ICS 35.040
L 70

中华人民共和国国家标准

GB/T 18336.2—2001
idt ISO/IEC 15408-2:1999

信息技术　安全技术
信息技术安全性评估准则
第2部分:安全功能要求

Information technology—Security techniques—
Evaluation criteria for IT security—
Part 2:Security functional requirements

2001-03-08 发布　　2001-12-01 实施

国家质量技术监督局　发布

前　言

本标准等同采用国际标准 ISO/IEC15408-2:1999《信息技术　安全技术　信息技术安全性评估准则　第 2 部分:安全功能要求》。

本标准介绍了信息技术安全性评估的安全功能要求。

GB/T 18336 在总标题《信息技术　安全技术　信息技术安全性评估准则》下,由以下几个部分组成:

——第 1 部分:简介和一般模型

——第 2 部分:安全功能要求

——第 3 部分:安全保证要求

本标准的附录 A 到附录 M 是提示的附录。

本标准由国家质量技术监督局提出。

本标准由全国信息技术标准化技术委员会归口。

本标准由中国国家信息安全测评认证中心、信息产业部电子第 30 研究所、国家信息中心、复旦大学负责起草。

本标准主要起草人:吴世忠、龚奇敏、陈晓桦、李守鹏、罗建中、方关宝、吴亚飞、雷利民、张建军、叶红、吴承荣、黄元飞、任卫红、崔玉华。

本标准委托中国国家信息安全测评认证中心负责解释。

ISO/IEC 前言

ISO(国际标准化组织)和IEC(国际电工委员会)形成了全世界标准化的专门体系。作为ISO或IEC成员的国家机构,通过相应组织所建立的涉及技术活动特定领域的委员会参加国际标准的制定。ISO和IEC技术委员会在共同关心的领域里合作,其它与ISO和IEC有联系的政府和非政府的国际组织也参加了该项工作。

国际标准的起草符合ISO/IEC导则第3部分的原则。

在信息技术领域,ISO和IEC已经建立了一个联合技术委员会——ISO/IEC JTC1。联合技术委员会采纳的国际标准草案分发给国家机构投票表决。作为国际标准公开发表,需要至少75%的国家机构投赞成票。

国际标准ISO/IEC 15408-2是由联合技术委员会ISO/IEC JTC1(信息技术)与通用准则项目发起组织合作产生的。与ISO/IEC 15408-2同样的文本由通用准则项目发起组织作为《信息技术安全性评估通用准则》发表。有关通用准则项目的更多信息和发起组织的联系信息由ISO/IEC 15408-1的附录A提供。

ISO/IEC 15408在“信息技术——安全技术——信息技术安全性评估准则”的总标题下,由以下几部分组成:

第1部分:简介和一般模型

第2部分:安全功能要求

第3部分:安全保证要求

ISO/IEC 15408本部分的附录A到M仅供参考。

以下具有法律效力的提示已按要求放置在ISO/IEC 15408的所有部分:

在ISO/IEC 15408-1附录A中标明的七个政府组织(总称为通用准则发起组织),作为《信息技术安全性评估通用准则》第1至第3部分(称为“CC”)版权的共同所有者,在此特许ISO/IEC在开发ISO/IEC 15408国际标准中,非排他性地使用CC。但是,通用准则发起组织在他们认为适当时保留对CC的使用、拷贝、分发以及修改的权利。

中华人民共和国国家标准

信息技术　安全技术
信息技术安全性评估准则
第2部分：安全功能要求

GB/T 18336.2—2001
idt ISO/IEC 15408-2:1999

Information technology—Security techniques—Evaluation criteria for IT security—Part 2:Security functional requirements

1　范围

本标准定义的安全功能组件是保护轮廓(PP)或安全目标(ST)中所表述的TOE IT 安全功能要求的基础。这些要求描述了对评估对象(TOE)所期望的安全行为，目的是满足PP或ST中陈述的安全目的。这些要求描述用户通过与TOE直接交互(即输入，输出)或通过TOE对刺激的反应，可以检测到的安全特性。

安全功能组件表达用于在假定的TOE运行环境中对抗威胁的要求，或涉及所有标识的组织安全策略和假设。

本标准的读者包括安全IT系统和产品的用户、开发者和评估员。GB/T 18336第1部分第4章提供了关于本标准的目标读者，以及这些目标读者群使用本标准的附加信息。这些读者群可按如下形式使用本标准：

——用户，当选择组件来表达功能要求以满足PP或ST中的安全目的时，使用本标准。GB/T 18336第1部分5.3条给出了有关安全目的和安全要求之间关系的详细信息。

——开发者，针对实际或预期的用户安全要求建立TOE时，可以在本标准中找到理解这些安全需求的标准化方法。他们也可以将本标准的内容作为进一步定义符合这些要求的TOE安全功能和机制的基础。

——评估者，使用本标准中定义的功能要求，验证PP或ST中的TOE功能要求是否满足IT安全目的，并且应考虑所有依赖关系是否得到满足。评估者也应使用本标准内容来帮助确定给定TOE满足所陈述的要求。

1.1　功能要求的扩展和维护

本标准及在此描述的相关安全功能要求，并不打算成为所有IT安全问题的确定答案，而是提供一组广为理解的安全功能要求，用于创建反映市场需求的可信产品或系统。这些安全功能要求的给出，体现当前要求规范和评估的技术发展水平。

本标准不包括所有可能的安全功能要求，而是包含那些在发布时作者已知并认为有价值的那些要求。

因为用户的理解和需求可能会变化，因此需要维护本标准中的功能要求。PP/ST作者可能还有一些安全要求未包含在本标准功能要求组件中。此时，PP/ST的作者可考虑使用不是来自本标准的功能要求(称之为可扩展性)，参见GB/T 18336第1部分中的附录B和附录C。

1.2　本标准的结构

国家质量技术监督局2001-03-08批准　　2001-12-01实施

第 1 章是本标准的简介。

第 2 章介绍本标准功能组件的分类，第 3 章到第 13 章描述这些功能类。

附录 A 为可能使用功能组件的用户提供感兴趣的附加信息，其中包括完整的功能组件间依赖关系的交叉参照表。

附录 B 至附录 M 提供功能类的应用注释。它们是本标准用户的参考资料库，可以帮助用户应用相关的操作并选择恰当的审计或文档信息。

有关结构、规则和指南的信息，编写 PP 或 ST 的作者应参考 GB/T 18336 第 1 部分第 3 章：

——第 1 部分第 3 章，定义本标准中使用的术语。

——第 1 部分附录 B，定义 PP 的结构。

——第 1 部分附录 C，定义 ST 的结构。

1.3 功能要求范例

本条描述本标准中安全功能要求所使用的范例。图 1.1 和图 1.2 描述了范例的一些关键概念。本条为这些图和图中没有的其他关键概念提供文字描述。所讨论的关键概念以粗斜体突出表示。本条并不打算替换或取代 GB/T 18336 第 1 部分第 3 章标准术语表中的任何术语。

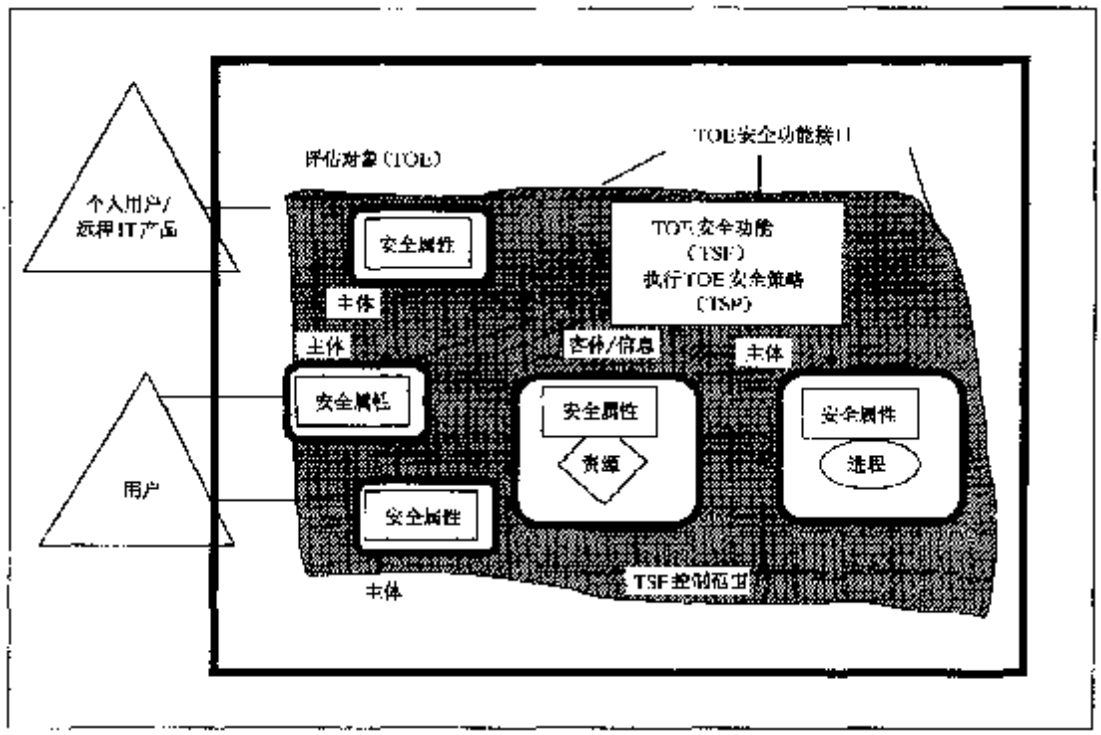


图 1.1 安全功能要求范例(单个 TOE)

本标准是一个可为**评估对象(TOE)**规定安全功能要求的目录。TOE 是包含电子存储媒体(如磁盘)、外设(如打印机)和计算能力(如 CPU 时间)等资源的 IT 产品或系统(同时带有用户和管理员指南文档)，可用于处理和存储信息，是评估的对象。

TOE 评估主要关系到：确保对 **TOE** 资源执行了规定的**TOE 安全策略(TSP)**。**TSP** 定义了一些规则，通过这些规则 **TOE** 支配对其资源的访问，这样 **TOE** 就控制了所有信息和服务。

而 TSP 又由多个**安全功能策略(SFP)**所构成。每一 SFP 有其控制范围，定义该 SFP 控制下的主体、客体和操作。SFP 由**安全功能(SF)**实现，SF 的机制执行该策略并提供必要的能力。

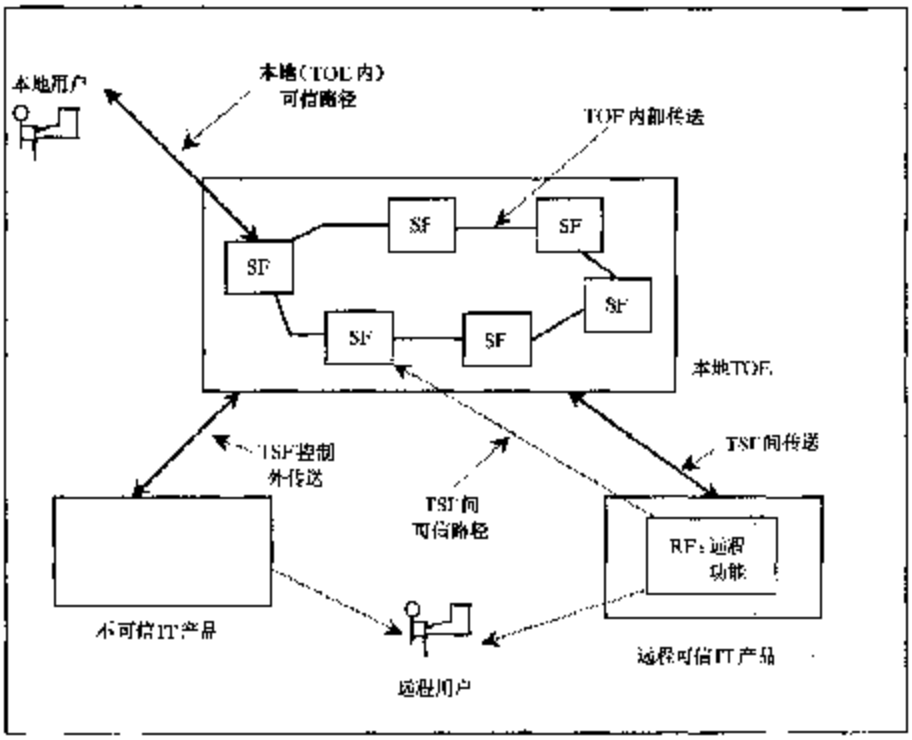


图 1.2　分布式 TOE 内的安全功能图

为正确执行 TSP 而必须依赖的 TOE 中的那些部分，统称为**TOE 安全功能(TSF)**。TSF 包括实施安全所直接或间接依赖的 TOE 中的所有软件、硬件和固件。

参照监视器是实施 TOE 的访问控制策略的抽象机。**参照确认机制**是参照监视器概念的实现，它具有以下特性：防篡改、一直运行、简单到能对其进行彻底的分析和测试。*TSF* 可能包括一个参照确认机制或 TOE 运行所需要的其他安全功能。

TOE 可能是一个包含硬件、固件和软件的单个产品，也可能是一个分布式产品，内部包括多个单独的部分，每一部分都为 TOE 提供一个特别的服务，并且通过一个**内部通信信道**与 TOE 其他部分相连接。该信道可以与处理器总线一样小，也可能包含 TOE 的一个内部网络。

当 TOE 由多个部分组成时，TOE 的每一部分可拥有自己的 TSF 部分，此部分通过内部通信信道与 TSF 的其他部分交换用户数据和 TSF 数据。这种交互称为**TOE 内部传送**。在这种情况下，这些 TSF 的分离部分抽象地形成一个复合的 TSF 来实施 TSP。

TOE 接口可能限于特定的 TOE 使用，也可能允许通过**外部通信信道**与其他 IT 产品交互。这些与其他 IT 产品的外部交互可以采取两种形式：

a) “远程可信 IT 产品”的安全策略和本地 TOE 的 TSP 已在管理上进行了协调和评估。这种情况下的信息交换称为**TSF 间传送**，如同它们是在不同可信产品的 TSF 之间。

b) 远程 IT 产品可能没有被评估，因此它的安全策略是未知的，如图 1.2 中所示的“不可信 IT 产品”。这种情况下的信息交换称为**TSF 控制外传送**，如同在远程 IT 产品中没有 TSF(或它的策略特性未知)。

可与 TOE 或在 TOE 中发生的并服从 TSP 规则的交互集合称为**TSF 控制范围(TSC)**。TSC 包括一组根据主体、客体和 TOE 内的操作定义的交互集，但不必包括 TOE 的所有资源。

一组交互式(人机接口)或编程 (应用编程接口)接口，通过它，TSF 访问、调配 TOE 资源，或者从 TSF 中获取信息，称为**TSF 接口(TSFI)**。TSFI 定义了为执行 TSP 而提供的 TOE 功能的边界。

用户在TOE的外部，因此也在TSC的外部。但为请求TOE执行服务，用户要通过TSFI和TOE交互。本标准安全功能要求关心两种用户：**个人用户和外部IT实体**。个人用户进一步分为**本地个人用户**，他们通过TOE设备(如工作站)直接与TOE交互，或**远程个人用户**，他们通过其他IT产品间接与TOE交互。

用户和TSF间的一段交互期称为用户**会话**。可以根据各种考虑来控制用户会话的建立，如：用户鉴别、时段、访问TOE的方法和每个用户允许的并发会话数。

本标准使用术语**“已授权”**来表示用户具有执行某种操作所必需的权力或特权。因此术语**“授权用户”**表示允许用户执行TSP定义的操作。

为表达需要管理员责任分离的要求，本标准相关的安全功能组件(来自子类FMT_SMR)明确说明要求管理性**角色**。角色是预先定义的一组规则，这些规则建立起用户和TOE间所允许的交互。TOE可以支持定义任意数目的角色。例如，与TOE安全运行相关的角色可能包括“审计管理员”和“用户帐号管理员”。

TOE包括可用于处理和存储信息的资源。TSF的主要目标是完全并正确地对TOE所控制的资源和信息执行TSP。

TOE资源能以多种方式结构化和利用。但是，本标准作出了特殊区分，以允许规定所期望的安全特性。所有由资源产生的实体能以两种方式中的一种来表征：实体可能是主动的，意指他们是TOE内部行为发生的原因，并导致对信息执行操作；实体也可能是被动的，意指他们是发出信息或存入信息的容器。

主动的实体称为**主体**。TOE内可能存在以下几种类型的主体：

a) 代表授权用户，遵从TSP所有规则的那些实体(例如：UNIX进程)；

b) 作为特定功能进程，可以轮流代表多个用户的那些实体(例如：在客户/服务器结构中可能找到的功能)；

c) 作为TOE自身一部分的那些实体(例如：可信进程)。

本标准所述的安全功能针对上述列出的各种主体执行TSP。

被动实体(即信息存储器)在本标准中被称作**“客体”**。客体是可以由主体执行操作的对象。在一个主体(主动实体)是某个操作的对象(例如进程间通信)的情况下，该主体也可以作为客体。

客体可以包含**信息**。在FDP类中说明信息流控制策略时，需要这个概念。

用户、主体、信息和客体具有确定的**属性**，这些属性包括使TOE正确运转的信息。有些属性，可能只是提示性信息(即，增加TOE的用户友好性)，如文件名，而另一些属性，可能专为执行TSP而存在，如访问控制信息，后面这些属性通常称为**“安全属性”**。在本标准中，属性一词将用作“安全属性”的简称，除非另有说明。但正如TSP规定的那样，无论属性信息的预期目的如何，对属性加以控制还是必要的。

TOE中的数据分为用户数据和TSF数据，图1.3表明了这种关系。**用户数据**是存储在TOE资源中的信息，用户可以根据TSP对其进行操作，而TSF对它们并不附加任何特殊的意义。例如，电子邮件消息的内容是用户数据。**TSF数据**是在进行TSP决策时TSF使用的信息。如果TSP允许的话，TSF数据可以受用户的影响。安全属性、鉴别数据以及访问控制表都是TSF数据的例子。

有几个用于数据保护的SFP，诸如**访问控制SFP**和**信息流控制SFP**。实现访问控制SFP的机制，是基于控制范围内的主体属性、客体属性和操作来决定建立他们的策略，这些属性用于控制主体可以对客体执行操作的规则集中。

实现信息流控制SFP的机制，是基于控制范围内的主体和信息的属性以及制约主体对信息操作的一组规则来决定他们的策略。信息的属性，可能与容器属性相关联(也可能没有关联，如多级数据库)，在信息移动时与其相随。

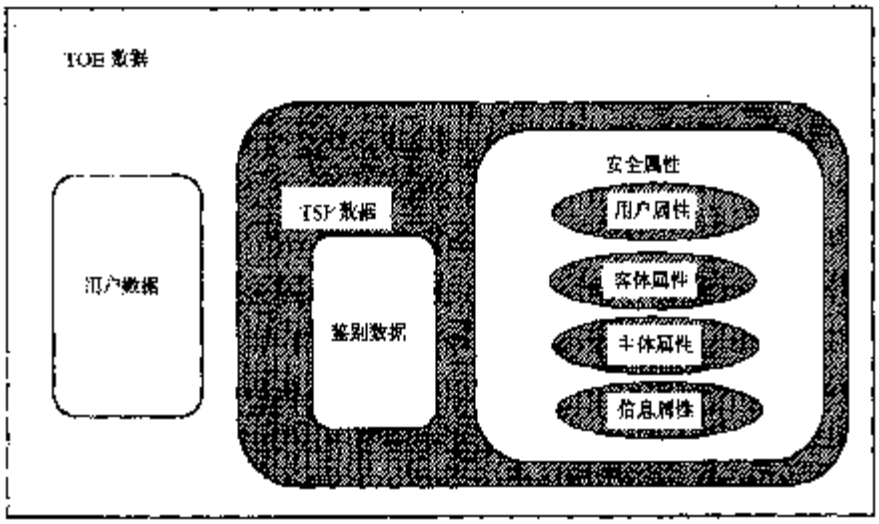


图 1.3　用户数据和TSF 数据的关系

本标准涉及的两种特殊 TSF 数据，**鉴别数据**和 **秘密**，可以是但不必一定是相同的。

鉴别数据用于验证向 TOE 请求服务的用户声明的身份。最通用的鉴别数据形式是口令。口令要成为有效的安全机制，依赖于对其进行保密。但是，不是所有形式的鉴别数据都需要保密，生物测定学鉴别设备（例如，指纹阅读器、视网膜扫描仪）就不依赖于数据保密，因为这些数据只有一个用户拥有，其他人不能伪造。

本标准功能要求中用到的术语“秘密”，对鉴别数据适用，对其他为执行一特定 SFP 而必须保密的数据也同样适用。例如，依靠密码技术保护在信道中传送信息的保密性的可信信道机制，其强度应与用来保持密钥的秘密以防止未授权泄露的方法的强度相当。

因此，不是所有的鉴别数据都需要保密；也不是所有的秘密都被用作鉴别数据。图 1.4 说明了秘密和鉴别数据间的关系。图中指出了常见的鉴别数据和秘密的数据类型。

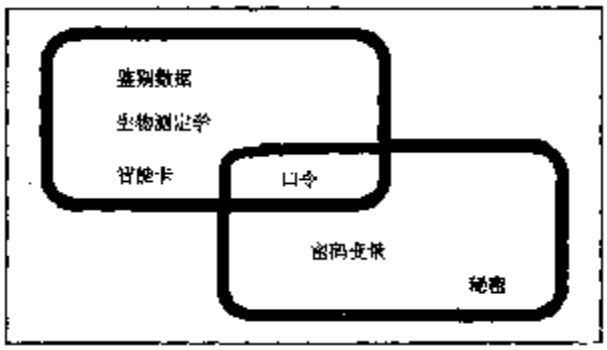


图 1.4　“鉴别数据”和“秘密”的关系

2　引用标准

下列标准所包括的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 18336.1—2001　信息技术　安全技术　信息技术安全性评估准则　第 1 部分：简介和一般模型（idt ISO/IEC 15408-1:1999）

3　安全功能组件

3.1　综述

本章定义本标准的功能要求的内容和形式，并为需要向 ST 中添加新组件的组织提供指南。功能要

求以类、子类和组件来表达。

3.1.1 类结构

图 3.1 以图表的形式阐明了功能类的结构。每个功能类包括一个类名、类介绍及一个或多个功能子类。

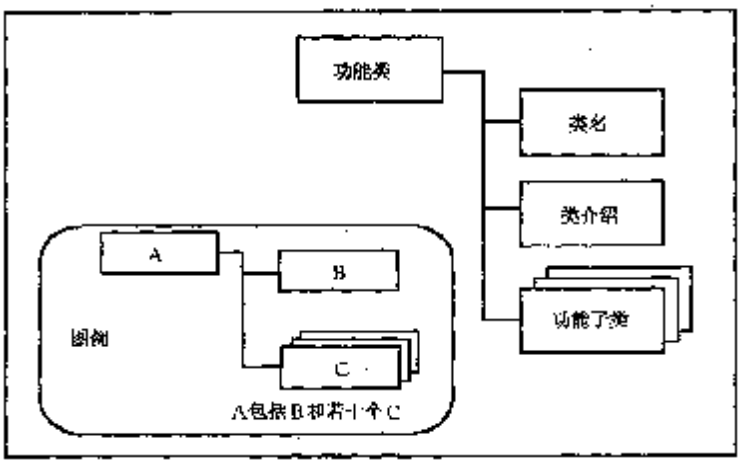


图 3.1 功能类结构

3.1.1.1 类名

类名提供标识和化分功能类所必需的信息。每个功能类都有一个唯一的名称，类的分类信息由三个字符的简名组成。类的简名用于该类中的子类的简名规范中。

3.1.1.2 类介绍

类介绍描述这些子类满足安全目标的通用意图或方法。功能类的定义不反映要求规范中的任何正式分类法。

类介绍用图来描述类中的子类和每个子类中组件的层次结构，见 3.2 条的解释。

3.1.2 子类结构

图 3.2 以框图形式说明功能子类的结构。

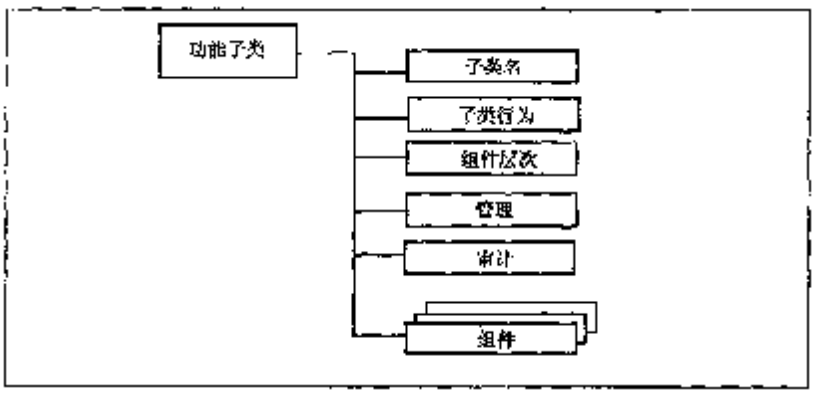


图 3.2 功能子类结构

3.1.2.1 子类名

子类名部分提供标识和化分功能子类所必需的分类和描述信息。每个功能子类有一个唯一的名称。子类的分类信息由七个字符的简名组成，开头三个字符与类名相同，后跟一个下划线和子类名，例如 XXX_YYY。唯一的简短子类名为组件提供主要的引用名。

3.1.2.2 子类行为

子类行为是对功能子类的叙述性描述，陈述其安全目的，以及对功能要求的一般描述。以下是更详细的描述：

a）子类的**安全目的**阐述在包含该子类的一个组件的 TOE 的帮助下，可以解决的安全问题；

b）**功能要求**的描述总结组件中包含的所有要求。该描述针对PP、ST 和功能包的作者，他们希望评价该子类是否与他们的特定需求相关。

3.1.2.3 组件层次

功能子类包含一个或多个组件，任何一个组件都可被选择包括在PP、ST 和功能包中。本条的目的是，一旦子类被认为是用户安全要求的一个必要或有用的部分时，向用户提供选择恰当的功能组件的信息。

功能子类描述部分描述所用组件和它们的基本原理。组件的更多细节包含在每个组件中。

功能子类内组件间的关系可能是也可能不是层次化的。如果一个组件相对另一个组件提供更多的安全，那么该组件对另一个组件来说是有层次的。

如3.2 条所述，子类的描述中提供了关于子类内组件层次结构的图示。

3.1.2.4 管理

管理要求包含PP/ST 作者应考虑的作为给定组件的管理活动的信息。管理要求在管理类(FMT)的组件里详述。

PP/ST 作者可以选择已指出的管理要求或者可以包括其他没有列出的管理要求。因而这些信息应认为是提示性的。

3.1.2.5 审计

如果PP/ST 中包含来自类FAU(安全审计)中的要求，则**审计**要求包含供PP/ST 作者选择的可审计的事件。这些要求包括按FAU _GEN(安全审计数据产生)子类的组件所支持的以各种不同详细级别表示的安全相关事件。例如，一个审计记录可能包括下述行动：最小级——安全机制的成功使用；基本级——安全机制的成功使用以及所涉及到的安全属性的相关信息；详细级——所有对机制配置的改变，包括改变前后的实际配置值。

显然可审计事件的分类是层次化的。例如，当期望“基本级审计产生”时，所有标识为最小级和基本级的可审计事件都应通过适当的赋值操作包括在PP/ST 内，只是高级事件仅仅比低级事件提供更多的细节。当期望“详细级审计产生”时，所有标识为最小级、基本级和详细级的可审计事件都应包括在PP/ST 内。

FAU 类更详尽地解释了管理审计的规则。

3.1.3 组件结构

图3.3 描绘功能组件的结构。

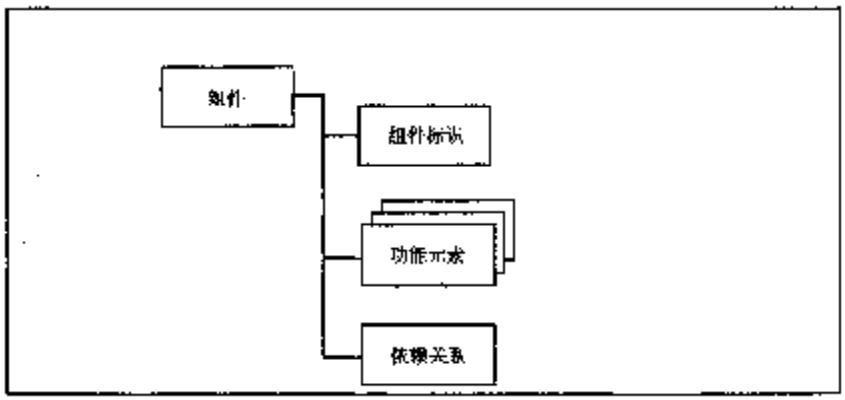


图3.3 功能组件结构

3.1.3.1 组件标识

组件标识提供标识、分类、注册和交叉引用组件时所必需的描述性信息。下列各项作为每个功能组件的部分：

一个唯一的名字，该名字反映了组件的目的。

一个简名，即功能组件名的唯一简写形式。简名作为分类、注册和交叉引用组件的主要引用名。简名反映出组件所属的类和子类以及在子类中组件的编号。

一个从属于表。这个组件所从属于的其他组件列表，以及该组件可用来满足与所列组件间的依赖关系。

3.1.3.2 功能元素

为每一组件提供了一组元素。每个元素都分别定义并且是相互独立的。

功能元素是一个安全功能要求，如果进一步划分将不会产生有意义的评估结果。它是GB/T 18336中标识和认同的最小安全功能要求。

当建立包、PP或ST时，不允许从一个组件中只选择一个或几个元素，必须选择组件的全部元素。

每个功能元素名都有一个唯一的简化形式。例如，要求名FDP_IFF.4.2意义如下：F——功能要求，DP——“用户数据保护”类，_IFF——“信息流控制功能”子类，.4——第四个组件，名为“部分消除非法信息流”，.2——该组件的第2个元素。

3.1.3.3 依赖关系

当一个组件本身不充分而要依赖于其他组件的功能，或依赖于与其他组件的交互才能正确发挥其功能时，就产生了功能组件间的依赖关系。

每个功能组件都提供一个对其他功能和保证组件的完整的依赖关系表。有些组件可能列出“无依赖关系”。所依赖的组件又可能依赖其他组件，组件中提供的列表是直接的依赖关系。这只是为该功能要求能正确完成其功能提供参考。间接依赖关系，也就是由所依赖组件产生的依赖关系，见本标准附录A。值得注意的是，在某些情况下依赖关系可在提供的多个功能要求中选择，这些功能要求中的每一个都足以满足依赖关系(例如FDP_UIT.1)。

依赖关系列表标识出，为满足与已标识组件相关的安全要求所必需的最少功能或保证组件。从属于已标识组件的那些组件也可用来满足依赖关系。

本标准指明的依赖关系是规范的，在PP/ST中它们必须得到满足。在特定的情况下这种依赖关系可能不适用，只要PP/ST作者在基本原理中说清不适用的理由，就可以在包、PP和ST中不考虑依赖的组件。

3.1.4 允许的功能组件操作

用于在PP、ST或功能包内定义要求的功能组件可以与本标准第4到第14章中说明的完全一样，也可以经裁剪以满足特定的安全目的。但是，选择和裁剪这些功能组件是复杂的，因为必须考虑所标识组件依赖关系。因此这种裁剪只限于一组允许的操作。

每个功能组件都包括一个允许的操作列表。对所有功能组件，并非一切操作都是允许的。

允许的操作选自：

——反复：采用不同的操作多次使用同一组件；

——赋值：对指定参数的说明；

——选择：对列表中的一个或多个元素的说明；

——细化：增加细节。

3.1.4.1 反复

当需要覆盖同一要求的不同方面时(如，标识一个以上类型的用户)，允许重复使用本标准的同一组件来覆盖每个方面。

3.1.4.2 赋值

某些功能组件元素包含一些参数和变量，这些参数和变量使PP/ST作者可以指定PP或ST中包含的一个策略或一组值，以满足特定的安全目的。这些元素清楚地标识出每个参数及其可以分配给该参数的值。

元素任一方面的可接受值如能无歧义地描述和列举，就可用一个参数来表述。该参数可能是一个属

性或规则，它把要求限定为一个确定的值或值的范围。例如，根据指定的安全目的，功能组件元素可以规定一给定的操作应执行数次。在这种情况下，赋值应提供用于该参数中的次数或次数范围。

3.1.4.3 选择

这是为缩小一个组件元素的范围，从列表中选取一个或多个项目的操作。

3.1.4.4 细化

对所有功能组件元素来说，为满足安全目的，允许 PP/ST 作者通过增加细节来限定可接受的实现集。元素的细化由这些增加的技术细节来组成。

在 ST 中，可能需要就 TOE 对术语“主体”和“客体”的含义作出有意义的解释，因此需要细化。

像其他操作一样，细化不增加任何完全新的要求。根据安全目的，它对要求、规则、常量和条件施以详细阐述、解释或特别的含义。细化应只是进一步限定实现要求所可能接受的功能或机制集，而不是增加要求。细化不允许建立新要求，因此不会增加与组件相关的依赖关系列表。PP/ST 作者必须注意，其他要求对该要求的依赖关系仍应得到满足。

3.2 组件分类

本标准中组件的分组不代表任何正式的分类法。

本标准包括子类和组件的分类，它们是基于相关的功能和目的的粗略分组，按字母顺序给出。每个类的开头是一个提示性框图，指出该类的分类法、类中的子类和子类中的组件。这个图对指示可能存在于组件间的层次关系是有用的。

在功能组件的描述中，有一段指出该组件和任何其他组件之间的依赖关系。

在每个类中，都有一个与图 3.4 类似的描述子类层次关系的图。在图 3.4 中，第 1 个子类(子类 1)包括了三个有从属关系的组件，其中组件 2 和组件 3 都可以用来满足对组件 1 的依赖关系。组件 3 从属于组件 2，并且可以用来满足对组件 2 的依赖关系。

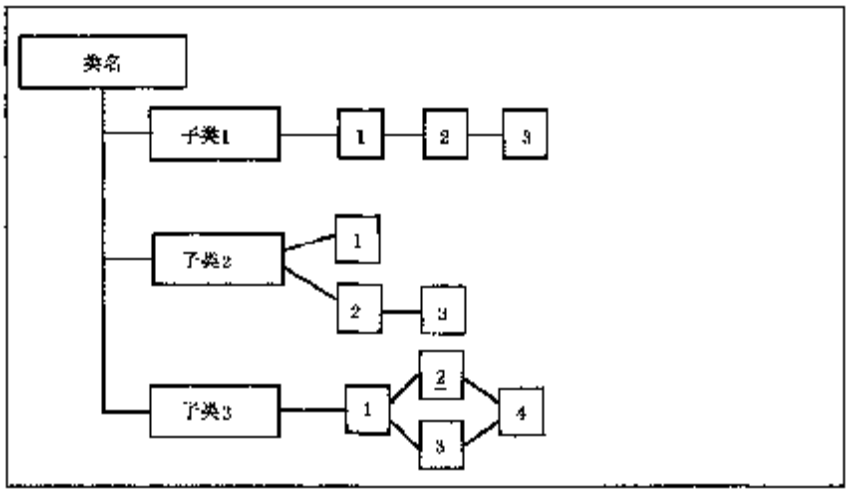


图 3.4 示范类分解图

在子类 2 中有三个组件，这三个组件不全都有从属关系。组件 1 和组件 2 不从属于其他组件。组件 3 从属于组件 2，可以用来满足对组件 2 的依赖关系，但不能满足对组件 1 的依赖关系。

在子类 3 中，组件 2、3、4 从属于组件 1。组件 2 和 3 也都从属于组件 1，但无可比性。组件 4 从属于组件 2 和 3。

这些图的目的是补充子类中的文字说明，使关系的识别更容易。它们并不取代每个组件中的“从属于：”注释，这些注释是对每个组件从属关系的强制声明。

3.2.1 突出组件变化

子类中组件的关系约定以粗体字突出表示。粗体字约定所有新的要求用粗体表示。对于有从属关系的组件，当要求或依赖关系被增强或修改而超出前一组件的要求时，要用粗体字表示。另外，超出前一

组件的任何新的或增强的允许操作，也使用粗体字突出表示。

4 FAU 类：安全审计

安全审计包括识别、记录、存储和分析那些与安全相关活动(即由 TSP 控制的活动)有关的信息。检查审计记录结果可用来判断发生了哪些安全相关活动以及哪个用户要对这些活动负责。

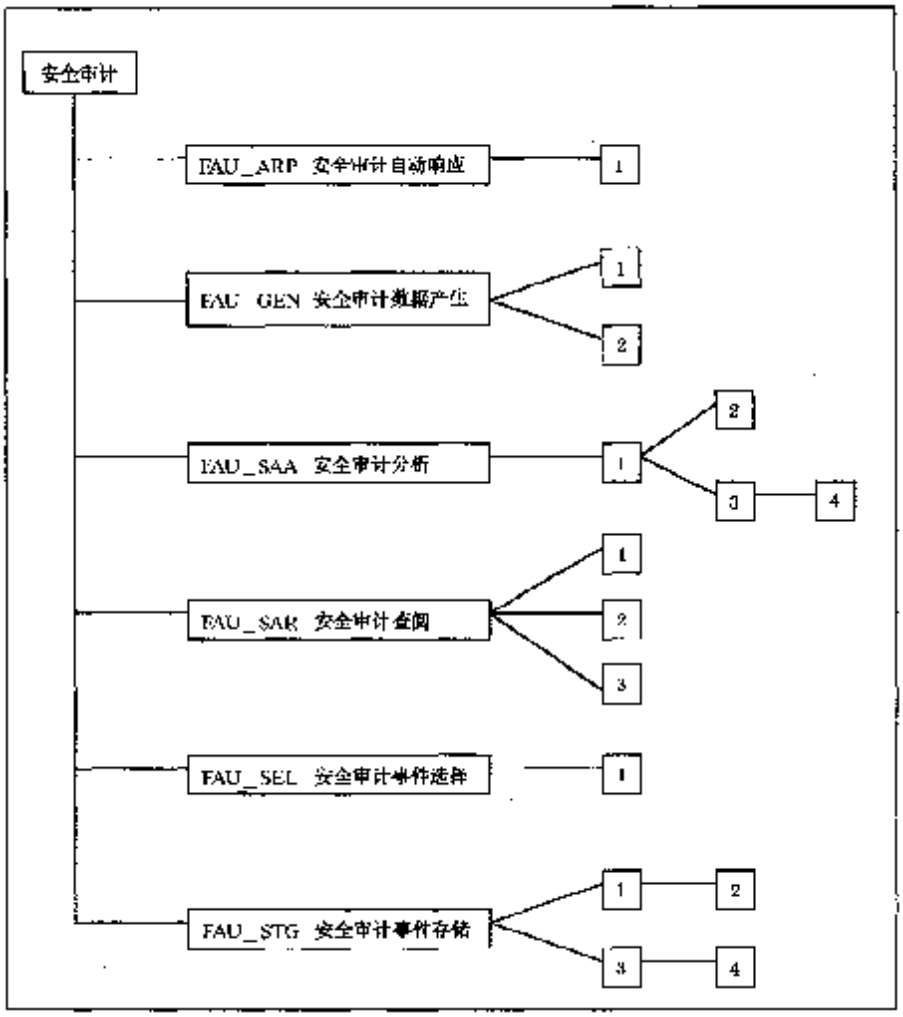


图 4.1 安全审计类分解

4.1 安全审计自动应答(FAU _ ARP)

子类行为

本子类定义在检测到的事件表明可能有安全侵害发生时作出的应答。

组件层次

对于 FAU _ ARP.1 安全警告，当检测到可能的安全侵害时 TSF 应采取行动。

管理：FAU _ ARP.1

应为 FMT 的管理功能考虑以下行动：

a）对行动的管理(添加、移去、修改)。

审计:FAU _ ARP.1

如果在PP/ST 中包括FAU _ GEN 安全审计数据产生,那么以下行动应可审计:

a）最小级:当即将发生安全侵害时采取的行动。

FAU _ ARP.1 安全警告

从属于:无其他组件。

FAU _ ARP.1.1 当检测到潜在的安全侵害时,TSF 应进行[赋值:最小扰乱行动表]。

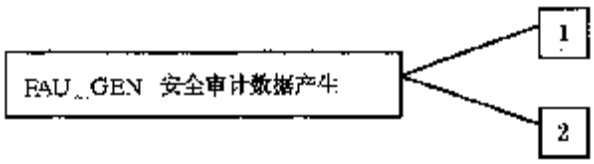
依赖关系:FAU _ SAA.1 潜在侵害分析

4.2 安全审计数据产生(FAU _ GEN)

子类行为

对于在TSF 控制下发生的安全相关事件,本子类定义了记录其出现的要求。本子类确定审计的级别,列举TSF 可审计的事件类型,以及应在各审计记录内提供的审计相关信息的最小集合。

组件层次



FAU _ GEN.1 审计数据产生定义可审计事件的级别,并规定在每个记录中将记录的数据表。

FAU _ GEN.2 用户身份关联,TSF 应把可审计事件与单个用户身份相关联。

管理:FAU _ GEN.1,FAU _ GEN.2

尚无预见的管理活动。

审计:FAU _ GEN.1,FAU _ GEN.2

如果在PP/ST 中包含FAU _ GEN 安全审计数据产生,此处不存在任何明确的可审计行动。

FAU _ GEN.1 审计数据产生

从属于:无其他组件。

FAU _ GEN.1.1 TSF 应能为下述可审计事件产生审计记录:

a）审计功能的启动和关闭;

b）在[选择:最小级,基本级,详细级,未规定]审计级别以内的所有可审计事件;

c）[赋值:其他专门定义的可审计事件]。

FAU _ GEN.1.2 TSF 应在每个审计记录中至少记录如下信息:

a）事件的日期和时间,事件类型,主体身份,事件的结果(成功或失败);

b）对每种审计事件类型,基于PP/ST 中功能组件的可审计事件定义的[赋值:其他审计相关信息]。

依赖关系:FPT _ STM.1 可信时间戳

FAU _ GEN.2 用户身份关联

从属于:无其他组件。

FAU _ GEN.2.1 TSF 应能将每个可审计事件与引起该事件的用户身份相关联。

依赖关系:FAU _ GEN.1 审计数据产生;

FIA _ UID.1 标识定时。

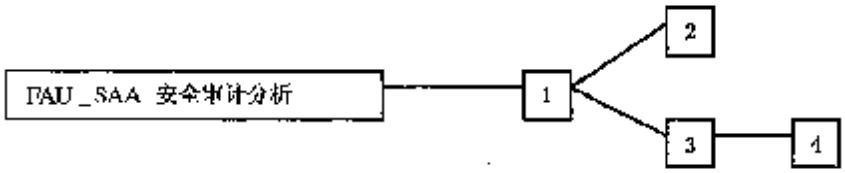
4.3 安全审计分析(FAU _ SAA)

子类行为

本子类定义,为寻找可能的或真正的安全侵害,用来分析系统活动和审计数据的自动化措施的要求。这种分析可用入侵检测来支持,或对即将来临的安全侵害作出自动应答。

基于检测结果,可采取 FAU _ ARP 子类指定的行为。

组件层次



在 FAU _ SAA.1 潜在侵害分析中,需要一个基于固定规则集的基本门限检测。

在 FAU _ SAA.2 基于轮廓的异常检测中,TSF 维护个人的系统使用轮廓,这里"轮廓"代表由**轮廓目标组**成员完成的历史使用模式。轮廓目标组是指与 TSF 交互的一个或多个人(如单个用户、共享一个身份或帐号的用户、指定角色的用户、整个系统或网络节点的用户)。轮廓目标组的每个成员都被分配给一个单独的**置疑等级**,表明成员当前的行动与轮廓中已建立的使用模式的一致程度如何。此分析可在运行期间完成,或在信息采集后的批量分析阶段完成。

FAU _ SAA.3 简单攻击探测,TSF 应能检测到那些表明对 TSP 实施将产生重大威胁的特征事件的发生。对特征事件的搜索可以实时进行,也可以在信息采集后的批量分析阶段进行。

FAU _ SAA.4 复杂攻击探测,TSF 应能描述并检测到多步骤入侵情景。TSF 应能根据已知的事件序列把系统事件(可能是由多个用户执行的)模拟成完整的入侵情景。TSF 应能指出特征事件或事件序列发生的时间,指出对 TSP 的潜在侵害。

管理:FAU _ SAA.1

应为 FMT 的管理功能考虑以下行动:

a) 通过(添加/修改/删除)规则集中的规则来维护规则。

管理:FAU _ SAA.2

应为 FMT 的管理功能考虑以下行动:

a) 对轮廓目标组中的用户组进行维护(删除/修改/添加)。

管理:FAU _ SAA.3

应为 FMT 的管理功能考虑以下行动:

a) 对系统事件的子集进行维护(删除/修改/添加)。

管理:FAU _ SAA.4

应为 FMT 的管理功能考虑以下行动:

a) 对系统事件的子集进行维护(删除/修改/添加);

b) 对系统事件的序列集进行维护(删除/修改/添加)。

审计:FAU _ SAA.1,FAU _ SAA.2,FAU _ SAA.3,FAU _ SAA.4

如果在 PP/ST 中包含了 FAU _ GEN 安全审计数据产生,那么下述行动应为可审计:

a) 最小级:开启和关闭任何分析机制;

b) 最小级:以工具完成自动应答。

FAU _SAA.1 潜在侵害分析

从属于:无其他组件。

FAU _SAA.1.1 **TSF** 应能用一系列的规则去监控审计事件,并根据这些规则指示出 **TSP** 的潜在侵害。

FAU _SAA.1.2 **TSF** 应用下列规则来监控审计事件:

a) 已知的用来指示潜在安全侵害的[赋值:已定义的可审计事件的子集]的积累或组合;

b) [赋值:任何其他规则]。

依赖关系:FAU _GEN.1 审计数据产生

FAU _SAA.2 基于轮廓的异常检测

从属于:FAU _SAA.1

FAU _SAA.2.1 TSF 应能维护系统使用轮廓。在这里个人轮廓代表[赋值:规定轮廓目标组]成员的历史使用模式。

FAU _SAA.2.2 TSF 应维护与每个用户相对应的置疑等级,这些用户的活动已记录在轮廓中。在这里,“置疑等级”代表用户当前活动与轮廓中已建立的使用模式不一致的程度。

FAU _SAA.2.3 当用户的置疑等级超过门限条件[赋值:**TSF** 报告“异常”的条件]时,**TSF** 应能指出即将发生对 **TSP** 的侵害。

依赖关系:FIA _UID.1 标识定时

FAU _SAA.3 简单攻击探测

从属于:FAU _SAA.1

FAU _SAA.3.1 **TSF** 应能维护预示对 **TSP** 侵害的以下特征事件[赋值:系统事件的一个子集]的内部表示。

FAU _SAA.3.2 **TSF** 应根据系统活动的记录来比较特征事件,这里系统活动可以通过对[赋值:用来决定系统活动的信息]检查而辨明。

FAU _SAA.3.3 当一个系统事件被发现与一个预示对 **TSP** 的潜在攻击的特征事件匹配时,**TSF** 应指出对 **TSP** 的攻击即将到来。

依赖关系:无依赖关系。

FAU _SAA.4 复杂攻击探测

从属于:FAU _SAA.3

FAU _SAA.4.1 TSF 应能维护**已知入侵情景的事件序列**[赋值:已知攻击出现的系统事件序列表]和预示对 TSP 的潜在攻击的特征事件[赋值:系统事件的一个子集]的内部表示。

FAU _SAA.4.2 TSF 应比较系统活动的记录与特征事件**和事件序列**,这里的系统活动可以通过对[赋值:用来决定系统活动的信息]检查来辨明。

FAU _SAA.4.3 当一个**系统事件或事件序列**被发现与一个预示对 TSP 的潜在攻击的特征事件匹配时,TSF 应能指示出对 TSP 的攻击即将到来。

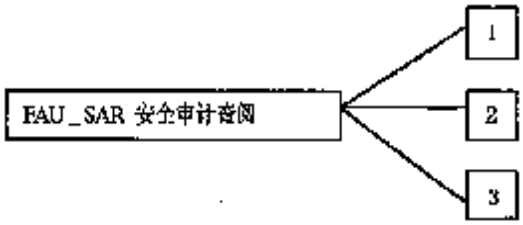
依赖关系:无依赖关系。

4.4 安全审计查阅(FAU _SAR)

子类行为

本子类定义了为授权用户查阅审计数据提供审计工具的要求。

组件层次



FAU_SAR.1 审计查阅,提供从审计记录中读取信息的能力。

FAU_SAR.2 有限审计查阅,要求除在FAU_SAR.1中确定的用户外,其他用户不能读取信息。

FAU_SAR.3 可选审计查阅,要求审计查阅工具根据条件来选择要查阅的审计数据。

管理:FAU_SAR.1

应为FMT的管理功能考虑以下行动:

a) 维护(删除/修改/添加)对审计记录有读访问权的用户组。

管理:FAU_SAR.2,FAU_SAR.3

尚无预见的管理活动。

审计:FAU_SAR.1

如果在PP/ST中包含了FAU_GEN安全审计数据产生,那么下述行为应为可审计:

a) 基本级:从审计记录中读取信息。

审计:FAU_SAR.2

如果在PP/ST中包含了FAU_GEN安全审计数据产生,那么下述行为应为可审计:

a) 基本级:尝试从审计记录中读取信息而未成功。

审计:FAU_SAR.3

如果在PP/ST中包含了FAU_GEN安全审计数据产生,那么下述行为应为可审计:

a) 详细级:用于查阅的各种参数。

FAU_SAR.1 审计查阅

本组件应为授权用户提供获得和解释信息的能力。用户是人时必须以人类可理解的方式表示信息;用户是外部IT实体时必须以电子方式无歧义地表示信息。

从属于:无其他组件。

FAU_SAR.1.1 TSF应为[赋值:授权用户]提供从审计记录中读取[赋值:审计信息列表]的能力。

FAU_SAR.1.2 TSF应以便于用户理解的方式提供审计记录。

依赖关系:FAU_GEN.1 审计数据产生

FAU_SAR.2 有限审计查阅

从属于:无其他组件。

FAU_SAR.2.1 除具有明确读访问权限的用户外,TSF应禁止所有用户对审计记录的读访问。

依赖关系:FAU_SAR.1 审计查阅

FAU_SAR.3 可选审计查阅

从属于:无其他组件。

FAU_SAR.3.1 TSF应根据[赋值:具有逻辑关系的条件]提供对审计数据进行[选择:搜索、分类、排序]的能力。

依赖关系:FAU _SAR.1 审计查阅

4.5 安全审计事件选择(FAU _SEL)

子类行为

本子类定义,在TOE 运行期间选择事件来审计的要求。它定义向可审计事件集中加入或从中排除事件的要求。

组件层次

FAU _SEL.1 选择性审计,要求根据由PP/ST 作者规定的属性包括或排除来自审计事件集中事件的可能。

管理:FAU _SEL.1

应为FMT 的管理功能考虑以下行动:

a)维护查阅/修改审计的权限。

审计:FAU _SEL.1

如果在PP/ST 中包含了FAU _GEN 安全审计数据产生,那么下述行为应是可审计的:

a) 最小级:对审计收集功能正在运行时出现的审计配置的所有修改。

FAU _SEL.1 选择性审计

从属于:无其他组件。

FAU _SEL.1.1 TSF 根据以下属性包括或排除审计事件集中的可审计事件:

a) [选择:客体身份,用户身份,主体身份,主机身份,事件类型]

b) [赋值:作为审计选择性依据的附加属性表]

依赖关系: FAU _GEN.1 审计数据产生

FMT _MTD.1 TSF 数据管理

4.6 安全审计事件存储(FAU _STG)

子类行为

本子类定义TSF 能够创建并维护安全审计迹的要求。

组件层次

FAU _STG.1 受保护的审计迹存储,该要求保护审计迹避免未授权的删除或修改。

FAU _STG.2 审计数据可用性保证,规定TSF 在意外情况出现时对审计数据维护的保证。

FAU _STG.3 在审计数据可能丢失的情况下的行为,规定当超出审计迹门限时所采取的行动。

FAU _STG.4 防止审计数据丢失,规定当审计迹溢满时的行为。

管理:FAU _STG.1

尚无预见的管理活动。

管理:FAU _STG.2

应为FMT 的管理功能考虑以下行为:

a) 维护控制审计存储能力的参数

管理:FAU _STG.3

应为FMT 的管理功能考虑以下行为:

a) 维护门限值;

b) 即将发生审计存储失败时,维护(删除/修改/添加)相应的行为。

管理:FAU _STG.4

应为FMT 的管理功能考虑以下行为:

a)审计存储失败时,维护(删除/修改/添加)相应的行为。

审计:FAU _STG.1,FAU _STG.2

如果在PP/ST 中包含了FAU _GEN 安全审计数据产生,此处就没有可审计的确定行为。

审计:FAU _STG.3

如果在PP/ST 中包含了FAU _GEN 安全审计数据产生,那么下述行为应是可审计的:

a) 基本级:因超过门限而采取的行动。

审计:FAU _STG.4

如果在PP/ST 中包含了FAU _GEN 安全审计数据产生,那么下述行为应是可审计的:

a) 基本级:因审计存储失败而采取的行动。

FAU _STG.1 受保护的审计迹存储

从属于:无其他组件。

FAU _STG.1.1 TSF 应保护所存储的审计记录,以避免未授权的删除。

FAU _STG.1.2 TSF 应能[选择:防止,检测]对审计记录的修改。

依赖关系:FAU _GEN.1 审计数据产生

FAU _STG.2 审计数据可用性保证

从属于:FAU _STG.1

FAU _STG.2.1 TSF 应保护所存储的审计记录,以避免未授权的删除。

FAU _STG.2.2 TSF 应能[选择:防止,检测]对审计记录的修改。

FAU _STG.2.3 当下述情况发生时:[选择:审计存储耗尽、失败、受攻击],TSF 应确保审计记录[赋值:保存审计记录的量度]不被破坏。

依赖关系:FAU _GEN.1 审计数据产生

FAU _STG.3 在审计数据可能丢失情况下的行为

从属于:无其他组件。

FAU _STG.3.1 如果审计迹超过[赋值:预定的限制],TSF 应采取[赋值:在审计数据可能丢失情况下的行为]。

依赖关系:FAU _STG.1 受保护的审计迹存储

FAU _STG.4 防止审计数据丢失

从属于:FAU _STG.3

FAU _STG.4.1 如果审计迹已满,TSF 应[选择:‘忽略可审计事件’,‘阻止产生除有特权的授权用户外的所有可审计事件’,‘覆盖所存储的最早的审计记录’]并进行[赋值:一旦审计存

储失败所采取的其他行动]。

依赖关系:FAU _STG.1　受保护的审计迹存储

5　FCO 类:通信

本类提供两个子类,专门用以确保在数据交换中参与方的身份。这些子类与确保信息传送的发起者的身份(原发证明)和确保信息传送的接收者的身份(接收证明)相关。这些子类既确保发起者不能否认发送过信息,又确保收信者不能否认收到过信息。

本类的组件构成分解如图 5.1 所示:

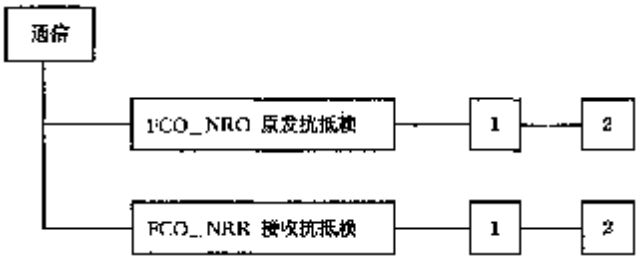


图 5.1　通信类分解

5.1　原发抗抵赖(FCO _NRO)

子类行为

原发抗抵赖确保信息的发起者不能成功地否认曾经发送过信息。本子类要求 TSF 提供一种方法来确保,接收信息的主体在数据交换期间获得了证明信息原发的证据,此证据可由该主体或其他主体验证。

