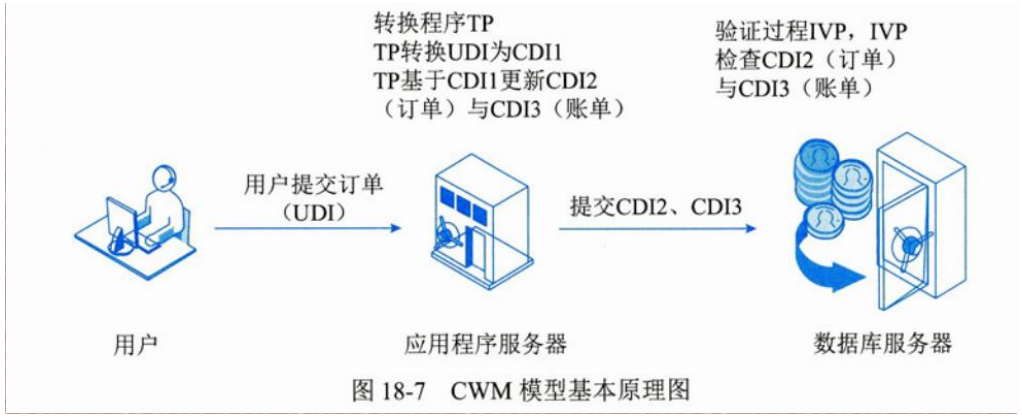


图 18-7　CWM 模型基本原理图

安全模型-Chinese Wall模型

◆ Chinese Wall模型(又名Brew and Nash模型)是应用在多边安全系统中的安全模型。也就是说，是指通过行政规定和划分、内部监控、IT系统等手段防止各部门之间出现有损客户利益的利益冲突事件。（★★★）

◆ Chinese Wall模型的安全策略的基础是客户访问的信息不会与当前他们可支配的信息产生冲突。在投资银行中，一个银行会同时拥有多个互为竞争者的客户，一个银行家可能为一个客户工作，但他可以访问所有客户的信息。因此，应当制止该银行家访问其他客户的数据。银行家可以选择为谁工作(DAC)，一旦选定，他就只能为该客户工作(MAC)。

◆Chinese Wall模型的访问客体控制的安全规则如下：（★★★）
(1）与主体曾经访问过的信息属于同一公司数据集合的信息，即墙内信息可以访问；
(2）属于一个完全不同的利益冲突组的可以访问；
(3）主体能够对一个客体进行写的前提是主体未对任何属于其他公司数据集进行过访问。
定理1：一个主体一旦访问过一个客体，则该主体只能访问位于同一公司数据集的客体或在不同利益组的客体。
定理2：在一个利益冲突组中，一个主体最多只能访问一个公司数据集。

典型真题

BLP模型是（）模型。
A.机密性
B.完整性
C.可用性
D.真实性
参考答案：A

目录

安全技术体系架构

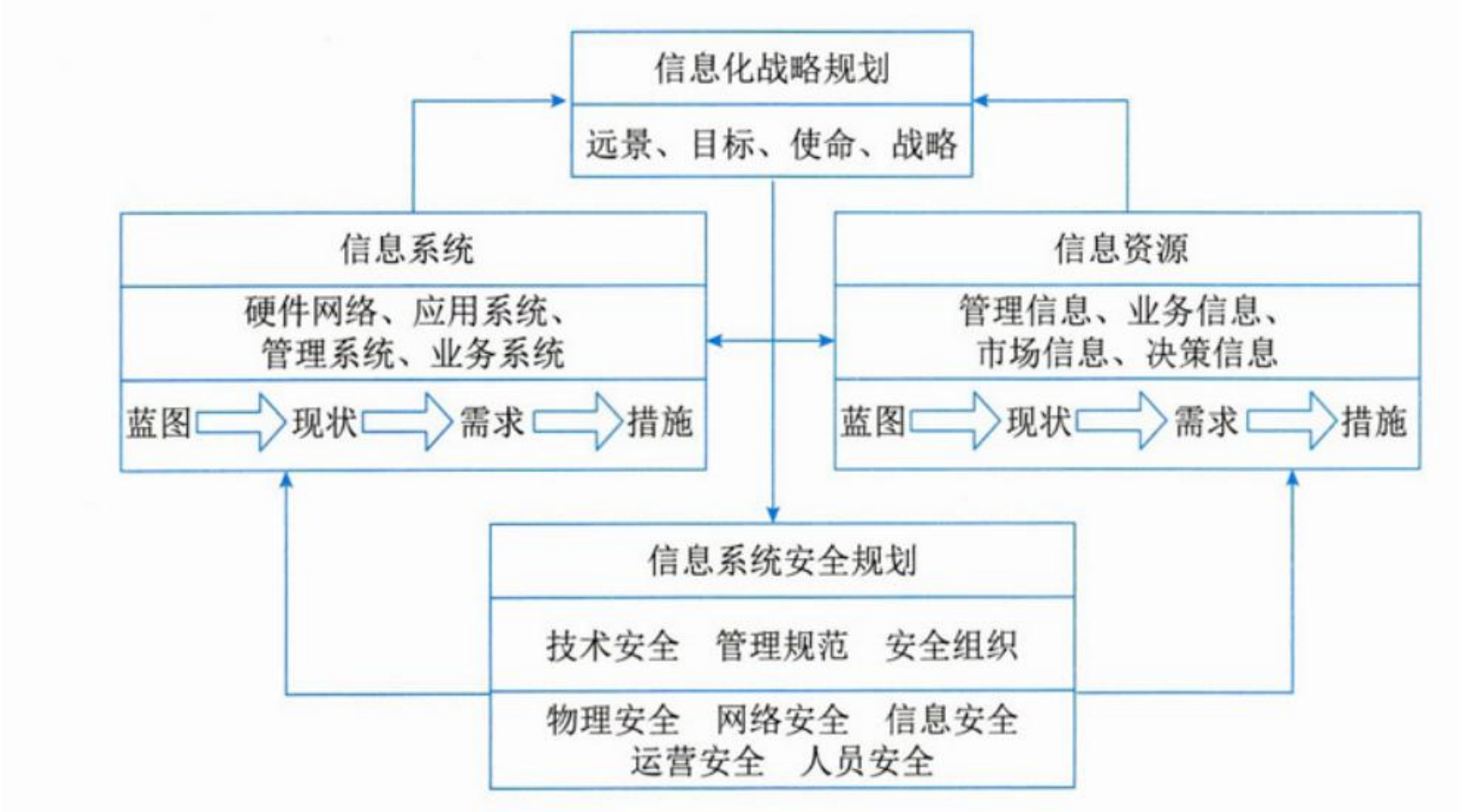
◆安全技术体系架构是对组织机构信息技术系统的安全体系结构的整体描述。安全技术体系架构的目标是建立可持续改进的安全技术体系架构的能力。

