DOI: 10.13656/j.cnki.gxkx.2001.03.003
广西科学 Guangxi Sciences 2001, 8 (3): 168~171

计算机安全标准演化与安全产品发展*
Evolution of Computer Security Evaluation Criteria and Progress in Computer Security Products

石文昌　　孙玉芳
Shi Wenchang　　Sun Yufang

(中国科学院软件研究所　北京　100080)
(Institute of Software, Chinese Academy of Sciences, Beijing, 100080, China)

摘要　分析计算机系统安全标准的演化过程，以及安全评价标准在安全产品评价中的实际应用情况。阐明在计算机系统安全标准演化中，TCSEG、ITSEC和CC是影响较大的主要标准；其中，CC标准是在各国寻求共同认可的安全评价标准的意愿驱使下产生的，它基于TCSEC等以往的标准，形式上更加接近于ITSEC。中国1999年颁布的2001年开始实施的“计算机信息系统安全保护等级划分准则”采用的是TCSEC的形式，其不可避免地存在与TCSEC同样的缺陷，按TCSEC标准的原有思路实施中国的标准，是否有利于安全产品的发展，值得认真深思。

关键词　计算机安全　安全评价标准　安全产品
中图法分类号　TP 309

Abstract　The evolution history of computer security evaluation criteria and the application of security evaluation criteria to the evaluation of security products are analyzed. The TCSEC, the ITSEC and the Common Criteria (CC) are of heavy weights on the progress of computer security evaluation criteria. The CC is the outcome of the quest of the United States, Canada, the United Kingdom and other countries to seek a basis for mutual recognition of security product evaluation. It is developed on the basis of all the older criteria and much more closely resembles the ITSEC. The Chinese Classified Criteria for Security Protection of Computer Information System (CCSPCIS), which was issued in 1999 and put into effect from 2001 on, inherits the philosophy of the TCSEC completely. The CCSPCIS is hence inevitably of the same drawback as the TCSEC. Whether shaping the Chinese security evaluation standard in accordance with the obsolete TCSEC is possible to advance the development of security products in China is in need of serious consideration.

Key words　computer security, security evaluation criteria, security products

安全评价是衡量安全产品安全性的重要手段，安全评价标准是安全产品评价的重要依据。安全评价标准的制定有引导安全产品发展方向的意图，特别是当政府或其他权力机构强制推行某一安全评价标准的实施时更是如此。安全评价标准在一定意义上具有安全产品发展的导向职责，正确的导向能促进安全产品的进步，有利于有效地解决计算机应用中可能面临的安全问题，不合理的导向不但起不到应有的作用，还会束缚安全产品的健康发展。

计算机技术的发展步伐以惊人的速度不断向前推进，计算机应用的范围不断扩大，随着第三代互联网时代的到来，计算机的应用将不断向纵深方向发展。技术的进步在为人们提供更大的应用潜力的同时，也为人们带来新的和更大的安全挑战。应用环境在变化，安全问题在变化，安全产品的性能也必须随之有所变化。在这样的技术和应用背景下，一个有生命力的安全评价标准应该能够反映安全产品处理旧问题和解决新问题的能力。

本文以C. P. Pfleeger提供的结果[1]为基础，考察计算机安全评价标准的历史演化情况，在R. E. Smith工作[2]的基础上，结合计算机安全产品评价的最新进展[3]，进一步分析安全评价标准在安全产品评价中的实际应用，探讨计算机安全评价标准的发展问题，对中国安全评价标准的状况提出一些值得讨论的看法。

2001-07-04收稿。
* 国家863高科技项目(863-306-ZD12-14-2)和中国科学院知识创新工程项目(KGCX1-09)资助。
该文最初交流于第十六次全国计算机安全学术交流会(2001年6月，四川成都)。

