信息安全的现状和展望*

Present State and Prospect of Information Security

魏仲山
（天津大学，教授）

提　要　作者从广义信息保护概念将信息安全技术发展分为三个阶段。第一阶段，信息安全只涉及信息存储和处理过程。第二阶段，安全对策是使信息内容难懂而不易被识破。第三阶段，安全问题是由共享数据和程序引起的，传统方法已不能应付由此引起的威胁。作者提出以存取、隔离、加密、信息流向和推断控制原理作为信息安全学的基础理论，以解决机、网、库内包括计算机病毒在内的整个应用领域的安全问题。

一、现　状

信息是把数据加工成知识、智慧过程中的一个主要阶段。数据是信息的原材料，是一堆数字或符号的总结。信息是依据某种目的组织起来、经过加工处理和具有一定结构的数据总括。知识是经过整理、分析、评论和验证的一堆信息。智慧是一种不断显露出的、又经历与客观现实经常对照而得到充实的知识。信息具有非物质性。它存在于人脑，包括观察到的和记忆中的一切事物以及由分析、归纳得到的结果。信息资源不同于自然资源。后者不依附于人的观念而独立存在，前者则是人的观念的反映。信息技术的飞速发展已经使国民经济各个应用领域的数据采集、处理和扩散活动汇聚成“信息工业”。其产值已占工业发达国家生产总值的一半以上，而且还在增长。计算机如此广泛和深入的应用已经将人类社会的财富、机密和智慧汇集于一体，成为高度文明社会的基础和支柱。但是，当代计算机信息系统突出的问题是其安全保护已脆弱到“不堪一击”的地步。

早在六七十年代，计算机安全问题已屡见不鲜。在艾德里安·诺曼（Adrian R. D. Norman）所著《计算机不安全性》（Computer Insecurity）一书中列有百起案例。其中1973年发案的一起损失就达10亿美元。在以军用计算机为代表的国家安全领域内，80年代北约组织的所有活动都采用计算机。在计算机信息系统内存储有高机密数据。北约利用它们来控制飞机、舰艇、武器和作战部署。为防止电子间谍窃密，北约花费了上亿美元。1987年5～7月，前西德电脑迷攻入美国国家航空和航天局（NASA）所属“空间物理分析网”。该网连接全世界1 600多台计算机，向NASA提供有关航天研究、核物理和分子生物学的情报。这些电脑迷通过“航天飞机”、“挑战者”号和“机密”这类单词攻入NASA数据网，接着在屏幕上他们看到了有关“航天飞机C研究合同”、“系统安全调查”和“助推火箭事故”等机密，并逐步渗透直到获取所有数据库资料，并随意操纵存储在这些数据库内的所有情报。

在以银行计算机为代表的商用安全领域内，1988年前西德公民丢失欧洲支票（蓝色塑料支票卡）达15万张。仅在西班牙被案犯兑走的就约3万张。据前西德联邦刑事警察局估计，总的损失约达6 000万西德马克。其中90%的损失由银行和保险公司承担。遍布法国巴黎街头的自动付款机（ATM）是各大银行为方便顾客而设置的。取款人只要把自己银行信用卡插入ATM并通过电子检测器检验核实，然后根据所需现金额按一下按钮，就可迅速从ATM提取出现款。法国一个犯罪团伙利用伪造信用卡在巴黎各处ATM内窃走近150万法郎现钞。据法国警方调查，这一团伙共5人，主犯精通电子技术，设计了一套能骗过ATM电子检测器的伪卡。他们一共制作了165张伪卡用于作案。另外，当前国际商品竞争的一大威胁是冒牌货。据美国工商界估计美国每年损失达200亿

* 国家自然科学基金资助项目。

美元。其中尤以伪造计算机软件为甚。因为软件研制费很高，但再生产（复制）费却很低。例如，在美国伪造的软件在美国卖价约为500美元，而在亚洲售价却不到10美元。围绕以计算机软件为主体的智力产权纠纷已在世界范围内爆发。形成新潮流的高科技到处出现。没有智力产权要想赶上新潮流是不堪设想的。

80年代中期，计算机病毒就已出现。1988年11月初，美国一位25岁的计算机专家研制成名为Worm（"蠕虫"）的病毒程序，使约6 000台与美国著名ARPA网络连接的计算机，包括NASA、军事要塞和横跨美国本土的几十所主要大学的计算机工作陷于瘫痪。从此，计算机病毒威震整个世界。计算机病毒是指一个能传染其他程序的程序。它是靠修改其他程序并把自身的拷贝嵌入其他程序实现的。计算机病毒起源于共享、信息流传递和解释通用性。当今一个有实用价值的信息系统都必须具备这些特点。所以，只要有计算机的普及应用，就免不了有病毒产生和蔓延；只要有计算机间的信息共享，就免不了有计算机病毒的传染。计算机病毒所以难以对付，关键也在于此。

