标题：GTB 18336等同ISO 15408解析

时间：2020.06.10

目录：

参考文献：

1. GB/T 18336-2015 信息技术 安全技术 信息技术安全评估准则
2. ISO/IEC 15408:2008 Information technology-Security techniques-Evaluation criteria for IT security
3. 李爱萍，崔东华，李东生.软件工程.人民邮电出版社，2014
4. 刘文清.《结构化保护级》安全操作系统若干关键技术的研究.中国科学院研究生院，2002
5. 王瑜.安全操作系统标识与鉴别及访问控制机制的设计与实现.中国科学院研究生院，2004

正文：

# 第一章 标准要求

本部分为GB/T 18336（以下简称CC）中所规定的安全功能要求中的标识与鉴别部分的内容。

### 1.1 术语和缩写

1. TOE 评估对象
2. SFR 安全功能要求
3. SFP 安全功能策略
4. TSF TOE安全功能
5. TSFI TSF接口

### 1.2 相关概念

（1）用户

用户在TOE外部。但为了请求由TOE执行且由SFR中定义的规则所控制的服务，用户通过TSFI和TOE交互。本部分关注两种类型用户：人类用户和外部IT实体。人类用户可进一步分为本地用户和远程用户，本地用户通过TOE设别（如工作站）直接与TOE交互，远程用户通过其他IT产品间接与OTE交互。

（2）会话

用户和TSF之间的一段交互期称为用户会话。可以根据各种因素来控制用户会话的建立，例如：用户鉴别、时段、访问TOE的方法以及允许的（每个用户的或总的）并发会话数。

（3）角色

为了表达分离管理责任的要求，相关的安全功能组件（来自TMF\_SMR族）明确指出了所要求的管理性角色。角色是预定义的一组规则，用户建立用户按此角色操作时所允许的与TOE之间的交互。一个TOE可以支持任意多个角色的定义。例如，与TOE安全运行相关的角色可以包括“审计管理员”和“用户账号管理员”。

（4）主体

TOE中对客体执行操作的主动实体，被称为主体。TOE可存在在下列类型的主体：

1. 代表一个授权用户的那些实体（如Unix进程）
2. 作为一个特殊功能进程，可依次代表多个用户的那些实体（如在客户/服务器结构中可能找到的某些功能）
3. 作为TOE自身一部分的那些实体（如不代表某个用户的进程）

（5）客体

TOE中包含和接收信息，且主体得以在这些信息上执行操作的被动实体，称作客体。在一个主体（主动实体）是某个操作对象（如进程间通信）的情况下，该主体也可以作为一个客体。客体可以包含信息。

（6）属性

由SFR中各规则所控制的用户、主体、信息、客体、会话和资源，可具有某些属性。属性包含TOE为了正确运行而使用的信息。某些属性，如文件名，可能只是提示性的，或者可用来标识单个资源，而另外一些属性，如访问控制信息，可能是专为执行SFR而存在的。后面这些属性通常称为“安全属性”。

（7）数据

TOE中的数据可分为用户数据和TSF数据。用户数据是存储在TOE资源中的信息，用户可以根据SFR对其进行操作，而TSF对用户数据并不赋予任何特殊含义。TSF数据是TSF在按SFR的要求做决策时使用的信息。如果SFR允许，TSF数据可以受用户的影响。安全属性、鉴别数据、有SFR中定义的规则，或成为保护TSF及访问控制列表条目所使用的TSF内部状态变量都是TSF数据的例子。

### 1.3 FIA类：标识与鉴别

标识与鉴别类描述了关于建立和验证所声称的用户身份的功能要求。需要通过标识与鉴别确保用户与正确的安全属性（如身份、组、角色、安全性或完整性等级）相关联。授权用户的明确标识以及安全属性与用户和主体的正确关联是实施预定安全策略的关键。

本类中的族负责确认和验证用户身份、确认他们与TOE（评估目标）交互的权限以及每个授权用户安全属性的正确关联。

1. 鉴别失败FIA\_AFL；
2. 用户属性定义FIA\_ATD；
3. 秘密的规范FIA\_SOS；
4. 用户鉴别FIA\_UAU；
5. 用户标识FIA\_UID；
6. 用户-主体绑定FIA\_USB。