1 安全评价标准的演化

以文献[1]为基础,可以用图1来描绘国际上主要的安全评价标准的演化进程。图中刻画了各个标准颁布的年限。

作者认为,在计算机安全发展史上,J. P. Anderson在1972年发表的计算机安全技术规划研究报告[4]具有奠基石的作用,它不但提出了引用监控机、引用验证机制和安全核等根本思想,以及揭示安全规则的严格模型化的重要性,还提出了独立的安全评价方法问题。之后,D. E. Bell和 L. J. La Padula提出了著名 Bell & La Padula模型[5,6],该模型在 Multics系统中得到了成功实现,至今仍是实施保密性强制访问控制的基础。70年代中后期在安全 Multics上的努力及其他相关的工作标志着计算机安全进程的开端。

在以上成果的基础上,美国国防部于1983年颁布了第一个计算机安全评价标准 TCSEC[7]。该标准用可信计算基(TCB)描述计算机系统中的安全支持机制,在高安全等级的要求中追求实现具备引用验证机制和安全核性质的 TCB。在 TCSEC的影响下,德国、英国、加拿大等在80年代后期陆续推出了各自的标准,欧洲各国的标准最终发展成统一的欧洲标准 ITSEC[8]。90年代初,看到 TCSEC中的不足,美国制定了联邦标准草案,但没有实施就放弃了,转而与欧洲国家和加拿大等联合制定了 CC标准。1999年,CC标准被确立为国际标准[9],TCSEC随即被宣布废弃。

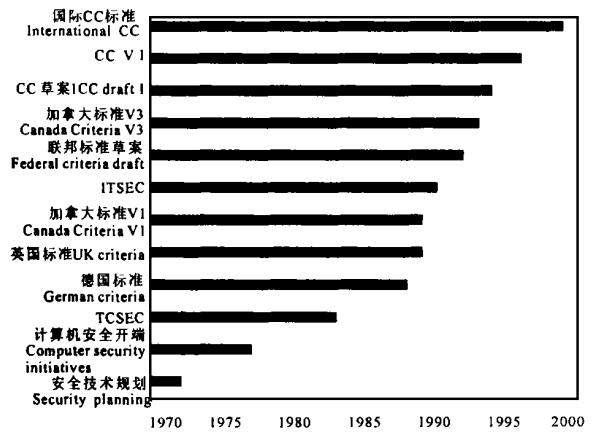

图1 计算机安全评价标准的颁布历程

Fig. 1 Evolution of computer security evaluation criteria

2 安全产品的历史评价情况

制定安全评价标准的目的在于对安全产品的安全性进行评价。根据 R. E. Smith提供的结果[2],我们可以得出如图2所示的安全产品在1984至1999年间的评价情况。

图2总评价曲线反映通过评价的安全产品总数,新评价曲线反映对以前没有评价过的产品进行的评价,再评价曲线反映对以前已评价过的产品的新版本的再度评价情况。总的来说,通过评价的产品数呈逐年上升的趋势,但1990年和1994年有两次较大的波动,这两年的增长幅度特别大。通过图3,可看到新评价和重复评价的产品占总评价产品的百分比情况。

1987年以后出现产品的重复评价,新评价产品数占总评价产品数的百分比的评价值为62%,重复评价产品百分比的平均值为38%。

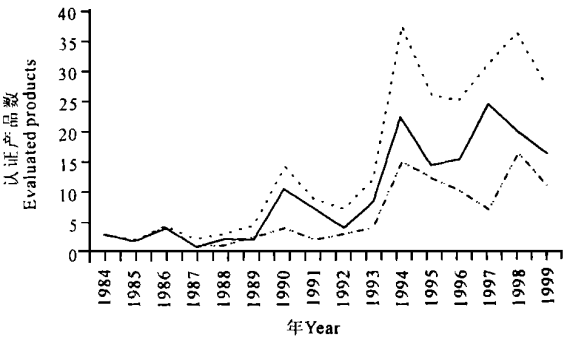

图2 各年度通过评价的安全产品数

Fig. 2 Number of evaluated products from 1984 to 1999

—— 新评价 New evaluation; …… 总评价 Total evaluation; _·· _·· _ 再评价 Repeat evaluation.