组件层次

FCO _NRO.1　选择性原发证明,要求 TSF 为主体提供请求原发信息证据的能力。

FCO _NRO.2　强制原发证明,要求 TSF 总是对传送信息产生原发证据。

管理:FCO _NRO.1,FCO _NRO.2

应为 FMT 的管理功能考虑以下行动:

a) 对改变信息类型、域、原发者属性和证据接收者的管理。

审计:FCO _NRO.1

如果在 PP/ST 中包含了 FAU _GEN 安全审计数据产生,那么下述行动应为可审计:

a) 最小级:请求产生原发证据的用户的身份;

b) 最小级:调用抗抵赖服务;

c) 基本级:标识所提供证据的信息、目的地及其拷贝;

d) 详细级:请求验证证据的用户的身份。

审计:FCO _NRO.2

如果在 PP/ST 中包含了 FAU _GEN 安全审计数据产生,那么下述行动应为可审计:

a) 最小级:调用抗抵赖服务;

b) 基本级:标识所提供证据的信息、目的地及其拷贝;

c) 详细级:请求验证证据的用户的身份。

FCO _ NRO.1 选择性原发证明

从属于:无其他组件。

FCO _ NRO.1.1 在[选择:原发者、接收者或[赋值:第三方列表]]请求时,TSF 应能对传送的[赋值:信息类型表]产生原发证据。

FCO _ NRO.1.2 TSF 应能将信息原发者的[赋值:属性表],与证据适用的信息的[赋值:信息域表]相关联。

FCO _ NRO.1.3 TSF 应能为给定[赋值:原发证据的限制]的[选择:原发者、接收者或[赋值:第三方列表]]提供验证信息原发证据的能力。

依赖关系:FIA _ UID.1 标识定时

FCO _ NRO.2 强制原发证明

从属于:FCO _ NRO.1

FCO _ NRO.2.1 TSF 在任何时候都应对[赋值:信息类型表]强制产生原发证据。

FCO _ NRO.2.2 TSF 应能使信息原发者的[赋值:属性表],与证据适用的信息的[赋值:信息域表]相关联。

FCO _ NRO.2.3 TSF 应能为给定[赋值:原发证据的限制]的[选择:原发者、接收者,[赋值:第三方列表]]提供验证信息原发证据的能力。

依赖关系:FIA _ UID.1 标识定时

5.2 接收抗抵赖(FCO _ NRR)

子类行为

接收抗抵赖确保信息的接收者不能成功地否认对信息的接收。本子类要求 TSF 提供一种方法来确保,发送信息的主体在数据交换期间获得了证明信息接收的证据,此证据可由该主体或其他主体验证。

组件层次

FCO _ NRR.1 选择性接收证明,要求 TSF 为主体提供请求信息接收证据的能力。

FCO _ NRR.2 强制性接收证明,要求 TSF 总是对接收到的信息产生接收证据。

管理:FCO _ NRR.1,FCO _ NRR.2

应为 FMT 的管理功能考虑以下行动:

a) 对改变信息类型、域、原发者属性和证据的第三方接收者的管理。

审计:FCO _ NRR.1

如果在 PP/ST 中包含了 FAU _ GEN 安全审计数据产生,那么下述行动应可审计:

a) 最小级:请求产生提供接收证据的用户的身份;

b) 最小级:调用抗抵赖服务;

c) 基本级:标识所提供证据的信息、目的地及其拷贝;

d) 详细级:请求验证证据的用户的身份。

审计:FCO _ NRR.2

如果在 PP/ST 中包含了 FAU _ GEN 安全审计数据产生,那么下述行动应可审计:

a) 最小级:调用抗抵赖服务;

b) 基本级:标识所提供证据的信息、目的地及其拷贝;

c) 详细级：请求验证证据的用户的身份。

FCO _NRR.1　选择性接收证明

从属于：无其他组件。

FCO _NRR.1.1　在[选择：原发者、接收者或[赋值：第三方列表]]请求时，**TSF** 应能对接收的[赋值：信息类型表]产生接收证据。

FCO _NRR.1.2　**TSF** 应使将信息接收者的[赋值：属性表]，与证据适用的信息的[赋值：信息域表]相关联。

FCO _NRR.1.3　**TSF** 应能为给定[赋值：接收证据的限制]的[选择：原发者、接收者或[赋值：第三方列表]]提供验证信息接收证据的能力。

依赖关系：**FIA _UID.1**　标识定时

FCO _NRR.2　强制接收证明

从属于：**FCO _NRR.1**

FCO _NRR.2.1　**TSF** 应对收到的[赋值：信息类型表]强制产生接收证据。

FCO _NRR.2.2　**TSF** 应能使信息接收者的[赋值：属性表]与证据适用的信息的[赋值：信息域表]相关联。

FCO _NRR.2.3　**TSF** 应能为给定[赋值：接收证据的限制]的[选择：原发者、接收者或[赋值：第三方列表]]提供验证信息接收证据的能力。

依赖关系：**FIA _UID.1**　标识定时

6　FCS 类：密码支持

TSF 可以利用密码功能来满足一些高级安全目的。这些功能包括(但不限于)：标识与鉴别，抗抵赖，可信路径，可信信道和数据分离。本类可用硬件、固件或软件来实现，在 **TOE** 执行密码功能时使用。

FCS 类由两个子类组成：**FCS _CKM** 密钥管理和 **FCS _COP** 密码运算。**FCS _CKM** 子类解决密钥管理方面的问题，而 **FCS _COP** 子类则与密钥在运算中的使用情况有关。

本类的组件分解如图 6.1 所示：

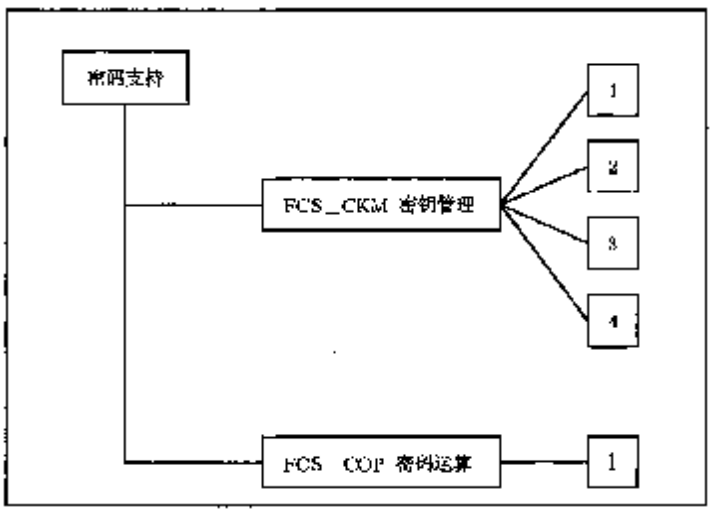


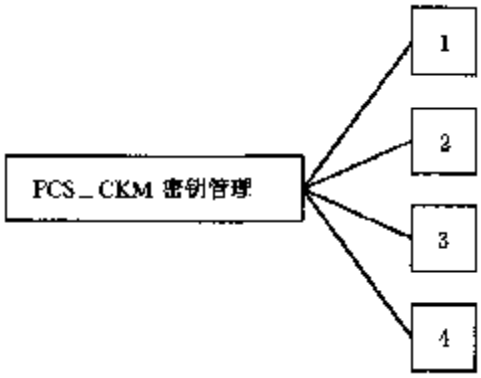
图 6.1　密码支持类分解

6.1 密钥管理(FCS _ CKM)

子类行为

密钥在其整个生存期内都必须进行管理。为此,本子类定义了对以下几种操作的要求:密钥产生,密钥分配,密钥访问和密钥销毁。凡是存在对密钥进行管理的功能要求时,都必须包含本子类。

组件层次



FCS _ CKM.1 密钥产生,要求根据基于某个指定标准的特定的算法和密钥长度来产生密钥。

FCS _ CKM.2 密钥分配,要求根据基于某个指定标准的特定的分配方法来分配密钥。

FCS _ CKM.3 密钥访问,要求根据基于某个指定标准的特定的访问方法来访问密钥。

FCS _ CKM.4 密钥销毁,要求根据基于某个指定标准的特定的销毁方法来销毁密钥。

管理:FCS _ CKM.1,FCS _ CKM.2,FCS _ CKM.3,FCS _ CKM.4

应为 FMT 的管理功能考虑以下行动:

a) 对修改密钥属性的管理。比如,密钥属性包括:用户、密钥类型(如公开密钥、私有密钥、秘密密钥)、有效期和使用(如数字签名、密钥加密、密钥协商、数据加密)。

审计:FCS _ CKM.1,FCS _ CKM.2,FCS _ CKM.3,FCS _ CKM.4

如果在 PP/ST 中包含了 FAU _ GEN 安全审计数据产生,那么下述行动应是可审计的:

a) 最小级:操作成功和失败;

b) 基本级:除一切敏感信息(如秘密密钥或私有密钥)外的客体属性和客体值。

FCS _ CKM.1 密钥产生

从属于:无其他组件。

FCS _ CKM.1.1 TSF 应根据符合下述标准[赋值:标准列表]的特定的密钥产生算法[赋值:密钥产生算法]和特定的密钥长度[赋值:密钥长度]来产生密钥。

依赖关系:[FCS _ CKM.2 密钥分配

FCS _ COP.1 密码运算]

FCS _ CKM.4 密钥销毁

FMT _ MSA.2 保密的安全属性

FCS _ CKM.2 密钥分配

从属于:无其他组件。

FCS _ CKM.2.1 TSF 应根据符合标准[赋值:标准列表]的特定的密钥分配方法[赋值:密钥分配方法]来分配密钥。

依赖关系:[FDP _ ITC.1 不带安全属性的用户数据输入
FCS _ CKM.1 密钥产生]
FCS _ CKM.4 密钥销毁
FMT _ MSA.2 保密的安全属性

FCS _ CKM.3 密钥访问
从属于:无其他组件。
FCS _ CKM.3.1 TSF 应根据符合标准[赋值:标准列表]的特定的密钥访问方法[赋值:密钥访问方法]来执行[赋值:密钥访问类型]。
依赖关系:[FDP _ ITC.1 不带安全属性的用户数据输入
FCS _ CKM.1 密钥产生]
FCS _ CKM.4 密钥销毁
FMT _ MSA.2 保密的安全属性

FCS _ CKM.4 密钥销毁
从属于:无其他组件。
FCS _ CKM.4.1 TSF 应根据符合标准[赋值:标准列表]的特定的密钥销毁方法[赋值:密钥销毁方法]来销毁密钥。
依赖关系:[FDP _ ITC.1 不带安全属性的用户数据输入
FCS _ CKM.1 密钥产生]
FMT _ MSA.2 保密的安全属性

6.2 密码运算(FCS _ COP)

子类行为

为了保证密码运算的功能正确,必须按照特定的算法和一定长度的密钥来运算。凡有执行密码运算要求的,都需包含本子类。

密码运算通常包括:数据加密或解密、数字签名产生或验证、针对完整性的密码校验和产生或校验和检验、安全散列(信息摘要)、密钥加密或解密,以及密钥协商。

组件层次

FCS _ COP.1 密码运算,要求根据基于指定标准的特定的算法和特定长度的密钥来进行密码运算。
管理:FCS _ COP.1
尚无预见的管理活动。
审计:FCS _ COP.1
如果在 PP/ST 中包含了 FAU _ GEN 安全审计数据产生,那么下述行动应是可审计的:
a) 最小级:密码运算的成功、失败和类型;
b) 基本级:所有有效的密码运算模式、主体属性和客体属性。

FCS _ COP.1　密码运算

从属于：无其他组件。

FCS _ COP.1.1　TSF 应根据符合标准[赋值：标准列表]的特定的密码算法[赋值：密码算法]和密钥长度[赋值：密钥长度]来执行[赋值：密码运算列表]。

依赖关系：[FDP _ ITC.1 不带安全属性的用户数据输入

FCS _ CKM.1　密钥产生]

FCS _ CKM.4　密钥销毁

FMT _ MSA.2　保密的安全属性

7　FDP 类：用户数据保护

本类包含若干子类，这些子类规定了与保护用户数据相关的 TOE 安全功能要求和 TOE 安全功能策略。FDP 分为四组子类(将在下面列出)，这些子类处理 TOE 内部在输入、输出和存储期间的用户数据，以及和用户数据直接相关的安全属性。

本类中的子类分成以下四组：

a) 用户数据保护安全功能策略：

——FDP _ ACC 访问控制策略；

——FDP _ IFC 信息流控制策略。

这些子类中的组件允许 PP/ST 作者命名用户数据保护安全功能策略，并定义该安全策略的控制范围，这对于说明安全目的是必要的。这些安全策略的名字将在所有余下的选择“访问控制 SFP”或“信息流控制 SFP”或为其赋值的功能组件中使用。已命名的访问控制和信息流控制 SFP 功能的规则将分别在 FDP _ ACF 和 FDP _ IFF 子类中定义。

b) 用户数据保护形式：

——FDP _ ACF 访问控制功能；

——FDP _ IFF 信息流控制功能；

——FDP _ ITT 内部 TOE 传送；

——FDP _ RIP 残余信息保护；

——FDP _ ROL 反转；

——FDP _ SDI 存储数据的完整性。

c) 脱机存储、输入和输出：

——FDP _ DAU 数据鉴别；

——FDP _ ETC 输出到 TSF 控制之外；

——FDP _ ITC 从 TSF 控制之外输入。

这些子类内的组件说明进出安全功能控制范围时的可信传送。

d) TSF 间的通信：

——FDP _ UCT　TSF 间用户数据传送的保密性保护；

——FDP _ UIT　TSF 间用户数据传送的完整性保护。

这些子类内的组件说明 TOE 的 TSF 与其他可信 IT 产品间的通信。

图 7.1 和 7.2 是本类的组件分解图。

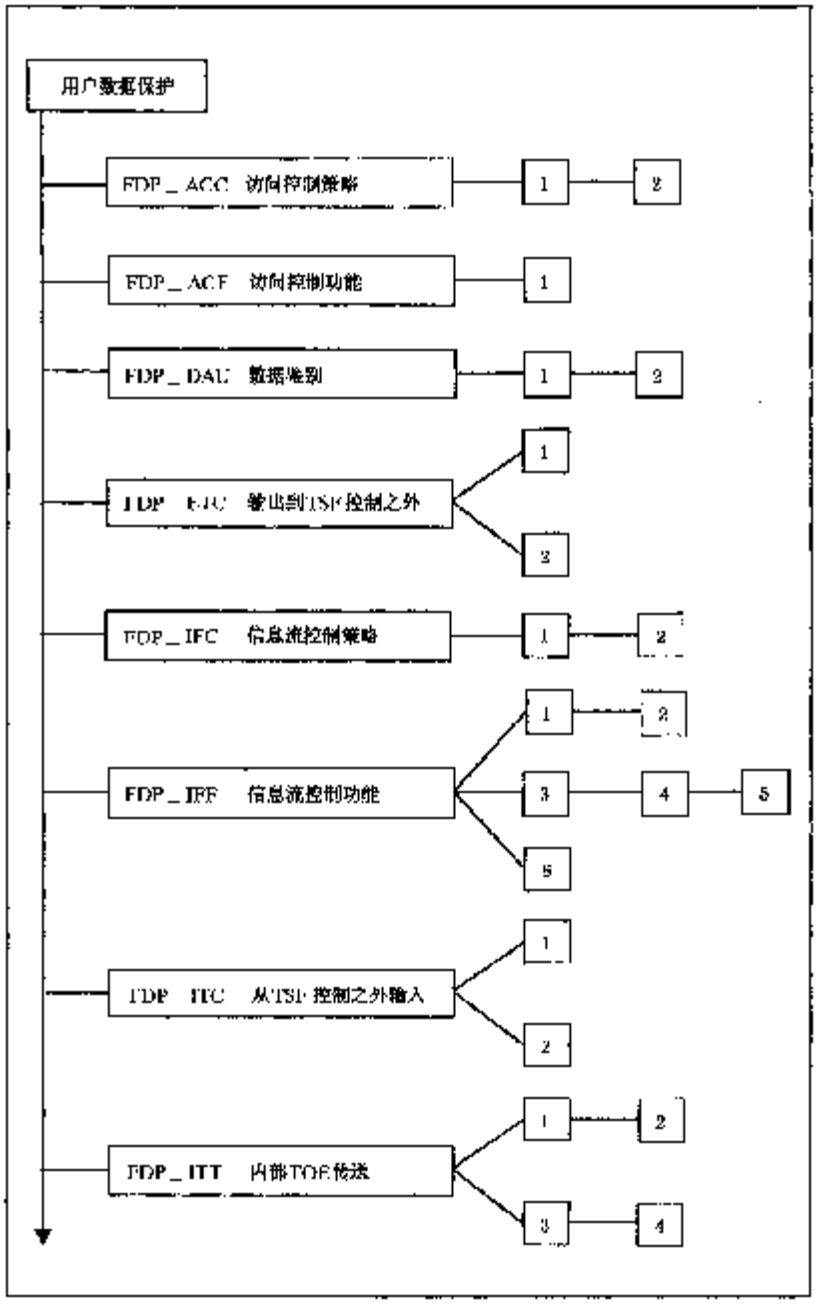


图 7.1　用户数据保护类分解

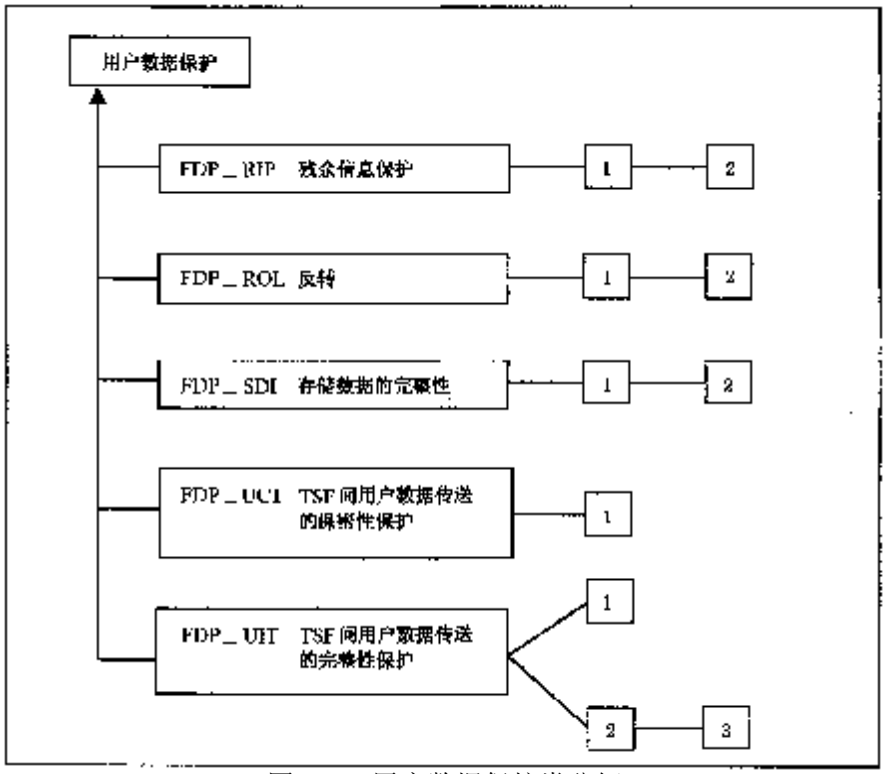


图 7.2 用户数据保护类分解

7.1 访问控制策略(FDP_ACC)

子类行为

本子类(通过名字)确定访问控制 SFP 及其控制范围,这些策略组成了所确定的 TSP 的访问控制部分。该控制范围包括三部分:策略控制下的主体、策略控制下的客体以及策略所覆盖的受控主体和受控客体间的操作。本准则允许存在多个策略,每个策略有一个唯一的名字。可通过为每个命名的访问控制策略反复使用本子类中的组件来实现。定义访问控制 SFP 功能的规则将在其他子类中定义,如 FDP_ACF 和 FDP_SDI。在 FDP—ACC 中所确定的访问控制 SFP 的名字将在所有余下的选择"访问控制 SFP"或为其赋值的功能组件中使用。

组件层次

FDP_ACC.1 子集访问控制,要求每个确定的访问控制 SFP 适用于某个 TOE 客体子集上可能的操作子集。

FDP_ACC.2 完全访问控制,要求每个确定的访问控制 SFP 覆盖所有被该 SFP 覆盖的所有主体和客体之间的操作。它甚至要求 TSC 内的所有客体和操作都至少被一个确定的访问控制 SFP 所覆盖。

管理:FDP_ACC.1,FDP_ACC.2

本组件没有可预见的管理活动。

审计:FDP_ACC.1,FDP_ACC.2

如果 PP/ST 包括了 FAU_GEN 安全审计数据产生,那么就没有确定的可审计事件。

FDP _ ACC.1　子集访问控制

从属于:无其他组件。

FDP _ ACC.1.1　**TSF** 应对[赋值: **SFP** 覆盖的主体列表、客体列表及其他们之间的操作列表]执行[赋值:访问控制 **SFP**]。

依赖关系:FDP _ ACF.1　基于安全属性的访问控制

FDP _ ACC.2　完全访问控制

从属于:FDP _ ACC.1

FDP _ ACC.2.1 TSF 应对[赋值:**SFP** 覆盖的主体列表和客体列表]以及它们之间的所有操作执行[赋值:访问控制 SFP]。

FDP _ ACC.2.2　**TSF** 应确保 **TSC** 内的所有主体和客体之间的所有操作将被一个访问控制 **SFP** 所覆盖。

依赖关系:FDP _ ACF.1　基于安全属性的访问控制

7.2　访问控制功能(FDP _ ACF)

子类行为

本子类描述能实现 FDP _ ACC 中所命名的访问控制策略的特定功能的规则。FDP _ ACC 规定了策略控制的范围。

组件层次

本子类说明这些策略的特征以及如何使用安全属性。本组件将用来描述功能规则,以实现 FDP _ ACC 中确定的 SFP。PP/ST 作者可以反复使用本组件以说明 TOE 中的多个策略。

FDP _ ACF.1　基于安全属性的访问控制允许 TSF 执行基于安全属性和命名属性组的访问控制。此外,TSF 有能力根据安全属性明确地授权或拒绝对某个对象的访问。

管理:FDP _ ACF.1

对于 FMT 管理中的管理功能,应考虑以下的活动:

a) 管理用于作出明确访问或拒绝访问决策的属性。

审计:FDP _ ACF.1

如果 PP/ST 包括 FAU _ GEN 安全审计数据产生,则以下事件应可审计:

a) 最小级:对 SFP 覆盖的客体执行某操作的成功请求;

b) 基本级:对 SFP 覆盖的客体执行某操作的所有请求;

c) 详细级:用于进行访问检查的特定安全属性。

FDP _ ACF.1　基于安全属性的访问控制

从属于:无其他组件。

FDP _ ACF.1.1 **TSF** 应基于[赋值:安全属性、命名的安全属性组]对客体执行[赋值:访问控制 **SFP**]。

FDP _ ACF.1.2　**TSF** 应执行以下规则,以决定受控主体与受控客体间的操作是否被允许:[赋值:在受控主体和受控客体中,通过对受控客体采取受控操作来管理访问的规则]。

FDP _ ACF.1.3　**TSF** 应基于以下附加规则:[赋值:基于安全属性明确授权主体访问客体的规则],授权主体对客体的访问。

FDP _ ACF.1.4 TSF 应基于[赋值:基于安全属性明确拒绝主体访问客体的规则] 明确拒绝主体对客体的访问。

依赖关系:FDP _ ACC.1 子集访问控制

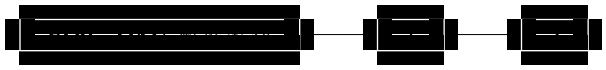
FMT _ MSA.3 静态属性初始化

7.3 数据鉴别(FDP _ DAU)

子类行为

数据鉴别允许一个实体承担信息真实性的责任(如,通过数字签名)。本子类提供一种方法,以保证特定数据单元的有效性,并进而验证信息内容没有被伪造或篡改。与FCO 类不同,本子类用于"静态"数据而不是正在传送的数据。

组件层次



FDP _ DAU.1 基本数据鉴别,要求 TSF 能够保证客体(如文档)信息内容的真实性。

FDP _ DAU.2 伴有保证者身份的数据鉴别,还另外要求TSF 能够产生提供真实性保证的主体身份。

管理:FDP _ DAU.1,FDP _ DAU.2

对于FMT 管理中的管理功能,应考虑以下活动:

a) 系统中,要对其进行数据鉴别的客体,其赋值和修改应是可配置的。

审计:FDP _ DAU.1

如果PP/ST 包括FAU _ GEN 安全审计数据产生,则以下事件应可审计:

a) 最小级:有效证据的成功生成;

b) 基本级:有效证据未成功生成;

c) 详细级:请求证据的主体身份。

审计:FDP _ DAU.2

如果PP/ST 包括FAU _ GEN 安全审计数据产生,则以下事件应可审计:

a) 最小级:有效证据的成功生成;

b) 基本级:有效证据未成功生成;

c) 详细级:请求证据的主体身份;

d) 详细级:产生证据的主体身份。

FDP _ DAU.1 基本数据鉴别

从属于:无其他组件。

FDP _ DAU.1.1 TSF 应提供产生保证[赋值:客体列表或信息类型列表]的有效性证据的能力。

FDP _ DAU.1.2 TSF 应为 [赋值:主体列表] 提供能力,以验证指定信息有效的证据。

依赖关系:无依赖关系。

FDP _ DAU.2 伴有保证者身份的数据鉴别

从属于:FDP _ DAU.1

FDP _ DAU.2.1 TSF 应提供产生保证[赋值:客体列表或信息类型列表]的有效性证据的能力。

FDP _ DAU.2.2 TSF 应为[赋值:主体列表]提供一种能力,以验证指定信息有效的证据以及产生证

据的用户身份。

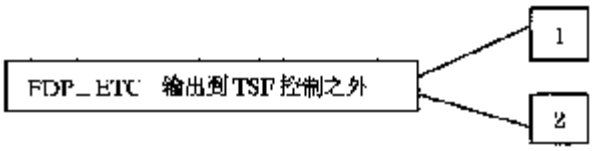
依赖关系:FIA _ UID.1　标识定时

7.4　输出到 TSF 控制之外(FDP _ ETC)

子类行为

本子类定义从 TOE 输出用户数据的功能,使得数据在输出后可以明确保留或忽略其安全属性和保护措施。这涉及对输出的限制以及安全属性与输出的用户数据之间的关联。

组件层次



FDP _ ETC.1　没有安全属性的用户数据输出,要求 TSF 在把用户数据输出到 TSF 之外时执行合适的 SFP。经由本功能输出的用户数据输出时没有输出相关的安全属性。

FDP _ ETC.2　有安全属性的用户数据输出,要求 TSF 在把用户数据输出到 TSF 之外时执行合适的 SFP。经由本功能输出的用户数据输出时将连同确切的安全属性一并输出。

管理:FDP _ ETC.1

对本组件,尚无预见的管理活动。

管理:FDP _ ETC.2

对 FMT 管理中的管理功能,要考虑以下活动:

a) 一个已定义角色的用户可以配置附加的输出控制规则。

审计:FDP _ ETC.1,FDP _ ETC.2

如果 PP/ST 包括 FAU _ GEN 安全审计数据产生,则以下事件应可审计:

a) 最小级:成功的信息输出;

b) 基本级:所有输出信息的尝试。

FDP _ ETC.1　没有安全属性的用户数据输出

从属于:无其他组件。

FDP _ ETC.1.1 TSF 在 SFP 控制下输出用户数据到 TSC 之外时,应执行[赋值:访问控制 SFP 或信息流控制 SFP]。

FDP _ ETC.1.2　TSF 应输出没有关联安全属性的用户数据。

依赖关系:[FDP _ ACC.1　子集访问控制,或
FDP _ IFC.1　子集信息流控制]

FDP _ ETC.2　有安全属性的用户数据输出

从属于:无其他组件。

FDP _ ETC.2.1　TSF 在 SFP 控制下输出用户数据到 TSC 之外时,应执行[赋值:访问控制 SFP 或信息流控制 SFP]。

FDP _ ETC.2.2　TSF 应输出带有相关安全属性的用户数据。

FDP _ ETC.2.3　TSF 在安全属性输出到 TSC 之外时,应确保其与输出的数据确切关联。

FDP _ ETC.2.4　TSF 在用户数据从 TSC 输出时应执行[赋值:附加的输出控制规则]。

依赖关系:[FDP _ ACC.1　子集访问控制,或

FDP _ IFC.1 子集信息流控制]

7.5 信息流控制策略(FDP _ IFC)

子类行为

本子类(通过名字)确定信息流控制SFP及其控制范围,这些策略组成已确定的TSP的信息流控制部分。该控制范围包括以下三个集合:策略控制下的主体、策略控制下的信息,以及引起受控信息流入、流出策略覆盖的受控主体的操作。本准则允许存在多个策略,每个策略有唯一的名字。这可以通过为每个命名的信息流控制策略反复使用本子类组件来实现。定义信息流控制SFP功能的规则将在其他子类中定义,如FDP _ IFF和FDP _ SDI。这里所确定的信息流控制SFP的名字将用于所有余下的有选择"信息流控制SFP"或为其进行赋值操作的组件中。

TSF机制根据信息流控制SFP控制信息的流向。通常不允许改变信息的安全属性的操作,因为这将违背信息流控制SFP。不过,如果明确指明,这种操作也可以作为信息流控制SFP的例外得到允许。

组件层次

FDP _ IFC.1 子集信息流控制,要求每个确定的信息流控制SFP适用于TOE内某个信息流子集上的可能的操作子集。

FDP _ IFC.2 完全信息流控制,要求每个确定的访问控制SFP覆盖被该SFP覆盖的主体和信息上的所有操作,并进一步要求TSC的所有信息流和操作都至少被一个确定的信息流控制SFP覆盖。它与组件FPT _ RVM.1的组合,要求一个参照监视器在这方面总是处于激发状态。

管理:FDP _ IFC.1,FDP _ IFC.2

对于本组件,尚无预见的管理活动。

审计:FDP _ IFC.1,FDP _ IFC.2

如果PP/ST包括FAU _ GEN安全审计数据产生,则没有可以审计的确定事件。

FDP _ IFC.1 子集信息流控制

从属于:无其他组件。

FDP _ IFC.1.1 **TSF应对[赋值:SFP覆盖的主体列表、信息列表和导致受控信息流入、流出受控主体的操作列表]执行[赋值:信息流控制SFP]。**

依赖关系:FDP _ IFF.1 简单安全属性

FDP _ IFC.2 完全信息流控制

从属于:FDP _ IFC.1

FDP _ IFC.2.1 TSF应对[赋值:主体列表和信息列表]以及**所有导致信息流入、流出SFP所覆盖主体的操作**执行[赋值:信息流控制SFP]。

FDP _ IFC.2.2 **TSF应确保所有导致TSC内的任意信息流入、流出TSC内的所有主体的操作被一个信息流控制SFP覆盖。**

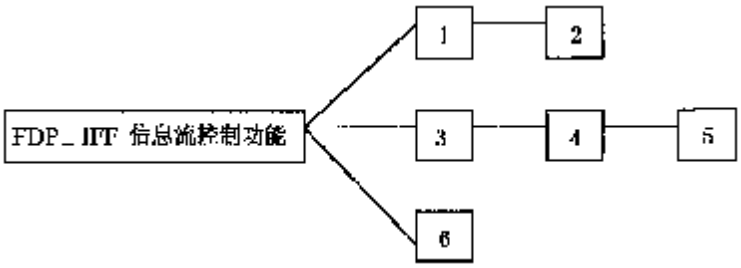
依赖关系:FDP _ IFF.1 简单安全属性

7.6 信息流控制功能(FDP _ IFF)

子类行为

本子类描述能实现在FDP _ IFC 中命名的信息流控制SFP 的特定功能的规则，同时规定该策略的控制范围。子类中包含两种要求：一是针对通用的信息流功能问题，再就是针对非法的信息流(如隐蔽信道)。之所以这样划分是因为，非法信息流涉及的问题在某种意义上与其余的信息流控制SFP 是泾渭分明的。根据其性质，它们将规避信息流控制SFP，导致控制策略的违背，因而需要特定的功能限制或防止非法信息流的出现。

组件层次



FDP _ IFF.1 简单安全属性，需要有关信息、导致信息流动的主体以及作为信息接收者的主体的安全属性。它规定该功能必须执行的规则，并描述该功能如何得到安全属性。

FDP _ IFF.2 分级安全属性，是在简单安全属性FDP _ IFF.1 的要求基础上进行的扩展。它要求TSP 中的所有信息流控制SFP 使用形成点阵的分级安全属性。

FDP _ IFF.3 受限的非法信息流，要求SFP 覆盖非法信息流，但不必消除。

FDP _ IFF.4 部分消除非法信息流，要求SFP 覆盖部分(不必是全部)的非法信息流的消除。

FDP _ IFF.5 无非法信息流，要求SFP 覆盖所有非法信息流的消除。

FDP _ IFF.6 非法信息流监视，要求SFP 根据指定的和最大的容限监视非法信息流。

管理：FDP _ IFF.1，FDP _ IFF.2

对于FMT 管理中的管理功能，要考虑以下活动：

a)管理用于作出明确访问决定的属性

管理：FDP _ IFF.3，FDP _ IFF.4，FDP _ IFF.5

对这些组件，尚无预见的管理活动。

管理：FDP _ IFF.6

对于FMT 管理中的管理功能，要考虑以下活动：

a) 监视功能的启动或关闭；

b) 对出现监视的最大容量的修改。

审计：FDP _ IFF.1，FDP _ IFF.2，FDP _ IFF.5

如果PP/ST 包括FAU _ GEN 安全审计数据产生，则下面的事件应可审计：

a) 最小级：允许请求的信息流的判决；

b) 基本级：对信息流请求的所有判决；

c) 详细级：用于做出信息流执行判决的特定安全属性；

d) 详细级：基于策略目标(如审计降级媒体)，已流动信息的某些特定子集。

审计：FDP _ IFF.3，FDP _ IFF.4，FDP _ IFF.6

如果PP/ST 包括FAU _ GEN 安全审计数据产生，则以下事件应可审计：

a) 最小级：允许请求的信息流的判决；

b) 基本级：对信息流请求的所有判决；

c) 基本级：确定的非法信息流信道的使用；

d) 详细级：用于做出信息流执行判决的特定的安全属性；

e) 详细级：基于策略目标(如审计降级媒体)，已流动信息的某些特定子集；

f) 详细级：对其估算的最大容量超过规定值的非法信息流信道的使用。

FDP_IFF.1 简单安全属性

从属于：无其他组件。

FDP_IFF.1.1 **TSF** 应基于下列类型的主体和信息安全属性[赋值：最小数目和类型的安全属性]执行[赋值：信息流控制 **SFP**]。

FDP_IFF.1.2 如果有下面的规则[赋值：对每一个操作，在主体和信息安全属性间必须有基于安全属性的关系]，**TSF** 应允许受控主体和受控信息之间存在经由受控操作的信息流。

FDP_IFF.1.3 **TSF** 应执行[赋值：附加的信息流控制 **SFP** 规则]。

FDP_IFF.1.4 **TSF** 应提供下列[赋值：附加 **SFP** 能力列表]。

FDP_IFF.1.5 **TSF** 应根据下列规则[赋值：基于安全属性，明确授权信息流的规则]明确授权信息流。

FDP_IFF.1.6 **TSF** 应根据下列规则[赋值：基于安全属性，明确拒绝信息流的规则]明确拒绝信息流。

依赖关系：FDP_IFC.1 子集信息流控制

FMT_MSA.3 静态属性初始化

FDP_IFF.2 分级安全属性

从属于：FDP_IFF.1

FDP_IFF.2.1 TSF 应基于下列类型的主体和信息安全属性[赋值：最小数目和类型的安全属性]，执行[赋值：信息流控制 SFP]。

FDP_IFF.2.2 如果有下面基于安全属性间有序关系的规则[赋值：对每一个操作，在主体和信息安全属性间必须有基于安全属性的关系]，TSF 应允许受控主体和受控信息之间存在经由受控操作的信息流。

FDP_IFF.2.3 TSF 应执行[赋值：附加的信息流控制 SFP 规则]。

FDP_IFF.2.4 TSF 应提供下列[赋值：附加 SFP 能力列表]。

FDP_IFF.2.5 TSF 应根据下列规则[赋值：基于安全属性，明确授权信息流的规则]明确授权信息流。

FDP_IFF.2.6 TSF 应根据下列规则[赋值：基于安全属性，明确拒绝信息流的规则]明确拒绝信息流。

FDP_IFF.2.7 **TSF** 应对任意两个有效的信息流控制安全属性执行下面的关系：

a) 存在排序功能，也就是说，给定两个有效的安全属性，可判断它们是否相等，是否其中一个大于另一个，还是两者不可比较；

b) 在安全属性集中存在“最小上界”，也就是说，给定任意两个有效的安全属性，存在一个有效的安全属性大于或等于这两个有效安全属性；

c) 在安全属性集中存在“最大下界”，也就是说，给定任意两个有效的安全属性，存在一个有效的安全属性不大于这两个有效安全属性。

依赖关系：FDP_IFC.1 子集信息流控制

FMT_MSA.3 静态属性初始化

FDP_IFF.3 受限的非法信息流

从属于：无其他组件。

FDP_IFF.3.1 **TSF** 应执行[赋值：信息流控制 **SFP**]，以限制[赋值：非法信息流类型]的容限为[赋值：最大容限]。

依赖关系:AVA _ CCA.1　隐蔽信道分析
　　FDP _ IFC.1　子集信息流控制

FDP _ IFF.4　部分消除非法信息流
从属于:FDP _ IFF.3
FDP _ IFF.4.1　TSF 应执行[赋值:信息流控制 SFP],以限制[赋值:非法信息流类型]的容限为[赋值:最大容限]。
FDP _ IFF.4.2　TSF 应避免[赋值:非法信息流类型]。
依赖关系:AVA _ CCA.1　隐蔽信道分析
　　FDP _ IFC.1　子集信息流控制

FDP _ IFF.5　无非法信息流
从属于:FDP _ IFF.4
FDP _ IFF.5.1　TSF 应确保没有规避[赋值:信息流控制 SFP 名字]的非法信息流存在。
依赖关系:AVA _ CCA.3　详尽的隐蔽信道分析
　　FDP _ IFC.1　子集信息流控制

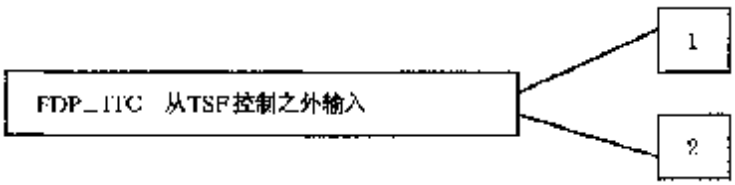
FDP _ IFF.6　非法信息流监视
从属于:无其他组件。
FDP _ IFF.6.1　TSF 应执行[赋值:信息流控制 SFP],以监视[赋值:非法信息流类型]是否超过了[赋值:最大容限]。
依赖关系:AVA _ CCA.1　隐蔽信道分析
　　FDP _ IFC.1　子集信息流控制

7.7　从 TSF 控制之外输入(FDP _ ITC)

子类行为

本子类定义引入用户数据到 TOE 内的机制,使得数据在输入时有合适的安全属性和保护措施。涉及到对输入的限制、所需安全属性的确定以及对用户数据相关安全属性的解释。

组件层次



本子类包含两个组件,描述用于访问控制和信息控制策略的输入用户数据的安全属性的保持情况。

FDP _ ITC.1 没有安全属性的用户数据输入,要求安全属性正确反映用户数据,且和客体分离。

FDP _ ITC.2 有安全属性的用户数据输入,要求安全属性正确反映用户数据,并且与从 TSC 外输入的数据确切地联系在一起。

管理:FDP _ ITC.1,FDP _ ITC.2

对于 FMT 管理中的管理功能,要考虑以下活动:

a) 对用户数据输入的附加控制规则的修改。

审计:FDP _ ITC.1,FDP _ ITC.2

如果PP/ST 包括 FAU _ GEN 安全审计数据产生，则以下事件应可审计：

a）最小级：用户数据，包括任何安全属性的成功输入；

b）基本级：用户数据，包括任何安全属性的所有输入尝试；

c）详细级：授权用户提供的用于输入的用户数据的安全属性规范。

FDP _ ITC.1　没有安全属性的用户数据输入

从属于：无其他组件。

FDP _ ITC.1.1　TSF 在 SFP 控制下从 TSC 之外输入用户数据时，应执行[赋值：访问控制 SFP 或信息流控制 SFP]。

FDP _ ITC.1.2　从 TSC 外部输入用户数据时，TSF 应略去任何相关的安全属性。

FDP _ ITC.1.3　TSF 在 SPF 控制下从 TSC 外部输入用户数据时应执行下面的规则：[赋值：附加的输入控制规则]。

依赖关系：[FDP _ ACC.1　子集访问控制，或

FDP _ IFC.1　子集信息流控制]

FMT _ MSA.3　静态属性初始化

FDP _ ITC.2　有安全属性的用户数据输入

从属于：无其他组件。

FDP _ ITC.2.1　TSF 在 SFP 控制下从 TSC 之外输入用户数据时，应执行[赋值：访问控制 SFP 或信息流控制 SFP]。

FDP _ ITC.2.2　TSF 应使用与输入的数据相关的安全属性。

FDP _ ITC.2.3　TSF 应确保使用的协议在安全属性和接收的用户数据之间提供了明确的联系。

FDP _ ITC.2.4　TSF 应确保对输入的用户数据安全属性的解释与用户数据源的解释是一致的。

FDP _ ITC.2.5　TSF 在 SFP 控制下从 TSC 之外输入用户数据时应执行[赋值：附加的输入控制规则]。

依赖关系：[FDP _ ACC.1　子集访问控制，或

FDP _ IFC.1　子集信息流控制]

[FDP _ ITC.1　TSF 间的可信信道，或

FTP _ TRP.1　可信路径]

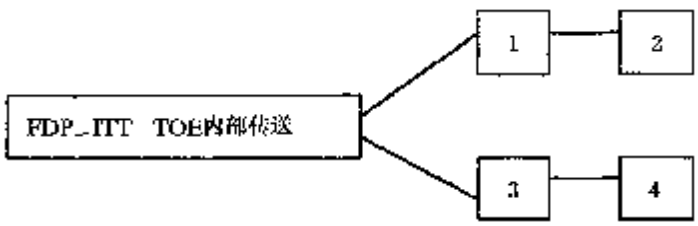
FPT _ TDC.1　TSF 间基本的 TSF 数据一致性

7.8　TOE 内部传送(FDP _ ITT)

子类行为

本子类提供当用户数据通过内部信道在TOE 各部分之间传递时，对数据进行保护的要求。和 FDP _ UCT 与 FDP _ UIT 的不同之处在于，后两者为数据经外部信道在不同的 TSF 间传递时提供保护；而与 FDP _ ETC 和 FDP _ ITC 的不同之处则在于，它们描述的是数据进出 TSF 时的控制。

组件层次



FDP_ITT.1　基本内部传送保护，要求用户数据在TOE的各部分间传递时受保护。

FDP_ITT.2　属性分隔传送，除第一个组件的要求外，还要求基于与SFP相关的属性值把数据分隔开。

FDP_ITT.3　完整性监视，要求SF监视在TOE各部分间传递的用户数据的完整性错误。

FDP_ITT.4 基于属性的完整性监视，是对第3个组件的扩展，它允许根据不同的与SFP相关的属性，进行完整性监视。

管理：FDP_ITT.1，FDP_ITT.2

对于FMT管理中的管理功能，要考虑以下活动：

a）如果TSF提供多种方法保护在TOE的物理上分隔的部分间传递的用户数据，则TSF应提供一个预定义的角色，使其有能力选择某种方法。

管理：FDP_ITT.3，FDP_ITT.4

对于FMT管理中的管理功能，要考虑以下活动：

a）对于检测到完整性错误将采取的行动的规范应是可配置的。

审计：FDP_ITT.1，FDP_ITT.2

如果PP/ST包括FAU_GEN安全审计数据产生，则以下事件是可审计的：

a）最小级：用户数据的成功传送，包括所用的保护方法的标识；

b）基本级：所有传送用户数据的尝试，包括所用的保护方法和所有出现的错误。

审计：FDP_ITT.3，FDP_ITT.4

如果PP/ST包括FAU_GEN安全审计数据产生，则以下事件是可审计的：

a）最小级：用户数据的成功传送，包括所用的保护方法的标识；

b）基本级：所有传送用户数据的尝试，包括所用的保护方法和所有出现的错误；

c）基本级：未授权地改变完整性保护方法的尝试；

d）详细级：检测到完整性错误后采取的行动。

FDP_ITT.1　基本内部传送保护

从属于：无其他组件。

FDP_ITT.1.1　在TOE物理上分隔的部分间传递用户数据时，TSF应执行[赋值：访问控制SFP或信息流控制SFP]，以防止[选择：泄露，篡改，丢失]。

依赖关系：[**FDP_ACC.1　子集访问控制，或**
FDP_IFC.1　子集信息流控制]

FDP_ITT.2　属性分隔传送

从属于：FDP_ITT.1

FDP_ITT.2.1　在TOE物理上分隔的部分间传递用户数据时，TSF应执行[赋值：访问控制SFP或信息流控制SFP]，以防止[选择：泄露，篡改，丢失]。

FDP_ITT.2.2　在TOE物理上分隔的部分间传递用户数据时，TSF应基于下列值[赋值：需要分隔的安全属性]，将SFP控制的数据分隔开。

依赖关系：[FDP_ACC.1　子集访问控制，或
FDP_IFC.1　子集信息流控制]

FDP_ITT.3　完整性监视

从属于：无其他组件。

FDP_ITT.3.1　在TOE物理上分隔的部分间传递用户数据时，TSF应执行[赋值：访问控制SFP或信

息流控制 SFP],以监视是否有下列错误出现[赋值:完整性错误]。

FDP _ ITT.3.2 检测到数据完整性错误时,TSF 应[赋值:规定对完整性错误应采取的行动]。

依赖关系:[FDP _ ACC.1 子集访问控制,或
FDP _ IFC.1 子集信息流控制]
FDP _ ITT.1 基本内部传送保护

FDP _ ITT.4 基于属性的完整性监视

从属于:FDP _ ITT.3

FDP _ ITT.4.1 在 TOE 的物理上分隔的部分间传递用户数据时,基于下面的属性[赋值:需要分隔传送信道的安全属性],TSF 级执行[赋值:访问控制 SFP 或信息流控制 SFP],以监视是否有下列错误出现[赋值:完整性错误]。

FDP _ ITT.4.2 检测到数据完整性错误时,TSF 应[赋值:规定对完整性错误应采取的行动]。

依赖关系:[FDP _ ACC.1 子集访问控制,或
FDP _ IFC.1 子集信息流控制]
FDP _ ITT.2 属性分隔传送

7.9 残余信息保护(FDP _ RIP)

子类行为

本子类针对如下需要,即确保已经被删除的信息不再是可访问的,并且,新生成的客体确实不包含不应被访问的信息。本子类要求保护已逻辑删除或释放的信息,但信息仍旧可以保留在 TOE 内部。

组件层次

FDP _ RIP.1 子集残余信息保护,要求 TSF 确保任何资源的任何残余信息内容,在分配或释放资源时,对于 TSC 内已定义的客体子集而言是不可用的。

FDP _ RIP.2 完全残余信息保护,要求 TSF 确保在分配或释放资源时,任何资源的任何残余信息内容对于所有客体都是不可用的。

管理:FDP _ RIP.1,FDP _ RIP.2

对于 FMT 管理中的管理功能,应考虑以下活动:

a) TOE 内,选择何时(如分配或释放时)执行残余信息保护是可以配置的。

审计:FDP _ RIP.1,FDP _ RIP.2

如果 PP/ST 包括 FAU _ GEN 安全审计数据产生,就没有确定的事件可审计。

FDP _ RIP.1 子集残余信息保护

从属于:无其他组件。

FDP _ RIP.1.1 TSF 对下列客体[赋值:客体列表][选择:分配或释放资源]时,应确保该资源任何以前的信息内容不再可用。

依赖关系:无依赖关系。

FDP _ RIP.2 完全残余信息保护

从属于:FDP _ RIP.1

FDP _ RIP.2.1 TSF 应确保对**所有客体**[选择：分配或释放资源]时，使该资源任何以前的信息内容不再可用。

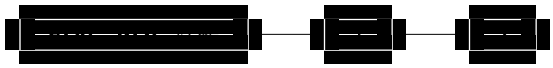
依赖关系：无依赖性。

7.10 反转(FDP _ ROL)

子类行为

反转操作涉及在一定条件的限制下(如时间长短)，撤消上一次或一系列操作，并返回到某个以前的已知状态。反转提供了取消上一次或一系列操作结果的能力以保持用户数据的完整性。

组件层次



FDP _ ROL.1 基本反转，满足在确定的范围内，反转或撤消有限操作的需要。

FDP _ ROL.2 高级反转，满足在确定的范围内，反转或撤消所有操作的需要。

管理：FDP _ ROL.1，FDP _ ROL.2

对于 FMT 管理中的管理功能，要考虑以下活动：

a) 限制反转可实施的边界，在 TOE 内可以是一个可配置的条目；

b) 实施反转操作的权限可以被限制到一个精心定义的角色。

审计：FDP _ ROL.1，FDP _ ROL.2

如果 PP/ST 包括 FAU _ GEN 安全审计数据产生，则以下事件应可审计：

a) 最小级：所有成功的反转操作；

b) 基本级：所有实施反转操作的尝试；

c) 详细级：所有实施反转操作的尝试，包括被反转的操作类型的标识。

FDP _ ROL.1 基本反转

从属于：无其他组件。

FDP _ ROL.1.1 **TSF 应执行**[赋值：访问控制 SFP 或信息流控制 SFP]，**以允许在**[赋值：客体列表]上**的**[赋值：操作列表]**的反转。**

FDP _ ROL.1.2 **TSF 应允许在**[赋值：反转可以实施的边界范围]内进行反转操作。

依赖关系：[FDP _ ACC.1 子集访问控制，或
FMT _ IFC.1 子集信息流控制]

FDP _ ROL.2 高级反转

从属于：FDP _ ROL.1

FDP _ ROL.2.1 TSF 应执行[赋值：访问控制 SFP 或信息流控制 SFP]，以允许在[赋值：客体列表]上的**所有操作**的反转。

FDP _ ROL.2.2 TSF 应允许在[赋值：反转可以实施的边界范围]内进行反转操作。

依赖关系：[FDP _ ACC.1 子集访问控制，或
FMT _ IFC.1 子集信息流控制]

7.11 存储数据的完整性(FDP _ SDI)

子类行为

本子类提供了对存储在TSC内部的用户数据保护的要求。完整性错误可能会影响存放在内存中的,或存储设备中的数据。本子类与TOE内部传送FDP_ITT不同之处,后者保护的是数据在TOE内部传送时的完整性。

组件层次

FDP_SDI.1 存储数据的完整性监视,要求SF监视存储在TSC内的用户数据是否出现已确定的完整性错误。

FDP_SDI.2 存储数据的完整性监视与行动,则是在FDP_SDI.1的基础上增加了附加的能力,允许在检测到某错误时,采取相应的行动。

管理:FDP_SDI.1

本组件没有可预见的管理活动。

管理:FDP_SDI.2

对于FMT管理中的管理功能,要考虑以下活动:

a) 可以配置在检测到完整性错误时所要采取的行动。

审计:FDP_SDI.1,

如果PP/ST包括FAU_GEN安全审计数据产生,则以下事件应可审计:

a) 最小级:检测用户数据完整性的成功尝试,包括指示检测结果;

b) 基本级:检测用户数据完整性的所有尝试,如果完成的话,还包括指示检测结果;

c) 详细级:出现的完整性错误的类型。

审计:FDP_SDI.2,

如果PP/ST包括FAU_GEN安全审计数据产生,则以下事件应可审计:

a) 最小级:检测用户数据完整性的成功尝试,包括指示检测结果;

b) 基本级:检测用户数据完整性的所有尝试,如果完成有的话,还包括指示检测结果;

c) 详细级:发生的完整性错误的类型;

d) 详细级:检测到完整性错误时所采取的行动。

FDP_SDI.1 存储数据完整性监视

从属于:无其他组件。

FDP_SDI.1.1 TSF应基于下列属性[赋值:用户数据属性]对所有客体,监视存储在TOE内的用户数据是否出现[赋值:完整性错误]。

依赖关系:无依赖关系。

FDP_SDI.2 存储数据的完整性监视与行动

从属于:FDP_SDI.1

FDP_SDI.2.1 TSF应基于下列属性[赋值:用户数据属性]对所有客体,监视存储在TOE内的用户数据是否出现[赋值:完整性错误]。

FDP_SDI.2.1 检测到完整性错误时,TSF应[赋值:采取的行动]。

依赖关系:无依赖关系。

7.12 TSF间用户数据传送的保密性保护(FDP_UCT)

子类行为

本子类定义当用户数据通过外部信道在不同的TOE之间,或是在不同的TOE用户之间传递时,确保用户数据保密性的要求。

组件层次

FDP_UCT.1 基本的数据交换保密性,目的是为用户数据提供保护,防止其在传送过程中被泄露。

管理:FDP_UCT.1

对本组件,没有可预见的管理活动。

审计:FDP_UCT.1

如果PP/ST包括FAU_GEN安全审计数据产生,则以下事件应可审计:

a) 最小级:使用数据交换机制的任何用户或主体的身份;

b) 基本级:企图使用用户数据交换机制的任何未授权用户或主体的身份;

c) 基本级:对确定被传送或接收的用户数据有用的名字或其他索引信息的引用,可能包括与信息相关联的安全属性。

FDP_UCT.1 基本的数据交换保密性

从属于:无其他组件。

FDP_UCT.1.1 TSF应执行[赋值:访问控制SFP或信息流控制SFP],使得能以某种防止未授权泄露的方式[选择:传送,接收]客体。

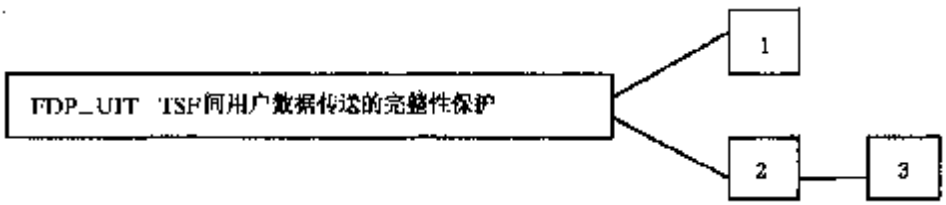
依赖关系:[FTP_ITC.1 TSF间的可信信道,或
FTP_TRP.1 可信路径]
[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制]

7.13 TSF间用户数据传送的完整性保护(FDP_UIT)

子类行为

本子类定义用户数据在TSF和其他可信IT产品间传送时,提供完整性并从可检测的错误中恢复的要求。本子类至少监视用户数据针对篡改的完整性,此外,还支持检测到完整性错误时采取的各种纠正方法。

组件层次



FDP_UIT.1 数据交换的完整性,解决对被传送的用户数据的篡改、删除、插入和重用等错误的检测。

FDP_UIT.2 原发端数据交换恢复，解决由接收端 TSF 借助于原发端可信 IT 产品，恢复原始的用户数据。

FDP_UIT.3 接受端数据交换恢复，解决由接收端 TSF 自己，无需原发端可信 IT 产品的任何帮助，恢复原始的用户数据。

管理：FDP_UIT.1，FDP_UIT.2，FDP_UIT.3

对本组件，尚无预见的管理活动。

审计：FDP_UIT.1，

如果 PP/ST 包括 FAU_GEN 安全审计数据产生，则以下事件应可审计：

a）最小级：使用数据交换机制的任何用户或主体的身份；

b）基本级：企图使用用户数据交换机制的任何未授权用户或主体的身份；

c）基本级：对确定被传送或接收的用户数据有用的名字或其他索引信息的引用，可能包括和信息相联的安全属性；

d）基本级：任何确定的阻塞用户数据传送的尝试；

e）详细级：任何检测到的用户数据传送中的篡改类型或后果。

审计：FDP_UIT.2，FDP_UIT.3

如果 PP/ST 包括 FAU_GEN 安全审计数据产生，则以下事件应可审计：

a）最小级：使用数据交换机制的任何用户或主体的身份；

b）最小级：从错误中成功的恢复，包括检测到的错误类型；

c）基本级：企图使用用户数据交换机制的任何未授权用户或主体的身份；

d）基本级：对确定被传送或接收的用户数据有用的名字或其他索引信息的引动，可能包括和信息相联的安全属性；

e）基本级：任何确定的阻塞用户数据传送的尝试；

f）详细级：任何检测到的用户数据传送中的篡改类型或后果。

FDP_UIT.1 数据交换完整性

从属于：无其他组件。

FDP_UIT.1.1 TSF 应执行[赋值：访问控制 SFP 或信息流控制 SFP]，使得能以某种方式[选择：传送，接收]用户数据，保护数据避免[选择：篡改，删除，插入，重用]错误。

FDP_UIT.1.2 TSF 应能根据收到的用户数据判断，是否出现了[选择：篡改，删除，插入，重用]。

依赖关系：[FDP_ACC.1 子集访问控制，或
FDP_IFC.1 子集信息流控制]
[FTP_ITC.1 TSF 间的可信信道，或
FTP_TRP.1 可信路径]

FDP_UIT.2 原发端数据交换恢复

从属于：无其他组件。

FDP_UIT.2.1 TSF 应执行[赋值：访问控制 SFP 或信息流控制 SFP]，以便能在原发端可信 IT 产品的帮助下，从[赋值：可恢复的错误列表]中恢复。

依赖关系：[FDP_ACC.1 子集访问控制，或
FDP_IFC.1 子集信息流控制]
FDP_UIT.1 数据交换完整性
FTP_ITC.1 TSF 间的可信信道

FDP _ UIT.3　接受端数据交换恢复

从属于:FDP _ UIT.2

FDP _ UIT.3.1　TSF 应执行[赋值:访问控制 SFP 或信息流控制 SFP],使得可以在没有任何源可信 IT 产品的帮助下,从[赋值:可恢复的错误列表]中恢复。

依赖关系:[FDP _ ACC.1　子集访问控制,或

FDP _ IFC.1　子集信息流控制]

