os security

精通TPM的结构

> TPM芯片:可信平台模块,提供硬件级的安全密钥存储、加密计算、完整性测量等功能。

- 标志位管理器:管理关键标志位

- 加密算法引擎:RSA和对称加密算法
- 随机数生成器:生成随机数和密钥
- 密码杂凑引擎:计算杂凑值
- 存储器:非易失存储器和易失存储器
- 电源和I/O模块:电源管理、物理信号检测和通信

1. 标志位管理器:用于存储和维护TPM内部重要标志位,如使能标志位、激活标志位和属主标志位等。这些标志位对TPM的正常工作至关重要。
2. RSA算法引擎:实现RSA算法的运算,用于数据加密、解密、数字签名和验证功能。支持2048位、1024位和512位三种安全级别。
3. 对称加密算法引擎:实现Vernam算法和AES算法。用于数据加密和密钥生成等。
4. 随机数生成器:生成协议需要的随机数和对称加密算法使用的密钥。符合IEEE P1363标准。
5. 密码杂凑引擎:实现SHA-1算法,用于计算密码杂凑值。符合FIPS-180-1标准。
6. 非易失存储器:用于存储TPM的长期密钥、完整性信息、所有者授权信息和重要应用数据。
7. 易失存储器:用于临时存储计算过程中的数据。
8. 电源管理模块:用于常规电源管理和检测物理现场信号。后者对某些技术很重要,如动态度量信任根。
9. I/O模块:用于TPM内部各模块之间以及TPM与外部之间的通信。包括消息编解码、转发和模块访问控制等功能。

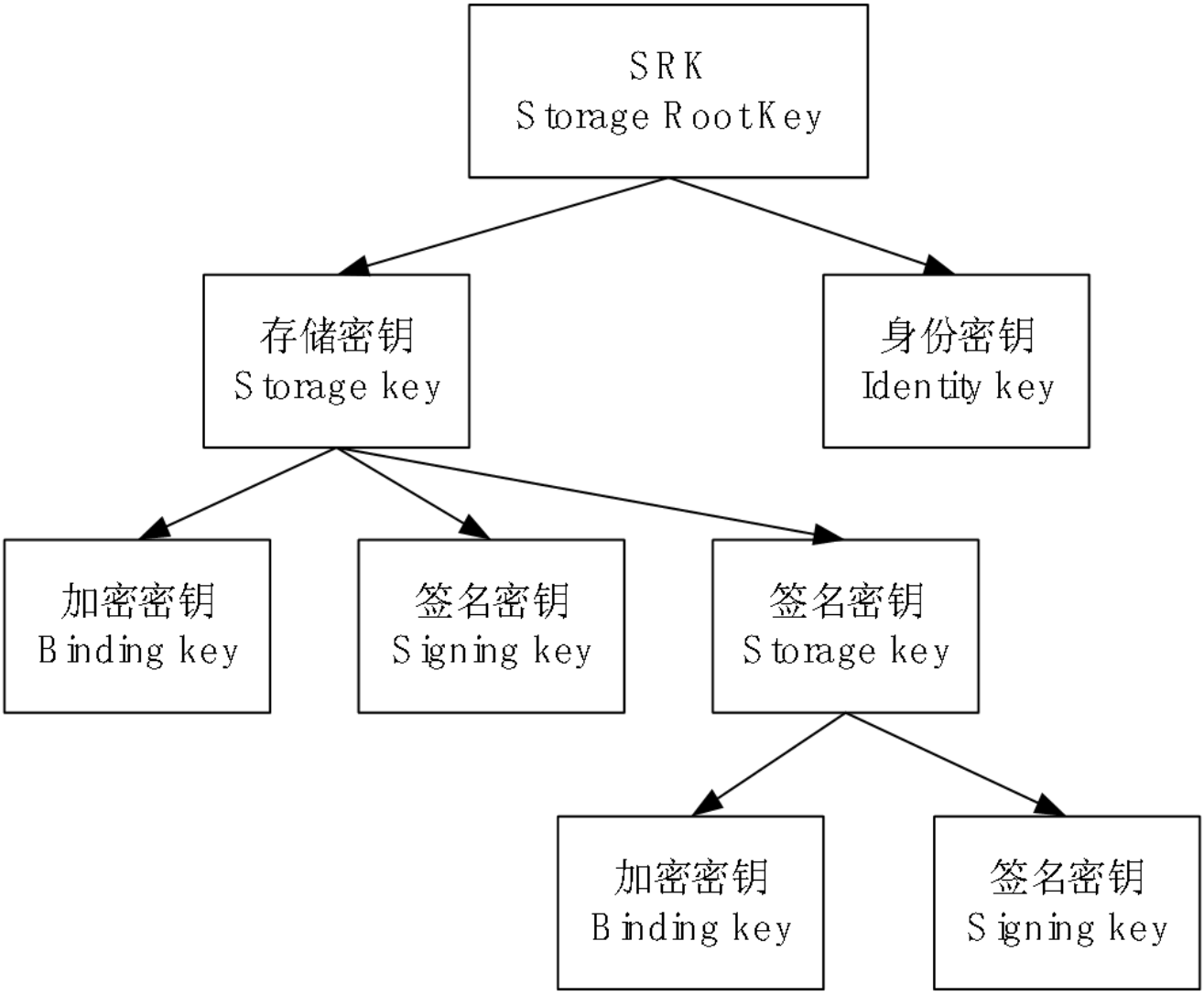
主要功能:

- 密码学系统:TPM可以生成RSA等算法的公钥和私钥,并安全存储私钥。
- 平台数据保护:TPM使用加密技术保护系统和用户数据的机密性和完整性。
  平台数据保护功能包括密钥管理/数据存储/数据迁移
- 身份标识:TPM具有唯一的芯片标识,可以为系统和设备提供身份标识。
- 完整性存储与报告:TPM可以对系统软件和设备进行完整性测量和报告。
- 资源保护:TPM通过密钥和凭证管理保护系统资源的访问。
- 辅助功能:TPM还提供随机数生成、绑定密钥等辅助加密功能。

精通TPM中各种密钥类型，生成方法、性质、使用方法、 在可信计算中作用。
见本子

1. 不可迁移密钥(Non-migratable key):
   在TPM内部产生，在TPM产生后被打上了TPM的标记。
   不可迁移密钥的本质是可用于一个并且只能用于一个TPM。
   密钥仅绑定在第一次使用它的设备上,无法迁移到其他设备上使用。 这种密钥通常存储在设备的受保护存储器中,如TPM芯片中,具有**良好的安全性**。但是由于不可迁移,使用较为不便,且**如果设备损坏则密钥可能丢失**。
   如果系统或TPM发生故障，所有不可迁移密钥及与它们关联的所有数据将不可访问，而且无法恢复。不可迁移密钥可以被TPM签名，从而可以向挑战者或者用户证明其不可迁移的属性，从而证明其安全性。
2. 迁移密钥(Migratable key):
   密钥可以在多个设备之间迁移和共享,具有**较高的便利性**。但是由于可以迁移,不像不可迁移密钥那样只与第一个设备绑定,**安全性略有不及**。如果在迁移和共享的过程中遭到攻击,密钥可能被窃取或复制。可迁移密钥的另一个优点是可以将数据从一个发生故障的平台备份并恢复到一个新的平台上。

密钥树:
产生密钥的时候要指定其父密钥、新产生的密钥及其授权数据。
指定的父密钥应该是一个存储类型的密钥，它可以是存储根密钥SRK，也可以是一个已经生成的存储密钥。
用指定的父密钥对新密钥进行加密之后存储到TPM外部。



TCG使用授权数据机制来控制建立TPM所有权、密钥使用、对象的迁移等行为。

TCG规定密钥的使用必须经过授权。

这种授权体现在使用者必须拥有该密钥的授权数据的验证码，并且必须通过验证，否则就不能使用密钥。

密钥的授权数据是在密钥产生时设定的，就像设定密钥的迁移属性那样。

TCG规定：授权数据= Hash(共享的秘密数据 II 随机数)