1.1.1 鉴别失败

本组包含为不成功的鉴别尝试次数定义数值和鉴别尝试失败时TSF应采取的动作等方面的要求。参数包括但不限于失败的鉴别尝试次数和次数临界值。

1. 鉴别失败处理：要求TSF（安全功能要求）能够在用户鉴别尝试失败达到指定的次数后，终止会话建立进程。此外，它还要求会话建立进程终止后，TSF能够是进行尝试的用户账号或登录点（如工作站）无效，直到满足管理员定义的条件才再次激活。
   1. TSF应检测当[选择：[赋值：正整数]， 管理员可设置的[赋值：可接受数值范围]内的一个正整数]时，与[赋值：鉴别事件列表]相关的未成功鉴别尝试。
   2. 当[选择：达到，超时]所定义的未成功鉴别尝试次数时，TSF应采取[赋值：动作列表]

FMT中管理可考虑下列行为：

1. 未成功鉴别尝试的阈值的管理；
2. 鉴别失败时间中要采取的动作的管理。

如果包含安全审计数据产生FAU\_GEN，下列行为是可审计的：

1. 最小级：未成功鉴别尝试达到阈值、达到阈值后所采取的动作，及后来还原到正常状态。

1.1.2 用户属性定义

所有授权用户可能都有一组除用户身份外的安全属性来执行SFR。本族定义了关联用户属性和用户的要求，以为TSF做安全决策时提供支持。

1. 用户属性定义：允许对每个用户的安全属性分别加以维护；
   1. TSF应维护属于单个用户的下列安全属性列表：[赋值：安全属性列表]

FTM中的管理功能可考虑下列行为：

1. 如果赋值中提及的话，授权管理员应该能够为用户定义附加的安全属性；

1.1.3 秘密的规范

本族定义秘密应满足规定的质量度量，并生成秘密以满足所定义的度量机制的要求。

1. 秘密的验证：要求TSF验证秘密满足规定的质量度量要求；
   1. TSF应提供一种机制以验证秘密满足[赋值：一个既定的质量度量要求]；
2. 生成秘密：要求TSF能够产出满足规定质量要求的秘密。
   1. TSF应提供一直机制以产生满足[赋值：一个既定的质量度量要求]的秘密
   2. TSF应能够为[复制：TSF功能列表]使用TSF产生的秘密

FMT中管理功能可考虑下列行为：

1. 用于验证秘密的度量方法的管理；
2. 用于产生秘密的度量方法的管理。

下列行为是可审计的：

1. 最小级：TSF对任何已测试秘密的拒绝；
2. 基本级：TSF对任何已测试秘密的拒绝或接受；
3. 详细级：对既定的质量度量要求的任何改动的标识。

1.1.4 用户鉴别

本族定义了TSF所支持的用户鉴别机制的类型，也定义了用户鉴别机制所依赖的必要属性。

1. 鉴别的时机：允许用户在其身份被鉴别前执行某些动作；
   1. 在用户被鉴别前，TSF应允许执行代表用户的[赋值：由TSF促成的动作列表]
   2. 在允许执行代表用户的任何其他有TSF促成的动作前，TSF应要求每个用户都已被成功鉴别。
2. 热河动作前的用户鉴别：要求在TSF允许采取任何动作之前，先鉴别用户；
   1. 在允许执行代表用户的任何其他有TSF促成的动作前，TSF应要求每个用户都已被成功鉴别。
3. 不可伪造的鉴别：要求鉴别机制能够检测并防止伪造或复制的鉴别数据的使用；
   1. TSF应[选择：检测、防止]由任何TSF用户伪造的鉴别数据的使用；
   2. TSF应[选择：检测、防止]从任何其他的TSF用户处拷贝的鉴别数据的使用。
4. 一次性鉴别机制：要求鉴别机制使用一次性的鉴别数据；
   1. TSF应防止与[赋值：确定的鉴别机制]有关的鉴别数据的重用；
5. 多从鉴别机制：要求提供和使用不同的鉴别机制，为特定的事件鉴别用户的身份；
   1. TSF应提供[赋值：多重鉴别机制列表]以支持用户鉴别；
   2. TSF应根据[赋值：描述多重鉴别机制如何提供鉴别的规则]鉴别用户所声称的身份。
6. 重鉴别：要求有能力指定对于那些特定事件，用户需要被重新鉴别；
   1. TSF应在[赋值：需要重鉴别的条件列表]条件下重新鉴别用户。
7. 受保护的鉴别反馈：要求在鉴别期间，只提供给用户有限的反馈信息。
   1. 鉴别进行时，TSF应仅向用户提供[赋值：反馈列表]。