FDP _ UIT.1　数据交换完整性

FTP _ ITC.1　TSF 间的可信信道

8　FIA 类:标识和鉴别

本类中的子类提出建立和验证所声称的用户身份的功能要求。

需要通过标识和鉴别确保用户与正确的安全属性相关联(如身份、组、角色、安全或完整性等级)。

授权用户的无歧义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。本类中的子类处理:用户身份的确定和验证、确定它们与 TOE 交互的权利,以及每个授权用户安全属性的正确关联。其他类(如用户数据保护、安全审计)的有效性建立在对用户的正确标识和鉴别基础上。

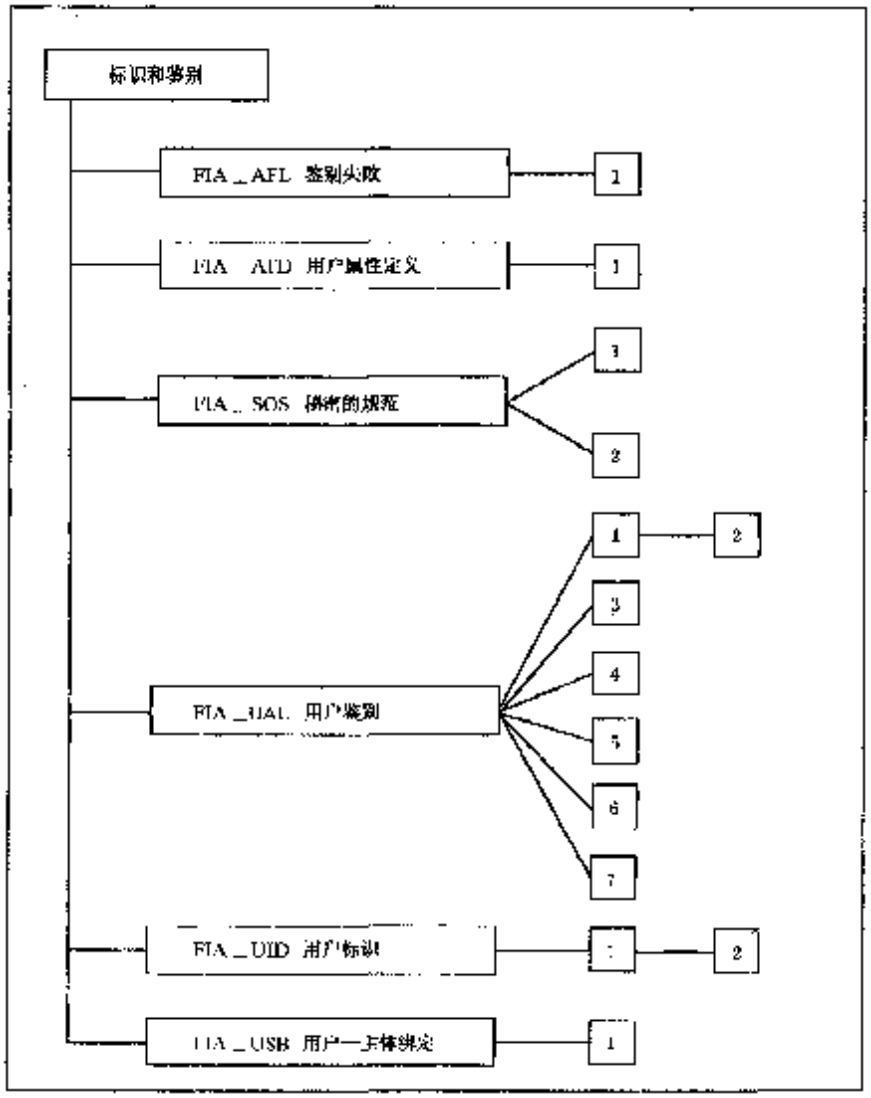


图 8.1　标识和鉴别类分解

8.1 鉴别失败(FIA _ AFL)

子类行为

本子类要求为不成功的鉴别尝试次数定义值,以及鉴别尝试失败时 TSF 的行动。参数包括但不限于,失败的鉴别尝试次数和时间门限值。

组件层次

FIA _ AFL.1 要求 TSF 能够在用户鉴别尝试失败了指定的次数后,终止会话建立进程。此外,它还要求会话建立进程终止后,直到管理员定义的条件出现前,TSF 能够使用户帐号无效,或者使进行尝试的登录点无效(如,某工作站)。

管理:FIA _ AFL.1

FMT 中的管理功能,可考虑如下行动:

a) 管理失败的鉴别尝试门限值;

b) 管理鉴别失败时将要采取的行动。

审计:FIA _ AFL.1

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生,下列事件应可审计:

a) 最小级:未成功鉴别尝试达到门限值及所采取的行动(如,使终端无效),及随后(适当时)还原到正常状态(如,重新使终端有效)。

FIA _ AFL.1 鉴别失败处理

从属于:无其他组件。

FIA _ AFL.1.1 当与[赋值:鉴别事件列表]相关的[赋值:数目]次不成功鉴别尝试出现时,TSF 应加以检测。

FIA _ AFL.1.2 当达到或超过所定义的不成功鉴别尝试的次数时,TSF 应[赋值:行动列表]。

依赖关系:FIA _ UAU.1 鉴别定时

8.2 用户属性定义(FIA _ ATD)

子类行为

所有授权用户可能都有一组除用户身份外的安全属性用来执行 TSP。本子类定义用于支持 TSP 所需的将用户安全属性与用户相关联的要求。

组件层次

FIA _ ATD.1 用户属性定义,允许对每个用户的用户安全属性分别加以维护。

管理:FIA _ ATD.1

FMT 中的管理功能,可考虑如下行动:

a) 如果赋值中如此指明的话,授权管理员应能够为用户定义附加的安全属性。

审计:FIA _ ATD.1

如果PP/ST中包含FAU _GEN安全审计数据产生,无确定的可审计行动。

FIA _ATD.1 用户属性定义

从属于:无其他组件。

FIA _ATD.1.1 TSF应保存属于每个用户的下列安全属性:[赋值:安全属性列表]。

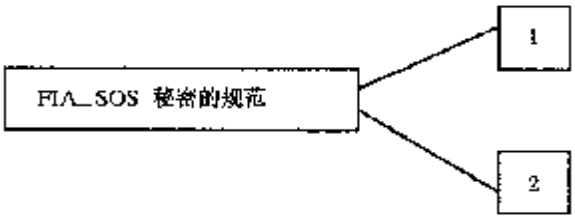
依赖关系:无依赖关系。

8.3 秘密的规范(FIA _SOS)

子类行为

本子类定义对所提供的秘密执行规定的质量量度以及生成满足规定的量度的秘密的机制方面的要求。

组件层次



FIA _SOS.1 秘密的验证,要求TSF验证秘密满足规定的质量量度。

FIA _SOS.2 秘密的TSF生成,要求TSF能够产生满足规定的质量量度的秘密。

管理:FIA _SOS.1

FMT中的管理功能,可考虑如下行动:

a) 管理用于验证秘密的量度。

管理:FIA _SOS.2

FMT中的管理功能,可考虑如下行动:

a) 管理用于产生秘密的量度。

审计:FIA _SOS.1,FIA _SOS.2

如果PP/ST中包括FAU _GEN安全审计数据产生,下列事件应可审计:

a) 最小级:TSF对所有已测试秘密的拒绝;

b) 基本级:TSF对所有已测试秘密的拒绝或接受;

c) 详细级:对所定义质量量度的所有改动的标识。

FIA _SOS.1 秘密的验证

从属于:无其他组件。

FIA _SOS.1.1 TSF应提供一种机制以验证秘密满足[赋值:一个确定的质量量度]。

依赖关系:无依赖关系。

FIA _SOS.2 秘密的TSF生成

从属于:无其他组件。

FIA _SOS.2.1 TSF应提供一种机制以产生满足[赋值:一个确定的质量量度]的秘密。

FIA _SOS.2.2 TSF应能够为[赋值:TSF功能列表]使用TSF产生的秘密。

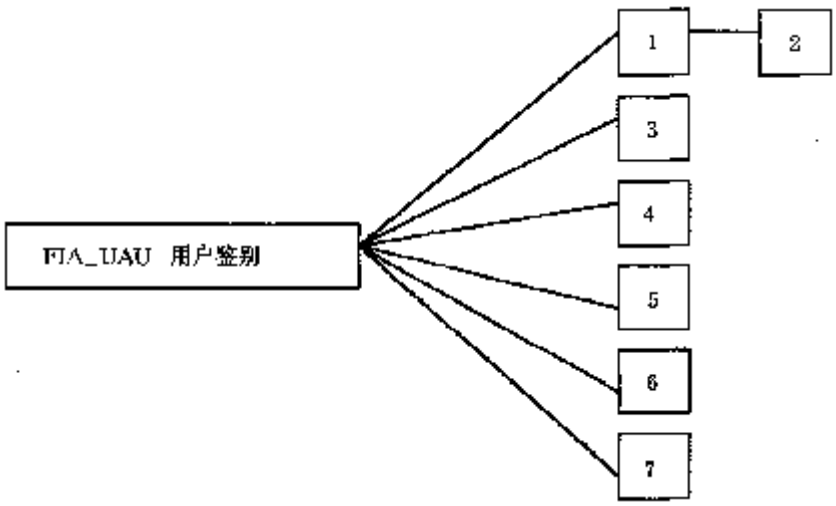
依赖关系:无依赖关系。

8.4 用户鉴别(FIA_UAU)

子类行为

本子类定义TSF所支持的用户鉴别机制的类型,和作为用户鉴别机制基础所需要的属性。

组件层次



FIA_UAU.1 鉴别定时,允许用户在其身份被鉴别前执行某些行动。

FIA_UAU.2 在任何行动前的用户鉴别,要求用户在TSF允许任何行动之前,先鉴别它们自己。

FIA_UAU.3 不可伪造的鉴别,要求鉴别机制能够检测和防止使用伪造或复制的鉴别数据。

FIA_UAU.4 一次性鉴别机制,要求使用一次性鉴别数据的鉴别机制。

FIA_UAU.5 多重鉴别机制,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。

FIA_UAU.6 重鉴别,要求有能力说明哪些事件用户需要被重新鉴别。

FIA_UAU.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。

管理:FIA_UAU.1

FMT中的管理功能,可考虑如下行动:

a) 管理员对鉴别数据的管理;

b) 相关用户对鉴别数据的管理;

c) 用户鉴别前可执行的行动列表的管理。

管理:FIA_UAU.2

FMT中的管理功能,可考虑如下行动:

a) 管理员对鉴别数据的管理;

b) 与鉴别数据相关的用户,对鉴别数据的管理。

管理:FIA_UAU.3,FIA_UAU.4,FIA_UAU.7

尚无预见的管理活动。

管理:FIA_UAU.5

FMT中的管理功能,可考虑如下行动:

a) 鉴别机制的管理;

b) 鉴别规则的管理。

管理:FIA_UAU.6

FMT 中的管理功能，可考虑如下行动：

a）如果一个授权管理员能请求重鉴别，则管理包含重鉴别请求。

审计：FIA _ UAU.1

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生，下列事件应可审计：

a）最小级：使用鉴别机制失败；

b）基本级：所有对鉴别机制的使用；

c）详细级：用户鉴别前，执行的所有由 TSF 促成的行动。

审计：FIA _ UAU.2

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生，下列事件应可审计：

a）最小级：使用鉴别机制失败；

b）基本级：所有对鉴别机制的使用。

审计：FIA _ UAU.3

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生，下列事件应可审计：

a）最小级：欺骗性鉴别数据的发现；

d）基本级：对欺骗性的数据立即采取的所有措施和检查结果。

审计：FIA _ UAU.4

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生，下列事件应可审计：

a）最小级：重用鉴别数据的企图。

审计：FIA _ UAU.5

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生，下列事件应可审计：

a）最小级：鉴别的最终判决；

b）基本级：每个被激活机制的结果以及最终判决。

审计：FIA _ UAU.6

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生，下列事件应可审计：

a）最小级：重鉴别失败；

b）基本级：所有重鉴别尝试。

审计：FIA _ UAU.7

尚无预见的可审计事件。

FIA _ UAU.1 鉴别定时

从属于：无其他组件。

FIA _ UAU.1.1 在用户鉴别前，TSF 应允许代表用户的[赋值：TSF 促成的行动列表]被执行。

FIA _ UAU.1.2 在允许任何其他代表用户的 TSF 促成的行动执行前，TSF 应要求该用户已被成功鉴别。

依赖关系：FIA _ UID.1 标识定时

FIA _ UAU.2 任何行动前的用户鉴别

从属于：FIA _ UAU.1

FIA _ UAU.2.1 在允许任何代表用户的其他 TSF 促成的行动执行前，TSF 应要求该用户已被成功鉴别。

依赖关系：FIA _ UID.1 标识定时

FIA _ UAU.3 不可伪造的鉴别

从属于:无其他组件。

FIA_UAU.3.1 TSF 应[选择:检测,防止]一切 TSF 用户伪造的鉴别数据的使用。

FIA_UAU.3.2 TSF 应[选择:检测,防止] 从任何其他 TSF 用户处拷贝的鉴别数据的使用。

依赖关系:无依赖关系。

FIA_UAU.4 一次性鉴别机制

从属于:无其他组件。

FIA_UAU.4.1 TSF 应防止与[赋值:确定的鉴别机制]有关的鉴别数据的重用。

依赖关系:无依赖关系。

FIA_UAU.5 多重鉴别机制

从属于:无其他组件。

FIA_UAU.5.1 TSF 应提供[赋值:多重鉴别机制列表]以支持用户鉴别。

FIA_UAU.5.2 TSF 应根据[赋值:描述多重鉴别机制如何提供鉴别的规则]鉴别一切用户所声称的身份。

依赖关系:无依赖关系。

FIA_UAU.6 重鉴别

从属于:无其他组件。

FIA_UAU.6.1 在[赋值:需要重鉴别的条件列表]条件下,TSF 应重新鉴别用户。

依赖关系:无依赖关系。

FIA_UAU.7 受保护的鉴别反馈

从属于:无其他组件。

FIA_UAU.7.1 鉴别进行时,TSF 应仅向用户提供[赋值:反馈列表]。

依赖关系:FIA_UAU.1 鉴别定时

8.5 用户标识(FIA_UID)

子类行为

本子类定义在什么条件下要求用户在执行任何其他由 TSF 促成的要有用户标识的行动之前,先标识他们自己。

组件层次

FIA_UID.1 标识定时,允许用户在被 TSF 标识前,执行某些行动。

FIA_UID.2 任何行动前的用户标识,在 TSF 允许任何行动之前,要求用户标识它们自己。

管理:FIA_UID.1

FMT 中的管理功能,可考虑如下行动:

a) 对用户身份的管理;

b) 如果一个授权管理员能够改变在标识前所允许的行动,那么对行动列表的管理。

管理:FIA_UID.2

FMT 中的管理功能，可考虑如下行动：

a) 用户身份的管理。

审计：FIA _ UID.1，FIA _ UID.2

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生，下列事件应可审计：

a) 最小级：用户标识机制的使用失败，包括所提供的用户身份；

b) 基本级：用户标识机制的所有使用，包括所提供的用户身份。

FIA _ UID.1 标识定时

从属于：无其他组件。

FIA _ UID.1.1 在用户被标识之前，TSF 应允许执行代表用户的[赋值：TSF 促成的行动列表]。

FIA _ UID.1.2 在允许代表用户的其他 TSF 促成的任何行动之前，TSF 应要求用户被成功标识。

依赖关系：无依赖关系。

FIA _ UID.2 任何行动前的用户标识

从属于：FIA _ UID.1

FIA _ UID.2.1 在允许任何代表用户的其他 TSF 促成的行动之前，TSF 应要求用户标识自己。

依赖关系：无依赖关系。

8.6 用户_主体绑定(FIA _ USB)

子类行为

一个已鉴别了的用户，为了使用 TOE，一般要先激活一个主体。用户的安全属性则（全部或部分地）与该主体相关联。本子类定义建立和维护用户的安全属性与代表用户活动的主体间的关联的要求。

组件层次

FIA _ USB.1 用户—主体绑定，要求维持用户的安全属性与代表用户活动的主体间的关联。

管理：FIA _ USB.1

FMT 中的管理功能，可考虑如下行动：

a) 授权管理员可以定义默认的主体安全属性。

审计：FIA _ USB.1

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生，下列事件应可审计：

a) 最小级：用户安全属性与一个主体绑定的失败(如，创建一个主体)；

b) 基本级：用户安全属性与一个主体绑定的成功与失败(如，创建一个主体的成功与失败)。

FIA _ USB.1 用户—主体绑定

从属于：无其他组件。

FIA _ USB.1.1 TSF 应将合适的用户安全属性与代表用户活动的主体相关联。

依赖关系：FIA _ ATD.1 用户属性定义

9 FMT 类：安全管理

本类目的是规定 TSF 几个方面的管理：安全属性、TSF 数据和功能、可说明不同的管理角色及其相

互作用，如能力的分离。

本类有几个目的：

a）管理 TSF 数据，例如旗标；

b）管理安全属性，例如访问控制表和能力表；

c）管理 TSF 功能，例如功能的选择，影响 TSF 行为的规则或条件；

d）定义安全角色。

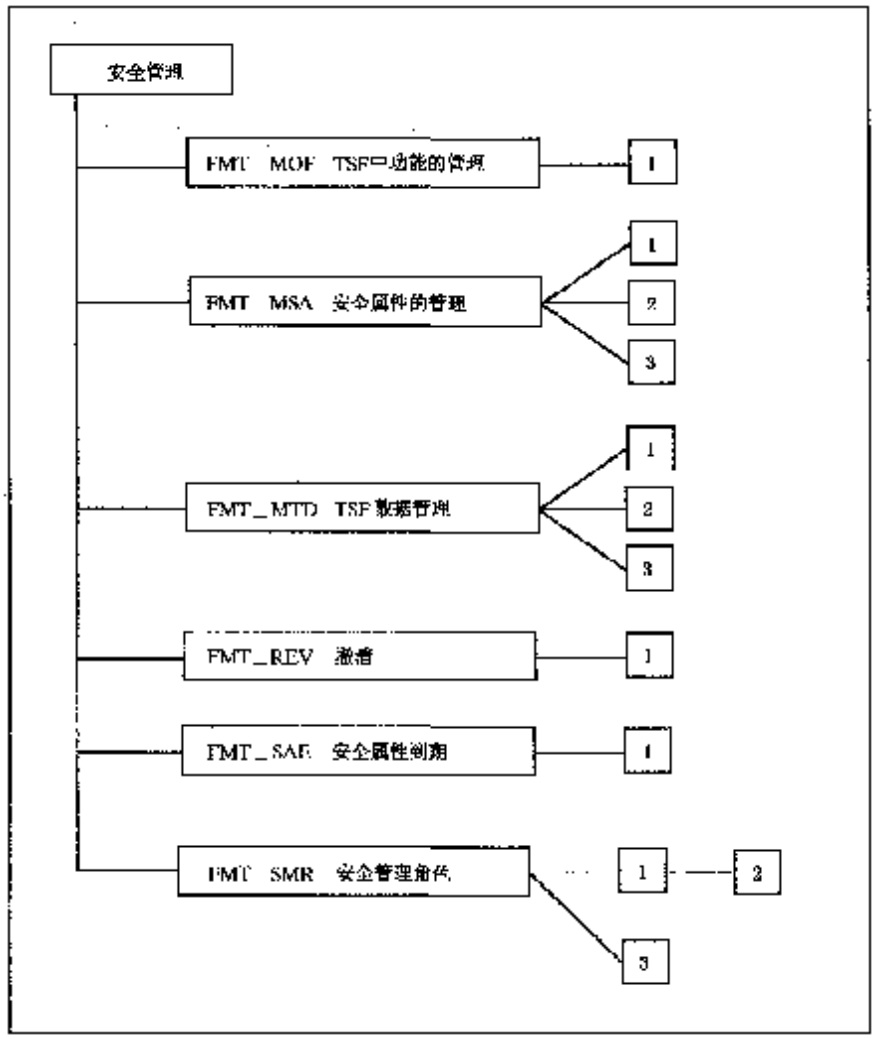


图 9.1　安全管理类分解

9.1　TSF 中功能的管理(FMT _ MOF)

子类行为

本子类允许授权用户控制 TSF 中功能的管理。例如审计功能和多重鉴别功能都是 TSF 中的功能实例。

组件层次

[redacted]

FMT _ MOF.1　安全功能行为的管理，允许授权用户(角色)管理 TSF 中使用规则或具有指定可

管理条件的功能的行为。

管理:FMT _ MOF.1

FMT 中的管理功能,可考虑如下行动:

a) 管理可以与 TSF 中的功能相互作用的角色组。

审计:FMT _ MOF.1

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生,下列事件应可审计:

a) 基本级:TSF 中功能行为的所有改动。

FMT _ MOF.1 安全功能行为的管理

从属于:无其他组件。

FMT _ MOF.1.1 TSF 应仅限于[赋值:已识别授权角色]对功能[赋值:功能列表]具有[选择:确定其行为,禁止,允许,修改其行为]的能力。

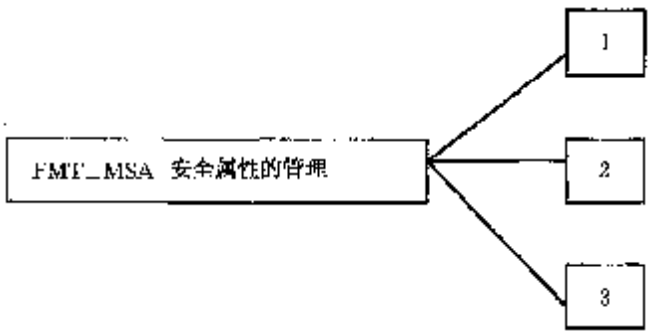
依赖关系:FMT _ SMR.1 安全角色

9.2 安全属性的管理(FMT _ MSA)

子类行为

本子类允许授权用户控制安全属性的管理。这种管理可能包括查看和修改安全属性的能力。

组件层次



FMT _ MSA.1 安全属性的管理,允许授权用户(角色)管理指定的安全属性。

FMT _ MSA.2 安全的安全属性,确保赋给安全属性的值针对安全状态是有效的。

FMT _ MSA.3 静态属性初始化,确保安全属性的默认值实际上设成了适当的允许或禁止。

管理:FMT _ MSA.1

FMT 中的管理功能,可考虑如下行动:

a) 管理可以和安全属性交互的角色组。

管理:FMT _ MSA.2

尚无预见的额外管理活动。

管理:FMT _ MSA.3

FMT 中的管理功能,可考虑如下行动:

a) 管理可以指定初始值的角色组;

b) 对于某给定的访问控制 SFP,管理默认值的允许或限制设置。

审计:FMT _ MSA.1

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生,下列事件应可审计:

a) 基本级:所有对安全属性值的改动。

审计:FMT _ MSA.2

如果PP/ST中包括FAU _ GEN安全审计数据产生,下列事件应可审计:

a) 最小级:对某安全属性,所有提供和被拒绝的值;

b) 详细级:对某安全属性,所有提供和接受的安全值。

审计:FMT _ MSA.3

如果PP/ST中包括FAU _ GEN安全审计数据产生,下列事件应可审计:

a) 基本级:对允许或限制规则的默认设置的修改;

b) 基本级:所有对安全属性的初始值的修改。

FMT _ MSA.1 安全属性的管理

从属于:无其他组件。

FMT _ MSA.1.1 TSF应执行[赋值:访问控制SFP,信息流控制SFP],以仅限于[赋值:已标识的授权角色]能够对安全属性[赋值:安全属性列表][选择:改变默认值,查询,修改,删除,[赋值:其他操作]]。

依赖关系:[FDP _ ACC.1 子集访问控制,或
FDP _ IFC.1 子集信息流控制]
FMT _ SMR.1 安全角色

FMT _ MSA.2 安全的安全属性

从属于:无其他组件。

FMT _ MSA.2.1 TSF应确保安全属性只接受安全的值。

依赖关系:ADV _ SPM.1 非形式化的TOE安全策略模型
[FDP _ ACC.1 子集访问控制,或
FDP _ IFC.1 子集信息流控制]
FMT _ MSA.1 安全属性的管理
FMT _ SMR.1 安全角色

FMT _ MSA.3 静态属性初始化

从属于:无其他组件。

FMT _ MSA.3.1 TSF应执行[赋值:访问控制SFP,信息流控制SFP],以便为用于执行SFP的安全属性提供[选择:受限的,许可的,其他特性]默认值。

FMT _ MSA.3.2 TSF应允许[赋值:已标识授权角色]为生成的客体或信息指定替换性的初始值以代替原来的默认值。

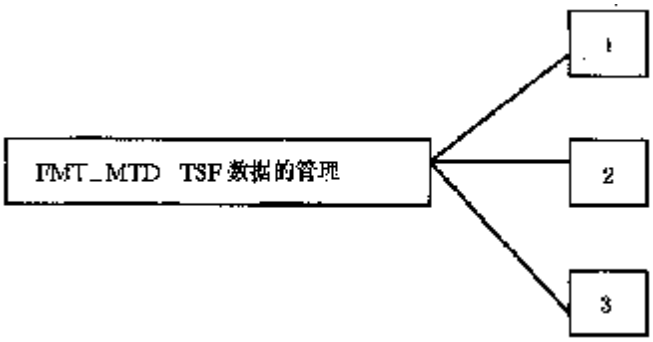
依赖关系:FMT _ MSA.1 安全属性的管理
FMT _ SMR.1 安全角色

9.3 TSF数据的管理(FMT _ MTD)

子类行为

本子类允许授权用户(角色)控制TSF数据的管理。这里的TSF数据包括审计信息、时钟、系统配置和其他TSF配置参数。

组件层次



FMT _MTD.1 TSF 数据的管理，允许授权用户管理 TSF 数据。

FMT _MTD.2 TSF 数据限值的管理，说明如果达到或超过了 TSF 数据的限值所应采取的行动。

FMT _MTD.3 安全的 TSF 数据，确保赋给 TSF 数据的值针对安全状态而言是有效的。

管理：FMT _MTD.1

FMT 中的管理功能，可考虑如下行动：

a) 管理可以和 TSF 数据相互作用的角色组。

管理：FMT _MTD.2

FMT 中的管理功能，可考虑如下行动：

a) 管理可以和 TSF 数据的限值相互作用的角色组

管理：FMT _MTD.3

尚无预见的额外管理活动。

审计：FMT _MTD.1

如果 PP/ST 中包括 FAU _GEN 安全审计数据产生，下列事件应可审计：

a) 基本级：所有对 TSF 数据的值的改动。

审计：FMT _MTD.2

如果 PP/ST 中包括 FAU _GEN 安全审计数据产生，下列事件应可审计：

a) 基本级：所有对 TSF 数据的限值的改动；

b) 基本级：在超出该限值时，对一切所要采取的行动的修改。

审计：FMT _MTD.3

如果 PP/ST 中包括 FAU _GEN 安全审计数据产生，下列事件应可审计：

a) 最小级：所有被拒绝的 TSF 数据的值。

FMT _MTD.1 TSF 数据的管理

从属于：无其他组件。

FMT _MTD.1.1 TSF 应仅限于[赋值：已标识的授权角色]能够对[赋值：TSF 数据列表] [选择：改变默认值，查询，修改，删除，清空，[赋值：其他操作]]。

依赖关系：FMT _SMR.1 安全角色

FMT _MTD.2 TSF 数据限值的管理

从属于：无其他组件。

FMT _MSA.2.1 TSF 应仅限于[赋值：已识别的授权角色]说明对[赋值：TSF 数据列表]的限值。

FMT _MSA.2.2 如果 TSF 数据达到或超过了指明的限值，TSF 应采取下面的行动：[赋值：要采取的行动]。

依赖关系：FMT _MTD.1 TSF 数据的管理

FMT _SMR.1　安全角色

FMT _MTD.3　安全的 TSF 数据
从属于:无其他组件。
FMT _MSA.3.1　TSF 应确保 TSF 数据只接受安全的值。
依赖关系:ADV _SPM.1　非形式化 TOE 安全策略模型
FMT _MTD.1　TSF 数据的管理

9.4　撤消(FMT _REV)

子类行为

本子类涉及 TOE 内各种实体的安全属性的撤消。

组件层次

FMT _REV.1　撤消,提供对某一时刻将实施的安全属性的撤消。
管理:FMT _REV.1
FMT 中的管理功能,可考虑如下行动:
a) 管理能够调用撤消安全属性这一功能的角色组;
b) 管理可能发生撤消的用户、主体、客体和其他资源列表;
c) 管理撤消规则。
审计:FMT _REV.1
如果 PP/ST 中包括 FAU _GEN 安全审计数据产生,下列事件应可审计:
a) 最小级:撤消安全属性失败;
b) 基本级:所有撤消安全属性的尝试。

FMT _REV.1　撤消
从属于:无其他组件。
FMT _REV.1.1　TSF 应仅限于[赋值:已标识的授权角色]能够撤消 TSC 内与[选择:用户,主体,客体,其他附加资源]相关联的安全属性。
FMT _REV.1.2　TSF 应执行规则[赋值:撤消规则说明]。
依赖关系:FMT _SMR.1　安全角色

9.5　安全属性到期(FMT _SAE)

子类行为

本子类涉及对安全属性的有效性实施时间限制的能力。

组件层次

FMT _SAE.1　时限授权,为授权用户提供对指定的安全属性说明有效期的能力。

管理:FMT _SAE.1

FMT 中的管理功能,可考虑如下行动:

a) 管理支持有效期的安全属性表;

b) 如果到期,将要采取的行动。

审计:FMT _SAE.1

如果 PP/ST 中包括 FAU _GEN 安全审计数据产生,下列事件应可审计:

a) 基本级:属性有效期的说明;

b) 基本级:因属性到期而采取的行动。

FMT _SAE.1 时限授权

从属于:无其他组件。

FMT _SAE.1.1 TSF 应仅限于[赋值:已标识的授权角色]能够为[赋值:支持有效期的安全属性列表]说明有效期。

FMT _REV.1.2 对每个这样的安全属性,在超过指定的安全属性的有效期后,TSF 应能够[赋值:对每一安全属性将要采取的行动列表]。

依赖关系:FMT _SMR.1 安全角色

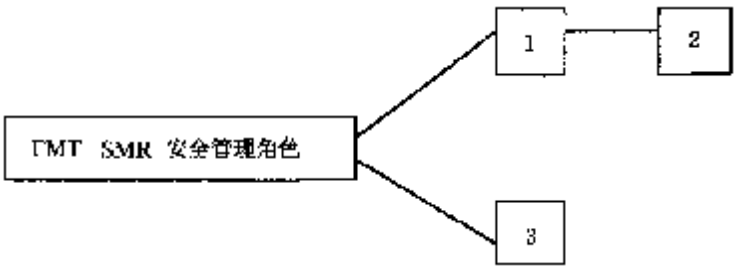
FPT _STM.1 可靠时间戳

9.6 安全管理角色(FMT _SMR)

子类行为

本子类目的是控制对用户指定不同角色。这些角色的安全管理能力将在本类的其他子类中描述。

组件层次



FMT _SMR.1 安全角色,说明 TSF 认同的与安全相关的角色。

FMT _SMR.2 安全角色限制,除了对角色的说明外,还有控制角色之间关系的规则。

FMT _SMR.3 承担角色,要求向 TSF 明确请求承担某个角色。

管理:FMT _SMR.1

FMT 中的管理功能,可考虑如下行动:

a) 管理构成角色的一部分的用户组。

管理:FMT _SMR.2

FMT 中的管理功能,可考虑如下行动:

a）管理构成角色一部分的用户组；

b）管理角色必须满足的条件。

管理：FMT _SMR.3

尚无预见的额外管理活动。

审计：FMT _SMR.1

如果 PP/ST 中包括 FAU _GEN 安全审计数据产生，下列事件应可审计：

a）最小级：对构成角色一部分的用户组的修改；

b）详细级：对角色权限的每一次使用。

审计：FMT _SMR.2

如果 PP/ST 中包括 FAU _GEN 安全审计数据产生，下列事件应可审计：

a）最小级：对构成角色一部分的用户组的修改；

b）最小级：由于对角色所给定的条件，尝试使用某角色失败；

c）详细级：对角色权限的每一次使用。

审计：FMT _SMR.3

如果 PP/ST 中包括 FAU _GEN 安全审计数据产生，下列事件应可审计：

a）最小级：承担角色的明确请求。

FMT _SMR.1　安全角色

从属于：无其他组件。

FMT _SMR.1.1　TSF 应维护角色[赋值：已标识的授权角色]。

FMT _SMR.1.2　TSF 应能够把用户和角色关联起来。

依赖关系：FIA _UID.1　标识定时

FMT _SMR.2　安全角色限制

从属于：FMT _SMR.1

FMT _SMR.2.1　TSF 应维护角色[赋值：已标识的授权角色]。

FMT _SMR.2.2　TSF 应能够把用户和角色关联起来。

FMT _SMR.2.3　TSF 应确保条件[赋值：不同角色的条件]得到满足。

依赖关系：FIA _UID.1 标识定时

FMT _SMR.3　承担角色

从属于：无其他组件。

FMT _SMR.3.1　TSF 应要求承担下列角色[赋值：角色]的明确请求。

依赖关系：FMT _SMR.1　安全角色

10　FPR 类：隐私

此类包括隐私要求。这些要求为用户提供其身份不被其他用户发现或滥用的保护。

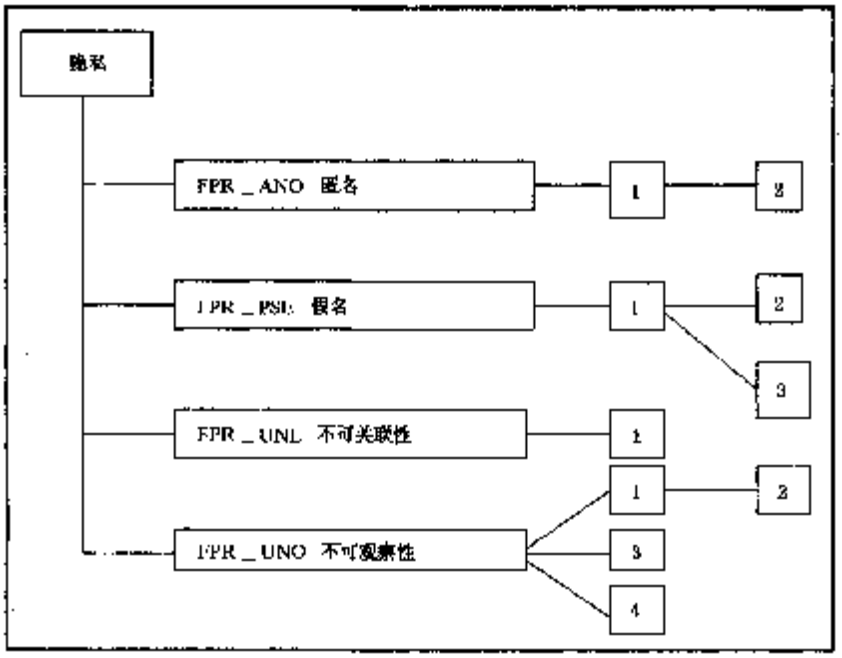


图 10.1 隐私类分解

10.1 匿名(FPR _ ANO)

子类行为

本子类确保一用户在使用资源或服务时不暴露他的身份。匿名需要对用户的身份提供保护。匿名并不保护主体的身份。

组件层次

FPR _ ANO.1 匿名,要求其他用户或主体不能决定与某个主体或操作所绑定的那一用户的身份。

FPR _ ANO.2 无征求信息的匿名,通过确保 TSF 不询问用户身份来增强 FPR _ ANO.1 的要求。

管理:FPR _ ANO.1 ,FPR _ ANO.2

对这些组件,没有可预见的管理行动。

审计:FPR _ ANO.1 ,FPR _ ANO.2

如果在 PP/ST 中 FAU _ GEN 安全审计数据产生,则下面的行动应是可审计的。

a) 最小级:匿名机制的调用。

FPR _ ANO.1 匿名

从属于:无其他组件。

FPR _ ANO.1.1 TSF 应确保 [赋值:用户或主体集]不能确定与 [赋值:主体或操作或客体列表]绑定的真实用户名。

依赖关系:无依赖关系。

FPR _ ANO.2 无征求信息的匿名。

从属于:**FPR _ ANO.1**

FPR _ ANO.2.1 **TSF** 应确保 [赋值:用户或主体集]不能确定与[赋值:主体或操作或客体列表]绑定的真实用户名。

FPR _ ANO.2.2 **TSF** 应提供 [赋值:服务列表]给[赋值:主体列表],而不询问真实的用户名。

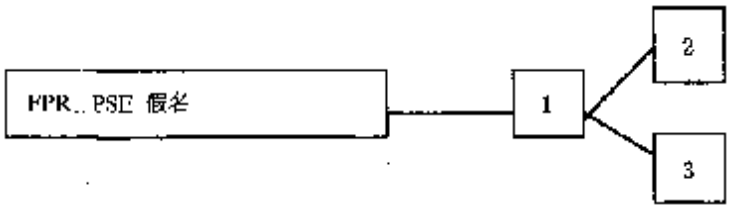
依赖关系:无依赖关系。

10.2 假名(FPR _ PSE)

子类行为

本子类确保一用户在使用资源或设备时不暴露其用户身份,但仍能对该次使用负责。

组件层次



FPR _ PSE.1 假名,要求一组用户或主体不能确定与主体或操作绑定的用户身份,但是该用户仍能对其行为负责。

FPR _ PSE.2 可逆假名,要求 TSF 根据所提供的化名提供一种确定原始用户身份的能力。

FPR _ PSE.3 化名假名,要求 TSF 对用户身份的化名采用某种构造规则。

管理:**FPR _ PSE.1**, **FPR _ PSE.2**, **FPR _ PSE.3**

对这些组件没有可能预知的管理行为。

审计:**FPR _ PSE.1**, **FPR _ PSE.2**, **FPR _ PSE.3**

如果 PP/ST 中包括 **FAU _ GEN** 安全审计数据产生,下面的行动应是可审计的。

a) 最小级:请求辨析用户身份的主体/用户。

FPR _ PSE.1 假名

从属于:无其他组件。

FPR _ PSE.1.1 **TSF** 应确保 [赋值:用户或主体集]不能确定与[赋值:主体或操作或客体列表]绑定的真实用户名。

FPR _ PSE.1.2 **TSF** 应能提供真实用户名的[赋值:化名的数目]个化名给 [赋值:主体列表]。

FPR _ PSE.1.3 **TSF** 应[选择:决定一用户的化名,接受该用户的化名]和验证它是否符合 [赋值:化名的量度]

依赖关系:无依赖关系。

FPR _ PSE.2 可逆假名

从属于:**FPR _ PSE.1**

FPR _ PSE.2.1 TSF 应确保 [赋值:用户或主体集]不能确定与[赋值:主体或操作或客体列表]绑定

的真实用户名。

FPR _ PSE.2.2 TSF 应能提供真实用户名的[赋值:化名的数目]个化名给 [赋值:主体列表]。

FPR _ PSE.2.3 TSF 应能 [选择:决定一用户的化名,接受该用户的化名]和验证它是否符合 [赋值:化名的量度]。

FPR _ PSE.2.4 TSF 应对[选择:授权用户,[赋值:可信主体列表]] 提供只在以下 [赋值:各种条件列表]下基于提供的化名来决定用户身份的能力。

依赖关系:FIA _ UID.1 标识定时

FPR _ PSE.3 化名假名

从属于:FPR _ PSE.1

FPR _ PSE.3.1 TSF 应确保 [赋值:用户或主体集]不能确定与[赋值:主体或操作或客体列表]绑定的真实用户名。

FPR _ PSE.3.2 TSF 应能提供真实用户名的[赋值:化名的数目]个化名给 [赋值:主体列表]。

FPR _ PSE.3.3 TSF 应能 [选择:决定一用户的化名,接受该用户的化名]和验证它是否符合 [赋值:化名的量度]。

FPR _ PSE.3.4 TSF 应能给真实用户名提供一化名,它应当与在以下[赋值:各种列表]下以前提供的化名相同,要不然提供的化名应与以前提供的化名毫不相关。

依赖关系:无依赖关系。

10.3 不可关联性(FPR _ UNL)

子类行为

本子类确保一用户可多次使用资源和服务,但任何人都不能将这些使用联在一起。

组件层次

FPR _ UNL.1 不可关联性,要求用户或主体不能决定是否同一个用户在系统中进行了某种特定的操作。

管理:FPR _ UNL.1

对于在 FMT 中的管理功能,要考虑以下的活动。

a) 不可关联功能的管理。

审计:FPR _ UNL.1

如果 PP/ST 中包括 FAU _ GEN 安全审计数据产生,下面的行动应是可审计的。

a) 最小级:不可关联性机制的调用。

FPR _ UNL.1 不可关联性

从属于:无其他组件。

FPR _ UNL.1.1 TSF 应确保 [赋值:用户或主体集]不能确定是否[赋值:操作列表][选择:由同一用户引起,与如下 [赋值:关系列表] 有关] 。

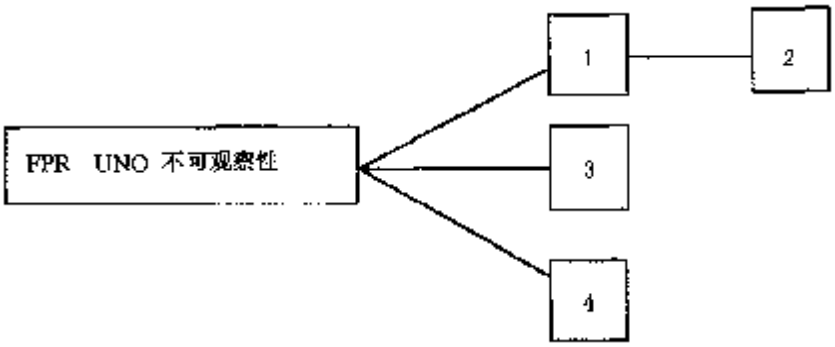
依赖关系:无依赖关系。

10.4 不可观察性(FPR _ UNO)

子类行为

本子类确保一用户在使用资源和服务时其他人尤其是第3方不能观察到该资源和服务正被使用。

组件层次



FPR _ UNO.1 不可观察性，要求用户或主体不能确定一个操作是否在执行。

FPR _ UNO.2 影响不可观察性的信息的分配，要求TSF能提供专门的机制以防止TOE内有关隐私信息的集中。当出现安全性损害时，如此的集中可能会影响到不可观察性。

FPR _ UNO.3 无征求信息的不可观察性，要求TSF不要试图获得可能会损害不可观察性的有关隐私信息。

FPR _ UNO.4 授权用户可观察性，要求TSF能够提供给一个或多个授权用户观察资源或服务使用情况的能力。

管理：**FPR _ UNO.1，FPR _ UNO.2**

对FMT中的管理功能，可考虑以下活动：

a)不可观察性功能的行为的管理。

管理：**FPR _ UNO.3**

对这些组件没有可预知的管理活动。

管理：**FPR _ UNO.4**

对在FMT中的管理功能，可考虑以下活动：

a)有能力决定操作发生的授权用户列表。

审计：**FPR _ UNO.1，FPR _ UNO.2**

如果在PP/ST中包括FAU _ GEN安全审计数据产生，下面的行动应是可审计的。

a)最小级：调用不可观察性机制。

审计：**FPR _ UNO.3**

如果在PP/ST中包括FAU _ GEN安全审计数据产生时，就没有确定的行动可审计。

审计：**FPR _ UNO.4**

如果在PP/ST中包括FAU _ GEN安全审计数据产生，下面的行动应是可审计的。

a)最小级：用户或主体对资源或服务使用的观察行为。

FPR _ UNO.1 不可观察性

从属于：无其他组件。

FPR_UNO.1.1 TSF 应确保[赋值:用户或主体列表]不能观察由[赋值:受保护的用户或主体列表]对[赋值:客体列表]进行的操作[赋值:操作列表]。

依赖关系:无依赖关系。

FPR_UNO.2 影响不可观察性的信息的分配

从属于:FPR_UNO.1

FPR_UNO.2.1 TSF 应确保[赋值:用户或主体列表]不能观察由[赋值:受保护的用户或主体列表]对[赋值:客体列表]进行的操作[赋值:操作列表]。

FPR_UNO.2.2 TSF 应在 TOE 的不同部分中分配[赋值:不可观察性相关信息],使得在信息的生存期间,下列条件成立:[赋值:条件列表]。

依赖关系:无依赖关系。

FPR_UNO.3 无征求信息的不可观察性

从属于:无其他组件。

FPR_UNO.3.1 TSF 应当在没有征求任何[赋值:隐私相关信息]的情况下为[赋值:主体列表]提供[赋值:服务列表]。

依赖关系:FPR_UNO.1 不可观察性。

FPR_UNO.4 授权用户可观察性

从属于:无其他组件。

FPR_UNO.4.1 TSF 应提供[赋值:授权用户集]观察[赋值:资源或服务列表]使用情况的能力。

依赖关系:无依赖关系。

11 FPT 类:TSF 保护

本类包含了多个功能要求子类。一方面与提供 TSF(和特定 TSP 无关)的机制的完整性和管理有关,另一方面与 TSF 数据(和 TSP 数据的特定内容无关)的完整性有关。在某种意义下,FPT 类的子类可能出现与 FDP 类(用户数据保护)中完全相同的组件;它们甚至用相同的机制来实现。但是,FDP 主要针对用户数据的保护,而 FPT 则针对 TSF 数据的保护。实际上,FPT 类的组件对保证 TOE 中的 SFP 不被篡改和旁路是必需的。

从 FPT 类的观点看,TSF 有以下三大部分:

a) TSF 抽象机,它可以是虚拟的,也可以是物理机器,这取决于评估执行时特定的 TSF 实现。

b) TSF 实现,在抽象机上执行并实现执行 TSP 的机制。

c) TSF 数据,这是指导执行 TSP 的管理数据库。

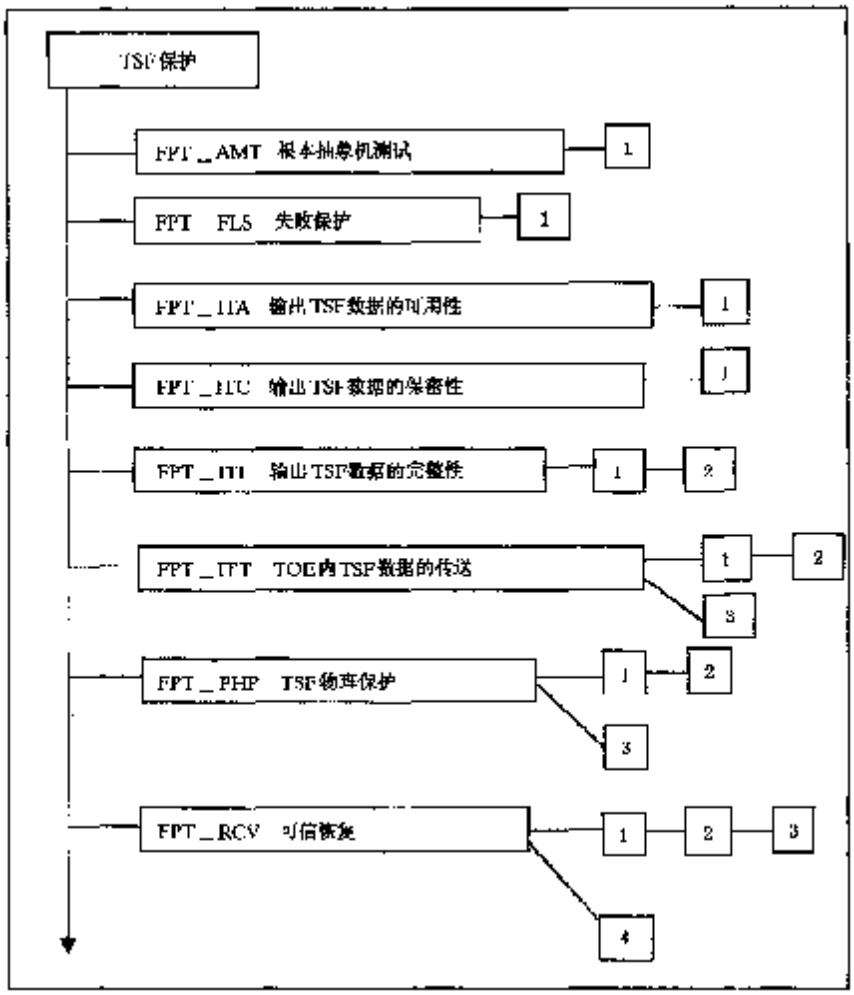


图 11.1 TSF 保护类分解

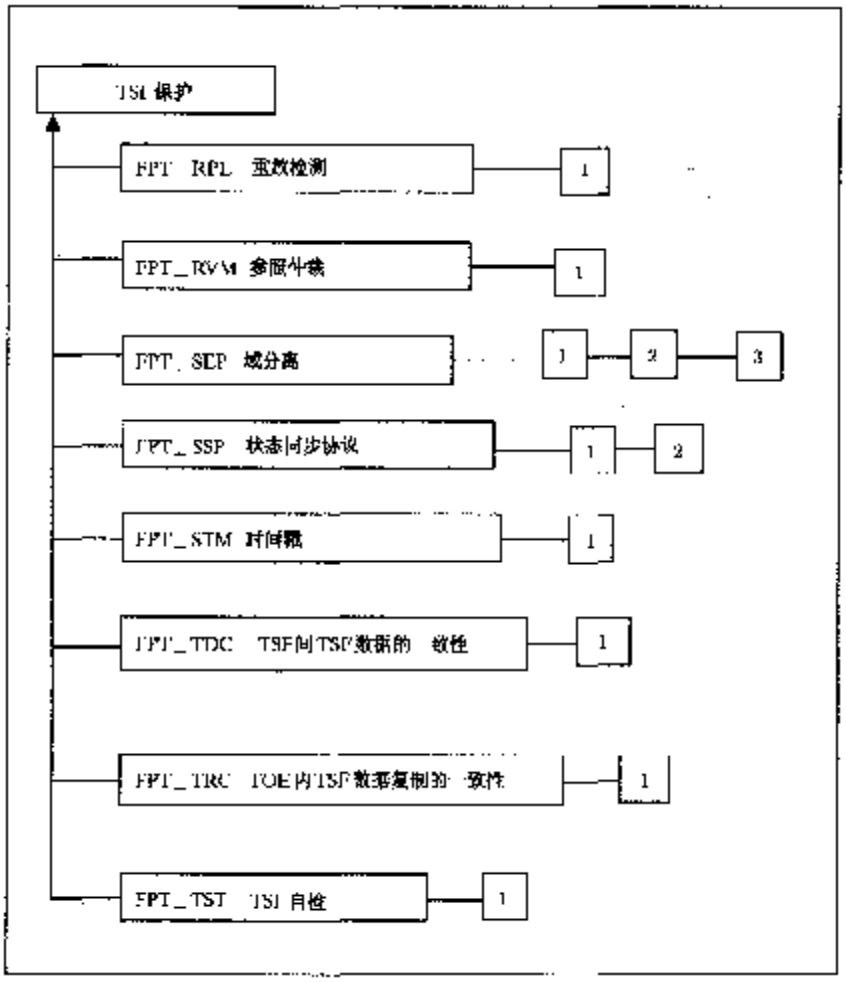


图 11.2　TSF 保护类分解

11.1　根本抽象机测试(FPT _ AMT)

子类行为

本子类定义了 TSF 执行用来验证所作的安全假定而进行测试的要求,这些安全假定是与 TSF 所依赖的根本抽象机有关的。这种“抽象的”机器既可以是硬件/固件平台,也可以是某些已知的并经评价的软硬件结合构成的虚拟机。

组件层次

FPT _ AMT.1　抽象机测试,提供了对根本抽象机的测试。

管理:FPT _ AMT.1

在 FMT 的管理功能中,考虑以下活动:

a) 抽象机测试产生条件的管理,比如初始启动期间、规定的时间间隔或在某些特定条件下。

b) 恰当的时间间隔管理。

审计:FPT _ AMT.1

如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生,下列行动应审计:

a) 基本级:抽象机的测试执行和测试结果。

FPT _ AMT.1　抽象机测试

从属于:无其他组件。

FPT _ AMT.1.1　TSF 应运行一测试套[选择:初始化启动期间,正常运转时周期性地,授权用户提出请求时,其他条件]来验证由 TSF 所基于的抽象机提供的安全假定的正确执行。

依赖关系:无依赖关系。

11.2　失败保护(FPT _ FLS)

子类行为

本子类要求确保当 TSF 中确定的失败类型出现时,该 TOE 不会违背其 TSP。

组件层次

本子类仅有一个组件,FPT _ FLS.1 带保存安全状态的失败,要求 TSF 当确定的失败出现时保存一个安全状态。

管理:FPT _ FLS.1

尚无可预知的管理活动。

审计:FPT _ FLS.1

如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生,下列行动应是可审计的:

a) 基本级:TSF 失败。

FPT _ FLS.1　带保存安全状态的失败

从属于:无其他组件。

FPT _ FLS.1.1　TSF 在下列失败发生时应保存一个安全状态[赋值:TSF 的失败类型列表]。

依赖关系:ADV _ SPM.1　非形式化的 TOE 安全策略模型

11.3　输出 TSF 数据的可用性(FPT _ ITA)

子类行为

本子类定义了一些规则,这些规则防止 TSF 数据在该 TSF 与一远程可信 IT 产品之间移动时失去其可用性。这些数据可能是 TSF 的关键数据,如口令、密钥、审计数据或 TSF 可执行的代码。

组件层次

本子类由一个组件组成:FPT _ ITA.1 在所定义可用性量度范围内的 TSF 间的可用性。本组件要求 TSF 以确定的可能性程度,确保向远程可信 IT 产品提供的 TSF 数据的可用性。

管理:FPT _ ITA.1

在 FMT 的管理功能中,可考虑以下活动:

a）管理对远程可信 IT 产品必须可用的 TSF 数据的类型列表。

审计：FPT _ ITA.1

如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生，下列行动应是可审计的：

a）最小级：TOE 要求 TSF 数据时，TSF 数据不存在。

FPT _ ITA.1　在所定义可用性量度范围内的 TSF 间的可用性

从属于：无其他组件。

FPT _ ITA.1.1　在下述条件[赋值：确保可用性的条件]下，TSF 应确保提供给[赋值：所定义可用性量度范围]内的远程可信 IT 产品的 [赋值：TSF 数据类型列表] 的可用性。

依赖关系：无依赖关系。

11.4　输出 TSF 数据的保密性(FPT _ ITC)

子类行为

本子类定义了保护 TSF 数据在 TSF 与远程可信 IT 产品之间传送时，不被未授权泄露的规则。这些数据可以是 TSF 的关键数据，如口令、密钥、审计数据或 TSF 的可执行代码。

组件层次

本子类仅有一个组件，FPT _ ITC.1　传送过程中 TSF 间的保密性，它要求 TSF 确保数据在 TSF 与远程可信 IT 产品间传送时不被泄露。

管理：FPT _ ITC.1

尚无可预见的管理活动。

审计：FPT _ ITC.1

即使 PP/ST 中包含 FAU _ GEN 安全审计数据产生，也没有确定的活动可审计。

FPT _ ITC.1　传送过程中 TSF 间的保密性

从属于：无其他组件。

FPT _ ITC.1.1　在 TSF 数据从 TSF 到远程可信 IT 产品的传送过程中，TSF 应保护所有的 TSF 数据不被未授权泄漏。

依赖关系：无依赖关系。

11.5　输出 TSF 数据的完整性(FPT _ ITI)

子类行为

这子类定义了一些保护规则，防止 TSF 数据在 TSF 与远程可信 IT 产品的传送过程中被未授权修改。这些数据可以是 TSF 的关键数据，如口令、密钥、审计数据或 TSF 的可执行代码。

组件层次

FPT _ ITI.1　TSF 间修改的检测，假设远程可信 IT 产品知道所使用的机制，则本组件提供了检测

在TSF与远程可信IT产品间传送的TSF数据是否在传送过程中被修改的能力。

FPT_ITI.2 TSF间修改的检测与改正，假设远程可信IT产品知道所使用的机制，则本组件提供了让远程可信IT产品不仅可以检测到TSF数据的修改，还可以更正被修改数据的能力。

