atsec information security
Tel: +86-10-82893001
Fax: +86-10-82890017
www.atsec.com

从研发角度来理解 CC

张力

（atsec　北京市 100085）

摘要：CC（Common Criteria）给研发人员提供了一套完整且清晰的方法描述产品的安全，但对研发人员来说，如果研发人员不能够真正理解其内在的含义的话，很难用CC“语言”来描述产品的安全。本文档的目的是帮助研发人员更好地理解CC，希望对今后参与CC评估工作的研发人员起到一定的指引作用。

关键词： CC、EAL、ST、SFR、ADV、ATE

Understanding CC from viewpoint of research and development

Zhang Li

(atsec Beijing 100085)

Abstract: CC (Common Criteria) provides a complete and unambiguous method for the developers to describe the security of a product, but if developers cannot thoroughly understand it, it will be very difficult for them to use CC language to describe the security of a product. This document aims to help researchers or developers better understand CC, and hope it will guide them to participate into the future CC evaluation work very well.

Keywords: CC、EAL、ST、SFR、ADV、ATE

作者简介

张力（1973 -），男，西安电子科技大学硕士，资深咨询顾问，主要从事 FIPS 与 CC 方面的研究、咨询与测评工作。

CC（Common Criteria）给研发人员提供了一套完整且清晰的方法描述产品的安全，但对研发人员来说，如果你不能够真正理解其内在的含义的话，很难用CC“语言”来描述产品的安全。

本文档的目的是帮助研发人员更好地理解 CC 评估，在此基础上对 CC 标准中一些晦涩、难懂的概念进行了深入的探讨与阐释，以帮助大家更好地理解标准，希望对今后参与 CC 评估工作的研发人员起到一定的指引作用。

1　产品研发与 CC 评估的关联概述

每个产品都有自身的安全功能需求，不同的产品安全功能可能会有所不同，但对安全功能的保障方式依据 CC 则有着相同的预定义准则，CC 标准中提出了评估保障级别（EAL：Evaluation Assurance Level）的概念，分为 EAL1~EAL7，EAL1 为最低保障级别，EAL7 为最高保障级别，每一级 EAL 要比其下的所有 EAL 有更多的保障要求，下面以 EAL4（商业互认的最高级别）为例来说明产品研发过程与实际评估过程的对应关系。

对一个产品做安全评估，首先需要基于该产品用户的安全问题形成安全需求描述，然后针对

这些安全需求，确定评估范围和被评估范围的安全功能，之后通过审核产品的开发流程（即生命周期）、开发（产品设计）、测试与脆弱性分析以及产品交付等方面评估产品是否符合了相应的保障级别要求。下图说明了 CC 的整个评估流程，重点描述了产品研发过程的各个环节与评估保障类的对应关系。

