CC标准浅析

张耀疆，CISSP
colababy@263.net.cn

- 信息安全标准化概述
- CC标准简介
- CC标准中的关键概念
- CC的核心内容和组织结构
- 安全评估
- 通用评估方法（CEM）
- 总结和展望

以Internet为代表的信息化网络化进程，日益深刻地渗透到政府、企业、团体、军队、家庭、个人等社会和经济生活的各个角落，并日益深刻地改变着人们传统的工作模式、商业模式、管理模式和生活模式。

与Internet全面应用和信息化全面发展相伴随的一个更重大的问题是信息安全问题。对信息安全问题，特别是我国的信息安全问题，目前最急需的就是建立国家信息安全标准体系，全面推动国家信息安全技术标准化建设，为国家信息化进程中的信息安全问题提供技术依据。

无规矩不成方圆

信息安全标准概述

重要的标准化组织（1）

- 国际标准化组织（ISO）
  - ISO/IDC JTC1/SC27负责通用信息技术安全标准的制定
  - ISO/TC68负责银行和金融服务业务应用范围内信息安全标准的制定
- 国际电工委员会（IEC）
  - 世界上最早的国际性电工标准化机构，负责有关电工、电子领域的国际标准化工作。在信息安全技术标准化方面，除了同ISO联合成立的JTC1下属几个分委员会外，还在电磁兼容等方面成立技术委员会，并制定相关国际标准
- 国际电信联盟（ITU）
  - 前身是CCITT，单独或与ISO 合作开发诸如消息处理系统、目录系统（X.400系列、X.500系列）和安全框架、安全模型等标准
- Internet工程任务组（IETF）
  - IETF主要提出Internet标准草案和称为“请提意见”RFC“的协议文稿，内容广泛，也包括安全方面的建议稿，经过网上讨论修改，被大家接受的就成了事实上的标准

信息安全标准概述

重要的标准化组织（2）

- 欧洲计算机厂商协会（ECMA）
  - 制定计算机及其相关应用的标准和技术报告，经常向ISO提交标准提案。目前制定了商用和政府用信息技术产品和系统安全性评估标准化框架，还制定了在开放系统环境下逻辑安全设备的框架
- 美国国家标准协会（ANSI）
  - 于80年代初开始数据加密标准化工作，只制定了三个通用的国家标准
- 美国联邦信息处理安全标准（FIPS）
  - FIPS由美国国家标准技术研究所（NIST）颁发。FIPS由NIST在广泛搜集政府各部门及私人部门的意见的基础上写成，由商业部长签字划押同意或反对这个标准。数据加密标准（DES）就是一例
- 美国电气电工工程师协会（IEEE）
  - IEEE在信息安全方面主要是提出LAN/WAN安全方面的标准（SILS）和公钥密码标准（P1363）
- 美国国防部的信息安全指令和标准（DODDI）
  - 美国国防部发布了一些有关信息安全和自动信息系统安全的指令、指示和标准，并加强信息安全的管理，特别是DOD 5200.28-STD《国防可信和计算机系统评估准则》，受到广泛的关注

信息安全标准概述

我国的信息安全标准体系

- **基础类标准**
  - 信息技术安全术语，信息技术安全体系结构，信息技术安全框架（GB9387-2，等同采用ISO7498-2），信息技术安全模型
- **技术机制类标准**
  - 加密，签名，完整性，鉴别，访问控制，抗抵赖，路由选择控制，通信业务填充，公证，可信功能度，事件检测和报警，安全审计跟踪，安全标记，安全恢复
- **应用类标准**
  - 物理环境和保障、信息处理、传输和存储、计算机病毒防治等应用基础
  - 商用密码、防火墙、应用代理、安全路由器等应用产品
  - 电子商务、电子政务、涉秘系统、金融处理等应用系统
  - 金融服务等特殊行业的安全标准
- **安全管理类标准**
  - 管理基础，系统管理，测评认证（GB17859等）

信息安全标准概述

一些重要的信息安全标准

- ISO7498-2（GB/T9387-2,1995）
  - 1989年ISO组织制定的《信息处理系统 开放系统互连 基本参考模型 第2部分 安全体系结构》，该标准对安全服务及相关机制进行了一般描述
- CC（ISO15408，GB/T18336,2001）
  - 1993年6月，美国、加拿大及欧洲四国共同协商并起草通过了CC标准，其目的是建立一个各国都能接受的通用的信息安全产品和系统的安全性评价标准
- SSE-CMM（ISO/IEC DIS 21827）
  - 美国国家安全局（NSA）于1993年提出的专门用于系统安全工程的能力成熟度模型构想
- IATF
  - NSA制定的Information Assurance Technical Framework，为保护美国政府和工业界的信息与信息技术设施提供技术指南
- BS7799（Part1：ISO17799）
  - BSI制定的关于信息安全管理的标准，分两个部分，定义了如何实施ISMS
- ISO/IEC TR 13335
  - 即IT安全管理指南（GMITS），分5个部分。是信息安全管理方面的指导性标准

信息安全技术测评标准

- **可信计算机系统评估标准**
  - Trusted Computer System Evaluation Criteria，TCSEC，即“桔皮书”
  - U.S. Department of Defense 5200.28-STD（1985）
- **可信网络解释**
  - Trusted Network Interpretation，TNI，即“红皮书”（1987）
- **信息技术安全评估标准**
  - Information Technology Security Evaluation Criteria，ITSEC
  - 西欧四国（英、法、荷、德），欧洲白皮书（1991年）
- **加拿大可信计算机产品评估标准**
  - Canadian Trusted Computer Product Evaluation Criteria，CTCPEC（1993）
- **美国联邦标准**
  - Federal Criteria，FC（1993）
- **通用标准**
  - Common Criteria，CC。Version 2 (Finalized 1998), ISO 15408

TCSEC简介

- 1985年美国国防部制定，是彩虹系列之一，即桔皮书；
- 主要用作军事领域，后沿用至民用，针对的是保密性；
- 使用了可信计算基础（Trusted Computing Base，TCB）的概念，这是一种实现安全策略的机制，包括硬件、固件和软件，它们根据安全策略处理主体对客体的访问，具有抗篡改的性质和易于分析和测试的机构；
- 定义了系统安全的4个方面：安全策略、可追溯性、安全保障和文档，并将这4个方面分成7个安全等级：D、C1、C2、B1、B2、B3和A级；
- 在TCSEC的评价准则中，从B级开始就要求具有强制访问控制和形式化模型技术的应用（Bell & LaPadula 保密模型）；
- 桔皮书论述的重点是通用的操作系统，为了使其评判方法适用于网络，NCSC于1987年出版了一系列有关可信计算机数据库、可信计算机网络等的指南（俗称彩虹系列）。