存储密钥的作用

主要用于对由TPM使用但是存储在TPM之外硬盘上的密钥进行保护。

可迁移、不可迁移密钥的性质是如何设计的

实施密钥迁移功能时，TPM需要用户提供密钥的迁移授权值，而迁移授权值的设定在密钥生成时完成：

- 如果TPM生成的是可迁移密钥，则需要指定其迁移授权信息；

- 如果生成的是不可迁移密钥，则为其指定一个用户不可能知道的TPM内部的随机量作为“迁移授权值”，因而用户试图迁移一个不可迁移密钥时，会因为授权值错误而被制止。
  (了解)密钥迁移的具体过程分为REWRAP和MIGRATE两种方式。
- REWRAP方式
  在密钥复制等存在明确的目标TPM的场景下，一般采用REWRAP方式进行密钥迁移，包含两个步骤(记被迁移的密钥为MK)。
  (1) 密钥迁移包生成：源TPM获取目标TPM的用于保护被迁移密钥的公钥PK，使用PK加密MK。
  - 选择PK所需的目标TPM所有者授权信息
  - MK的迁移授权信息
  - 解密MK所需的父密钥授权信息
    (2) 密钥迁移包转换：目标TPM使用PK解密得到MK。
- MIGRATE方式
  在密钥备份等不存在明确的目标TPM的场景下，需要引入名为迁移权威(Migration Authority，MA)的第三方暂时代管密钥，以便在未来某个时刻将密钥传递至目标TPM，这种密钥迁移方式被称为MIGRATE。
  (1)密钥迁移包生成：源TPM获取MA的一个公钥PKMA，使用PKMA加密MK；为防止恶意MA的窥探，使用PKMA加密MK信息之前，源TPM使用一次一密方式先加密密钥信息，并将一次一密密钥以带外方式保存和传递至目标TPM。
  (2)密钥迁移包传递：MA解密得到MK，获取目的TPM的一个公钥PKDT，使用PKDT加密MK。
  (3)密钥迁移包转换：目标TPM使用PKDT和一次一密密钥解密得到MK。

平台绑定的概念和操作方法

TPM平台绑定的概念是:将TPM生成和存储的密钥或其他敏感数据与TPM所在平台(即设备)绑定,只允许在该设备上使用,不允许迁移到其他设备上。平台绑定的主要目的是保护数据和密钥的安全,防止在迁移过程中遭到窃取或泄露。
TPM内部存在一个包括TPM拥有者在内的任何人都不确知的秘密随机数TPMproof。
一旦将某一数据与TPMproof关联后，则该数据将只能在该TPM内使用。
这样就约束了数据的流动和使用。
利用TCG的这种密钥和数据可以与平台关联的机制，可以开发出许多有特色的应用。

例如，可以限定数字产品只能在指定平台上应用。甚至限定数字产品只能在指定平台的指定环境上应用。从而实现数字产权的保护。

密封存储

这是一种将机密数据锁定于某种平台配置的特殊加密机制。
解封一个数据必须要1.在特定的状态下 2.有解密密钥

TPM提供数据封装功能

- TPM Seal
  - 输入存储密钥句柄、PCR信息(标识了平台配置)、要封装的数据以及为使用数据而设定的授权信息
  - TPM输出数据封装包
- TPM_UnSeal
  - 输入存储密钥句柄和数据封装包
  - TPM对比自身当前PCR值是否与封装包中指定的值相同，只有相同时才会执行解密操作，输出秘密信息。
  - 需要存储密钥的授权信息，需要封装数据包的授权信息
- 需要说明的是，TPM_UnSeal是TPM规范中少数几个需要两个授权信息的命令，其既需要存储密钥的授权信息，也需要封装数据包的授权信息。

密封与绑定的不同

- 密封(Sealing)就是使被加密的小规模数据(包括对称密钥)与反映平台可信状态的PCR关联起来。实际上是把PCR的值当做授权数据了。因此不需另外设置其他的授权数据。
- 绑定密钥BK和遗传密钥LK都可以绑定数据，而只有存储密钥SK才能密封数据。这就是常把密封称为密封存储的原因。

PCR的概念和作用

TPM在内部开辟了专门的完整性值存储空间一平台配置寄存器(PCR)。
PCR(Platform Configuration Register)是TPM中的一组寄存器,**用于记录平台的配置与状态信息。**
PCR的主要概念和作用包括:1. PCR是TPM的内部存储器,包含多个PCR寄存器。每个PCR寄存器可以存储一个哈希值,代表平台的某个配置或状态。
存储系统组件的完整性测量值/用于启动完整性验证/作为密钥绑定的参照/支持远程完整性验证

可信启动的原理和过程

可信启动(Trusted Boot)是指计算机从上电开始启动到操作系统完全控制计算机这个过程中,各个启动组件的完整性和启动顺序都是可信的。它依赖于可信平台模块(TPM)和信任链(Chain of Trust)来验证系统的启动完整性。

可信启动的主要作用是保证操作系统最终得到控制的计算机系统是完整和可信的。这可以防止恶意软件在系统启动早期插入木马或病毒,确保操作系统运行在一个干净的环境中。

可信启动的基本过程如下:

1. 上电自检(Power-On Self Test,POST)。BIOS进行自检确保硬件设备正常工作。
2. 可信平台模块(TPM)初始化与故障检测。TPM模块完成初始化,检测自身是否可用,无法使用时触发相关响应(如报警)。
3. BIOS启动完整性测量与记录。TPM对 BIOS 进行完整性检测,并将结果记录在持久性存储中。
4. Option ROM 启动完整性测量(如有)。TPM 对各类 Option ROM 进行完整性检测与记录。
5. 硬盘主引导记录(MBR)或统一可扩展固件接口(UEFI)启动完整性测量。TPM 对 MBR 或 UEFI进行完整性检测与记录。
6. 系统引导管理器(Boot Manager)与引导程序启动完整性测量。TPM 对 Boot Manager与引导程序(如Grub)进行完整性检测与记录。
7. 操作系统启动完整性测量。操作系统与TPM配合启动,TPM对操作系统内核与关键驱动等进行完整性检测与记录。
8. 操作系统启动验证。操作系统获取TPM的各阶段完整性测量报告,验证系统的启动过程是否可信,若不可信则采取响应措施(如报警、重启等)。
9. 清理加密密钥(可选)。若启动不可信,TPM清除其内部的加密密钥以防止被进一步利用,触发重置系统为出厂状态的过程。
10. 操作系统继续完成启动。当启动过程可信或不采取强硬响应时,操作系统继续完成启动到正常运行状态。

3.3静态信任链构建系统 — 可信启动

- 可信引导信任链构建是以TPM/TCM为信任根，从计算机系统的底层硬件出发，建立操作系统启动之前的BIOS和Bootloader的信任链；
- 为操作系统启动建立可信的运行环境；
- 这是计算机信任链构建的第一个环节；
- 是其他信任链建立的基础。