管理：FPT_ITI.1

尚无可预见的管理活动。

管理：FPT_ITI.2

在FMT的管理功能中，可考虑以下活动：

a) 管理TSF数据的类型，本类TSF数据若在传送期间被修改，TSF应试图将其改正；

b) 管理TSF数据在传送过程中被修改后，TSF能采取的行动类型。

审计：FPT_ITI.1

如果PP/ST中包含FAU_GEN安全审计数据产生，下列行动应是可审计的：

a) 最小级：检测传送的TSF数据的修改；

b) 基本级：根据检测到的传送TSF数据被修改情况所采取的行动。

审计：FPT_ITI.2

当PP/ST中有FAU_GEN安全审计数据产生时，须进行下列审计：

a) 最小级：检测传送TSF数据是否被修改；

b) 基本级：根据检测到的传送TSF数据被修改情况所采取的行动；

c) 基本级：改正机制的使用。

FPT_ITI.1 TSF间修改的检测

从属于：无其他组件。

FPT_ITI.1.1 TSF应提供在下列量度范围内：[赋值：已定义的修改量度]，检测TSF与远程可信IT产品间传送的所有TSF数据是否被修改的能力。

FPT_ITI.1.2 TSF应提供验证在TSF与远程可信IT产品间传送的所有TSF数据的完整性及执行如果检测到修改所采取的[赋值：采取的行动]的能力。

依赖关系：无依赖关系。

FPT_ITI.2 TSF间修改的检测与改正

从属于：FPT_ITI.1

FPT_ITI.2.1 TSF应提供在下列量度范围内[赋值：定义的修改量度]，检测TSF与远程可信IT产品间传送的所有TSF数据被修改的能力。

FPT_ITI.2.2 TSF应提供验证在TSF与远程可信IT产品间传送的所有TSF数据的完整性执行，如果检测到修改所采取的[赋值：采取的行动]的能力。

FPT_ITI.2.3 TSF应提供改正在TSF与远程可信IT产品间传送的被修改的[赋值：修改类型]所有TSF数据的能力。

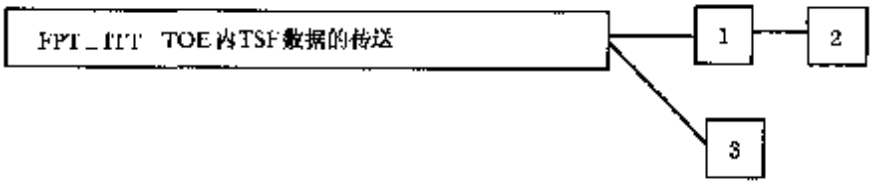
依赖关系：无依赖关系。

11.6 TOE内TSF数据的传送(FPT_ITT)

子类行为：

本子类提供了旨在使TSF数据当其通过内部信道在TOE的分离部分间传送时受到保护的要求。

组件层次



FPT_ITT.1 内部TSF数据传送的基本保护，要求对在TOE的分离部分间传送的TSF数据进行保护。

FPT_ITT.2 TSF数据传送的分离，要求TSF在传送过程中把用户数据从TSF数据中分离出来。

FPT_ITT.3 TSF数据完整性的监视，要求监视在TOE分离部分间传送的TSF数据的确定的完整性错误。

管理：**FPT_ITT.1**

在FMT的管理功能中，可考虑下面的活动：

a）管理TSF要防止的修改类型；

b）管理用来保护在TSF不同部分间传送的数据的保护机制。

管理：**FPT_ITT.2**

在FMT的管理功能中，可考虑下面的活动：

a）管理TSF要防止的修改类型；

b）管理用来保护在TSF不同部分间传送的数据的保护机制；

c）管理分离机制。

管理：**FPT_ITT.3**

在FMT的管理功能中，可考虑下面的活动：

a）管理TSF要防止的修改类型；

b）管理用来保护在TSF不同部分间传送的数据的保护机制；

c）管理TSF试图要检测的TSF数据的修改类型；

d）管理将采取的行动。

审计：**FPT_ITT.1**，**FPT_ITT.2**

如果PP/ST中包含FAU_GEN安全审计数据产生，没有可审计的确定的行动。

审计：**FPT_ITT.3**

如果PP/ST中包含FAU_GEN安全审计数据产生，下列行动应是可审计的：

a）最小级：检测TSF数据的改动；

b）基本级：检测到完整性错误后采取的行动。

FPT_ITT.1 内部TSF数据传送的基本保护

从属于：无其他组件。

FPT_ITT.1.1 TSF应保护TSF数据在TOE的分离部分间传送时不被[选择：泄漏，修改]。

依赖关系：无依赖关系。

FPT_ITT.2 TSF数据传送的分离

从属于：FPT_ITT.1

FPT_ITT.2.1 TSF应保护TSF数据在TOE的分离部分间传送时不被[选择：泄漏，修改]。

FPT_ITT.2.2 当数据在不同的TOE部分间传送时，TSF应将用户数据从TSF数据中分离出来。

依赖关系：无依赖关系。

FPT _ ITT.3　TSF 数据完整性监视

从属于:无其他组件。

FPT _ ITT.3.1　TSF 应能检测在 TOE 的分离部分间传送的 TSF 数据的[选择:数据的修改,数据的替换,数据的重排,数据的删除,[赋值:其他完整性错误]]。

FPT _ ITT.3.2　检测到数据的完整性错误后,TSF 应采取下列行动:[赋值:规定采取的行动]。

依赖关系: FPT _ ITT.1　内部 TSF 数据传送的基本保护

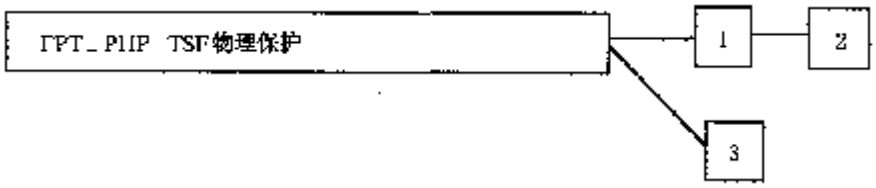
11.7　TSF 物理保护(FPT _ PHP)

子类行为

TSF 物理保护组件指限制对 TSF 的未授权的物理访问及阻止并抵抗对 TSF 未授权的物理修改及替换。

本子类组件的要求确保了 TSF 不被物理篡改和干扰。若满足了这些组件的要求,TSF 就可以用一种可检测出物理篡改或对物理篡改执行抵抗的方式封装起来并使用。如果没有这些组件,在物理危险无法避免的环境中 TSF 的保护功能就会失效。关于 TSF 如何对物理篡改企图作出反应,本子类也提供了要求。

组件层次



FPT _ PHP.1 物理攻击的被动检测,提供指示 TSF 设备或 TSF 元件遭到篡改的功能。但是检测到篡改后不会自动进行提示,授权用户必须激活安全管理功能或手动检查以判断篡改是否发生。

FPT _ PHP.2 物理攻击报告,对确定的一个物理侵入子集提供自动篡改报告。

FPT _ PHP.3 物理攻击抵抗,提供防止或抵抗对 TSF 设备和 TSF 元件的物理篡改的功能。

管理:FPT _ PHP.1,FPT _ PHP.3

没有可预见的管理活动。

管理:FPT _ PHP.2

在 FMT 的管理功能中,可考虑下面的活动:

a) 管理获取入侵报告的用户或角色;

b) 管理一系列设备,这些设备向指定的用户或角色报告入侵。

管理:FPT _ PHP.3

在 FMT 的管理功能中,可考虑下面的活动:

a) 管理对物理篡改的自动应答。

审计: FPT _ PHP.1

如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生,如下行动应是可审计的:

a) 最小级:用 IT 手段检测入侵。

审计: FPT _ PHP.2

如果 PP/ST 中给 FAU _ GEN 安全审计数据产生,如下行动应是可审计的:

a) 最小级:检测入侵。

审计: FPT _ PHP.3

如果PP/ST中包含FAU _GEN安全审计数据产生,没有确定的可审计的行动。

FPT _PHP.1　物理攻击的被动检测

从属于:无其他组件。

FPT _PHP.1.1　对可能危及TSF的安全的物理篡改提供明确的检测。

FPT _PHP.1.2　为TSF提供判断TSF设备或TSF元件是否已被物理篡改的能力。

依赖关系:FMT _MOF.1　安全功能行为管理

FPT _PHP.2　物理攻击报告

从属于:FPT _PHP.1

FPT _PHP.2.1　对可能危及TSF的安全的物理篡改提供明确的检测。

FPT _PHP.2.2　为TSF提供判断TSF设备或TSF元件是否已被物理篡改的能力。

FPT _PHP.2.3　对[赋值:需主动检测的TSF设备及元件列表],TSF应监视这些设备和元件,并当其发生物理篡改时通报给[赋值:指定的用户或角色]。

依赖关系:FMT _MOF.1　安全功能行为管理

FPT _PHP.3　物理攻击抵抗

从属于:无其他组件。

FPT _PHP.3.1　TSF应通过自动应答来抵抗对[赋值:TSF设备/元件列表]的[赋值:各种物理篡改],以遵从TSP。

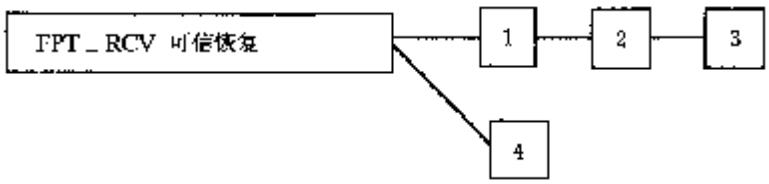
依赖关系:无依赖关系。

11.8　可信恢复(FPT _RCV)

子类行为

本子类的要求确保TSF能确定TOE是在没有减弱安全的状况下启动的,并在运行中断后能在不减弱保护的情况下恢复。因为TSF的启动状态决定了对后续状态的保护,故本子类是很重要的。

组件层次



FPT _RCV.1　手工恢复,容许TOE只提供人工干预以返回安全状态的机制。

FPT _RCV.2　自动恢复,至少对一种类型的服务中断,在无人工干预的情况下能恢复到安全状态;对其他类型服务中断的恢复可以要求人工干预。

FPT _RCV.3　无过度损失的自动恢复,也提供自动恢复,但通过不容许被保护客体的过度损失来加强要求。

FPT _RCV.4　功能恢复,在特定的SF级别上恢复,保障成功完成恢复或将TSF数据回到一个安全状态。

管理:FPT _RCV.1

在FMT的管理功能中,可考虑下面的活动:

a) 管理在维护模式下谁能够获得恢复能力。

管理:FPT _RCV.2 ,FPT _RCV.3

在FMT 的管理功能中,可考虑下面的活动:

a) 管理在维护模式下谁能够获得恢复能力;

b) 管理通过自动化过程来处理的失败及服务中断列表。

管理:FPT _RCV.4

没有可预见的管理活动。

审计: FPT _RCV.1 ,FPT _RCV.2 ,FPT _RCV.3

如果PP/ST 中含有FAU _GEN 安全审计数据产生,如下行动应是可审计的:

a) 最小级:出现失败或服务中断;

b) 最小级:恢复正常运行;

c) 基本级:失败或服务中断类型。

审计: FPT _PCV.4

如果PP/ST 中含有FAU _GEN 安全审计数据产生,如下行动应是可审计的:

a) 最小级:如有可能,安全功能失败后,不能返回到安全状态的可能性;

b) 基本级:如有可能,检测安全功能的失败情况。

FPT _RCV.1 手工恢复

从属于:无其他组件。

FPT _RCV.1.1 发生失败或服务中断后,TSF 应进入维护方式,该方式提供将TOE 返回到一个安全状态的能力。

依赖关系:FPT _TST.1 TSF 测试

AGD _ADM.1 管理员指南

ADV _SPM.1 非形式化的TOE 安全策略模型

FPT _RCV.2 自动恢复

从属于: FPT _RCV.1

FPT _RCV.2.1 当不能从失败或服务中断自动恢复时,TSF 应进入维护方式,该方式提供将TOE 返回到一个安全状态的能力。

FPT _RCV.2.2 对[赋值:失败/服务中断列表],TSF 应确保通过自动化过程使TOE 返回到一个安全状态。

依赖关系:FPT _TST.1 TSF 测试

AGD _ADM.1 管理员指南

ADV _SPM.1 非形式化TOE 安全策略模型

FPT _RCV.3 无过度损失的自动恢复

从属于: FPT _RCV.2

FPT _RCV.3.1 当不能从失败或服务中断自动恢复时,TSF 应进入维护方式,该方式提供将TOE 返回到一个安全状态的能力。

FPT _RCV.3.2 对[赋值:失败/服务中断列表],TSF 应确保通过自动化过程使TOE 返回到一个安全状态。

FPT _RCV.3.3 TSF 提供的从失败或服务中断状态恢复的功能,应确保TSC 内的TSF 数据或客体在无过度[赋值:数量]损失的情况下恢复到初始状态。

FPT _RCV.3.4 TSF 应提供决定客体能否被恢复的能力。

依赖关系:FPT _ TST.1　TSF 测试
AGD _ ADM.1　管理员指南
ADV _ SPM.1　非形式化的 TOE 安全策略模型

FPT _ RCV.4　功能恢复
从属于:无其他组件。
FPT _ RCV.4.1　TSF 应确保[赋值:SF 和失败情况列表]有如下特性,即 SF 或者被成功完成,或者对指明的失败情况恢复到一致的安全状态。
依赖关系:ADV _ SPM.1　非形式化的 TOE 安全策略模型

11.9　重放检测(FPT _ RPL)

子类行为

本子类解决对各种类型实体(如消息、服务请求及应答)的重放检测及随后的改正行动。只要检测出重放,就可以有效地避免重放。

组件层次

本子类仅有一个组件,FPT _ RPL.1 重放检测,它要求 TSF 能够检测出确定实体的重放。
管理:FPT _ RPL.1
在 FMT 的管理功能中,可考虑下面的活动:
a) 管理应该检测出其重放的确定实体列表;
b) 管理发生重放时须采取的行动列表。
审计:FPT _ RPL.1
如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生,如下行动应是可审计的:
a) 基本级:检测重放攻击;
b) 详细级:对特定情况采取的行动。

FPT _ RPL.1　重放检测
从属于:无其他组件。
FPT _ RPL.1.1　TSF 应检测以下实体的重放[赋值:确定实体列表]。
FPT _ RPL.1.2　检测到重放时,TSF 应执行 [赋值:具体操作列表]。
依赖关系:无依赖关系。

11.10　参照仲裁(FPT _ RVM)

子类行为

本子类要求解决传统参照监视器的“一直运行”这一方面。本子类的目的是对一个给定的 SFP,确保要求执行策略的所有行动,都必须由 TSF 根据 SFP 加以确认。如果 TSF 中执行该 SFP 的部分也满足来自 FPT _ SEP(域分离)和 ADV _ INT(TSF 内部)的合适组件的要求,那么 TSF 的该部分就为 SFP 提供了一个“参照监视器”。

当且仅当不可信主体所请求的有关任何或全部 SFP 的所有可执行行动(例如:访问客体)在成功前都要被 TSF 确认,实现该 SFP 的 TSF 才能提供有效抵抗非授权操作的保护。如果一个可被 TSF 执行

的操作，被不正确地执行或旁路，则该SFP的整体执行将受危害。这样，主体就可通过多种未授权的途径旁路掉该SFP(例如逃避对主体或客体的存取校验、旁路掉对保护措施由应用程序执行的客体的校验、将存取权保留到超过其预定的生存期、旁路掉对被审计行动的审计或旁路掉鉴别)。注意，某些主体，对SFP而言也称作“可信主体”，他们自己执行该SFP或许是可信的，并旁路掉该SFP的仲裁。

组件层次

本子类仅有一个组件，FPT _ RVM.1　TSP的不可旁路性，它要求对TSP中的所有SFP都不可旁路。

管理：FPT _ RVM.1

没有可预见的管理活动。

审计：FPT _ RVM.1

如果PP/ST中包含FAU _ GEN安全审计数据产生，无确定的行动是可审计的。

FPT _ RVM.1　TSP的不可旁路性

从属于：无其他组件。

FPT _ RVM.1.1　TSF应确保在TSC内允许继续执行每一项功能前，TSP的执行功能都被成功激活。

依赖关系：无依赖关系。

11.11　域分离(FPT _ SEP)

子类行为

本子类的组件确保TSF自己的执行时至少有一个安全域可用，并保护该TSF不被不可信主体从外部干扰篡改(如修改TSF编码或数据结构)。满足本子类要求的TSF具有自我保护能力，即不可信主体将不能修改或破坏该TSF。

本子类的要求如下：

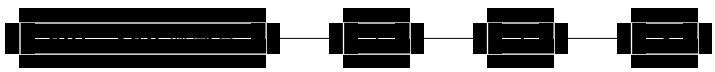
a) 将TSF的安全域(“保护域”)的资源和该域外的主体及不受约束的实体分离开，使得保护域外的实体不能观察或修改保护域内的TSF数据或TSF编码。

b) 域间的传送是受控的，不能随意地进入保护域或随意从保护域返回。

c) 通过传地址方式传到保护域的用户或应用参数，应通过保护域地址空间进行确认；而通过传值方式传到保护域的那些用户或应用参数，则应通过该保护域所期望的值进行确认。

d) 除了通过TSF控制的共享部分外，主体的安全域是不同的。

组件层次



FPT _ SEP.1　TSF域分离，为TSF提供不同的的保护域，并在TSC内将主体分离。

FPT _ SEP.2　SFP域分离，要求对TSF进一步细分成不同的域，一些是针对作为策略参照监视器的SFP的确定集合，一个是针对TSF剩余部分，也有一些是针对TOE内的非TSF部分。

FPT _ SEP.3　完全的参照监视器，要求有针对TSP执行的不同的域，有针对TSF剩余部分的

域，还有针对 TOE 内的非 TSF 部分的域。

管理：FPT _SEP.1，FPT _SEP.2，FPT _SEP.3

没有可预见的管理活动。

审计：FPT _SEP.1，FPT _SEP.2，FPT _SEP.3

如果 PP/ST 中包含 FAU _GEN 安全审计数据产生，无确定的活动可审计的。

FPT _SEP.1 TSF 域分离

从属于：无其他组件。

FPT _SEP.1.1 TSF 应为自身执行时维护一个安全域，防止不可信主体的干扰和篡改。

FPT _SEP.1.2 TSF 应分离 TSC 内各主体的安全域。

依赖关系：无依赖关系。

FPT _SEP.2 SFP 域分离

从属于：FPT _SEP.1

FPT _SEP.2.1 TSF 的未隔离部分应为自身执行时维护一个安全域，防止不可信主体的干扰和篡改。

FPT _SEP.2.2 TSF 应分离 TSC 内各主体的安全域。

FPT _SEP.2.3 TSF 应在一个安全域中为其自身执行维护与[赋值：访问控制或信息流控制 SFP 列表]有关的 TSF 部分，以防止他们被相对于这些 SFP 而言的不可信主体和 TSF 剩余部分的干扰和篡改。

依赖关系：无依赖关系。

FPT _SEP.3 完全的参照监视器

从属于：FPT _SEP.2

FPT _SEP.3.1 TSF 的未隔离部分应为自身执行维护一个安全域，防止不可信主体的干扰和篡改。

FPT _SEP.3.2 TSF 应分离 TSC 内各主体的安全域。

FPT _SEP.3.3 TSF 应在一个安全域中为其自身执行，维护执行访问控制或信息流控制 SFP 的 TSF 部分，以防止他们被相对于 TSP 而言的不可信主体和 TSF 剩余部分的干扰和篡改。

依赖关系：无依赖关系。

11.12 状态同步协议(FPT _SSP)

子类行为

分布式系统由于存在系统各部分间潜在的状态差别及通信延迟等问题，因而比单一系统复杂得多。大多数情况下，分布式功能间的状态同步涉及到交换协议，而不是一个简单的操作。当在这些协议的分布式环境中存在蓄意的危害时，就需要更为复杂的防御协议。

FPT _SSP 对 TSF 的某些关键安全功能使用该可信的协议提出了要求。FPT _SSP 确保 TOE 的两个分布部分(如主机)在完成与安全有关的活动后，状态保持同步。

组件层次

FPT _SSP.1 简单的可信回执，只要求数据接收者给出简单回执。

FPT _SSP.2 相互的可信回执，要求对交换数据相互回执。

管理:FPT _SSP.1,FPT _SSP.2

没有可预见的管理活动。

审计:FPT _SSP.1 ,FPT _SSP.2

如果PP/ST 中包含FAU _GEN 安全审计数据产生,如下行动应是可审计的:

a) 最小级:接收期待的回执时,发生失败。

FPT _SSP.1 简单的可信回执

从属于:无其他组件。

FPT _SSP.1.1 当TSF 的另一部分发出请求时,TSF 应对接收到未经修改的TSF 数据给出回执。

依赖关系:FPT _ITT.1 内部TSF 数据传送的基本保护

FPT _SSP.2 相互的可信回执

从属于:FPT _SSP.1

FPT _SSP.2.1 当TSF 的另一部分发出请求时,TSF 应对接收到未经修改的TSF 数据给出回执。

FPT _SSP.2.2 TSF 应通过回执来确保TSF 的有关部分知道在其各部分间传送数据处于正确状态。

依赖关系:FPT _ITT.1 内部TSF 数据传送的基本保护

11.13 时间戳(FPT _STM)

子类行为

本子类对TOE 内可靠的时间戳功能提出要求。

组件层次

本子类仅有一个组件,FPT _STM.1 可靠的时间戳,要求TSF 为TSF 功能提供可靠的时间戳。

管理:FPT _STM.1

在FMT 的管理功能中,可考虑下面的活动:

a) 时间管理。

审计:FPT _STM.1

如果PP/ST 中包含FAU _GEN 安全审计数据产生,如下行动应是可审计的:

a) 最小级:时间的变动;

b) 详细级:提供时间戳。

FPT _STM.1 可靠的时间戳

从属于:无其他组件。

FPT _STM.1.1 TSF 应能为自身的应用提供可靠的时间戳。

依赖关系:无依赖关系。

11.14 TSF 间TSF 数据的一致性(FPT _TDC)

子类行为

在分布式或复合系统环境下,TOE 或许需要与其他可信IT 产品交换TSF 数据(如与数据有关的SFP 属性、审计信息、标识信息等等)。本子类定义了一些要求,这些要求是关于TOE 的TSF 及不同的

可信 IT 产品间共享这些属性并对其作出一致性解释。

组件层次

FPT _ TDC.1　TSF 间基本 TSF 数据的一致性，要求 TSF 提供确保 TSF 间属性的一致性的能力。

管理：FPT _ TDC.1

没有可预见的管理活动。

审计：FPT _ TDC.1

如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生如下行动应是可审计的：

a）最小级：成功使用 TSF 数据一致性机制；

b）基本级：使用 TSF 数据一致性机制；

c）基本级：标识已解释的 TSF 数据；

d）基本级：检测被修改的 TSF 数据。

FPT _ TDC.1　TSF 间基本 TSF 数据的一致性

从属于：无其他组件。

FPT _ TDC.1.1　当 TSF 与其他可信 IT 产品共享 TSF 数据时，TSF 应提供对[赋值：TSF 数据类型列表]一致性解释的能力。

FPT _ TDC.1.2　当解释来自其他可信 IT 产品的 TSF 数据时，TSF 应使用[赋值：TSF 使用的解释规则列表]。

依赖关系：无依赖关系。

11.15　TOE 内 TSF 数据复制的一致性(FPT _ TRC)

子类行为

本子类的要求用以确保在 TOE 内部复制 TSF 数据的一致性。当 TOE 的内部不同部分间的信道不能工作时，这些 TSF 数据就可能不一致，如果 TOE 内部被构造成网络，而一部分网络连接又断掉了，则当那些部分失去正常工作能力时，就会发生这种不一致的情况。

组件层次

本子类仅有一个组件，FPT _ TRC.1　内部 TSF 的一致性，要求 TSF 确保在多点复制时，TSF 数据的一致性。

管理：FPT _ TRC.1

没有可预见的管理活动。

审计：FPT _ TRC.1

如果 PP/ST 中给 FAU _ GEN 安全审计数据产生如下行动应是可审计的：

a）最小级：重新连接时恢复一致性；

b）基本级：检测 TSF 数据间的不一致性。

FPT _ TRC.1　内部 TSF 的一致性

从属于:无其他组件。

FPT _ TRC.1.1　**TSF 应确保 TOE 各部分间的 TSF 数据复制的一致性。**

FPT _ TRC.1.2　**当包含复制的 TSF 数据的 TOE 部分断开时,TSF 应确保在处理任何对[赋值:依赖于 TSF 数据复制一致性的 SF 列表]的请求前,来自重建连接的复制的 TSF 数据的一致性。**

依赖关系:**FPT _ ITT.1　内部 TSF 数据传送的基本保护**

11.16　TSF 自检(FPT _ TST)

子类行为

本子类定义了一些关于 TSF 自检的要求,这些检测与期待的正确操作有关,如执行功能的接口和 TOE 关键部分的抽样算术运算。这些检测可在启动时进行,或周期性地进行,或应授权用户的请求进行,或满足其他条件时进行。TOE 根据自检结果所采取的行动在其他子类中定义。

本子类要求也用于检测由多种失败造成的 TSF 可执行码(如 TSF 软件)和 TSF 数据腐败,这些失败并不需要 TOE 停止工作(这将由别的子类处理)。因为这些失败不可避免,故必须执行这些检查。这些失败可能是由不可预见的失败方式或硬件、固件、软件设计的某些忽略所造成,或由于逻辑的或物理保护的不适当导致 TSF 恶意腐败所造成。

组件层次

FPT _ TST.1　**TSF 检测**,提供对 TSF 正确操作的测试能力。这些检测可在启动时进行,或周期性地进行,或当授权用户要求时,或满足别的条件时进行。同时也提供对 TSF 数据及可执行码的完整性的验证能力。

管理:**FPT _ TST.1**

在 FMT 的管理功能中,可考虑下面的活动:

a) 管理 TSF 自检产生条件,如初始化启动期间、固定间隔或特定条件;

b) 适当地管理时间间隔。

审计:**FPT _ TST.1**

如果 PP/ST 中包含 FAU _ GEN 安全核查数据产生如下行动应是可审计的:

a) 基本级:执行 TSF 自检及检测结果。

FPT _ TST.1　TSF 检测

从属于:无其他组件。

FPT _ TST.1.1　**TSF 应运行一套自检[选择:初始化启动期间,正常工作期间周期性地,授权用户要求,满足[赋值:产生自检的条件]]以表明 TSF 操作的正确性。**

FPT _ TST.1.2　**TSF 为授权用户提供对 TSF 数据完整性的验证能力。**

FPT _ TST.1.3　**TSF 为授权用户提供对存储的 TSF 可执行代码完整性的验证能力。**

依赖关系:**FPT _ AMT.1　抽象机测试**

12 FRU 类:资源利用

本类提供三个子类支持所需资源的诸如处理能力或存储能力。容错子类提供保护以防止由 TOE 失败引起的上述资源不可用。服务优先级子类确保资源将被分配到更重要的和时间要求更苛刻的任务中,而且不能被优先级低的任务所独占。资源分配子类提供可用资源的使用限制,从而防止用户独占资源。

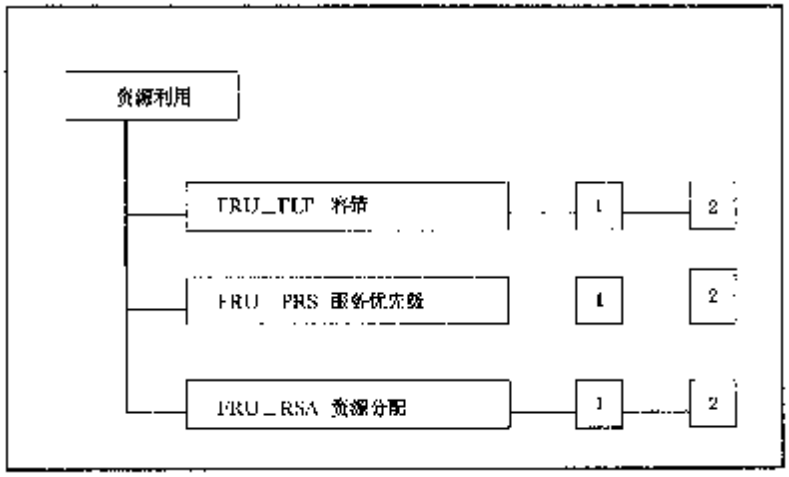


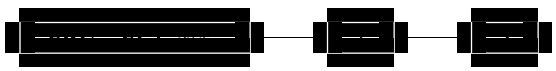
图 12.1 资源利用类分解

12.1 容错(FRU _ FLT)

子类行为

本子类的要求确保 TOE 即便出现故障事件也将维持正常运转。

组件层次



FRU _ FLT.1 低容错,要求 TOE 在确定的故障事件下能继续正确运行确定的能力。

FRU _ FLT.2 受限容错,要求 TOE 在确定的故障事件下能继续正确运行全部能力。

管理: FRU _ FLT.1,FRU _ FLT.2

没有可预见的管理活动。

审计:FRU _ FLT.1

如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生,以下行动应是可审计的:

a) 最小级:TSF 检测出的任何故障;

b) 基本级:所有由于一故障而中断的 TOE 能力。

审计:FRU _ FLT.2

如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生,以下行动应是可审计的:

a) 最小级:TSF 检测出的任何故障。

FRU _FLT.1 低容错

从属于:无其他组件。

FRU _FLT.1.1 TSF 应确保当以下故障[赋值:故障类型列表]发生时[赋值:TOE 能力列表]能运行。

依赖关系:FPT _FLS.1 带保存安全状态的失败

FRU _FLT.2 受限容错

从属于:FRU _FLT.1

FRU _FLT.2.1 TSF 应能确保当[赋值:故障类型列表]发生时所有 TOE 能力均能运行。

依赖关系:FPT _FLS.1 带保存安全状态的失败

12.2 服务优先级(FRU _PRS)

子类行为

本子类的要求允许 TSF 控制用户和主体对 TSC 资源的使用,使得 TSC 内高优先级任务的完成总是不受低优先级的务造成的过分干扰或延迟影响。

组件层次

FRU _PRS.1 有限服务优先级,提供主体使用 TSC 内某个资源子集的优先级。

FRU _PRS.2 全部服务优先级,提供主体使用 TSC 内全部资源的优先级。

管理:FRU _PRS.1, FRU _PRS.2

在 FMT 的管理功能中,可考虑下列活动:

a) 在 TSF 中每个主体优先级的分配。

审计:FRU _PRS.1, FRU _PRS.2

如果 PP/ST 中包含 FAU _GEN 安全审计数据产生,以下行动应是可审计的:

a) 最小级:对基于使用配置中优先级的操作的拒绝;

b) 基本级:包括服务功能的优先级在内的配置功能的所有尝试运用。

FRU _PRS.1 有限服务优先级

从属于:无其他组件。

FRU _PRS.1.1 TSF 应给在 TSF 中的每个主体分配一种优先级。

FRU _PRS.1.2 TSF 应确保对[赋值:受控资源]的每次访问都应该基于主体配得的优先级进行协调。

依赖关系:无依赖关系。

FRU _PRS.2 全部服务优先级

从属于:FRU _PRS.1

FRU _PRS.2.1 TSF 应给在 TSF 中的每个主体分配一种优先级。

FRU _PRS.2.2 TSF 应确保对所有可共享资源的每次访问都应基于主体配得的优先级进行协调。

依赖关系:无依赖关系。

12.3 资源分配(FRU _ RSA)

子类行为

本子类的要求允许TSF控制用户和主体对资源的使用,使得不因未授权地独占资源而出现拒绝服务。

组件层次

FRU _ RSA.1 最高配额,要求配额机制确保用户和主体将不会独占某种受控的资源。

FRU _ RSA.2 最低和最高配额,要求配额机制确保用户和主体,至少获得最小的规定资源且不会独占受控资源。

管理:FRU _ RSA.1

在FMT的管理功能中,可考虑以下活动:

a) 由管理者为用户组、单个用户或主体规定某资源的最大使用限度。

管理:FRU _ RSA.2

在FMT的管理功能中,可考虑以下活动:

a) 由一管理者为用户组、单个用户或主体规定某资源的最小和最大使用限度。

审计:FRU _ RSA.1, FRU _ RSA.2

如果PP/ST中包含FAU _ GEN安全审计数据产生,以下行动应是可审计的。

a) 最小级:由于资源的限制导致分配操作的拒绝;

b) 基本级:对TSF控制资源的资源分配功能的所有尝试使用。

FRU _ RSA.1 最高配额

从属于:无其他组件。

FRU _ RSA.1.1 TSF应对以下资源:[赋值:受控资源]分配最高配额,这些资源是[选择:单个用户,预定义用户组,主体] 能 [选择:同时地,在规定的时间间隔内]使用的。

依赖关系:无依赖关系。

FRU _ RSA.2 最低和最高配额

从属于:FRU _ RSA.1

FRU _ RSA.2.1 TSF应对以下资源:[赋值:受控资源]分配最高配额,这些资源是[选择:个体用户,定义的用户组,主体] 能 [选择:同时地,规定的时间间隔内]使用的。

FRU _ RSA.2.2 TSF应确保每个 [赋值:受控资源]最低量的供应,这些资源是[选择:个体用户,定义的用户组,主体] 能 [选择:同时地,规定的时间间隔内]使用的。

依赖关系:无依赖关系。

13 FTA类:TOE访问

本类规定用以控制建立用户会话的功能要求。图13.1给出了本类中子类的分解情况。

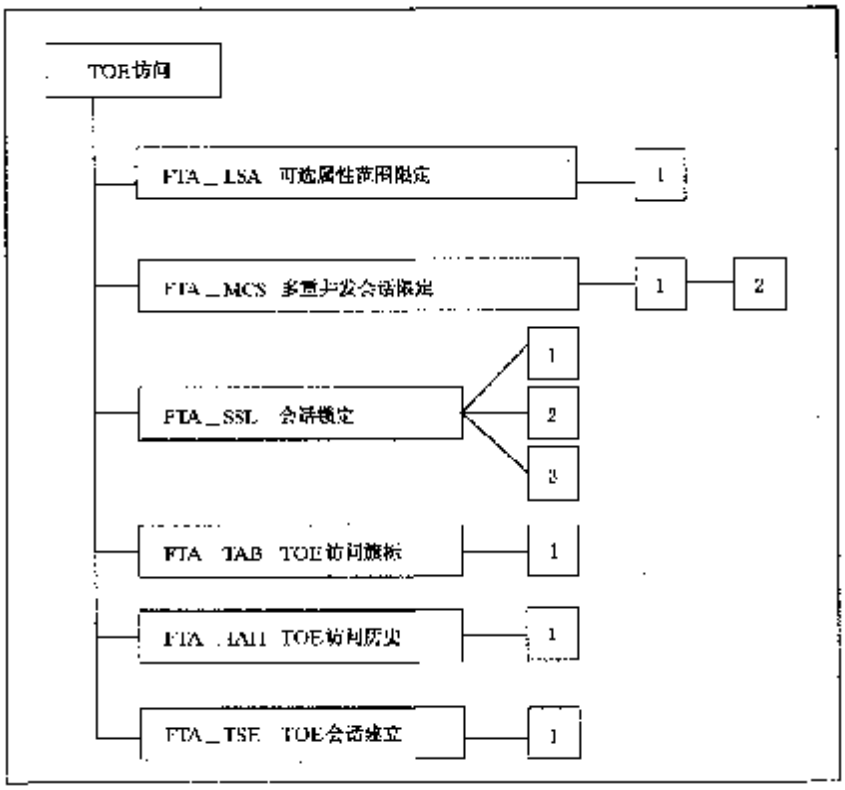


图 13.1 TOE 访问类分解

13.1 可选属性范围限定(FTA_LSA)

子类行为

本子类定义了限制用户选择会话安全属性范围的要求。

组件层次

FTA_LSA.1 可选属性范围限定,提供 TOE 建立会话时限制会话安全属性范围的要求。

管理:FTA_LSA.1

在 FMT 的管理行为中,可考虑以下活动:

a) 管理者对会话安全属性范围的管理。

审计:FTA_LSA.1

如果 PP/ST 中包含 FAU_GEN 安全审计数据产生,以下行动应是可审计的。

a) 最小级:选择某种会话安全属性的所有失败尝试;

b) 基本级:选择某种会话安全属性的所有尝试;

c) 详细级:每种会话安全属性的值的获得。

FTA_LSA.1 可选属性范围限定

从属于:无其他组件。

FTA _ LSA.1.1 **TSF** 应基于[赋值:属性] 限制会话安全属性 [赋值:会话安全属性]的范围 。
依赖关系:无依赖关系。

13.2 多重并发会话限定 (FTA _ MCS)

子类行为

本子类定义了同一用户并发会话的数量限制要求。

组件层次

FTA _ MCS.1 多重并发会话的基本限定,提供了适用于 TSF 内所有用户的限定。

FTA _ MCS.2 每个用户属性对多重并发会话的限定,通过要求有能力规定基于有关安全属性的并发会话数量的限定来对 FTA _ MCS.1 进行扩展。

管理:FTA _ MCS.1

在 FMT 的管理行为中,可考虑以下活动:

a) 管理者所允许的用户并发会话的最大数量的管理。

管理:FTA _ MCS.2

在 FMT 的管理行为中,可考虑以下活动:

a) 管理者所允许的用户并发会话的最大数量支配规则的管理。

审计:FTA _ MCS.1, FTA _ MCS.2

如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生,以下行动应是可审计的:

a) 最小级:基于多重并发会话限定对新会话的拒绝。

b) 详细级:当前的用户并发会话数和用户安全属性的获得 。

FTA _ MCS.1 多重并发会话的基本限定

从属于:无其他组件。

FTA _ MCS.1.1 **TSF** 应限制属于同一用户的并发会话的最大数量。

FTA _ MCS.1.2 **TSF** 应缺省执行每个用户[赋值:缺省数]次会话的限定。

依赖关系:FIA _ UID.1 标识定时

FTA _ MCS.2 每个用户属性对多重并发会话的限定

从属于:FTA _ MCS.1

FTA _ MCS.2.1 TSF 应依据规则[赋值:并发会话最大数目的规则] 对属于同一用户的并发会话最大数目加以限定。

FTA _ MCS.2.2 TSF 应缺省执行每个用户[赋值:缺省数]次会话的限定。

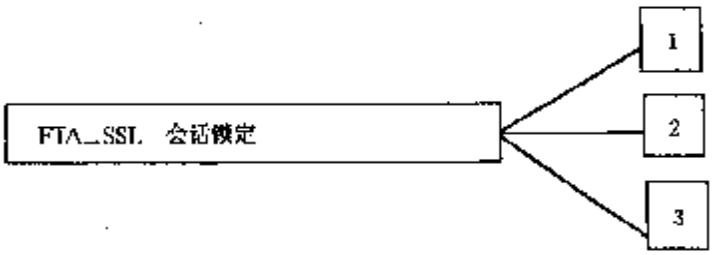
依赖关系:FIA _ UID.1 标识定时

13.3 会话锁定 (FTA _ SSL)

子类行为

本子类为 TSF 定义了提供 TSF 原发的和用户原发的交互式会话的锁定和解锁能力的要求。

组件层次



FTA _SSL.1 TSF 原发会话锁定，包括用户静止了规定的时间后，系统原发的交互会话锁定。

FTA _SSL.2 用户原发锁定，提供用户锁定和解锁其本身的交互会话的能力。

FTA _SSL.3 TSF 原发终止，在用户静止状态后的时间，为 TSF 提供在用户静止了一段时间后终止该会话的要求。

管理：FTA _SSL.1

在 FMT 的管理行为中，可考虑以下活动：

a) 在用户被锁定后，用户静止时间的规定；

b) 用户被锁定后，该用户被锁定的默认时间的规定；

c) 会话解锁前发生事件的管理。

管理：FTA _SSL.2

在 FMT 的管理行为中，可考虑以下活动：

a) 会话解锁前发生事件的管理。

管理：FTA _SSL.3

在 FMT 的管理行为中，可考虑以下活动：

a) 用户交互式会话终止后，该用户静止时间的规定；

b) 用户交互式会话终止后，该用户静止的默认时间的规定；

审计：FTA _SSL.1，FTA _SSL.2

如果 PP/ST 中包含 FAU _GEN 安全审计数据产生，以下行动应是可审计的。

a) 最小级：利用会话锁定机制对交互式会话的锁定；

b) 最小级：交互式会话的成功解锁；

c) 基本级：对交互式会话解锁的各种尝试；

审计：FTA _SSL.3

如果 PP/ST 中包含 FAU _GEN 安全审计数据的产生，以下行动应是可审计的。

a) 最小级：利用会话锁定机制对交互式会话的终止；

FTA _SSL.1 TSF 原发会话锁定

从属于：无其他组件。

FTA _SSL.1.1 应在[赋值：用户静止的时间间隔]后，通过以下方法锁定一交互式会话：

a) 在显示设备上清除或覆写，使当前的内容不可读；

b) 取消除了会话解锁之外的用户数据存取/显示设备的任何活动。

FTA _SSL.1.2 TSF 应要求先于会话解锁之前出现以下事件：[赋值：出现的事件]。

依赖关系：FIA _UAU.1 鉴别定时

FTA _SSL.2 用户原发锁定

从属于：无其他组件。

FTA _SSL.2.1 TSF 应允许通过以下方法实现对用户自己的交互会话的用户原发锁定：

a）在显示设备上清除或覆写，使当前的内容不可读；

b）取消除了会话解锁之外的用户数据存取/显示设备的任何活动。

FTA_SSL2.2 TSF 应要求先于会话解解锁之前出现下列事件，[赋值：出现的事件]

依赖关系：FIA_UAU.1 鉴别定时

FTA_SSL.3 TSF 原发终止

从属于：无其他组件。

FTA_SSL.3.1 TSF 应在 [赋值：用户静止的时间间隔]之后终止一交互式会话。

依赖关系：无依赖关系。

13.4 TOE 访问旗标(FTA_TAB)

子类行为

本子类定义了向用户显示有关适当使用 TOE 的可配置劝告性警示信息的要求。

组件层次

FTA_TAB.1 缺省的 TOE 访问旗标，为一“TOE 访问旗标”提供要求。该旗标应在会话的对话建立之前予以显示。

管理：FTA_TAB.1

在 FMT 的管理行为中，可考虑以下活动：

a）授权管理者对旗标的维护。

审计：FTA_TAB.1

如果 PP/ST 中包含 FAU_GEN 安全审计数据产生，没有确定的行动可审计。

FTA_TAB.1 缺省的 TOE 访问旗标

从属于：无其他组件。

FTA_TAB.1.1 在建立一用户会话之前，TSF 应显示有关未授权使用 TOE 的劝告性警示信息。

依赖关系：无依赖关系。

13.5 TOE 访问历史 (FTA_TAH)

子类行为

本子类定义了 TSF 在成功的会话建立的基础上，显示一用户级访问该用户帐号的成功的和不成功的访问历史的要求。

组件层次

FTA_TAH.1 TOE 访问历史，提供 TOE 显示与先前建立一个会话尝试相关的信息的要求。

管理：FTA_TAH.1

没有可预见的管理活动。

审计:FTA _ TAH.1

如果PP/ST中包含FAU _ GEN安全审计数据产生,就没有确定的行动可审计。

FTA _ TAH.1 TOE访问历史

从属于:无其他组件。

FTA _ TAH.1.1 在会话成功建立的基础上,TSF应显示用户上一次成功的会话建立的[赋值:日期,时间,方法,位置]。

FTA _ TAH.1.2 在会话成功建立的基础上,TSF应显示用户的上一次不成功的会话建立的尝试的[赋值:日期,时间,方法,位置]和从上一次成功的会话建立以来的不成功的尝试的次数。

FTA _ TAH.1.3 TSF在没有给用户回顾访问历史信息的机会的情况下,是不能从用户界面上抹去该信息的。

依赖关系:无依赖关系。

13.6 TOE会话建立(FTA _ TSE)

子类行为

本子类定义了拒绝允许用户与TOE建立会话的要求。

组件层次

FTA _ TSE.1 TOE会话建立,提供了拒绝用户基于属性对TOE访问的要求。

管理:FTA _ TSE.1

在FMT的管理行为中,可考虑以下活动:

a) 授权管理者对会话建立条件的管理。

审计:FTA _ TSE.1

如果PP/ST中包含FAU _ GEN安全审计数据产生,以下行动应是可审计的:

a) 最小级:依据会话建立的机制拒绝会话建立。

b) 基本级:一用户会话建立的所有尝试。

c) 详细级:所选的访问参数值(例如访问位置、访问时间)的获得。

FTA _ TSE.1 TOE会话建立

从属于:无其他组件。

FTA _ TSE.1.1 TSF应能拒绝基于[赋值:属性]的会话建立。

依赖关系:无依赖关系。

14 FTP类:可信路径/信道

本类中的子类提供关于用户和TSF之间可信通信路径,以及关于TSF和其他可信IT产品之间可信通信信道的要求。可信路径和信道有以下一般特点:

——通信路径使用内部和外部通信信道构成(对组件适当的话),它将TSF数据和命令的确定子集与余下的TSF和用户数据分开。

——通信路径的启用可由用户或TSF来发起(对组件适当的话)。

——通信路径有能力保证,用户正在同正确的TSF通信,并且TSF也正在同正确的用户通信(对组件适当的话)。

在本范例中,**可信信道**是可以由该信道的任何一端发起的一条通信信道,并且提供该信道两端身份的抗抵赖特性。

可信路径为用户提供一种手段,通过有保证地与TSF直接交互来执行功能。可信路径通常用于初始标识或鉴别等用户活动,但也可能用于用户会话过程中的其他时刻。可信路径的交换可以由用户或TSF发起。应确保经可信路径的用户应答受到保护,不会被不可信应用所修改或泄露给不可信应用。

图14.1给出了本类中子类的分解情况。

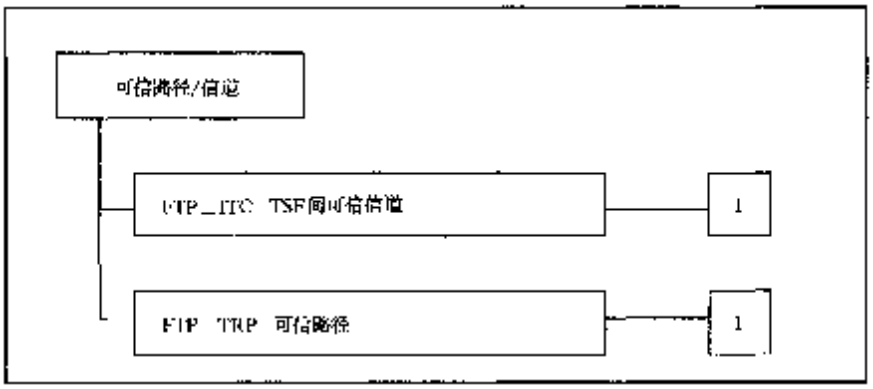


图14.1 可信路径/信道类分解

14.1 TSF间可信信道(FTP_ITC)

子类行为

本子类定义为执行关键的安全操作,在TSF和其他可信IT产品之间建立一可信信道的要求。每当存在TOE和其他可信IT产品之间的用户或TSF数据的保密通信的要求时,就应包括本子类。

组件层次

FTP_ITC.1 TSF间可信信道,要求TSF在它自身和另一个可信IT产品之间提供一条可信信道。

管理:FTP_ITC.1

FMT中的管理功能,可考虑如下行动:

a) 如果支持的话,配置需要可信信道的行动。

审计:FTP_ITC.1

如果PP/ST中包含FAU_GEN安全审计数据产生,下列行动应可审计。

a) 最小级:可信信道功能的失败;

b) 最小级:失败的可信信道功能的原发者及目标的标识;

c) 基本级:可信信道功能的所有使用尝试;

d) 基本级:所有可信信道功能的原发者及目标的标识。

FTP_ITC.1 TSF间可信信道

从属于:无其他组件。

FTP _ ITC.1.1 TSF 应在它自身和一远程可信 IT 产品之间提供一条通信信道,此信道在逻辑上与其他通信信道不同,并且对其端点提供确定的标识,以及保护信道中数据免遭修改和泄露。

FTP _ ITC.1.2 TSF 应允许 [选择:TSF,远程的可信 IT 产品]经可信信道发起通信。

FTP _ ITC.1.3 对于[赋值:需要可信信道的功能列表],TSF 应经可信信道发起通信。

依赖关系:无依赖关系。

14.2 可信路径(FTP _ TRP)

子类行为

本子类定义建立和维护用户和 TSF 的可信通信的要求。可信路径对任何与安全有关的交互活动可能都是需要的。可信路径的交换可以由用户在与 TSF 交互期间发起,或者 TSF 可能经一条可信路径与用户建立通信。

组件层次

FTP _ TRP.1 可信路径,要求对 PP/ST 作者定义的一组事件,在 TSF 和用户之间提供一条可信路径。用户或 TSF 均有能力发起该可信路径。

管理:FTP _ TRP.1

FMT 中的管理功能,可考虑如下行动:

a) 如果支持的话,配置需要可信路径的行动。

审计:FTP _ TRP.1

如果 PP/ST 中包含 FAU _ GEN 安全审计数据产生,下列行动应可审计:

a) 最小级:可信路径功能的失败;

b) 最小级:如果有的话,与所有可信路径故障相关的用户标识;

c) 基本级:所有可信路径功能的使用尝试;

d) 基本级:如果有的话,与所有可信路径的启用相关的用户标识。

FTP _ TRP.1 可信路径

从属于:无其他组件。

FTP _ TRP.1.1 TSF 应在它自身和 [选择:远程,本地] 用户之间提供一条通信路径,此路径在逻辑上与其他通信路径不同,并且对其端点提供确定的标识,以及保护通信数据免遭修改或泄露。

FTP _ TRP.1.2 TSF 应允许 [选择:TSF,本地用户,远程用户]经可信路径发起通信。

FTP _ TRP.1.3 对于[选择:初始化用户鉴别,[赋值:需要可信路径的其他服务]TSF 应要求使用可信路径。

依赖关系:无依赖关系。

附 录 A
（提示的附录）
安全功能要求应用注释

本附录包含本标准中的标准元素中定义的子类和组件的资料性指南，用户、开发人员和评估人员使用组件，可能需要这些指南。为了便于查找，本附录中类、子类和组件的表示与标准元素中的表示相似。但本附录中类、子类和组件的结构和本标准正文中的不同，因为本附录只是提示性的。

A1 注释的结构

本章定义与CC功能要求相关的注释的内容和表示。

A1.1 类结构

下面的图A1说明本附录中的功能类结构。

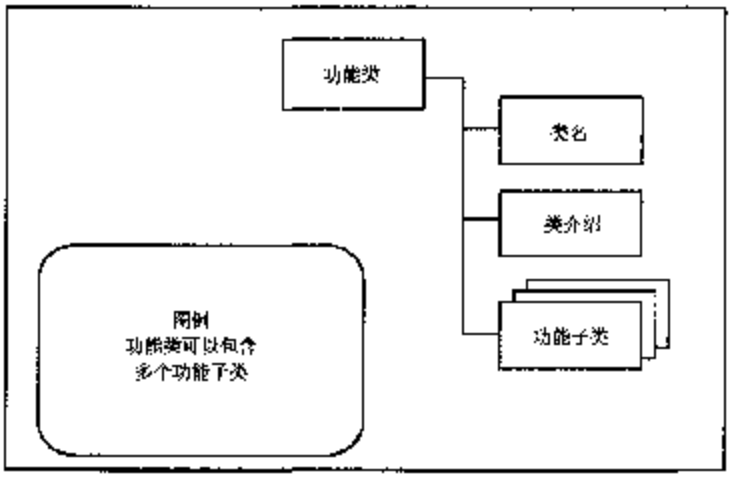


图 A1 功能类结构

A1.1.1 类名

这是本标准中标准元素定义的类的唯一名字。

A1.1.2 类介绍

本附录中的类介绍提供使用类中的子类和组件的有关信息，该信息使用图解方式提供，这些图解描述每个类的组织，以及每个子类中组件间的层次关系。

A1.2 子类结构

图A2用图解形式说明应用注释的功能子类结构。

A1.2.1 子类名

这是本标准中标准元素定义的子类的唯一名字。

A1.2.2 用户注释

用户注释包含功能子类潜在的用户感兴趣的附加信息，潜在用户包括使用功能组件的PP、ST和功能包的作者，以及TOE的开发者。说明是提示性的，可能涉及使用限制的警告，以及使用组件时应当特别注意的方面。

A1.2.3 评估者注释

评估者注释包含TOE开发者与评估者感兴趣的信息，该TOE声称符合子类中某一组件。表示是提示性的，可覆盖评估TOE时，需特别注意的各个方面。其中可包括澄清含义，说明表达要求的方式，以及评估者特别感兴趣的警告和说明等信息。

用户注释和评估者注释部分不是强制性的，仅在适当时出现。

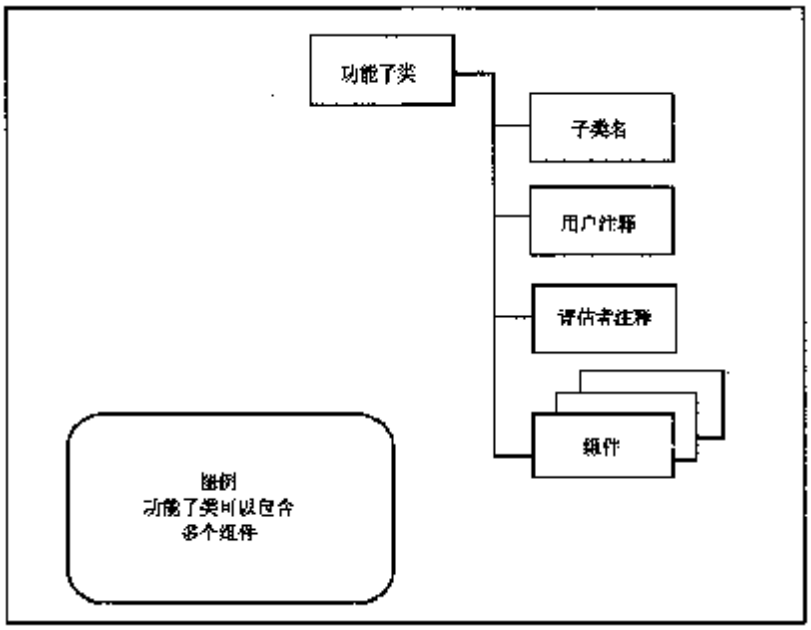


图 A2　功能子类结构

A1.3　组件结构

图 A3 说明应用注释的功能组件结构。

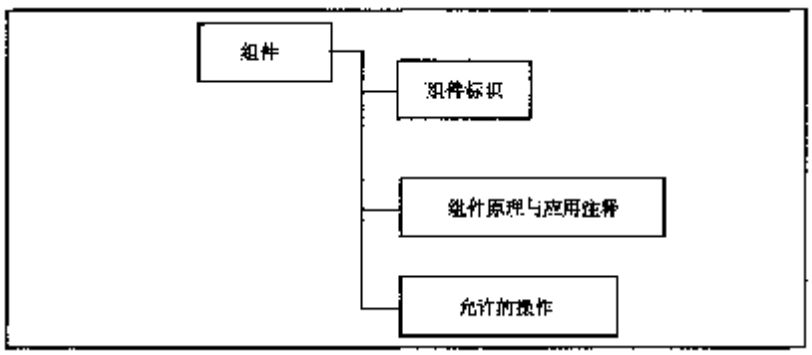


图 A3　功能组件结构

A1.3.1　组件标识

这是本标准中标准元素定义的组件的唯一名字。

A1.3.2　组件原理与应用注释

任何与组件有关的特定信息都可在本部分中找到。

——组件原理包括在特定级别下细化原理一般说明的细节，且应仅在要求加强该级别的情况下使用。

——应用注释包含用属于指定组件的限制陈述说明的附加细节。这种细化可适合于 A1.2 部分所描述的用户注释或评估者注释。这种细化可用于解释依赖关系的性质(例如，共享信息或共享操作)。

本部分不是必须的，仅在适当时出现。

A1.3.3　允许的操作

每个组件的这部分内容包括与该组件所允许的操作有关的建议。

本部分不是必须的，仅在适当时出现。

A2 依赖关系表

表 A1-功能组件依赖关系表，说明功能组件的直接、间接和可选的依赖关系。作为功能组件的依赖组件的每一个组件都在表中占据一列。每个功能组件都在表中占据一行。表格单元中的值表示行中标的组件是直接要求列中标的组件(用“×”表示)，间接要求列中标的组件(用“—”表示)，还是可选要求列中标的组件(用“○”表示)。例如，FDP _ ETC.1 具有可选依赖关系，要求出现 FDP _ ACC.1 或 FDP _ IFC.1，所以如果出现了 FDP _ ACC.1，就不必出现 FDP _ IFC.1，反之亦然。如果表格单元为空，则该组件不依赖于另一个组件。

表 A1 功能组件依赖关系表

	ADV_SPM.1	ACD_ADM.1	ACA_CCA.1	ACA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAA.2	FAU_SAA.3	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPR_UNO.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FAU _ ARP.1					—	×																											—					
FAU _ GEN.1																																	×					
FAU _ GEN.2					×																	×											—					
FAU _ SAA.1					×																												—					
FAU _ SAA.2																						×																
FAU _ SAA.3																																						
FAU _ SAA.4																																						
FAU _ SAR.1					×																												—					
FAU _ SAR.2					—	×																											—					
FAU _ SAR.3					—	×																											—					
FAU _ SEL.1					×																	—					×	—					—				
FAU _ STG.1					×																												—					
FAU _ STG.2					×																												—					
FAU _ STG.3					—		×																										—					
FAU _ STG.4					×																												—					
FCO _ NRO.1																						×																
FCO _ NRO.2																						×																
FCO _ NRR.1																						×																
FCO _ NRR.2																						×																
FCS _ CKM.1	—								—	○	×	○	—	—	—	—							—		—	×	—		—									
FCS _ CKM.2	—								○	—	×	—	—	—	—	○							—		—	×	—		—									
FCS _ CKM.3	—								○	—	×	—	—	—	—	○							—		—	×	—		—									
FCS _ CKM.4	—								○	—	—	—	—	—	—	○							—		—	×	—		—									
FCS _ COP.1	—								○	—	×	—	—	—	—	○							—		—	×	—		—									
FDP _ ACC.1													—	×	—	—							—		—		—		—									
FDP _ ACC.2													—	×	—	—							—		—		—		—									
FDP _ ACF.1													×	—	—	—							—		—		×		—									
FDP _ DAU.1																																						
FDP _ DAU.2																						×																
FDP _ ETC.1													○	—	○	—							—		—		—		—									
FDP _ ETC.2													○	—	○	—							—		—		—		—									
FDP _ IFC.1													—	—	—	×							—		—		—		—									