TCSEC安全等级

- **D级 —— 最低保护（Minimal Protection）**
  - 未加任何实际的安全措施，不要求进行用户登陆和密码保护，整个系统是不可信的，硬件和软件都容易被侵袭。本地操作系统，或一个完全没有保护的网络。DOS，Windows3x，Windows9x
- **C级 —— 被动的自主访问策略（Discretionary Access Policy Enforced）**
  - 提供谨慎的保护，并为用户的行为和走人提供审计能力，包括C1和C2两级
  - **C1级** —— 自主安全保护级。将用户和数据分开，用户登录需认证，所有文档具有相同机密性
  - **C2级** —— 受控访问控制保护级。引入审计机制，引入受控访问环境（用户权限级别），通过登录过程、安全时间和资源隔离来增强控制。Unix，WindowsNT，Novell3.x以上版本
- **B级 —— 被动的强制访问策略（Mandatory Access Policy Enforced）**
  - **B1级** —— 标记安全保护级。对网络上每个对象实施保护，支持多级安全
  - **B2级** —— 结构化保护级。系统的TCB是基于明确定义的形式化模型，对系统所有主体和客户实施DAC和MAC，具有可信通道机制、最小特权管理和对隐蔽通道的分析处理等
  - **B3级** —— 安全域级。对TCB提出了更多要求，支持安全管理者的实现，支持系统恢复
- **A级 —— 形式化证明的安全（Formally Proven Security）**
  - **A1级** —— 验证设计级。包含以上各级别的安全措施，形式化的顶级设计规范、形式化验证

GB 17859-1999

- 《计算机信息系统安全保护等级划分准则》：
  - 是中国计算机信息系统安全等级保护系列标准的核心，是实行计算机信息系统安全等级保护制度建设的重要基础，也是信息安全评估和管理的重要基础。
- 本质上等同于TCSEC，不同的是舍弃了D和A1级，将计算机信息系统安全性从低到高划分为5个等级：
  - **第一级：用户自主保护级**
  - **第二级：系统审计保护级**
  - **第三级：安全标记保护级**
  - **第四级：结构化保护级**
  - **第五级：访问验证保护级**
- 该标准中一个重要的概念是可信计算基础（TCB）：
  - TCB是一种实现安全策略的机制，包括硬件、固件和软件，它们根据安全策略来处理主体对客体的访问。TCB主要实现隔离和访问控制两大特征，各安全等级之间的差异在于TCB的构造不同以及所具有的安全保护能力不同。

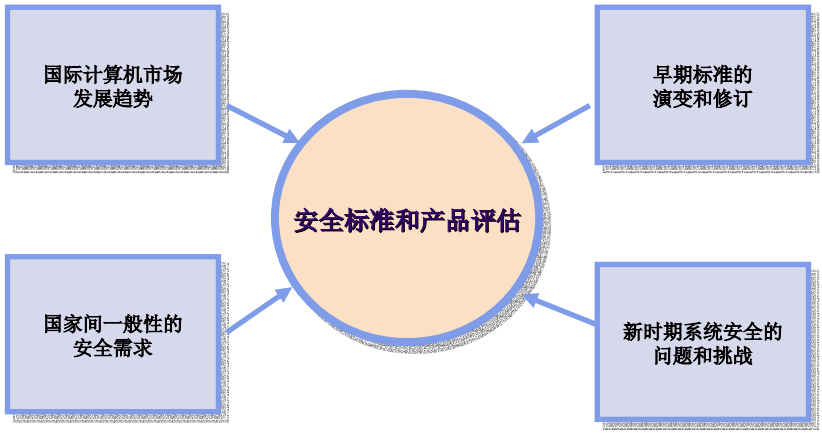
ITSEC简介

- 1991年，西欧四国（英、法、荷、德）联合提出了ITSEC
- 比桔皮书更宽松，目的是适应各种产品、应用和环境的需要，试图超越桔皮书
- 首次提出了信息安全的保密性、完整性和可用性的概念
- 将安全性要求分为“功能”和“保证”两个部分：
  - 功能：为满足安全需求而采取的一系列技术安全措施，如AC、审计、鉴别等
  - 保证：确保功能正确实现及有效性的安全措施
- ITSEC提出一个基本观点：分别衡量安全功能和安全保证
  - 安全功能等级（Functionality，F1～F10），F1～F5与桔皮书的C1～B3相对应
  - 安全保证等级（European Assurance，E0～E6）
- ITSEC还首次提出了安全目标（ST）的概念
- ITSEC认为，被评估的应是整个系统，而不只是计算平台
- ITSEC成为欧共体信息安全计划的基础

- 信息安全标准化概述
- **CC标准简介**
- CC标准中的关键概念
- CC的核心内容和组织结构
- 安全评估
- 通用评估方法（CEM）
- 总结和展望

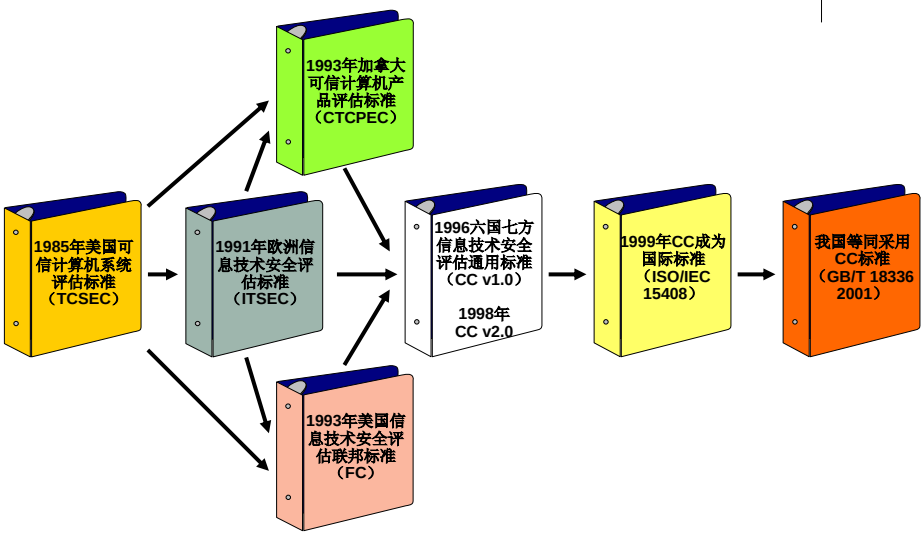
CC标准简介

CC的驱动因素



CC标准简介

CC标准的发展历程



CC标准简介

CC要实现的目标

- 成为统一的国际（通用）IT产品和系统安全标准
- 目前，CC已经成为ISO国际标准（15408）
- 在不同国家间达成协议，相互承认产品评估
- 为开发者拓展国际舞台
- 改善IT安全产品在全世界的可用性

CC标准简介

CC的适用范围

- CC定义了评估信息技术产品和系统安全性所需的基础准则，是度量信息技术安全性的基准
- 针对在安全评估过程中信息技术产品和系统的安全功能及相应的保证措施提出一组通用要求，使各种相对独立的安全评估结果具有可比性
- 有助于信息技术产品和系统的开发者或用户确定产品或系统对其应用而言是否足够安全，以及在使用中存在的安全风险是否可以容忍
- 该标准主要保护的使信息的CIA三大特性，其次也考虑了可控性、可追溯性等
- 该标准适用于对信息技术产品或系统的安全性进行评估，不论其实现方式使硬件、固件还是软件；还可用于指导产品或系统开发
- 该标准的主要目标读者是用户、开发者和评估者

