关于发展我国信息安全的几点建议

冯登国*

(软件研究所信息安全国家重点实验室　北京　100080)

关 键 词　信息安全, 建议

随着我国信息技术的迅速发展, 计算机和网络已经广泛应用到国民经济和社会生活的各个领域及部门, 成为国家事务、经济建设、国防建设、尖端科技等重要领域管理中必不可少的工具和手段。与国家经济命脉密切相关的金融、外贸、铁路、民航、交通和气象等专用计算机网络已经建成。目前, 我国的信息化建设正蓬勃发展, 并极大地促进了文化教育、科学技术的对外交流和经济发展, 给人们的学习、工作、生活带来了极大的方便, 降低了企业、政府的管理成本, 提高了管理效率。在肯定信息技术改善了人们的生活、促进了社会进步的同时, 我们也不得不承认, 伴随信息技术发展的信息安全问题也日益突出。

政府加大了对信息安全建设的投入; 信息技术各领域的大批专家也开始转入信息安全领域的研究; 受媒体影响, 普通老百姓也开始讨论信息安全, 哪怕他们可能还不知道计算机网络为何物。

信息安全虽然重要, 但不能过分炒作, 评价要中肯。只有给大家一个正确的认识, 才能真正提高全民的信息安全意识。

1　注重应用的同时, 加强基础研究

信息安全的竞争表现为高技术的竞争, 信息安全技术是各国竞相争夺的制高点。我国信息技术基础薄弱, 缺乏核心技术, 许多产品的技术水平远远落后于信息技术发达的国家, 甚至一些关键性产品我们仍然没有能力自主开发。虽然国家在信息安全方面的投入有所增加, 但我国在这方面的基础研究水平却呈下降趋势。为了避免永远落后的被动局面, 我们在注重应用技术研究的同时, 必须加强基础研究。

基础研究是核心技术突破的关键, 要有突破就必须有创新, 不能老是跟着别人的思路走。但创新是有风险的, 一种思路是否可行, 需要研究、分析和试验才会有结果。国内目前好像对于研究立项的项目只允许成功, 不允许失败, 过于关心最后结果, 而忽略了研究过程。其实, 研究、论证过程本身就应该是一种研究成果。只强调最后的定论, 会限制研究人员的思路, 使他们不能放开去做真正的研究, 怕承担风险, 而只去申请一些已有定论的东西, 做一些修修补补的工作。基础研究要想有新的突破, 就应该对敢于创新的人给予支持, 当然也应该注意项目审查方式, 不能让一些滥竽充数的人蒙混过去。

2　加强人才培养和培训的力度

信息系统的安全性很重要的一点是人员素质, 管理人员的安全意识和技术水平直接影响到整个系统的安全性。目前, 已有许多成熟的安全技术、安全产品, 但能否让这些技术和产品在实际应用中充分发挥作用, 关键还在于我们如何规划、组织及配置, 这些都是和管理人员与工程技术人员的素质分不开的。

现在的企事业单位普遍存在专业人员缺乏的

* 软件研究所信息安全国家重点实验室主任, 国家计算机网络入侵防范中心主任, 博士生导师
收稿日期: 2002 年 5 月 13 日

问题。特别是对于一些关系到国计民生的大型企业与国家机关,更是应该建立一支强有力的信息安全专业队伍。因此,我们应该加强人才培养力度,根据信息安全的特殊性和各种不同人才需求层次,进行有针对性的培养和培训,为国家信息安全建设培养一支实力强劲的专业队伍。

信息安全技术需要的人才是多方面的,必须针对不同的要求采取不同的培养方式。像网管、应急响应等技术性人才,实践性很强,知识的时效性也很强,仅学习书本知识是远远不够的。因此,我们要多提供实践的机会,尽量提供接近实战的模拟环境,让他们在实践过程中提高,掌握最新的知识和技术。

3 加强学科建设,增强师资力量

由于信息安全方面的专业人才需求越来越大,相关高校和研究机构都加强了信息安全专业人才的培养,部分高校已经设立信息安全本科专业。实际上,在当前状况下设立信息安全本科专业,条件还不是很成熟,有许多问题亟需解决,如学科的设置、教材的内容和教学方式等人才培养过程中非常重要的环节。

既然木已成舟,我认为,目前信息安全学科应以现有的相关学科(如应用数学、计算机和通信)为基础,结合信息安全自身的特色来设置课程和研究方向。

教材建设是培养人才的一个重要环节,尤其是教材内容的合理性和新颖性十分重要。教材的质量直接影响学生的质量。目前,国内已有很多有关信息安全方面的书,但大部分书的专业性太强,适合于研究生使用而不适用于本科生,教材的种类也不够齐全。国外的教材很多,内容上虽有一定的参考价值,但大部分不适合国内教学使用,需要本土化。因此,编写适合于本科生使用的信息安全专业的主干教材已刻不容缓,但在编写过程中,应特别注重"本土化"和"内容安排的合理性"。

一本好的教科书的形成需要经过多个环节的考验,如内容安排、文字表述、学生接受程度等。要完成好上述这些教科书的编写,需要大批一流的、在一线执教的教师参与。因此,摆在我们面前的任务是十分艰巨的。