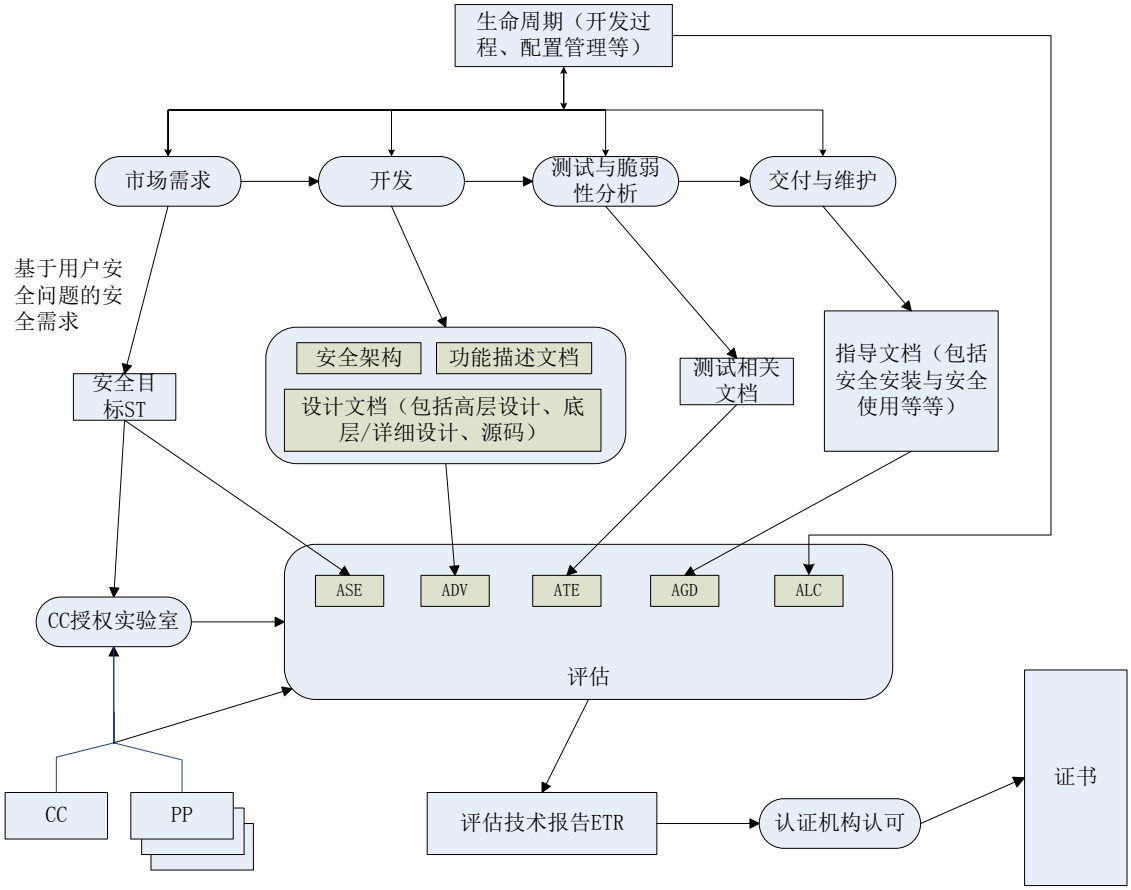

图 1 产品研发与CC评估的关联关系

由上图我们可以看出，对产品的评估主要关注在下面五个层面：

1） 安全目标（ST：Security Target）
2） 生命周期
3） 产品开发
4） 测试与脆弱性分析
5） 产品交付

下面从研发角度对这5个方面给出详细的阐述。

1.1 ST

ST是针对一款特定产品的安全需求描述，是开发人员、评估人员以及产品（TOE：Target Of Evaluation）的最终用户在产品的安全特性与评估范围方面达成一致的基础。ST基于用户的安全问题来描述产品的安全需求，包括产品的安全功能、产品抵御的安全威胁以及环境的支持。

一个实际的评估项目首先要确定评估的范围，即哪些安全功能需要评估，被评估的安全功能要求按照特定的格式在ST中给出描述。ST中必须包含的内容如下：

- 需要解决的安全问题描述，包括：产品抵御的威胁列表， 产品实现或遵从的安全策略列表（比如国家的法律或法规），功能实现所需要的预期环境描述（包括人员安全意识的培训）。
- 针对安全问题的解决方案的高层描述，由一套抵御威胁与在预期环境中实现策略的安全目标组成。
- 运用CC标准来明确描述产品的安全需求。
- 产品怎么实现所选的安全需求。
- 论证安全功能如何实现安全需求、安全需求如何实现安全目标、安全目标如何抵御威胁，以及这些方面描述的一致性。

1.2 生命周期

生命周期贯穿于产品从市场需求、研发到最终交付实施与使用的整个过程，关注产品的开发流程，包括配置管理、审核流程、项目管理控制、变更控制过程、测试方法、办公场所安全、开发工具与交付使用等方面。

配置管理系统，必须对产品的每个版本与配置项分配唯一的标识，必须阻止未授权的更改，支持添加或更改配置项的过程。配置管理系统必须管理所有的设计描述、测试文档、用户与管理员指导手册、配置管理文档、所有发现与报告的安全缺陷信息。

办公场所安全需要关注开发与设计过程的人员安全，是否安装了摄像监控系统，开发环境是否连接到了公共网络，外部人员的进出访问控制等等。

1.3 产品开发

产品开发需要有产品设计文档描述，针对EAL4，至少应该包括功能说明文档、安全架构文档、TOE设计文档（高层设计文档、底层设计/详细设计文档），源码实现等等。

功能说明描述产品的所有外部接口，针对每个接口，需要详细描述它的目的、使用方法、参数、相关的行为与错误处理。功能说明必须描述与安全相关的所有部分，必须能够证明它与ST中描述的安全需求是一致的。

TOE设计可以按照子系统、模块的划分来描述，必须描述每个子系统或模块提供的安全功能和所有的接口，每个接口需要详细描述它的目的、使用方法、行为与错误处理。必须说明产品必需依赖的底层硬件、软件与固件，描述由他们提供的保护机制。必须也能证明TOE设计与ST中描述的安全需求是一致的，并且能正确且完整地映射到功能说明。