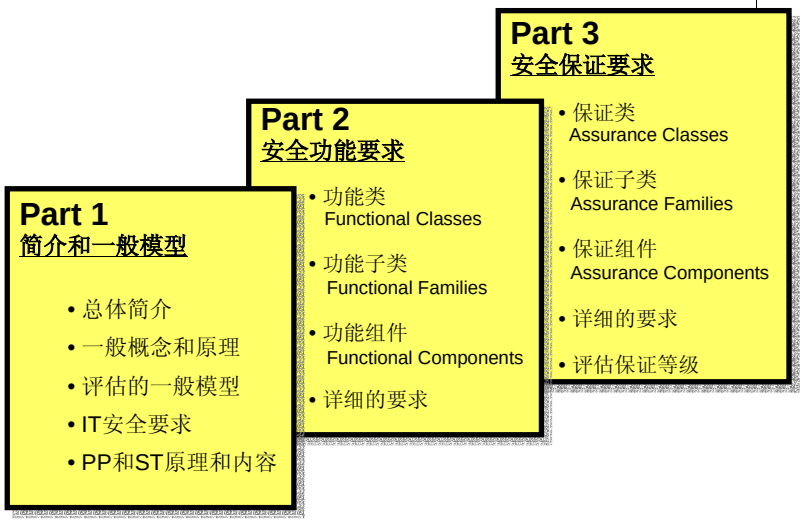
CC标准简介

CC的目标读者

- **用户（定义安全需求）**
  - 可以用CC的结构和语言来定义安全需求；可用评估结果决定一个已评估的产品或系统是否满足他们的安全需求；可用评估结果比较不同的产品或系统；可为系统的使用、运行提供支持。
  - 为用户提供一个独立于实现的框架（PP），供用户提出对被评估产品或系统的特殊的安全要求。
- **开发者（描述产品的安全能力）**
  - 为开发者在确定其产品或系统所要满足的安全需求方面提供支持；
  - 为他们准备和协助对其产品或系统的评估提供支持；
  - 通过评估证实产品或系统的安全功能，保证满足特定的安全需求。
  - 标准中提出的安全功能可被开发者在其产品或系统中实现，促进其技术进步；
  - 标准中的保证要求可帮助开发者规范其研发、生产和集成等过程，提高生产管理能力。
- **评估者（度量产品的置信程度）**
  - 遵照标准，依据通用评估方法（CEM）对产品或系统的安全性进行评估，以判断产品或系统在安全性方面与标准要求的一致性，实现正确性和有效性，使评估结果具有可重复性和客观性。

CC标准简介

CC的内容组织



Common Criteria

- 信息安全标准化概述
- CC标准简介
- **CC标准中的关键概念**
- CC的核心内容和组织结构
- 安全评估
- 通用评估方法（CEM）
- 总结和展望

关键概念

CC定义了两类安全需求

功能需求
Functional Requirements

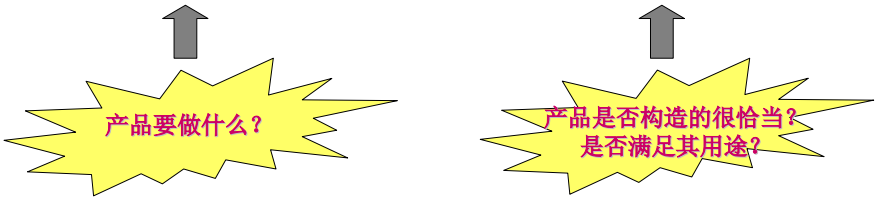
定义了IT产品和系统的安全行为:

- **对此类需求的实现就成了安全功能**

保证需求
Assurance Requirements

为建立对安全功能的信任而设:

- **功能实现的正确性**
- **满足安全目标的有效性**



关键概念

CC的关键概念（1）

- **评估对象（Target of Evaluation，TOE）**
  - 用于安全评估的信息技术产品、系统或子系统（如防火墙、计算机网络、密码模块等），包括相关的管理员指南、用户指南、设计方案等文档
- **保护轮廓（Protection Profile，PP）**
  - 为既定的一系列安全对象提出功能和保证要求的完备集合，表达了一类产品或系统的用户需求
  - PP与某个具体的TOE无关，它定义的是用户对这类TOE的安全需求
  - 主要内容：需保护的对象；确定安全环境；TOE的安全目的；IT安全要求；基本原理
  - 在标准体系中PP相当于产品标准（同TCSEC级别类似），也有助于过程规范性标准的开发
  - 国内外已对应用级防火墙、包过滤防火墙、智能卡、IDS、PKI等开发了相应的PP
- **安全目标（Security Target，ST）**
  - ST针对具体TOE而言，它包括该TOE的安全要求和用于满足安全要求的特定安全功能和保证措施
  - ST包括的技术要求和保证措施可以直接引用该TOE所属产品或系统类的PP
  - ST是开发者、评估者、用户在TOE安全性和评估范围之间达成一致的基础
  - ST相当于产品和系统的实现方案，与ITSEC的“安全目标”类似。例如ST for Oracle v7

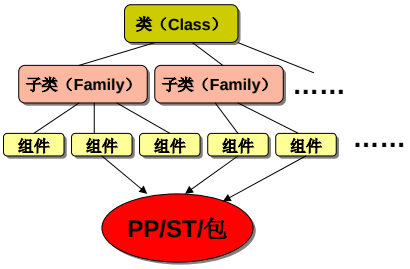
关键概念

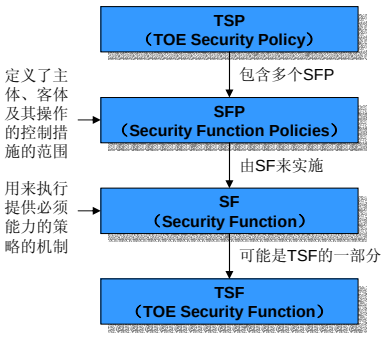
CC的关键概念（2）

- TOE Security Policy（TSP）
  - 控制TOE中资产如何管理、保护和分发的规则
- TOE Security Functions（TSF）
  - 必须依赖于TSP正确执行的TOE的所有部件
- **组件（Component）**
  - 组件描述了一组特定的安全要求，是可供PP、ST或包选取的最小的安全要求集合
  - 在CC中，以“类_子类.组件号”的方式来标识组件
- **包（Package）**
  - 组件依据某个特定关系的组合，就构成了包
  - 构建包的目的是定义那些公认有用的、对满足某个特定安全目的有效的安全要求
  - 包可以用来构造更大的包、PP和ST。包可以重复使用
  - CC中有功能包和保证包两种形式

关键概念

一些概念之间的关系



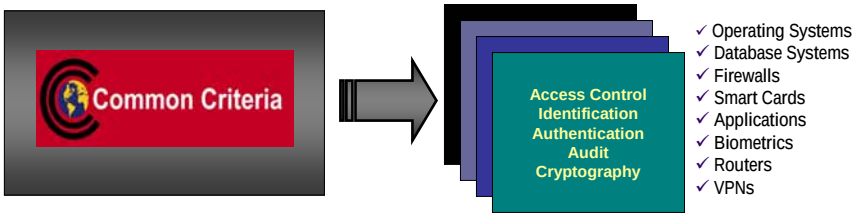


关键概念

用户借助PP来定义需求

ISO/IEC Standard 15408

Protection Profiles



一个灵活的、健壮的标准化IT安全需求的目录（特点和保证）

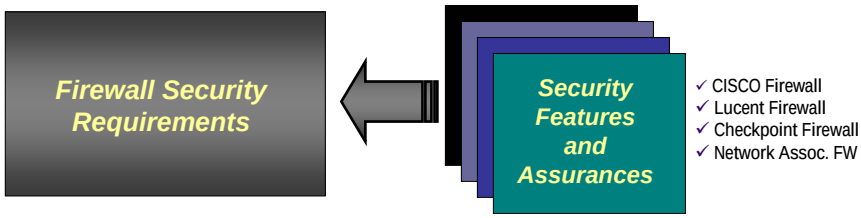
在特定IT领域，用户驱动的安全需求

关键概念

厂商对用户需求作出响应

Protection Profile

Security Targets



用户向业界厂商陈述对某个特定IT领域的安全需求

厂商陈述其对自身IT产品的安全承诺

关键概念

PP、ST和TOE之间的关系

Protection Profile (PP) 用户想要的东西

Security Target (ST) 厂商声称提供的东西

Design documents

Target of Evaluation (TOE) 产品本身

- 信息安全标准化概述
- CC标准简介
- CC标准中的关键概念
- **CC的核心内容和组织结构**
- 安全评估
- 通用评估方法（CEM）
- 总结和展望