信任链的概念

系统启动过程中各组件完整性验证机制,只有全部可信才启动下一组件,实现可信启动环境。是构建计算机系统可信执行环境的方式。

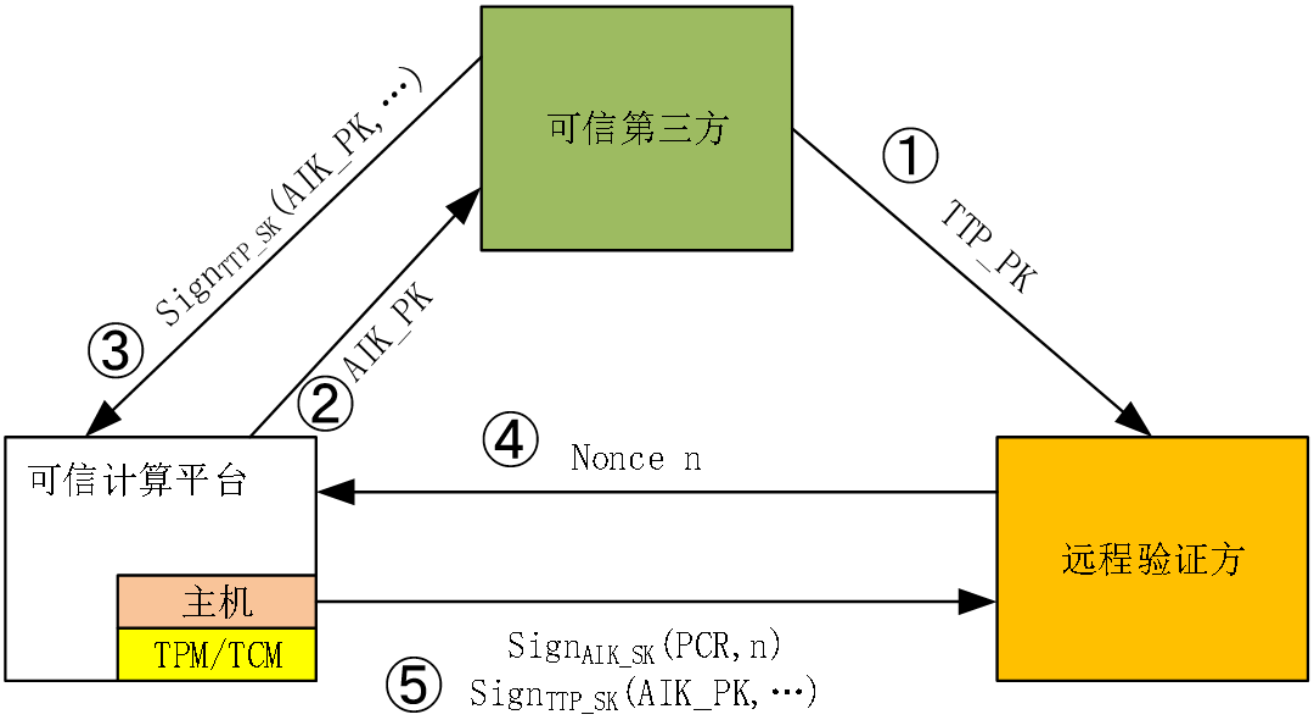
信任链

- TCG在其信任定义基础上，给出一种构建计算机系统可信执行环境的方式 — 信任链。
- TCG信任链的建立方法
  - 对计算机系统的逐层度量
  - 信任链传递
    - 建立从最底层可信硬件到目标应用程序的信任
    - 利用植入在硬件平台上的安全芯片对度量数据进行保护，建立了计算机系统的可信执行环境。
- 信任链构建的意义
  - 给用户提供可信的执行环境
  - 向远程用户提供证明可信执行环境的运行证据
  - 与传统网络技术相结合将信任进一步扩展到网络环境

平台身份认证的原理

平台身份证明 — 平台身份密钥引证

- TPM远程证明的签名过程也被称为平台身份密钥引证(quote)
  - TPM所有者首先加载平台身份密钥AIK
  - TPM所有者就选择需要证明的代表平台完整性的PCR寄存器
  - 然后输入挑战随机数和PCR寄存器
  - 执行TPM命令接口TPM_Quote
  - 最后TPM就输出相应远程证明的签名



平台身份证明 — 模型

- 可信计算平台
  - 包含TPM/TCM安全芯片和主机平台，它们共同完成平台完整性的证明。
  - 主机平台主要是对平台的完整性进行度量和报告。
  - 安全芯片TPM/TCM主要是完成远程证明的签名过程。
- 远程验证方是远程证明的挑战方
  - 它请求可信计算平台证明当前系统的完整性状态。
  - 验证可信计算平台的完整性日志和安全芯片签名。
  - 远程证明之前，远程验证方还必须知道可信计算平台的AIK公钥和可信第三方的公钥。
- 可信第三方
  - 是PrivacyCA。它负责颁发可信计算平台的身份密钥证书，并提供证书的有效性的验证。
  - 在为可信计算平台颁发AIK证书时，必须验证TPM/TCM芯片的EK，从而保证TPM身份真实性。

远程证明 — Privacy CA实名身份证明 平台身份证明

- **可信计算平台身份证明的主要步骤**

(1) 平台A所有者向平台B发送证明请求。

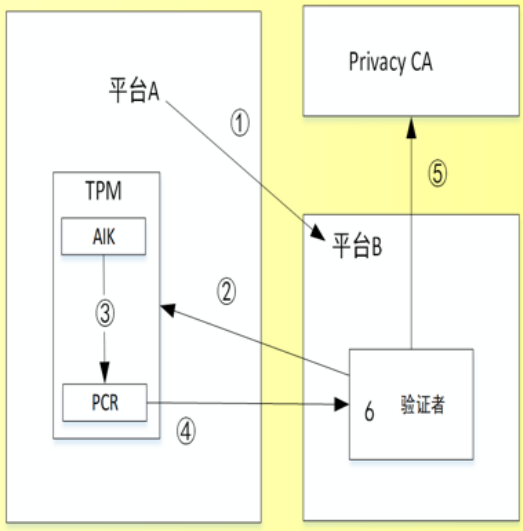
(2) 平台B向平台A发出证明挑战随机数，同时指明需要证明的PCR。

(3) 平台A所有者加载AIK密钥，然后使用AIK私钥对需要证明的PCR值签名。

(4) 平台A将远程证明签名以及完整性日志发送给平台B的验证者。

(5) 平台B请求Privacy CA，查询平台A的TPM身份是否可信。

(6) 平台B验证平台A的远程证明签名以及平台配置完整性日志。



动态远程认证的原理

动态远程认证主要用于远程验证平台的身份与完整性。它的基本原理是:

1. 平台身份证明:平台产生非对称密钥对,公钥导出并由认证机构签发证书,证书绑定平台身份。平台可以使用私钥对数据签名,外部实体验证签名与证书,实现对平台身份的认证。
2. 平台完整性证明:平台收集自身的完整性度量值(如文件哈希、PCR值等),使用私钥对度量值签名,外部实体验证签名来判断平台的配置与运行状态是否完整可信。
3. 远程证明:将身份证明与完整性证明的结果发送给远程实体,使其可以在远程判断平台的身份与完整性。

TESEC的基本原理

将系统安全性分为不同等级。TCSEC将系统安全性定义为四个基本度量:完整性(Integrity)、可用性(Availability)、保密性(Confidentiality)和账户管理(Accountability),并根据系统对这四个度量达成的程度将其分为不同安全等级,共定义了A级至D级7个安全等级,A级最高。

TCSEC安全级别

等级分类	保护等级
D类：最低保护等级	D级：无保护级
C类：自主保护级	C1级：自主安全保护级
	C2级：受控访问保护级
B类：强制保护级	B1级：标记安全保护级
	B2级：机构化保护级
	B3级：安全区域保护级
A类：验证保护级	A1级：验证设计级

D类是最低保护等级，即无保护级

- 为那些经过评估，但不满足较高评估等级要求的系统设计的，只具有一个级别
- 该类是指不符合要求的那些系统，因此，这种系统不能在多用户环境下处理敏感信息

C类为自主保护级

- 具有一定的保护能力，采用的措施是自主访问控制和审计跟踪
- 一般只适用于具有一定等级的多用户环境
- 具有对主体责任及其动作审计的能力

B类为强制保护级

- 主要要求是TCB应维护完整的安全标记，并在此基础上执行一系列强制访问控制规则
- B类系统中的主要数据结构必须携带敏感标记
- 系统的开发者还应为TCB提供安全策略模型以及TCB规约
- 应提供证据证明访问监控器得到了正确的实施

A类为验证保护级

- A类的特点是使用形式化的安全验证方法，保证系统的自主和强制安全控制措施能够有效地保护系统中存储和处理的秘密信息或其他敏感信息
- 为证明TCB满足设计、开发及实现等各个方面的安全要求，系统应提供丰富的文档信息

