浅议可信计算的发展

朱海卫[1]，施蕾[2]
([1]北京信息技术应用研究所，北京 100091；[2]中国信息安全测评中心，北京)

【摘　要】可信计算已成为信息安全行业的热点之一。文章介绍和分析了可信计算的背景以及国内外可信计算的发展现状，认为可信必须建立在自主的基础之上，呼吁国内可信计算行业应重点加强可信的操作系统、软件应用环境建设，最终实现“自主、可控”的安全目标。

【关键词】可信计算；信息安全；自主；可控
【中图分类号】TP393.08　　【文献标识码】A　　【文章编号】1009-8054(2009) 03-0079-03

Development and Prospects of Trusted Computing

ZHU Hai-wei[1], SHI Lei[2]
([1]Institute of Beijing Information Technology Application, Beijing 100091, China;
[2]China Information Technology Security Evaluation Center, Beijing 100085, China)

【Abstract】Trusted computing has become one of the hot issues in inforsec industry. This paper describes the history of Trusted Computing and analyzes the development of Trusted Computing both at home and abroad, then it suggests that the trusted computing must be based on independence, and proposes that the domestic industry of trusted computing should emphatically strengthen the trusted operating system and software application environment.

【Keywords】trusted computing; information security; independence; controllable

0　引言

可信计算已成为信息安全行业的热点之一。当前，国内可信计算行业一直将工作重点放在可信链的硬件(可信平台模块)研发方面，较少去关心可信链中的操作系统、应用软件环境的建设。

本文作者通过调研分析，认为可信必须建立在自主的基础之上，提出“安全 = 自主 + 可控”的理念，并呼吁国内可信计算行业应重点加强可信的操作系统、软件应用环境建设，最终实现“自主、可控”的安全目标。

收稿日期：2009-02-16
作者简介：朱海卫，1979年生，研究方向：信息安全、计算机技术应用；施蕾，1980年生，研究方向：信息安全、网络安全技术。

1　可信计算的由来

1999年，由Intel、惠普、康柏、微软、IBM等计算机巨头联合发起，成立了“可信计算平台联盟”(TCPA)，最初基于反盗版目的，并提出了“可信计算”(Trusted Computing)的概念。2003年3月，可信计算平台联盟(TCPA)更名为可信计算工作组(TCG))，成员也扩大到200多个，遍布全球各大洲。2001年1月TCG发布了可信计算平台标准规范；2003年10月，TCG更新了TPM核心规范，目前最新为1.2版，之前被称为1.1b。规范要求符合TPM的芯片首先必须具有产生加解密密匙的功能，此外，还必须能够进行高速的资料加密和解密，以及充当保护BIOS和操作系统不被修改的辅助处理器。

从另外一个角度上讲，可信计算工作组(TCG))旨在对整个系统建立完整性保护，通过安全芯片架构与软件保护，从根本上提高终端乃至整个网络系统的安全性。其要求首先是建立一个信任根，信任根的可信性由技术安全和管理

安全同时保障。通过信任根建立信任链，一级保护一级，一级信任一级，从而把信任扩大到整个系统，成为信息安全的整体解决方案[1]。

专家们相信，利用“可信计算”技术构建通用的终端硬件平台，建立可信的信任链传递模式，可以增强计算机体系结构的安全性。“可信计算”所体现的终端安全思想，已成为发展信息安全的重要理念。

2 我国的可信计算研究现状

2004年6月，武汉瑞达推出国内首台基于TPM的计算机产品。2005年1月，我国成立国家安全标准委员会WG1可信计算工作小组，专门规划相关标准。2008年4月底，中国可信计算联盟(CTCU)在国家信息中心成立，沈昌祥、何德全院士担任CTCU顾问，吴亚非为CTCU秘书长。CTCU的成立标志着中国在可信计算领域的一次成功尝试。