FMT中的管理功能考虑下列行为：

1. 管理员对鉴别数据的管理
2. 相关用户对鉴别数据的管理
3. 用户被鉴别前可执行的动作列表的管理
4. 与鉴别数据相关的用户对鉴别数据的管理
5. 鉴别机制的管理
6. 鉴别规则的管理
7. 如果一个授权管理员能请求重鉴别，则管理将包含一个重鉴别请求

审计包括：

1. 最小级：鉴别机制的未成功使用
2. 基本级：鉴别机制的所有使用
3. 详细级：用户鉴别前执行的所有由TSF促成的动作
4. 最小级：对欺骗性鉴别数据的检测
5. 基本级：当前采用的所有措施以及对欺骗性数据检查的结果
6. 最小级：重鉴别数据的企图
7. 最小级：对鉴别的最终裁决
8. 基本级：每个已激活机制的结果以及最终裁决
9. 最小级：重鉴别失败
10. 基本级：所有重鉴别尝试

1.1.5 用户标识

本族定义了在执行任何其他由TSF促成的、且需要用户标识的动作前，要求用户标识其身份的条件。

1. 标识的时机：允许用户在被TSF识别前，执行某些动作
   1. 用户被标识之前，TSF应允许执行代表用户的[赋值：TSF促成的动作列表]
   2. 在允许执行代表该用户的任何其他TSF仲裁动作之前，TSF应要求每个用户身份都已被成功识别
2. 任何动作前的用户标识：在TSF允许其执行任何动作之前，要求用户进行身份识别
   1. 在允许执行代表该用户的任何其他TSF仲裁动作之前，TSF应要求每个用户身份都已被成功识别

FMT中的管理功能可考虑下列行为：

1. 用户身份的管理
2. 如果一个授权管理员能够改变在标识前所允许的动作，则可考虑对动作列表的管理。

审计包括：

1. 最小级：用户标识的未成功使用，包括所提供的用户身份
2. 基本级：所有用户标识机制的使用，包括所提供的用户身份

1.1.6 用户-主体绑定

已成功鉴别的用户，为了使用TOE，一般会先激活一个主体。用户的安全属性（全部或部分地）与该主体相关联。本族定了了建立和维护用户安全属性与代表该用户的主体间关联关系的要求。

1. 用户-主体绑定：要求对用户属性及其映入的主体属性之间的关联关系的管理规则进行规范
   1. TSF应将下列用户安全属性：[赋值：用户安全属性列表]与代表用户活动的主体相关联
   2. TSF应对用户安全属性与代表用户活动的主体初始关联关系执行下列规则：[赋值：属性初始关联规则]
   3. TSF应执行下列规则管理用户安全属性与代表用户活动的主体间的关联关系的变化：[赋值：属性更改规则]

TMF中管理功能可考虑下列行为：

1. 授权管理计可以定义默认的主体安全属性
2. 授权管理员可以改变主体的安全属性

审计包括：

1. 最小级：用户安全属性与一个主体的未成功绑定（如，创建一个主体）
2. 基本级：用户安全属性与一个主体的成功绑定和失败绑定（如，创建一个主体的成功和失败）

# 第二章 安全保护框架

安全保护框架（以下简称PP）是一个安全需求说明书。一个PP是为一类目标TOE定义的一组与实现无关的安全需求。由于未找到数据库的PP，本部分采用来源于论文《《结构化保护级》安全操作系统若干关键技术的研究》中的“《结构化保护级》安全操作系统的安全保护框架（Structured Protection Level Protection Profile， SPLPP）”,该PP中大部分内容适用于数据库。