CC

CC(Common Criteria)是一个信息技术安全评估标准。它包含:

4. CC模型:提供一个框架,定义和说明IT产品与系统安全方面的各种概念和类别。
5. CC安全功能需求:定义IT产品与系统需要实现的安全机能,如访问控制、审计、加密等。
6. CC安全保证需求:定义IT产品与系统实现安全功能需求的程度与严苛度,按7个评估等级进行分类。

7. PP(Protection Profile):由用户自行编写,用于描述IT产品应遵循的安全需求,包括功能需求与保证需求。
8. ST(Security Target):由开发者编写,描述产品实现的安全需求与对应CC安全功能/保证需求。
9. CC评估:由独立评估机构针对ST来判断产品是否正确满足声明的安全需求与CC规范。

所以,CC为用户、开发者与评估者提供一个共同的安全需求规范与语言框架:用户可以在PP中明确定义所需产品的安全需求。 开发者需要在ST中说明产品如何通过设计与开发满足安全需求与CC规范。 评估者则根据ST来判断产品是否正确实现Declared Security Capabilities,并给出合格认证。

CC三个part组成

(General model)介绍与通用模型:阐述构建上述安全目标、需求、高层规约的模型或方法。

(security functional requirements)安全功能需求:详细阐述用于 达成既定的安全目标 的安全功能组件 。

(security assurance requirements)安全保障需求:提供一组标准的保障组件,通过选择不同的组件或组合可以表达不同强度的安全保障,并基此定义了EAL1-7共7个层次的预定义安全等级。同时,它也规定了对智力作品(PP、ST等)进行评估的标准与方法。

CC标准有三类主要读者:

1. 开发者:开发IT产品或系统的厂商、集成商等。CC为其提供:(1) 安全功能需求:可以选择实现适合产品及面向的应用环境和威胁的安全机制。(2) 安全保障需求:给出达到不同安全保障级别所需要采取的安全措施,为产品安全设计、评估与认证提供依据。(3) 高层规约:采用形式语言描述产品或系统的安全性能、安全接口和安全属性等,为开发提供规范并为验证活动提供基础。(4) 一般概念与过程:定义开发与评估涉及的各方、步骤和活动,有助于厂商理解CC认证要求与过程。

2. 评估者:进行IT产品或系统安全评估与认证的机构。CC为其提供:(1) 安全认证过程与要求:明确评估、验证各安全保障级别须采取的措施与活动。(2) 保障级别:为产品或系统的安全强度提供一般标度,以选择对应的评估方法。 (3) 一般概念与过程:理解CC认证涉及的各方职责、评估的步骤与活动流程等,为实施评估与认证活动提供框架。

3. 用户:购买或使用IT产品与系统的客户。CC为其提供: (1) 安全保障级别:代表产品或系统的安全强度,选择对应用户的安全要求。(2) 一般概念:理解产品认证的意义,各参与方的职责,认证的价值等。 (3) 安全目标及功

能需求:理解产品或系统实现的主要安全机制与防护功能。

*CC*的使用对象

最终用户

- 保证评估结果满足用户的需求。
- 判断被评估的产品或系统是否满足他们的需求（风险分析、安全策略）
- 比较不同的产品或系统（安全保证需求）。
- 给予用户一个独立于实现的表达对于产品或系统IT安全措施需求的一种方法： Protection Profile (PP)。

开发者

- 评价他们开发的产品或系统。
- 明确他们的产品或系统的能够满足的安全需求。
- 支持其他人来评估开发的评估对象。
- 开发者可以声明所开发的产品或系统满足指定的安全功能需求和安全保障需求。

评估者

- 提供评估者来判断评估对象是否满足安全需求的系列准则。
- 描述评估者在评估过程中实施在安全功能上的一般行为。
- 并不固定评估行为的具体步骤。

^^CC方法^^

CC方法主要由TOE的开发、第三方评估和用户实施三个阶段组成。

（2） CC 的方法 — 开发

- **安全目标**：安全产品或安全系统的功能必须能实现用户的安全目标。
- **关注过程**：必须要从产品或系统的开发一开始就考虑其安全需求，否则即使采用良好的工程方法也难以满足用户期望的安全目标。
- **逐层细化**：开发过程就是将安全产品或安全系统的目标到系统的实现进行逐层细化的过程。
  - 底层的细化就是上层功能的分解和设计细节。
  - 最上层是安全目标，最下层是产品或系统的实现。

CC 保障性评估必须验明功能规约的各个抽象层次：高层设计、底层设计、系统实现。

开发者必须根据所要求的保障级别来证实所采用的开发方法达到了保障性需求。

（2） CC 方法 — TOE 测评

- 评估任务的主要输入
  - 测评过的ST，作为评估工作的依据。
  - 评估对象。
  - 评估准则、方法和方案。

开发者为了通过严格的评估，在他们的设计和开发过程需求更加认真仔细。评估过程可以对**原始的需求**、**开发过程**、**最终产品**、**运行环境**进行严格评估。

(2) CC 方法 — 实施

- 用户可以选择测评过的产品或系统应用到他们的环境中。
- 在实施过程中，产品或系统的错误或弱点就会浮现，对环境的假定可能需要更该。
- 开发者会收到反馈，更新产品或系统。
- 更新后的产品或系统需要重新进行评测。

CC评估准则的model

- security environment
  - 1.TOE physical environment
  - 2.Assets requiring protection
  - 3.TOE purpose

> 安全环境包括所有被确定为相关的法律、组织安全政策、习俗、专业知识和技能。因此，它定义了 TOE 意图使用的上下文环境。安全环境还包括环境中存在或被认为存在的安全威胁。为了确定安全环境，PP或ST的撰写人必须考虑以下因素：
> a.TOE物理环境，它识别了与TOE安全相关的所有TOE操作环境方面，包括已知的物理和人员安全安排；
> b.需要通过适用安全要求或策略的TOE元素保护的资产；这可能包括直接涉及的资产，如文件和数据库，以及间接受到安全要求影响的资产，例如授权凭据和IT实现本身；
> c.TOE目的，它将涉及产品类型和TOE的预期使用方式。

  - 1.Assumptions

- 2.Threats
- 3.Security policies

> **条件的假设声明**:规定环境中必须满足哪些条件，才能使 TOE 被视为安全。这个声明可以被认为是TOE 评估的公理。
> **资产安全面临的威胁声明**:将确定安全分析认为与 TOE 相关的所有威胁。CC 用威胁主体、攻击方式、为攻击奠定基础的任何漏洞以及攻击的资产标识来描述威胁。对安全风险的评估将对每个威胁进行评估，评估威胁发展成实际攻击的可能性、攻击成功的可能性以及可能造成的任何损害后果。
> **适用的组织安全策略声明将确定相关政策和规则**:对于 IT 系统，这些政策可能会被明确引用，而对于通用 IT 产品或产品类别，则可能需要作出有关组织安全策略的工作假设。

在安全环境的背景下,根据识别出的主要威胁、安全政策与假设条件,可以推导出TOE的安全目标。

- security objectives

  根据分析安全环境的结果设计安全目标
  1.安全目标能够解决TOE在假定的物理环境中实现其操作目标
  2.安全目标用来设计对已识别的威胁实施反制的安全功能
  3.安全目标必须与组织的安全政策一致
  确定安全目标的目的是解决所有安全问题，并声明哪些安全方面由TOE本身或其环境直接解决。此分类基于包括工程判断、安全策略、经济因素和风险接受决策的过程。
  安全目标对于环境将在IT领域内实施，而且通常采用非技术性或程序性手段。

  - security objectives

    是TOE在实际应用环境中为抵御主要威胁和满足安全政策而需要达成的主要安全目的,如数据保密性、访问控制等。它们是从TOE环境与运作目的出发推导出的高层次安全需求。
  - CC requirements catalogue