标准内容

CC-Part1的内容（1）

1 范围（Scope）

2 定义（Definitions）

- 常用的缩略语，基本术语

3 概述（Overview）

- CC的目标受众（Consumers、Developers、Evaluators、Others）
- 评估上下文（评估体制框架）
- CC的内容组织

4 一般模型（General Model）

- 一般性的安全上下文关系模型，IT安全上下文
- CC的途径，安全概念，CC的描述性材料，评估的类型（评估PP、ST、TOE）

5 CC需求和评估结果

- PP和ST的需求，TOE的需求，关于评估结果

标准内容

CC-Part1的内容（2）

附录A CC项目介绍

- CC的项目背景，CC的开发，资助CC项目的组织

附录B PP规范

- 概述
- PP的内容包括：PP介绍，TOE描述，TOE安全环境，安全目标，IT安全需求，应用要点

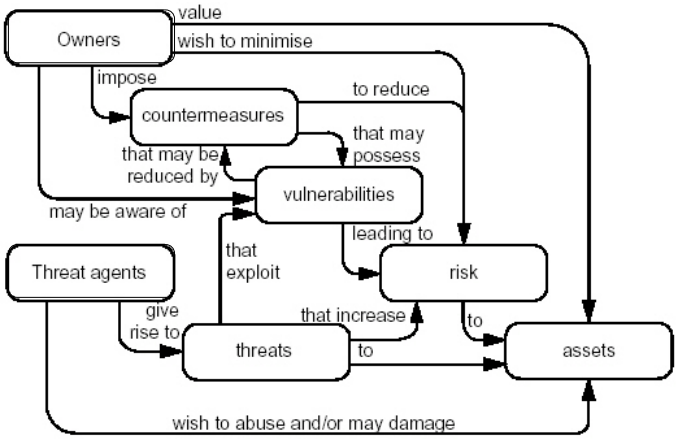
附录C ST规范

- 概述
- ST的内容包括：ST介绍，TOE描述，TOE安全环境，安全目标，IT安全需求，TOE概要规范，PP声明

附录D 参考书目

标准内容

一般性安全关系模型

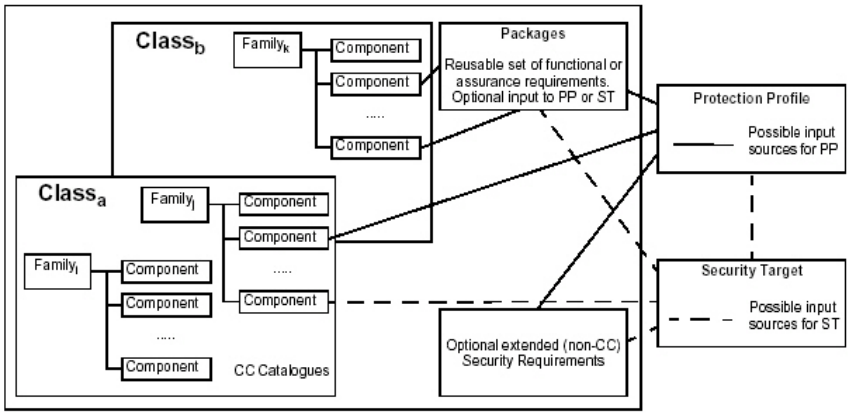


标准内容

评估概念及关系

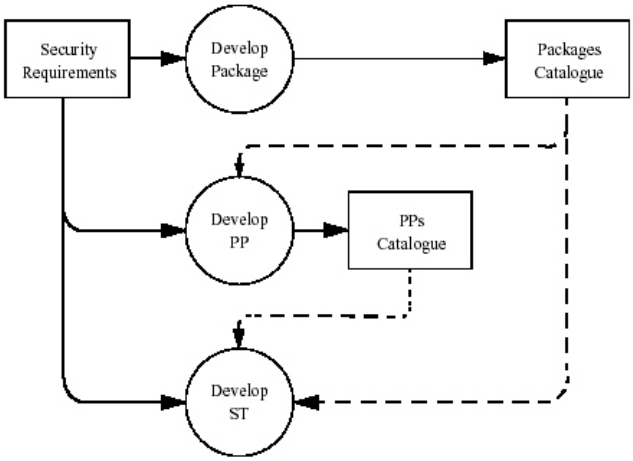
标准内容

表达安全需求的各种构造形式



标准内容

对安全需求的应用



标准内容

PP的内容结构

1. 保护轮廓引言 1.1 PP标识 1.2 PP概述	标识PP 叙述性概括PP
2. TOE描述	TOE的背景信息
3. 安全环境 3.1 假设 3.2 威胁 3.3 组织性安全策略	指明安全问题（要保护的资产、已知的攻击方式、TOE必须使用的组织性安全策略）
4. 安全目的 4.1 TOE安全目的 4.2 环境安全目的	对安全问题的相应反应（包括非技术性措施）
5. IT安全需求 5.1 TOE安全功能需求 5.2 TOE安全保证需求 5.3 IT环境安全需求	CC第二部分的功能组件 CC第三部分的保证组件 IT环境中软件、硬件、固件要求
6. 基本原理 6.1 安全目的基本原理 6.2 安全要求基本原理	目的和要求可以解决已指出的安全问题
7. 应用注解	附加信息

标准内容

ST的内容结构

1. 安全目标引言 1.1 ST标识 1.2 ST概述 1.3 CC一致性声明	标识ST和TOE（包括版本号） 叙述性总结ST
2. TOE描述	TOE背景信息（评估环境）
3. 安全环境 3.1 假设 3.2 威胁 3.3 组织性安全策略	指明安全问题（要保护的资产、已知的攻击、TOE必须使用的组织性安全策略、假定的安全问题）
4. 安全目的 4.1 TOE安全目的 4.2 环境安全目的	对安全问题的相应反应（包括非技术性措施）
5. IT安全需求 5.1 TOE安全功能需求 5.2 TOE安全保证需求 5.3 IT环境安全需求	CC第二部分的功能组件 CC第三部分的保证组件 IT环境中软件、硬件、固件需求
6. TOE概要规范 6.1 TOE安全功能 6.2 保证措施	IT安全功能满足哪一个特定的安全功能需求 IT保证措施满足哪一个特定的安全保证需求
7. 保护轮廓声明 7.1 PP参照 7.2 PP裁减 7.3 PP附加项	解释、证明和其他支持材料，以证实一致性声明

标准内容

CC-Part2的内容（1）

1 范围（Scope）

2 安全功能组件（Class、Family、Component的结构，Component catalogue）

3 Class FAU：Security Audit

- 安全审计包括识别、记录、存储和分析那些与安全行为有关的信息。审计记录的检查结果用来判断发生了哪些安全行为，以及哪个用户要对这些行为负责。
- 6个子类：安全审计自动应答（FAU_ARP），安全审计数据产生（FAU_GEN），安全审计分析（FAU_SAA），安全审计查阅（FAU_SAR），安全审计事件选择（FAU_SEL），安全审计事件存储（FAU_STG）