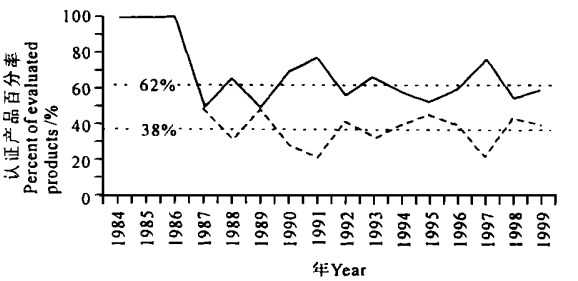

图3 新评价与重复评价的比率对比

Fig. 3 Percentage of new evaluation and repeat evaluation products from 1984 to 1999

—— 新评价 New evaluation; …… 再评价 Repeat evaluation.

TCSEC、ITSEC和 CC是影响较大的几个主要标准,通过这些标准的产品情况如图4所示。以这三个标准评价的产品总数为基准,各个标准评价的产品数所占百分比情况如图5所示。

到1987年为止,只有 TCSEC一个标准在起作用,1988年起,情况发生了变化。实际上,1990年起,ITSEC的作用已超过了 TCSEC,只有1992年例外。而自1993年起,ITSEC占有压倒的优势,TCSEC直走下坡路,实际上已逐步被 ITSEC和 CC取代。

在评价的产品类型方面,我们有图6的结果。1988年之前,评价的产品100%是操作系统,1988年开始

有其他产品参与评价。到1989年止，操作系统的评价比例都处于绝对优势，但从1990年起，操作系统比例的优势已经丧失（1992年例外）。1996年起，其他产品的比例已转为绝对优势，这反映出人们已把解决安全问题的主要注意力从操作系统转移到了其他产品之上。

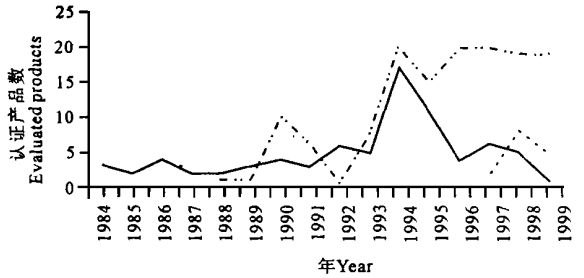

图4　3个标准评价产品的情况

Fig. 4　Products evaluated against TCSEC, ITSEC and CC from 1984 to 1999

—— TCSEC; …… CC; —··—··— ITSEC

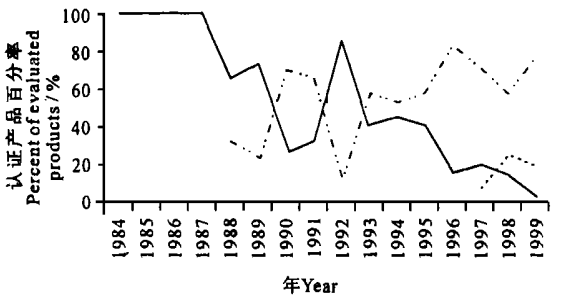

图5　3个标准评价产品的百分比

Fig. 5　Percentage of evaluated products against TCSEC, ITSEC and CC from 1984 to 1999

—— TCSEC; …… CC; —··—··— ITSEC

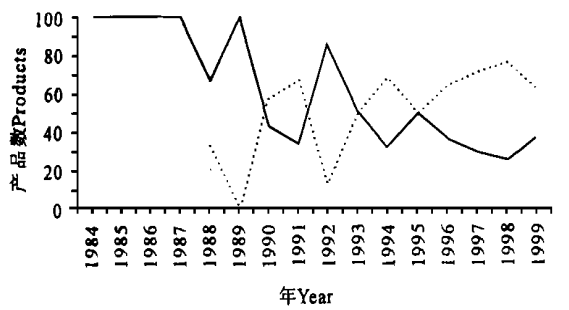

图6　评价的产品类型比较

Fig. 6　Percentage of evaluated product classes from 1984 to 1999

—— 操作系统 Operating system; ……其他产品 Other products

3　执行CC标准的安全产品评价情况

CC标准1999年成为国际标准，到2000年，已有美、加、英、德、法等13个国家签署了CC标准认可协定。根据最新公布的CC标准安全产品评价信息[3]，我们得到图7、图8、图9的结果。

