成卫青 1972 年生，女，南京邮电学院计算机系讲师，在职博士生。研究方向：网络安全和网络管理。
龚俭 东南大学计算机系教授，博导。

网络安全评估

成卫青[①②] 龚俭[①]
[①](东南大学计算机科学系 南京 210096)
[②](南京邮电学院计算机科学与技术系 南京 210003)

摘要：本文指出网络安全评估具有重要意义；然后给出参照CC的网络安全评估实施框架，重点讨论TOE评估依据——安全指标的建立，并给出EAL1级和EAL2级TOE评估的内容；最后说明实施评估还有很多问题有待考虑。

关键词：评估对象(Target of Evaluation) 安全目标 安全指标(Security Target) 安全功能要求 安全保证要求 评估保证级别 评估技术报告

1 引言

网络给人们带来很多便利，大大提高了人们的工作效率，因此应用越来越广泛。同时，随着各式邮件传播的病毒的出现，网络安全波及面越来越大。越来越多的用户希望对自己所用或将要用的网络产品或系统的安全性具有清晰的认识，但大多缺乏相关的知识、专家经验和资源，无法判定自己对网络产品或系统的安全性的置信度是否适当，而又不想在这方面完全依赖系统或产品的开发者，因此希望有第三方帮助分析其网络系统或产品的安全性，即进行安全评估。评估可使用户能够判断其网络产品和系统相对于自己的应用来说是否足够安全，其中隐含的安全风险是否可以接受。另外，有关管理部门为了保证国家信息基础设施的安全性，也要求对各种网络产品或系统进行安全评估，以确定其安全可靠程度。可见，对网络产品或系统进行安全评估很有必要，对网络发展也将具有重要意义。

本文第1节介绍评估意义，第2节介绍所参考的标准，第3节给出评估框架，第4节讨论安全指标的确定，第5节说明不同的评估保证级别包含不同的评估内容，最后是本文总结和进一步的工作。

2 评估标准

为使评估结果得到大家认可，网络安全评估应遵照国际标准。网络安全属于信息技术(IT)范畴，目前可依据的最新标准是 1998 年 5 月发布的，由加拿大、法国、德国、荷兰、英国和美国六个国家的七个政府组织制定的，信息技术安全评估通用标准 CC 2.1，它与 ISO/IEC 15408 兼容，及 CC 相关标准——信息技术安全评估通用方法 CEM 1.0。

CC定义了一组通用安全功能要求与保证措施要求，可引用作为网络产品和系统的安全性评估的根据，使评估的结论具有广泛的适用性和可比较性。CEM描述评估者在按CC所定义的标准和证据进行评估时所要执行的最小动作。

3 评估环境和过程

评估对象（TOE）是一个网络产品或系统及其文档，如一个计算机网络系统、一个防火墙、一个应用程序等。安全评估针对的是信息的机密性、完整性和可用性保护。为使评估结果间达到更大的可比较性，评估应在一个权威的评估方案框架内进行。评估方案规定所用标准，监督评估质量，并管理评估工具和评估者必须遵守的规章。不同的评估机构的规章框架之间应保持一致，以达到相互认可评估结果的

目的。图 1 描述组成评估环境的主要元素。

评估应该导出能够被引为证据的客观、可重复的结果，使用公共的评估方法保证了结果的可重复性和客观性，但仅此还不够。评估标准为各评估机构间相互承认评估结果提供技术基础，但标准的应用既包含客观成分也包含主观成分，如评估标准的许多部分要求运用专家判断和背景知识，在这方面一致性较难实现。因此为提高评估判决的一致性，最终评估结果可以提交给认证处理。认证处理是在应用安全评估标准中获得较高一致性的一个方法。认证处理对评估结果进行独立检查，得到最终的**证书或认可，**证书通常公开可用。运行评估方案的评估机构负责评估方案、方法和认证处理。