安全架构需要证明产品不能被篡改，安全机制不能被迂回。下一章节我会对这一部分进行深入的探讨。

源码是设计的最终体现，要能正确、完整地映射到TOE设计。

1.4 测试与脆弱性分析

CC评估中所说的测试侧重于测试产品的安全方面，需要审核的信息包括测试计划、测试流程描述、期望的测试结果与实际的测试结果。要求功能说明中的每一项至少被测试一次，并且测试要求深入到产品设计的每个子系统级别。评估人员需要通过一系列脆弱性分析来证实产品的安全机制足以抵制每种攻击。

1.5 产品交付

在对产品的研发版本经历了严格的测试与脆弱性分析后，将形成一个稳定的可以发布的版本，但在安全交付客户使用前需要注意两个问题，一个是安全交付，一个是安全安装。

安全交付需要有相应的交付流程描述，其中描述了安全的交付方式，以及辨别真伪的方法。

安全安装需要有相应的安装向导文档，描述用户怎样创造一个安全的操作版本，这包括安装软件与硬件的过程，包括配置、个性化设置、生成密钥，创造一个安全的物理环境、等等。

除了安装向导文档外，EAL4还需要提供操作指南，包括安全操作、错误与警告、带特权用户的处理、操作模式，安全事件等等。

整个评估过程，最为重要的部分即为开发与测试的评估，这两部分也与我们的产品研发人员最为密切，当然这并不是说其它部分的评估不重要，而是其他部分在CC标准中的描述要相对容易理解，而对于开发与测试，CC保障需求（ADV：Assurance of Development 与ATE：Assurance of Tests）的描述包含了更多的专业术语，也比较难于理解，下面主要就ADV与ATE中一些难点进行深入的探讨。

2 CC 标准的难点解析

2.1 安全架构

CC标准中的安全架构需要保护三个要素信息的描述，即自保护、域隔离与防迂回。下面分别进行说明。

- 自保护

TOE实现的某种安全功能以阻止未信任的用户或进程干扰安全功能。TOE需要保证没有非信任的用户能篡改TSF功能。以Redhat Linux为例，内核与应用程序的分离即为一种自保护的机制，应用程序对内核的访问仅能通过系统调用完成。内存管理（限定应用程序对内存的使用），以及对配置文件和其他关键数据的自主访问控制（DAC: Discretionary Access Control）也是自保护的一部分。

- 域隔离

域隔离是支持自保护的一种机制。还以Redhat Linux为例，Linux通过页表、页读写保护、内存虚拟化等方法建立不重叠的地址空间来实现内存保护；带不同特权级别的不同处理器模式（仅在特权模式能更改内存保护），无特权进程禁止I/O操作；存放核心代码在管理状态域（即内核），存放信任程序的代码在独立的用户状态域（即程序），存放未信任的程序代码在其它用户状态域（不同于拥有信任程序代码的用户状态域），域之间仅能通过友好定义的接口来交互；应用进程间仅能通过内核提供的通信机制通信；这些方面都实现了域隔离机制。

包过滤防火墙并不实现域隔离机制，这是因为防火墙仅有一个域就是防火墙自身，防火墙通常不拥有未信任的实体，它仅分析网络数据。防火墙可以拥有不实现安全功能的非信任实体，仅提供方便的功能。例如允许远程监视防火墙设置的应用（不更改设置），周期性的复制审计日志到外部实体的应用。

大多数应用类型TOE实现的域隔离，是借助底层的操作系统建立的不同域或分布式环境来完成的。

- 防迂回

防迂回是TOE保护用户数据与TSF（TOE Security Functionality）数据的机制，以用户通过友好定义接口的方式访问它们。防迂回确保非信任的实体能做关键性的安全操作，如仅通过友好定义的接口（如Redhat Linux中IPC、命令行或配置文件）访问被保护的对象，所有这些接口能确保安全功能被正确执行。防迂回是针对TOE所有的安全功能，而不是针对TOE的部分安全功能，因为如果部分安全功能没有实现防迂回，这部分安全功能将会给TOE带来安全威胁，比如迂回认证能潜在地迂回所有用户基于安全功能的识别，迂回审计可以允许用户尝试违反策略而没

有被监测，迂回加密可能泄露数据，等等。

2.2 SFR-enforcing、SFR-supporting 与 SFR-no-interfering 含义

在对TOE设计部分进行评估时，评估人员通常会将TOE系统划分为SFR-enforcing（Security Functionality Requirement执行）、SFR-supporting（SFR支撑）与SFR-non-interfering（SFR不相关）子系统或模块，然后再按照子系统或模块所完成的功能进行进一步的评估。