4 Class FCO：Communication

- 用于确保在数据交换中参与方的身份。既确保发送者不能否认，又确保接收者不能否认收到。
- 2个子类：原发抗抵赖（FCO_NRO），接收抗抵赖（FCO_NRR）

5 Class FCS：Cryptographic support

- 产品或系统含有密码功能时，将使用密码支持类。
- 2个子类：密钥管理（FCS_CKM），密码运算（FCS_COP）

标准内容

CC-Part2的内容（2）

6 Class FDP：User data protection

- 规定了与保护用户数据相关的所有安全功能要求和策略。涉及用户数据输入、输出和存储。
- 13个子类：访问控制策略（FDP_ACC），访问控制功能（FDP_ACF），数据鉴别（FDP_DAU），输出到TSF控制之外（FDP_ETC），信息流控制策略（FDP_IFC），信息流控制功能（FDP_IFF），从TSF控制之外输入（FDP_ITC），TOE内部传送（FDP_ITT），残余信息保护（FDP_RIP），反转（FDP_ROL），存储数据的完整性（FDP_SDI），TSF间用户数据传送的保密性保护（FDP_UCT），TSF间用户数据传送的完整性保护（FDP_UIT）

7 Class FIA：Identification and authentication

- 提出了用户身份确定和验证、与TOE交互的授权，以及每个授权用户安全属性的正确关联等三方面的安全要求。
- 6个子类：TSF功能管理（FMT_MOF），安全属性管理（FMT_MSA），TSF数据管理（FMT_MTD），撤消（FMT_REV），安全属性到期（FMT_SAE），安全管理角色（FMT_SMR）

8 Class FMT：Security Management

- 规定了安全属性、数据和功能三方面的管理，也定义不同管理角色及其相互作用。
- 6个子类：安全审计自动应答（FAU_ARP），安全审计数据产生（FAU_GEN），安全审计分析（FAU_SAA），安全审计查阅（FAU_SAR），安全审计事件选择（FAU_SEL），安全审计事件存储（FAU_STG）

标准内容

CC-Part2的内容（3）

9 Class FPR：Privacy

- 要求为用户提供其身份不被其他用户发现或滥用的保护。
- 4个子类：匿名（FPR_ANO），假名（FPR_PSE），不可关联性（FPR_UNL），不可观察性（FPR_UNO）

10 Class FPT：Protection of the TSF

- TSF指的是TOE安全功能，TSF类侧重于保护TSF数据，而不是用户数据。
- 16个子类：根本抽象机测试（FPT_AMT），失败保护（FPT_FLS），输出TSF数据的可用性（FPT_ITA），输出TSF数据的保密性（FPT_ITC），输出TSF数据的完整性（FPT_ITI），TOE内 TSF数据的传送（FPT_ITT），TSF物理保护（FPT_PHP），可信恢复（FPT_RCV），重放检测（FPT_RPL），参照仲裁（FPT_RVM），域分离（FPT_SEP），状态同步协议（FPT_SSP），时间戳（FPT_STM），TSF间TSF数据的一致性（FPT_TDC），TOE内 TSF数据复制的一致性（FPT_TRC），TSF自检（FPT_TST）

11 Class FRU：Resource utilisation

- 支持所需资源的可用性。
- 3个子类：容错（FRU_FLT），服务优先级（FRU_PRS），资源分配（FRU_RSA）

标准内容

CC-Part2的内容（4）

12 Class FTA：TOE access

- 规定了用以控制建立用户会话的一些功能要求，是对标识和鉴别类安全要求的进一步补充。
- 6个子类：可选属性范围限定（FTA_LSA），多重并发会话限定 (FTA_MCS)，会话锁定 （FTA_SSL），TOE访问旗标（FTA_TAB），TOE 访问历史 (FTA_TAH)，TOE 会话建立(FTA_TSE)

13 Class FTP：Trusted path/channels

- 规定了关于用户和TSF之间可信通信路径，以及TSF和其他可信IT产品间可信通信信道的要求。
- 2个子类：TSF间可信信道（FTP_ITC），可信路径（FTP_TRP）

附录A 安全功能需求应用要点

附录B

……

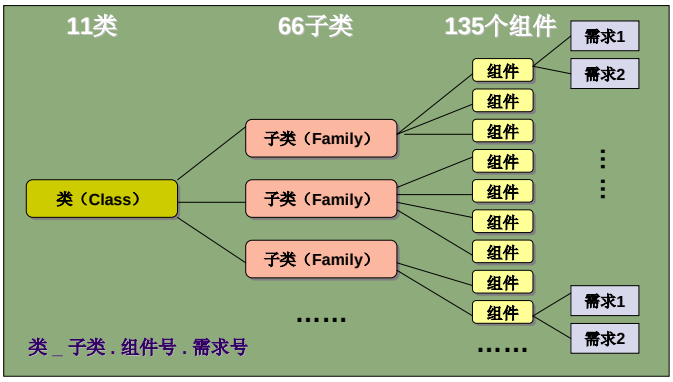
…… 对11个功能类及其子类、具体需求点的详细解释

……

附录M

标准内容

安全功能需求层次关系



标准内容

CC-Part3的内容（1）

1 范围（Scope）

2 安全保证需求

- Class、Family、Component、EAL的结构
- 组件分类，PP和ST评估标准类结构，保证分类，维护分类

3 PP和ST评估标准

- PP和ST是评估TOE及其功能和保证需求的基础，在评估TOE之前需要证明PP和ST对TOE评估来说是否适用，即确定PP和ST是否完整、一致、技术上可靠，以至于适合用作一个或多个待评估TOE的需求声明
- 用以下两个类来规范对PP和ST的评估

4 Class APE：Protection Profile evaluation

- 该类相当于规范了对产品或系统标准的评审，评估过的PP可进一步到权威机构注册并发布
- 该类提出了TOE描述、安全环境、安全目的和安全需求等方面的评估要求

5 Class ASE：Security Target evaluation

- 提出了TOE描述、安全环境、安全目的、PP声明、安全需求和TOE概要规范等方面的评估要求

标准内容

CC-Part3的内容（2）

6 评估保证等级（Evaluation Assurance Levels）

- 一个保证等级（EAL）是评估保证要求的一个基线集合——保证包。每一评估保证级定义一套一致的保证要求，合起来构成一个预定义CC保证级尺度。CC定义了7个递增的评估保证等级

7 保证类、子类和组件

- 保证系指对功能产生信心的方法。保证要求包含开发者行为、产生的证据以及评估者行为
- 以下7个保证类，确保安全功能在TOE的整个生命周期中正确有效地实施，这些保证类是定义评估保证等级的基础，是具体TOE评估的依据和准则

8 Class ACM：Configuration Management

- 通过跟踪TOE的任何变化，确保所有修改都已授权，以保证TOE的完整性。特别是，通过配置管理确保用于评估的TOE和相关文档正是预先所准备的那份
- 3个子类：配置管理自动化（ACM_AUT），配置管理能力（ACM_CAP），配置管理范围（ACM_SCP）

9 Class ADO：Delivery and Operation

- 该类规定了TOE交付、安装、生成和启动方面的措施、程序和标准，以确保TOE所提供的安全保护在这些关键过程中不被泄漏
- 2个子类：交付（ADO_DEL），安装、生成和启动（ADO_IGS）