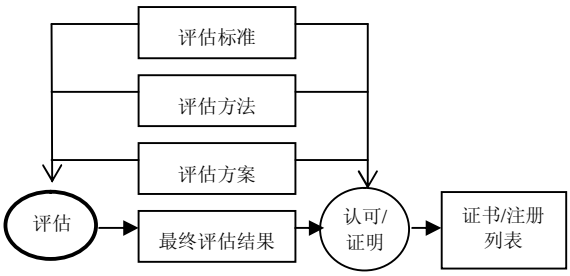

图 1 评估上下文

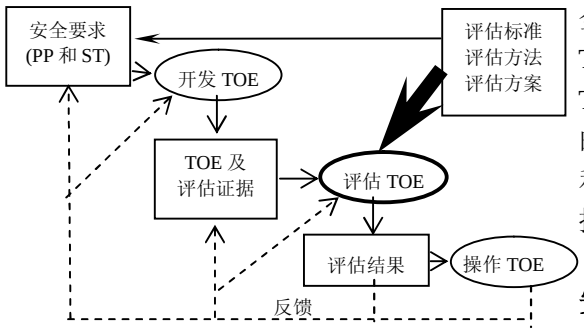

图 2 评估过程

对 TOE 的评估要遵循评估标准、评估方法和评估方案，并利用 TOE 开发过程中得出的证据，参见图 2。此外，评估结果可用于改善 TOE 的操作；而且若有可能还应将评估结果与 TOE 运转情况反馈用于修正安全要求（ST 和 PP）和环境假设或作为新的评估证据，进而对 TOE 予以再开发和再评估。

安全指标(Security Target)是一组安全要求和 TOE 汇总说明书，用作一个**特定 TOE** 评估的根据。保护子集(Protection Profile)定义用于**一类 TOE** 的与实现无关的一组安全要求，针对的是能够满足特定用户需要的一类 TOE。安全要求为满足安全目标(Security Objective)而设，描述对 TOE 所期望的理想的安全行为，描述用户能够通过直接与 TOE 交互或 TOE 对刺激的反应而检测到的安全属性。

4 确定安全指标

ST 描述对网络产品或系统的安全要求，其中可以直接引用 PP 陈述，PP 针对某类 TOE，而 ST 针对某个具体的 TOE，PP 针对一类 TOE，内容较少，其构建与 ST 的构建完全类似。ST 是 TOE 评估的依据，构建安全指标是 TOE 评估最重要的首要环节。构建方法是首先要分析并确定安全环境，然后确定安全目标，再参考 CC 安全要求类别确定安全要求，最后定义安全功能和保证措施。

4.1 分析安全环境

安全环境包括所有有关的法律、组织的安全政策、习俗、专家意见和知识，定义了使用 TOE 的环境。为确定安全环境，必须考虑：(1) TOE 物理环境；（2） 需要受 TOE 元素保护的资产，资产包括可直接查阅的资产，如文件和数据库，也包括间接有安全需求的资产，如授权证书和 IT 实现本身；（3）TOE 用途。

在调查安全政策、威胁和风险之后，确定**安全环境，包括：**

（1）关于 TOE 的使用和 TOE 的使用环境的假定；

（2）所有与 TOE 安全操作有关的对资产的威胁（并非所有威胁）；

（3）TOE 必须遵从的的组织安全政策。

4.2 确定IT安全目标

安全环境的分析结果用于陈述安全目标，安全目标应针对所有已标识威胁，涵盖已标识的组织安全政策和假定，还应反映声称的 TOE 用途。

确定安全目标的意图是提出所有的安全隐患，并声明直接由 TOE 或由其环境提出的安全因素。安全目标的确定将综合考虑设计意见、安全政策、经济因素和风险承诺决定。对于环境的安全目标常在 IT 领域内用非技术或程序性的方法实现；IT 安全要求只针对 TOE 及其 IT 环境的安全目标。

4.3 确定IT安全要求

IT 安全要求是将安全目标细化为一组对 TOE 的安全要求和对环境的安全要求，对 TOE 的安全要求包括对 TOE 的功能要求和对 TOE 的保证要求两部分。如果 IT 安全要求被满足，将保证 TOE 能够满足其安全目标。为提高可读性，表达安全要求可参照 CC 中定义的分类的功能要求和保证要求。CC 中安全功能要求和安全保证要求均分类，类又细分为族，族中包含不同的组件，组件由元素组成。