SFR-enforcing是直接实现SFR的部分，比如自主访问控制DAS、用户管理、用户认证。

SFR-supporting是SFR执行功能依赖的部分，比如设备驱动、内存管理。

SFR-non-interfering是不实现TSF的TOE其他软件部分，或SFR执行或支撑依赖的其他软件部分，

为了帮助大家理解，下面以防火墙与Linux为例来阐述一下这三个概念的区别与含义。

- 防火墙

SFR-enforcing：包过滤功能。

SFR-supporting：防火墙的操作系统内核。

SFR-non-interfering：日志分析器（如果日志检查功能没有声称在SFR中）。

- Redhat Linux

在Redhat Linux操作系统中，通常仅部分内核实现安全执行机制（如DAC、审计等），而在内核域的设备驱动程序虽然不直接实现安全功能，但它们可能会导致产品的安全功能失效，因而，贡献于安全执行的设备驱动程序为SFR-supporting部分，内核中也存在没有实现SFR的其他功能（例如，优化调度策略的负载管理器），也没有安全功能依赖于它，因而这些机制是SFR不相关的。针对应用程序也是相同的，“passwd”应用实现了更新用户口令的安全执行机制，这个应用包含了解析文件“/etc/passwd”的逻辑，它应属于SFR-supporting部分，当这种解析逻辑失败时，更新用户口令的安全执行功能也会失败。

2.3 产品安全功能接口（TSFI：TOE Security Functionality Inferface）

在产品的功能说明描述中，需要详细阐述所有TSFI的目的与方法，以及每个TSFI所有参数的描述，并且要对每个TSFI依据其所完成的功能来划分为SFR-enforcing TSFI、SFR-supporting TSFI或SFR-non-interfering TSFI。下面以Linux 操作系统与防火墙为例来进行说明。

- Linux操作系统

SFR-enforcing TSFI：系统调用（open, msgctl），应用的命令行（passwd, login），配置文件（/etc/passwd, /etc/shadow）。

SFR-supporting TSFI：非执行 TSFI 的系统调用。

SFR-non-interfering TSFI：应用的命令行（ls, rm），配置文件（vimrc）。

- 防火墙

SFR-enforcing TSFI：网络接口。

SFR-supporting TSFI：检验日志的接口。

SFR-non-interfering TSFI：N/A

2.4 针对自保护、域分离与防迂回的脆弱性分析

自保护、域分离与防迂回是TOE的特性。评估人员在做脆弱性分析时不仅要看直接支持这些特性的功能，而且还要以所有可能的方式与TSF交互以检查破坏与自保护、域分离与防迂回相关的安全目标的潜在方式。

在自保护实例中，评估人员检查影响TSF行为的潜在方式，这种潜在方式可能会导致TSF不执行部分安全策略。举例来说：TOE的TSF为每个用户进程包含一个数据结构，其中包含了用户的特权级别，紧邻特权级别的元素是一个用于统计进程已分配资源的32位计数器，通常进程不

会分配超过2^{16}的资源，因而计数器是足够大的，从而会存在这样的假定：在TSF内没有检查是否计数器达到了它的限制，那么用户能够通过导致进程分配资源数的内存溢出而潜在地操纵特权级别。

域分隔允许在一个域中存储域管理关键数据，这些数据应该被保护以禁止其它域的访问。举例来说，操作系统为所有激活用户存储关键用户数据（如密钥或口令）在一个特定域中，其它域的用户不可直接访问，仅能通过这个特定域提供的域间接口同步函数进行查询与修改操作，比如查询是否这个用户的数据已经存在这个特定域中，或者将一个新的用户数据加入这个特定域中。脆弱性分析时需要考虑这个域间同步函数是否进行很好的安全保护，比如是否仅在特权模式才能执行修改操作，而查询可以在任何模式，如果没有进行很好的保护则有可能导致用户口令或密钥的泄露。

3 结束语

CC标准是最为全面和公认的面向产品评估的信息安全评估标准，它已经被世界上诸多的国家所完全采用成为自己的信息安全评估标准，它可以用于评估任何具有安全功能的IT产品，包括智能卡产品、操作系统、数据库、无线通讯设备、数据通讯设备等等。我国虽然还没有加入CCRA（Common Criteria Recognition Agreement），但对产品的信息安全评估工作越来越重视，越来越多的厂商也认识到产品安全的重要性，为了更好的进入国际市场，很多产品的CC评估也势在必行，希望有更多的研发人员投入到CC的研究中来，为今后顺利完成相应产品的评估工作做出贡献。

参考文献

[1] Common Criteria for Information Technology Security Evaluation (CC), version 3.1 Revision 3, July 2009.

[2] CC 官方网站 http://www.commoncriteriaportal.org

[3] Red Hat Enterprise Linux 4 EAL4 High Level Design.