标准内容

CC-Part3的内容（3）

10 Class ADV：Development

- 该类涉及将ST中定义的TOE概要规范细化为具体的TOE安全功能（TSF）实现，以及安全要求到最低级别表示之间的映射两个方面
- 7个子类：功能规范（ADV_FSP），高层设计（ADV_HLD），实现表示（ADV_IMP），TSF内部（ADV_INT），低层设计（ADV_LLD），表示对应性（ADV_RCR），安全策略模型（ADV_SPM）

11 Class AGD：Guidance documents

- 规定用户指南和管理员指南编写方面的要求。
- 2个子类：管理员指南（AGD_ADM），用户指南（AGD_USR）

12 Class ALC：Life cycle support

- 在TOE开发和维护阶段，对相关过程进一步细化并且建立相应的控制规则，以确保TOE与其安全要求之间的符合性
- 4个子类：开发安全（ALC_DVS），缺陷纠正（ALC_FLR），生命周期定义（ALC_LCD），工具和技术（ALC_TAT）

标准内容

CC-Part3的内容（4）

13 Class ATE：Tests

- 测试关心的是TOE是否满足其安全功能要求
- 4个子类：覆盖范围（ATE_COV），深度（ATE_DPT），功能测试（ATE_FUN），独立性测试（ATE_IND）

14 Class AVA：Vulnerability assessment

- 该类定义了与识别可利用的脆弱性相关的安全要求，这些脆弱性可能在开发、集成、运行、使用和配置时进入TOE
- 3个子类：隐蔽信道分析（AVA_CCA），误用（AVA_MSU），TOE安全功能强度（AVA_SOF）

15 保证维护范例（Assurance maintenance paradigm）

- 保证维护的目的是确保TOE或其环境发生变化时，还能继续满足安全目标
- 对保证进行维护的一种方法是再次评估TOE，但势必增加开销
- CC通过AMA类定义一套要求，确保有关保证都得到维护，而不需要全面再评估

标准内容

CC-Part3的内容（5）

16 Class AMA：Maintenance of assurance

- 该类提出的要求必须在TOE通过CC认证之后才适用，这些要求旨在确保TOE或其环境变更后，继续满足安全目标
- 4个子类：保证维护计划（AMA_AMP），TOE组件分类报告（AMA_CAT），保证维护证据（AMA_EVD），安全影响分析（AMA_SIA）

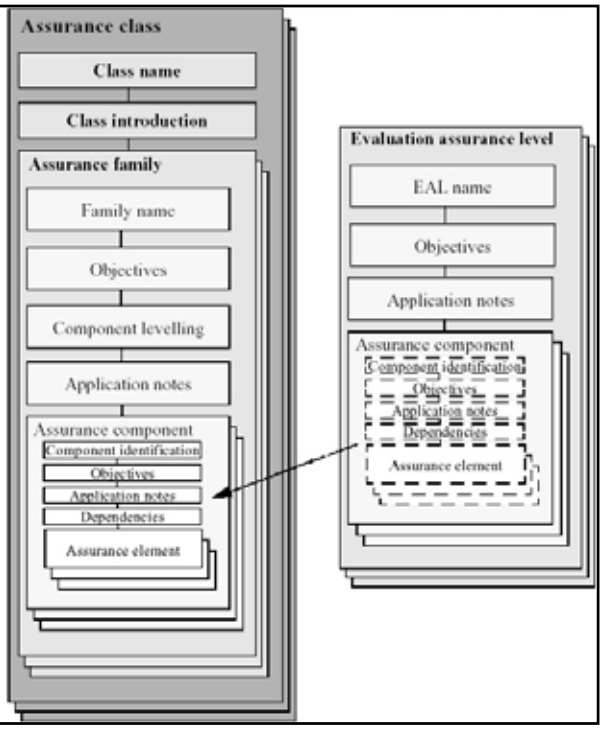
附录A 保证组件依从性交叉引用

附录B EALs及保证组件交叉引用

标准内容

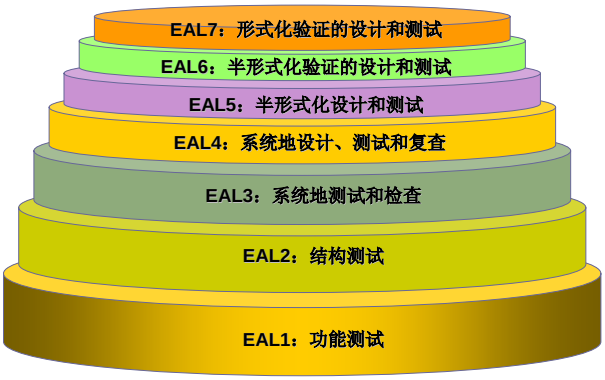
安全保证需求层次结构及EAL引用关系

EAL不能对具体的保证需求进行引用，而只能引用到保证类中包含的某个保证组件



标准内容

评估保证等级（EAL）



标准内容

EAL解释（1）

- **EAL1：functionally tested**
  - 适用于对正确运行需要一定信任的场合，对该场合的安全威胁应视为并不严重
  - 依据一个规范的独立性测试和对所提供指导性文档的检查来为用户评估TOE。没有开发者帮助也能评估。通过评估，可以确信TOE的功能与其文档在形式上是一致的，且对已标识的威胁提供了有效的保护
- **EAL2：structurally tested**
  - 要求开发者递交设计信息和测试结果，但不需要开发者增加过多费用或时间投入
  - 适用于：在缺乏现成可用的完整的开发记录时，开发者或用户需要一种低等到中等级别的独立保证的安全性
- **EAL3：methodically tested and checked**
  - 适用于：开发者或用户需要一个中等级别的独立保证的安全性，且在不带大量重建费用的情况下，对TOE及其开发过程进行彻底审查
- **EAL4：methodically designed, tested, and reviewed**
  - 适用于：开发者或用户对传统的商品化的TOE需要一个中等到高等级别的独立保证的安全性，并且准备负担额外的安全专用工程费用
  - 需要分析TOE模块的低层设计和实现的子集

标准内容

EAL解释（2）

- **EAL5：semiformally designed and tested**
  - 适用于：开发者和使用者在有计划的开发中，采用严格的开发手段，以获得一个高级别的独立保证的安全性，不会因采取专业性安全工程技术而增加一些不合理的开销
  - 需要分析所有的实现，还需要额外分析功能规范和高层设计的形式化模型和半形式化表示和论证
- **EAL6：semiformally verified design and tested**
  - 适用于在高风险环境下的特定安全产品或系统的开发，且要保护的资源值得花费一些额外的人力、物力和财力
- **EAL7：formally verified design and tested**
  - 适用于一些安全性要求很高的TOE开发。这些TOE将应用在风险非常高的地方，或者所保护资产的价值很高的地方
  - 目前，该级别的TOE比较少，一方面是对安全功能全面的形式化分析难以实现，另一方面在实价应用中也很少有这类需求

标准内容

各评估保证等级所含组件

7个EAL等级是递增的关系，这种递增靠替换成同一保证子类中的一个更高级别的保证组件（即增加严格性、范围和深度）和添加另外一个保证子类的保证组件（如添加新的要求）来实现