4.3.1 安全功能要求

功能要求是对那些特别支持 IT 安全的 TOE 功能的要求，它定义了想得到的安全行为。网络安全功能包括安全审计、源无否认、接收无否认、加密操作、密钥管理、用户数据保护、标识和鉴别、安全管理、保密、TOE 安全功能保护、资源利用、TOE 访问、信任路径/信道等。举例说明功能要求，例如为实现接收无否认，要求该安全功能提供一个方法保证在数据交换期间发送信息的主体拥有该信息被接收的证据；然后该证据可以被此主体或其它主体验证。

4.3.2 安全保证要求

对于给定的一组功能要求，保证程度可以有变化。CC 中预定义了几个等级渐增的评估保证级别(EAL)，每个 EAL 由若干保证组件构成。在陈述保证要求前应先决定评估保证等级，可以选用预定义的保证包 EAL，也可自行定义由适当的保证要求组成的保证等级。保证要求规定了评估者的动作，也即决定了 TOE 评估活动的内容。

网络安全评估将涉及到的保证要求包括：

- 配置管理保证类 配置管理防止对 TOE 的未经授权的增删改，从而保证 TOE 和用于评估的文档正是待销售的那些。
- 交付和操作保证类是为正确地交付、安装、产生、和启动 TOE 而设的保证要求。
- 开发保证类定义逐步细化 TOE 安全功能描述的要求。
- 指导文档保证类是对指导文档的要求。为管理员和用户安全地管理和使用 TOE，要求文档必须描述一切有关 TOE 安全应用的方方面面。
- 测试保证类包括测试的广度、测试的深度、独立测试、和功能测试四个方面的保证要求。测试有助于确定“TOE 安全功能要求是被满足的”；测试提供“TOE 至少满足 TOE 安全功能要求”的保证；对照说明书对子系统和模块的测试还可以导向 TOE 安全功能的内部结构。
- 弱点估计保证类讨论可利用隐蔽信道的存在性、误用或不正确配置 TOE 的可能性、战胜概率或排列机制的可能性、及在 TOE 开发或操作中引入可利用弱点的可能性。

4.4 TOE汇总说明书

对于一个特定 TOE 的评估，需要根据功能要求和保证要求建立 TOE 汇总说明书。它定义 TOE 安全要求的示例，应包括满足功能要求的安全功能和用来满足保证要求的保证措施。

5 TOE 评估

为查明 PP 和 ST 中表述的安全要求和 TOE 汇总说明书是否合理，是否可作为 TOE 评估有意义的根据，在 TOE 评估之前要先评估 PP 和 ST。

5.1 PP评估

如果 ST 中引用了 PP 声明，PP 要最先被

评估，PP 内容如图 3 所示。各个 PP 的评估方法与要求是一样的，与评估保证级别也无关，因为 PP 是一类产品或系统的安全要求描述，给出了在给定假设下实施安全政策和防御指定威胁所需的安全要求。评估的目的是显示 PP 是完备的、一致的，技术上完美。一个已评估的 PP 适宜被 ST 引用，作为待评估 TOE 安全要求的陈述。

一个完整的PP评估涉及的活动包括：

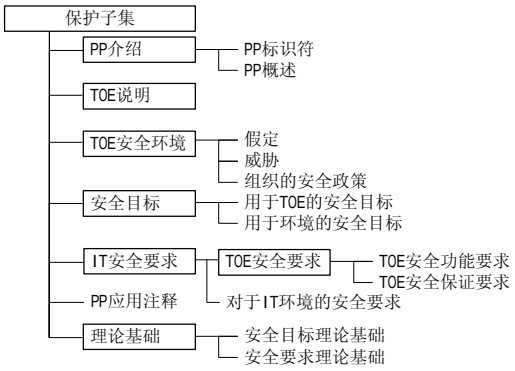

图3 PP内容

评估输入任务，该任务保证评估者能获得所需的，并得到妥善保护的评估证据，否则评估结果是不可信的；

- PP评估活动，包括下列子活动：评估TOE描述、评估安全环境、评估PP的介绍、评估安全目标、评估IT安全要求、评估显式指定的IT安全要求；
- 评估输出任务，评估的输出包括观察报告(OR)和评估技术报告(ETR)。另外由监督者负责保证评估报告的一致性。