表 A1(续)

	ADV_SPM.1	AC D_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_IT T.2	FDP_UIT.1	FIA_AFL.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_SMR.1	FPR_UNO.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FDP_IFC.2													○	○	×																							
FDP_IFF.1													○	○	×																							
FDP_IFF.2													○	○	×																							
FDP_IFF.3			×										○	○	×																							
FDP_IFF.4			×										○	○	×																							
FDP_IFF.5				×									○	○	×																							
FDP_IFF.6			×										○	○	×																							
FDP_ITC.1													○	○																					×		○	
FDP_ITC.2													○	○																					×		○	
FDP_ITT.1													○	○																								
FDP_ITT.2													○	○																								
FDP_ITT.3													○	○		×																						
FDP_ITT.4													○	○			×																					
FDP_RIP.1																																						
FDP_RIP.2																																						
FDP_ROL.1													○	○																								
FDP_ROL.2													○	○																								
FDP_SDI.1																																						
FDP_SDI.2																																						
FDP_UCT.1													○	○																							○	○
FDP_UIT.1													○	○																							○	○
FDP_UIT.2													○	○						×																	×	
FDP_UIT.3													○	○						×																	×	
FIA_AFL.1																					×																	
FIA_ATD.1																																						
FIA_SOS.1																																						
FIA_SOS.2																																						
FIA_UAU.1																							×															
FIA_UAU.2																							×															
FIA_UAU.3																																						
FIA_UAU.4																																						
FIA_UAU.5																																						
FIA_UAU.6																																						
FIA_UAU.7																					×																	
FIA_UID.1																																						
FIA_UID.2																																						
FIA_USB.1																					×																	
FMT_MOF.1																																						
FMT_MSA.1													○	○																								
FMT_MSA.2	×												○	○																								
FMT_MSA.3													○	○																								

表 A1(续)

	ADV_SPM.1	ACD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPR_ANO.1	FPT_AMT.1	FPT_FLS.1	FPT_ITA.1	FPT_ITC.1	FPT_ITI.1	FPT_ITT.1	FPT_PHP.1	FPT_RCV.1	FPT_RPL.1	FPT_SEP.1	FPT_SSP.1	FTP_ITC.1	FTP_TRP.1
FMT_MTD.1																							—					×															
FMT_MTD.2																							—				×	×															
FMT_MTD.3	×																						—				×	—															
FMT_REV.1																							—					×															
FMT_SAE.1																							—					×															
FMT_SMR.1																							×																				
FMT_SMR.2																																											
FMT_SMR.3																							—					×															
FPR_ANO.1																																											
FPR_ANO.2																																											
FPR_PSE.1																																											
FPR_PSE.2																							×																				
FPR_PSE.3																																											
FPR_UNL.1																																											
FPR_UNO.1																																											
FPR_UNO.2																																											
FPR_UNO.3																																											
FPR_UNO.4																																											
FPT_AMT.1																																											
FPT_FLS.1	×																																										
FPT_ITA.1																																											
FPT_ITC.1																																											
FPT_ITI.1																																											
FPT_ITI.2																																											
FPT_ITT.1																																											
FPT_ITT.2																																											
FPT_ITT.3																																											
FPT_PHP.1																							—	×				—															
FPT_PHP.2																							—	×				—															
FPT_PHP.3																																											
FPT_RCV.1	×	×																															—				×						
FPT_RCV.2	×	×																															—				×						
FPT_RCV.3	×	×																															—				×						
FPT_RCV.4	×																																										
FPT_RPL.1																																											
FPT_RVM.1																																											
FPT_SEP.1																																											
FPT_SEP.2																																											
FPT_SEP.3																																											
FPT_SSP.1																																											
FPT_SSP.2																																											

表 A1(完)

	ADV_SPM.1	ACD_ADM.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPR_UNO.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FPT_STM.1																																			
FPT_TDC.1																																			
FPT_TRC.1																														×					
FPT_TST.1																												×							
FRU_FLT.1	—																												×						
FRU_FLT.2	—																												×						
FRU_PRS.1																																			
FRU_PRS.2																																			
FRU_RSA.1																																			
FRU_RSA.2																																			
FTA_LSA.1																																			
FTA_MCS.1																					×														
FTA_MCS.2																					×														
FTA_SSL.1																				×	—														
FTA_SSL.2																				×	—														
FTA_SSL.3																																			
FTA_TAB.1																																			
FTA_TAH.1																																			
FTA_TSE.1																																			
FTP_ITC.1																																			
FTP_TRP.1																																			

附 录 B
(提示的附录)
功能类、子类和组件

下面的附录 C 到附录 M 提供本标准正文中定义的功能类的应用注释。

附 录 C
(提示的附录)
安全审计(FAU)

CC 的审计子类允许 PP/ST 作者能够定义要求,以监控用户活动以及在某些情况下检测对 TSP 真实的、潜在的或即将发生的侵害。TOE 的安全审计功能用于帮助监控与安全有关的事件,并能对安全侵害起到威慑作用。审计子类的要求涉及到包括审计数据保护、记录格式和事件选择,以及分析工具、侵害报警和实时分析等功能。审计迹应以人们可以直接(例如:以人们可读的格式存储)或间接读取(例如:使用审计归纳工具)的格式加以提供,或以这两种格式提供。

当开发安全审计要求时,PP/ST 的作者必须对审计子类及其组件之间的相互关系加以注意。存在这样的可能:规定一组遵从子类/组件依赖表的审计要求,而同时导致有缺陷的审计功能(例如:某个审

计功能需要对所有与安全有关的事件加以审计，但是却缺乏在诸如单个用户或客体的任何一种合理的基础上对它们加以控制的选择)。

在分布式环境中的审计要求

对网络和其他大系统的审计要求，实现上可能明显地有别于那些独立系统。对于更大、更复杂和更活跃的系统而言，由于对所收集的审计数据进行解释(甚至存储)缺乏灵活性，所以必须更多地考虑收集哪些审计数据以及如何进行管理的问题。在一个随时可能发生许多事件的多时区全球网络中，被审计事件按时间排序表示“跟踪”的传统记法可能不适用。

此外，在分布式 TOE 中的不同主机和服务器将有不同的命名策略和赋值。对于审计查阅而言，符号表示名称可能需要在整个网络范围内约定以避免重复和“命名冲突”。

如果审计存储库服务于分布式系统，则可能需要一个多客体审计存储库，其每部分都可以接受潜在的大量授权用户的访问。

最后，应通过系统地避免本地存储与管理员活动有关的审计数据，解决授权用户对权限的滥用。

本类的组件构成分解如图 C1 所示。

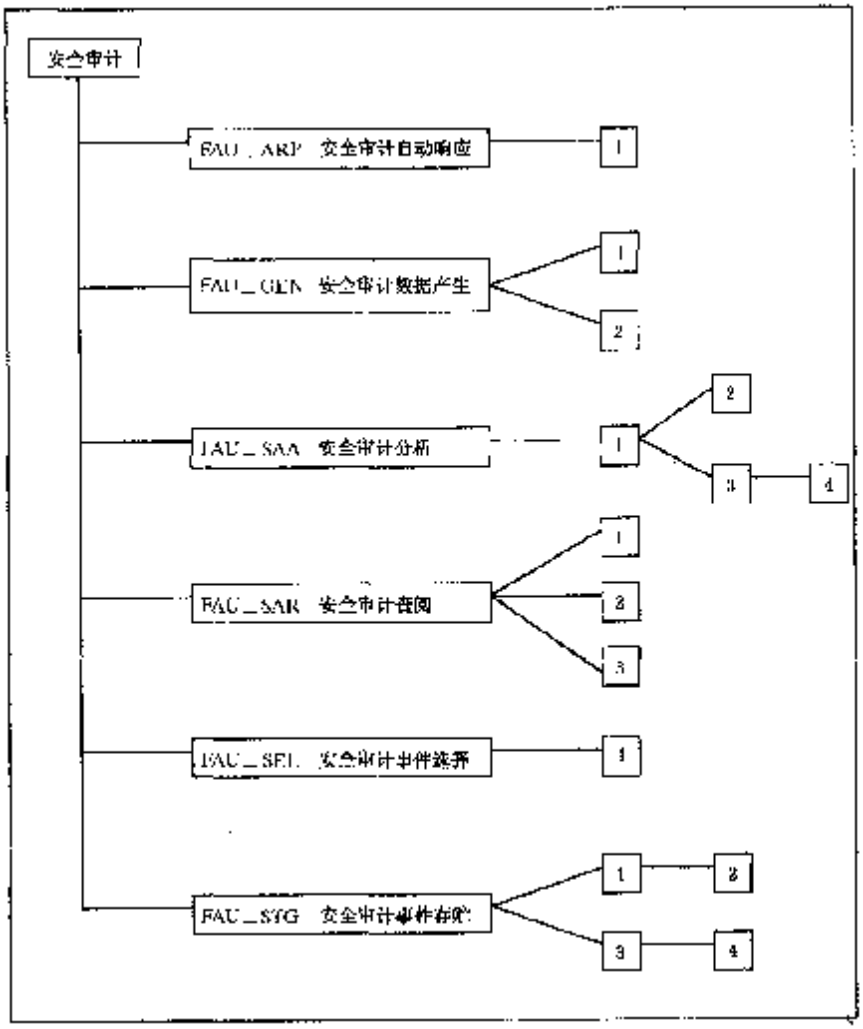


图 C1　安全审计类分解

C1 安全审计自动应答(FAU _ APR)

安全审计自动响应子类描述了处理审计事件的要求。这些要求包括警告或 TSF 行动(自动应答)。例如,TSF 可能包括实时报警的产生、违例进程的终止、服务的取消或者是用户帐号的断开与失效等。

应用注释

如果一个审计事件被定义为“潜在的安全侵害”,那么这个事件就由 FAU _ SAA 组件表示。

FAU _ APR.1 安全警告

用户应用注释

应在一个警告事件之后随即采取行动。这种行动可以是通知授权用户,可以是向授权用户提供一组可能的遏制行动,或采取纠正行动,PP/ST 作者应认真考虑采取这些行动的时间。

操作

赋值:

在 FAU _ ARP.1.1 中,PP/ST 作者应规定一旦出现潜在安全侵害事件时要采取的行动,例如:“通知授权用户,使产生潜在安全侵害的主体失效”,也可以规定由授权用户来确定要采取的行动。

C2 安全审计数据产生(FAU _ GEN)

安全审计数据产生子类包括了规定应由 TSF 对与安全有关的事件生成审计事件的要求。

为避免在所有需要审计支持的组件的依赖性中出现,本子类以下述方式提出,每个组件都设一个审计部分,在这部分中列出该功能域中要审计的事件。当 PP/ST 作者编写 PP/ST 时,在审计部分中的各项将用于填补该组件的变量。这样,对于一个功能域中能够被审计事件的详细描述就局限在该功能域中。

可审计事件列表完全依赖于 PP/ST 内的其他功能子类。所以每个子类的定义应包括本子类所规定的可审计事件的列表。在这个功能子类中所特定的可审计事件列表里,每个可审计事件必须相应于在本子类中所规定的某个级别的审计事件产生(例如,最小、基本和详细)。这就向 PP/ST 作者提供了必要的信息,以确保所有适当的可审计事件在 PP/ST 中加以规定。下面的例子说明了可审计事件如何在适当的功能子类中加以规定:

“如果 PP/ST 中包含了 FAU _ GEN 安全审计数据产生,那么下列行动应可审计:

a) 最小级:成功使用用户安全属性管理功能

b) 基本级:所有尝试使用用户安全属性管理功能

c) 基本级:验证用户安全属性已被修改

d) 详细级:除特定敏感属性数据项(例如,口令字,密钥等)以外,应俘获新的属性值。”

对于每一个选定的功能组件,该组件中所有可审计事件中,属 FAU _ GEN 指定的级别及以下级别的都应是可审计的。例如,如果在上面的例子中,FAU _ GEN 中选择了“基本级”,则 a),b)和 c)中提到的可审计事件必须是可审计的。

很明显,可审计事件的分类是层次化的。例如,当期望产生基本级审计时,通过使用适当赋值操作,应该将所有最小级或基本级的可审计事件包括在 PP/ST 之内,除非高级别的事件只是比低级别事件提供信息更详细。当期望产生详细级审计时,所有确定的可审计事件(最小级、基本级和详细级)都应该包括在 PP/ST 之内。

PP/ST 的作者可以决定增加一些给定审计级别要求之外的可审计事件。例如,PP/ST 尽管具备了

大部分基本级能力，因为有几个没有被包括进来的基本级能力与其他 PP/ST 约束条件相冲突，(例如，因为它们需要收集不可用的数据)，也只能称作有最小级审计能力。

应用注释

创建可审计事件功能应在 PP 或 ST 中作为一项功能要求加以规定。以下列举了在每个 PP/ST 功能组件之内，应该定义为可审计事件类型的例子：

a) 把 TSC 之内的客体引入主体的地址空间；

b) 删除客体；

c) 分配和撤消访问权限或能力；

d) 改变主体或客体的安全属性；

e) 当主体请求时，由 TSF 所执行的策略检查；

f) 使用旁路策略检查的访问权限；

g) 使用标识和鉴别功能；

h) 由操作员或授权用户采取的行动(例如，禁止可读标签方式的 TSF 保护机制)；

i) 从可移动介质输入或输出数据(例如，打印输出、磁带和磁盘等)。

FAU _ GEN.1 审计数据产生

用户应用注释

本组件定义，要求确定产生审计记录的可审计事件以及审计记录中所应提供的信息。

当 TSP 不要求用户身份与审计事件相关联，或当 PP/ST 包含私密要求时，可单独使用 FAU _ GEN.1。而如果必需结合用户身份，应增加使用 FAU _ GEN.2。

评估者应用注释

对 FPT _ STM 有依赖关系，如果时间的正确性不成为该 TOE 的一个问题，可删去这一依赖关系。

操作

选择：

对于 FAU _ GEN.1.1b，PP/ST 的作者应该选择 PP/ST 中由其他功能组件的审计部分引出的可审计事件的级别。这些级别可以是“最小级”，“基本级”，“详细级”或“未规定”等。如果选择“未规定”，则 PP/ST 作者应在 FAU _ GEN.1.1c 中列出所有期望的可审计事件，而这部分(b 项)可以完全取消。

赋值：

对于 FAU _ GEN.1.1c，PP/ST 的作者应该指定一份其他专门定义的可审计事件列表，一并归入可审计事件列表中。这些可审计事件可能来自比 FAU _ GEN.1.1.b 中所要求的审计级别更高的功能要求，也可能产生于使用特定的应用程序接口(API)。对于 FAU _ GEN.1.2b，PP/ST 的作者应对每个 PP/ST 中的可审计事件指定一份其他审计相关信息列表，并将其纳入审计事件记录中。

FAU _ GEN.2 用户身份关联

用户应用注释

本组件解决可审计事件责任追溯到单个用户身份级别上的要求。本组件应用作 FAU _ GEN.1“审计数据产生”的补充。

审计要求和隐私要求之间存在着潜在的冲突，为了审计，希望能了解谁完成了一个行动，而该用户则可能希望使他的行动只有自己知道，而不为他人识别出(如带作业提供的站点)，或者可能是组织安全

策略要求必须保护用户身份，在这些情况下，审计与隐私的目标是互相矛盾的。所以，如果选定这一审计要求，并且隐私也很重要，应考虑增加用户假名组件。隐私类中规定了基于假名确定真实用户名的要求。

C3 安全审计分析(FAU _ SAA)

本子类定义，要求提供分析系统活动和审计数据的自动化措施，以寻找可能的或真实的安全侵害。该分析可以入侵检测来支持，或对即将来临的安全侵害作出自动应答。

FAU _ ARP 安全审计自动应答组件定义了在检测到可能即将发生或潜在的安全侵害后，TSF 所采取的行动。

应用注释

为了实时分析，审计数据可能被转换成一个对自动处理有用的格式，而转换给授权用户用于查阅的是不同的格式。

FAU _ SAA.1 潜在的侵害分析

用户应用注释

本组件用于规定一个可审计事件集，这些事件的出现或累计出现表明有对 TSP 的潜在的侵害，本组件也规定用于执行侵害分析的所有规则。

操作

赋值：

对于 FAU _ SAA.1.2.a，PP/ST 作者应该确定已定义的可审计事件的子集，这些事件的出现或累计出现需要作为对 TSP 潜在的侵害的迹象来检测。

赋值：

在 FAU _ SAA.1.2.b 中，PP/ST 作者应该规定 TSF 用于其审计迹分析的所有其他规则，这些规则可以包括需要某些事件在确定的时间周期内(例如：天数，持续时间)出现的特殊要求。

FAU _ SAA.2 基于轮廓的异常检测

轮廓是一个表征用户或主体活动特征的结构，它表现了用户/主体怎样以各种方法与 TSF 交互。相应于用户/主体所从事的各种类型的活动建立使用模式，例如例外出现模式、资源利用模式(何时、哪个、怎样)、行为模式等。轮廓中记录各种类型的活动方法(例如：资源测量、事件计数器、定时器)，称做轮廓量度。

每个轮廓代表由轮廓目标组成员执行的预期使用模式。此模式可以基于过去的使用(历史模式)或相似目标组用户的正常使用(预期模式)。轮廓目标组指与 TSF 交互的一个或多个用户，轮廓组每个成员的活动被分析工具用于建立轮廓中出现的使用模式。以下是几个轮廓目标组的例子：

a) 单用户帐号：每个用户一个轮廓。

b) 组 ID 或组帐号：所有拥有同一个组 ID 或使用同一个组帐号的用户为一个轮廓。

c) 操作角色：共享一个给定操作角色的所有用户为一个轮廓。

d) 系统：一个系统的所有用户为一个轮廓。

对一个轮廓目标组的每个成员分配了一个单独的置疑等级，它表示成员的每个新活动对应于在组轮廓中已建立的使用模式的相近程度。

异常检测工具的复杂程度将主要由 PP/ST 要求的目标轮廓组的数量和要求的轮廓量度的复杂性来决定。

本组件用于规定一个可审计事件集，这些事件的出现或累计出现表明有对 TSP 的潜在的侵害，本组件也用来规定用于执行侵害分析的所有规则。该事件集或规则集能够由授权用户通过增加、修改或删除事件或规则来修改。

PP/ST 作者应该明确列举出由 TSF 监控或分析的活动。PP/ST 作者也应该明确确定构造的使用轮廓所需的相关活动信息。

FAU _ SAA.2 要求 TSF 维护系统使用轮廓。“维护”这个词隐含了异常检测工具基于轮廓目标组成员进行的新活动主动更新使用轮廓。重要的是由 PP/ST 作者来定义表现用户活动的量度准则，例如，一个个体可能完成一千个不同的行动，而异常检测工具可以仅选择监控这些活动的一个子集。异常活动可以像正常活动一样集成到轮廓中(假设工具正在监控那些活动)。在四个月以前可能已出现异常的事件经过一段时间，随着用户职责的改变可能已变成正常(反之亦然)。如果 TSF 利用轮廓更新算法过滤掉异常活动，它将不能够接受此记法。

应提供管理性通知使授权用户能理解的置疑等级的意义。

PP/ST 作者应定义如何解释置疑等级和向 FAU _ ARP 机制指示异常活动的条件。

操作

赋值：

对于 FAU _ SAA.2.1，PP/ST 作者应规定轮廓目标组。单个 PP/ST 可包括多个轮廓目标组。

对于 FAU _ SAA.2.3，PP/ST 作者应规定由 TSF 报告的异常活动的条件。条件可以包括达到某一确定值的置疑等级，或基于观察到的异常活动的类型。

FAU _ SAA.3 简单攻击探测

用户应用注释

实际上，很少有分析工具能确切检测到安全侵害即将何时发生，但确实有一些系统事件非常重要，值得进行单独查阅。这种事件如删除一个关键 TSF 安全数据文件(如：口令文件)或远程用户试图获得管理级特权的行为。这些事件称做 特征事件，它们隔离于系统其他活动的出现，表示为入侵活动。

给定工具的复杂程度将在很大程度上依赖于 PP/ST 作者在确定特征事件基础集时所定义的赋值。

为执行分析，PP/ST 作者必须逐一列举出哪些事件应该由 TSF 所监控。PP/ST 作者应标识那些与事件有关的必要信息，以决定该事件是否映射为特征事件。

应发出行政通告，使授权用户能够理解事件的含义以及如何做出适当的应答。

为了避免把审计数据作为监控系统活动唯一的输入，在这些功能要求的详细说明中要求利用以前开发的入侵检测工具，而该工具不只使用审计数据进行系统活动分析，(其他输入数据包括如：网络数据报、资源与计帐数据或者各类系统数据的组合等)。

FAU _ SAA.3 的元素不要求实现直接攻击探测的 TSF 与其活动受监控的 TSF 为同一个。因此，可以开发一个入侵检测组件，本组件能够独立于其活动正被分析的系统而操作。

操作

赋值：

对于 FAU _ SAA.3.1，PP/ST 作者应确定系统事件的一个基础子集，与所有其他系统活动隔离的这些事件的出现可能预示对 TSP 的违背，这个子集包括那些本身就清晰地指明对 TSP 违背的事件，或其出现对证明活动正常十分重要的事件。

对于 FAU _ SAA.3.2，PP/ST 作者应该规定用于判定系统活动的信息。该信息是分析工具所使用的输入数据，用来确定发生在 TOE 上的系统活动。这些数据可包括审计数据、审计数据与其他

系统数据的组合，或者也可由非审计数据组成。PP/ST 的作者应该精确定义在输入数据范围内正被监控的系统事件及其属性。

FAU _SAA.4　复杂攻击探测

用户应用注释

实际上，很少有分析工具能确切检测到安全侵害即将何时发生，但确实有一些系统事件非常重要，值得进行单独查阅。这种事件如删除一个关键 TSF 安全数据文件(如：口令文件)或远程用户试图获得管理级特权的行为。这些事件称做特征事件，它们隔离于系统其他活动的出现，表示为入侵活动。事件的序列是可指明入侵活动的特征事件有序集。

给定工具的复杂程度将在很大程度上依赖于 PP/ST 作者在确定特征事件基础集以及事件序列中所定义的赋值。

PP/ST 作者应定义一个由 TSF 表达的特征事件基础集和事件序列，附加的特征事件和事件序列可以由系统开发人员加以定义。

为执行分析，PP/ST 作者必须逐一列举出哪些事件应该由 TSF 所监控。PP/ST 作者应标识那些与事件有关的必要信息，以决定该事件是否映射为特征事件。

应发出行政通告，使得授权用户能够理解事件的含义以及如何做出适当的应答。

为了避免把审计数据作为监控系统活动唯一的输入，在这些功能要求的详细说明中要求利用以前开发的入侵检测工具，而该工具不只使用审计数据进行系统活动分析(，其他输入数据包括如：网络数据报、资源与计帐数据或者各类系统数据的组合等)，因此需要 PP/ST 作者定义用于监控系统活动的输入数据的类型。

FAU _SAA.4 的元素不要求实现复杂攻击探测的 TSF 与其活动受监控的 TSF 为同一个。因此，可以开发一个入侵检测组件，本组件能够独立于其活动正被分析的系统而操作。

操作

赋值：

对于 FAU _SAA.4.1，PP/ST 作者应确定系统事件序列列表的基础集，该类事件的出现表示已经有入侵的情况发生。这些事件序列表示已知的入侵情形，序列中表示的每一个事件应映射到受监控的一个系统事件，从而使得随着这些系统事件被执行，它们就映射到已知的入侵事件序列。

对于 FAU _SAA.4.1，PP/ST 作者应确定系统事件的一个基础子集，与所有其他系统活动隔离的这些事件可能预示对 TSP 的违背，它包括本身就清晰地指明对 TSP 的违背的事件，或其出现对证明活动正常十分重要的事件。

对于 FAU _SAA.4.2，PP/ST 作者应该规定用于判定系统活动的信息。该信息是分析工具所使用的输入数据，用来确定发生在 TOE 上的系统活动。这些数据可包括审计数据、审计数据与其他系统数据的组合，或者也可由非审计数据组成。PP/ST 的作者应该精确定义在输入数据范围内正被监控的系统事件及其属性。

C4　安全审计查阅(FAU _SAR)

安全审计查阅子类定义了与审计信息查阅有关的要求。

这些功能应该允许对审计选择预存储和事后存储，例如包括能够选择查阅下列几个方面内容：

——一个或者多个用户的行动(例如：标识，鉴别，TOE 输入项以及访问控制活动)。

——对一个特定客体或 TOE 资源采取的行动。

——规定的审计例外情况集的全部。

——与特定的TSP属性有关的行动。

应用注释

以下几种审计查阅之间的区别是基于功能性的。审计查阅只包含查阅审计数据的能力。而可选择的审计查阅更加复杂些，要求能够基于某个标准或带逻辑关系(即“与”，“或”)的多个条件执行搜索，并能够在查阅审计数据之前对它们进行分类和筛选。

FAU_SAR.1 审计查阅

用户应用注释

本组件用于规定用户或授权用户能够读取审计记录。审计记录将以适合于对用户的方式加以提供。不同类型的用户(个人用户、机器用户)可能有不同的需要。

可以规定能被查阅的审计记录内容。

操作

赋值：

在FAU_SAR.1.1中，PP/ST作者应该规定能够使用这种能力的授权用户。如果合适，PP/ST作者可以选择包括安全角色功能(参见FMT_SMR.1安全角色)。

在FAU_SAR.1.1中，PP/ST作者应该规定准许指定的用户从审计记录中获得信息的类型，例如：可以是“全部”、“主体身份”或“涉及这个用户的所有审计记录信息”。

FAU_SAR.2 有限审计查阅

用户应用注释

本组件规定，未在FAU_SAR.1中标识的所有用户不能读取审计记录。

FAU_SAR.3 可选审计查阅

用户应用注释

本组件规定应能对要查阅的审计数据进行选择。如果基于多个条件，这些条件之间必须具有某种逻辑关系(即“与”、“或”)，审计工具也应该提供处理审计数据的能力(如：分类、筛选等)。

操作

选择：

对于FAU_SAR.3.1中，PP/ST作者应该选定是否由TSF执行搜索、排序、分类。

赋值：

对于FAU_SAR.3.1，PP/ST作者应该指定用于选择查阅审计数据的条件(可能连同逻辑关系一起)。逻辑关系预期用于规定是否对单个属性或属性的集合进行操作。这种赋值可能形如：“应用、用户帐号或位置”，在这种情况下，操作可用应用、用户帐号和位置这三种属性的任意组合来规定。

C5 安全审计事件选择(FAU_SEL)

安全审计事件选择子类提供关于应能够在可能的可审计事件中确定哪一个要被审计的要求。FAU_GEN安全审计数据产生子类中定义了可审计事件，但这些事件在本组件中应定义为可选。

应用注释

本子类通过适当定义所选择的安全审计事件的粒度，确保存储的审计跟踪事件不至过于庞大而无法使用。

FAU_SEL.1 选择性审计

用户应用注释

组件定义了用于选择被审计事件的条件。这些条件允许根据用户属性、主体属性、客体属性或事件类型，增减可审计事件集中的事件。

本组件中并没有假设单个用户身份的存在性，如路由器等设备就可能是不支持用户记法的TOE。

对分布式环境，主机身份可以用做待审计事件的选择条件。

管理功能FMT_MTD.1(TSF数据的管理)将处理授权用户对选择进行查询或修改的权限。

操作

选择：

对于FAU_SEL.1.1a，PP/ST作者应该选择审计选择性所依据的安全属性是否与客体身份、用户身份、主体身份、主机身份或事件类型相关。

赋值：

对于FAU_SEL.1.1b，PP/ST作者应规定审计选择性所依据的所有附加属性。

C6 安全审计事件存储(FAU_STG)

安全审计事件存储子类描述了存储审计数据以备今后使用的要求，包括对由于系统失败、攻击或存储空间溢满等原因所引起审计数据丢失的控制要求。

FAU_STG.1 受保护的审计迹存储

应用注释

在分布式环境中，由于审计跟踪位于TSC中，但是不一定要与生成审计数据的功能模块在一起，PP/ST作者可能要求对该审计记录的原发者鉴别，或在将此记录存入审计迹之前请求记录的源抗抵赖。

TSF将保护审计迹免遭未经授权的删除或修改。值得注意的是在某些系统中，审计员(角色)可能在一定的时期内不能得到删除审计记录的授权。

操作

选择：

在FAU_STG.1.2中，PP/ST作者应该规定TSF是应防止还是只能检测审计迹的修改。

FAU_STG.2 审计数据可用性保证

用户应用注释

本组件允许PP/ST作者规定审计迹应该符合的量度准则。在分布式环境中，由于审计跟踪位于TSC中，但是不一定要与生成审计数据的功能模块在一起，PP/ST作者可能请求对该审计记录的原发者鉴别，或在将此记录存到审计跟踪中之前请求记录的源抗抵赖。

操作

选择：

在 FAU _ STG.2.2 中，PP/ST 作者应该规定 TSF 是应防止还是只能检测审计迹的修改。

在 FAU _ STG.2.3 中，PP/ST 作者应该规定 TSF 在某些条件下仍能维护确定数量的审计数据，这些条件可能是：审计存储空间溢满、失败和攻击。

赋值：

在 FAU _ STG.2.3 中，PP/ST 作者应对于审计迹规定 TSF 必须确保的量度。该量度通过计算必须保持的记录数或计算保证记录维护的时间来限制数据的丢失。例如：量度值“100000”就意味着能够存储 100000 条审计记录。

FAU _ STG.3 在审计数据可能丢失情况下的行动

用户应用注释

本组件要求当审计迹超过预先定义限定值时应采取行动。

操作

赋值：

在 FAU _ STG.3.1 中，PP/ST 作者应该指明预定义界限值。如果管理功能表明这个数值可被授权用户改变，该值便为默认值，PP/ST 作者可选择让授权用户来定义该值，在这种情况下，该赋值可以是“授权用户设定界限值”。

在 FAU _ STG.3.1 中，PP/ST 作者应该规定，由于超过门限表明即将发生审计存储失败时所应采取的行动，这些行动可能包括通知授权用户。

FAU _ STG.4　防止审计数据丢失

用户应用注释

本组件规定了审计迹已满时 TOE 的行为：或者忽略审计记录，或者冻结 TOE 以便不能发生任何可审计事件。本要求还说明无论怎样陈述这类要求，对此具有特殊权限的授权用户总可以继续生成可审计的事件(行动)，这是因为要不这样，授权用户甚至将无法重启系统。因此一旦审计存储空间溢满，应考虑选择 TSF 要采取的行动，如忽略事件，它既能提供 TOE 更好的可用性，也将准许不带记录且不可追查用户责任地执行行动。

操作

选择：

在 FAU _ STG.4.1 中，PP/ST 作者应该选定 TSF 是否忽略可审计的行动，或者是否应该防止可审计行动发生，或当 TSF 不能再存储审计记录时将最早的审计记录覆盖。

赋值：

在 FAU _ STG.4.1 中，PP/ST 作者应该规定一旦发生审计存储失效，所应采取的其他行动，例如：通知授权用户。

附　录　D
(提示的附录)
通信(FCO)

本类所描述的要求对用于传送信息的 TOE 有特殊意义。本类中各子类都涉及抗抵赖。

本类的组件构成分解如图 D1 所示。

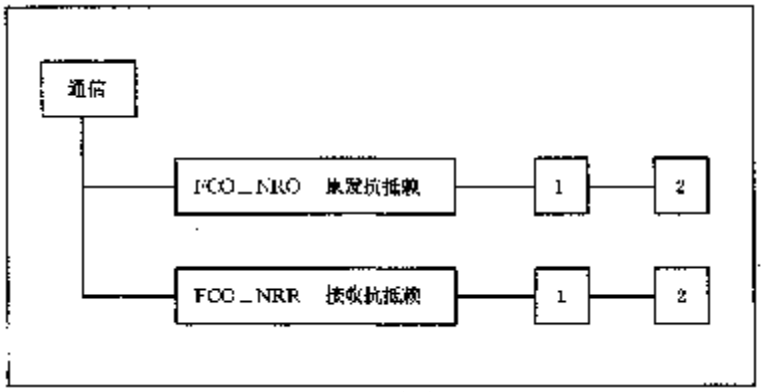


图 D1 通信类分解

本类中使用了“信息”这一概念。在这里信息应该解释为被交换的客体，它可以包括电子邮件消息、一个文件或一组预定义属性的类型集。

术语“接收证明”和“原发证明”通常在文献中使用，然而这里认为术语“证明”在法律意义上被解释为隐含某种数学原理。本类中的组件按“证据”的具体情况来解释如何“证明”TSF 显示了各种类型信息的抗抵赖传送。

D1 原发抗抵赖(FCO _ NRO)

原发抗抵赖定义了向用户/主体提供有关信息原发者的身份证据的要求。由于发送证据(例如：数字签名)在原发者和发送的信息之间提供了绑定证据，原发者不能成功地否认已发送该信息，接收者或第三方可验证原发证据，此证据应是不可伪造的。

用户注释

如果信息或相关属性被以任何方式改变，对原发证据的验证就可能失败。因此 PP/ST 作者应考虑在 PP/ST 中加入完整性要求，例如 FDT _ UIT.1 数据交换完整性。

抗抵赖涉及几个不同的角色，每个角色都可能结合一个或多个主体。第一个角色是请求原发证据的主体(仅在 FCO _ NRO.1 选择性原发证明中)，第二个角色是接收者和(或)其他向其提供证据的主体(例如：公证人)，第三个角色是请求验证原发证据的主体，例如：接收者或第三方(例如：仲裁者)。

PP/ST 作者必须规定为了能验证证据的有效性所必须满足的条件。例如：可能规定的一个条件是对证据的验证必须在 24 h 内进行。因此，这些条件允许按法律要求对抗抵赖进行裁剪，例如：能够在几年内提供证据。

在多数情况下，接收者的身份将是接收传送的用户的身份。在一些情况下，PP/ST 作者不希望用户身份被输出，此时 PP/ST 作者应该考虑包括此类是否合适，或者是否应使用传送服务提供者的身份或主机的身份。

除了(或代替)用户身份，一个 PP/ST 作者可能更关注信息被发送的时间。例如，提案请求必须在某个确定日期之前发送才能被接纳，在这种情形下，功能要求应能被定制以提供时间戳指示(原发时间)。

FCO _ NRO.1 选择性原发证明

操作

赋值：

在 FCO _ NRO.1.1 中，PP/ST 作者应将信息主体的类型填写到发功能的证据中，例如：电子邮件消息。

选择：

在 FCO _ NRO.1.1 中，PP/ST 作者应规定可以请求原发证据的用户/主体。

赋值：

在 FCO _ NRO.1.1 中，PP/ST 作者根据选择结果应规定能请求原发证据的第三方。第三方可以是仲裁者、法官和法律团体。

在 FCO _ NRO.1.2 中，PP/ST 作者应填写可链接到信息的属性表，例如：原发者身份、发送时间和发送位置。

在 FCO _ NRO.1.2 中，PP/ST 作者应在信息中填写信息域表，表上的属性提供发送证据，例如：消息体。

选择：

在 FCO _ NRO.1.3 中，PP/ST 作者应规定能验证发送证据的用户/主体。

赋值：

在 FCO _ NRO.1.3 中，PP/ST 作者应根据选择结果规定能验证原发证据的第三方。

在 FCO _ NRO.1.3 中，PP/ST 作者应填写限制表，证据在这些限制下被验证。例如：证据只能在 24 h 时间间隔之内被验证。一个“立即的”或“不确定的”赋值是可接受的。

FCO _ NRO.2　强制原发证明

操作

赋值：

在 FCO _ NRO.2.1 中，PP/ST 作者应将信息主体的类型填写到原发功能的证据中，例如：电子邮件消息。

在 FCO _ NRO.2.2 中，PP/ST 作者应填写可链接到信息的属性表，例如：原发者身份、发送时间和发送位置。

在 FCO _ NRO.2.2 中，PP/ST 作者应在信息中填写信息域表，表上的属性提供发送证据，例如：消息体。

选择：

在 FCO _ NRO.2.3 中，PP/ST 作者应规定能验证原发证据的用户/主体。

赋值：

在 FCO _ NRO.2.3 中，PP/ST 作者应根据选择结果规定能验证原发证据的第三方。

在 FCO _ NRO.2.3 中，PP/ST 作者应填写限制表，证据在这些限制下被验证。例如：证据只能在 24 小时时间间隔之内被验证。一个“立即的”或“不确定的”赋值是可接受的。

D2　接收抗抵赖(FCO _ NRR)

接收抗抵赖定义了向其他用户/主体提供信息已被接收者接收的证据的要求。由于接收证据(例如：数字签名)在接收者和接收的信息之间提供了绑定证据，接收者不能成功地否认已接收该信息，原发者或第三方可验证接收证据。此证据应是不可伪造的。

用户注释

应该注意的是，提供收到信息的证据不一定暗示信息主体被读取或被理解，而只是被交付了。

如果信息或相关属性被以任何方式改变，验证与原始信息相关的接收证据可能失败。因此 PP/ST 作者应考虑在 PP/ST 中加入完整性要求，如：FDT _ UIT.1 数据交换完整性。

抗抵赖涉及几个不同的角色，每个角色都可能结合一个或多个主体。第一个角色是请求接收证据的主体(仅在 FCO _ NRO.1 选择性接收证明中)，第二个角色是接收者和(或)其他向其提供证据的主体(例如：公证人)，第三个角色是请求验证接收证据的主体，例如：接收者或第三方(例如：仲裁者)。

PP/ST 作者必须规定为了能验证证据的有效性所必须满足的条件。例如：可能规定的一个条件是

对证据的验证必须在 24 h 内进行。因此,这些条件允许按法律要求对抗抵赖进行裁剪,例如:能够在几年内提供证据。

在多数情况下,接收者的身份将是接收传送的用户的身份。在一些情况下,PP/ST 作者不希望用户身份被输出。此时 PP/ST 作者必须考虑包括此类是否合适,或者是否应使用传送服务提供者的身份或主机的身份。

除了(或代替)用户身份,一个PP/ST 作者可能更关注接收信息的时间。例如,报价将在某个日期终止,定单必须在某个确定日期前接收到才能被接纳,在这些情况下,功能要求应能被定制以提供时间戳指示(接收时间)。

FCO _ NRR.1　选择性接收证明

操作

赋值:

在 FCO _ NRR.1.1 中,PP/ST 作者应将信息主体的类型填写到接收功能的证据中,例如:电子邮件消息。

选择:

在 FCO _ NRR.1.1 中,PP/ST 作者应规定可以请求接收证据的用户/主体。

赋值:

在 FCO _ NRR.1.1 中,PP/ST 作者根据选择结果应规定能请求接收证据的第三方。第三方可以是仲裁者、法官和法律机构。

在 FCO _ NRR.1.2 中,PP/ST 作者应填写可链接到信息的属性表,例如:接收者身份、接收时间和接收位置。

在 FCO _ NRR.1.2 中,PP/ST 作者应将信息填写信息域表上,信息中的属性提供接收证据,例如:消息体。

选择:

在 FCO _ NRR.1.3 中,PP/ST 作者应规定能验证接收证据的用户/主体。

赋值:

在 FCO _ NRR.1.3 中,PP/ST 作者应根据选择结果规定能验证接收证据的第三方。

在 FCO _ NRR.1.3 中,PP/ST 作者应填写限制表,证据在这些限制下被验证。例如:证据只能在 24 h 时间间隔之内被验证。一个“立即的”或“不确定的”赋值是可接受的。

FCO _ NRR.2　强制接收证明

操作

赋值:

在 FCO _ NRR.2.1 中,PP/ST 作者应将信息主体的类型填写到接收功能的证据中,例如:电子邮件消息。

在 FCO _ NRR.2.2 中,PP/ST 作者应填写可链接到信息的属性表,例如:接收者身份、接收时间和接收位置。

在 FCO _ NRR.2.2 中,PP/ST 作者应将信息填写到信息域表上,信息中的属性提供接收证据,例如:消息体。

选择:

在 FCO _ NRR.2.3 中,PP/ST 作者应规定能验证接收证据的用户/主体。

赋值：

在FCO _NRR.2.3中，PP/ST作者应根据选择结果规定能验证接收证据的第三方。

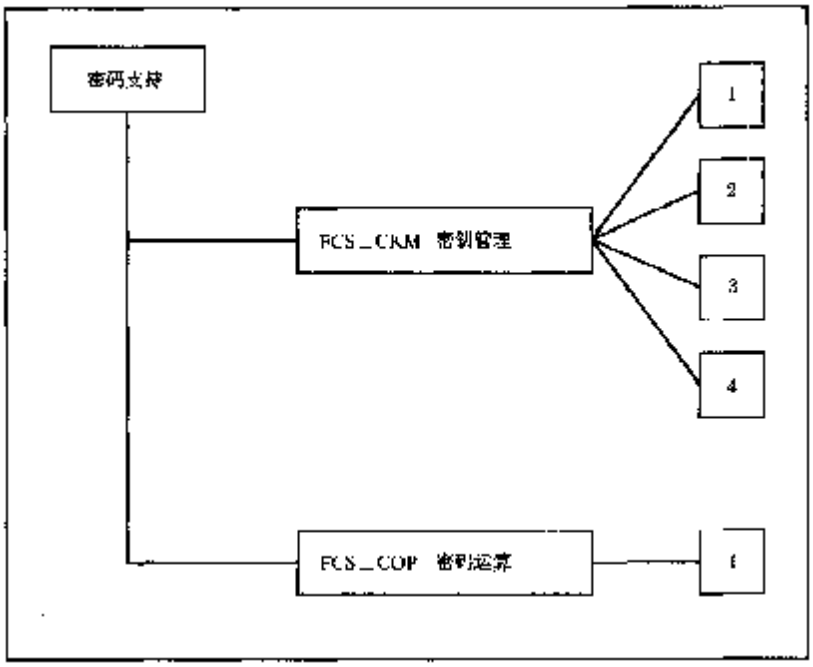
在FCO _NRR.2.3中，PP/ST作者应填写限制表，证据在这些限制下被验证。例如：证据只能在24 h时间间隔之内被验证。一个“立即的”或“不确定的”赋值是可接受的。

附 录 E
（提示的附录）
密码支持（FCS）

TSF可以利用密码功能来帮助满足几种高级安全目标。这包括了（但不限于）：标识和鉴别、抗抵赖、可信路经、可信信道和数据分离。当TOE实现密码功能时使用此类，其实现可为硬件、固件或软件。

FCS类是由两个子类构成：FCS _CKM密钥管理和FCS _COP密码运算。FCS _CKM子类提出密钥的管理，而FCS _COP子类这些密钥的运算使用相关的。

本类的组件构成分解如图E1所示。



图E1 密码支持类分解

由TOE实现每个密钥的生成方法时，PP/ST作者应选择FCS _CKM.1组件。

由TOE实现每个密钥的分配方法时，PP/ST作者应选择FCS _CKM.2组件。

由TOE实现每个密钥的访问方法时，PP/ST作者应选择FCS _CKM.3组件。

由TOE实现每个密钥的销毁方法时，PP/ST作者应选择FCS _CKM.4组件。

由TOE实现每个密钥的运算（例如：数字签名、数据加密、密钥协定、安全散列等）时，PP/ST作者应该选择FCS _COP.1组件。

密码功能可用于满足FCO类中规定的安全目标，和在FDP _DAU、FDP _SDI、FDP _UCT、FDP _UIT、FIA _SOS、FIA _UAU子类中满足各种目标。当密码功能用于满足其他类的目标时，单个功能组件应规定密码功能度必须满足的目标。当消费者要求TOE的密码功能时，应使用FCS类中的目标。

E1 密钥管理（FCS _CKM）

用户注释

密钥管理必须在其整个生命期内进行，密钥生命期中的典型事件包括(但不限于)：产生、分配、登录、存储、访问(例如备份、托管、归档、恢复)和销毁。

最低限度密钥要经历以下阶段：产生、存储和销毁。是否包括其他阶段取决于实施的密钥管理策略，因为 TOE 不一定涉及到所有的密钥生存期(例如；TOE 可以只产生和分配密钥)。

本子类预期要支持密钥生存期，因此定义了对以下活动的要求：密钥产生、密钥分配、密钥访问和密钥销毁。当对密钥管理有功能要求时应选择本子类。

如果 PP/ST 中包括 FAU _ GEN(安全审计数据生成)，则在被审计的事件的内容应有：

a) 客体属性可包括密钥的指定用户、用户角色、将使用该密钥的密码运算、密钥标识和密钥有效期。

b) 客体值可包括密钥的值和除了任何敏感信息外的参数(例如：秘密密钥或私有密钥)

一般来讲，随机数用于产生密钥，在这种情况下，应使用 FCS _ CKM.1 密钥生成而不使用 FIA _ SOS.2 TSF 秘密产生。当不是为密钥产生而要求随机数生成时，应使用组件 FIA _ SOS.2 TSF 秘密产生。

FCS _ CKM.1　密钥生成

用户应用注释

本组件要求规定密钥的长度和用于产生密钥的方法，这要遵循一个指定标准，它能被用于规定密钥的长度和规定用于产生密钥的方法(例如：算法)。对使用同一种方法和多种长度的密钥的情况，本组件只需赋值一次。密钥长度对于不同的实体可能是共同的或不同的，可以作为方法的输入或从方法输出。

操作

赋值：

在 FCS _ CKM.1.1 中，PP/ST 作者应规定所使用的密钥产生算法。

在 FCS _ CKM.1.1 中，PP/ST 作者应规定使用的密钥长度。规定的密钥长度应适合于算法及其预期使用。

在 FCS _ CKM.1.1 中，PP/ST 作者应规定指定的标准，该标准描述生成密钥所使用的方法。指定的标准可不包含或包含一个或多个实际发布的标准，例如：国际、国家、工业或组织标准。

FCS _ CKM.2　密钥分配

用户应用注释

本组件要求规定用于分配密钥的方法，该方法应遵循一个指定的标准。

操作

赋值：

在 FCS _ CKM.2.1 中，PP/ST 作者应规定所使用的密钥分配方法。

在 FCS _ CKM.2.1 中，PP/ST 作者应规定指定的标准，该标准描述分配密钥的方法。指定的标准可不包含或包含一个或多个实际发布的标准，例如：国际、国家、工业或组织标准。

FCS _ CKM.3　密钥访问

用户应用注释

本组件要求规定用于密钥访问的方法，该方法应遵循一个指定的标准。

操作

赋值：

在 **FCS _ CKM.3.1** 中，**PP/ST** 作者应规定所使用的密钥访问类型，密钥访问的类型包括（但不限于）：密钥备份、密钥归档、密钥托管和密钥恢复。

在 **FCS _ CKM.3.1** 中，**PP/ST** 作者规定所使用的密钥访问方法。

在 **FCS _ CKM.3.1** 中，**PP/ST** 作者应规定指定的标准，该标准描述访问密钥的方法。指定的标准可不包含或包含一个或多个实际发布的标准，例如：国际、国家、工业或组织标准。

FCS _ CKM.4 密钥销毁

用户应用注释

本组件要求规定用于密钥销毁的方法，该方法应遵循一个指定的标准。

操作

赋值：

在 **FCS _ CKM.4.1** 中，**PP/ST** 作者应指定用来销毁密钥的方法。

在 **FCS _ CKM.4.1** 中，**PP/ST** 作者应规定指定的标准，该标准描述了密钥销毁的方法。指定的标准可不包含或包含一个或多个实际发布的标准，例如：国际的、国家的、工业的或组织的标准。

E2 密码运算（FCS _ COP）

用户注释

密码运算可能有与之相关联的密码运算模式，这样就必须规定密码摸式，例如密码块链接模式、输出反馈模式、电子密本模式和密码反馈模式等。

密码运算可用于支持一个或多个 **TOE** 安全服务。**FCS _ COP** 组件可以根据需要重复几次，这取决于：

a）用户应用所使用的安全服务；

b）所使用的不同密码算法或密钥长度；

c）所运算的数据类型或敏感度。

如果 **PP/ST** 中包括 **FAU _ GEN** 安全审计数据产生，则将审计密码运算事件的上下文中有：

a）密码运算的类型可以包括：数字签名的产生或验证、用于完整性或校验和检验的密码校验和的产生，安全散列（消息摘要）的计算，数据加密或解密、密钥加密或解密、密钥协定和随机数生成。

b）主体属性可包括同主体有关的主体角色和用户。

c）客体属性可包括密钥的指定用户、用户角色、所用密钥的密码运算、密钥标识和密钥有效期。

FCS _ COP.1 密码运算

用户应用注释

本组件要求用于执行规定的密码运算的密码算法和密钥长度，该密码运算可基于一个指定的标准。

操作

赋值：

在 **FCS _ COP.1.1** 中，**PP/ST** 作者应规定所执行的密码运算。通常密码运算包括：数字签名的生成或验证，用于完整性或校验和检验的密码校验和的产生，安全散列（消息摘要）的计算，数据加密或解密、密钥加密或解密、密钥协定和随机数生成。密码运算可对用户数据或 **TSF** 数据执行。

在 **FCS _ COP.1.1** 中，**PP/ST** 作者应规定所使用的密码算法。通常的密码算法包括（但不限于）**DES**、**RSA** 和 **IDEA** 等。

在 FCS_COP.1.1 中，PP/ST 作者应规定所使用的密钥长度。规定的密钥长度应适合于算法及其预期使用。

在 FCS_COP.1.1 中，PP/ST 作者应规定所指定的标准，该标准文本应描述如何执行已确定的密码运算。指定的标准可不包含或包含一个或多个实际的公开发布的标准，例如：国际、国家、工业或组织标准。

附 录 F
（提示的附录）
用户数据保护（FDP）

本类包含若干子类，这些子类详细规定了与保护用户数据相关的 TOE 安全功能和 TOE 安全功能策略。本类中的组件不同于 FIA 和 FPT 中的组件，FIA 规定保护与用户相关属性的组件，FPT 规定保护 TSF 信息的组件。

本类没有对常用的强制访问控制（MAC）和自主访问控制（DAC）做明确的要求，然而，要构建这些要求时需要使用本类中的一些组件。

FDP 并不明确地处理保密性、完整性或可用性，而上述三性经常与策略和机制紧密相关。但在 PP/ST 中，TOE 安全策略必须完全覆盖这三个目的。

本类的最后一个方面就是用术语“操作”来规定访问控制。操作就是对特定客体的一种特定类型的访问。它依赖于 PP/ST 作者的抽象水平，确定将这些操作描述成“读”或“写”，或者是更复杂的操作，比如“更新数据库”。

访问控制策略是控制对信息容器访问的策略。其属性代表该容器的属性。一旦信息在容器之外，访问者就可以自由地修改，包括将信息写入具有不同属性的容器中。相对应的，信息流策略控制对信息的访问，而与容器无关。信息的属性，可能与容器的属性相关（也许无关，如多级数据库），将与信息一起移动。没有明确的授权，访问者无法改变信息的属性。

本类并不像人们想像的那样，是一个 IT 访问策略的完备分类。这里所包括的策略仅仅是当前实际系统中具有的一些经验，这些经验对指定要求提供了一个基础。也可能还存在其他形式的意图。

比如：你可以设想一个由用户实行的（和用户定义的）对信息流的控制（例如：一个非外部自动告警工具），这种概念可以做为 FDP 组件的细化或扩展。

最后要强调一点，在阅读 FDP 中的组件时要记住，实现某机制中的功能所要求的这些组件，同样可能服务于或能够服务于另外的目的。比如，可以建立一种访问控制策略（FDP_ACC），此策略使用标记（FDP_IFF.1）作为访问控制机制的基础。

TOE 安全策略可以包含许多安全功能策略（SFP），每一个都可标识为组件 FDP_ACC 和 FDP_IFC 所确定的策略。典型的，这些策略已经考虑了 TOE 所要求的保密性、完整性和可用性方面的内容。值得注意的是，要确保所有客体都至少被一个 SFP 覆盖，并且在执行多个 SFP 时不会出现冲突。

图 F1 和图 F2 说明了本类组成组件的分解。

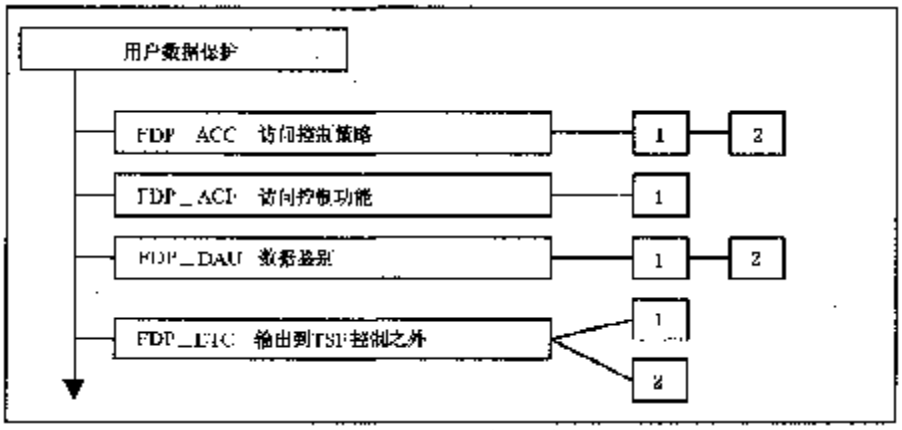


图 F1　用户数据保护类分解

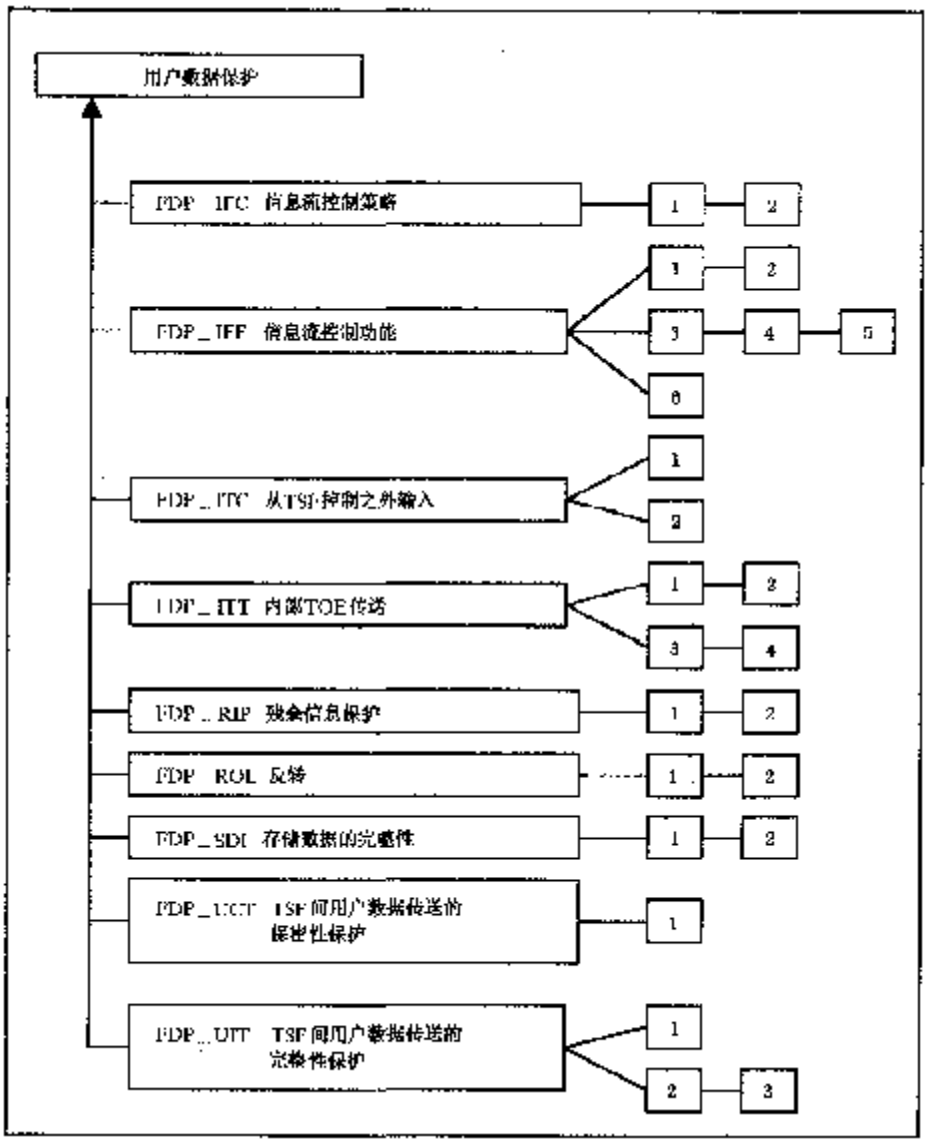


图 F2　用户数据保护类分解

在构造 PP/ST 时，以下信息有助于查找和选择 FDP 类中的组件。

FDP 类中的要求被定义为安全功能(缩写为 SF)，它应执行一个 SFP。由于 TOE 可以同时执行多个 SFP，PP/ST 作者必须为每一个 SFP 命名，以便能在其他子类中引用。这个名字将用于选定的每一个