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

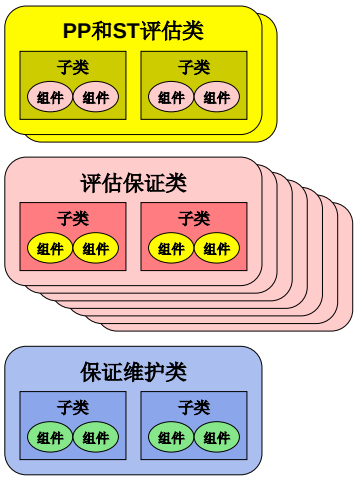
标准内容

CC的EAL与其他标准等级的比较

CC	中国 GB17859	美国 TCSEC	美国 FC	加拿大 CTCPEC	欧洲 ITSEC
EAL1		D	-	-	-
EAL2	第一级：用户自主保护级	C1	-	-	E1
EAL3	第二级：系统审计保护级	C2	T-1	T-1	E2
EAL4	第三级：安全标记保护级	B1	T-2	T-2	E3
-		-	T-3	T-3	-
-		-	T-4	-	-
EAL5	第四级：结构化保护级	B2	T-5	T-4	E4
EAL6	第五级：访问验证保护级	B3	T-6	T-5	E5
EAL7		A1	T-7	T-6	E6
-		-	-	T-7	-

标准内容

安全保证需求总结



1个PP和ST评估类

用来证明PP和ST对TOE评估是否适用，是评估TOE的前提和基础

7个评估保证类

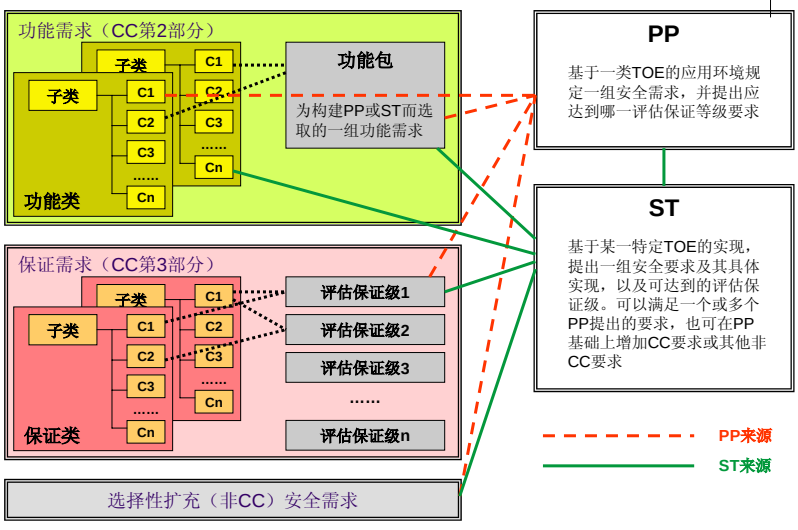
安全保证需求的主体。是定义评估保证等级的基础，是具体TOE评估的依据和准则

1个保证维护类

适用于TOE通过CC认证之后，确保TOE或环境变化时，还能继续满足安全目标

标准内容

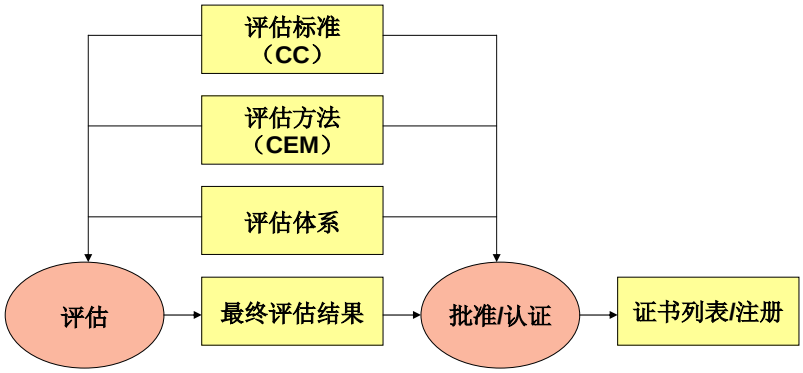
CC总体结构



- 信息安全标准化概述
- CC标准简介
- CC标准中的关键概念
- CC的核心内容和组织结构
- **安全评估**
- 通用评估方法（CEM）
- 总结和展望

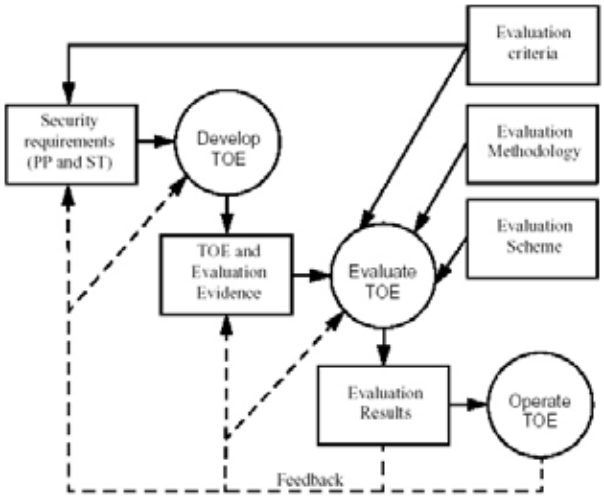
安全评估

安全评估框架模型



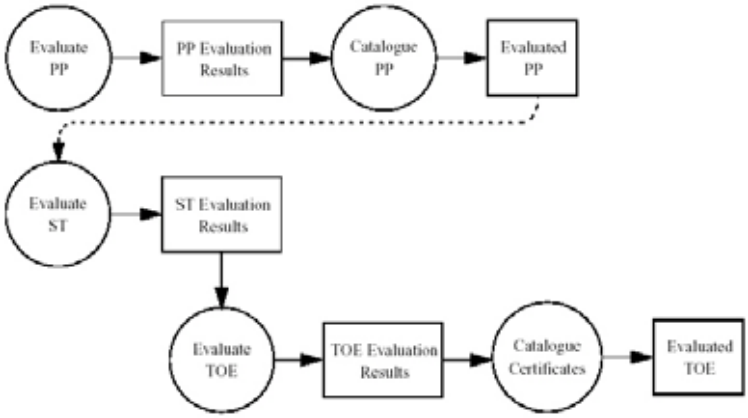
安全评估

TOE评估过程



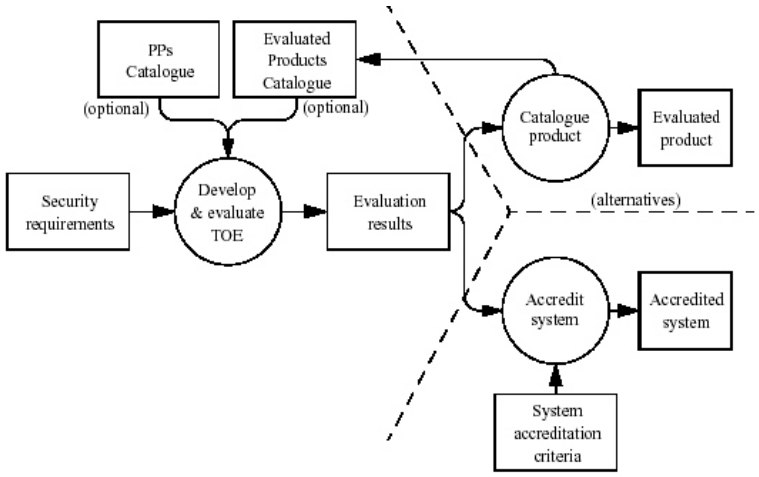
安全评估

PP、ST和TOE评估的关系



安全评估

对TOE评估结果的应用



- 信息安全标准化概述
- CC标准简介
- CC标准中的关键概念
- CC的核心内容和组织结构
- 安全评估
- **通用评估方法（CEM）**
- 总结和展望