◆根据网络中风险威胁的存在实体划分出5个层次的实体对象：应用、存储、主机、网络和物理。

◆信息系统安全体系主要是由技术体系、组织机构体系和管理体系三部分共同构成的。（★★）
1）技术体系是全面提供信息系统安全保护的技术保障系统，该体系由物理安全技术和系统安全技术两大类构成。
2）组织体系是信息系统的组织保障系统，由机构、岗位和人事三个模块构成。
3）管理体系由法律管理、制度管理和培训管理三部分组成。

信息系统安全规划框架

◆**信息系统安全规划框架**



信息系统安全规划框架

1.信息系统安全规划依托企业信息化战略规划
◆信息系统安全规划的目标应该与企业信息化的目标是一致的，而且应该比企业信息化的目标更具体明确、更贴近安全。

2.信息系统安全规划需要围绕技术安全、管理安全、组织安全考虑
◆规划的内容基本上应涵盖：确定信息系统安全的任务、目标、战略以及战略部门和战略人员，并在此基础上制定出物理安全、网络安全、系统安全、运营安全、人员安全的信息系统安全的总体规划。

3.信息系统安全规划以信息系统与信息资源的安全保护为核心（★）
◆规划工作需要围绕着信息系统与信息资源的开发、利用和保护工作进行，要包括蓝图、现状、需求和措施4个方面。
(1)对信息系统与信息资源的规划需要从信息化建设的蓝图入手，知道企业信息化发展策略的总体目标和各阶段的实施目标，制定出信息系统安全的发展目标。
(2)对企业的信息化工作现状进行整体的、综合、全面的分析，找出过去工作中的优势与不足。
(3)根据信息化建设的目标提出未来几年的需求，这个需求最好可以分解成若干个小的方面，以便于今后的实施与落实。
(4)要明确在实施工作阶段的具体措施与方法，提高规划工作的执行力度。

典型真题

◆信息系统安全体系主要是由技术体系、（）和管理体系三部分共同构成的
A.组织结构体系
B.管理方法
C.可靠性
D.组织战略
参考答案：A

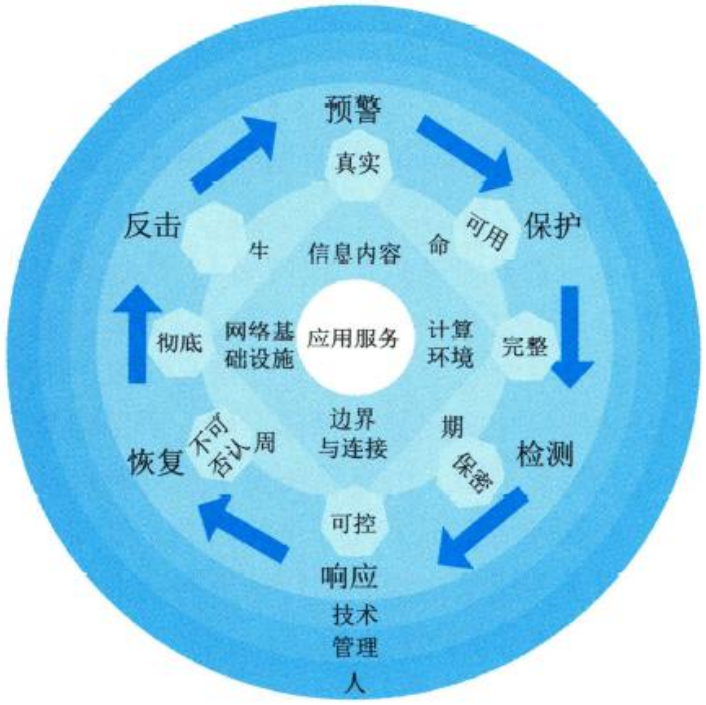
目录

WPDRRC模型

◆ WPDRRC(Waring/Protect/Detect/React/Restore/Counterattack)模型有6个环节和3大要素。（★★★）

◆ 6个环节包括：预警、保护、检测、响应、恢复和反击，它们具有较强的时序性和动态性，能够较好地反映出信息系统安全保障体系的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力。

◆ 3大要素包括：人员、策略和技术。人员是核心，策略是桥梁，技术是保证，落实在WPDRRC 的6个环节的各个方面，将安全策预警略变为安全现实。



WPDRRC模型

环节	解释
W.预警	利用远程安全评估系统提供的模拟攻击技术来检查系统存在的、可能被利用的薄弱环节，收集和测试网络与信息的安全风险所在，并以直观的方式进行报告，提供解决方案的建议，在经过分析后，分解网络的风险变化趋势和严重风险点，从而有效降低网络的总体风险，保护关键业务和数据。
P 防护	通过采用成熟的信息安全技术及方法来实现网络与信息的安全。主要内容有加密机制，数字签名机制，访问控制机制，认证机制，信息隐藏和防火墙技术等。
D 检测	通过检测和监控网络以及系统，来发现新的威胁和弱点，强制执行安全策略。 在这个过程中采用入侵检测、恶意代码过滤等技术，形成动态检测的制度，奖励报告协调机制，提高检测的实时性。主要内容有入侵检测，系统脆弱性检测，数据完整性检测和攻击性检测等。
R 响应	指在检测到安全漏洞和安全事件之后必须及时做出正确的响应，从而把系统调整到安全状态。为此需要相应的报警、跟踪、处理系统，其中处理包括了封堵、隔离、报告等能力。主要内容有应急策略、应急机制、应急手段、入侵过程分析和安全状态评估等。
R 恢复	当前网络、数据、服务受到黑客攻击并遭到破坏或影响后，通过必要技术手段，在尽可能短的时间内使系统恢复正常。主要内容有容错、冗余、备份、替换、修复和恢复等。
C 反击	是指采用一切可能的高新技术手段，侦察、提取计算机犯罪分子的作案线索与犯罪证据，形成强有力的取证能力和依法打击手段。

WPDRRC模型

网络安全体系模型经过多年发展，形成了PDP 、 PPDR、 PDRR、 MPDRR和WPDRRC 等模型，这些模型在信息安全防范方面功能更加完善

	预警	保护	检测	响应	恢复	反击	管理
PDR	无	有	有	有	无	无	无
PPDR	无	有	有	有	无	无	无
PDRR	无	有	有	有	有	无	无
MPDRR	无	有	有	有	有	无	有
WPDRRC	有	有	有	有	有	有	有