当前，国内可信计算行业一直将工作重点放在了TPM研发上，取得了非常大的成果。2005年至2008年间，武汉瑞达、清华同方、北大方正、联想、兆日、长城电脑等公司纷纷推出基于安全计算芯片(TPM)的可信计算机产品。据国内某大学研究所对国外与国内相关产品进行标准符合度测试后发现，国外产品基于TPM 1.2标准的符合度远不及国内产品，在这种程度上可以说，我国的可信平台模块技术及产品化已经处于国际领先地位[2]。

2005年，某权威机构曾预测：未来几年，中国安全PC市场将呈现爆炸式增长的趋势。其中，2006年安全PC将占据整个PC市场份额的10%-15%，而到2007年，这一数字将达到50%左右。2008年12月，有杂志曾报道称：2008年将有70%的笔记本和40%的台式机装配可信安全芯片，而到2010年，这一数字将有望达到100%。这些预测均基于可信芯片的装配数量，而基本没有涉及可信应用方面。一个装配了可信安全芯片的计算机并非等于安全PC。

国内可信计算行业的这种“重硬件轻软件”的现状，加大了可信计算机在国内推广的难度。究其根本原因，就是当前主流的操作系统、应用软件环境大多为国外掌握核心技术，对国内用户不可信。因此，可信计算行业应重点加强可信的操作系统、应用环境建设，最终实现“自主、可控”的安全目标。

3 可信等于可控，而非安全

从国家信息安全战略层次上讲，可信并非意味着安全。

在国际标准ISO/IEC 15408中对可信给出了以下定义：一个可信(trusted)的组件、操作或过程的行为在任意操作条件下是可预测的，并能很好地抵抗应用程序软件、病毒以及一定的物理干扰造成的破坏。从这个角度看，可信计算仅仅是保护用户机器内的数据不能以用户(特别是软件开发商、内容提供商等)所不希望的方式被他人访问。可信是期望做到一个实体在实现给定目标时其行为总是如同预期一样的结果，强调行为的结果可预测和可控性。对于国家信息安全，只有在自主的前提下实现可预测性和可控性，才是我们想要的安全。

可信传递链是这样的：主机→可信芯片→可信CPU→可信Bootloader→可信操作系统→可信应用。

在这个可信链中，可信操作系统与可信应用才是安全的核心体现。“所有的事情都是进程干的，包括坏事”。我们只有实现操作系统和应用程序的“自主、可控”，才能真正让一个计算机只运行“我”的东西。

4 安全 = 自主 + 可控

对于信息安全，以“自主、可控”的原则来衡量，在没有“自主”的前提下实现“可控”，后果是非常可怕的。可信计算解决的是不可信代码不能运行的问题，也就是说，可信计算不能检查一段可信代码是否有漏洞，只能检查这个代码是否是某一注册软件商比如微软开发的，是，即表示可信。

而且，可信计算无法检查代码是否是恶意代码，假设某注册软件商要做恶意代码，对目标网络或设备形成攻击，那么该恶意代码是不能被可信计算检测出来的。近期闹得沸沸扬扬的微软反盗版黑屏事件就很好地说明了“非自主的可控”的严重后果。

宣称完全实现可信计算的新一代微软操作系统Vista，在安全性方面确实有很大增强，这意味着黑客、病毒的入侵更加困难。但中国科学院倪光南院士认为Vista的‘安全’并不等于我们所要的“信息安全”，如果以信息安全的“自主、可控”原则来衡量，Vista将比以前的所有Windows版本更加不“可控”。

代码的可信度校验基本上都是由操作系统调用TPM接口来完成，而当前我国自主的操作系统远远达不到可信计算的要求。因此，在国外公司全面掌握核心技术的前提下推广使用可信计算，等于将我们的全部信息公开，这并非我们想要的信息安全。

通过对武汉瑞达、清华同方、北大方正、联想、兆日、长城电脑等公司陆续推出的可信计算机产品调研，我们可以发现除武汉瑞达以外，当前其他可信计算机产品的功能主要集中在完整性度量、敏感数据的加密存储、身份认证

功能、内部资源授权访问、数据的加密传输等方面，其可信都是基于微软操作系统的可信基础之上，与我们“自主、可控”的要求相差甚远。武汉瑞达开发了专用的操作系统和应用软件，其基本方向是正确的，但其产品化程度远达不到当前用户的需要。