面对各种安全威胁，传统的安全对策忙于招架却毫无还手之力。当务之急是重新制定符合新形势的安全对策。

二、历史和转折

研究信息安全的历史可以追溯到古代。早在我国春秋战国时期（约公元前473年），相传吴越交战，城池久攻不下，后因城防图被窃而战败灭国。这里讲的"城防图被窃"也就是"信息遭泄密"。可见保护信息机密何等重要。"保密"也就成为信息安全的同义语。千百年来这种观念世世代代沿用下来。为达到保密目的而采用的密码学一直被视为一种神秘技巧。电子计算机问世至今还不到半个世纪。计算机信息安全首先在军用领域倍受关注。就信息存储、处理和传输而言，信息在传输过程中受到的安全威胁最大。计算机网络的实体防护最为薄弱。对此，用密码学方法对传输信息加密，就成为最有效的手段。它也是当今公认的计算机安全热门课题。

近十余年来，事实上在新材料、超大规模集成电路、微电子技术、光电子技术、系统技术和软件技术有重大突破基础上，通信技术和信息处理技术已经融合而成为不可分割的领域。随着信息化社会主体从硬件转向软件，只从过去的工业产权范畴保护人类合法权益已显得不适应。用法律保护以软件为主体的智力产权。已是国际社会发展的总趋势。

在这个总趋势下，本文在分析信息特征及其活动规律的基础上，提出广义信息保护概念，它把信息安全技术的发展分为三个阶段。第一阶段资源共享范围为单台计算机。计算机信息安全只涉及信息存储和处理过程。早期单用户独占计算机资源时，只要做好实体防护，安全问题就不复存在。多用户使用计算机时，应保证不同用户各进程并发执行而互不干扰。为此，安全对策是把各进程占用的存储空间划分成物理或逻辑上相互隔离区域（隔离控制）。另外，不论对信息存储（如文件存储）或处理（如程序执行），均需通过存取控制对用户进程合法性作鉴定和授权。第二阶段资源共享范围为计算机通信网络。这时除存储和处理外，信息尚需传输。利用传输线路或远程终端易于作案。其安全对策并非以授权为基础，而是使信息内容难懂且不为对手识破（加密控制）。在开放式环境下，实际上计算机网络所受到的安全威胁更为严重和复杂。它分为被动和主动攻击两类。被动攻击旨在破坏信息机密性，主动攻击旨在破坏信息真实性或完整性。两者的作用均是双重性的。前者不易发觉，但易制止；后者不易制止，但能发觉。加密仅对前者奏效，后者则需靠鉴定。鉴定技术采用加密口令字（证明件）。数字签名是鉴定用户或进程合法性更为一般的手段。在计算机和网络融合的基础上，把数据库广泛应用与之结合，就形成资源共享范围为机、网、库结合为一体的新阶段，即第三阶段。

这一阶段突出的安全问题是由共享软资源引起的。它分为共享数据和程序两类。就共享数据而言，一个主体不信赖另一个与其共享存取权的主体，就出现可疑问题。前者猜疑后者滥用存取权而把所共享的数据非法扩散给其它主体。此处出现的是信息传递而非存取权转让。这是存取控制力所不及的，要由信息流向控制决定。影响数据库内数据安全的因素很多。如果存取控制机构把共享资源当作语义上相关的实体集合处理，则数据安全性不仅有赖于对受保护实体的存取，也有赖于对语义上与受保护实体相关的推断实体的存取。统计数据库安全性不由存取控制而由推断控制决定。

共享程序要比共享数据引起的安全问题更复杂。这是因为共享（或租用）程序内能够埋伏可疑程序段。它利用未在程序说明中描述的功能，取得调用环境下复制、滥用或破坏系统（或用户数据）的权利。它也可以是计算机病毒。为获取对系统的非法存取权，可疑程序段常利用系统程序内设置的入口点或陷门。租用专利软件的安全问题有，软件主猜疑租用人偷专利程序，租用人猜疑软件主偷输入专利程序的机密信息，彼此互相猜疑。减少可疑程序段安全威胁而采取的一项措施是，把租用程序压缩到只为完成其任务而无任何多余存取权的小保护域内。即使这样，也不能保证不走漏信