信息系统安全架构设计

◆信息系统安全设计重点考虑两个方面；其一是系统安全保障体系；其二是信息安全体系架构。（★）

1.系统安全保障体系：是由安全服务、协议层次和系统单元等三个层面组成，且每个层都涵盖了安全管理的内容。系统安全保障体系设计工作主要考虑以下几点：

(1)安全区域策略的确定：根据安全区域的划分，主管部门应制定针对性的安全策略。

(2)统一配置和管理防病毒系统：主管部门应当建立整体防御策略，以实现统一的配置和管理。

(3)网络安全管理：加强网络安全管理，制定有关规章制度。

2.信息安全体系架构：具体在安全控制系统，我们可以从下面5个方面开展分析和设计工作。（★★）

1)物理安全：保证计算机信息系统各种设备的物理安全是保障整个网络系统安全的前提。包括：环境安全、设备安全、媒体安全等。

2)系统安全：主要是指对信息系统组成中各个部件的安全要求。系统安全是系统整体安全的基础。它主要包括：网络结构安全、操作系统安全和应用系统安全。

3)网络安全：是整个安全解决方案的关键。它主要包括：访问控制、通信保密、入侵检测、网络安全扫描系统和防病毒等。

4)应用安全：主要是指多个用户使用网络系统时，对共享资源和信息存储操作所带来的安全问题。它主要包括资源共享和信息存储两个方面。

5)安全管理：主要体现在三个方面。其一是制定健全的安全管理体制；其二是构建安全管理平台；其三是增强人员的安全防范意识。

典型真题

（）是通过检测和监控网络以及系统，来发现新的威胁和弱点，强制执行安全策略。 在这个过程中采用入侵检测、恶意代码过滤等技术，形成动态检测的制度，奖励报告协调机制，提高检测的实时性。