通用评估方法

CEM简介

◆ 通用评估方法（Common Evaluation Methodology，CEM）是为CC评估而开发的一种国际公认方法，CEM支撑着信息安全评估的国际互认

◆ CEM主要是针对评估者而开发的，其他团队（开发者、监督者等）也可从CEM中得到一些有用的信息

◆ PP开发者（一组用户代表或IT产品的一个制造商）使用CEM：
- 有利于在执行PP评估的一致性和独立性方面证实PP方面的应用

◆ TOE开发者（产品制造商，系统集成商，或其他解决方案提供者）使用CEM有利于：
- 在PP和ST中，文档化提出的安全特性可被独立地证实和验证；
- 开发者的顾客将更容易确信TOE提供了所声称的安全特性；
- 评估后的产品在所组成的安全系统中可以更有效地使用

◆ 评估发起者（启动一个评估的组织实体，可以是开发者或顾客）：
- 把CEM用于以文档形式提出TOE的安全特性，并要求评估者独立地证实和验证

◆ 评估者使用CC时要与CEM一致

◆ 监督者时确保所进行的评估过程与CC、CEM一致性的实体

通用评估方法

评估的普遍原则

◆ **适当性原则**
- 为达到一个预定的保证级所采取的评估活动应该是适当的

◆ **公正性原则**
- 所有的评估应当没有偏见

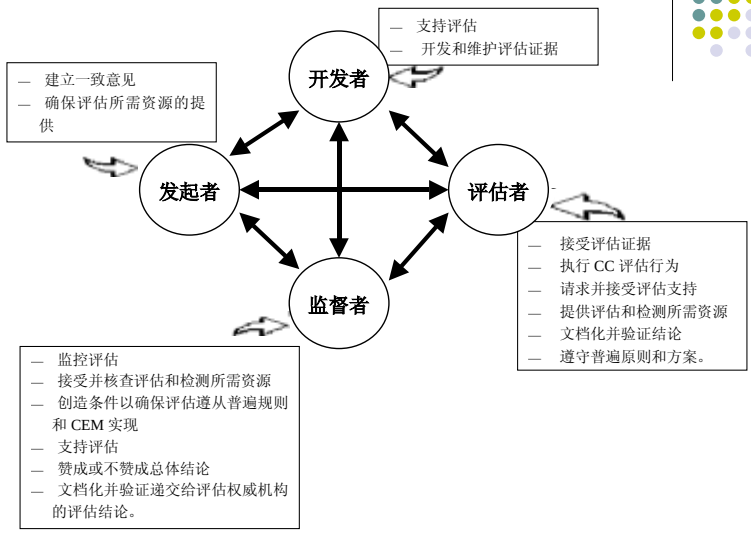
◆ **客观性原则**
- 应当在最小主观判断或主张情形下，得到评估结果

◆ **可重复性和可再现性原则**
- 依照同样的要求，使用同样的评估证据，对同一TOE或PP的重复评估应该导出同样的结果

◆ **结果的完善性原则**
- 评估结果应当是完备的并且采取的技术恰当

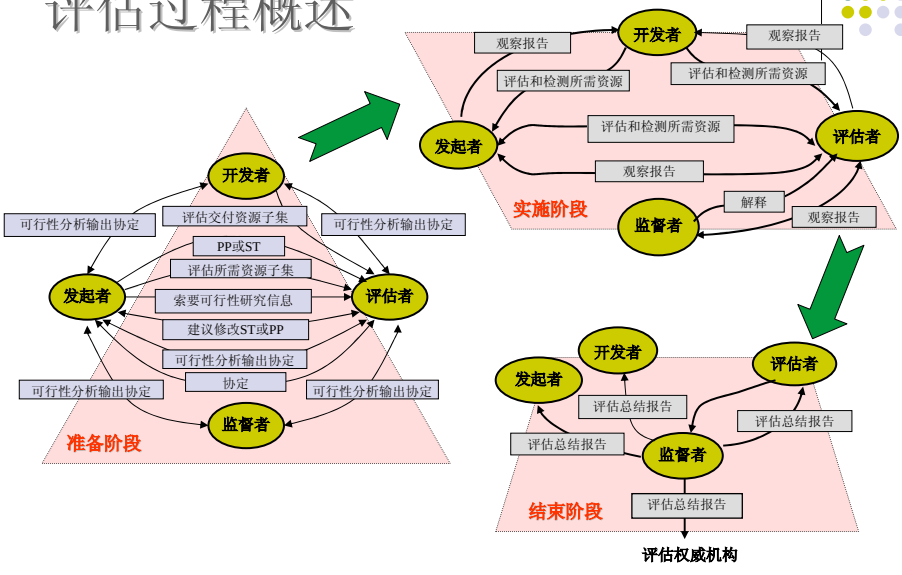
通用评估方法

评估的角色和职责关系



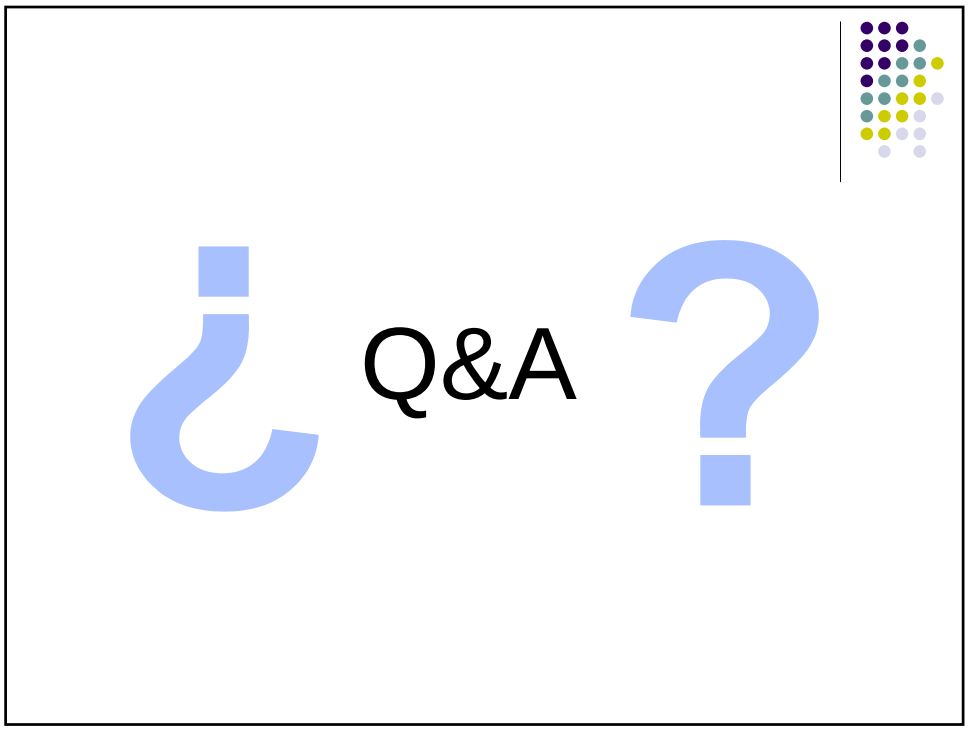
通用评估方法

评估过程概述



- 信息安全标准化概述
- CC标准简介
- CC标准中的关键概念
- CC的核心内容和组织结构
- 安全评估
- 通用评估方法（CEM）
- **总结和展望**

总结和展望


¿
Q&A
?