### 2.1 概述

安全保护框架PP由以下部分构成：

1. PP引言：PP的标识和概述信息
2. TOE描述：将要实现PP所定义的安全需求的安全产品的类型和一般特性
3. 安全环境：安全产品的使用环境中的有关因素
4. 安全目的：为解决安全环境中的各种问题所应确定的安全目的
5. 安全需求：安全产品为达到已确立的安全目的而应该满足的安全需求，包括安全功能需求和安全保证要求
6. PP应用注释：包含安全产品的研制、评价和使用等方面的附加支持信息
7. 基本原理：为两个论点提供依据：
   1. 该PP是一个完全的、一致的需求集合
   2. 符合该PP要求的安全产品能在其安全环境中提供有效的安全对策。安全目的的理论依据需要证明PP中的安全目的是从安全环境中导出的并能覆盖其中安全问题的各个方面，安全要求理论依据需要证明PP中的安全要求是从安全目标中导出的并能满足安全目的的各个方面的要求。

安全功能应满足以下要求：

1. 完备性：PP不应有安全漏洞。安全子系统的设计应全面考虑硬件、固件、系统软件、应用软件的安全，以及与人等相关的管理与操作安全。保证系统运行安全和信息保护安全，考虑恶意攻击的安全防范和自然灾害和意外失误所造成危害的避免。
2. 一致性：安全功能应采用各种不同的安全策略，以响应的安全机制实现各自确定的安全功能，各功能之间应遵循“木桶原理”而相互匹配。
3. 有效性：安全功能既可以与计算机信息系统同步设计，也可以采用对原系统加固的方法设计。无论采用哪一种设计方法，安全功能都必须是有效的，完全起作用的，不会被绕过的。

2.2 SPLPP

该节省略了PP引言、TOE描述、PP应用注释和威胁等部分。

2.2.1 安全环境

（1）威胁

略

（2）组织安全策略

组织安全策略为一个组织为了保护其敏感信息而实施的一组规则或程序。

1. 用户授权策略：只有那些授权存取系统中信息的用户才可以访问系统，非法用户不能访问系统
2. 需知策略：限制用户对系统中受保护信息的存取，系统根据需知的原则，让授权用户访问、修改和删除其信息
3. 可记账策略
4. 信息分级策略：系统必须基于用户和信息的安全标记来控制主体对可以的存取
5. 可信路径/通道策略：系统必须在用户与TSF通信时，提供一个可信的通道信道，确保用户正在与正确的TSF通信，TSF也正在与正确的用户通信。同时，在TSF和其他可信IT产品之间建立一条可信的通道信道，提供信道两端身份的抗抵赖性性和传输数据的机密性、完整性
6. 隐蔽通道处理策略：系统要确定非预期的信道（例如非法信息流）的存在性及其潜在的容量
7. 密码服务策略：系统基于密码服务功能可以实现标识与鉴别，抗抵赖，数据传输的机密性、完整性，数据存储的机密性，完整性等服务。密码实现支持硬件、固件和软件等形式
8. 最小特权管理策略：基于安全角色的定义和管理降低由于用户在其所赋有的功能职责外采取行动、滥用职权而导致破坏的可能性，降低不适当的机制对TSF进行安全管理的威胁。

（3）假设

假设描述了TOE环境方面的安全问题，包括物理的、人员的以及互联性等方面的假设。

1. 物理环境假设：
   1. 物理位置：TOE的资源应放置在有物理控制手段的地方，避免非授权的物理接触
   2. 物理保护：TOE中实施安全策略的硬件和软件应受到保护，以避免非授权的物理改动
2. 人员假设：假定以下人员环境监理
   1. 人员管理：有一个或几个专门人员负责管理TOE及其中信息的安全性
   2. 无恶意：系统管理员应细心，没有疏忽和敌意，能够遵循和严格按照《系统管理员指南》要求配置和管理系统
   3. 用户合作：授权用户存取系统资源时，拥有必要的授权，并能够在一个良好的环境中，以合作的态度使用系统
3. 程序假设：SPLPP实施组织安全策略的能力，假设这些程序是存在的
   1. 赋予许可权：系统中存在这样的程序，授权用户能够获取指定安全级（敏感级、完整级）
   2. 确定安全级：系统中存在这样的程序，以确定所有输入系统信息的安全级，标识所有输出信息的安全级，确定所有外围设备（比如打印机、磁带机、软盘等）的安全级