组件，表明其已用于功能要求所定义的部分。这便于作者指定操作的范围，如覆盖的客体、操作和授权用户等等。

组件的每个实例只能用于一个SFP。因此，如果一个组件指定了某个SFP，则该SFP将适用于此组件中的所有元素。在PP/ST中，可以对组件多次实例化，以满足预期的各种策略。

从本子类中选取组件的关键，是有一个明确定义的TOE安全策略，以便能够从两个策略组件(FDP_ACC和FDP_IFC)中选择合适的组件。

分别在FDP_ACC和FDP_TFC组件中，为全部的访问控制策略和信息流控制策略命名，并进一步用该安全功能覆盖的主体、客体和操作的形式，明确这些组件的控制范围。如果此功能组件的其他部分有选择访问控制SFP和信息流控制SFP或为其赋值的操作，就必须使用这些策略的名字，并分别在FDP_ACF和FDP_IFF子类中定义规则，明确所命名的访问控制SFP和信息流控制SFP的功能。

下面的步骤指导我们在开发PP/ST时如何使用本类：

a) 从FDP_ACC和FDP_IFC子类中确定将执行的策略。这两个子类确定了策略的控制范围、控制粒度，并可以确定一些与策略相对应的规则。

b) 在策略组件中确定组件，并执行所有适用的操作。赋值操作可以针对共通的(如表述为“所有文件”)或特定的(如指定文件“A”，“B”等)对象进行，这取决于掌握的详细程度。

c) 从FDP_ACF和FDP_IFF中确定所有适用的功能组件，以满足FDP_ACC和FDP_IFC中所命名的策略子类。执行这个操作，使组件定义出已命名的策略所执行的规则。应当使组件满足预期的或已建立的所选功能要求。

d) 确定该功能中，谁能控制和改变安全属性，比如只有安全管理员、客体所有者等等。从FMT安全管理类中选择合适的组件并执行操作。这里可能需要细化操作，以确定缺少的特征，比如部分或所有的修改都必须通过可信路径来完成。

e) 对于新客体和主体的初始值，在FMT安全管理类中确定所有合适的组件。

f) 在FDP_ROL子类中确定所有适用的反转组件。

g) 在FDP_RIP子类中确定所有适用的残余信息保护要求。

h) 在FDP_ITC和FDP_ETC子类中，确定所有适用的输入、输出组件，以及在输入、输出中应如何处理安全属性。

i) 在FDP_ITT子类中确定所有适用的TOE内部通信组件。

j) 在FDP_SDI中确定存储信息完整性保护的所有要求。

k) 在FDP_UCT或FDP_UIT子类中确定所有适用的TSF间的通信组件。

F1 访问控制策略(FDP_ACC)

本子类是基于独立的概念控制主体和客体间的相互作用。控制的范围和目的是基于访问者的属性(主体)、被访问的容器(客体)的属性、行为(操作)和相关的访问控制规则。

用户注释

本子类中的组件能(通过名字)确定传统的自主访问控制机制(DAC)执行的访问控制SFP。进一步定义确定的访问控制SFP所覆盖的主体、客体和操作，并在其他子类中定义访问控制SFP功能的规则，如FDP_ACF和FDP_RIP。

如果此功能组件的其他部分有选择“访问控制SFP”或为其赋值的操作，就必须使用FDP_ACC中定义的访问控制SFP的名字。

访问控制SFP包含由主体、客体和操作组成的三元集合。因此一个主体可由多个访问控制SFP覆盖，但只涉及单个不同的操作或客体。对于客体和操作也同样如此。

实施访问控制SFP的访问控制功能的关键点是用户能够修改访问控制抉择中涉及的属性，而FDP_ACC子类没有说明这些方面。有些要求没有定义，但可以在细化操作中增加，而余下的要求可包含在

其他子类和类中，比如 FMT 类：FMT 安全管理。

FDP _ ACC 用于指定访问控制 SFP 要求，而没有指定审计要求。审计要求将在确定功能以满足本子类中指定的访问控制 SFP 的类中出现。

本子类为 PP/ST 的作者提供了指定多种策略的能力，比如：在一个控制范围内实施固定的访问控制 SFP，在另外的控制范围中实施灵活的访问控制 SFP。要在 PP/ST 中指定多个访问控制策略，本子类中的组件可以在不同的操作和客体子集中多次反复。这与具有多重策略的 TOE 相适应，每一个策略适用于一个特定的操作和客体集合。也就是说，PP/ST 作者应对 TSF 执行的每一个访问控制 SFP 指定 ACC 组件中所要求的信息。比如，一个实施三个访问控制 SFP 的 TOE，其中每个 SFP 只包含 TOE 中客体、主体和操作的一个子集，对于各个访问控制 SFP，都将包含一个访问控制组件 FDP _ ACC.1 子集，从而需要总共三个 FDP _ ACC.1 组件。

FDP _ ACC.1　子集访问控制

用户应用注释

术语客体和主体都是相对于 TOE 中的一般元素而言的。对于将实现的策略，应清晰地定义其实体。在 PP 中，客体和操作可以表示为类型，比如：命名的客体、数据仓、观察访问等等。对于特定的系统，这些一般的术语（主体、客体）必须细化，比如：文件、寄存器、端口、守护进程、公开调用等。

本组件对一些客体子集定义得很好的操作集指定策略。而不对集合外部的操作做任何限制——包括对部分操作受控的客体的其他操作。

操作

赋值：

在 FDP _ ACC.1.1 中，PP/ST 作者应指定 TSF 执行的唯一命名的访问控制 SFP。

在 FDP _ ACC.1.1 中，PP/ST 作者应指定一个 SFP 覆盖的主体列表、客体列表以及主体在对客体进行的操作列表。

FDP _ ACC.2　完全访问控制

用户应用注释

本组件要求在 SFP 中覆盖的、所有可能实施于客体的操作都包含在一个访问控制 SFP 中。

PP/ST 的作者必须证明每一组客体和主体都包含在该访问控制 SFP 中。

操作

赋值：

在 FDP _ ACC.2.1 中，PP/ST 作者应指定由 TSF 执行的唯一命名的访问控制 SFP。

在 FDP _ ACC.2.1 中，PP/ST 作者应指定 SFP 包含的主体列表和客体列表，并且主体对客体的所有操作都包含于 SFP 中。

F2　访问控制功能（FDP _ ACF）

本子类描述一些特定功能的规则，以实现 FDP _ ACC 中命名的访问控制策略，并指定策略控制的范围。

用户注释

本子类为 PP/ST 作者提供了描述访问控制规则的能力。这导致系统中对客体的访问不会发生改变。作为这种客体的一个例子就是，“今日消息”，它可以被所有人阅读，但只能被授权管理员修改。

本子类同样允许PP/ST 作者描述正常访问控制规则之外的规则。这些例外规则可以明确允许或者拒绝授权对客体的访问。

没有明确的组件指定其他可能的功能，比如双人控制、操作顺序规则或互斥控制。然而，这些机制以及传统DAC 机制，能够通过仔细制定访问控制规则，用所存在的组件来表示。

各种可接受的访问控制SF 在本子类中可描述为：

——访问控制列表(ACL)

——基于时间的访问控制规范

——基于原发端的访问控制规范

——属主控制的访问控制属性

FDP _ ACF.1　基于安全属性的访问控制

用户应用注释

本组件对基于与主体和客体有关的安全属性执行访问控制的机制提出要求。每一个客体和主体都有一组相关的属性，比如位置、创建时间、访问权限(如：访问控制列表(ACL))。本组件允许PP/ST 作者指定用于访问控制调度的属性，并允许使用这些属性来指定访问控制规则。

下面的段落中给出PP/ST 作者对属性进行赋值的例子。

标识属性可能与用户、主体或用于调停的客体有关。作为这种属性的例子，它可能是创建主体使用的程序镜像名，或者是授予程序镜像的安全属性。

时间属性用来指定在一天中的哪些时间，或者是一星期中的哪几天，或哪年授予访问权限。

位置属性能指定是否是操作请求的地址、或操作执行的地址、或两者同时进行的地址。它基于内部表将TSF 逻辑接口转换成位置，比如通过终端位置、CPU 位置，等等。

组属性允许为了访问控制的目的将单个用户组与操作相关联。如果需要，应使用细化操作来指定最大组数、该组最多的成员、以及用户可以同时关联的最大组数。

本组件同样要求访问控制安全功能能基于安全属性，明确授权或拒绝对一个对象的访问，它可用来在TOE 中设置特权、访问权限或访问授权。这些特权、权限或授权可适用于用户、主体(代表用户或应用)和客体。

操作

赋值：

在FDP _ ACF.1.1 中，PP/ST 作者应指定TSF 要执行的访问控制SFP 名称。访问控制SFP 名称，以及该策略的控制范围定义于FDP _ ACC 的组件中。

在FDP _ ACF.1.1 中，PP/ST 作者应指定安全属性或命名的安全属性组，其功能将用于指定规则。例如，这些属性可以是用户标识、主体标识、角色、赋值、时间、位置、ACL 或者PP/ST 作者指定的其他属性。可指定命名的安全属性组以提供便捷的方式来引用多重安全属性。命名组提供了一种有效的方法，将FMT _ SMR 安全管理角色中定义的角色，以及所有相关的角色与主体相关联。换句话说，每个角色都与一命名的属性组相关联。

在FDP _ ACF.1.2 中，PP/ST 作者应在受控主体和受控客体中，对受控客体执行受控操作来指定管理访问的SFP 规则。这些规则指定访问被允许或拒绝的时间。可以指定通用的访问控制功能(典型的，如许可位)或精细的访问控制功能(如：ACL)。

在FDP _ ACF.1.3 中，PP/ST 作者应基于安全属性指定规则，明确授权主体对明确用于授权访问的客体的访问。这些规则是FDP _ ACF.1.1 中指定规则的补充。所以存在于FDP _ ACF.1.3 中。是因为包含FDP _ ACF.1.1 中指定规则的例外情况。对于明确授权访问规则的示例是基于与主体相关的特权向量，总是允许访问指定的访问控制SFP 所覆盖的客体。如果不需要这种能力，

PP/ST 作者应指明“无”。

在 FDP _ ACF.1.4 中,PP/ST 作者应基于安全属性指定规则,明确地拒绝主体对客体的访问。这些规则是对 FDP _ ACF.1.1 中指定规则的补充。之所以存在于 FDP _ ACF.1.4 中,是因为包括 FDP _ ACF.1.1 中指定规则的例外情况。对于明确拒绝访问规则的示例是基于与主体相关的特权向量,总是拒绝访问指定的访问控制 SFP 所覆盖的对象。如果不需要这种能力,PP/ST 作者应指明“无”。

F3 数据鉴别(FDP _ DAU)

本子类描述能用来鉴别“静态”数据的特定功能。

用户注释

对“静态”数据鉴别有要求时将使用本子类中的组件。也就是数据需要标识,但没有传送。(注意,在数据交换时 FCO _ NRO 子类将提供被接收信息的源抗抵赖。)

FDP _ DAU.1 基本数据鉴别

用户应用注释

可通过单向 hash 函数(密码核验和、指纹、信息摘要)来满足本组件的要求,它对确定的文档产生 hash 值,从而对文档的有效性进行验证或对信息内容进行鉴别。

操作

赋值:

在 FDP _ DAU.1.1 中,PP/ST 作者应指定客体或信息类型列表,在它们中 TSF 应能够生成数据鉴别的证据。

在 FDP _ DAU.1.2 中,PP/ST 作者应指定一个主体列表,这些主体能够为在前面元素中定义的客体验证数据鉴别所需的证据。如果主体已知,主体列表可以非常具体,或者是更一般化并引用一“类”主体,比如一个确定的角色。

FDP _ DAU.2 伴有保证者身份的数据鉴别。

用户应用注释

另外的,本组件还要求校验提供鉴别保证(如可信第三方)的用户身份的能力。

操作

赋值:

在 FDP _ DAU.2.1 中,PP/ST 作者应指定 TSF 能为它们生成数据鉴别证据的客体或信息类型列表。

在 FDP _ DAU.2.2 中,PP/ST 作者应指定一个主体列表,这些主体应能验证在前面元素中所定义客体的数据鉴别证据以及产生数据鉴别证据的用户身份。

F4 输出到 TSF 控制之外(FDP _ ETC)

本子类定义从 TOE 中输出用户数据的功能,既可以在输出时明确保留安全属性,或者是忽略。这些安全属性的一致性在 FPT _ TDC 的组件 TSF 间 TSF 数据的一致性中说明。

FDP _ ETC 关心对数据输出的限制和输出的用户数据与安全属性的关联性。

用户注释

本子类以及相应的 FDP _ ITC 输入子类,用来说明 TOE 如何处理用户数据输入和输出其控制范

围。原则上本子类只涉及用户数据及其相关安全属性的输出。

下面包含其中各种可能的活动：

a）输出没有任何安全属性的用户数据。

b）输出具有安全属性的用户数据，这两者彼此相互关联，并且安全属性明显地反映输出的用户数据。

如果存在多重(访问控制或信息流控制)SFP，对每一个命名的 SFP 可以反复使用这些组件。

FDP _ ETC.1　没有安全属性的用户数据输出

用户应用注释

本组件用来指定在输出用户数据时，并不输出其安全属性。

操作

赋值：

在 FDP _ ETC.1.1 中，PP/ST 作者应指定输出用户数据时将执行的访问控制 SFP 或信息流控制 SFP，这些 SFP 限定了此功能输出的用户数据的范围。

FDP _ ETC.2　有安全属性的用户数据输出

用户应用注释

用户数据与它的安全属性一起输出，并且安全属性明确的与用户数据相关联。有多种方法实现这种关联。一种方法是将用户数据和安全属性在物理上连用(如同一张软盘)或使用密码技术如安全签字将属性和用户数据相关联。TSF 间可信信道 FTP _ ITC 可以用来保证属性被另一个 IT 产品正确接收，同时，TSF 间 TSF 数据的一致性 FPT _ TDC 可以用来保证那些属性得到正确的解释。进一步，可信路径 FTP _ TRP 可用来保证输出由正确的用户发起。

操作

赋值：

在 FDP _ ETC.2.1 中，PP/ST 作者应指定在输出用户数据时要执行的访问控制 SFP 或信息流控制 SFP。这些 SFP 限定了此功能输出的用户数据的范围。

在 FDP _ ETC.2.4 中，PP/ST 作者应指定所有附加的输出控制规则，如果没有应指明为“无”。TSF 应执行那些在 FDP _ ETC.2.1 中选择的访问控制 SFP 或信息流控制 SFP 之外的附加规则。

F5　信息流控制策略(FDP _ IFC)

本子类包含标识信息流控制 SFP 并分别确定每个 SFP 的控制范围。

下面的安全策略能满足这个目的：

——Bell 和 La Padula 安全模型〔B&L〕；

——Biba 完整性模型〔Biba〕；

——无干扰〔Gogul，Gogu2〕；

用户注释

本子类中的组件能够识别 TOE 中传统的强制访问控制(MAC)机制执行的信息流控制 SFP。然而他们已经超出了传统 MAC 机制的范围，可用来识别和描述无干扰策略和状态转变，并进一步为 TOE 中各个信息流控制 SFP 定义策略控制下的主体、信息以及引发受控信息流入、流出受控主体的操作。定义信息流控制 SFP 规则的功能将由其他诸如 FDP _ IFF 和 FDP _ RIP 等子类定义。在 FDP _ IFC 中命

名的访问控制SFP应在其他所有选择“信息流控制SFP”或为其进行赋值操作的功能组件中使用。

这些组件非常灵活，它们允许指定信息流控制的域而对基于标签的机制没有要求，并允许信息流控制组件的不同元素对策略有不同程度的偏离。

每个SFP都包含一个三元集合：主体、信息以及引发信息流入、流出主体的操作。一些信息流控制策略可能处于低层，并明确用操作系统中的进程来描述主体。另一些可能处于高层，用通常意义上的用户或输入、输出信道来描述主体。如果信息流控制策略处于高层，有可能不能清晰地定义所需要的IT安全功能。在这种情况下，将描述信息流控制策略作为目的会更合适。这样能指定所需要的IT安全功能，作为对那些目的的支持。

在第二个组件(FDP_IFC.2完全信息流控制)中，每一个信息流控制SFP将覆盖可能引发SFP覆盖的信息流入、流出SFP覆盖的主体的所有操作。进而，所有信息流应被SFP所覆盖。因此，对于引发信息流的每一个行动，都有一组规则来决定其是否被允许。如果有多个SFP适用于给定的信息流，在其发生之前，应得到所有涉及的SFP的允许。

一个信息流控制SFP包含一组良好定义的操作。SFP覆盖的范围对一些信息流而言可能很“完备”，或仅描述了部分影响信息流的操作。

访问控制SFP控制对包含信息的客体的访问。信息流控制SFP控制对信息的访问，而独立于它的容器。信息流动时其属性可能与承载信息的容器属性相关(也可能无关，如多级数据库)。在没有明确授权的情况下，访问者不能改变信息属性。

信息流和操作可以用多种级别表达。对于ST，信息流和操作可以在特定系统级指定：如TCP/IP包基于已知IP地址通过防火墙转发。对于PP，信息流和操作可表示为类型，如：电子邮件、数据仓、保持访问等等。

本子类中的组件对PP/ST中不同的操作和客体子集可以多次使用，能满足包含多种策略的TOE，其中每个策略对应特定的客体、主体和操作子集。

FDP_IFC.1　子集信息流控制

用户应用注释

本组件要求信息流控制策略实施于TOE中所有可能操作的一个子集。

操作

赋值：

在FDP_IFC.1.1中，PP/ST作者应指定TSF执行的唯一命名的信息流控制SFP。

在FDP_IFC.1.1中，PP/ST作者应指定SFP覆盖的主体、信息和引发受控制信息流入、流出受控主体的操作列表。与上面描述的一样，根据PP/ST作者的需要，主体列表可有不同的详细程度，比如可以指定用户、机器或进程。信息可以引用数据，如电子邮件、网络协议或类似访问控制策略中指定的更特殊的客体。如果指定的信息包含于受访问控制策略控制的客体中，则指定的信息在流入、流出客体之前，访问控制策略和信息流控制策略都必须执行。

FDP_IFC.2　完全信息流控制

用户应用注释

本组件要求信息流控制SFP覆盖了所有引发信息流入、流出SFP中主体的所有可能的操作。

PP/ST作者必须证明信息流控制SFP覆盖了每一个信息流及其相应的主体。

操作

赋值：

在 FDP _ IFC.2.1 中，PP/ST 作者应指定 TSF 执行的唯一命名的信息流控制 SFP。

在 FDP _ IFC.2.1 中，PP/ST 作者应指定 SFP 覆盖的主体、信息列表，SFP 应覆盖所有引发信息流入、流出主体的操作。与上面描述的一样，根据 PP/ST 作者的需要，主体列表可有不同的详细程度。比如可以指定用户、机器或者进程。信息可以引用数据，如电子邮件、网络协议或类似访问控制策略中指定的更特殊的客体。如果指定的信息包含于受访问控制策略控制的客体中，则指定的信息在流入、流出客体之前，访问控制策略和信息流控制策略都必须执行。

F6 信息流控制功能(FDP _ IFF)

本子类描述能实现 FDP _ IFC 中命名的信息流控制 SFP 的特定功能的规则，这些规则同样指定了策略的控制范围。它由两棵“树”组成，一个说明通常的信息流控制功能，另一个说明在一个或多个信息流控制 SFP 中的非法信息流问题。这种划分是由于与非法信息流有关的问题，在某种程度上与其余的 SFP 无关。非法信息流是违背策略的信息流，因而不是一个策略问题。

用户注释

对于不可信任的软件，为了实现强有力的保护来防止泄露和修改，对信息流的控制是必须的。单独的访问控制是不够的，因为它只控制对信息容器的访问，而允许容器中的信息没有控制地在系统中流动。

本子类使用了短语“非法信息流类型”。这个短语可以用于将信息流分为：“存贮信道”或“定时信道”，或者是体现 PP/ST 作者需要的改进的分类方法。

这些组件的灵活性允许在 FDP _ IFF.1 和 FDP _ IFF.2 中定义特权策略，以允许全部或部分特定的 SFP 能够得到受控旁路。如果有预定义的 SFP 旁路需求，PP/ST 作者应考虑与某个特权策略合并使用。

FDP _ IFF.1 简单安全属性

用户应用注释：

本组件需要有信息以及引发信息流动和接收信息的主体的安全属性。如果需要它们在信息流控制决定中起一定的作用，或者它们包含在访问控制策略中，那么信息容器的属性也应考虑。本组件指定应执行的关键规则，并描述如何导出安全属性。比如，当至少一个 TSP 中的信息流控制 SFP 像 Bell—LaPadula 安全策略模型[B&L]中定义的那样，是基于标签时，应使用本组件，但这些安全属性并没有形成层次。

本组件没有指定如何赋予安全属性的细节(比如，相对于进程的用户)。如果需要，可以通过赋值来指定附加策略和功能要求，从而提供了策略的灵活性。

本组件也提供了对信息流控制功能的要求，能基于安全属性明确的授权或拒绝信息流，用来实现包含本组件所定义的基本策略之外的特权策略。

操作

赋值：

在 FDP _ IFF.1.1 中，PP/ST 作者应指定 TSF 执行的信息流控制 SFP。信息流控制 SFP 的名字及其控制范围由 FDP _ IFC 的组件定义。

在 FDP _ IFF.1.1 中，PP/ST 作者应指定本功能在规则规范中将使用的最少数量和类型的安全属性。比如，这些属性可以是主体标识、主体敏感性级别、主体通行级别、信息敏感性级别等。各类安全属性的最少数量应足以满足环境的需要。

在 FDP _ IFF.1.2 中，PP/ST 作者应为 TSF 执行的每一个操作，指定主体和信息安全属性之

间保持的基于安全属性的相互关系。

在FDP_IFF.1.3中,PP/ST作者应指定TSF要执行的所有附加的信息流控制SFP规则。如果没有附加规则,PP/ST作者应指明为“无”。

在FDP_IFF.1.4中,PP/ST作者应指定TSF提供的所有附加的SFP能力。如果没有附加能力,PP/ST作者应指明为“无”。

在FDP_IFF.1.5中,PP/ST作者应基于安全属性,指定明确授权信息流动的规则。这些规则是前面元素中指定规则的补充。之所以包含于FDP_IFF.1.5中,是因为它们包含前面元素中指定规则的例外情况。明确授权信息流动的规则例子是,基于与主体相关的特权向量,总是授权主体具有引发指定SFP包含的信息流动的能力。如果不需要这种能力,PP/ST作者应指明为“无”。

在FDP_IFF.1.6中,PP/ST作者应基于安全属性,指定明确拒绝信息流动的规则。这些规则是前面元素中指定规则的补充。之所以包含于FDP_IFF.1.6中,是因为它们包含前面元素中指定规则的例外情况。明确授权信息流动的规则例子是,基于与主体相关的特权向量,总是拒绝主体具有引发指定SFP包含的信息流动的能力。如果不需要这种能力,PP/ST作者应指明为“无”。

FDP_IFF.2 分级安全属性

用户应用注释

本组件要求所有TSP中的信息流控制SFP使用形成点阵的**分级**安全属性。

比如:TSP中至少一个信息流控制SFP是基于Bell—LaPadula安全策略模型[B&L]定义的标签时,应使用本组件并形成分级。

值得注意的是,FDP_IFF.2.5中定义的分级关系要求,仅需应用于在FDP_IFF.2.1中确定的信息流控制SFP的信息流控制安全属性。本组件不用于其他的SFP,比如:访问控制SFP。

像前面的组件一样,本组件也可实现包含明确授权或拒绝信息流规则的特权策略。

如果指定了多重信息流控制SFP,各SFP都有自己的安全属性,并且互不相关时,PP/ST作者应为每个SFP反复使用本组件。否则会因为不存在所要求的相互关系,使FDP_IFF.2.5的各子项之间相互冲突。

操作

赋值:

在FDP_IFF.2.1中,PP/ST作者应指定TSF执行的信息流控制SFP。信息流控制SFP的名字及其控制范围由FDP_IFC的组件定义。

在FDP_IFF.2.1中,PP/ST作者应指定本功能在规则规范中将使用的最少数量和类型的安全属性。比如,这些属性可以是主体标识、主体敏感性级别、主体通行级别、信息敏感性级别等。各类安全属性的最少数量应足以满足环境的需要。

在FDP_IFF.2.2中,PP/ST作者应为TSF执行的每一个操作,指定主体和信息安全属性之间保持的基于安全属性的相互关系。**这些相互关系应基于安全属性之间指定的关系。**

在FDP_IFF.2.3中,PP/ST作者应指定TSF要执行的所有附加的信息流控制SFP规则。如果没有附加规则,PP/ST作者应指明为“无”。

在FDP_IFF.2.4中,PP/ST作者应指定TSF执行的所有附加的SFP能力。如果没有,PP/ST作者应指明为“无”。

在FDP_IFF.2.5中,PP/ST作者应基于安全属性,指定明确授权信息流动的规则。这些规则是前面元素中指定规则的补充。之所以包含于FDP_IFF.2.5中,是因为它们包含前面元素中指定规则的例外情况。明确授权信息流动的规则例子是,基于与主体相关的特权向量,总是授权主体具有引发指定SFP包含的信息流动的能力。如果不需要这种能力,PP/ST作者应指明为“无”。

在FDP _ IFF.2.6中,PP/ST 作者应基于安全属性,指定明确拒绝信息流动的规则。这些规则是前面元素中指定规则的补充。之所以包含于FDP _ IFF.2.6中,是因为它们包含前面元素中指定规则的例外情况。明确授权信息流动的规则例子是,基于与主体相关的特权向量,总是拒绝主体具有引发指定SFP包含的信息流动的能力。如果不需要这种能力,PP/ST 作者应指明为"无"。

FDP _ IFF.3 受限的非法信息流

用户应用注释:

当至少一个SFP要求控制但并不消除非法信息流时,应使用本组件。

对于指定的非法信息流,应提供某种程度的最大容限。此外,PP/ST 作者能够指定是否必须审计非法信息流。

操作

赋值:

在FDP _ IFF.3.1中,PP/ST 作者应指定TSF执行的信息流控制SFP。信息流控制SFP的名字及其控制范围在FDP _ IFC的组件中定义。

在FDP _ IFF.3.1中,PP/ST 作者应指定非法信息流的类型,并服从最大容限。

在FDP _ IFF.3.1中,PP/ST 作者应对任何标识的非法信息流指定最大容限。

FDP _ IFF.4 部分消除非法信息流

用户应用注释

当所有要求控制非法信息流的SFP要求消除部分(而不是全部)非法信息流时,应使用本组件。

操作

赋值:

在FDP _ IFF.4.1中,PP/ST 作者应指定TSF执行的信息流控制SFP。信息流控制SFP的名字及其控制范围在FDP _ IFC的组件中定义。

在FDP _ IFF.4.1中,PP/ST 作者应指定非法信息流类型,并服从最大容限。

在FDP _ IFF.4.1中,PP/ST 作者应对所有标识的非法信息流指定最大容限。

在FDP _ IFF.4.2中,PP/ST 作者应指定要消除的非法信息流类型。该列表不能为空,因为本组件要求消除一些非法信息流。

FDP _ IFF.5 无非法信息流

用户应用注释

当要求控制非法信息流的SFP要求消除所有非法信息流时,应使用本组件。然而,PP/ST 作者应仔细考虑消除所有非法信息流对正常的TOE功能操作可能造成的影响。许多实际应用表明,TOE中的功能与非法信息流之间存在着某种间接的联系,消除所有非法信息流将减少预期的TOE功能。

操作

赋值:

在FDP _ IFF.5.1中,PP/ST 作者应指定需要消除非法信息流的信息流控制SFP。信息流控制SFP的名字及其控制范围在FDP _ IFC的组件中定义。

FDP _ IFF.6 非法信息流监视

用户应用注释

需要TSF监视非法信息流的使用是否超出指定范围时，应使用本组件。如果需要审计这种流动，那么本组件可作为安全审计数据产生FAU _ GEN子类的组件所使用的审计事件源。

操作

赋值：

在FDP _ IFF.6.1中，PP/ST作者应指定TSF执行的信息流控制SFP。信息流控制SFP的名字及其控制范围在FDP _ IFC的组件中定义。

在FDP _ IFF.6.1中，PP/ST作者应指定非法信息流类型，并监视此类信息流是否超出最大容限。

在FDP _ IFF.6.1中，PP/ST作者应指定TSF监视非法信息流是否超出最大容限。

F7 从TSF控制之外输入(FDP _ ITC)

本子类定义从TSC之外向TOE输入用户数据的机制，同时用户数据的安全属性能得到保持。安全属性的一致性由FPT _ TDC——TSF间TSF数据的一致性说明。

FDP _ ITC关心对输入的限制、用户安全属性规范以及安全属性与用户数据的关联。

用户注释

本子类以及相应的FDP _ ETC输出子类，说明TOE如何处理TSF控制之外的用户数据。本子类关心用户数据安全属性的赋值和抽象。

下面包含了各种可能的活动：

a) 从未格式化媒体(如：软盘、磁带、扫描仪、视频或音频信号)输入用户数据，不包含任何安全属性，并通过对媒体进行物理标记来表示其内容。

b) 从媒体输入用户数据，包括安全属性并校验客体安全属性是否合适。

c) 从媒体输入用户数据，包括安全属性，并使用密码封装技术保护用户数据及其安全属性的关联性。

本子类并不确定用户数据是否可以输入，而只关心安全属性值与输入的用户数据之间的关系。

用户数据的输入有两种可能：用户数据明确的与可靠的客体安全属性相关(安全属性的值和含义没有被修改)，或者从输入源没有获得可靠的安全属性(甚至没有安全属性)。本子类描述了以上两种情况。

如果有可靠的安全属性，它们可通过物理方式(安全属性在同一媒体上)或逻辑方式(安全属性分布各不相同，但包含唯一的客体标识，比如密码校验和)与用户数据相关联。

本子类关心用户数据的输入并保持与SFP所需安全属性的相互关联。其他子类关心输入的其他方面：比如超出本子类范围的一致性、可信信道和完整性。进一步，FDP _ ITC只关心与输入媒体的接口。FDP _ ETC负责媒体的另一端(原发端)。

下面是一些常见的输入要求：

a) 没有任何安全属性的用户数据输入；

b) 包含安全属性的用户数据输入，两者相互关联且安全属性明确地反映输入的信息。

有没有人为干预，TSF都可以处理这些输入要求，这取决于IT限制和组织安全策略。比如，如果通过“机密”信道接收用户数据，客体安全属性将置为“机密”。

如果有多个(访问控制或信息流控制)SFP，那么可能适合对每个命名的SFP分别反复使用这些组件。

FDP_ITC.1　没有安全属性的用户数据输入

用户应用注释

本组件用来指定没有可靠的(或者任何)安全属性与之关联的用户数据的输入。该功能要求输入的用户数据的安全属性要在TSF中初始化。也可能是PP/ST作者指定输入规则。在某些环境中,可能适用于要求通过可信路径或可信信道机制来提供这些属性。

操作

赋值:

在FDP_ITC.1.1中,当从TSC外部输入用户数据时,PP/ST作者应指定执行的访问控制SFP或信息流控制SFP。对这些SFP的赋值确定了该功能输入用户数据的范围。

在FDP_ITC.1.3中,PP/ST作者应指定所有附加的输入控制规则,没有时指明为"无"。这些规则将与FDP_ITC.1.1中选择的访问控制SFP或信息流控制SFP一起被TSF执行。

FDP_ITC.2　有安全属性的用户数据输入

用户应用注释

本组件用来指定输入具有可靠的关联安全属性的用户数据。该功能依赖于安全属性准确、无误地与输入媒体上的客体相关联。一旦输入后,那些客体将具有相同的属性。这要求FPT_TDC保证数据的一致性。也可以是PP/ST作者指定输入规则。

操作

赋值:

在FDP_ITC.2.1中,当从TSC外部输入用户数据时,PP/ST作者应指定执行的访问控制SFP或信息流控制SFP。对这些SFP的赋值确定了该功能输入用户数据的范围。

在FDP_ITC.2.5中,PP/ST作者应指定所有附加的输入控制规则,没有时应指明为"无"。这些规则将与FDP_ITC.2.1中选择的访问控制SFP或信息流控制SFP一起被TSF执行。

F8　TOE内部传送(FDP_ITT)

本子类提供通过内部信道在TOE的各部分间传送用户数据的保护要求。这与FDP_UCT和FDP_UIT子类——提供通过外部信道在远程TSF间传送用户数据的保护要求,以及FDP_ETC和FDP_ITC子类——解决在TSF控制之外用户数据的输入或输出形成对比。

用户注释

本子类中的要求允许PP/ST作者指定当数据在TOE内部传送时对用户数据所要求的安全,这种安全可以是避免泄露、篡改或可用性的丧失。

决定本子类应采用的物理隔离程度取决于预期使用的环境。在敌对环境中,只有系统总线分隔的TOE各部分间的数据传送可能会有风险产生。在更良性的环境中,传送可通过更多的传统媒体进行。

如果存在多个(访问控制或信息流控制)SFP,对每个命名的SFP应反复使用这些组件。

FDP_ITT.1　基本内部传送保护

操作

赋值:

在FDP_ITT.1.1中,PP/ST作者应指定访问控制SFP或信息流控制SFP,覆盖所传送的信

息。

选择：

在 FDP _ ITT.1.1 中，PP/ST 作者应指定用户数据在传送时由 TSF 防止发生的传送错误类型。这些错误类型为：泄露、篡改、可用性的丧失。

FDP _ ITT.2　属性分隔传送

用户应用注释

本组件可用于对具有不同许可级的信息提供不同的保护形式。

实现数据传送时相互隔离的方法之一是使用隔离的逻辑或物理信道。

操作

赋值：

在 FDP _ ITT.2.1 中，PP/ST 作者应指定访问控制 SFP 或信息流控制 SFP，覆盖所传送的信息。

选择：

在 FDP _ ITT.2.1 中，PP/ST 作者应指定用户数据在传送时由 TSF 防止发生的传送错误类型。这些错误类型为：泄露、篡改、可用性的丢失。

赋值：

在 FDP _ ITT.2.2 中，PP/ST 作者应指定 TSF 将使用的安全属性及其属性值，以决定在 TOE 物理上分隔的部分之间传送数据时何时进行隔离。比如：与一个属主身份标识相关联的用户数据会与关联另一个属主身份的用户数据分别传送。在这种情况下，数据属主的标识值，就用来决定何时分隔传送的数据。

FDP _ ITT.3　完整性监视

用户应用注释

本组件与 FDP _ ITT.1 或 FDP _ ITT.2 结合起来使用。它确保 TSF 检查接收到的用户数据（及其属性）的完整性。FDP _ ITT.1 或 FDP _ ITT.2 用保护数据不被篡改的方法提供数据（所以 FDP _ ITT.3 能检测数据的任何篡改）。

PP/ST 作者必须指定必须检测的错误类型。PP/ST 作者应考虑：数据篡改、替换、不可恢复的顺序改变、数据重放、不完备的数据以及其他完整性错误。

PP/ST 作者必须指定在检测到失败后 TSF 应采取的行动。比如：忽略用户数据、重新请求数据、提醒授权管理员、从其他线路重新路由。

操作

赋值：

在 FDP _ ITT.3.1 中，PP/ST 作者应指定覆盖所传送信息的信息访问控制 SFP 或信息流控制 SFP，并监视完整性错误。

在 FDP _ ITT.3.1 中，PP/ST 作者应指定在用户数据传送时，应监视的可能的完整性错误类型。

在 FDP _ ITT.3.2 中，PP/ST 作者应指定当产生完整性错误时 TSF 应采取的行动。比如：TSF 请求重新发送用户数据。FDP _ ITT.3.1 中指定的 SFP 将作为 TSF 采取的行动被执行。

FDP _ ITT.4　基于属性的完整性监视

本组件与FDP _ ITT.2结合使用，确保TSF检查所接收的通过隔离信道(基于指定的安全属性值)传送的用户数据的完整性。允许PP/ST作者指定检测到完整性错误后应采取的行动。比如：本组件可用来对不同完整性级别的信息提供不同的完整性错误检测和应采取的相应行动。

PP/ST作者必须指定必须检测的错误类型。PP/ST作者应考虑：数据篡改、替换、不可恢复的顺序改变、数据重放、不完备的数据以及其他完整性错误。

PP/ST作者应指定使得需要完整性错误监视的属性(以及相关的传送信道)。

PP/ST作者必须指定在检测到失败后TSF应采取的行动。比如：忽略用户数据、重新请求数据、提醒授权管理员、从其他线路重新路由。

操作

赋值：

在FDP _ ITT.4.1中，PP/ST作者应指定覆盖所传送信息的信息访问控制SFP或信息流控制SFP并监视完整性错误。

在FDP _ ITT.4.1中，PP/ST作者应指定在用户数据传送时，应监视的可能的完整性错误类型。

FDP _ ITT.4.1中，PP/ST作者应指定需要隔离传送信道的安全属性列表。该列表用来决定哪些用户数据需要基于安全属性和传送信道进行完整性错误监视。该元素直接与FDP _ ITT.2属性分隔传送相关。

在FDP _ ITT.4.2中，PP/ST作者应指定发生完整性错误时TSF应采取的行动。比如：TSF应请求重新发送用户数据。FDP _ ITT.4.1中指定的SFP将作为TSF采取的行动被执行。

F9　残余信息保护(FDP _ RIP)

本子类要求：已删除信息不应再能被访问，TOE中新产生的客体不应包含以前使用过的客体的信息。本子类没有对离线保存的客体提出要求。

用户注释

本子类要求保护已逻辑删除或释放的信息(尽管仍在系统中，并可以被恢复，但用户不可访问)。这特别包含客体中包含的、作为TSF部分重用资源的信息。客体的破坏并不必等同于资源或者资源内容的破坏。

它同样适用于被系统中不同主体连续重复使用的资源。比如：大多数典型的操作系统依赖硬件寄存器(资源)来支持系统中进程的运行。当进程从“运行”状态转换为“休眠”状态(反之亦然)，这些寄存器被不同的主体连续地重复使用。“转换”行动并没有被当作资源的分配或释放，而FDP _ RIP能用于这种事件和资源。

典型的，FDP _ RIP控制对不是当前所定义或作为可访问客体一部分的信息的访问。但在某些情况下可能并不如此。比如：客体A是一个文件，客体B是驻留该文件的磁盘，如果客体A被删除，尽管它仍是客体B的一部分，但其信息仍受FDP _ RIP的控制。

值得注意的是，FDP _ RIP仅适用于在线客体而非那些诸如备份在磁带上的离线客体。比如：如果一个TOE内的文件被删除，就可以实例化FDP _ RIP，要求在释放资源时不能有残余信息存在。然而TSF不能将该要求扩展到离线备份中的同一文件。因此该文件仍然可用。如果要关注离线客体，PP/ST作者应确保提出适当的环境目的来支持管理指南。

当FDP _ RIP要求在应用程序释放(比如：重新分配)客体到TSF的同时立即清除残余信息时，FDP _ RIP和FDP _ ROL会产生冲突。因而，FDP _ RIP选择“重新分配”不应与FDP _ ROL同时使用，因为没有信息可以反转。另一个选择，“在分配时的无效性”可与FDP _ ROL同时使用，但存在一个风

险，就是带有信息的资源在反转发生前分配给了新客体。如果是这样，反转就不可能实现。

在FDP_RIP中没有审计要求，因为这不是一个由用户使用的功能。分配或释放资源的审计将作为访问控制SFP或信息流控制SFP操作的一部分来进行。

本子类应用于诸如PP/ST作者所指定的，由访问控制SFP或信息流控制SFP所指定的客体。

FDP_RIP.1 子集残余信息保护

用户注释

对于TOE中的客体子集，本组件要求TSF确保在分配给客体的资源或从客体释放的资源中没有可用的残余信息。

操作

选择：

在FDP_RIP.1.1中，PP/ST作者应指定需要在分配或释放资源时激发残余信息保护功能的事件。

赋值：

在FDP_RIP.1.1中，PP/ST作者应指定服从残余信息保护功能的客体列表。

FDP_RIP.2 完全残余信息保护

用户应用注释

对于TOE中的所有客体，本组件要求TSF保证在分配或释放的资源中没有可用的残余信息。

操作

选择：

在FDP_RIP.2.1中，PP/ST作者应指定需要在分配或释放资源时激发残余信息保护功能的事件。

F10 反转(FDP_ROL)

本子类提出返回到一个良好定义的有效状态的需求，如用户取消修改文件的需求或在数据库中取消一连串未完成处理的需求。

本子类的目的在于帮助用户在取消最后一组行动后返回到良好定义的有效状态，或对于分布式数据库，将数据库所有的分布式拷贝返回到失败发生之前的状态。

当FDP_RIP使释放客体资源时其内容不再可用，那么FDP_RIP与FDP_ROL会相互冲突。因此FDP_RIP不能与FDP_ROL结合使用，因为已没有信息可以反转。当仅要求在给客体分配资源时使其内容不再可用，FDP_RIP可与FDP_ROL一起使用。这是因为FDP_ROL机制能有机会访问仍然存于TOE中的以前的信息，以成功实现反转操作。

反转要求受某些约束限制。比如，典型的文本编辑器只允许反转一定数量的命令。另一个例子是备份。在备份磁带重复使用后，它以前的信息将不能恢复，这同样对反转要求提出了限制。

FDP_ROL.1 基本反转

用户应用注释

本组件允许用户或主体在预先定义的客体集上取消一组操作。取消只能在某种限制下进行，如一定数量的字符或一定的时间段。

操作

赋值：

在 FDP _ ROL.1.1 中，PP/ST 作者应指定执行反转操作时需执行的访问控制 SFP 或信息流控制 SFP。这对于确保反转不是用于绕过指定的 SFP 是必须的。

在 FDP _ ROL.1.1 中，PP/ST 作者应指定能被反转的操作列表。

在 FDP _ ROL.1.1 中，PP/ST 作者应指定服从于反转策略的客体列表。

在 FDP _ ROL.1.2 中，PP/ST 作者应指定反转操作可以进行的边界限制。比如：该边界可以是预定义的时间段、可以在两分钟内取消执行的操作。其他可能的边界可定义为允许操作的最大数量或缓存大小。

FOP _ ROL.2　高级反转

用户应用注释

本组件要求 TSF 提供反转全部操作的能力，但用户能选择仅反转其中一部分。

操作

赋值：

在 FDP _ ROL.2.1 中，PP/ST 作者应指定进行反转操作时要执行的访问控制 SFP 或信息流控制 SFP。这对于确保反转不是用于绕过指定的 SFP 是必须的。

在 FDP _ ROL.2.1 中，PP/ST 作者应指定服从于反转策略的客体列表。

在 FDP _ ROL.2.2 中，PP/ST 作者应指定反转操作可以进行的边界限制。比如：该范围可以是预定义的时间段、在两分钟内可取消执行的操作。其他可能的边界可以是允许操作的最大数量或缓存的大小。

F11　存储数据的完整性(FDP _ SDI)

本子类提出对 TSC 内所存用户数据的保护要求。

用户注释

硬件的不稳定或错误可能影响内存中存贮的数据。本子类中提出检测这种不可预见错误的要求。本子类同样对 TSC 内保存在存贮设备上的用户数据的完整性提出要求。

为避免主体修改数据，应要求 FDP _ IFF 或 FDP _ ACF 子类(而不是本子类)。

本子类不同于 FDP _ ITT——TOE 内部传送，它是保护用户数据在 TOE 内部传送时不出现完整性错误。

FDP _ SDI.1　存储数据的完整性监视

用户应用注释

本组件监视媒体中存储数据的完整性错误。PP/ST 作者可指定各种用户数据属性作为监视的基础。

操作

赋值：

在 FDP _ SDI.1.1 中，PP/ST 作者应指定 TSF 应检测的完整性错误。

在 FDP _ SDF.1.1 中，PP/ST 作者应指定作为监视基础的用户数据属性。

FDP _ SDI.2　存储数据的完整性监视与行动

用户应用注释

本组件监视媒体中存储数据的完整性错误，PP/ST 作者应指定监视到完整性错误时应采取的行动。

操作

赋值：

在 FDP _ SDI.2.1 中，PP/ST 作者应指定 TSF 应检测的完整性错误。

在 FDP _ SDI.2.1 中，PP/ST 作者应指定作为监视基础的用户数据属性。

在 FDP _ SDI.2.2 中，PP/ST 作者应指定检测到完整性错误时应采取的行动。

F12 TSF 间用户数据传送的保密性保护(FDP _ UCT)

本子类提出当用户数据使用外部信道在 TOE 和可信 IT 产品间传递时保证其保密性的要求。用户数据在两点间传送时，通过防止未授权的泄露来实现保密性。

用户注释

本子类对传送中的用户数据保护提出了要求。相反，FTP _ ITC 处理的是 TSF 数据。

FDP _ UCT.1 基本的数据交换保密性

用户应用注释

TSF 具有能力保护用户数据在交换时不泄密。

操作

赋值：

在 FDP _ UCT.1.1 中，PP/ST 作者应指定交换用户数据时应执行的访问控制 SFP 或信息流控制 SFP。指定的策略将用于决定谁可以交换数据以及哪些数据可以交换。

选择：

在 FDP _ UCT.1.1 中，PP/ST 作者应指定本元素是否可用于传送或接收用户数据的机制中。

F13 TSF 间用户数据传送的完整性保护(FDP _ UIT)

本子类对用户数据在 TSF 和其他可信 IT 产品间传送时的完整性以及从可检测到的错误中恢复过来提出了要求。在最低限度上，本子类要监视用户数据针对篡改的完整性。进一步，本子类支持采用不同的方法来改正检测到的完整性错误。

用户注释

本子类对传送中的用户数据提出完整性要求，而 FPT _ ITI 处理的是 TSF 数据。

FDP _ UIT 和 FDP _ DCT 彼此都具有二重性，因为 FDP _ UCT 处理用户数据的保密性。因此，实现 FDP _ UIT 的相同机制可用于实现其他子类，比如 FDP _ UCT 和 FDP _ ITC。

FDP _ UIT.1 数据交换的完整性

用户应用注释

TSF 具有用某种方式发送和接收用户数据的基本能力，这种能力可检测到对用户数据的篡改。没有对试图从篡改中恢复的 TSF 机制提出要求。

操作

赋值：

在 FDP _ UIT.1.1 中，PP/ST 作者应指定在发送或接收数据时应执行的访问控制 SFP 或信息流控制 SFP。指定的策略将用于确定谁可以发送或接收数据以及哪些数据可以发送或接收。

选择：

在 FDP _ UIT.1.1 中，PP/ST 作者应指定本元素是否用于发送或接收客体的 TSF。

在 FDP _ UIT.1.1 中，PP/ST 作者应指定数据是否需要保护，以避免被篡改、删除、插入或重放。

在 FDP _ UIT.1.2 中，PP/ST 作者应指定是否应检测以下错误类型：篡改、删除、插入或重放。

FDP _ UIT.2　原发端数据交换恢复

用户应用注释

如果需要，在其他可信 IT 产品帮助下，本组件提供从确定的传送错误中恢复的能力。由于其他可信 IT 产品处于 TSC 之外，TSF 不能控制其行为。然而，它可提供能与其他可信 IT 产品合作，共同实现恢复目的的功能。比如：TSF 能包含这种功能，在检测到错误时，依靠原发端可信 IT 产品来重新发送数据。本组件涉及 TSF 恢复这种错误的能力。

操作

赋值：

在 FDP _ UIT.2.1 中，PP/ST 作者应指定在恢复用户数据时应执行的访问控制 SFP 或信息流控制 SFP。指定的策略用于确定哪些数据能被恢复以及如何恢复。

在 FDP _ UIT.2.1 中，PP/ST 作者应指定完整性错误列表，通过它 TSF 在原发端可信 IT 产品的帮助下能够恢复原来的用户数据。

FDP _ UIT.3　接受端数据交换恢复

用户应用注释

本组件提供从一组确定的传送错误中恢复的能力。它能在没有原发端可信 IT 产品的帮助下完成该任务。比如：如果检测到某些错误，传送协议必须足够健壮，使 TSF 能基于校验和和协议中可以得到的其他信息从错误中恢复。

操作

赋值：

在 FDP _ UIT.3.1 中，PP/ST 作者应指定在恢复数据时应执行的访问控制 SFP 或信息流控制 SFP。指定的策略用于确定哪些数据能够恢复以及如何恢复。

在 FDP _ UIT.3.1 中，PP/ST 作者应指定完整性错误的列表，仅通过它接收端的 TSF 就能恢复原始的用户数据。

附 录 G
（提示的附录）
标识和鉴别(FIA)

一个常见的安全要求是无歧义地标识执行 TOE 中的功能的人或实体。这不仅包括建立每一个用户所声称的身份，而且包括验证每一个用户确实是他或她所声称的人。这可通过要求用户向 TSF 提供一些已为 TSF 所知的与该用户有关的信息来实现。

此类中的子类涉及建立和验证所声称的用户身份方面的功能要求。为确保用户与正确的安全属性(比如：身份、组、角色、安全或完整性级别)相关联，需要标识和鉴别。

授权用户的明确标识和安全属性与用户和主体的正确相关是实施安全策略的关键。

FIA _ UID 子类用于确定用户的身份。

FIA _ UAU 子类用于验证用户的身份。

FIA _ AFL 子类用于对重复的未成功鉴别尝试定义限制。

FIA _ ATD 子类用于定义用于执行 TSP 的用户属性。

FIA _ USB 子类用于每一授权用户安全属性的正确关联。

FIA _ SOS 子类用于满足指定量度的秘密的生成和验证。

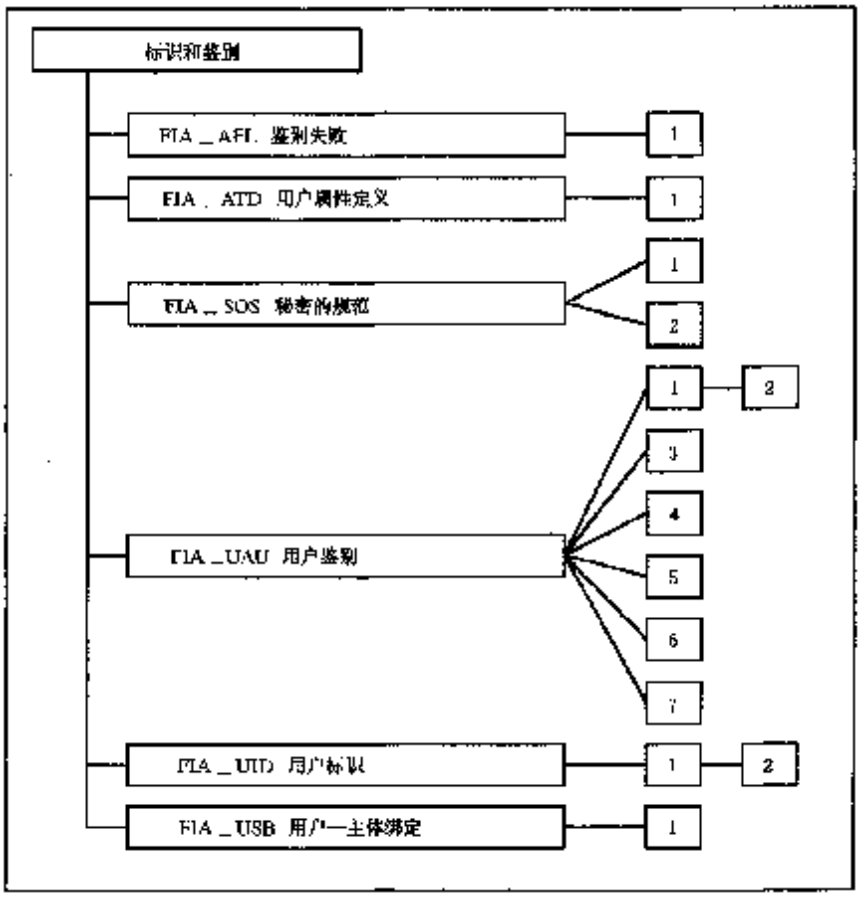


图 G1 标识和鉴别类分解

G1 鉴别失败(FIA _ AFL)

本子类用于定义鉴别尝试失败时鉴别尝试的值和 TSF 行动的要求。参数包括但不限于尝试的次数

和时间门限。

会话建立过程是与用户进行交互,执行会话建立的过程,独立于实际实现。如果不成功的鉴别尝试次数超过指定的门限,那么用户帐号或终端将被锁死。如果用户帐号被禁止,用户就不能登录到系统上。如果终端被禁止,终端(或终端所拥有的地址)就不能再使用。这两种状态都将保持到直到满足重建条件为止。

FIA_AFL.1 鉴别失败处理

用户应用注释

PP/ST 作者可以定义不成功鉴别尝试的次数,也可选择让 TOE 开发者或授权用户来定义该数值。鉴别不成功尝试的次数不必连续,但应与鉴别事件相关。如这种鉴别事件可以是:在指定的终端上从上一次成功建立会话以来的尝试次数。

PP/ST 作者可以说明在鉴别失败的情况下,TSF 将采取的行动列表。如果 PP/ST 作者认为合适的话,也可让授权的管理员来管理这些事件。这些行动可以是:终端失效,用户帐号失效或向管理员报警等。对这些行动必须说明,在什么条件下,情况可恢复正常。

为了防止拒绝服务,TOE 通常保证至少有一个用户帐号不能失效。

PP/ST 作者可以说明 TSF 的进一步行动,包括重新允许用户会话建立过程或向管理员报警的规则。例如这些行动有:直到过了指定的时间;直到授权管理员恢复终端/帐号;以及与上次失败尝试相关的时间调整(每次尝试失败,失效时间就加倍)。

操作

赋值:

在 FIA_AFL.1.1 中,如果 PP/ST 作者要说明不成功鉴别尝试的缺省次数的话,即达到或超过该次数后将触发这些事件,PP/ST 作者可以把这个数说明为"一授权管理员可配置的数值"。

在 FIA_AFL.1.1 中,PP/ST 作者应指定鉴别事件。例如这些鉴别事件有:对指定的用户身份自从上次鉴别成功以来的不成功鉴别尝试;当前终端自从上次成功鉴别以来的不成功鉴别尝试;最后 10 min 内不成功鉴别尝试的次数,等等。至少应规定一个鉴别事件。

在 FIA_AFL.1.2 中,PP/ST 作者应规定当达到或超过门限将采取的行动。这些行动可以是:使一个帐户失效 5 min;使终端失效一段随次数增加的时间(2 的不成攻鉴别次数次幂,单位是秒);或使帐号失效到直到管理员解除并且同时通知管理员。这些行动应规定措施以及措施的持续时间(若适用的话)或措施终止的条件。

G2 用户属性定义(FIA_ATD)

除了用户身份之外,所有授权用户还可以拥有一组安全属性,用以执行 TSP。本子类定义将用户安全属性与用户相关联的要求,这是支持 TSP 所必须的。

用户注释

在各单个的安全策略的定义间存在着依赖关系。这些单个定义应包含策略执行所必须的属性列表。

FIA_ATD.1 用户属性定义

用户应用注释

本组件规定应按用户级维护的安全属性。这意味着所列出的安全属性可以按用户级来分配和改变。也就是说,改变这个列表中与一个用户有关的一个安全属性,对其他任何用户的安全属性不会产生影

响。

在安全属性属于一组用户的情况下(如：组的能力列表)，用户将需要有一个对有关组的引用(作为安全属性)。

操作

赋值：

在 FIA _ ATD.1.1 中，PP/ST 作者应规定与单个用户相关的安全属性。例如，{“许可”、“组的标识符”、“权限”}就是此类列表的一个实例。

G3 秘密的规范(FIA _ SOS)

本子类定义对所提供的秘密执行所定义的质量量度，以及生成满足所定义的量度的秘密方面的机制的要求。例如，用户所提供的口令的自动校验或自动生成口令等。

秘密可以在 TOE 之外生成(比如：由用户选择并引入系统)。在这种情况下，FIA _ SOS.1 组件可用来确保外部生成的秘密遵从某些标准，比如：最小长度，非字典用字，或以前未用过。

秘密也可由 TOE 生成。在这种情况下，FIA _ SOS.2 组件可用来要求 TOE 确保秘密将遵从某些指定的量度。

用户注释

用户为鉴别机制提供的包含鉴别数据的秘密是基于用户具有的知识的。当采用密钥时，应使用 FCS 类来代替本子类。

FIA _ SOS.1 秘密的验证

用户应用注释

秘密可以由用户生成。这个组件确保，可以验证那些用户生成的秘密符合某一质量量度。

操作

赋值：

在 FIA _ SOS.1.1 中，PP/ST 作者应提供一个定义好的质量量度。该质量量度的说明可以简单到只是对一个要执行的质量检查的描述，也可像引用政府出版的定义秘密必须满足的质量量度的标准一样正式。例如：质量量度可包括对可接受的秘密的字母数字结构描述或可接受的秘密必须满足的空间大小的描述。