A.预警

B.防护

C.检测

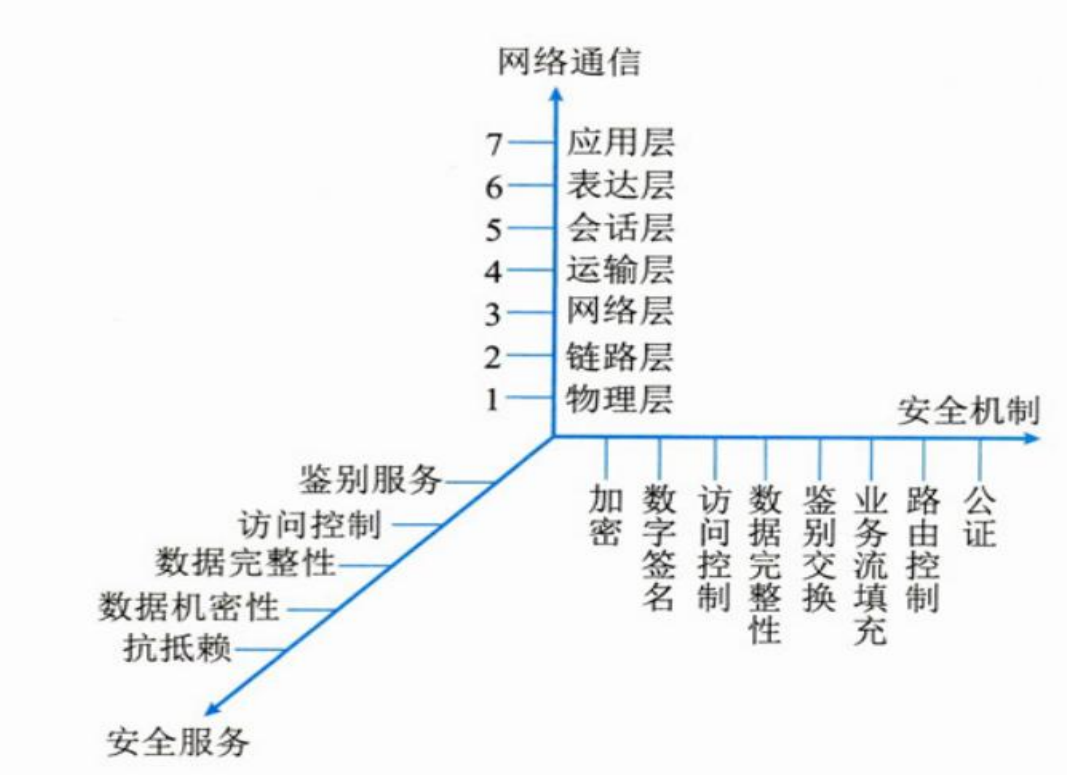
D.响应

参考答案：C

目录

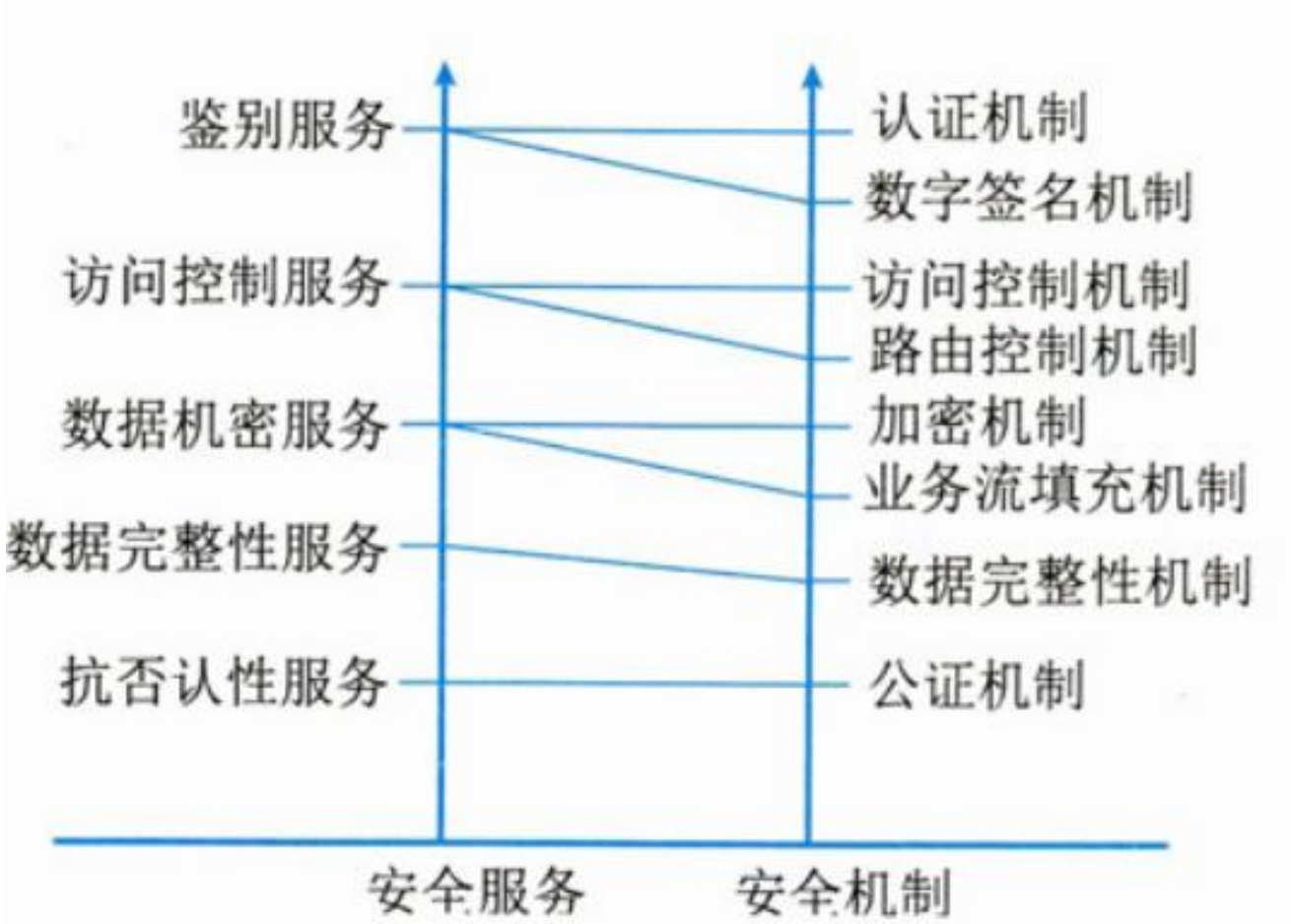
OSI的安全体系架构概述

◆ OSI 定义了7层协议，其中除第5层(会话层)外，每一层均能提供相应的安全服务。实际上，最适合配置安全服务的是在物理层、网络层、运输层及应用层上，其他层都不宜配置安全服务。
◆ OSI 开放系统互联安全体系的5类安全服务包括鉴别、访问控制、数据机密性、数据完整性和抗抵赖性。
◆信息安全体系结构示意图（★★）



OSI的安全体系架构概述

◆安全服务和安全机制的对应关系



OSI的安全体系架构概述

◆ OSI 定义分层多点安全技术体系架构，也称为深度防御安全技术体系架构，它通过以下三种方式将防御能力分布至整个信息系统中。（★）

1)多点技术防御：在对手可以从内部或外部多点攻击一个目标的前提下，多点技术防御通过对网络和基础设施、边界、计算环境这三个防御核心区域的防御达到抵御所有方式的攻击目的。

2)分层技术防御：即使最好的可得到的信息保障产品也有弱点，其最终结果将使对手能找到一个可探查的脆弱性，一个有效的措施是在对手和目标间使用多个防御机制。

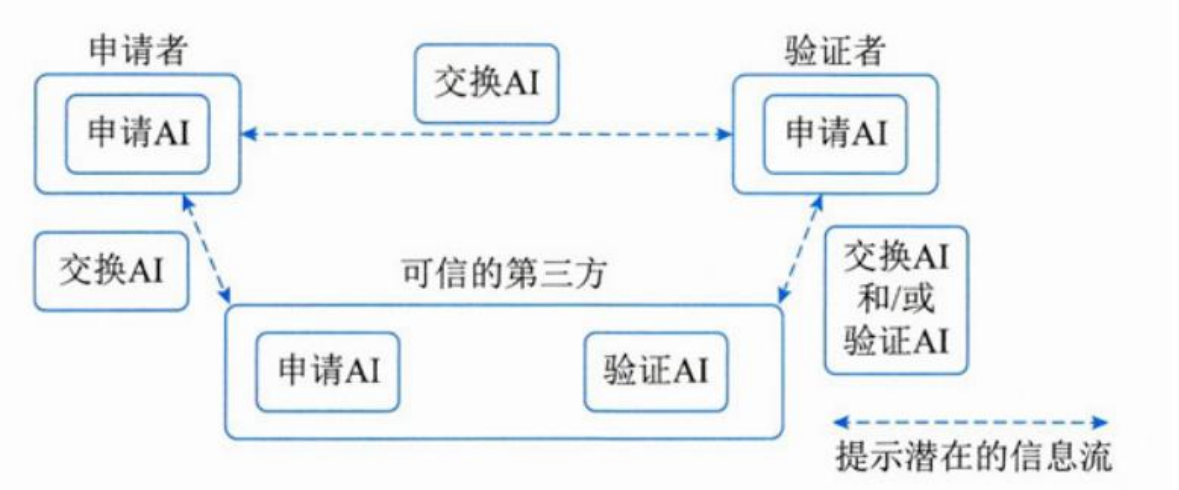
3)支撑性基础设施：为网络、边界和计算环境中信息保障机制运行基础的支撑性基础设施，包括公钥基础设施以及检测和响应基础设施。

认证框架

◆鉴别（Authentication ）的基本目的是防止其他实体占用和独立操作被鉴别实体的身份。鉴别信息是指申请者要求鉴别到鉴别过程结束所生成、使用和交换的信息。

◆鉴别信息的类型有交换鉴别信息、申请鉴别信息和验证鉴别信息。（★★）

◆鉴别的方式主要基于以下5 种。
(1 ）己知的，如一个秘密的口令。
(2 ）拥有的，如IC 卡、令牌等。
(3 ）不改变的特性，如生物特征。
(4 ）相信可靠的第三方建立的鉴别（递推）。
(5 ）环境（如主机地址等）。

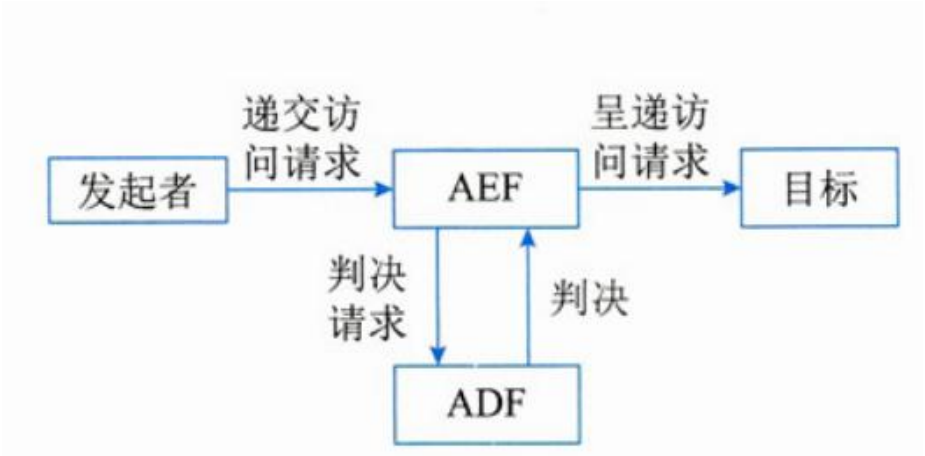


访问控制框架

访问控制框架（★★）

◆访问控制（Access Control）决定开放系统环境中允许使用哪些资源、在什么地方适合阻止未授权访问的过程。在访问控制实例中，访问可以是对一个系统（即对一个系统通信部分的一个实体）或对一个系统内部进行的。