息，不出安全问题。只有对租用程序采取禁锢措施，存取控制单独使用才能奏效。抵御计算机病毒的根本措施是隔离。隔离既可保证信息的完整性，也有助于制止病毒的传染。

综上所述，长期以来解决计算机安全问题的方法，多半是以密码学为基础的专门防护措施。它们限于运用若干分散规则得出直觉知识与实验安全效果，而每一种这样的规则又只限于特定的应用领域。显然，它无法应付机、网、库面临的形形色色威胁。随着知识积累及其应用领域的拓宽和深化，在广义信息保护范畴内，笔者提出少量却强有力的综合规则取代以往各种分散规则。这就是把存取、隔离、加密、信息流向和推断控制原理（即"五论"）作为安全学的基础理论，旨在全面系统解决机、网、库内包括计算机病毒在内的整个应用领域的安全问题。毋庸置疑，这将是由工业化向信息化社会转变过程中重要的一步。

三、信息安全学的形成

信息的共享和保护、破坏和安全、扩散和保密互为条件，相互制约。安全学研究机、网、库内数据安全的方法。信息安全性指不因人为疏漏和蓄谋作案而使信息被泄露、窜改或破坏。它的中心目标是反泄密、反窜改和反破坏。任何一个信息系统的安全问题都可以归结为对信息占有权（存取权）的合法性和信息内容本身的安全（即防泄密、防窜改和防破坏）两个方面。安全学的五论就是围绕这两个方面提出的基础理论。

保护信息占有权的合法性（授权）是安全学的核心问题，因为它是信息化社会对智力产权保护的直接体现。存取控制原理就是授权理论。理论上可以证明，无绝对安全的授权系统存在。但是，这不排除能找到使安全易于处理的实际条件，从而使一个授权系统有相对安全性。隔离是常用的信息保护方法。它把计算机硬件和软件资源分割成若干互斥部分，达到互不干扰的安全效果。隔离与共享是互为条件的。一方面，完全隔离就失去共享。另一方面，隔离法又使若干并行进程对非共享资源实现共享成为可能。虽然，隔离法是多进程共享资源的根本方法。但是，就机、网、库内有多种隔离层的复杂共享系统而言，估计它的安全效果并非易事。加密控制原理（即密码学）是一种最为古老的安全方法学。在存取控制力所不及的情况下，它对保护信息安全特别奏效，但伴有较高代价。加密控制基于对手从截获信息中不能求出唯一的密码解。利用信息论的随机加密模型，描述截获密文和一次攻击成功间的概率关系。随机加密模型是以假设"只从密文破译"为基点。事实上估价现代密码保密度时应以"已知明文破译"、"可选用明文破译"和"可选用密文破译"为基点。后者较前者易于破密。所以，现代密码只能有相对保密度。许多信息泄漏问题并非授权系统失控，而系缺乏信息流向策略所致。后者涉及信息传递而非权的转让。为保证信息流向安全，把客体划分成不同密级并对主体设置相应许可证。只具有许可证的主体对相应密级客体的信息存取才为合法。利用经授权状态定义安全信息流向，就有可能为存取控制和信息流向控制制定统一的安全策略。这也是对以存取控制为基础的授权系统的完善和扩充。在满足授权条件下，通过查询数据库（如统计数据库）会有失密威胁存在，表现为从获取授权信息群体推断出未经授权个体信息，从无机密信息群体推断出个体机密信息。推断控制原理是制止这类威胁的基础理论。然而，描述推断机制的方法很难。为统计数据库安全，在工程上简化推断控制模型很有必要。

存取控制为占有信息的授权理论，它与信息内容本身不相干。反之，加密控制使信息内容难懂，以不为对手识破，它与授权并无直接关系。信息流向控制涉及信息传递并非是权的转让。若对手借机"滥用授权"，则就有使信息流向失控而达到顺手牵羊的作案目的。推断控制面临的威胁是，在满足授权条件下，利用可获取信息内容而推断出机密信息。实质上，这是因"滥用信息内容"引起的失密。基于互斥原理的隔离控制以牺牲信息共享为代价，使信息互相隔离而达到保护信息安全的目的。由此可见，上述"五论"采取的安全对策并非孤行，而是相互依赖和补充，达到综合防治的安全效果。它们大致覆盖了整个应用领域内的安全问题。这标志信息安全学作为一门新兴学科已经形成。在当前，它尤其适用于以军用计算机为代表的国家安全领域（机密密集型）和以银行计算机为代表的商用安全领域（财富密集型）。

四、结　语

为适应向信息化社会过渡总趋势，本文提出广义信息保护概念。这是以资源共享范围为界把信息安全技术划分成三个不同发展阶段。其中以第三阶段共享软件资源引起的安全威胁尤为复杂和严重。在这种环境下，不再以传统密码学应用为核心，而代之以信息化社会保护智力产权为基点的信息授权理论为核心；不再把安全对策局限于防范计算机犯罪，而是拓宽为信息化社会中信息活动规范化准则。

在此基础上，本文提出安全学"五论"，为安全学作为一门新兴学科奠定理论基础。这也为全面系统防治包括计算机病毒在内的各种安全威胁开辟一条新途径。

（责任编辑　孙立明）