通过CC标准评价的产品数逐年增加，与图4反映的情况略有差别，这与当时公布的CC标准评价信息有关。美、加、英3国评价的产品数走在前列，美国遥遥领先。所有评价产品都是非操作系统类产品，绝大多数是防火墙产品，其次是其他安全工具软件。

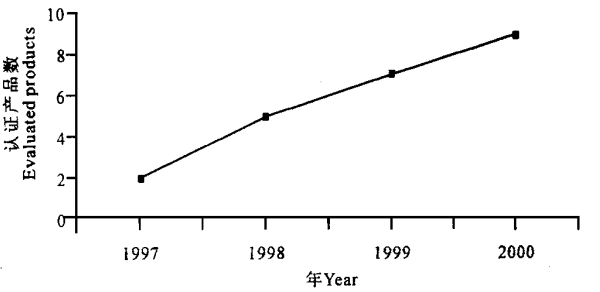

图7　CC标准评价产品数

Fig. 7　Number of products evaluated against CC from 1997 to 2000

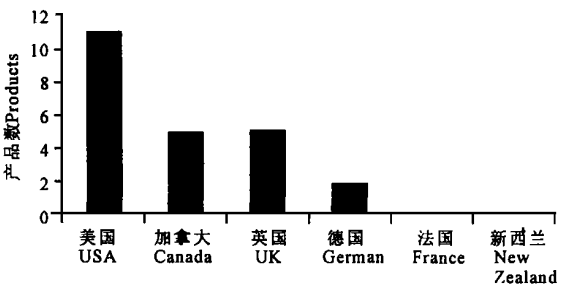

图8　各国实施CC标准评价的产品数

Fig. 8　Number of CC evaluated products in different countries

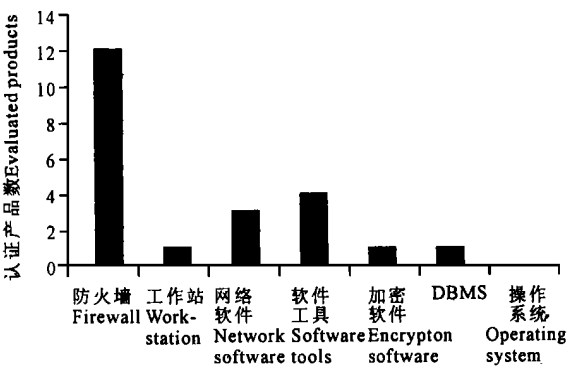

图9　通过CC标准评价的产品类型

Fig. 9　Product classes evaluated against CC

4　结语

计算机安全产品的评价是计算机安全评价标准实际应用和发挥作用的体现，综合过去10多年安全标准颁布和安全产品评价的实际事例，有助于把握安全标准和安全产品的发展情况。

TCSEC颁布初期，由于以前从未有过其他标准，人们纷纷以它作为安全产品的规范，集中大量的力量按照该标准开发和评价安全产品。随着开发和评价经验的不断积累，人们发现按照TCSEC开发和评价产

品的难度和投入非同小可,而且用户反映该标准所规定的安全功能所针对的并不是他们实际应用中迫切需要解决的问题。

90年代,互联网的兴起、发展和应用的扩大,安全问题显得更加突出、形式更加多样,ITSEC的推出,提供了一种比较灵活地表达安全问题和进行安全评价的手段,加上以前在操作系统上所付出的努力并未能达到人们预想的效果,人们试图探讨其他的安全解决途径,这促使 ITSEC和非操作系统产品的评价迅速占据了绝对的优势。