◆ACI（访问控制信息）是用于访问控制目的的任何信息，其中包括上下文信息。
ADI （访 问控制判决信息）是在做出一个特定的访问控制判决时可供ADF 使用的部分（或全部）ACI.
ADF （访问控制判决功能）是一种特定功能，它通过对访问请求、ADI以及该访问请求的上下文使用访问控制策略规则而做出访问控制判决。AEF （访问控制实施功能）确保只有对目标允许的访问才由发起者执行。



机密性、完整性、抗抵赖框架

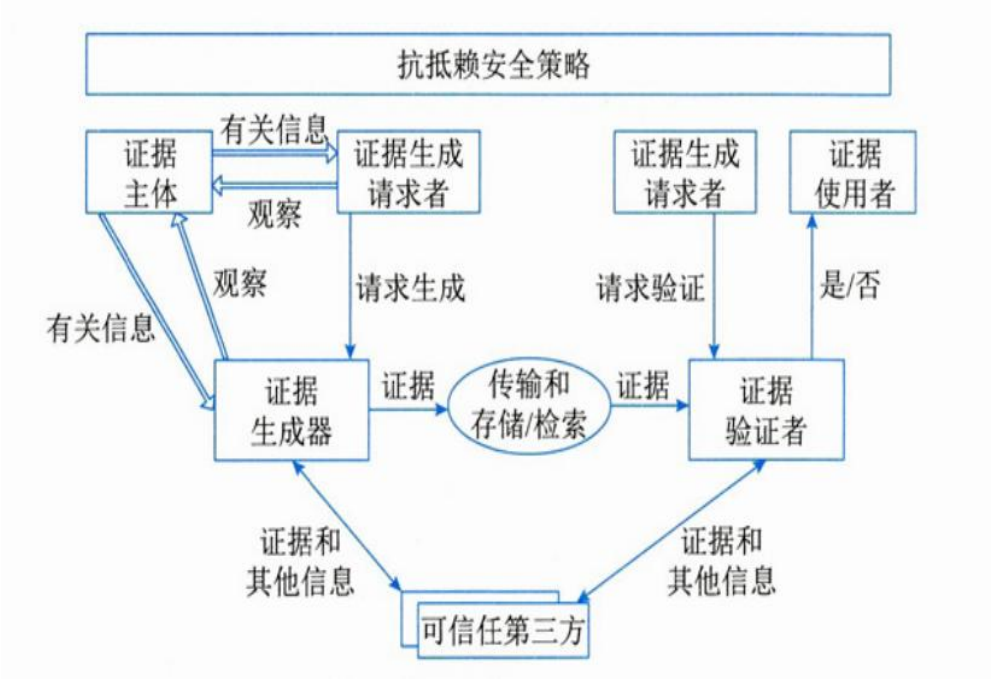
◆机密性框架（★★）
机密性服务的目的是确保信息仅仅是对被授权者可用。
1）通过禁止访问提供机密性
2）通过加密提供机密性

◆完整性框架（★★）
完整性框架的目的是通过阻止威胁或探测威胁，保护可能遭到不同方式危害的数据完整性和数据相关属性完整性。
(1）阻止对媒体访问的机制。包括物理隔离的不受干扰的信道、路由控制、访问控制。
(2）用以探测对数据或数据项序列的非授权修改的机制。

◆抗抵赖服务包括证据的生成、验证和记录，以及在解决纠纷时随即进行的证据恢复和再次验证。（★★）
抗抵赖由4 个独立的阶段组成：证据生成；证据传输、存储及恢复；证据验证和解决纠纷。

机密性、完整性、抗抵赖框架

1）证据生成
在这个阶段中，证据生成请求者请求证据生成者为事件或行为生成证据。卷入事件或行为 中的实体，称为证据实体，其卷入关系由证据建立。根据抗抵赖服务的类型，证据可由证据实 体，或可能与可信第三方的服务一起生成，或者单独由可信第三方生成。
2）证据传输、存储及恢复 在这个阶段，证据在实体间传输或从存储器取出来或传到存储器。
3）证据验证
在这个阶段，证据在证据使用者的请求下被证据验证者验证。本阶段的目的是在出现纠纷 的事件中，让证据使用者确信被提供的证据确实是充分的。可信第三方服务也可参与，以提供 验证该证据的信息。
4）解决纠纷
在解决纠纷阶段，仲裁者有解决双方纠纷的责任。



目录

数据库系统安全设计

◆数据库完整性是指数据库中数据的正确性和相容性。数据库完整性由各种各样的完整性约束来保证，因此可以说数据库完整性设计就是数据库完整性约束的设计。数据库完整性约束可以通过DBMS或应用程序来实现，基于DBMS的完整性约束作为模式的一部分存入数据库中。

◆在实施数据库完整性设计时，需要把握以下基本原则：（★）
(1)根据数据库完整性约束的类型确定其实现的系统层次和方式，并提前考虑对系统性能的影响。一般情况下，静态约束应尽量包含在数据库模式中，而动态约束由应用程序实现。
(2)实体完整性约束、引用完整性约束是关系数据库最重要的完整性约束，在不影响系统关键性能的前提下需尽量应用。用一定的时间和空间来换取系统的易用性是值得的。
(3)要慎用目前主流DBMS都支持的触发器功能，一方面由于触发器的性能开销较大；另一方面，触发器的多级触发难以控制，容易发生错误，非用不可时，最好使用Before型语句级触发器。
(4)在需求分析阶段就必须制定完整性约束的命名规范，尽量使用有意义的英文单词、缩写词、表名、列名及下画线等组合，使其易于识别和记忆。
(5)要根据业务规则对数据库完整性进行细致的测试，以尽早排除隐含的完整性约束间的冲突和对性能的影响。
(6)要有专职的数据库设计小组，自始至终负责数据库的分析、设计、测试、实施及早期维护。
(7)应采用合适的CASE工具来降低数据库设计各阶段的工作量。

数据库系统安全设计

◆数据库完整性的作用：
(1)数据库完整性约束能够防止合法用户使用数据库时向数据库中添加不合语义的数据。
(2)利用基于DBMS的完整性控制机制来实现业务规则，易于定义，容易理解，而且可以降低应用程序的复杂性，提高应用程序的运行效率。
(3)合理的数据库完整性设计，能够同时兼顾数据库的完整性和系统的效能。
(4)在应用软件的功能测试中，完善的数据库完整性有助于尽早发现应用软件的错误。
(5)数据库完整性约束可分为6类：列级静态约束、元组级静态约束、关系级静态约束、列级动态约束、元组级动态约束和关系级动态约束。

◆一个好的数据库完整性设计（★）
首先需要在需求分析阶段确定要通过数据库完整性约束实现的业务规则。
然后在充分了解特定DBMS提供的完整性控制机制的基础上，依据整个系统的体系结构和性能要求，遵照数据库设计方法和应用软件设计方法，合理选择每个业务规则的实现方式。
最后，认真测试，排除隐含的约束冲突和性能问题。