2.2.2 安全目的

安全目的分为IT安全目的和Non\_IT安全目的，能够对抗所有已知威胁，和/或覆盖所有已知的组织安全策略

（1）IT安全目的

1. 用户鉴别：TSF必须确保只有授权用户才能存取TOE及其资源
2. 自主存取控制：TSF必须基于用户标识控制对资源的存取，允许授权用户能够指定哪些资源可被哪些用户存取
3. 强制存取：TSF必须基于信息和用户的敏感级、完整级来控制用户对资源的存取
4. 审计：TSF必须记录TOE内用户与安全相关的活动，并提供这些信息给授权用户
5. 客体重用：TSF必须确保受保护资源内的任何信息，在资源被重用时不会泄露
6. 管理：TSF必须为授权管理员提供所有必须的职能和工具，以管理TOE的安全性
7. 执行：TSF必须设计和实现能够确保㢟安全策略在目标环境中得到执行
8. 可信路径/通道：系统必须在用户与与TSF以及TSF与其他可信IT之间通信时，提供一个可信的通信信道
9. 最下特权管理：禁止用户在其所赋有的功能职责外采取行动、滥用职权而导致破坏的可能性，降低用不适当的机制对TSF进行安全管理的威胁
10. 密码服务：系统必须能够基于密码服务功能实现标识与鉴别，抗抵赖，数据传输的机密性、完整性、数据存储的机密性，完整性等服务

（2）Non\_I安全目的

1. 安装：必须确保TOE的分发、安装、管理和操作是否能够维护IT安全目的
2. 物理：必须确保TOE中实施安全策略的关键部分不能受到物理攻击，从而影响IT安全目的
3. 信任：必须确保TOE中所有存取证书，比如口令或其他鉴别信息，受到用户的保护，已能够维护IT安全目的

2.2.3 安全功能要求

本部分主要关于用户数据保护。

1. 自主存取控制策略：
   1. TSF应对DAC覆盖的[进程]，[文件、目录、字符设备、块设别、IPC]以及它们之间的所有操作执行自主存取控制策略
   2. TSF应确保TSC内的所有主题和客体之间的所有操作被一个确定的自主存取控制策略所覆盖
2. 自主存取控制功能：
   1. TSF应能基于一下内容对客体实施自主存取控制策略：与主体相关的用户标识和用户组关系和与客体对应的存取控制属性。存取控制属性必须能够用来对对一个或几个用户标识符/组标识符/缺省的指定允许或拒绝操作
   2. TSF应能基于以下规则来决定受控主体和受控客体之间的一个访问操作是否被允许：当受控主有相应ACL时，则基于ACL，否则基于主体的用户标识符+客体的用户组关系来判定一个操作是允许还是拒绝
   3. TSF应基于以下附加规则，授权主体对客体的访问：基于安全属性明确授权主体访问客体的规则
   4. TSF应基于以下附加规则，明确拒绝主体对客体的访问：基于安全属性明确拒绝主体访问客体的规则
3. MAC控制策略（从此开始省略，内容太多了，留到访问控制模块补充）
4. MAC控制功能
5. IAC控制策略
6. IAC控制哦功能
7. 没有安全属性的用户数据输出
8. 有安全属性的用户数据输出
9. 没有安全属性的用户数据输入
10. 有安全属性的用户数据输入
11. 客体残余信息保护
12. 主体残余信息保护

2.2.4 安全保证要求

（暂时省略）

2.2.5 基本原理

# 第四章 安胜Linux标识与鉴别机制



（1）标识功能与标识数据

确保用户的唯一性和可区别性，一般通过用户名和用户标识符UID标识一个用户。对用户名和用户标识符的管理应限定为系统的特权用户。

（2）鉴别数据

1. passwd文件（账号属性）：用户名：用户标识UID：加密口令或口令符：组标识符：真实姓名：用户主目录：用户shell
2. shadow文件（加密口令）：用户名：加密的用户口令：口令最后一次修改的日期：在所指定天数内不能修改口令：在所指定天数内必须修改口令：提前警告用户必须修改口令的天数：在账号失败前用户必须修口令的天数：账号失效的天数：保留字段

（3）鉴别功能

鉴别信息与标识信息应尽可能分开，应为鉴别信息是保密的，而用户信息是公开的。对鉴别信息的修改应限定为用户自身和特权用户。当采用口令进行鉴别时，口令在输入时应是不可见的，并在存储时加密保护。

登录进程通过输入的用户名和口令进行身份认证。

# 第三章 基于软件工程建模

由于本文的重点在于架构设计与功能分析，且存在个人能力的限制，因此本文只选用简单的瀑布模型。

2.1 可行性分析

2.2 需求分析