CC标准是在各国寻求共同认可的安全评价标准的意愿驱使下产生的,它是在 TCSEC等以往的标准的基础上制定出来的,形式上更加接近于 ITSEC,为安全需求的表达提供了更加灵活和规范的手段,更有利于应对层出不穷的新的安全问题,因而很快得到了越来越多的技术先进国家的支持。

对比发现,中国 1999年颁布的、200l年开始实施的相应标准—— 计算机信息系统安全保护等级划分准则[10]—— 采用的是 TCSEC的形式,除了增加非常简单而有限的有关数据完整性和网络信息传输等的要求外,所规定的安全功能完全等同于 TCSEC所规定的安全功能。作者认为,中国的这个标准不可避免地存在与 TCSEC同样的缺陷,要在 TCSEC已被颁布国废弃的情况下采用该标准的原有思路实施中国的标准,是否有利于安全产品的发展,是一个值得认真深思的问题。

参考文献

1 Charles P Pfleeger. Security in Computing. Second Edition. Prentice Hall PTR, 1997.

2 Richard E Smith. Trends in Government Endorsed Security Product Evaluations. 23rd National Information Systems Security Conference, Baltimore, Maryland, USA, Oct 16- 19, 2000.

3 The National Information Assurance Partnership. Common Criteria NIAP Validated Products List. http: //niap. nist. gov/cc- scheme/ValidatedProducts. html, Mar 2001.

4 James P Anderson. Computer security technology planning study. Vol II. ESD-TR-73-51, Vol II. Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01730, Oct. 1972.

5 David E Bell, Leonard J LaPadula. Secure computer systems: mathematical foundations, ESD-TR-73-278, Vol I, AD 770 768, Electronic Systems Division, Air Force Systems Command, Hanscom AFB, Bedford, Massachusetts, Nov 1973.

6 David E Bell, Leonard J LaPadula. Secure computer system: unified exposition and MULTICS interpretation, MTR-2997 Rev 1. The MITRE Corporation, Bedford, MA 01730, Mar 1976.

7 Department of Defense. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Washington, DC, Dec 1985.

8 Information Technology Security Evaluation Criteria. Version 1.2 Office for Official Publications of the European Communities, Jun 1991.

9 Joint Technical Committee 1. Evaluation Criteria for IT Security. ISO/IEC 15408: 1999 (E). The International Organization for Standardization and the International Electrotechnical Commission, 1999.

10 中华人民共和国国家标准. 计算机信息系统安全保护等级划分准则. GB 17859-1999, 中国, 1999年 9月 13日.

(责任编辑: 蒋汉明)

巴西生产生物柴油

据科学时报报道,巴西东北部塞阿拉联邦大学教授帕伦特经20年研究,以蓖麻油为原料,生产出一种污染程度低、可再生的生物柴油。

在帕伦特教授的领导下,塞阿拉、皮奥伊和里约热内卢联邦大学和工业技术中心基金会的研究人员以氢氧化钠为催化剂,研制出生物柴油。在这种化学反应中产生的丙三醇也可为工业所用。

经巴西各汽车制造厂利用30万公升生物柴油进行的实验证明,这种柴油可用于各种发动机,也可用于发电机,而且无需对发动机进行改装。但由于蓖麻油的黏度比较大,在使用时需将20%的生物柴油混入80%的普通柴油。

研究人员在巴西常年干旱的东北部建立的蓖麻试点种植区已获得成功。在那里建立的第一家生物柴油厂已经开工,预计在90天内日产量将达到2000至3000公升。

研究中还发现,除蓖麻外;任何植物油,如豆油、花生油、玉米油等,以及动物油,如鱼油等,都可制成生物柴油。研究人员目前正在大力推广生物柴油的生产,以便减少石油进口。同时,这一发现也将为常年干旱的巴西东北部地区带来福音,当地政府已决定为农民种植蓖麻提供帮助,以增加他们的收入。