目录

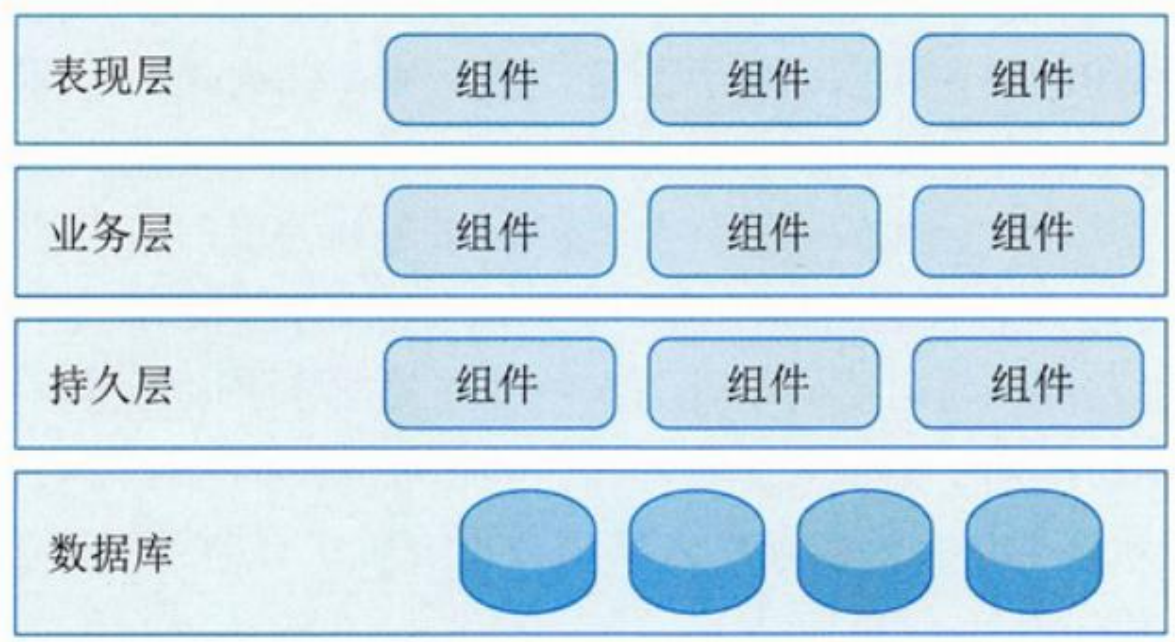
系统架构的脆弱性分析

◆典型软件架构的脆弱性分析（★★）

1.分层架构的脆弱性主要表现在两个方面：

(1)层间的脆弱性。一旦某个底层发生错误，那么整个程序将会无法正常运行。

(2)层间通信的脆弱性。将系统隔离为多个相对独立的层，这就要求在层与层之间引入通信机制。本来“直来直去”的操作现在要层层传递，势必造成性能下降。



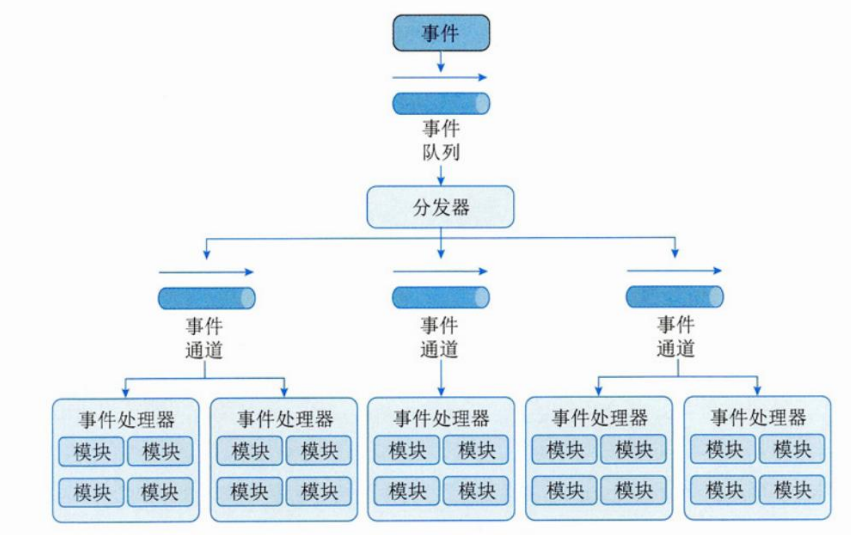
系统架构的脆弱性分析

2.C/S 架构的脆弱性主要表现在以下几个方面：（★★）
(1)客户端软件的脆弱性。因为在用户计算机上安装了客户端软件，所以这个系统就面临着程序被分析、数据被截取的安全隐患。
(2)网络开放性的脆弱性。目前很多传统的C/S 系统还是采用二层结构，也就是说所有客户端直接读取服务器端中的数据，在客户端包括了数据的用户名，密码等致命的信息，这样会给系统带来安全隐患。
(3)网络协议的脆弱性。C/S架构不便于随时与用户交流(主要是不便于数据包共享),并且C/S 架构软件在保护数据的安全性方面有着先天的弊端。由于C/S 架构软件的数据分布特性，客户端所发生的火灾、盗抢、地震、病毒等都将成为可怕的数据杀手。

3.B/S 架构的脆弱性主要表现在：系统如果使用HTTP 协议， B/S架构相对C/S 架构而言更容易被病毒入侵，虽然最新的H T T P协议在安全性方面有所提升，但还是弱于C/S。（★★）