评估者通过评估技术报告(ETR)提交裁定的技术判定，PP评估的ETR信息至少包括如下内容：

－介绍 评估者必须报告评估模式标识，为评估的监督提供依据；提供 ETR 配置控制标识，以标明具体的评估活动；提供 PP 配置控制标识，以表明评估的内容；提供开发者和发起者的标识，后者负责提供评估证据；提供评估者的标识，以表明评估的执行者和裁定的负责人。

－评估 评估者必须报告所使用的评估方法、技术、工具和标准；指出对评估的约束，以及所有可能影响评估结果的假设。

－评估结果 评估者必须报告对每个保证组件的裁定及其理由，表明这些评估证据如何满足或不满足评估标准的各个方面。

－结论和建议 评估者必须报告评估的结论，特别是总体的裁定。同时也可向监督者提出建议，包括在 PP 中发现的缺陷或特别有用的特性等。

－评估证据列表 评估者对评估证据要说明：提交者（如开发者或发起者）、名称、唯一的引用标识（如提交日期与版本号）。

－术语的缩略语 / 词汇表 评估者必须定义 ETR 中使用的各种符号与缩略语。

－观测报告 评估者必须完整地列出评估期间获得的所有 OR 及其状态。对于每个 OR，要给出其标识符，以及标题与内容摘要。

上述只定义了ETR的最少内容，具体的报告中可增加额外的内容和结构。

5.2 ST评估

ST 描述一个产品或系统的安全要求，并详细说明 TOE 所应提供的满足规定要求的安全功能与安全保证措施。ST 可以合并一或多条 PP 或声称遵从多条 PP。ST 还是开发者、评估者和用户（可选）各方商定 TOE 安全属性和评估范围的根据，ST 读者不限于负责 TOE 生产者和 TOE 评估者，还可包括负责管理、营销、购买、安装、配置、操作和使用 TOE 的那些人。ST 应呈交给用户，内容如图 4 所示。

对 ST 的评估先于各种 TOE 评估子活动，因为 ST 为这些子活动的执行提供了根据和上下文。在 TOE 的评估完成之前，可能无法对 ST 的评估作出最终裁定，因为子活动的评估结果和判决可能导致对 ST 的修改。各个 ST 的评估要求与方法是相同的，与 ST 的 EAL 无关。一个完整的 ST 评估包括的活动有：

- 评估输入任务；
- ST评估活动，包括的子活动有：TOE描述的评估、安全环境的评估、

ST简介的评估、安全目标的评估、PP声明的评估（可选）、IT安全要求的评估、显式陈述的IT安全要求的评估（可选）、TOE汇总说明书的评估。

- 评估输出任务。

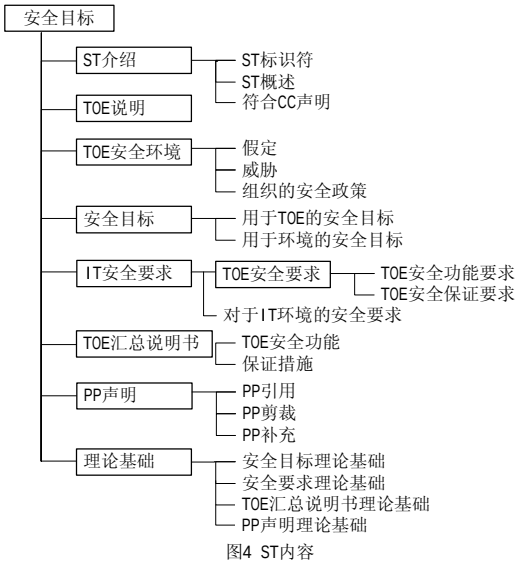

图4 ST内容

-

5.3 TOE评估

TOE 评估的目的是表明该 TOE 满足 ST 中定义的安全要求。如果评估结果显示 TOE 正确并有效地实现了 ST 中包含的所有安全要求，则 TOE 是满足安全目标的。