信息安全专业的教学必须要重点强调课堂教学与实验课的有机结合,但国内很多培养单位目前还不具备最起码的实验条件。

总而言之,既然大家热衷于建设信息安全学科,就应该为建设该学科做一份贡献,多做一些思考,不要只赶时髦,否则会误人子弟。

4 建立健全自主的信息安全标准体系

信息安全产品向标准化方向发展是一个主要趋势。标准化主要指密码算法的标准化、安全协议的标准化、安全机制实现的标准化以及应用编程接口的标准化。信息安全是个动态的、持续的、整体的、系统的概念。信息安全系统的各个部件必须通力合作,才能实现整体的安全功能。在安全系统的各个环节中,任何一个环节都不允许有差错。而各安全部件要能协调工作,就必须遵从统一的标准和规范。世界各国,尤其是信息技术较为发达的国家,都为信息安全领域陆续建立了许多标准。美国早在 70 年代就有了其加密的标准——数据加密标准(DES)。80 年代中期,美国国防部为适应军事计算机的保密需要,制定了"可信计算机系统安全评价标准"(TCSEC),此后又对网络系统、数据库方面做出了系列安全解释,形成了安全信息系统体系结构的最早原则。90 年代初,英、法、德、荷联合提出了包括保密性、完整性、可用性概念的"信息技术安全评价标准"(ITSEC)。近年来,六国七方共同提出了"信息技术安全评价通用准则"(CC for IT SEC)。2001 年,美国新一代的数据加密标准 AES 也已出台。

标准化的工作对于推动信息安全产品的应用,实现不同信息安全系统组件的互连和互操作,保证企业间公平、合理的竞争以及促进信息安全产业的良性发展,将起到决定性的作用。如果安全产品的厂商各自遵从一套独立的准则,则整个安全业将陷入混乱的局面而无从发展。因此,我们必须统一规划、统一建设,为信息安全系统的设计、生产、评估和使用提供一套健全的标准体系。

国外在这方面已有许多成功的经验,我们可以借鉴国外已有的标准体系的成果,但不能完全照

搬，而必须深入地进行分析研究。因为许多标准化的东西并不一定是最科学的，有些仅仅是因为相关产品占据了市场，而根据该产品制定的标准。各国的信息化水平不一样，对信息安全的要求也存在着差异。因此，我们必须根据实际情况，建立适合自己需求的标准体系。

此外，我们必须进行一些前瞻性研究，提出自己新的标准体系，不能总是跟在别人后面，处于落后被动局面。实际上，标准的研究是一项长期而艰巨的任务，技术含量很高，需要高水平的科研和技术人员的介入。

5　完善和健全信息安全法律法规体系

如同现实社会一样，网络社会也需要一套法律法规体系来维持正常秩序。由于我国信息化的发展程度较为落后，有关信息技术、信息安全的法律法规也不健全，不能适应现代信息时代的需要。我们必须全面规划信息安全立法工作，逐步完善信息安全法律法规体系。组织专家全面分析和评估现有法律法规体系对信息安全技术发展的适应性问题，提出对现有法律法规体系的调整意见；组织信息安全和法律专家共同研究信息安全立法问题。随着信息安全技术的发展，针对执法过程中出现的新情况、新问题，加强信息安全执法队伍的建设，确保信息安全法律法规的有效实施。

6　加强信息安全基础设施建设

信息技术是计算机、数学、通讯、物理等相结合的高科技领域，而信息安全除了涉及信息技术，还涉及管理、法律等诸多领域。对于许多中小企业来说，建立自己独立的信息安全机构负责所有相关的安全事务是不可行的。一则，自身实力不够，再则，各自建设也是不必要的浪费。我们应该把一些可以分离的基本安全服务由一些专业化机构来提供，这样，既减少了投入，又提高了安全服务质量。因此，发展专业化的服务机构，对于有效防范和及时解决各类信息安全问题是必不可少的。在这方面国外有一些有益的做法，我们应该认真借鉴，结合国情做积极的探索。

信息安全基础设施是信息安全建设的关键，也是政府的建设重点。我们应根据国内信息化建设的实际需求，建立健全相应的密码服务体系、数字证书授权体系、密钥管理体系、信息系统安全性与安全产品评估体系、应急响应与事件恢复体系等信息安全基础设施群，向社会提供全方位的信息安全保障服务。

7　根据实际需要进行信息安全建设

信息安全与其它科学和技术一样，还存在许多有待解决的问题，但我们不要过分夸大信息安全问题的威胁，否则会造成不必要的浪费，会导致信息恐怖现象。信息基础设施不发达的地方不应过多强调信息安全的建设，只是在建设时要从总体上有所考虑。要根据实际的保护需要，根据自己的不同特点，制定相应的安全防护策略，采购相应的安全保护产品，不应一味强调安全的高强度、高量级。我赞成“适度安全”这种提法。

独立自主地发展我国的信息安全产业，推动信息安全研究，是维护国家安全和利益的需要，是支撑信息产业迅猛发展，推进国家经济信息化进程的需要，也是提高我国综合国力、独立自主地进行现代化建设的需要。虽然我国在信息安全领域还存在许多问题，但我们要正确面对，一切从实际出发，冷静思考，寻找实际、有效的解决方案，推动国家信息安全建设。