FIA _ SOS.2 秘密的 TSF 生成

本组件允许 TSF 为指定的功能生成秘密，如利用口令方式的鉴别。

用户应用注释

当秘密的生成算法中使用伪随机数生成器时，能提供具有高度的不可预见性的输出的输入随机数，应得到接受。该随机数(种子)可从许多可用的参数中导出，如系统时钟、系统寄存器、日期、时间等。参数的选择应保证从这些输入中可生成的唯一的种子数至少应等于必须生成的最少秘密数。

操作

赋值：

在 FIA _ SOS.2.1 中，PP/ST 作者应提供一个定义好的质量量度。该质量量度的说明可以简单

到只是对一个要执行的质量检查的描述，也可像引用政府出版的定义秘密必须满足的质量量度的标准的参照一样正式。例如：质量量度可包括对可接受的秘密的字母数字结构描述或可接受的秘密必须满足的空间大小的描述。

在 FIA _ SOS.2.2 中，PP/ST 作者应提供一个必须使用 TSF 生成的秘密的 TSF 功能列表。例如，基于口令的鉴别机制即属此类功能。

G4 用户鉴别(FIA _ UAU)

本子类定义 TSF 所支持的用户鉴别机制类型。以及定义用户鉴别机制必须依赖的所需属性。

FIA _ UAU.1 鉴别定时

用户应用注释

本组件要求 PP/ST 作者定义，在用户声称的身份得到鉴别前，TSF 代表用户可执行的 TSF 促成的行动。这些 TSF 促成的行动应该与在得到鉴别之前错误标识自己的用户无安全关系。对于其他一切不在该列表中的 TSF 促成的行动，在行动能够被 TSF 代表用户执行前，用户必须得到鉴别。

本组件不能控制这些行动在标识发生前是否也可以被执行。这需要使用 FIA _ UID.1 和 FIA _ UID.2，且赋以适当的值。

操作

赋值：

在 FIA _ UAU.1.1 中，PP/ST 作者应规定在用户声称的身份得到鉴别前，TSF 代表用户可执行的 TSF 促成的行动列表。这个列表不能为空，如果没有合适的行动，应使用 FIA _ UAU.2 组件代替。此类行动的一个实例是：在登录过程中请求帮助。

FIA _ UAU.2 在任何行动前的用户鉴别

用户应用注释

本组件要求在代表用户的任何 TSF 促成的行动发生前，相应用户应已被标识。

FIA _ UAU.3 不可伪造的鉴别

用户应用注释

这个组件对提供鉴别数据保护机制提出了要求。应检测出或拒绝掉从另一个用户处拷贝来的，或用其他方法组成的鉴别数据。这些机制提供一种信任：TSF 鉴别了的用户确实是它们所声称的用户。

本组件可能只对基于不可分享的鉴别数据(比如：生物测量学)的鉴别机制有用。对 TSF 来说，检测或防止 TSF 之外的口令共享是不可能的。

操作

选择：

在 FIA _ UAU.3.1 中，PP/ST 作者应规定 TSF 是检测、防止还是检测并防止对鉴别数据的伪造。

在 FIA _ UAU.3.2 中，PP/ST 作者应规定 TSF 是检测、防止还是检测并防止对鉴别数据的拷贝。

FIA _ UAU.4 一次性鉴别机制

用户应用注释

本组件提出对基于一次性鉴别数据之鉴别机制的要求。一次性鉴别数据可以是用户拥有或知道的某些事情，而非用户是什么。例如，一次性鉴别数据包括：一次性口令、加密的时间戳或秘密查找表中的随机数。

PP/ST 作者可说明本要求适用于哪一个鉴别机制。

操作

赋值：

在 **FIA _ UAU.4.1** 中，**PP/ST** 作者应规定本要求适用的鉴别机制列表。该赋值可以是“所有鉴别机制”。例如，该赋值可以是“用于鉴别外部网络上的人员的鉴别机制”。

FIA _ UAU.5　多重鉴别机制

用户应用注释

本组件提出在 **TOE** 内使用一个以上鉴别机制的要求。对每一个不同的机制，必须从 **FIA** 类中选择合适的要求用于该机制。为了反映对鉴别机制的不同使用的不同要求，同一组件可能被多次选中。

FMT 类中的管理功能可以为这组鉴别机制，以及确定鉴别是否成功的规则提供维护能力。

为了让匿名用户进入系统，可以并入一个“无”鉴别机制。此类访问的使用应在 **FIA _ UAU.5.2** 的规则中清晰地加以解释。

操作

赋值：

在 **FIA _ UAU.5.1** 中，**PP/ST** 作者应定义可用的鉴别机制。例如，此类列表可以是：“无，口令机制，生物测定(视网膜扫描)，**S/Key** 机制”。

在 **FIA _ UAU.5.2** 中，**PP/ST** 作者应规定描述鉴别机制如何提供鉴别以及每一机制将在何时使用的规则。这意味着：对每一种情况必须描述可能用于鉴别用户的那组机制。例如：这种规则的一个列表是：“如果用户有特殊权限，口令机制和生物测定机制两者都将使用，只有两者都鉴别成功后，这个鉴别才成功；对所有其他用户将使用口令机制。”

PP/ST 作者可以给出一个范围，在这个范围内，授权管理员可以说规定具体规则。规则的例子如：“应总是使用令牌(**token**)的方法对用户来进行鉴别；管理员可以规定同样必须使用的附加鉴别机制”。**PP/ST** 作者也可以选择不指定任何范围，把鉴别机制和它们的规则全部留给授权管理员。

FIA _ UAU.6　重鉴别

用户应用注释

这个组件涉及在定义的时刻对用户重鉴别的潜在需要。可能包括用户请求 **TSF** 执行安全相关的行动，以及 **TSF** 实体请求重鉴别(例如：服务器应用程序请求 **TSF** 对其服务的客户进行重鉴别)。

操作

赋值：

在 **FIA _ UAU.6.1** 中，**PP/ST** 作者应规定要求重鉴别的条件列表。该列表可包括：所指定的用户不活动期已过，用户请求改变活动的安全属性，或用户请求 **TSF** 执行某关键的安全功能。

PP/ST 作者可以给出重鉴别应发生的范围，把细节留给授权管理员。这样一条规则的实例如：“用户在一天之内至少被鉴别一次；管理员可以指定重鉴别经常进行，但不能高于每 **10 min** 一次”。

FIA _ UAU.7　受保护的鉴别反馈

用户应用注释

本组件涉及在鉴别过程中提供给用户的反馈。在一些系统中，反馈显示出了用户打入的字符数，但不显示字符本身；在另一些系统中，甚至这些信息可能也是不合适的。

本组件要求不能把鉴别数据原样返回给用户。在工作站环境中，对每一个输入的口令字符，可显示一“哑元”(比如：星号)，不显示原始字符。

操作

赋值：

在 FIA _ UAU.7.1 中，PP/ST 作者应规定提供给用户的与鉴别过程相关的反馈。例如，可指定反馈：“打入的字符数”，另一种类型的反馈是“鉴别已失败的鉴别机制”。

G5 用户标识(FIA _ UID)

本子类定义用户在执行其他由 TSF 促成并要求用户标识的行动之前，要求用户自我标识的条件。这些行动是由 TSF 促成的，并要求用户识别。

FIA _ UID.1 标识定时

用户应用注释

本组件对需要标识的用户提出要求。PP/ST 作者可以指出在标识发生前可执行的具体行动。

如果使用了 FIA _ UID.1，在 FIA _ UID.1 中提到的 TSF 促成的行动也应在 FIA _ UAU.1 中出现。

操作

赋值：

FIA _ UID.1.1 中，PP/ST 作者应规定在用户必须标识自己之前，代表用户的 TSF 可执行的 TSF 促成行动列表。如果没有合适的行动，应使用组件 FIA _ UID.2 来替代。此行动的实例可能有：在登录过程中请求帮助。

FIA _ UID.2 在任何行动之前的用户标识

用户应用注释

在本组件中用户将被标识。在用户被标识之前，TSF 不允许用户执行任何行动。

G6 用户—主体绑定(FIA _ USB)

一个已鉴别了的用户，为了使用 TOE，一般要激活一个主体。用户的安全属性与这个主体相关联(全部或部分地)。本子类定义建立和维护用户安全属性与代表用户操作的主体之间的关联的要求。

FIA _ USB.1 用户—主体绑定

用户应用注释

已经证明“代表……的行动”一词在以前的准则中是有争议的问题。本意是，主体代表的是产生或激活它以执行某一任务的用户，因此，当一个主体被建立，该主体就代表发起建立它的用户。在使用匿名的情况下，主体仍代表着用户，但用户的身份是未知的。一类特殊的主体是它们服务于多个用户(例如：一个服务器进程)，在这种情况下，建立这个主体的用户就被假定为这个主体的“拥有者”。

附 录 H
（提示的附录）
安全管理（FMT）

本类规定 TSF 几个方面的管理：安全属性、TSF 数据和功能。不同的管理角色和它们之间的相互作用（如能力的分离）也可在本类中规定。

在 TOE 由多个物理上分离的部件组成，形成分布式系统的环境中，与安全属性、TSF 数据和功能修改的传播有关的定时问题变得非常复杂，尤其是当这些信息需要在 TOE 的各部分间复制时更是如此。当选取像 FMT _REV.1“撤消”或 FMT _SAE.1“时限授权”这样的组件时，由于它们的行为有可能被损害，更需要考虑上面的问题。在这种情况下，建议使用 FPT _TRC 中的组件。

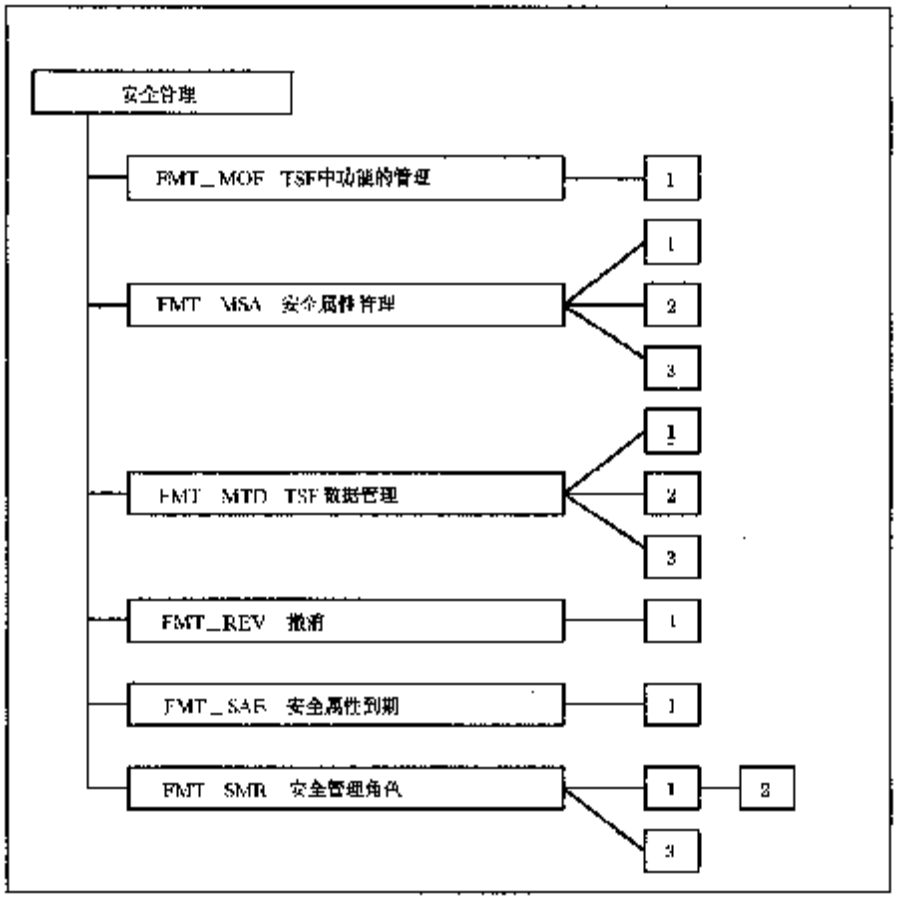


图 H1 安全管理类分解

H1 TSF 中功能的管理（FMT _MOF）

TSF 管理功能使授权用户能够建立和控制 TOE 的安全运行。这些管理功能通常分成几种不同的类别：

a）与 TOE 执行的访问控制、责任可追查性和鉴别控制相关的管理功能。例如，用户安全特征的定义和更新（如与用户名、用户帐号、系统入口参数相关的唯一标识符）；审计系统控制的定义与更新（如审计事件的选取、审计迹的管理、审计迹的分析以及审计报告的生成）；每个用户策略属性的定义和更新（如用户许可）；已知系统访问控制标签的定义；以及用户组的控制与管理。

b）与可用性控制相关的管理功能。例如，可用性参数或资源配额的定义和更新。

c）与一般安装和配置有关的管理功能。例如，TOE 的配置、手工恢复、TOE 安全补丁的安装（如果有的话）、硬件的修理和重新安装。

d）与常规控制和 TOE 资源维护有关的管理功能。例如，允许或禁止外围设备、可拆卸存储媒体的安装、用户和系统客体的备份与恢复。

注意，这些功能根据 PP 或 ST 中包含的子类，需出现在 TOE 中。PP/ST 作者有责任确保提供适当的功能，以便以安全的方式管理系统。

TSF 可能包括能够为管理员所控制的功能。例如，审计功能可以被关闭，时间同步可以是可切换的，或鉴别机制可以是可修改的。

FMT _ MOF.1　安全功能行为的管理

本组件允许所标识的角色管理 TSF 的安全功能。这可能需要获取安全功能的当前状态、禁止安全功能、允许安全功能、修改安全功能的行为。一个修改安全功能行为的例子是：改变鉴别机制。

操作

选择：

在 FMT _ MOF.1.1 中，PP/ST 作者应该选择角色是否能：确定安全功能的行为、禁止安全功能、允许安全功能、修改安全功能的行为。

赋值：

在 FMT _ MOF.1.1 中，PP/ST 作者应规定能够被指定的角色修改的功能，例如审计和确定时间等。

在 FMT _ MOF.1.1 中，PP/ST 作者应规定允许修改 TSF 中的功能的角色。可能的角色在 FMT _ SMR.1 中说明。

H2　安全属性的管理（FMT _ MSA）

本子类定义对安全属性的管理要求。

用户、主体和客体拥有的相关安全属性将影响 TSF 的行为。此类安全属性的例子有：用户所属的组、用户可能承担的角色、进程（主体）的优先权，以及属于一个角色或用户的权力。这些安全属性可能需要由用户、主体或特定的授权用户（即对于此管理具有明确给定权限的用户）去管理。

必须注意，给用户分配权利的权利本身就是一个安全属性，或者潜在地受 FMT _ MSA.1 管理。

FMT _ MSA.2 可用来确保任何可以接受的安全属性的组合都处于安全状态。“安全”含义的定义留待 TOE 指南和 TSP 模型中给出。如果开发者提供了安全值的清晰定义和认为其安全的理由，则 FMT _ MSA.2 对 ADV _ SPM.1 的依赖关系就可以不考虑。

在某些情况下，建立了主体、客体或用户帐号，如果对相关的安全属性没有给出明确的值，那么就需使用默认值。FMT _ MSA.1 可以用来规定这些默认值是可以管理的。

FMT _ MSA.1　安全属性的管理

本组件允许担当特定角色的用户去管理指定的安全属性。在组件 FMT _ SMR.1 内这些用户被赋予某个角色。

参数的默认值是指在参数创建时没有专门指定某个值时，该参数所取的值。初始值是在参数创建过程中提供的，且覆盖默认值。

操作

赋值：

在 FMT _ MSA.1.1 中，PP/ST 作者应列出安全属性所适用的访问控制 SFP 或信息流控制 SFP。

选择：

在 FMT _ MSA.1.1 中，PP/ST 作者应规定可应用于指定的安全属性的操作。PP/ST 作者可规定：某角色可以修改安全属性的默认值（改变默认值）、查询安全属性、修改安全属性、删除整个安全属性或定义他们自己的操作。

赋值：

在 FMT _ MSA.1.1 中（如果被选择），PP/ST 作者应规定该角色能够执行哪些其他操作。“创建”便可能是这种操作的一个例子。

FMT _ MSA.1.1 中，PP/ST 作者应规定那些能够由指定角色操作的安全属性。对 PP/ST 作者可能规定默认值，如默认访问权限，是可管理的。这些安全属性的例子有：用户许可，服务优先级，访问控制表，默认访问权限。

FMT _ MSA.1.1 中，PP/ST 作者应规定允许对安全属性进行操作的角色。可能的角色在 FMT _ SMR.1 中规定。

FMT _ MSA.2　安全的安全属性

本组件包含对安全属性的赋值要求。所赋值应使得 TOE 保持安全状态。

“安全”含义的定义在本组件中没有给出，而留给了 TOE 的开发（特别是 ADV _ SPM.1 非形式化 TOE 安全策略模型）和指南中的结果信息。例如：如果建立了一个用户帐号，则不应使用简单口令。

FMT _ MSA.3　静态属性初始化

用户应用注释

本组件要求 TSF 为相关客体的安全属性提供默认值，该默认值能够被初始值所覆盖。如果存在一种机制规定在创建时允许这样做的话，一个新客体在创建时仍可能有不同的安全属性。

操作

赋值：

FMT _ MSA.3.1 中，PP/ST 作者应列出安全属性所适用的访问控制 SFP 或信息流控制 SFP。

选择：

FMT _ MSA.3.1 中，PP/ST 作者应选择，访问控制属性的默认特性是受限的、许可的还是其他特性。如选择其他特性，PP/ST 作者应将其细化为一个特定的特性。

赋值：

FMT _ MSA.3.2 中，PP/ST 作者应规定允许修改安全属性值的角色。这些可能的角色在 FMT _ SMR.1 中规定。

H3　TSF 数据的管理（FMT _ MTD）

本组件对 TSF 数据管理提出要求。TSF 数据方面的例子有：当前时间、审计迹等。因此，本子类允许说明谁能读、删除或创建审计迹。

FMT _ MTD.1　TSF 数据的管理

本组件允许具有某个角色身份的用户去管理 TSF 数据的值。其中在组件 FMT _ SMR.1 中为用户分配了角色。

参数的默认值是指在参数创建时若没有专门指定某个值，该参数所取的值。初始值在参数创建过程

中提供,它将覆盖默认值。

操作

选择:

FMT _ MTD.1.1 中,**PP/ST** 作者应规定可用于指定 **TSF** 数据的操作。**PP/ST** 作者可规定,角色可以:修改 **TSF** 数据的默认值(改变默认值)、清除 **TSF** 数据、查询 **TSF** 数据、修改 **TSF** 数据或完全删除 **TSF** 数据。如希望这样,**PP/ST** 作者可以说明任何类型的操作。需要澄清的是"清除 **TSF** 数据"意味着 **TSF** 数据的内容被取消,但是该实体本身还保留在系统内。

赋值:

FMT _ MTD.1.1 中(如果被选择),**PP/ST** 作者应规定角色能够执行哪些其他操作。"创建"就是这样的例子。

FMT _ MTD.1.1 中,**PP/ST** 作者应规定能够被所标识的角色操作的 **TSF** 数据。**PP/ST** 作者可能规定,默认值可被管理。

FMT _ MTD.1.1 中,**PP/ST** 作者应规定允许对 **TSF** 数据进行操作的角色。可能的角色在 **FMT _ SMR.1** 中规定。

FMT _ MTD.2　TSF 数据限制的管理

本组件规定对 TSF 数据的限制,以及当超过这些限制时所要采取的行动。例如,本组件将允许定义对审计记录大小的限制,以及规定当这些限制被超越时,对所要采取的行动的规定。

操作

赋值:

在 **FMT _ MTD.2.1** 中,**PP/ST** 作者应规定可能有限值的 **TSF** 数据以及这些限值,这样的 **TSF** 数据的一个例子是:用户登录数。

FMT _ MTD.2.1 中,**PP/ST** 作者应规定允许修改 **TSF** 数据限制的角色以及待采取的行动。可能的角色在 **FMT _ SMR.1** 中规定。

FMT _ MTD.2.2 中,**PP/ST** 作者应规定如果超过对指定的 **TSF** 数据的指定限制所要采取的行动。此类 **TSF** 行动的一个例子是,通知授权用户且生成审计记录。

FMT _ MTD.3　安全的 TSF 数据

本组件包含了对 TSF 数据赋值的要求。所赋值应使得 TOE 保持在安全状态。

"安全"含义的定义在本组件中没有给出,而留给了 TOE 的开发者(特别是 ADV _ SPM.1 非正式 TOE 安全策略模型)和指南中的结论信息。如果开发者提供了安全值的清晰定义和认为它们安全的理由,则 FMT _ MSA.2 对 ADV _ SPM.1 的依赖性就可以不考虑。

H4　撤消(FMT _ REV)

本子类定义了对 TOE 内的各种实体的安全属性的撤消。

FMT _ REV.1　撤消

本组件规定对撤消权限的要求。它要求有撤消规则的规定,例如:

a) 撤消发生在用户下次登录时;

b) 撤消发生在下次试图打开该文件时;

c) 撤消发生在某一固定时间段内。这可能意味着所有开放的连接每隔 *X* 分钟后要重新评价。

操作

选择：

FMT _ REV.1.1 中，**PP/ST** 作者应规定 **TSF** 是否应提供从用户、主体、客体或其他任何资源撤消安全属性的能力。如果选择最后一个选项，则 **PP/ST** 作者须使用细化操作，定义该资源。

赋值：

FMT _ REV.1.1 中，**PP/ST** 作者应规定允许修改 **TSF** 中功能的角色。这些可能的角色在 **FMT _ SMR.1** 中规定。

FMT _ REV.1.2 中，**PP/ST** 作者应规定撤消规则。例如：撤消发生在“对相关资源的下一次操作之前”或“所有新主体的创建时”。

H5 安全属性到期(FMT _ SAE)

本子类涉及对安全属性的有效性实施时间限制的能力。本子类可用来为访问控制属性、标识和鉴别属性、证书(密钥证书，如 ANSI X.509)和审计属性等规定到期要求。

FMT _ SAE.1 时限授权

操作

赋值：

对 **FMT _ SAE.1.1**，**PP/ST** 作者应提供支持期限的安全属性列表，此类属性的一个例子是：用户安全许可。

FMT _ SAE.1.1 中，**PP/ST** 作者应规定允许修改 **TSF** 中安全属性的角色。可能的角色在 **FMT _ SMR.1** 中规定。

对 **FMT _ SAE.1.2**，**PP/ST** 作者应为每个安全属性提供一个到期时将采取的行动列表。例如：用户安全许可，当它到期时，被设置为 **TOE** 上允许的最低级别的许可。如果 **PP/ST** 希望立即撤消，则应指定“立即撤消”这一行动。

H6 安全管理角色(FMT _ SMR)

本子类用于减少因用户超越职责滥用授权而导致破坏的可能性。它也强调了用不适当的机制对 TSF 进行安全管理的威胁。

本子类要求维护用以识别一个用户是否有权使用特定的安全相关的管理功能方面的信息。

某些管理行动可由用户完成，另外一些仅能由组织内的指定人员完成。本子类允许定义不同的角色，如拥有者、审计员、管理员、日常管理员。

本子类中所指的角色是与安全有关的角色。每个角色可拥有一组广泛的能力(如 Unix 中的 root 权限)，也可以只拥有一个单一的权限(如读取帮助文件这样的单个客体的权利)。本子类定义了这些角色。角色的能力在 **FMT _ MOF**、**FMT _ MSA** 和 **FMT _ MTD** 中定义。

某些类型的角色可能是互斥的，例如日常管理员可能能够定义和激活用户，但可能不能删除用户(这留给管理员(角色))。本类将允许规定两人控制这样的策略。

FMT _ SMR.1 安全角色

本组件规定 TSF 应认同的不同角色。通常系统区分实体的拥有者、管理员和其他用户。

操作

赋值：

在 FMT _ SMR.1.1 中，PP/ST 作者应规定系统所认同的角色，就安全而言这些角色是用户可以拥有的角色。例如：拥用者、审计员和管理员。

FMT _ SMK.2　安全角色限制

本组件规定 TSF 应该认同的不同角色，以及管理这些角色的条件。通常系统区分实体的拥有者、管理员和其他用户。

这些角色的条件规定了不同角色之间的相互关系，以及用户何时能承担这些角色的限制条件。

操作

赋值：

在 FMT _ SMR.2.1 中，PP/ST 作者应规定系统所认同的角色。就安全而言这些角色是用户可以拥有的角色。例如：拥有者、审计员、管理员。

在 FMT _ SMK.2.3 中，PP/ST 作者应规定制约角色分配的条件。这些情况的例子如："一个帐号不能同时具有审计员和管理员两种角色"或"具有助理角色的用户也必须具有拥有者角色。"

FMT _ SMR.3　承担角色

本组件规定必须给出明确的请求以承担特定的角色。

操作

赋值：

在 FMT _ SMR.3.1 中，PP/ST 作者应规定需要作出明确请求才能承担的角色。例如：审计员和管理员。

附　录　I
（提示的附录）
隐私（FPR）

本类描述了这样的要求，它能被用来满足用户的隐私需要，同时允许具有尽可能强的系统灵活性以保持对系统操作的充分控制。

在本类的组件中，所要求的安全功能是否覆盖授权用户是具有灵活性的。例如，PP/ST 作者可认为对适当的授权用户而言不要求保护单个用户的隐私是合理的。

本类同其他的类一起（如涉及审计、访问控制、可信路径和抗抵赖）为满足规定期望的隐私行为提供了灵活性。另一方面，本类中的要求可能会对使用其他类的组件如 FIA 或 FAU 施加限制。例如，如果不允许授权用户看到用户的身份（如匿名或假名），则显然不可能让个别用户对他们执行的、被隐私要求覆盖的任何与安全相关的行为负责。然而，仍然有可能在 PP/ST 中包括审计要求，发生特定安全相关事件的这个事实比知道谁对它负责更加重要。

在应用注释中，对 FAU 类提供了附加的信息，其中解释了在审计上下文中定义的"身份"，也可能是一个化名或能标识用户身份的其他信息。

本类描述了 4 个子类：匿名、假名、不可关联性、不可观察性。匿名、假名和不可关联性有复杂的相互关系。当选择一子类时，该选择应依赖于所确定的威胁。对某些类型的隐私威胁，假名会比匿名更合适（如：有审计要求时）。此外，某些类型的隐私威胁，通过几个子类的组件组合可以很好地对抗。

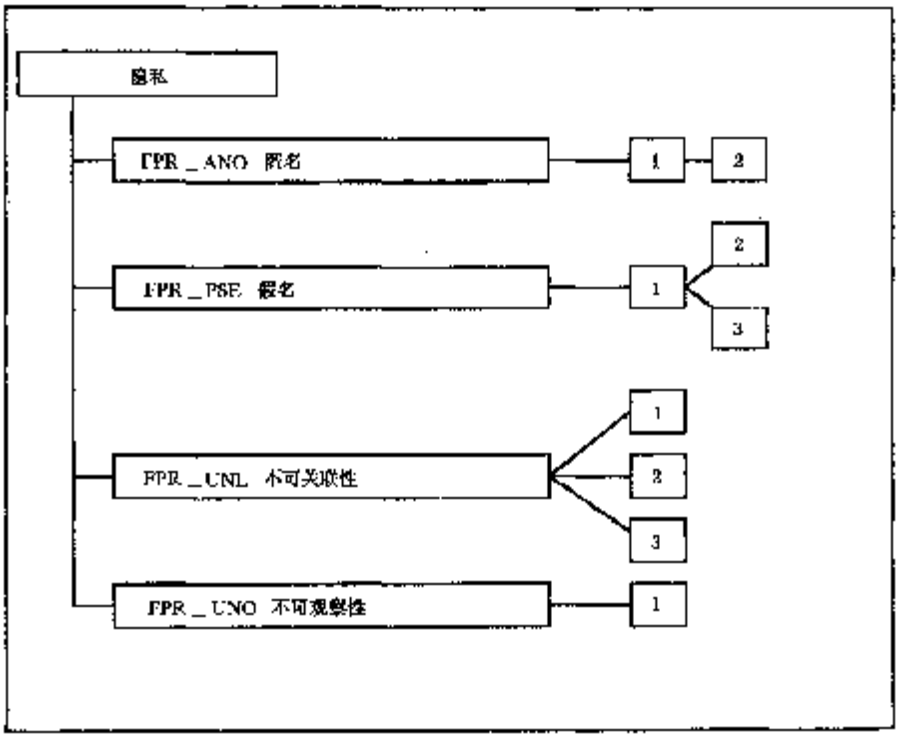


图 I1　隐私类分解

所有的子类都假定用户没有明确执行暴露用户自己身份的行动。例如，不期望 TSF 在电子消息或数据库中频显用户名。

本类中的所有子类都有可通过操作确定范围的组件。这些操作允许 PP/ST 作者指明 TSF 必须对其具有抵抗力的协作用户/主体。匿名的实例化可以是："TSF 应确保用户或主体不能确定与远程咨询应用相绑定的用户身份。"

要注意 TSF 保护不仅应该防止单个用户，而且应防止获取信息的协作用户。本类所提供的保护强度应与 GB/T 18336 第 1 部分附录 B 和附录 C 所规定的功能强度一样。

I1　匿名(FPR_ANO)

匿名保证主体可使用资源和服务而不暴露它的用户身份。

用户注释

本子类的意图是规定一个用户或主体可以采取行动而不把用户的身份暴露给其他的用户、主体或客体。本子类为 PP/ST 作者提供了一个方法去标识一些用户的身份，这些用户不能看到那些执行某些行动的人的身份。

因此，如果使用匿名的主体执行一个行动，另一个主体将不能确定其身份，甚至不能确定利用该主体的用户身份的引证。匿名的焦点是保护用户的身份，而不是保护主体的身份，所以主体的身份不受防止泄露的保护。

虽然主体的身份没有发布给其他主体和用户，并不明确禁止 TSF 获得用户的身份。如果不允许 TSF 知道用户的身份，可以调用 FPR_ANO.2，在那种情形下，TSF 不应要求用户的信息。

对"确定"一词的解释应在最广的字面意义上来理解。PP/ST 作者可能想使用一个功能强度来规定应用的严格程度。

本组件分级区分了用户和授权用户。一个授权用户经常被排除在本组件之外，因此被允许检索用户的身份。然而，并没有特别要求一个授权用户必须有能力确定用户的身份。对最终的隐私来说，本组件将表明没有用户或授权用户能看到执行行动的任何人的身份。

一些系统将为所提供的所有服务提供匿名，而另一些系统为某些确定的主体/操作提供匿名。为了提供这一灵活性，一个操作是包括在被定义了的要求范围内。如果 PP/ST 作者想满足所有的主体/操作，则应提供术语“所有的主体和所有的操作”。

可能的应用包括秘密查询公用数据库、应答电子民意测验、匿名支付或捐赠。

潜在的敌意用户或主体是把恶意的部分(如特洛伊木马) 偷引入系统中的提供者、系统操作员、通信伙伴和用户。所有这些用户会研究使用模式(如哪些用户使用哪些服务)和滥用这些信息。

FPR _ ANO.1　匿名

用户应用注释

本组件保证用户的身份受到保护而不泄露。然而，可能有这样的实例，即一个授权用户能确定谁执行某些行动。本组件给出了得到有限或是完全隐私策略的灵活性。

操作

赋值：

在 FPR _ ANO.1.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体这样的角色，但 TSF 不仅必须防范每一单个用户或主体，而且也必须防范协作用户或主体。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

在 FPR _ ANO.1.1 中，PP/ST 作者应标识出主体或操作或客体的一个列表，其中主体的真正用户名应受到保护，例如“表决应用”。

FPR _ ANO.2　无征求信息的匿名

用户应用注释

本组件用来确保不允许 TSF 知道用户的身份。

操作

赋值：

在 FPR _ ANO.2.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体这样的角色，但 TSF 不仅必须防范每一单个用户或主体，而且也必须防范协作用户或主体。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

在 FPR _ ANO.2.1 中，PP/ST 作者应标识出主体或操作或客体的一个列表，其中主体的真正用户名应受到保护，例如“表决应用”。

在 FPR _ ANO.2.2 中，PP/ST 作者应标识出满足匿名要求的服务列表，例如，“工作描述的访问”。

对 FPR _ ANO.2.2，PP/ST 应给出主体的列表，当提供规定的服务时，主体的真实用户名应受到保护。

I2　假名(FPR _ PSE)

假名确保一个用户能够使用资源或服务而不泄露自己的身份，但他仍能负责。通过直接将用户与 TSF 持有的引用名(化名)关联起来，或是通过提供用于处理目的的化名(如帐号)，所以他仍能负责。

用户注释

在许多方面，假名类似于匿名，假名和匿名都保护用户的身份，但假名对用户身份的引证信息是为责任可追查性或其他目的而保留的。

组件 FPR _ PSE.1 没规定对用户身份引证信息的要求。为了规定该要求，提供了两组要求：FPR _ PSE.2 和 FPR _ PSE.3。

使用引证信息的一种办法是通过能获取原始用户标识符。例如，在一个数字现金环境中，当一张支票已经被多次配发(即欺骗)时，若能追踪用户的身份会更有利一些。一般来说，用户身份须在特定的条件下才被检索。PP/ST 作者可能要结合 FPR _ PSE.2“可逆假名”来描述这些服务。

参考信息的另一个用法是作为用户的一个化名。例如，一个不希望被标识的用户可提供一个帐户，使用资源就向该帐户收费。在这种情形下，用户身份的引证是该用户的一个化名，其他用户或主体无需获得该用户的身份就可以利用此化名执行它们的功能(例如，对系统的使用进行统计操作)。在此情形下，PP/ST 作者可能希望结合 FPR _ PSE.3“化名假名”来规定引证信息须遵守的规则。

通过使用上面的这些结构，用 FPR _ PSE.2“可逆假名”可建立数字货币，它规定用户身份将得到保护，而且如果在条件中就是这么规定的话，则当数字货币被使用两次时，就有一个去追踪用户身份的要求。若用户是诚实的，用户身份受到保护；当用户试图欺骗时，可以追踪用户的身份。

一种不同的系统可以是一个数字信用卡，用户提供一个假名指定一个帐户，从中可提取现金。在这种情形下，可以使用 FPR _ PSE.3“化名假名”。本组件将规定用户身份会得到保护，进而同一个用户仅得到他(她)已经提供钱款的指定数目(如果在条件中已这样规定的话)。

应当认识到，更严格的组件可能不能同其他要求组合，诸如标识、鉴别或审计。“确定身份”的解释应在更广的字面意义上理解。在操作中 TSF 没提供这些信息，实体也不能确定主体或调用操作主体的拥有者，TSF 也不会记录用户或主体可用的、在将来会暴露用户身份的信息。

TSF 不揭示任何有损用户身份的信息，如代表用户行动的主体的身份。被认为是敏感的信息依赖于攻击者所花费的努力。因此，FPR _ PSE 假名子类主要服从功能要求的强度。

可能的应用包括通过电话服务向打电话者的收费，而不揭示其身份，或是对匿名使用电子支付系统收费。

潜在的敌意用户或主体是把恶意的部分(如特洛伊木马) 偷引入系统中的提供者、系统操作员、通信伙伴和用户。所有这些攻击者会研究哪些用户使用哪些服务，并滥用这些信息。作为对匿名服务的补充，假名服务包含了没有标识的授权方法，特别是对匿名支付(“数字现金”)。这帮助提供者以安全的方式获得他们的费用，同时还维持了顾客的匿名。

FPR _ PSE.1　假名

用户应用注释

本组件提供用户保护，防止身份泄露给其他用户。但用户仍能对其行为负责。

操作

赋值：

在 FPR _ PSE.1.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体这样的角色，但 TSF 不仅必须防范每一单个用户或主体，而且也必须防范协作用户或主体。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

在 FPR _ PSE.1.1 中，PP/ST 作者应标识出主体或操作或客体的一个列表，其中主体的真正用户名应受到保护，例如“工作提供者的访问”。注意“客体”包括能使其他用户或主体得到真实的用户身份的其他属性。

FPR _ PSE.1.2 中，PP/ST 作者应标识 TSF 能提供的化名的数目(一个或多个)。

FPR_PSE.1.2 中,PP/ST 作者应标识 TSF 能向其提供化名的主体的列表。

选择:

FPR_PSE.1.3 中,PP/ST 作者应规定用户化名是由 TSF 生成,还是由用户提供。

赋值:

FPR_PSE.1.3 中,PP/ST 作者应标识 TSF 生成的或用户生成的化名应遵守的量度。

FPR_PSE.2 可逆假名

用户应用注释

在此组件中,TSF 须确信在特定的条件下,可以确定与所提供参考相关的用户身份。

FPR_PSE.1 中,TSF 应提供化名代替用户身份。当满足规定的条件时,可以确定化名所属的用户身份。在电子现金环境下这样一个条件的例子是:"TSF 将向公证人提供仅在支票已经签发两次的条件下,依据所提供的化名能确定用户身份的能力。"

操作

赋值:

在 FPR_PSE.2.1 中,PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如,即使 PP/ST 作者只规定了单个用户或主体这样的角色,但 TSF 不仅必须防范每一单个用户或主体,而且也必须防范协作用户或主体。例如,用户集可以是一组用户,他们能在相同的角色下操作或都能用相同的进程。

在 FPR_PSE.2.1 中,PP/ST 作者应标识出主体或操作或客体的一个列表,其中主体的真正用户名应受到保护,例如"工作提供者的访问"。注意"客体"包括能使其他用户或主体得到真实的用户身份的其他属性。

FPR_PSE.2.2 中,PP/ST 作者应标识 TSF 能提供的化名的数目(一个或多个)。

FPR_PSE.2.2 中,PP/ST 作者应标识 TSF 能向其提供化名的主体的列表。

选择:

FPR_PSE.2.3 中,PP/ST 作者应规定用户化名是由 TSF 生成,还是由用户提供。

赋值:

FPR_PSE.2.3 中,PP/ST 作者应标识 TSF 生成的或用户生成的化名应遵守的量度。

选择:

FPR_PSE.2.4 中,PP/ST 作者应选择是否授权用户或可信主体能确定真正的用户名。

赋值:

FPR_PSE.2.4 中,PP/ST 作者应标识在规定条件下能获取真实用户名的可信主体列表,例如公证人或特定的授权用户。

FPR_PSE.2.4 中,PP/ST 作者应标识条件列表,在这些条件下可信主体和授权用户基于提供的引证能确定真正的用户名。这些条件可以是一天的时段或是他们像法院传票一样可被管理。

FPR_PSE.3 化名假名

用户应用注释

在此组件中,TSF 须确保所提供的引证满足了其构造规则,因此可被潜在的不安全主体以安全的方式使用。

如果一个用户想使用磁盘资源但不泄露自己的身份,可使用假名。然而,每次用户访问这个系统时,须用相同的化名。这样的条件可在本组件中规定。

操作

赋值：

在 FPR _ PSE.3.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体这样的角色，但 TSF 不仅必须防范每一单个用户或主体，而且也必须防范协作用户或主体。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

在 FPR _ PSE.3.1 中，PP/ST 作者应标识出主体或操作或客体的一个列表，其中主体的真正用户名应受到保护，例如“工作提供者的访问”。注意“客体”包括能使其他用户或主体得到真实的用户身份的其他属性。

FPR _ PSE.3.2 中，PP/ST 作者应标识 TSF 能提供的化名的数目(一个或多个)。

FPR _ PSE.3.2 中，PP/ST 作者应标识 TSF 能向其提供化名的主体的列表。

选择：

FPR _ PSE.3.3 中，PP/ST 作者应规定用户化名是由 TSF 生成，还是由用户提供。

赋值：

FPR _ PSE.3.3 中，PP/ST 作者应标识 TSF 生成的或用户生成的化名应遵守的量度。

FPR _ PSE.3.4 中，PP/ST 作者应标识条件列表，这些条件指出对真正的用户名使用引证信息何时是相同的，何时是不同的。例如“当用户登录到相同的主机上”时，它将用唯一的化名。

I3 不可关联性(FPR _ UNL)

不可关联性确保一个用户可以多次使用资源和服务，而无需其他的用户关联这些使用。不可关联性与假名的不同在于，虽然在假名中用户也是未知的，但可提供不同行动之间的关系。

用户注释

不可关联性要求的目的是保护用户身份，以防止使用操作轮廓。例如，当用唯一号码使用电话智能卡时，电话公司可确定该电话卡的用户行为。当知道用户的电话的基本情况时，此卡就同特定的用户相关联了。隐藏一个服务或资源访问的不同请求之间的关系会防止对这种信息的收集。

结果，对不可关联性的要求可能暗示一个操作的主体或用户身份必须得到保护。否则，该信息可用来与其他操作关联。

不同操作的不可关联性要求是不能关联的。这种关系有几种形式。例如，操作与用户相关，或与初始化行动的终端相关，或该行动执行的时间相关。PP/ST 作者可以规定必须对抗什么类型的关系。

可能的应用包括，多次使用假名，而无需建立一个可能泄露用户身份的使用模式。

潜在的敌意用户或主体是把恶意的部分(如特洛伊木马) 偷引入系统中的提供者、系统操作员、通信伙伴和用户，他们不做操作而只想获取有关信息。所有这些攻击者会研究(如哪些用户使用哪些服务)并滥用这些信息。不可关联性保护用户以防关联，这种关联可以从一个客户的几次行动中得出。一个例子是，匿名客户打给不同伙伴的一系列电话，这些伙伴身份的组合可以揭示该客户的身份。

FPR _ UNL.1 不可关联性

用户应用注释

本组件确保用户不能在系统上链接不同的操作和以此获取信息。

操作

赋值：

FPR _ UNL.1.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即

使 PP/ST 作者只规定了单个用户或主体这样的角色，但 TSF 不仅必须防范每一单个用户或主体，而且也必须防范协作用户或主体。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

FPR _ UNL.1.1 中，PP/ST 作者须应标识出操作的一个列表，它们要满足不可关联性要求，例如，“发送电子邮件”。

选择：

FPR _ UNL.1.1 中，PP/ST 应选取可被掩盖的关系。该选择将规定用户身份或者关系的指派。

赋值：

FPR _ UNL.1.1 中，PP/ST 作者应标识受到保护的关系列表，例如，“源来自相同的终端”。

I4 不可观察性(FPR _ UNO)

不可观察性确保一个用户可以使用一个资源或服务，而其他人，特别是第三方，不能观察到该资源或服务正被使用。

用户注释

与先前的“匿名”、“假名”和“不可关联性”子类不同，不可观察性从不同的方面研究用户的身份。在此情形下，目的是隐藏资源和服务的使用，而不是隐藏用户的身份。

一些技术可用来实现不可观察性。提供不可观察性的技术例子有：

a) 影响不可观察性的信息分配：不可观察性相关的信息(如描述一个操作发生的信息)可分配在 TOE 内的几个地方。一种方法是该信息可分配到一个随机选择的 TOE 单个部分，这样攻击者不知道应攻击 TOE 的哪部分。另一种方法是系统将该信息分布在不同的部分，以至于没有哪个单一的 TOE 部分有足够的信息，从而避免用户的秘密遭到破坏。这一技术在 FPR _ UNO.2 中明确提出。

b) 广播：当广播信息时(如以太网、无线电)，用户不能确定谁真正接收和使用这些信息。当信息送达对此信息(如敏感的医学信息)感兴趣的接受者，而接受者又害怕受到耻辱时，这一技术特别有用。

c) 密码保护和消息填充：观察消息流的人可从消息被传送这一事实以及从该消息的属性中获得信息。通过通信量填充、消息填充以及加密消息流，可以保护消息的传送和它的属性。

有时，用户不应看到一个资源的使用情况，但是一个授权用户须被许可知道资源的使用情况，以便完成他的职责。在此情形，FRO _ UNO.4 可用来提供使一个或几个授权用户知道使用情况的能力。

本子类使用了概念“TOE 的部分”，它可以是物理上或是逻辑上与 TOE 的其他部分分离的 TOE 的任何部分。在逻辑分离的情况下与 FPT _ SEP 相关。

通信的不可观察性在许多领域中是重要的因素。例如执行宪法权限、组织策略或与防御相关的应用。

FPR _ UNO.1 不可观察性

用户应用注释

本组件要求功能和资源的使用不被未授权用户观察到。除了此组件外，PP/ST 作者还希望结合使用隐蔽信道分析。

操作

赋值：

FPR _ UNO.1.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体这样的角色，但 TSF 不仅必须防范每一单个用户或主体，而且也必须防范协作用户或主体。例如，用户集可以是一组用户，他们能在相同的角色下操作或都

能用相同的进程。

FPR_UNO.1.1 中，**PP/ST** 作者应标识操作列表，这些操作服从不可观察性要求。其他的用户/主体因而不能够观察到在规定的列表中覆盖客体的操作(如对该客体的读写)。

对 **FPR_UNO.1.1**，**PP/ST** 作者应标识出被不可观察性要求覆盖的客体的列表。一个例子可以是一个特定的邮件服务器或 **ftp** 站点。

对 **FPR_UNO.1.1**，**PP/ST** 作者应规定一组受保护的用户或主体，他们的不可观察性信息是受保护的。这样的例子可以是："通过 **Internet** 访问该系统的用户。"

FPR_UNO.2 影响不可观察性的信息的分配

用户应用注释

本组件要求功能或资源的使用不能被规定的用户或主体观察到。进一步讲，本组件规定与用户隐私有关的信息分布是在 **TOE** 内的，这样攻击者可能不知道将 **TOE** 的哪一部分作为攻击目标，或是他们需要攻击 **TOE** 的多个部分。

使用此组件的例子是使用一个随机分配的节点去提供一个功能。在这种情况下，本组件可能要求与隐私相关的信息不仅只会被一个确定的 **TOE** 部分获得，而且不会传播到 **TOE** 这部分之外。

一个更复杂的例子可以在某些"投票算法"中找到。在该服务中将牵涉到 **TOE** 的几个部分，但任何 **TOE** 的个别部分都不能违反该策略。所以一个人可以投票(或不投票)而无需 **TOE** 能确定是否一个选票已投，及该选票的投票结果是怎样的(除非该选票一致通过)。

除了本组件，**PP/ST** 作者还希望结合使用隐蔽信道分析。

操作

赋值：

FPR_UNO.2.1 中，**PP/ST** 作者应规定 **TSF** 必须提供保护以防范的用户或主体集。例如，即使 **PP/ST** 作者只规定了单个用户或主体这样的角色，但 **TSF** 不仅必须防范每一单个用户或主体，而且也必须防范协作用户或主体。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

FPR_UNO.2.1 中，**PP/ST** 作者应标识操作列表，这些操作服从不可观察性要求。其他的用户/主体因而不能够观察到在规定的列表中覆盖客体的操作(如对该客体的读写)。

对 **FPR_UNO.2.1**，**PP/ST** 作者应标识出被不可观察性要求覆盖的客体的列表。一个例子可以是一个特定的邮件服务器或 **ftp** 站点。

对 **FPR_UNO.2.1**，**PP/ST** 作者应规定一组受保护的用户或主体，他们的不可观察性信息是受保护的。这样的例子可以是："通过 **Internet** 访问该系统的用户。"

对 **FPR_UNO.2.2**，**PP/ST** 作者应标识哪些与隐私相关的信息以受控制的方式被发布。这些信息的例子可以是：主体的 **IP** 地址、客体的 **IP** 地址、时间、使用的密钥。

对 **FPR_UNO.2.2**，**PP/ST** 作者应规定信息分发应遵循的条件。这些条件应在每个实例的与隐私有关的信息的整个生命期内保持。这些条件的例子可以是："该信息只能出现在 **TOE** 的单个分离部分，且不能传送到 **TOE** 这部分之外"，"该信息仅驻留在一个单一的 **TOE** 分离部分，但可定期地移动到 **TOE** 的另一个部分"，"该信息在 **TOE** 的不同部分之间分布，使得对任意 5 个不同的 **TOE** 部分的损害将不会破坏安全策略。"

FPR_UNO.3 无征求信息的不可观察性

用户应用注释

本组件用来要求当提供特定的服务时，**TSF** 不试图获取会破坏不可观察性的信息。因此 **TSF** 不请

求(即试图从其他实体获得)能用来破坏不可观察性的任何信息。

操作

赋值:

在 **FPR _ UNO.3.1** 中,**PP/ST** 作者应标识服从不可观察性要求的服务列表,例如,“对作业描述的访问”。

对 **FPR _ UNO.3.1**,**PP/ST** 作者应在提供特定服务时,标识应防范的主体列表,以保护与隐私相关的信息。

在 **FPR _ UNO.3.1** 中,**PP/ST** 作者应规定受保护的隐私相关的信息,以防范特定主体。例如包括使用一个服务的主体身份以及已被使用的服务量,如内存资源的使用情况。

FPR _ UNO.4　授权用户可观察性

用户应用注释

本组件用来要求有一个或几个授权用户有权查看资源的使用情况。如果没有本组件,则该审查是允许的,但不是强制的。

操作

赋值:

FPR _ UNO.4.1 中,**PP/ST** 作者应规定授权用户集,**TSF** 须为它们提供观察资源使用情况的能力。例如,授权用户集可以是一组授权用户,他们能在相同的角色下操作或都能使用相同的进程。

FPR _ UNO.4.1 中,**PP/ST** 作者应规定授权用户能观察的资源或服务集。

附　录　J
(提示的附录)
TSF 保护(FPT)

本类包容了功能要求的子类,这些要求与提供 TSF(独立于特定 TSP)的机制的完整性和管理有关,并与 TSF 数据的完整性有关(独立于 TSP 数据的特定内容)。在某种意义上,本类中的子类可能出现与 FDP(用户数据保护)类中相同的组件,甚至可以用同一个机制来实现。然而,FDP 针对用户数据的保护,而 FPT 针对 TSF 数据的保护。事实上,为了提供 TOE 中的 SFP 不能被篡改或旁路这一要求,需要来自 FPT 类的组件。

从这个类的观点来看,有三个重要的部分组成 TSF:

a) TSF 的抽象机,它可以是虚拟的,也可以是物理机器,这取决于评估执行时特定的 TSF 实现。

b) TSF 的实现,在抽象机上执行并实现执行 TSP 的机制。

c) TSF 的数据,它是指导执行 TSP 的管理数据库。

所有 FPT 类中的子类都与这几个部份相关,并分属下面几个组:

a) FPT _ PHP(TSF 物理保护),它向授权用户提供检测对组成 TSF 的 TOE 各部分的外部攻击的能力。

b) FPT _ AMT(根本抽象机测试)和 FPT _ TST(TSF 自检),它们向授权用户提供这样的能力:验证根本抽象机和 TSF 的正确操作,以及 TSF 数据和可执行代码的完整性。

c) FPT _ SEP(域分离)和 FPT _ RVM(参照仲裁),它们在执行期间保护 TSF,而且确保 TSF 不能被旁路。当这些子类中的适当组件与 ADV _ INT(TSF 内部)的适当组件相组合时,TOE 即可具有传统上所说的“参照监视器”特性。

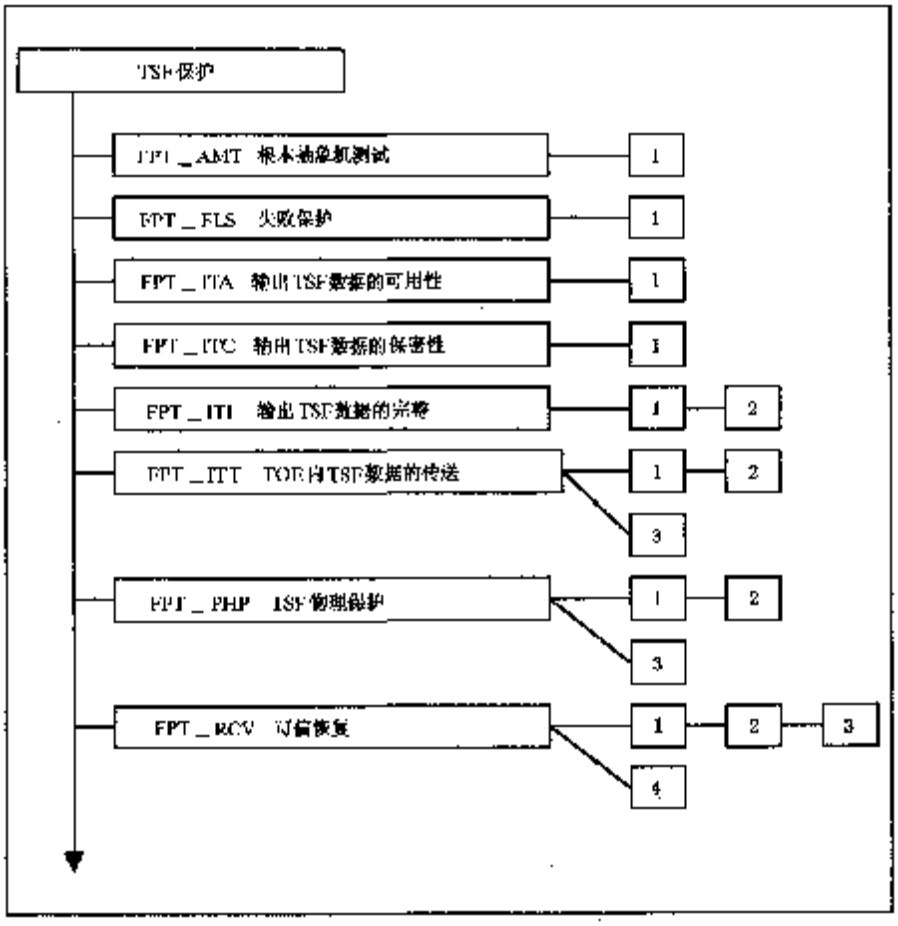


图 J1　TSF 保护类分解

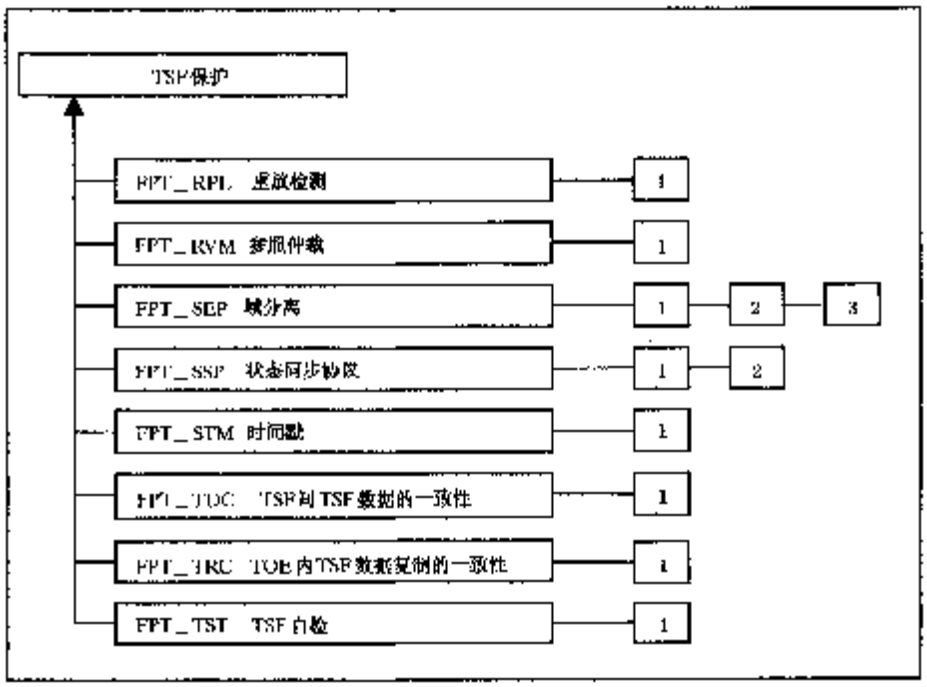


图 J2　TSF 保护类分解

d) FPT _ RCV（可信恢复）、FPT _ FLS（失败保护）和 FPT _ TRC（TOE 内 TSF 数据复制的一致性），它们处理失败发生时及紧接失败之后的 TSF 的行为。

e) FPT _ ITA（输出 TSF 数据的可用性）、FPT _ ITC（输出 TSF 数据的保密性）和 FPT _ ITI（输出 TSF 数据的完整性），它们处理 TSF 和远程可信 IT 产品之间的 TSF 数据的保护和可用性。

f) FPT _ ITT（TOE 内 TSF 数据的传送），当 TSF 数据在物理上分离的 TOE 部分间传送时，它处理 TSF 数据的保护。

g) FPT _ RPL（重放检测），它检测不同类型的信息或操作的重放。

h) FPT _ SSP（状态同步协议），依据 TSF 数据，它处理在一个分布的 TSF 的不同部分之间的状态同步。

i) FPT _ STM（时间戳），它处理可靠的计时。

j) FPT _ TDC（TSF 间 TSF 数据的一致性），它处理在 TSF 和远程可信 IT 产品之间共享的 TSF 数据的一致性。

J1 根本抽象机测试（FPT _ AMT）

本子类定义了对 TSF 安全假设的测试要求，它是对 TSF 所依赖的根本抽象机而言的。这个“抽象”的机器可以是一个硬件/固件平台，或是已知的且已评估的硬件/软件的组合，就如同一个虚拟机。这样测试的例子可以是测试硬件页面保护，也可以是通过网络发送样本包确认是否能收到或检验虚拟机接口的行为。这些测试可以在维护状态下、起动时、在线时或是连续不断地进行。TOE 根据测试结果采取的行动在 FPT _ RVC 中定义。