    CC安全功能需求目录(Part 2):提供了多种常见的IT安全机制的功能需求与保障需求的标准化描述。这是一个给出的安全需求库,供TOE开发者和评估者选择以构建安全产品或系统。
    安全需求:是为实现安全目标而选择的CC Part 2中的具体安全功能需

求,它转化和细化了安全目标的要求。安全需求在方案设计与TOE开发中得到具体实现。它包括功能需求和保障需求。

- security requirements
  - functional requirements

    > include identification, authentication, security audit, non-repudiation……
    > 功能需求针对TOE中专门用于支撑IT安全的功能提出要求,定义所需的安全行为。功能需求包括识别、认证、安全审计、不可否认性等
    > 描述TOE应该具有的安全机能或服务以满足其安全目标。这类需求定义了TOE作为一个安全产品或系统需要实现的具体安全功能,如访问控制、加密、审计等。

  - assurance requirements

    > include constraints on the rigour of the development process requirements to search for and analyse the impact of potential security vulnerabilities
    > 保障需求针对开发者的活动、生成的证据和评估者的活动提出要求。保障需求包括对开发过程严谨性的约束以及搜索和分析潜在安全漏洞影响的要求。
    > 用于衡量TOE安全功能设计与实现的充分性与可信赖性的一系列要求。这类需求规定了开发者在设计、开发与测试阶段需要执行的一系列保障活动,如设计检验、源代码审查、漏洞分析等。保障需求来自CC Part 3,它定义了从EAL1到EAL7共7个级别的保障包,每个级别包含的保障活动越来越严格和完备。选择高EAL级别的TOE需要满足更加严格的保障需求。

  - requirements for environments
    安全目标能够由所选安全功能达成的保证来自以下两个因素:1. 对安全功能实现正确性的信心,即评估它们是否被正确实现;2. 对安全功能有效性的信心,即评估它们是否实际满足声明的安全目标。

- summary specification
  概要规范(summary specification)是CC认证文件体系中的一种文件类型,其目的是**概述TOE的安全机制与功能**来满足相应的安全需求。它提供TOE安全保护能力与属性的**高层次定义和描述**,为读者理解TOE的总体安

全方案与措施提供参考。**概要规范(Summary Specification)则是对ST中出现的安全需求的详细描述。**

ST中提供的TOE概要规范定义了TOE的**安全需求实例**。它提供了高层次的安全功能定义,声称这些功能满足功能需求;以及采取的保障措施满足保障需求。

PP、ST的作用,精通其组成结构

PP(Protection Profile)和ST(Security Target)是CC认证中的两种评估类型。

- PP(Protection Profile):保护规范,是针对某类TOE(Target of Evaluation,评估对象)提出的详细安全需求声明。

  CC保护规范(**Protection Profiles，PP**)是一种与实现无关的安全需求集合，用于描述满足特定客户需求的一类产品或者系统。

  PP详细描述一类产品的威胁、环境问题和假设、安全目标以及CC需求。需求包括功能需求和安全保障需求，其中功能需求由PP的开发者从CC功能需求中选择，安全保障需包括7个EAL中的某一个等级的安全保障需求，也可能包括一些附加的安全保障需求。PP的最后一部分提供了基本原理形式的安全保障证据，以显示PP的完整性、一致性和技术合理性。

- PP的结构

  保护规范(Protection Profiles，PP)

  - 简介
  - 产品或者系统族的描述
  - 产品或者系统族的安全环境
  - 安全目标
  - 安全需求
  - PP应用说明
  - 基本原理

- PP的作用:

  a.为某类TOE产品定义统一的安全需求,指导产品开发与设计。

  b.指导开发者进行安全设计。开发者可以根据PP中定义的安全需求与环境假设进行产品的安全架构设计、控制选择与实现方法的确定

  c.简化产品评估工作。评估机构可以直接以PP作为TOE评估的依据,不需要再定义安全需求,只需检查TOE是否满足PP。

  d.帮助用户选择安全产品:通过比较不同产品遵循的PP,用户可以选择最符合自己安全与使用环境需求的产品。因为PP定义了产品达到的保护级别与具体安全机能。

- ST(Security Target):安全目标声明,是开发者针对其特定TOE产品提出的详细安全需求与实现描述。ST需要具体定义TOE将采用的安全机制与技术手段来满足需求。

  - ST针对一个具体的产品或系统的一组安全需求和规范，用户特定产品的或者系统的评估基础。
  - ST是开发者、评估者和用户达成对产品或系统一致认识的基础。
  - ST 可供管理、市场、采购、安装、配置、操作和使用人员使用。

- ST 的结构

  简介，产品或系统描述，产品或系统安全环境，安全目标，安全需求，产品或系统的总结性声明，PP声明，原则和理由（基本原理）

- ST的作用:

  a.详细定义TOE自身将采取的安全机制与设计方案来满足其所基于的PP或自行定义的安全需求。ST反映了TOE的安全属性与能力。

  b.作为TOE进入评估认证的主要依据。评估机构根据ST来检查TOE的设计与开发是否达到声明的安全目标和要求。

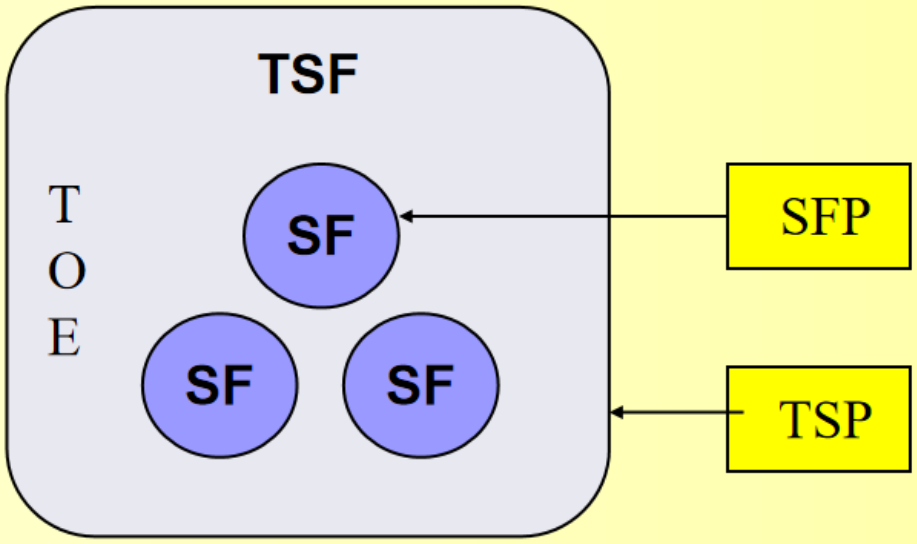
  c.为TOE的用户和运营者提供安全配置与管理指南。ST详细定义了TOE的安全特性与使用方法。

  d.支撑并增强市场宣传的效果。TOE供应商可以根据ST向客户展示产品的安全机制与功能。

> PP为ST的编写提供指引,简化评估工作;ST基于PP定制TOE自身的安全解决方案,是产品进入评估的依据与用户使用的参考。

> 模型→ST→选择参考PP→构建定制评估方案→评估ST是否达成安全目标。

Functional requirements paradigm



4.5 Types of evaluation

1. PP evaluation

评估的目标是展示*PP*是完整的、一致的、技术上可靠的，并且适用于作为可评估*TOE*的要求陈述。

2. ST evaluation

评估的目标有两个：第一是证明ST是完整、一致和技术上可靠的，因此适合作为相应TOE评估的基础；第二，在ST声称符合PP的情况下，证明ST正确地满足了PP的要求。

3. TOE evaluation

以经过评估的ST作为基础进行。这样的评估的目标是证明TOE符合ST中包含的安全要求。

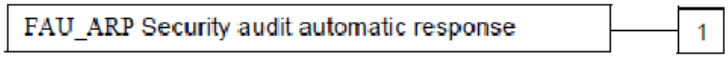
安全功能需求、安全保证需求的结构

3.1 Security audit automatic response (FAU_ARP)

Family behaviour

This family defines the response to be taken in case of detected events indicative of a potential security violation.