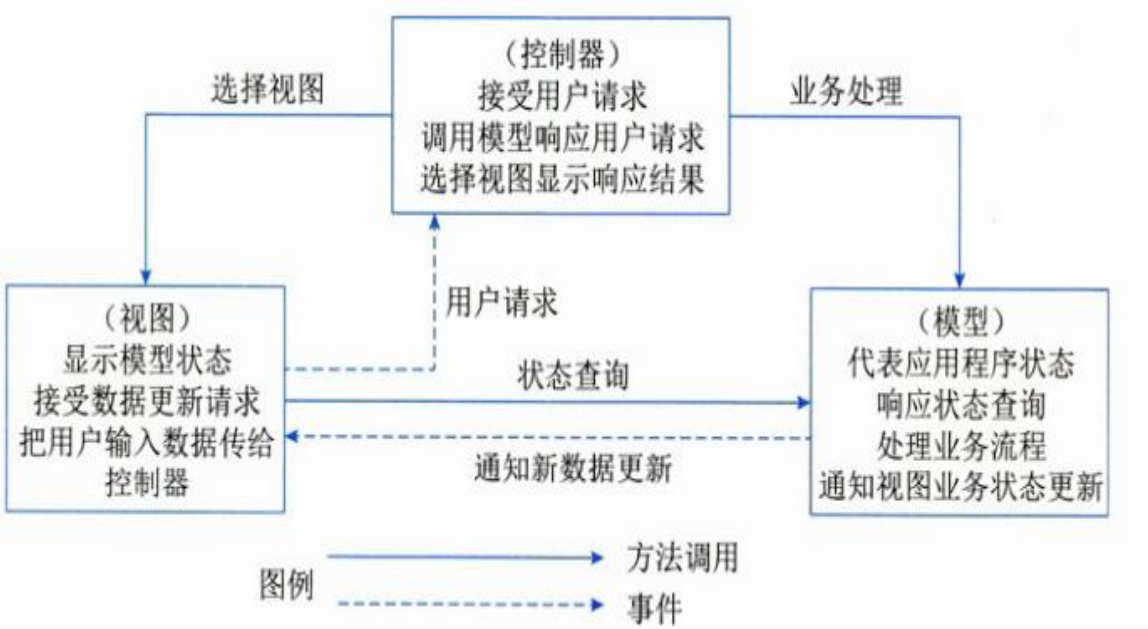
系统架构的脆弱性分析

4.事件驱动架构的脆弱性主要表现在：（★★）
(1)组件的脆弱性。组件削弱了自身对系统的控制能力，一个组件触发事件，并不能确定响应该事件的其他组件及各组建的执行顺序。
(2)组件间交换数据的脆弱性。组件不能很好地解决数据交换问题，事件触发时，一个组件有可能需要将参数传递给另一个组件，而数据量很大的时候，如何有效传递是一个脆弱性问题。
(3)组件间逻辑关系的脆弱性。事件架构使系统中各组件的逻辑关系变得更加复杂。
(4)事件驱动容易进入死循环，这是由编程逻辑决定的。
(5)高并发的脆弱性。虽然事件驱动可实现有效利用C P U 资源，但是存在高并发事件处理造成的系统响应问题，而且，高并发容易导致系统数据不正确、丢失数据等现象。
(6)固定流程的脆弱性。因为事件驱动的可响应流程基本都是固定的，如果操作不当，容易引发安全问题。



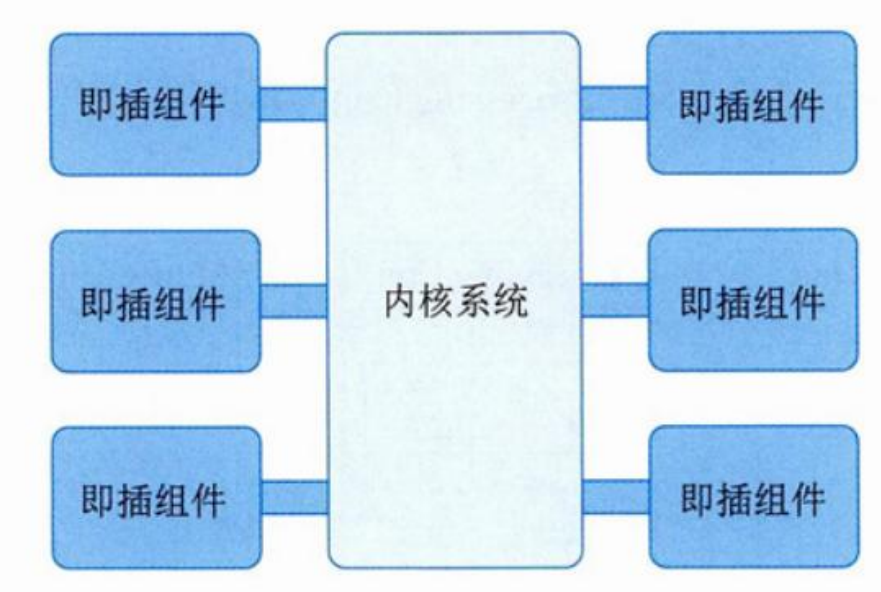
系统架构的脆弱性分析

5.M V C架构的脆弱性主要表现在：（★★）
(1) M V C架构的复杂性带来脆弱性。M V C架构增加了系统结构和实现的复杂性。比如说一个简单的界面，如果严格遵循M V C方式，使得模型、视图与控制器分离，会增加结构的复杂性，并可能产生过多的更新操作，降低运行效率。
(2)视图与控制器间紧密连接的脆弱性。视图与控制器是相互分离但确是联系紧密的部件，没有控制器的存在，视图应用是很有限的。反之亦然，这样就妨碍了它们的独立重用。
(3)视图对模型数据的低效率访问的脆弱性。依据模型操作接口的不同，视图可能需要多次调用才能获得足够的显示数据。对未变化数据的不必要的频繁访问也将损害操作性能。



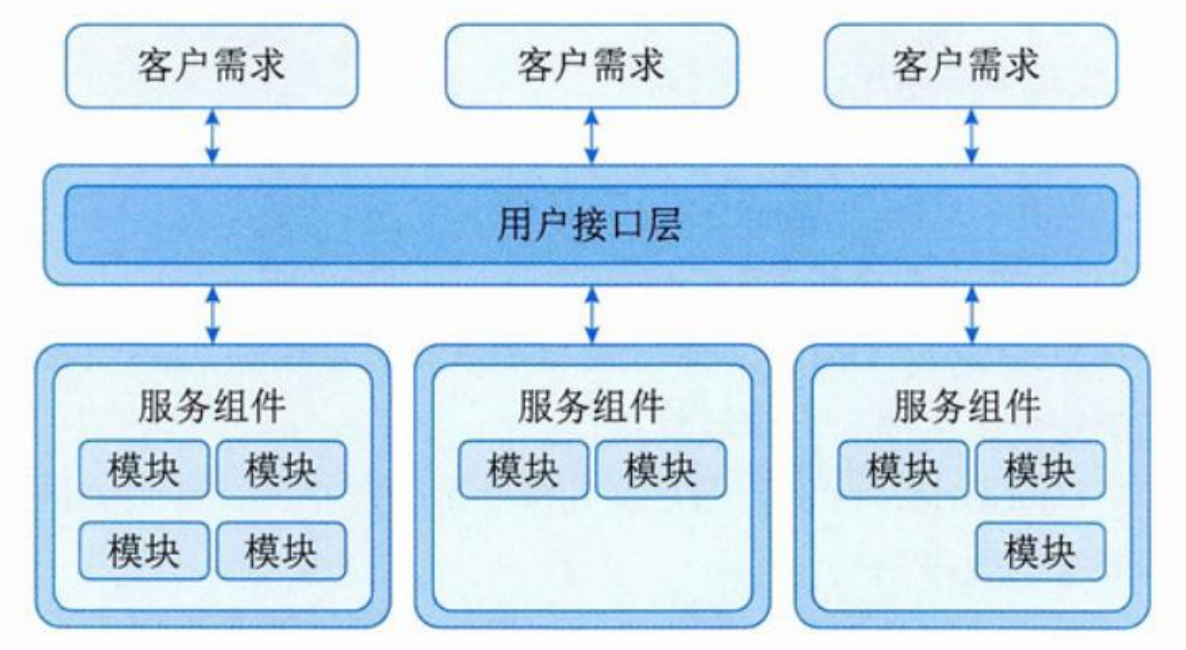
系统架构的脆弱性分析

6.微内核架构的脆弱性主要表现在：（★★）
(1)微内核架构难以进行良好的整体化优化。由于微内核系统的核心态只实现了最基本的系统操作，这样内核以外的外部程序之间的独立运行使得系统难以进行良好的整体优化。
(2)微内核系统的进程间通信开销也较单一内核系统要大得多。从整体上看，在当前硬件条件下，微内核在效率上的损失小于其在结构上获得的收益。
(3)通信损失率高。微内核把系统分为各个小的功能块，从而降低了设计难度，系统的维护与修改也容易，但通信带来的效率损失是一个问题。