用户注释

术语“根本抽象机”通常是指实现 TSF 的硬件组件。然而，这短语也可用来指一个下层的、已经评估的硬件和软件组合构成的虚拟机，TSF 运行于其上。

抽象机测试有几种形式：

a) **上电测试**：这些测试确保根本平台能正确操作。对硬件和固件，它包括如下测试：内存条、数据路径、总线、控制逻辑、处理器寄存器、通信端口、控制台接口、话筒以及外围设备。对软件（虚拟机），包括检验初始化和运行是否正确。

b) **可加载测试**：这些测试可由授权用户加载和执行，或在特定条件下激活。可包括处理器部件强化测试（逻辑单元，计算单元等等）以及控制存储。

评估者注释

根本抽象机测试应足以测试 TSF 所依赖的根本抽象机的所有特征。

FPT _ AMT.1 抽象机测试

用户应用注释

本组件通过要求周期性地调用测试功能，支持周期性地测试 TSF 操作依赖的根本抽象机的安全假设。

PP/ST 作者应细化这一要求，以声明在离线、在线或维护模式下是否可以获得该功能。

评估者应用注释

仅在离线或维护模式下可以执行周期性测试这样一种功能是可以接受的。在维护期间对授权用户应适当地限制访问。

操作

选择：

在 FPT _ AMT.1.1 中，PP/ST 作者应规定什么时候 TSF 要执行抽象机测试，如在初始化启动期间、正常运转时周期性地、授权用户提出请求时或在其他条件下。在最后一种情况下，PP/ST 作者应细化这些条件是什么。通过这种选择，PP/ST 作者能指出自检运行的频率。如果测试经常运行，则比起该测试不那么频繁地运行而言，终端用户会对该 TOE 正在正常运转更有信心。然而，对 TOE 正在正常运转这一信心的需求须同对 TOE 可用性的潜在影响相平衡，通常，自检会延迟 TOE 的正运转。

J2 失败保护(FPT _ FLS)

本子类的要求确保在 TSF 中发生某些类型的失败事件时 TOE 不会违背它的 TSP。

FPT _ FLS.1 带保存安全状态的失败

用户应用注释

术语“安全状态”指示一个状态，在这状态中 TSF 数据是一致的，而且 TSF 继续正确执行 TSP。“安全状态”定义在 TSP 模型中。如果开发者提供安全状态的明确定义和认为它是安全的理由，则可忽略 FPT _ FLS.1 对 ADV _ SPM.1 的依赖性。

虽然希望审计带保存安全状态的失败，但是不可能在所有的情况下都能审计。PP/ST 作者应规定希望审计并可执行审计的那些情形。

在 TSF 中的失败可能包括“硬”失败，它指示一个设备发生故障且需要维护、服务或修理 TSF。TSF 中的失败也可能包括可恢复的“软”失败，它仅要求初始化或重新设置 TSF。

操作

赋值：

对 FPT _ FLS.1.1，PP/ST 作者应列出 TSF 中失败的类型，对此故障 TSF 应是“失败保护”，也就是说，应保持一个安全的状态，且继续正确执行 TSP。

J3 输出 TSF 数据的可用性(FPT _ ITA)

本子类定义了防止丧失在 TSF 和远程可信任 IT 产品之间传送的 TSF 数据的可用性的有关规则。这些数据可能是 TSF 关键的数据，如口令、密钥、审计数据或 TSF 可执行代码。

用户应用注释

本子类被应用于分布式的系统背景中，其中 TSF 向远程可信 IT 产品提供 TSF 数据。该 TSF 只能在本端上采取措施，而不对其他可信 IT 产品的 TSF 负责。

如果对不同类型的 TSF 数据有不同的可用性量度的话，那么对于每种量度和 TSF 数据类型的配对都要重复这一组件。

FPT _ ITA.1 在所定义可用性量度范围内的 TSF 间的可用性

操作

赋值：

对 FPT _ ITA.1.1，PP/ST 作者应规定服从可用性量度的 TSF 数据的类型。

对 FPT _ ITA.1.1，PP/ST 应为可用的 TSF 数据规定可用性量度。

对 FPT _ ITA.1.1，PP/ST 作者应规定必须确保可用性的那些条件。例如：在 TOE 和远程可信任 IT 产品之间必须有一个连接。

J4 输出 TSF 数据的保密性(FPT _ ITC)

本子类定义了在TSF 和远程可信任IT 产品之间传送TSF 数据时防止未授权泄露的规则。例如这些数据可能是TSF 关键的数据,如口令、密钥、审计数据或TSF 可执行代码。

用户应用注释

本子类被应用于分布式的系统背景中,其中TSF 向远程可信任IT 产品提供TSF 数据。该TSF 只能在本端上采取措施,而不对其他可信IT 产品的行为负责。

FPT _ ITC.1 传送过程中 TSF 间的保密性

评估者应用注释

在传送过程中TSF 数据的保密性是必需防止这些信息被泄露。提供保密性的一些可能的措施包括使用加密算法和现行的系列技术。

J5 输出 TSF 数据的完整性(FPT _ ITI)

本子类定义了有关的保护规则,即在TSF 和远程可信IT 产品之间传送TSF 数据过程中,防止数据被未授权修改。这些数据有可能是TSF 的关键数据如口令、密钥、审计数据或是TSF 可执行代码。

用户注释

本子类用于分布式的系统背景中,在此背景中TSF 和远程可信IT 产品之间交换TSF 数据。注意不能规定在远程可信IT 产品上处理修改、检测和恢复的要求,因为不能事先确定远程可信IT 产品将用什么样的机制来保护它的数据。由于这一原因,这些要求被表述为"TSF 提供的一种能力",这种能力是远程可信IT 产品也能使用的。

FPT _ ITI.1 TSF 间修改的检测

用户应用注释

这一组件应被用于那些足以检测到数据何时被修改的场合。例如以下场合:当修改被检测到时,远程可信IT 产品可以要求TOE 的TSF 重新传送数据,或对这种类型的请求进行应答。

所需修改检测的强度基于一个规定的修改量度,它是所用算法的一个函数,其范围可从无法检测多个位更改的一个弱校验和与奇偶性机制,到更复杂的密码校检和方法。

操作

赋值:

对FPT _ ITI.1.1,PP/ST 应规定检测机制必须满足的修改量度。这一修改量度将规定所要求的修改检测的强度。

对FPT _ ITI.1.2,PP/ST 应规定检测到对TSF 数据的修改时应采取的行动。这样一个行动的例子就是"忽略TSF 数据,要求原发可信产品再次发送这些TSF 数据。"

FPT _ ITI.2 TSF 间修改的检测与改正

用户应用注释

这一组件应被用于有必要检测或改正对TSF 关键数据修改的场合。

所需的修改检测的强度基于一个规定的修改量度,它是所用算法的一个函数,其范围可从无法检测多个位更改的一个弱校验和与奇偶性机制,到更复杂的密码校检和方法。需被定义的量度既可参考它将

要抵御的攻击(如,仅在千分之一的概率下信息会被接受),也可以参考被公众所熟知的一些机制(如,这一强度必须与由安全散列算法提供的强度一致)。

改正修改采用的方法可以通过某种差错纠正校验和的形式来完成。

评估者注释

满足这一要求的某些方法可能包括使用密码功能或某种校验和的形式。

操作

赋值:

对 FPT _ITI.2.1,PP/ST 应规定检测机制必须满足的修改量度。这一修改量度将规定所要求的修改检测的强度。

对 FPT _ITI.2.2,PP/ST 应规定检测到对 TSF 数据的修改时应采取的行动。这样一个行动的例子就是“忽略 TSF 数据,要求原发可信产品再次发送这些 TSF 数据。”

对 FPT _ITI.2.3,PP/ST 作者应定义修改的类型,TSF 应能从这些修改中恢复。

J6 TOE 内 TSF 数据的传送(FPT _ITT)

本子类提供了通过内部信道在 TOE 的不同部分间传送 TSF 数据时,对这些数据进行保护的要求。

用户注释

如何确定分离程度(如物理的或逻辑的分离),以使本子类应用有用,这取决于所要使用的环境。在恶意环境中,如果仅通过一条系统总线或进程间通信信道来在分离的各个 TOE 部件间进行传送可能会由此产生一些风险。在比较良好的环境里,这一传送可通过更传统的网络媒体来完成。

评估者注释

一个适用于 TSF 的能提供这一保护的且实际可行的机制是建立在密码基础上的。

FPT _ITT.1 内部 TSF 数据传送的基本保护

操作

选择:

在 FPT _ITT.1.1 中,PP/ST 作者应规定希望提供的保护类型:是防止泄露的还是防止修改的。

FPT _ITT.2 TSF 数据传送的分离

用户应用注释

在 SFP 相关属性基础上获得 TSF 数据分离的方法之一,是通过使用分离的逻辑或物理信道。

操作

选择:

在 FPT _ITT.1.2 中,PP/ST 作者应规定希望提供的保护类型:是防止泄露的还是防止修改的。

FPT _ITT.3 TSF 数据完整性监视

操作

选择：

在 FPT _ ITT3.1 中，PP/ST 作者应规定 TSF 所能检测到的修改类型。PP/ST 作者应从以下类型中进行选择：数据修改、数据替换、数据重排、数据删除或任何其他完整性差错。

赋值：

在 FPT _ ITT3.1 中，如果 PP/ST 作者选择了上面段落中的最后一种选项，那么该作者同时也应该明确规定 TSF 有能力检测到的那些其他完整性差错。

在 FPT _ ITT3.2 中，PP/ST 作者应规定在确定出现了一个完整性差错时应采取的行动。

J7 TSF 物理保护(FPT _ PHP)

TSF 物理保护组件涉及对 TSF 进行未授权的物理访问的限制，以及阻止和抵制对 TSF 进行未授权的修改和替代。

本子类中的要求确保了 TSF 是被保护的，以防物理上的篡改和干扰。满足这些组件的要求将会使 TSF 在打包后以如下方式使用：物理篡改是可检测的，或基于既定工作因素对物理篡改的防御是可测的。没有这些组件，在物理破坏不能被阻止的环境下，TSF 的保护功能就失去了有效性。这一组件同时也提供了有关 TSF 必须如何对企图物理篡改的尝试作出反应的要求。

有关物理篡改情形的例子包括机械攻击、辐射、改变温度。

用户注释

对授权用户来讲，仅在离线或维护状态下才能检测到物理篡改这种功能是可接受的。在这些状态下，对授权用户应加以控制以限制访问。由于在这些状态下 TSF 可能是非“操作性”的，它也许不能为授权用户访问提供正常的执行。TOE 物理实现可能由几个结构组成：例如外部屏蔽、卡和芯片。这一组“元件”作为一个整体必须保护(保护、报告和抵抗)TSF 免受物理篡改。这并不意味着所有的设备都必须提供这些特征，不过作为一个完整的物理构造总体上应具备上述特征。

只有最小级审计与这些组件有关，这完全是因为在与审计子系统交互层下，存在完全以硬件实现检测和预警机制的可能(例如，一个基于硬件的检测系统，如果授权用户按下一个按钮时电路断开，该系统就中断电路和点亮发光二级管(LED))。不过，PP/ST 作者可决定对一个特定可预料的威胁环境下，是否需要审计物理篡改，如果需要，PP/ST 作者应在审计事件列表中包括合适的要求。注意加入这些要求可能会对硬件设计和它的软件接口产生影响。

FPT _ PHP.1 物理攻击的被动检测

用户应用注释

FPT _ PHP.1 应在程序化方法不能对抗对 TOE 部件进行的未授权的物理篡改威胁时使用。它处理对 TSF 的不可检测的物理篡改的威胁。授权用户通常应被赋予审计篡改是否发生的能力。如上所述，这一组件仅提供 TSF 检测篡改能力。要求建立对 FMT _ MOF.1 的依赖关系以规定谁可以使用这一功能及如何使用这一功能。如果这一功能由非 IT 机制(如物理检查)来实现，那么可以证明对 FMT _ MOF.1 的依赖关系是不能成立的。

FPT _ PHP.2 物理攻击的报告

用户应用注释

PT _ PHP.2 应在程序化方法不能对抗对 TOE 部件进行的未授权的物理篡改威胁时使用，它要求指定个体能得到有关物理篡改的通知。它处理尽管被检测到但可能不被报告的对 TSF 元件的物理篡改的威胁。

操作

赋值：

对 FPT _ PHP.2.3,PP/ST 作者应提供要求主动检测物理篡改的 TSF 设备/元件的列表。

对 FPT _ PHP.2.3,PP/ST 作者应指定在检测到篡改时应得到通知的用户或角色。用户或角色的类型可以根据 PP/ST 中包括的特定安全管理组件(来自 FMT _ MOF.1 子类中)而改变。

FPT _ PHP.3　物理攻击抵抗

对某些形式的威胁,TSF 不仅有必要监测到它们,更要真正地抵抗或延迟这些攻击者。用户应用注释

当希望 TSF 设备或 TSF 元件在其内部有物理篡改(如观察、分析或修改)威胁的环境下执行操作时,应使用本组件。

操作

赋值：

对 FPT _ PHP.3.1,PP/ST 应对 TSF 应抵抗物理篡改的 TSF 设备/元件的列表规定篡改情况。这一列表可能会被用于一个已被定义好的 TSF 物理设备或元件的子集,此子集的考虑基于技术限制和相关设备的物理泄露。应明确定义和证明这些子集。另外,TSF 应能自动响应物理篡改。此自动响应应是使设备受到保护的策略。例如,根据保密性策略,物理上“禁用”该设备以使被保护信息不能被检索是可接受的。

对 FPT _ PHP.3.1,PP/ST 作者应规定 TSF 设备/元件列表,TSF 应在已识别的情况下为其抵抗物理篡改。

J8　可信恢复(FPT _ RCV)

本子类的要求确保 TSF 可以决定 TOE 无须减弱保护即可启动,及在中断运行后无须减弱保护即可恢复。本子类很重要,因为 TSF 的启动状态决定了对后续状态的保护。

作为对发生的预期失败、中断运行或启动的直接响应,恢复组件重建 TSF 安全状态,或是阻止转变到不安全状态。一般必须预测的失败包括：

a) 总是导致系统崩溃的不可抵抗的失败 (如关键的系统表总是不一致,由瞬间的硬件或固件故障、电力中断、处理器故障、通信中断引起的 TSF 编码内非受控的传送)；

b) 导致代表 TSF 客体的媒体部分或全部不可访问或崩溃的媒体故障(如奇偶错误、磁盘头损坏、由磁盘头引起的持续读写失败、磁涂层损坏、磁盘表面的灰尘)；

c) 由错误的管理行为或缺乏及时的管理行为造成的操作间断(如不可预知的关掉电闸、没有注意到关键的资源已被用尽、系统安装的配置不适当)。

注意此恢复可以是整个或部分失败情形的恢复。整个的失败可能发生在一个单一操作系统,它不太可能发生在分布式的环境下。在分布式环境下,子系统可能失效,但其他部分仍能工作。另外,关键的组件可以冗余(磁盘镜像、可选路由),并且可能有检查点。因此,恢复是指恢复到安全状态。

本子类识别了一个维护模式。在这个维护模式中,正常的操作可能是不能进行的或被严格限制的,否则其他的不安全的情况可能发生。通常应只允许授权的用户使用这一模式,但究竟谁能使用这一模式的真正详情是 FMT 类安全管理的一个功能。如果 FMT 对谁能使用这一模式没进行控制,那么若 TOE 进入这种状态,则允许任何用户恢复系统是可接受的。但实际上,由于恢复系统的用户有机会以违反 TSP 的方式配置 TOE,因此可能并不希望这样。

用于检测操作中的异常情况的机制归到 FPT _ TST(TST 自检)、FPT _ TLS(失败保护)和涉及“软件安全”概念的其他领域。

用户注释

在本子类中使用“安全状态”一词。它指的是TOE具有一致的TSF数据及能正确地执行这个策略的TSF的一些状态。这些状态可能是一个干净系统的初始化“根”,或者是某个通过检查点检查的状态。“安全状态”在TSP模型中定义。如果开发者提供一个安全状态的清晰定义,及它之所以被认为安全的原因,则FPT_RCV中的每个组件对ADN_SPM.1的依赖性可忽略。

FPT_RCV.1 手工恢复

在可信恢复子类的层次上,最不希望的是只要求手工干涉的恢复,因为它排除了在无人维护的方式下使用系统。

用户应用注释

本组件在TOE不要求自动恢复到安全状态时使用。这一组件的要求降低了源于新增TOE在从一个失败或其他中断恢复后重又返回不安全状态时对保护泄露的威胁。

评估者应用注释

授权用户可用的可信恢复功能仅在一个维护模式下可用是可接受的。对授权用户在维护模式下的访问应加以限制。

FPT_RCV.2 自动恢复

由于自动恢复允许机器以无人干涉的方式进行操作,所以普遍认为自动恢复比手工恢复更有用。

用户应用注释

通过要求在失败或服务中断后至少有一种自动恢复的方法,组件FPT_RCV.2扩展了FPT_RCB.1涉及的特征范围。它解决了源于无人干涉的TOE在从失败或其他中断状态恢复后重新回到不安全状态时对保护泄露的威胁。

评估者应用注释

授权用户可用的可信恢复功能仅在一个维护模式下可用是可接受的。对授权用户在维护模式下的访问应加以限制。

对FPT_RCV2.1,TSF开发者有责任决定可恢复的失败或服务中断的集合。

假定自动恢复机制的牢固性得到了验证。

操作

赋值:

对FPT_RCV.2.2,PP/ST作者应规定可能自动恢复的失败或其他中断的列表。

FPT_RCV.3 无过度损失的自动恢复

自动恢复被认为比手工恢复更为有用,但它要冒有可能损失相当数量客体的风险。防止客体的过度损失为恢复工作提供额外的用途。

用户应用注释

通过要求在TSC中没有TSF数据或客体的过度损失,组件FPT_RCV.3扩展了FPT_RCV.2的特性覆盖面。在FPT_RCV.2中,自动恢复机制可通过删除所有客体并将TSF返回到一个已知的安全状态来进行恢复。这种极端的自动恢复形式被排除在FPT_RCV.3之外。

本组件解决了无人干涉的TOE在失败或其他中断发生后在TSC内损失了大量TSF数据或客体返回到一个不安全状态时对保护泄露的威胁。

评估者应用注释

授权用户可用的可信恢复功能仅在一个维护模式下可用是可接受的。对授权用户在维护模式下的访问应加以限制。

假定评估者将验证自动恢复机制的牢固性。

操作

赋值：

对FPT _RCV.3.2,PP/ST作者应规定可能自动恢复的失败或其他中断情况的列表。

对FPT _RCV.3.3,PP/ST作者应量化可接受的TSF数据或客体的损失数量。

FPT _RCV.4　功能恢复

功能恢复要求如果TSF发生了某个失败,TSF中的某一SF要么能成功地完成,要么恢复到一个安全的状态。

操作

赋值：

对FPT _RCV.4.1,PP/ST作者应规定SF和失败情况的列表。任何一种已被标识的失败情况发生时,已被规定的SF必须要么能成功地完成,要么恢复到一个安全状态。

J9　重放检测(FPT _RPL)

本子类解决对不同类型实体的重放的检测及随后的改正行为。

FPT _RPL.1　重放检测

用户应用注释

此处包括的实体的例子有:消息、服务请求、服务响应或是会话。

操作

赋值：

FPT _RPL1.1中,PP/ST作者应提供能进行重放检测的已标识实体的列表。这些实体的例子可能包括：消息、服务请求、服务响应和用户会话。

FPT _RPL1.2中,PP/ST作者应规定当检测到重放时TSF应采取的行动的列表。潜在的行动可能包括：忽略被重放的实体,请求从标识的源进行的实体确认,并终止重放实体的原发主体。

J10　参照仲裁(FPT _RVM)

本子类中的组件解决了一个传统的参照监视器的“一直运行”方面。相对于TSC来说,这些组件的目的是:当主体对于由SFP控制的客体在部分或全部SFP方面是不可信时,确保这些不可信主体调用执行策略的所有活动由TSF通过SFP来比较证实是有效的。如果实施SFP的TSF的这一部分也满足FPT _SEP(域分离)和ADV _INT(TSF内部)中适当组件的要求,那么TSF的这部分为该SFP提供了一个“参照监视器”。

参照监视器是TSF负责执行TSP的那个部分;它有以下三个特征:

a) 不可信主体不能干涉它的操作,即它是防篡改保护的。这由FPT_SEP子类中的组件来解决。

b) 不可信主体不能旁路它的检查,即它是一直运行的。这由FPT_RVM子类的组件来解决。

c) 它足够简单,易于分析且行为易懂(如它的设计概念十分简单)。这由ADV_INT子类中的组件来解决。

这一组件指出:"TSF将确保执行TSP的功能,在TSC中的每一个功能被允许继续进行之前,被调用并执行"。在任何系统(分布式或其他系统)中,都只有有限的功能对TSP的执行负责。这一要求中没有任何有关强制或规定调用单个功能以处理安全的内容。相反,它允许参照监视器角色有多个功能,这些对TSP负责的功能合在一起就被称作参照监视器。另外,它必须与保持参照监视器的简单性目的相平衡。

实现SFP的一个TSF提供有效的保护以对抗未授权功能,当且仅当相对于任何或全部SFP不可信主体所请求的可实施的行动(例如对客体的访问)都在完成之前被TSF验证。如果这个可实施的行动被不正确地执行或旁路的话,则全部的SFP执行操作已遭致损害。这样"不可信"主体就能以各种不同的未被授权的方法旁路此SFP(如设法避开对一些主体或客体的访问检查、旁路对已实施应用保护的客体的检查、保留超过有效期限的访问权利、旁路对被审计活动的审计或旁路鉴别)。注意术语"不可信主体"指的是相对任一或全部正被执行的特定SFP的不可信的主体;一个主体可能对于一个SFP是可信的,而对于另一个不同的SFP是不可信的。

FRT_RVM.1 TSP的不可旁路性

用户应用注释

为了获得等同的参照监视器,这一组件必须与FPT_SEP.2(SFP域分离)或FPT_SEP.3(完全的参照监视器)或ADV_INT.3(复杂性最小化)一起使用。进一步,如果要求有完全的参照仲裁的话,那么FDP类的用户数据保护组件必须覆盖所有的客体。

J11 域分离(FPT_SEP)

本子类的组件确保TSF自己的执行时至少有一个安全域可用,并保护该TSF不被不可信主体从外部干扰篡改(如修改TSF编码或数据结构)。满足本子类要求的TSF具有自我保护能力,即不可信主体将不能修改或破坏该TSF。

本子类的要求如下:

a) 将TSF的安全域("保护域")的资源和该域外的主体及不受约束的实体分离开,使得保护域外的实体不能观察或修改保护域内的TSF数据或TSF编码。

b) 域间的传送是受控的,不能随意地进入保护域或随意从保护域返回。

c) 通过其地址传到保护域的用户或应用参数,受保护域地址空间的确认,而通过其值传到保护域的那些用户或应用参数则受该保护域所期望的值的确认。

d) 除了通过TSF控制的共享部分外,主体的安全域是不同的。

用户注释

只要要求相信TSF还没被破坏,就需要本子类。

为了获得等同的参照监视器,本子类内的组件FPT_SEP.2(SFP域分离)、或FPT_SEP.3(完全的参照监视器)必须与FPT_RVM.1(TSP的不可旁路性)和ADV_INT.3(复杂性最小化)联合使用。进一步,如果要求有完整的参照仲裁的话,那么FDP类的用户数据保护组件必须覆盖所有的客体。

EPT _SEP.1 TSF 域分离

如果 TSF 没有独立的受保护的域，就不能保证 TSF 不受到不可信主体的篡改攻击。这些攻击可能涉及到修改 TSF 代码或 TSF 数据结构。

FPT _SEP.2 SFP 域分离

TSF 提供的最重要的功能在于执行 SFP。为了简化设计和增加那些有意义的 SFP 展现的参照监视器(RM)的属性的可能性，特别是防篡改保护，它们必须处在与 TSF 的其他部分所不同的域中。

评估者应用注释

按层次设计的参照监视器可能提供超出 SFP 的功能，这是层次化软件设计所致。目标应是使与 SFP 不相关的功能最小化。

注意，对参照监视器来说，所有包含的 SFP 在一个单独的独立参照监视器域内和有多个参照监视器域(每一个执行一个或多个 SFP 就有一个域)都是可接受的。如果存在 SFP 的多参照监视器域的话，则他们之间是对等的或是存在层次关系都是可接受的。

对 FPT _SEP.2，“TSF 未隔离部分”指的是 TSF 中没有被 FPT _SEP.3.2 覆盖的那些功能组成的 TSF 部分。

操作

赋值：

对 FPT _SEP.2.3，PP/ST 作者应规定 TSP 中需要有一个分离域的访问控制或信息流控制 SFP。

FPT _SEP.3 完全的参照监视器

TSF 提供的最重要的功能是执行 SFP。这一组件构建在前一个组件的意图的基础上，这是通过要求所有的访问控制或信息流控制 FSP 必须在一个与 TSF 其他的域相异的域内实现的，这进一步简化了设计，并增加了在 TSF 内发现参照监视器(RM)特性(特别是篡改保护)的可能性。

评估者应用注释

按层次设计的参照监视器可能提供超出 SFP 的功能，这是层次化软件设计所致。目标应是使与 SFP 不相关的功能最小化。

注意，对参照监视器来说，所有包含的 SFP 在一个单独的独立参照监视器域内和有多个参照监视器域(每一个执行一个或多个 SFP 就有一个域)都是可接受的。如果存在 SFP 的多参照监视器域的话，则他们之间是对等的或是存在层次关系都是可接受的。

J12 状态同步协议(FPT _SSP)

分布式系统因为系统不同部分之间潜在的状态差别和通信延迟，可能会比单一系统引起更多的复杂性。在大多数场合下，分布式功能之间的状态同步涉及一个交换协议，而不只是一个简单的行动。当在这些协议的分布式环境中存在恶意时，则要求更为复杂的防御协议。

FPT _SSP 为 TSF 特定的关键安全功能使用可信任协议提出了要求。FPT _SSP 确保在一个与安全有关的活动之后，TOE 的两个分布式的部分(如主机)已使他们的状态同步。

用户注释

有些状态可能永远不能被同步，或实际使用所需代价太高。加密密钥撤消就是一个例子。撤消活动

被初始化后的状态可能永远是不可知的:或者是采取了活动且回执不能发出,或者是敌意的通信方忽略了这一信息且永远不执行撤消。不确定性是分布式系统所特有的,不确定性和状态同步是相关的,可使用相同的解决方案。不确定的状态不能通过设计来解决,PP/ST 作者应针对此情况指出其他要求(如发出警报、审计事件)。

FPT _SSP.1 简单的可信回执

用户应用注释

本组件要求 TSF 必需在收到请求时为 TSF 的其他部分提供回执。这一回执应表明分布式 TOE 的一部分成功地接收到了来自分布式 TOE 其他不同部分的未被修改的传送。

FPT _SSP.2 相互的可信回执

用户应用注释

本组件要求 TSF 除了能对收到一个数据传送提供回执外,还必须遵守其他 TSF 部分对该回执给出回执的请求。

例如,本地 TSF 发送一些数据到 TSF 远程部分。TSF 远程部分给出成功地收到了该数据的回执,并请求 TSF 发送方证实它已收到这一回执。这一机制对此数据在传送过程中所涉的 TSF 双方都知道已成功地完成了传送提供了进一步的信任。

J13 时间戳(FPT _STM)

本子类解决 TOE 中一个可靠的时间戳功能的要求。

用户注释

PP/ST 作者有责任明确解释“可靠的时间戳”的含义,并指出确定可信接受的责任在何处。

FPT _SMT.1 可靠的时间戳

用户应用注释

可能用到这一组件的情况包括为审计目的和安全属性到期提供可靠的时间戳。

J14 TSF 间 TSF 数据的一致性(FPT _TDC)

在分布式或复合系统环境下,TOE 或许需要与其他可信 IT 产品交换 TSF 数据(如与数据有关的 SFP 属性、审计信息、标识信息等等)。本子类定义了一些要求,这些要求是关于 TOE 的 TSF 及不同的可信 IT 产品间共享这些属性并对其作出一致性解释。

用户注释

本子类中的这一组件预期用于提供当数据在 TOE 的 TSF 和另一个可信 IT 产品的 TSF 之间传送的时候,自动支持 TSF 数据一致性的要求。也有可能用完全程序化的方法来保证安全属性的一致性,但它们不在这里提供。

本子类不同于 FDP _ETC 和 FDP _ITC,因为那两个子类只涉及解决 TSF 和它的输入/输出媒体之间的安全属性。

如果关心 TSF 数据的完整性,应从 FPT _ITI 子类中选择要求。这些组件规定了 TSF 能检测或检测并改正传送中的 TSF 数据改动的要求。

FPT _TDC.1 TSF 间基本 TSF 数据的一致性

用户应用注释

TSF 负责指定功能保持TSF 数据的一致性，它们是两个或多个可信系统之间所共有的。例如，两个不同系统的TSF 数据可能有不同的内部约定。为了使可信 IT 产品的接收方能正确使用 TSF 数据(例如对用户数据提供像在 TOE 内部一样的保护)，TOE 和其他可信 IT 产品必须使用一个预先建立的协议来交换 TSF 数据。

操作

赋值：

在 FPT _ TDC.1.1 中，PP/ST 作者应定义一个 TSF 数据类型列表，从而当在 TSF 和其他可信 IT 产品间共享 TSF 数据时，TSF 将提供一致地解释它们的能力。

在 FPT _ TDC.1.2 中，PP/ST 应规定将要由 TSF 使用的解释规则。

J15 TOE 内 TSF 数据复制的一致性(FPT _ TRC)

本子类的要求用以确保在TOE 内部复制TSF 数据的一致性。当TOE 的内部不同部分间的信道不能工作时，这些 TSF 数据就可能不一致，如果 TOE 内部被构造成网络，而一部分网络连接又断掉了，则当那些部分失去正常工作能力时，就会发生这种不一致的情况。

用户注释

确保一致性的方法未在这一组件中规定。此方法可通过某种处理记录得到(在重新连接时上适当的处理记录被“反转”到某一点)，通过同步协议此方法可更新被复制的数据。如果 PP/ST 需要特定的协议，它可以通过细化来指定。

某些状态是不太可能同步的，或同步的开销太大。例如通信信道和加密密钥的撤销。不确定状态也可能发生；如果期望某个特定的行为，应通过细化来规定。

FPT _ TRC.1 内部 TSF 的一致性

操作

赋值：

在 FPT _ TRC.1.2 中，PP/ST 作者应规定依赖于 TSF 数据复制一致性的 SF 的列表。

J16 TSF 自检(FPT _ TST)

本子类定义了一些关于 TSF 自检的要求，这些检测与期待的正确操作有关，如执行功能的接口和 TOE 关键部分的抽样算术运算。这些检测可在启动时进行，或周期性地进行，或应授权用户的请求进行，或满足其他条件时进行。TOE 根据自检结果所采取的行动在其他子类中定义。

本子类要求也用于检测由多种失败造成的 TSF 可执行码(如 TSF 软件)和 TSF 数据腐败，这些失败并不需要 TOE 停止工作(这将由别的子类处理)。因为这些失败不可避免，故必须执行这些检查。这些失败可能是由不可预见的失败方式或硬件、固件、软件设计的某些忽略所造成，或由于逻辑的或物理保护的不适当导致 TSF 恶意腐败所造成。

另外，在合适的条件下，作为维护活动的结果，使用这一组件可帮助防止不合适的或有害的 TSF 更改被应用到运行中的 TOE 上。

用户注释

“TSF 正确操作”主要是指 TSF 软件的运行和 TSF 数据的完整性。实现 TSF 软件的抽象机是通过

对 FPT _ AMT 的依赖关系来检测的。

FPT _ TST.1　TSF 检测

用户应用注释

这一组件通过要求调用检测功能和检查 TSF 数据和可执行代码的完整性的能力，对 TSF 操作的关键功能的检测提供支持。

评估者应用注释

授权用户有效的周期性的检测功能仅在离线或维护模式下进行是可接受的。在这些模式下，对授权用户的访问应加以限制。

操作

选择：

在 FPT _ TST.1.1 中，PP/ST 作者应规定何时 TSF 将执行 TSF 检测：在初始启动中进行，在正常运行过程中周期性地进行，在授权用户提出这样的要求时进行，或在其他条件下执行。在最后一种选择的情况下，PP/ST 作者还应通过下面的赋值规定这些条件是什么。

赋值：

在 FPT _ TST.1.1 中，如果选择了最后一种情况，PP/ST 作者应规定应进行自检的条件。

附　录　K
（提示的附录）
资源利用（FRU）

本类提供三个子类支持所需资源的诸如处理能力或存储能力。容错子类提供保护以防止由 TOE 失败引起的上述资源不可用。服务优先级子类确保资源将被分配到更重要的和时间要求更苛刻的任务中，而且不能被优先级低的任务所独占。资源分配子类提供可用资源的使用限制，从而防止用户独占资源。

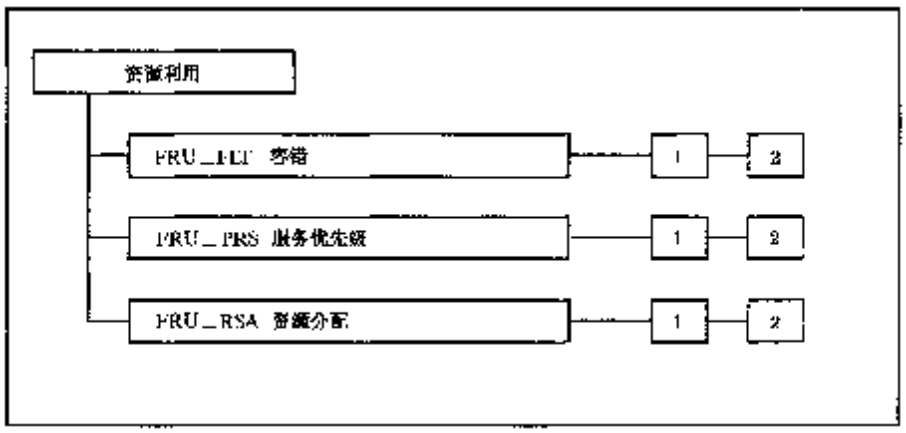


图 K1　资源利用类分解

K1　容错（FRU _ FLT）

本子类提供即使在发生故障时能力的可用性的要求。故障的例子有电力中断、硬件故障、软件错误。

发生这些差错时，如果按本子类规定，TOE 将维护规定的能力。例如，PP/ST 作者可能规定，在电力中断或通信中断时，一个核电站所使用的 TOE 将继续执行关闭程序的操作。

用户注释

在执行 TSP 的情况下，由于 TOE 只能继续它的正确操作，这样就要求系统必须在故障发生后保持一个安全状态。这种能力由 FPT _ FLS.1 提供。

提供的容错机制分为主动和被动两种。在主动的机制下，特定的功能在发生差错时将会被激活。例如，火警就是一种主动机制：TSF 检测到火情并能采取措施，如将操作切换到备份。在被动的机制下，TOE 的构造使其能处理差错。例如，使用多处理器的多数表决系统就是一个被动的解决方案，这样其中一个处理器故障并不会扰乱整个 TOE 的运行(尽管它需要检测以便允许更正)

对于本子类，故障的发生是偶然的(如进水或错拨设备)还是有意的(如独占)并不重要。

FRU _ FLT.1　低容错

用户应用注释

本组件规定在系统发生故障之后 TOE 仍将提供的能力。由于描述所有的具体的故障很困难，但可以规定故障的类别。一般故障的例子有计算机房进水、电力短时间中断、CPU 或主机的崩溃、软件错误或缓冲区溢出等。

操作

赋值：

在 FRU _ FLT.1.1 中，PP/ST 作者应规定在某个特定的故障发生期间或之后 TOE 将保持的能力的列表。

在 FRU _ FLT.1.1 中，PP/ST 作者应规定一个故障类型列表，对 TOE 必须加以明确保护以对抗这些故障。如果列表中的一种故障发生，TOE 仍能继续运行。

FRU _ FLT.2　受限容错

用户应用注释

本组件规定在系统发生故障之后 TOE 仍将提供的能力。由于描述所有的具体的故障很困难，但可以规定故障的类别。一般故障的例子有计算机房进水、电力短时间中断、CPU 或主机的崩溃、软件错误或缓冲区溢出等。

操作

赋值：

在 FRU _ FLT.2.1 中，PP/ST 作者应规定一个故障类型列表，对 TOE 必须加以明确保护以对抗这些故障。如果列表中的一种故障发生，TOE 仍能继续运行。

K2　服务优先级(FRU _ PRS)

本子类的要求允许 TSF 控制用户和主体对 TSC 资源的使用，使得 TSC 内高优先级任务的完成总是不受低优先级的务造成的过分干扰或延迟影响。换句话说，关键时间的任务不会被非关键时间的任务延迟。

本子类可被应用到几种不同类型的资源中，如处理能力、通信信道能力。

服务优先的机制可以是被动的，也可以是主动的。在一个被动的服务优先系统中，对两个等待中的应用作选择时，系统会选择具有最高优先级的任务。在使用被动优先服务机制时，当一个低优先级的任

务运行时，它不能被另一个高优先级的任务中断。而当使用主动服务优先机制时，低优先级的任务则有可能被新的高优先级的任务中断。

用户注释

审计要求表明所有拒绝的原因都应被审计。有关一个操作不被拒绝而是延缓执行的问题将留给开发者去考虑。

FRU _PRS.1 有限服务优先级

用户应用注释

这一组件定义一个主体的优先级，并指出了对何种资源将使用这一优先级。如果一个主体打算对由服务优先级控制的资源采取行动，那么其访问或访问时间将取决于该主体的优先级、当前活动的主体的优先级和仍在队列中的主体的优先级。

操作

赋值：

在 FRU _PRS.1.2 中，PP/ST 作者应规定 TSF 为之实施服务优先级的受控资源列表（诸如进程、磁盘空间、内存、带宽等资源）。

FRU _PRS.2 全部服务优先级

用户应用注释

本组件定义了一个主体的优先级。TSC 中所有可共享资源都服从服务优先级机制。如果一个主体打算对一个可共享的 TSC 资源采取行动，那么其访问或访问时间将取决于该主体的优先级、当前活动的主体的优先级和仍在队列中的主体的优先级。

K3 资源分配(FPR _RSA)

本子类的要求允许 TSF 控制用户和主体对资源的使用，使得不因未授权地独占资源而出现拒绝服务。

用户注释

资源分配规则允许通过建立配额或其他方式，来定义代表某个特定用户或主体进行分配的资源空间大小或时间长短的限制。例如，这些规则可以：

——提供客体配额，以控制某一特定用户可以分配的客体数量或大小。

——控制预先指定的资源单位的分配和再分配，这些单位受 TSF 的控制。

一般来讲，这些功能将通过使用赋给用户和资源的属性来实现。

这些组件的目标是为了确保在用户(如单个的用户不能分配所有的可用空间)和主体间保证一定的公平。由于资源的分配常常超出了一个主体的生命周期(即文件通常比产生它们的应用存在的时间更长)，并且同一用户对主体的多个例程不应对其他用户产生太多的负面影响，这些组件允许分配限值与用户相关。有些情况下资源是由一个主体来分配的(如主内存或 CPU 周期)，在那些例程中这一组件允许资源在主体级别上进行分配。

本子类的重点在对资源分配的要求，而没有对资源本身的使用提出要求。因而审计要求也将在资源的分配上，而不是在资源的使用上。

FRU _RSA.1 最高配额

用户应用注释

这一组件对仅应用于TOE中的一组特定的可共享资源的配额机制提出了要求。这些要求允许配额与用户有关，并如适用于TOE一样可以赋给用户组或主体。

操作

赋值：

在FRU _RSA.1.1中，PP/ST作者应规定要求最大资源分配限值的受控资源的列表，(如进程、磁盘空间、内存、带宽)。如果TSC中的所有资源都需包括在内的话，那么可规定“所有TSC资源”。

选择：

在FRU _RSA.1.1中，PP/ST作者应选择是将最高配额应用到：单个用户、预定义的用户组、主体或它们的任何组合上。

在FRU _RSA.1.1中，PP/ST作者应选择最高配额是在任何给定时间(同时)都可使用，还是在某一时间间隔中可使用。

FRU _RSA.2　最低和最高配额

用户应用注释

这一组件对仅应用于TOE中的一组特定的可共享资源的配额机制提出了要求。这些要求允许配额与用户有关，并如适用于TOE一样可能赋给用户组或主体。

操作

赋值：

在FRU _RSA.2.1中，PP/ST作者应规定要求最大资源分配限值的受控资源的列表，(如进程、磁盘空间、内存、带宽)。如果TSC中的所有资源都需包括在内的话，那么可规定“所有TSC资源”。

选择：

在FRU _RSA.2.1中，PP/ST作者应选择是将最高配额应用到：单个用户、预定义的用户组、主体或它们的任何组合上。

在FRU _RSA.2.1中，PP/ST作者应选择最高配额是在任何给定时间(同时)都可使用，还是在某一时间间隔中可使用。

赋值：

在FRU _RSA.2.2中，PP/ST作者应规定需要对其进行最小分配限值进行设定的受控资源(例如进程、磁盘空间、内存、带宽)。如果TSC中的所有资源都需包括在内的话，则可规定“所有TSC资源”。

选择：

在FRU _RSA.2.2中，PP/ST作者应选择是将最低配额应用到单个用户、规定的用户组，还是主体或它们的任何组合上。

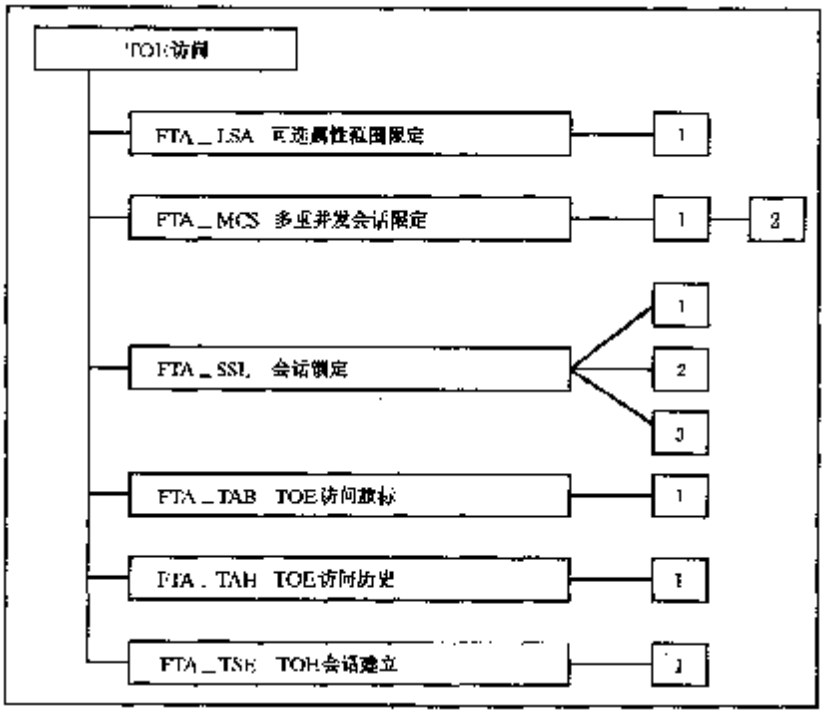
在FRU _RSA.2.2中，PP/ST作者应选择最低配额是在任何给定时间(同时)都可使用，还是在某一时间间隔中可使用。

附 录 L
（提示的附录）
TOE 访问(FTA)

用户会话的建立通常包括一个或多个主体的创建，这个(些)主体在TOE中代表用户执行操作。在会话创建过程的最后，如果满足TOE的访问要求，所创建的主体则具有由标识和鉴别功能决定的属性。本子类规定了控制用户会话建立的功能要求。

一个用户会话被定义为一个周期，它开始于标识/鉴别时间，更恰当地说是开始于用户和系统之间进行交互时，直到所有与那个会话相关的主体(资源和属性)都已被重新分配为止。

图L1给出了本类具体组件的分解情况。



图L1 TOE访问类分解

L1 可选属性范围限定(FTA_LSA)

本子类所定义的要求将限制用户可能选择的会话安全属性和用户可能要绑定到的主体，这些限定取决于：访问方法、访问的地址或端口、时间(如一日的某些时间、一周的某些天)。

用户注释

本子类使PP/ST作者能为TSF规定一些要求，以基于环境的条件对授权用户的安全属性域的设置限定。例如，可允许一个用户在正常的工作时间内建立一个“秘密会话”，但在此之外的时间里此用户就可能会受到制约，只能建立“不分级的会话”。对于可选属性域的相关限定的鉴别可通过使用选择操作来完成。这些限定可用于一个个属性上。当需要规定对多属性的限定时，这一组件将应被复制到每一属性上。可用于限制会话安全属性的属性例子有：

a) 访问方法可用于规定用户将在何种类型的环境下工作(如文件传送协议、终端、vtam)。

b) 访问地址可基于用户访问地址或访问端口之上用来限制用户可选属性的域。这种能力主要应用于拨号设备或网络设备环境下。

c) 访问时间可用来限制用户可选属性的域，例如，时间范围可基于一日的某些时间、一周的某些天或日历日期。为防止在正确的监控或正确的措施未实施时用户执行一些操作，这一限定提供了一些操作性的保护。

FAT _ LSA.1 可选属性范围限定

操作

赋值：

在 FTA _ LSA.1.1 中，PP/ST 作者应规定要受到限制的会话安全属性集。这些会话安全属性的例子有用户许可证级别、完整性水平和角色。

在 FTA _ LSA.1.1 中，PP/ST 作者应规定可用于决定会话安全属性范围的属性集，这些属性的例子有用户身份、原发地址、访问时间和访问方法。

L2 多重并发会话限定(FTA _ MCS)

本子类定义了一个用户在同一时间可能有的会话数(并发会话)。并发会话数也可为一组用户或为每一个用户单独设置。

FTA _ MCS.1 多重并发会话的基本限定

用户应用注释

本组件允许系统限制会话数以便有效地使用 TOE 资源。

操作

赋值：

在 FTA _ MCS.1.2 中，PP/ST 作者应规定可使用的最大并发会话数的默认值。

FTA _ MCS.2 每个用户属性对多重并发会话的限定

用户应用注释

本组件通过允许对用户可调用的并发会话的数量进行更进一步的限制，提供了超出 FTA _ MCS.1 的进一步的能力。这些限定是按照用户的安全属性规定的，如一个用户的身份或一个角色的成员资格。

操作

赋值：

在 FTA _ MCS.2.1 中，PP/ST 作者应规定决定最大并发会话数的规则。举一个规则的例子：“如果用户的分类级别为‘秘密的’，则最大并发会话数为 1，否则为 5”。

在 FTA _ MCS.2.2 中，PP/ST 作者应规定可使用的最大并发会话数的默认值。

L3 会话锁定(FTA _ SSL)

本子类为 TSF 定义了一些要求，以为交互式会话提供锁定和解锁能力(如键盘锁定)。

当一个用户直接与 TOE 中的主体进行交互(交互会话)时，用户的终端在无人照管的情况下很容易受到攻击。本子类为 TSF 提出了在规定的非活动周期后对终端锁定或结束会话的要求，并对用户提出了初始化终端锁定的要求。为了重新激活终端，必须发生由 PP/ST 作者规定的一个事件，如用户再次鉴别。

如果一个用户有一段时间没有向 TOE 提供任何动作，则该用户就被认为是处于非活动状态。

PP/ST 作者应考虑是否应该把FTP _ TRP.1 可信路径包括进去。那样的话,“会话锁定”功能应包括在FTP _ TRP.1 的操作中。

FTA _ SSL.1 TSF 原发会话锁定

用户应用注释

FTA _ SSC.1“TSF 原发会话锁定”向 TSF 提供了在指定的一段时间后锁定一个活动用户会话的能力。锁定一个终端可防止通过使用被锁的终端与现有活动会话进行进一步的交互。

如果重写显示设备,则替代内容不必是静态的(如使用“屏幕保护”)。

本组件允许PP/ST 作者规定何种事件将解锁会话。这些事件可能与终端(如用固定的击键设置来解锁会话)、用户(如重鉴别)或时间有关。

操作

赋值:

在FTA _ SSL.1.1 中,PP/ST 作者应规定用户非活动期的间隔以定时触发交互式会话上锁。如果有这样的要求,PP/ST 作者可通过这一赋值规定这一时间间隔是留给授权管理者还是用户。FMT 类中的管理功能可规定修改这一时间间隔或将其变为默认值的能力。

在FTA _ SSL.1.2 中,PP/ST 作者应规定解锁会话之前应发生的事件。例如这一事件可能是“用户重鉴别”或“用户输入解锁口令”。

FTA _ SSL.2 用户原发锁定

用户应用注释

FTA _ SSL.2“用户原发锁定”向授权用户提供了锁定和解锁自己的终端的能力。这使得授权用户无需终止活动的会话就能有效地阻止进一步使用他们的活动会话。

如果重写显示设备,则替代内容不必是静态的(如使用“屏幕保护”)。

操作

赋值:

在FTA _ SSL.2.2 中,PP/ST 作者应规定解锁会话之前应发生的事件。例如这一事件可能是“用户重鉴别”或“用户输入解锁口令”。

FTA _ SSL.3 TSF 原发终止

用户应用注释

FTA _ SSL.3“TSF 原发终止”要求 TSF 在一段时间的非活动状态后终止一个交互式用户会话。

PP/ST 作者应认识到在用户终止其活动后,会话可能仍在继续,如后台处理。在用户的一段非活动期后,不管主体处于何种状态,这一要求将能终止该后台主体。

操作

赋值:

在FTA _ SSL.3.1 中,PP/ST 作者应规定用户非活动期的间隔,以定时触发交互式会话锁定。如果有这样的要求,PP/ST 作者可通过这一赋值规定这一时间间隔是留给授权管理者还是用户。FMT 类中的管理功能可规定修改这一时间间隔或将其变为默认值的能力。

L4 TOE 访问旗标(FTA _ TAB)

在标识和鉴别之前,TOE 访问要求为 TOE 提供向适当使用 TOE 的潜在用户显示警告消息的能力。

FTA _ TAB.1 缺省的 TOE 访问旗标

本组件要求对未经授权使用 TOE 有一个警告。PP/ST 作者可细化这一要求以增加一个缺省旗标。

L5 TOE 访问历史 (FTA _ TAH)

本子类为 TSF 定义了一些要求,要求在成功地建立与 TOE 的会话后,向用户显示那些不成功地企图访问该帐户的历史记录。这些历史记录包括日期、时间、访问方法、最后一次成功访问 TOE 的端口,以及已标识的用户自最后一次成功访问后企图访问这个 TOE 的未成功的次数。

FTA _ TAH.1 TOE 访问历史

本子类可向授权用户提供可指出对其用户帐号可能发生的滥用的信息。

本组件请求向用户提供这些信息。用户应能够查阅这些信息,但并不强制这么做。如果一个用户想这么做的话,他可以创建忽视这些信息并开始其他处理的角本。

操作

选择:

在 FTA _ TAH.1.1 中,PP/ST 作者应选择那些将在用户界面上显示的最后一次成功的会话建立的安全属性,包括:日期、时间、访问方法(如 FTP)或位置(如终端 50)。

在 FTA _ TAH.1.2 中,PP/ST 作者应选择那些将在用户界面上显示的最后一次未成功的会话建立的安全属性,包括:时间、日期、访问方法(如 FTP)或位置(如终端 50)

L6 TOE 会话建立(FTA _ TSE)

本子类定义了拒绝允许用户与 TOE 建立会话的要求,它是基于下面的属性,如访问位置或端口、用户安全属性(如用户身份、许可等级、完整性等级、角色中的成员资格)、时间范围(如一日的某些时间、一周的某些天、日历日期)或这些条件的组合。

用户注释

本子类为 PP/ST 作者提供了一种能力,它规定 TOE 对授权用户与 TOE 建立会话的能力设置限制的要求。相关限制的定义可通过使用选择性操作来完成。可被用来规定会话建立限制的属性如:

a) 基于用户的访问位置或端口,访问位置可用于限制用户与 TOE 建立一个活动的会话的能力。这一能力尤其可用于拨号设备或网络设备环境。

b) 用户的安全属性可用于限制用户与 TOE 建立一个活动的会话的能力。例如,这些属性将提供基于下述情况拒绝会话建立的能力:

——用户身份;

——用户许可等级;

——用户完整性等级;

——在角色中用户的成员资格。

这一能力尤其与授权或登录有关,可发生在执行 TOE 访问检查的不同的位置。

c) 访问时间可用来限制用户基于时间范围与 TOE 建立活动的会话的能力。例如,时间范围可基于

一日的某些时间、一周的某些天或日历日期。为防止在正确的监控或正确的措施未实施时用户执行一些操作，这一限制提供了一些操作性的保护。

FTA _ TSE.1　TOE 会话建立

操作

赋值：

在 FTA _ TSE.1.1 中，PP/ST 作者应规定可用于限制会话建立的属性。例如可能的属性有用户身份、原发地址（如非远程终端）、访问时间（如外部时间）或访问方法（如 X-windows）。

附　录　M
（提示的附录）
可信路径/信道（FTP）

用户经常需要直接与 TSF 进行交互来执行一些功能。一条可信路径提供了一种信任，即用户无论何时都可调用 TSF 直接与之通信。通过可信路径的用户响应确保那些不可信应用不能截取或修改用户的响应。同样，可信信道是在 TSF 和远程 IT 产品之间安全通信的一种方式。

本标准中图 1.2 例示了可能发生在一个 TOE 或 TOE 网络中的各种通信类型之间的关系（如 TOE 内部传送、TSF 间传送、TSF 的控制之外的导入导出）和各种形式的可信路径和信道。

缺少一条可信路径可能引起使用不可信应用的环境中的责任可追查性或访问控制的缺口。这些应用可截取用户私有的信息，如口令，并用它来冒名顶替其他用户。因而，对所有系统行为的职责都不能可靠地赋予一个可追查责任的实体。同样，这些应用可在可信用户的显示上输出错误信息，导致用户后来的行动是错误的，进而导致安全缺口。

图 M1 给出了本类的组件的分解图。

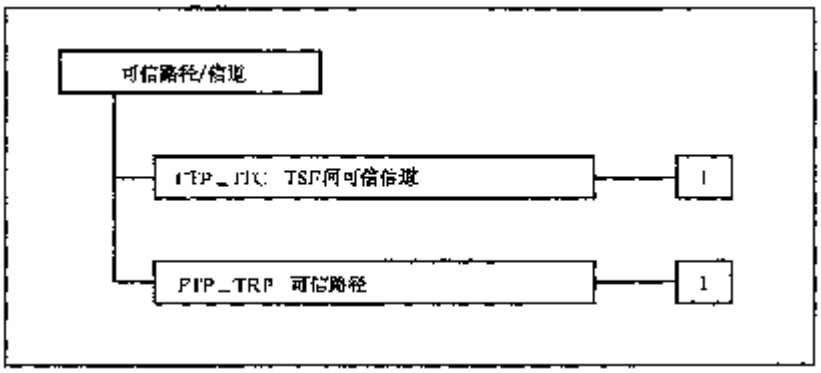


图 M1　可信路径/信道类分解

M1　TSF 间可信信道（FTP _ ITC）

本子类定义了在 TSF 和其他可信 IT 产品之间为执行关键安全操作而创建可信信道连接的规则。关键安全操作的一个例子是通过从其功能是收集审计数据的可信产品传送数据来更新 TSF 鉴别数据库。

FTP _ ITC.1　TSF 间可信信道

用户应用注释

在 TSF 和其他可信 IT 产品之间要求有可信通信信道的时候应使用这一组件。

操作

选择：

在FTP_ITC.1.2中，PP/ST作者必须规定是本地TSF、远程可信IT产品还是两者都具有初始化可信信道的能力。

赋值：

在FTP_ITC.1.3中，PP/ST作者应规定要求可信信道的功能。这些功能的例子可包括用户、主体或客体安全属性的传送，和保持TSF数据的一致性。

M2 可信路径(FTP_TRP)

本子类定义了建立和维护用户和TSF间的可信通信的要求。任何与安全相关的交互都可能要求有可信路径。可信路径交换可由用户在与TSF进行交互的时候初始化，TSF也可通过可信路径与用户建立通信。

FTP_TRP.1 可信路径

用户应用注释

为了原发鉴别的目的或仅为了补充特定的用户操作，当要求一个用户和TSF之间有可信通信的时候，应使用本组件。

操作

选择：

在FTP_TRP.1.1中，PP/ST作者应规定可信路径是否必须扩展到远程或本地的用户。

在FTP_TRP.1.2中，PP/ST作者应规定TSF、本地用户或远程用户是否能初始化可信路径。

在FTP_TRP.1.3中，PP/ST作者应规定可信路径是否应被应用于原发用户鉴别或其他特定的服务。

赋值：

在FTP_TRP.1.3中，如果选择了的话，PP/ST作者应标识要求可信路径的其他服务(如果有的话)。