Component levelling



At FAU_ARP.1 Security alarms, the TSF shall take actions in case a potential security violation is detected.

Management: FAU_ARP.1

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit: FAU_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Actions taken due to imminent security violations.

FAU_ARP.1 Security alarms

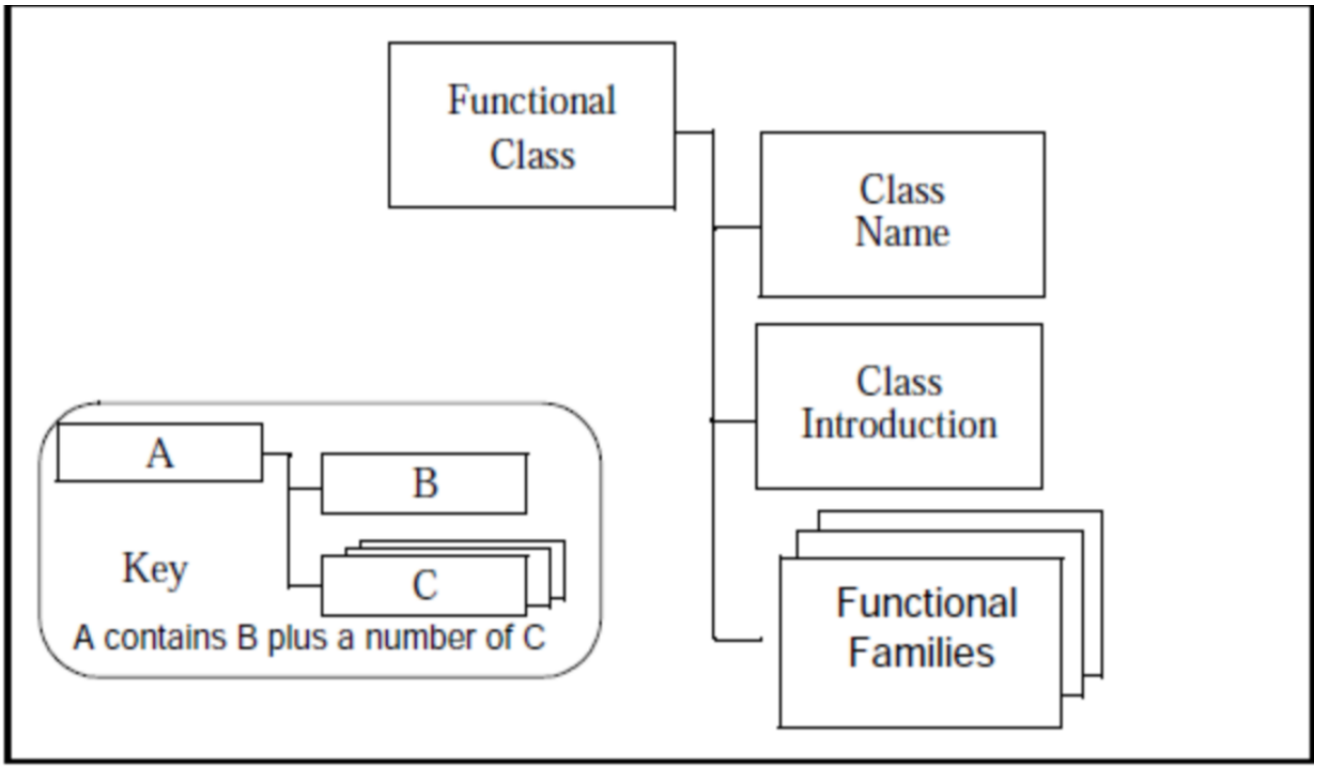
Hierarchical to: No other components.

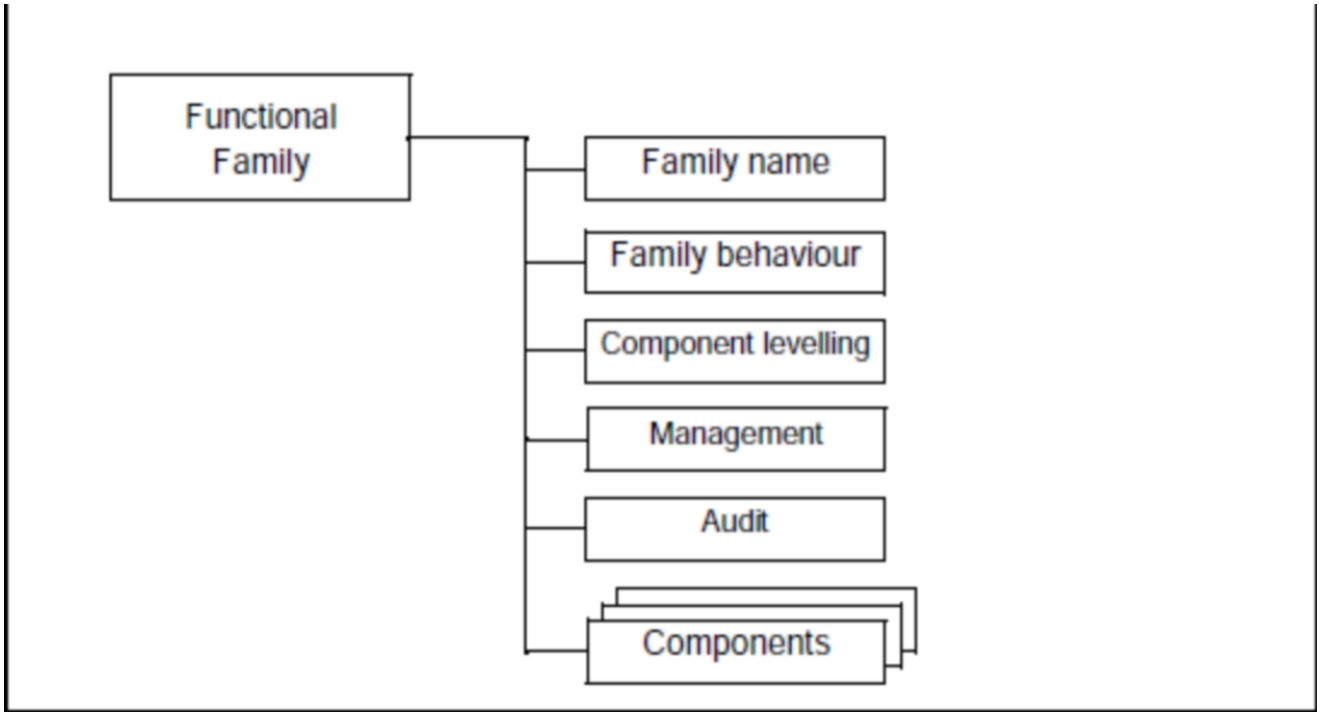
FAU_ARP.1.1 **The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation.**