系统架构的脆弱性分析

7.微服务架构的脆弱性主要表现在：（★★）
(1)开发人员需要处理分布式系统的复杂结构。
(2)开发人员要设计服务之间的通信机制，通过写代码来处理消息传递中速度过慢或者不可用等局部实效问题。
(3)服务管理的复杂性，在生产环境中要管理多个不同的服务实例，这意味着开发团队需要全局统筹。



目录

安全架构设计案例分析1

◆RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）。是应用最广泛的高安全级别 AAA 协议（认证 Authentication、授权 Authorization、审计 Accounting况），具有高性能和高可扩展性，且可用多种协议实现。

◆RADIUS 通常由协议逻辑层，业务逻辑层和数据逻辑层三层组成层次式架构。

（1）协议逻辑层：起到分发处理功能，相当于转发引擎。

（2）业务逻辑层：实现认证、计费、授权三种类型业务及其服务进程间的通信。

（3）数据逻辑层：实现统一的数据访问代理池，降低数据库依赖，减少数据库压力，增强系统的数据库适应能力。

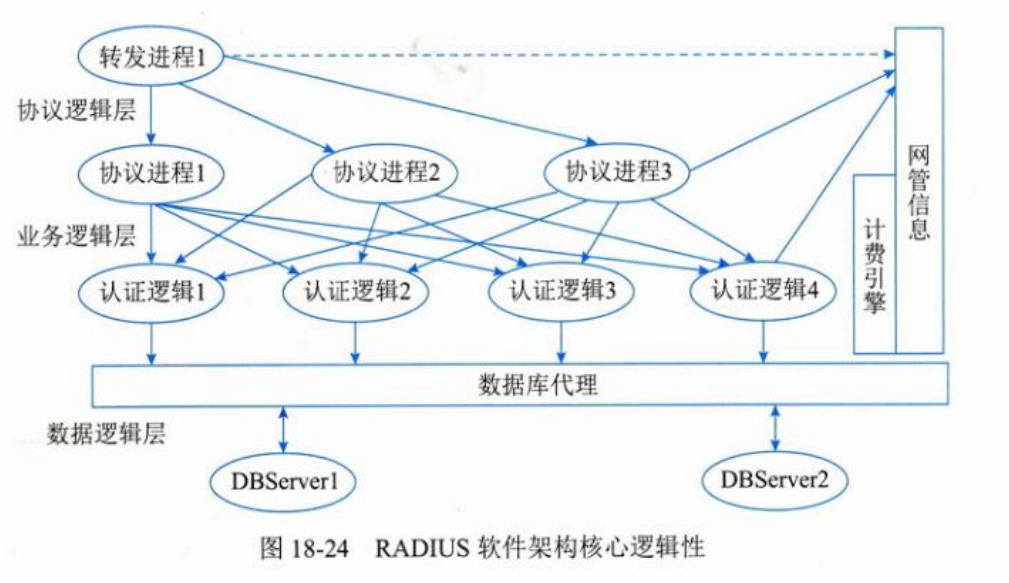


图 18-24　RADIUS 软件架构核心逻辑性

安全架构设计案例分析2

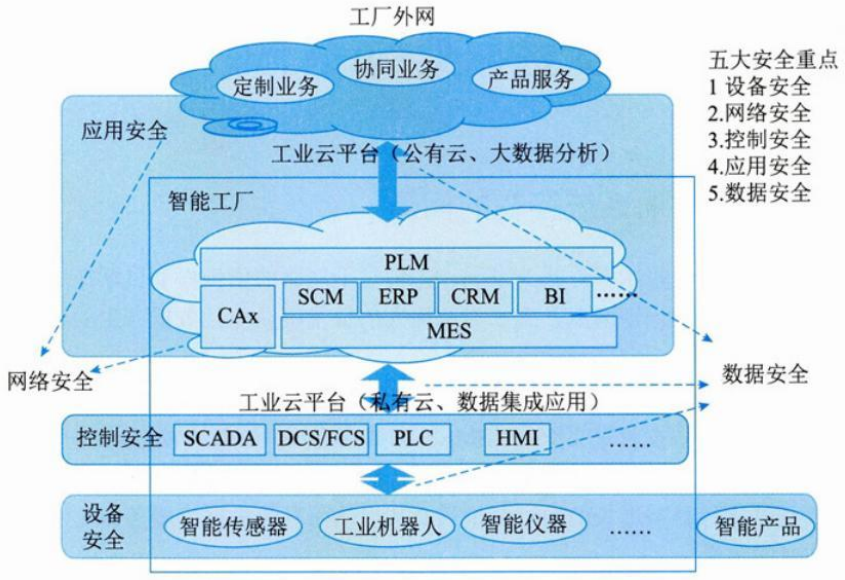
◆基于混合云的工业安全生产管理系统。混合云融合了公有云和私有云。在基于混合云的工业安全生产管理系统中，工厂内部的产品设计、数据共享、生产集成使用私有云实现。公有云则用于工厂间与公司总部与智能工厂间的业务管理、协调和统计分析等。整个生产管理系统架构采用层次式架构，分为设备层、控制层、设计/管理层、应用层。

（1）设备层：包括智能工厂生产用设备，包括智能传感器，智能仪器仪表，工业机器人，其他生产设备。

（2）控制层：包括智能设备控制用自动控制系统，包括采集与监视控制系统 SCADA，分布式控制系统 DCS，现场总线控制系统 FCS，可编程控制器 PLC（内置编程程序），人机接口 HMI，其他现场控制程序。

（3）设计/管理层：包括智能工厂所有控制开发，业务控制和数据管理相关系统及其功能的集合，实现了数据集成和应用，包括制造执行系统 MES（很多企业称之为生产信息管理系统），计算机辅助设计/工程/制造 CAD/CAE/CAM，供应链管理 SCM，企业资源规划 ERP，客户关系管理 CRM，供应商关系管理 SRM，商业智能分析 BI，产品生命周期管理 PLM。

（4）应用层：云平台上的信息处理，包括数据处理与管理、数据与行业应用相结合，如定制业务、协同业务、产品服务。



本章重点回顾

1、安全威胁
2、安全模型
3、安全框架

THANKS