TOE 评估可以与开发过程并行,也可以随后。TOE 评估的主要输入有：

a) TOE证据集，包括作为TOE评估根据的已评估过的ST；
b) 要求评估的TOE；
c) 评估标准、方法和方案；
d) 其它丰富的资料及评估者与评估团体的IT安全专家意见。

评估过程期待的结果是证实 TOE 满足了 ST 中规定的安全要求。评估者可用一份或数份报告来表示根据评估标准确定的对 TOE 的裁决(通过、无结论、失败)，这些报告对于该 TOE 代表的产品或系统的实际用户或潜在用户以及开发者们都有用处。TOE 的评估技术报告与 PP 的类似。通过评估获得的置信度取决于所满足的保证要求(由评估保证等级决定)。

评估能够通过两种方式改善IT安全产品。其一，识别TOE中的差错和弱点，开发者可以改正以减少将来操作中故障发生的概率；其二，开发者在准备日后严密的评估中会更加关注TOE的设计与开发。可见，评估过程能够对初始要求、开发过程、最终产品以及运行环境施加强的、间接但积极的影响。下小节给出EAL1和EAL2级TOE评估内容，其它级别的TOE评估类似。

5.3.1 EAL1 级 TOE 评估

EAL1提供基本级保证。它使用功能与接口说明书和指导文档来了解安全行为，通过安全功能分析提供保证。本级安全功能分析要对TOE安全功能进行独立测试（非开发者进行的测试）。

EAL1评估包括：

- 评估输入任务，具体输入见上文；
- EAL1评估活动包括：1) 评估ST；2) 评估配置管理；3) 评估交付与操作文档；4) 评估开发文档；5) 评估指导文档；6) 独立测试安全功能；
- 评估输出任务（评估技术报告等）。

评估活动是从 EAL 的保证要求中导出的，测试是为了检查 TOE 安全功能要求是否被满足，测试的依据是与 TOE 汇总说明书一致的开发者提供的功能与接口说明书；而 EAL、功能要求和保证要求都是在 ST 的 IT 安全要求中声明的，TOE 汇总说明书也是 ST 的一部分，由此可见 ST 是评估的基础。

5.3.2 EAL2 级 TOE 评估

EAL2 提供中低级的独立安全保证。它使用功能与接口说明书、指导文档、以及 TOE 的高级设计来了解安全行为，通过安全功能分析提供保证。本级安全功能分析需下列支持：对 TOE 安全功能的独立测试、开发者基于功能说明书进行测试的证据、有选择地独立证实开发者测试结果、功能强度分析、以及开发者搜索明显弱点的证据。

EAL2 级评估包括：

- 评估输入任务；
- EAL2 的评估活动由下列子活动构成：评估 ST；评估配置管理；评估交付与操作文档； 评估开发文档；评估指导文档；评估开发者所进行的功能测试的广度；独立测试安全功能；评估 TOE 安全功能强度；评估开发者的弱点分析；
- 评估输出任务。

6 结束语

本文指出网络安全评估具有重要意义，介绍了网络安全评估所要涉及的内容，重点讨论了评估的关键——安全指标的确定，最后给出 EAL1 和 EAL2 级评估活动内容。然而真正进行网络安全评估还有很多工作要做，如，规范开发行为，研究各种用户需求制定出更多更可行的评估保证等级，测试工具的选用等等。

参考文献：

[1]http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF
[2]http://www.commoncriteria.org/docs/PDF/CCPART2V21.PDF
[3]http://www.commoncriteria.org/docs/PDF/CCPART3V21.PDF
[4]http://www.commoncriteria.org/docs/PDF/CEMV10.PDF

NETWORK SECURITY EVALUATION

CHENG Wei-Qing[①②], GONG Jian[①]

[①](Computer Science Dept., Southeast University, Nanjing 210096)

[②](Dept. of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003)

Abstract: In this paper the significance of network security evaluation is addressed, how to establish Security Target for a specific target of evaluation in accordance with CC is discussed, and then the steps for TOE evaluation conforming to the rules stated in CEM is provided.

Keywords: Target of Evaluation (TOE), security objectives, Security Target (ST), security functional requirements, security assurance requirements, Evaluation Assurance Level (EAL), Evaluation Technical Report (ETR)