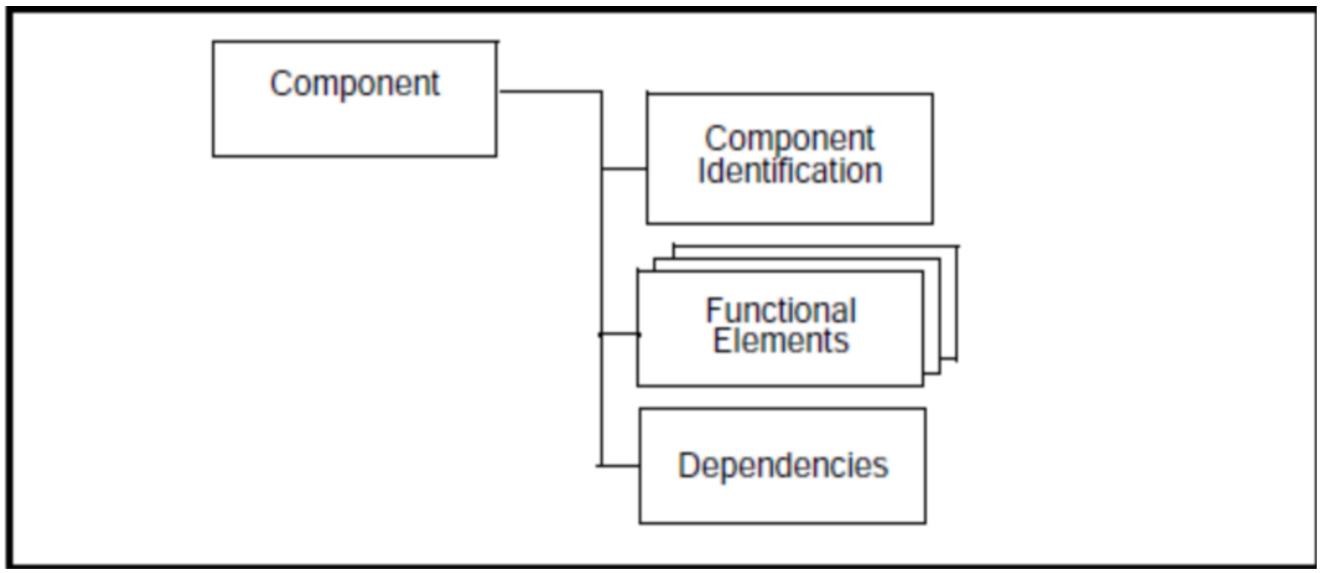
Dependencies: **FAU_SAA.1 Potential violation analysis**

结构：

class family component element


Functional Class
Class Name
Class Introduction
Functional Families
A
B
C
Key
A contains B plus a number of C


Functional Family
Family name
Family behaviour
Component levelling
Management
Audit
Components


Component
Component Identification
Functional Elements
Dependencies

elements:

1.组件由一组独立的功能要素构成,每个要素都有自己完整的定义和内容。2. 功能要素代表一个最小的安全功能原子需求。如果再进行划分就失去意义,无法进行有效评估。3. 在使用组件时,必须选择其中定义的所有功能要素。不能只选取部分要素。只有当组件的全部功能要素都得到满足时,该组件的功能和安全机制才会完全实现。4. 功能要素是组件的基本组成部分

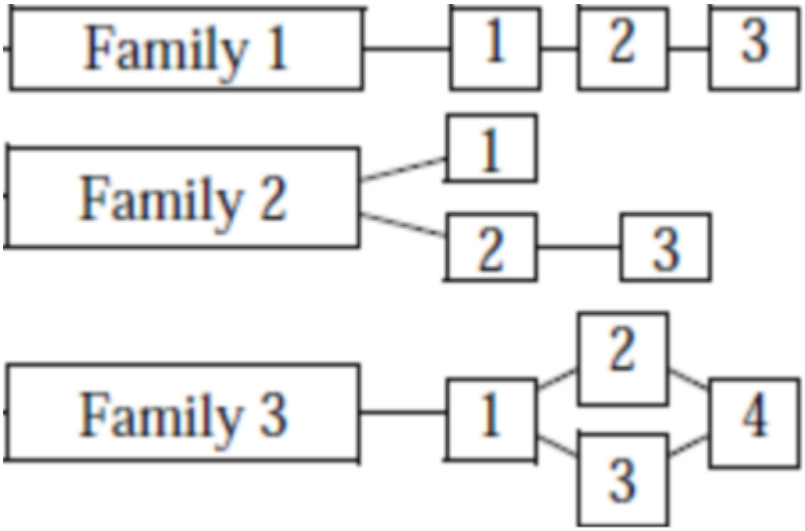
example

要求名称FDP_IFF.4.2 如下:F – 功能需求, DP – 类“用户数据保护”, _IFF – 家族 “信息流控制功能”,.4 – 第4个名为“部分消除非法信息流”的组件, .2 – 组件的第2个要素。

- *hierarchy/hierarchical*

  分层到关系仅存在于同一功能家族内的组件之间。它表示被分层到的组件提供了更强或更具体的安全机制。

  如果一个组件提供更高的安全性,那么它就是另一个组件的上级。



- *management*

  管理要求包含了PP/ST作者为给定组件考虑的管理活动信息。

  例如,

  在FAU_SAA.1潜在违规分析中,需要根据固定规则集进行基本阈值检测。通过从规则集中添加、修改和删除规则来维护规则。

  在FAU_SAA.3简单攻击启发法中,TSF应能够检测表示对TSP实施重大威胁的特征事件的发生。 维护系统事件子集(删除、修改、添加)。

  > 管理要求定义了使用各功能组件需要进行的管理和维护活动,比如:
  > 规则的增加、删除和修改
  > 阈值和基线的更新
  > 特征事件定义的变更

> 系统日志记录内容和级别的配置
> 各种列表(如黑名单、白名单)的更新

- *audit*

  审计要求为PP/ST作者提供了可以选择的可审计事件。
  这些要求包括各种详细级别的与安全相关的事件。
  - 最低 - 安全机制的成功使用;
  - 基本 - 安全机制的任何使用以及涉及的安全属性的相关信息;
  - 详细 - 对机制所做的任何配置更改,包括更改前和更改后实际的配置值。
    所以,审计要求定义了使用某个功能组件时需要记录的事件和细节级别,以支持后续的审计和审查。
- *dependencies*

  当一个组件不足以自给自足并依赖于另一个组件的功能或交互作用以正确运行时,功能组件之间就会产生依赖关系。每个功能组件都提供与其他功能组件和保证组件相关的完整依赖关系列表。
  依赖关系不局限于同一功能家族,也可以存在于不同家族的组件之间。它表示依赖组件需要使用被依赖组件提供的安全机制或输出来满足其自身的需求。
  + FAU_SAA.1依赖于FAU_GEN.1。因为FAU_SAA.1的事件关联分析机制需要使用FAU_GEN.1生成的审计事件数据作为输入。
  ***在PP、ST或功能包的要求定义中使用的功能组件可以定制以满足特定的安全目标。
  Thus, this tailoring is restricted to an approved set of operations.
- *operation(iteration ,assignment, selection, refinement) .*

  1. 迭代:重复使用同一组件,但要素的参数或选择各异。用于满足数量上的变化,如识别不同类型用户。
  2. 分配:为组件中定义的可分配参数指定具体值。用于将组件实例化到具体系统环境中。
  3. 选择:从组件中要素定义的选项列表中选择一个或多个。用于根据需要使用组件的部分功能。
  4. 精化:在不改变原有要素内容和依赖的前提下添加细节。用于满足环境中的具体实现需要。

  举例来说:
  1. 迭代:可以在同一ST中多次使用FAU_GEN.1来定义识别不同类型用户

(如普通用户和管理员)的审计事件集。
2. 分配:可以为FAU_SAR.1的复审事件类型列表赋具体值,如"所有用户登录事件"。
3. 选择:从FAU_SAR.3定义的可选审计复审范围中选择"特权用户操作"。
4. 精化:可以在FAU_SAA.1的规则集中加入针对具体系统的规则,但这不应改变原有规则内容。这些操作允许我们在使用组件满足具体需求时进行必要的定制,但同时也保证了组件功能的稳定与依赖的满足。这为我们提供了在保证安全机制可信与可评估的同时进行灵活设计。
Example of selection, assigment (FAU_GEN1.1)
The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection: minimum, basic, detailed, not specified] level of audit; and
c) [assignment: other specifically defined auditable events].
a)要素直接使用了原有定义,未做更改。这不属于选择或分配操作。 b)要素从"最低,基本,详细,未指定"四个选项中进行了选择。这属于选择操作。
c)要素为参数"其他特定定义的可审计事件"进行了分配。这属于分配操作。
+ iteration
在测试过程中，评估人员可能会发现设备无法承受某种类型的攻击或漏洞利用。评估人员需要回到之前的测试步骤重新测试，以确认该问题的根本原因并识别解决方案。在这个过程中，评估人员可能需要修改测试方法，增加测试用例或者对测试环境进行更改，以便更准确地模拟攻击场景。这种反复测试和分析的过程就是 *Common Criteria* 中的 *iteration* 操作。
安全审计功能需求

FAU-安全审计

- 该类包含6个族，分别是审计自动响应、审计数据生成、审计分析、审计审查、审计事件选择以及审计事件存储。

3 Class FAU: Security audit

Security auditing involves recognising, recording, storing, and analysing information related to security relevant activities (i.e. activities controlled by the TSP). The resulting audit records can be examined to determine which security relevant activities took place and whom (which user) is responsible for them.