由此可见，当前的可信计算厂商只注重芯片的研发，其对于操作系统、应用软件开发的投入远远没有达到我们当前对可信计算机的安全要求，实现“自主、可控”的信息安全还尚需时日。

5 可信计算未来发展展望

可信计算是基于TPM而建立的，其核心算法都在TPM内部完成，安全性高，配合可信的操作系统、应用软件，可以从底层根本上实现信息安全，彻底杜绝病毒、木马等恶意代码的困扰。当前，我国的TPM产业已初具规模，技术领先。然而，作为可信链中的核心体现环节，操作系统与应用软件环境远没有达到自主、可控的目标，使得可信计算在市场上未能有效推广。

基于此，本文作者认为，当前的可信计算在信息安全体系中，仅仅能作为一个基础平台服务设施，提供标准接口，供合法的进程进行访问、使用，从而提供高强度、安全的密码服务。

要使可信计算在国内得到大规模的应用推广，就必须实现操作系统、应用软件环境的“自主、可控”，不解决这个问题，就无法从根本上解决安全的问题，这也是下一步可信计算行业的发展重点，不解决这个问题，就无法从根本上解决安全的问题[3]。

6 结语

总之，面对国际IT巨头们以强化自身垄断与控制地位为目的而推行的可信计算，我们应该积极研究、认真应对，借鉴其优秀的技术思想，在自主的前提下，发展可控的可信计算体系，重点建设自主的可控软件应用环境，才是我们应该选择的正确道路。

参考文献

[1] 李晓勇，韩臻，沈昌祥. Windows环境下信任链传递及其性能分析[J]. 计算机研究与发展，2007，44(11).
[2] 樊静淳. 论可信计算的研究与发展[J]. 济南职业学院学报，2007，(03).
[3] 沈昌祥. 坚持自主创新加速发展可信计算[J]. 计算机安全，2006，(06).

(上接第78页)

过某个阈值，则标记为正面，否则为负面。第二种方法是把加权向量的各维求和，通过阈值来判定倾向性。第三种方法是机器学习的方法，效果最好。我们通过支持向量机的学习算法，训练出分类器来判定文本的倾向性。3种评价方法的召回率和正确率如表1所示。

表1 3种评价方法的召回率和准确率比较

方法	原始向量统计和		加权向量统计和		支持向量机	
	正面	负面	正面	负面	正面	负面
召回率	69.70%	69.40%	71.50%	70.60%	82.20%	81.40%
正确率	69.49%	69.61%	70.86%	71.25%	81.55%	82.06%

3 结语

本文结合句法分析技术和知网知识，提出了一种基于主题相关性分析的文本语义倾向性研究新思路。在系统实现过程中，采用了一种新的文本向量表示方法，即以名词对象作为向量维，以与该名词对象相关的主观性词汇倾向性评分加权和作为该维的向量值。实验数据表明，新的模型具有较好的召回率和正确率，在内容安全领域具有良好的应用前景，而我们下一步的工作包括分析程度副词对词汇倾向性的加强或减弱作用，以及动词、副词等的语义倾向，以期取得更好的判别准确率。

参考文献

[1] V Hatzivassiloglou, K McKeown. Predicting the Semantic Orientation of Adjectives[A]. In:Proceedings of the 35th Annual Meeting of the ACL[C]. New Jersey：ACL，1997：174-181.
[2] Peter D Turney. Thumbs Up or Thumbs Down Semantic Orientation Applied to Unsupervised Classification of Reviews[A]. In:Proceedings of the 40th ACL[C]. New Jersey：ACL，2001：417-424.
[3] 徐琳宏，林鸿飞，杨志豪. 基于语义理解的文本倾向性识别机制[J]. 中文信息学报，2007，21(01)：98-102.
[4] 刘永丹，曾海泉，等. 基于语义分析的倾向性文本过滤[J]. 通信学报，2004，25(07)：80-87.
[5] 董振东，董强. 知网[EB/OL]. [2008-08-01]. http：//www.keenage.com.