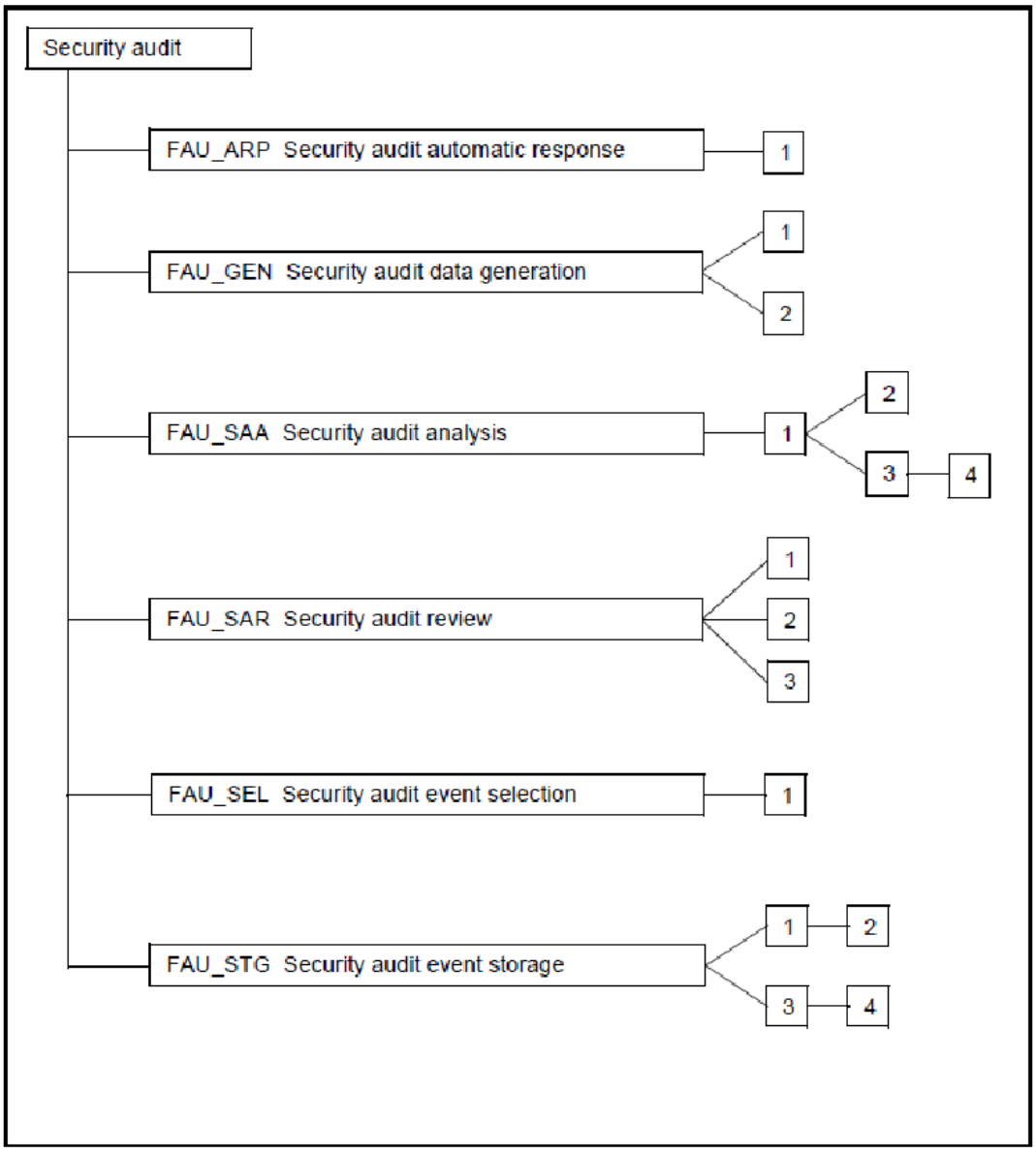


Figure 3.1 - Security audit class decomposition

- 安全功能需求:规定系统应实现的安全机制和控制措施。如访问控制、审计等。
- 安全保证需求:对系统安全性特征的主观信任进行量化和评价的要求。如开发环境审查、测试覆盖率等。

- 所以,简而言之:
  1. 特定安全功能要求侧重规定系统应具备的安全控制与机制,以实现安全处理和保护。
  2. 保证要求则侧重评估这些安全机制的有效性和可信度。它指定了评估系统安全性的具体方法与标准。
- 这两类要求相辅相成,共同确保系统的安全:
  1. 没有特定安全功能,系统无法提供安全保障与保护。
  2. 没有保证要求,无法判断安全机制是否有效和可信,安全性无法保证。

安全保证需求、安全评估与安全配置管理

安全保证需求、安全评估与安全配置管理之间存在以下关系:

1. 安全保证需求是安全工作的出发点,它定义系统需要达到的安全级别与应遵守的规则,为后续安全评估与配置管理提供方向。可以比喻为旅游的目的地设定,它决定了我们的行程方向与规划。
2. 安全评估是对系统当前安全状态的判断与分析,它根据保证需求检查现有安全措施是否达标,找出系统的漏洞与不足,为安全配置管理提供依据。 可以比喻为旅游路线的考察,我们需要评估各种交通工具费用、Timing、景点等,以决定一个可行的旅行方案。
3. 安全配置管理是根据评估结果,选择并实施必要的安全配置与控制来满足保证需求,达到系统期望的安全级别。可以比喻为旅游的具体安排,根据考察结果选择交通与住宿,制定详细行程,购买门票等,以确保旅行满足出发前的要求与目的。

   所以,安全保证需求是目的,安全评估是手段,而安全配置管理实际上是解决手段。

   三者之间存在明显的因果关系:

   保证需求 → 评估判断 → 配置实施

   目标设定 → 现状考核 → 解决方案

   只有在明确系统安全保证需求的基础上,通过全面准确的安全评估,选择有效的安全配置与控制来实施,才能真正满足安全要求,达到可接受的安全级别。它们是安全管理工作的三个关键步骤,缺一不可,需要贯穿始终,不断地检测与优化。

EAL的思想和评估方法

- 思想

  EAL等级体现了安全评估的严密性和全面性。高等级表示对产品安全性的信心更高,但也意味着更加繁重与耗时的评估过程。不同应用环境需要权衡安全性与实用性,选择恰当的EAL等级。

  评估保证等级（EALs）提供了一个逐渐增加的刻度，平衡了获得的保证水平与获得该保证水平的成本和可行性。

  从一个EAL到另一个EAL的保证水平增加是通过以下方式实现的：首先，通过将来自同一保证家族的更高级别保证组件进行替换（即增加严谨性、范围和/或深度）。其次，通过添加来自其他保证家族的保证组件（即增加新的要求）来增加保证水平。这样的替换和添加操作实现了从低级别到高级别的逐步增加保证水平的目标。

- 评估方法

  EAL1-4主要依靠开发者的开发流程与文档,EAL5-6会进行设计与模型检查,而EAL6以上则需要开发者提供实现的详细设计规格与测试记录以支持评估过程。

  EAL安全评估采用文档审查、源代码分析、测试观察、模型检查与再现测试等手段,对规范遵循性、设计健全性和测试全面性进行检查、评估与验证。高EAL等级评估往往需要开发者提供详尽设计文档与大量测试报告。